Padjadjaran Law Review
Volume 13, Nomor 1, 2025
P-ISSN: 2407-6546 | E-ISSN: 2685-2357
DOI: https://doi.org/10.56895/plr.v13i1.2212
Submitted: March 30th, 2025| Published: July 14th, 2025

Upaya Penguatan Hukum Pelindungan Data Pribadi Dalam Keamanan Transaksi Menggunakan Dompet Elektronik Melalui Penerapan *Zero-Knowledge Proof*

Annisa Monica[*], Cahya Yulianti[**], Azzahra Nurintiara[***]

Abstrak

Perkembangan teknologi mendorong transformasi terhadap berbagai aspek kehidupan manusia, mencakup transformasi metode transaksi yang semula dilakukan secara konvensional kini mulai beralih kepada transaksi digital. Dompet elektronik hadir sebagai salah satu bentuk transaksi digital yang menawarkan kemudahan dan efisiensi dalam bertransaksi. Namun terdapat tantangan keamanan dan perlindungan data pribadi pengguna dikarenakan tingginya kerentanan kebocoran data di dalam aplikasi dompet elektronik. Artikel ini mengkaji regulasi perlindungan data pribadi di Indonesia dalam konteks keamanan transaksi menggunakan dompet elektronik menggunakan metode penelitian yuridis normatif. Penulis mengusulkan penerapan metode *Zero-Knowledge Proof* (ZKP) untuk meningkatkan perlindungan data pribadi pengguna layanan dompet digital. Untuk mendukung inovasi tersebut, diperlukan pembaruan regulasi, antara lain pembentukan otoritas pengawas independen (DPA), penambahan persyaratan persetujuan eksplisit atas transmisi data lintas negara dalam UU PDP, serta penyusunan regulasi teknis yang mewajibkan penggunaan ZKP sebagai bagian dari standar keamanan transaksi digital di Indonesia.

Kata Kunci: dompet elektronik, pelindungan data pribadi, *zero-knowledge proof*.

Strengthening Legal Protection for Personal Data in Transaction Security Using Electronic Wallets Through the Implementation of Zero-Knowledge Proof

Abstract

Technological developments are driving transformations in various aspects of human life, including the transformation of transaction methods that were originally carried out conventionally, now starting to shift to digital transactions. E-wallets have emerged as a form of digital transaction, offering convenience and efficiency in financial activities. However, challenges concerning the security and protection of user's personal data arise because of the high risk of data breaches within e-wallet applications. This article examines the legal framework of Personal Data Protection in Indonesia regarding securing transactions through e-wallets, employing a normative juridical research method. The author proposes the implementation of the Zero-Knowledge Proof (ZKP) method to enhance the protection of personal data for e-wallet service users. To support this innovation, several regulatory reforms are required, including the establishment of an independent data protection authority (DPA), amendments to require explicit user consent for cross-border data transfers under the Personal Data Protection Law, and the formulation of technical standards mandating the use of ZKP as a security protocol in digital transaction systems in Indonesia.

***Keywords**: e-wallet, data protection, zero-knowledge proof.*

[*] Fakultas Hukum Universitas Padjadjaran, Jl. Raya Bandung Sumedang KM.21, Hegarmanah, Kec. Jatinangor, Kabupaten Sumedang, Jawa Barat 45363, annisamonica1@gmail.com.

[**] Fakultas Hukum Universitas Padjadjaran, Jl. Raya Bandung Sumedang KM.21, Hegarmanah, Kec. Jatinangor, Kabupaten Sumedang, Jawa Barat 45363, cahya21001@mail.unpad.ac.id.

[***] Fakultas Hukum Universitas Padjadjaran, Jl. Raya Bandung Sumedang KM.21, Hegarmanah, Kec. Jatinangor, Kabupaten Sumedang, Jawa Barat 45363, azzahra21007@mail.unpad.ac.id.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

PENDAHULUAN

Perkembangan pesat teknologi mengubah berbagai komponen kehidupan manusia, salah satunya adalah perkembangan transaksi digital. Transaksi digital mengacu kepada setiap transaksi yang dilakukan tanpa memerlukan uang tunai (kertas) dari awal hingga akhir transaksi yang melibatkan teknologi di dalamnya.[1] Adanya era teknologi yang disruptif ini merevolusi pasar tradisional yang memberikan tantangan besar kepada industri yang telah terbentuk untuk beradaptasi atau akan tergerus oleh zaman.[2] Pemanfaatan teknologi dilakukan oleh perusahaan *Financial Technology* (Fintech) untuk mempersingkat proses, meningkatkan aksesibilitas, dan solusi yang inovatif untuk individu dan bisnis melalui transaksi digital.[3]

Salah satu bentuk dari transaksi digital adalah transaksi menggunakan dompet elektronik. Dompet elektronik merupakan sebuah layanan berbasis aplikasi yang berfungsi menyimpan data dan instrumen pembayaran seperti untuk melakukan berbagai jenis transaksi, seperti melakukan pembayaran secara daring, pembelian barang, pembayaran tagihan, hingga mengirim uang.[4] Dompet elektronik memiliki kemiripan dengan dompet biasa yang dimiliki individu yang berfungsi untuk menyimpan uang, namun yang menjadi pembeda adalah kemampuan dompet elektronik untuk melakukan transaksi secara instan sehingga memberikan kemudahan dan efisiensi kepada penggunanya. Selain itu dompet elektronik juga memiliki beberapa kelebihan lainnya seperti kemudahan untuk mengakses tanpa harus terbatas dengan jam kerja dari penyedia layanan dompet elektronik, terdapat promo yang ditawarkan oleh pihak penyelenggara layanan, hingga pencatatan transaksi yang akurat sehingga memberikan kemudahan dalam melakukan pelacakan detail transaksi.[5]

Secara sederhana, cara kerja dari dompet elektronik adalah dengan memindahkan saldo dari akun konsumen ke akun pebisnis.[6] Dalam bekerja, dompet elektronik menggunakan beberapa teknologi termasuk di dalamnya aplikasi seluler, perangkat keras seluler, *Near-field communication* (NFC), dan metode keamanan seperti tokenisasi.[7] Untuk dapat digunakan, pengguna dompet elektronik perlu memasukkan informasi yang diperlukan untuk mengaktivasi akun dompet elektronik yang kemudian informasi tersebut dienkripsi sehingga hanya dapat digunakan oleh pengguna yang mengotorisasinya.[8] Terdapat beberapa jenis teknologi yang populer untuk digunakan di dalam dompet elektronik, yakni *QR Code* (QR), *Magnetic Secure Transmission* (MST), dan NFC. QR memberikan kode informasi ke dalam bentuk pola hitam putih yang dapat diakses pengguna dengan kamera ponsel pintar atau dengan sistem pemindaian dompet elektronik untuk melakukan transaksi.[9] NFC bekerja menggunakan sinyal elektromagnetik kepada perangkat keras pengguna agar dapat berbagi dan mentransfer data saat berada dalam jarak dekat.[10] Sedangkan MST bekerja dengan menggunakan sinyal magnetik

---

1 GoCardless, "Digital transactions: what are they?", https://gocardless.com/guides/posts/what-are-digital-transactions/#what-is-a-digital-transaction, diakses pada Juli 2024.

2 FasterCapital, "How Technology is Disrupting Traditional Markets", https://fastercapital.com/content/How-Technology-is-Disrupting-Traditional Markets.html#:~:text=Traditional%20methods%2C%20such%20as%20cash,online%20transactions%20seamless%20and%20efficient, diakses pada Juli 2024.

3 *Ibid.*

4 Fitriyani Puspa Samodra, "E-Wallet adalah dompet elektronik, Ketahui Jenis dan Kelebihannya", https://www.liputan6.com/hot/read/5439316/e-wallet-adalah-dompet-digital-ketahui-jenis-dan-kelebihannya, diakses pada Juni 2024.

5 *Ibid.*

6 Digibank, "*E-Wallet*: Manfaat dan Cara Kerjanya", https://www.dbs.id/digibank/id/id/articles/e-wallet-manfaat-dan-cara-kerjanya, diakses pada Juni 2024.

7 Kinza Yasar, "*Digital Wallet*", https://www.techtarget.com/whatis/definition/digital-wallet, diakses pada Juni 2024.

8 *Ibid.*

9 *Ibid.*

10 *Ibid.*

P-ISSN : 2407-6546
E-ISSN : 2685-2357

yang memiliki kemiripan dengan cara kerja strip magnetik pembaca kartu kredit.[11] Dalam menggunakan dompet elektronik, pengumpulan data pribadi menjadi hal yang penting. Hal ini dikarenakan pengguna dompet elektronik diperlukan untuk mengisi data pribadi konsumen sebelum melakukan transaksi.[12]

Minat masyarakat Indonesia terhadap penggunaan dompet elektronik dari tahun ke tahun semakin meningkat secara masif.[13] Pada semester pertama tahun 2019 saja, Bank Indonesia (BI) mencatat bahwa nilai transaksi menggunakan uang elektronik telah melampaui lima puluh enam triliun rupiah melalui berbagai platform, termasuk dompet elektronik.[14] Berdasarkan riset Insight Asia pada tahun 2022, sebanyak 71% responden aktif menggunakan dompet elektronik.[15] Hal yang mempengaruhi peningkatan minat terhadap dompet elektronik tersebut adalah kemudahan dalam bertransaksi, kenyamanan, kecepatan, kepercayaan, keamanan, inovasi, hingga promosi yang dapat menguntungkan pengguna.[16] Selain dari keuntungan dan layanan yang ditawarkan oleh platform dompet elektronik, perkembangan dompet elektronik di Indonesia semakin berkembang semenjak pandemi Covid-19 juga membuat masyarakat yang semula melakukan kegiatan secara tatap muka, kini melakukan semua dari rumah dengan memanfaatkan kecanggihan teknologi.[17]

Dibalik dari manfaat dalam bertransaksi menggunakan dompet elektronik, terdapat beberapa tantangan yang perlu diatasi, yakni tantangan dalam pelindungan privasi pengguna, data, akses internet dan tata kelola, gap skill, pembuatan kebijakan di era digital, hingga keamanan siber.[18] Penggunaan dompet elektronik berbasis aplikasi internet memberikan kemungkinan adanya *error* dalam aplikasi yang membuat saldo dari pemilik akun menjadi hilang.[19] Seperti kasus yang menimpa Akromi pada bulan Maret 2023 yang kehilangan saldo dompet elektronik dalam aplikasi DANA lebih dari enam ratus ribu rupiah.[20] Hal ini terjadi dikarenakan adanya transaksi tidak dikenal dalam akun dompet elektronik DANA milik korban.[21] Hal serupa pun pernah terjadi kepada Nur sebagai pengguna dompet elektronik aplikasi ShopeePay yang kehilangan saldonya sebesar empat ratus tiga puluh enam ribu rupiah secara tiba-tiba tanpa adanya rincian jenis transaksi.[22]

Saat ini, Indonesia telah mengatur perlindungan data pribadi pengguna dompet elektronik melalui sejumlah regulasi, antara lain Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik beserta perubahannya, Undang-undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi dan Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang

---

11 *Ibid.*

12 Nurul Adiyah, (et.al.), "Perlindungan Data Pribadi Pengguna dompet elektronik OVO", *Journal of Islamic Economic Law,* Volume 6, Nomor 1, 2021, hlm.77, https://ejournal.iainpalopo.ac.id/index.php/alamwal/article/view/3706.

13 Desvronita, "Faktor-faktor Yang Mempengaruhi Minat Menggunakan Sistem Pembayaran *E-Wallet* Menggunakan *Technology Acceptance Model*", *Jurnal Akmenika,* Volume 18, Nomor 2, 2021, hlm.1, https://journal.upy.ac.id/index.php/akmenika/article/view/2142/0.

14 Damasha Khoiri Clevalda, Dona Budi Kharisma, "Perlindungan Hukum terhadap Nasabah dompet elektronik Oleh Bank Indonesia", *Privat Law Journal,* Volume 9, Nomor 1, 2021, hlm. 2, https://jurnal.uns.ac.id/privatlaw/article/view/41483.

15 Almadinah Putri Brilian, "Survei: 71% Orang RI Pakai dompet elektronik, Mana yang Paling Laris?", https://finance.detik.com/fintech/d-6433675/survei-71-orang-ri-pakai-dompet-digital-mana-yang-paling-laris, diakses pada 8 Juni 2024.

16 Desvronita, *Loc.cit.*

17 Rosa Anggreati, "Perkembangan E-wallet di Indonesia dan Manfaat Sehari-hari", https://www.medcom.id/ekonomi/bisnis/ob34oX8k-perkembangan-e-wallet-di-indonesia-dan-manfaat-sehari-hari, diakses pada 8 Juni 2024.

18 Damasha Khoiri Clevalda dan Dona Budi Kharisma, *Loc.cit.*

19 *Ibid.*

20 Akromi, "Saldo DANA Hilang, Customer Service Tak Bisa Membantu", https://news.detik.com/suara-pembaca/d-6709588/saldo-dana-hilang-customer-service-tak-bisa-membantu, diakses pada 8 Juni 2024.

21 *Ibid.*

22 Nur, "Saldo ShopeePay Hilang Tanpa Kejelasan, CS Shopee Berbelit-belit", https://mediakonsumen.com/2023/04/29/surat-pembaca/saldo-shopeepay-hilang-tanpa-kejelasan-cs-shopee-berbelit-belit, diakses pada 8 Juni 2024.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

Nomor 7 Tahun 1992 Tentang Perbankan.[23] Secara umum, Undang-Undang tersebut mengatur hak pengguna dompet elektronik serta kewajiban penyelenggara dompet elektronik sebagai Penyelenggara Sistem Elektronik (PSE) dalam menjaga kerahasiaan data pribadi pengguna dompet elektronik guna melindungi keamanan data pribadi dan mencegah terjadinya sengketa.[24] Bank Indonesia (BI) berupaya untuk memberikan perlindungan transaksi digital melalui pembentukan Standar Nasional Open API (SNAP) untuk menjadi standar keamanan transaksi digital di Indonesia. Adanya standarisasi ini dilakukan untuk memastikan bahwa semua penyedia layanan mematuhi protokol keamanan yang ketat.

Sayangnya hukum positif di Indonesia belum melindungi transaksi digital secara komprehensif. Selain kurangnya regulasi dan pedoman yang memadai, tingkat literasi digital masyarakat Indonesia masih rendah yakni berada dalam tahap mampu.[25] Hal-hal tersebut menjadi celah bagi pihak tidak bertanggung jawab dalam melancarkan kejahatan siber dengan mengakses akun pemilik dompet elektronik secara tidak sah untuk kepentingan dirinya.[26] Tulisan ini akan membahas tiga hal utama, yakni yang pertama mengenai mengenai perkembangan regulasi perlindungan data pribadi dalam keamanan transaksi digital di Indonesia, kedua mengenai peningkatan Standar Nasional OpenAPI sebagai standarisasi keamanan transaksi dompet elektronik, dan urgensi pembaharuan regulasi dalam rangka penguatan hukum perlindungan data pribadi keamanan transaksi digital menggunakan dompet elektronik. Dalam industri kriptografi, terdapat metode *Zero-Knowledge Proof* (ZKP) yang digunakan sebagai metode verifikasi informasi tanpa mengharuskan adanya pengungkapan konten informasi tersebut.[27] Dengan karakteristik tersebut, ZKP berpotensi menjadi solusi untuk mencegah penyalahgunaan dan kebocoran data pribadi dalam layanan dompet elektronik. Diharapkan penerapan metode ZKP sebagai standar dalam penyimpanan data pribadi oleh penyedia layanan dompet elektronik dapat memperkuat perlindungan hukum terhadap data pribadi pengguna serta meningkatkan keamanan transaksi digital di Indonesia.

METODE PENELITIAN

Pada penelitian ini, penulis mengadopsi pendekatan yuridis normatif dengan fokus terhadap bahan hukum primer, seperti peraturan perundang-undangan, serta literatur yang berkaitan dengan isu yang dibahas. Data yang digunakan dalam penelitian ini berasal dari data sekunder yang diperoleh melalui kajian pustaka, yang mencakup dokumen, arsip, buku, artikel, karya ilmiah, serta sumber-sumber lain yang mendukung isu yang diteliti. Data sekunder ini dikelompokkan menjadi dua kategori yakni bahan hukum primer, yang meliputi peraturan perundang-undangan dan catatan resmi, sementara bahan hukum sekunder berfungsi menjelaskan bahan hukum primer, yang mencakup rancangan undang-undang, buku, literatur, serta pendapat para pakar hukum. Metode yang diterapkan dalam penelitian ini mencakup pengumpulan data melalui kajian pustaka, yang selanjutnya akan diperiksa lalu dianalisis berdasarkan tujuan serta pertanyaan penelitian.

---

[23] Muhammad Fahri Fauzadeli, Rani Apriani, "Perlindungan Hukum Terhadap Nasabah *E-Wallet* Atas Kebocoran Data dan Kehilangan Sejumlah Dana", *Jurnal Ilmiah Ilmu Hukum QISTIE,* Volume 15, Nomor 2, 2022, hlm. 224, https://repository.uinjkt.ac.id/dspace/bitstream/123456789/82889/1/skripsi%20fiks%20banget%20TTD.pdf.

[24] *Ibid.*

[25] Nurul Adiyah (*et.al.*), *Op.cit,* hlm. 79.

[26] Apriyanto, Bagus Putu Pramana, Anggraeni Widya Purwita, Transformasi Ekosistem Digital, PT. Sonpedia Publishing Indonesia, Jambi, 2025, hlm. 135.

[27] Ari Budi Santosa, "Apa itu Zero-Knowledge dan Bagaimana Cara Kerjanya", https://pintu.co.id/academy/post/apa-itu-zero-knowledge, diakses pada 13 Juli 2024.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

PEMBAHASAN DAN ANALISIS

Perkembangan Regulasi Perlindungan Data Pribadi Dalam Keamanan Transaksi Digital di Indonesia

Perkembangan digital yang merasuk ke setiap simpul kehidupan memungkinkan segala aktivitas dijalankan lintas batas geografis. Teknologi tidak sekadar alat bantu, melainkan menjadi medium yang mengefisienkan gerak, serta menghidupkan ulang jejaring sosial-ekonomi melalui ruang transaksi digital.[28] Pesatnya pertumbuhan transaksi digital di Indonesia menuntut adanya regulasi yang menyeluruh, yang tidak hanya mencakup keamanan tetapi juga kenyamanan bagi seluruh pengguna. Sebagai lembaga yang diberi kewenangan oleh Undang-Undang, Bank Indonesia memegang peranan penting dalam mengatur dan memastikan kelancaran sistem pembayaran. Tugas utama Bank Indonesia adalah memastikan mekanisme pemindahan dana antar pihak dapat berlangsung secara efisien dan aman.[29]

Berdasarkan data yang dirilis oleh Bank Indonesia (BI), transaksi Uang Elektronik (UE) tercatat mencapai Rp 80,03 triliun pada Februari 2024, mencatatkan peningkatan signifikan sebesar 44,24% (year on year/yoy). Sementara itu, transaksi menggunakan Quick Response Indonesian Standard (QRIS) melonjak 161,51% (yoy), dengan jumlah pengguna mencapai 46,98 juta dan merchant sebanyak 31,27 juta.[30] Peran Bank Indonesia sebagai lembaga pengawas dalam penyelenggaraan dompet elektronik sangat esensial, demi menjamin perlindungan maksimal bagi nasabah sekaligus menjaga kestabilan sistem pembayaran yang lebih luas. Penetapan otoritas pengawas ini bertujuan untuk menghindari potensi risiko yang bisa muncul, seperti penipuan, pencurian data, dan kerusakan sistem. Dengan adanya pengawasan yang ketat, PSE dituntut untuk memenuhi standar keamanan tinggi, memastikan data dan dana nasabah terlindungi secara utuh. Pengawasan yang efektif akan memperkuat kepercayaan publik terhadap penggunaan dompet elektronik, menciptakan rasa aman, serta kenyamanan bagi para penggunanya.[31]

Perlindungan hukum bagi nasabah dompet elektronik oleh BI dimulai dengan penyusunan peraturan dan kebijakan, yang mencakup pembuatan kebijakan terkait penyelenggaraan jasa sistem pembayaran.[32] Negara wajib memperkuat instrumen hukum yang menjamin perlindungan data pribadi guna mencegah adanya kebocoran maupun penyalahgunaan oleh pihak yang tidak bertanggung jawab. Perlindungan ini tidak semata bersifat teknis, melainkan menyangkut martabat dan otonomi individu dalam ruang privatnya. Negara-negara dengan sistem hukum maju telah mengafirmasi hak atas privasi sebagai hak fundamental.[33] Penyalahgunaan data pribadi seperti NIK, KTP-el, dan KK oleh pihak tidak bertanggung jawab menunjukkan lemahnya pengawasan negara. Ketika perlindungan data diabaikan, hak konstitusional warga atas privasi tercederai. Tanpa pusat data nasional yang aman dan regulasi yang ketat, pelanggaran semacam ini akan terus terjadi dan menggerus kepercayaan publik

---

[28] Cynthia H., "Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia," *Jurnal HAM,* Volume 9, Nomor 2, 2018, hlm. 191-204, https://scholar.archive.org/work/nkdl4fqbm5hjzdfjlfu3jw5r3i/access/wayback/http://ejournal.balitbangham.go.id/index.php/ham/article/download/523/pdf_1.

[29] Damasha Khoiri Clevalda dan Dona Budi Kharisma, *Op.cit*, hlm. 3.

[30] Lida Puspaningtyas, "BI: Nominal Transaksi Perbankan Capai Rp 5.103,03 Triliun, https://ekonomi.republika.co.id/berita/san6a4502/bi-nominal-transaksi-perbankan-digital-capai-rp-510303-triliun, diakses pada 6 Juli 2024.

[31] Damasha Khoiri Clevalda dan Dona Budi Kharisma, *Op.cit*, hlm. 7.

[32] Candrawati dan Ni Nyoman Anita, "Perlindungan Hukum Terhadap Pemegang Kartu E-Money Sebagai Alat Pembayaran Dalam Transaksi Komersial," *Jurnal Magister Hukum Udayana,* Volume 3, Nomor 1, 2014, hlm. 3, https://scholar.archive.org/work/rivtr7c5uvgrvcskb5pz3ef24e/access/wayback/https://ojs.unud.ac.id/index.php/jmhu/article/download/8448/6302.

[33] Rosalinda Elsina Latumahina,"Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya", *Jurnal Gema Aktualita,* Volume 3, Nomor 22, 2014, hlm. 17.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

terhadap negara.[34]

Ketiadaan penjabaran normatif mengenai frasa "jaminan pemenuhan atas perlindungan diri" dalam Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) menimbulkan problematika interpretatif yang cukup serius. Peraturan ini tidak memberikan batasan konseptual yang jelas—tidak dari segi pengertian, bentuk perlindungan yang dimaksud, maupun mekanisme jaminan yang seharusnya tersedia bagi individu pengguna sistem elektronik. Ketidakjelasan tersebut menjadi sumber ketidakpastian hukum, terutama dalam konteks insiden kebocoran data yang melibatkan penyedia layanan dompet digital. Dalam praktiknya, pengguna tidak memperoleh kejelasan mengenai hak apa yang melekat pada mereka ketika data pribadinya telah terekam dalam sistem digital. Kealpaan legislator untuk merinci norma perlindungan tersebut menjadikan perlindungan hak privat tidak lebih dari sekadar janji normatif tanpa daya paksa. Frasa "jaminan" dalam Pasal 26 UU ITE pun bernasib serupa menyisakan ruang interpretasi yang terlalu luas dan tanpa instrumen yang memadai untuk menegakkannya. Padahal, hak atas privasi merupakan hak konstitusional yang bersifat *non-derogable* tidak dapat dikurangi dalam keadaan apa pun.[35]

Dalam kerangka hukum yang ditetapkan oleh Peraturan Bank Indonesia, terminologi "Perlindungan Konsumen" dimaknai sebagai perlindungan yang melekat pada pihak yang memanfaatkan produk maupun layanan dari entitas yang berada dalam lingkup pengawasan dan pengaturan Bank Indonesia. Salah satu entitas tersebut adalah penyelenggara sistem pembayaran, yang menurut ketentuan Pasal 4, mencakup penyedia layanan dompet elektronik. Oleh karena itu, dompet elektronik bukan hanya tunduk pada regulasi tersebut secara struktural, tetapi juga menjadi titik pijak bagi pengguna dalam menuntut kepastian dan perlindungan atas hak-haknya dalam setiap transaksi digital yang dilakukan. Namun demikian, jika terjadi pelanggaran terhadap hak-hak tersebut—termasuk dalam bentuk kebocoran data pribadi—regulasi yang ada hanya menyediakan konsekuensi berupa sanksi administratif. Sanksi ini, yang sebatas mencakup penghentian sementara aktivitas usaha, tidak memiliki daya tekan yang proporsional untuk menanggulangi pelanggaran serius seperti penyalahgunaan data pribadi. Lebih jauh, norma teknis terkait pelaksanaan penghentian pun tidak diuraikan secara rinci, menciptakan ruang tafsir yang berpotensi melemahkan fungsi perlindungan hukum.[36]

Pengesahan UU PDP merupakan tonggak penting dalam penguatan rezim hak konstitusional warga negara atas privasi, khususnya dalam konteks pengelolaan data pribadi. UU ini tidak hanya menetapkan standar normatif bagi para pengendali dan pemroses data, tetapi juga menetapkan instrumen sanksi—baik administratif maupun pidana—sebagai bagian dari mekanisme penegakan hukum. Pemberlakuan sanksi tersebut bukan semata-mata berfungsi sebagai pembalasan, melainkan bertujuan untuk menciptakan kepatuhan struktural serta melindungi kepentingan hukum individu atas integritas data pribadinya.

Lebih lanjut, keberadaan Rancangan Peraturan Pemerintah sebagai peraturan pelaksana UU PDP dimaksudkan untuk menutup kekosongan normatif yang tidak terakomodasi dalam UU ITE maupun Peraturan Bank Indonesia. Secara eksplisit, Pasal 115 dan 116 dari RPP tersebut mengafirmasi hak subjek data untuk memperoleh ganti kerugian apabila terjadi pelanggaran dalam bentuk kebocoran data oleh PSE. Meski demikian, perlindungan terhadap data pribadi dalam konteks layanan dompet digital belum diatur secara khusus, sehingga memunculkan celah hukum yang berpotensi dimanfaatkan secara sewenang-wenang. Studi normatif tentang pengguna dompet digital, seperti pada aplikasi OVO, mengungkap bahwa terdapat celah hukum

[34] Ririn Aswandi dkk., "Perlindungan Data dan Informasi Pribadi Melalui Indonesia Data Protection System (IDPS)," LEGISLATIF, Volume 3, Nomor 2, 2020, hlm. 176, http://journal.unhas.ac.id/index.php/jhl/article/view/14321.

[35] Pasal 26 Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

[36] Nurul Adliyah, Fitriani Jamaluddin, Muhammad Ashabul Kahfi, dan Susisanti, "Perlindungan Data Pribadi Pengguna dompet elektronik Ovo," *Al-Amwal: Journal of Islamic Economic Law*, Volume 6, Nomor 1, 2021, hlm. 84-88, http://ejournal.iainpalopo.ac.id/index.php/alamwal/article/view/3706.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

akibat penyebaran data pribadi yang tidak bertanggung jawab, termasuk akses tidak resmi terhadap foto KTP dan swafoto pengguna. Selain itu, penelitian tentang kesadaran keamanan data pada pengguna Dana menunjukkan bahwa meskipun adopsinya meningkat, sekitar 30 % pengguna masih khawatir terhadap risiko kebocoran dan penyalahgunaan data.[37] Regulasi saat ini masih bersifat umum, yaitu mensyaratkan penyelenggara sistem elektronik menjaga kerahasiaan data elektronik hingga pemusnahannya, namun tidak menjabarkan standar teknis berlaku untuk *Financial Technology* (*fintech*). Begitu pula UU Perlindungan Konsumen hanya memberikan ruang kompensasi bagi korban kebocoran data, tanpa menyentuh aspek teknis dan tanggung jawab operasional penyelenggara dompet digital.

Lanskap digital yang semakin kompleks membuat data pribadi menjelma sebagai komoditas yang memiliki nilai strategis tinggi. Ketika terjadi pelanggaran terhadap kerahasiaan data ini—melalui kebocoran maupun akses ilegal—konsekuensinya bukan sekadar bersifat individual, tetapi juga mengganggu tatanan keamanan digital secara kolektif. Risiko yang muncul tidak hanya terbatas pada pencurian identitas atau praktik penipuan, tetapi meluas ke ranah kejahatan siber yang lebih sistemik. Dalam kerangka ini, kebutuhan terhadap pendekatan regulatif berbasis standardisasi menjadi niscaya, guna memastikan seluruh pelaku dalam industri layanan digital tunduk pada protokol keamanan yang bersifat preskriptif. Implementasi standar semacam ini tidak hanya memperkuat posisi hukum konsumen, tetapi juga mengukuhkan prinsip transparansi dan akuntabilitas dalam ekosistem digital. Menjawab kebutuhan tersebut, Bank Indonesia menginisiasi pembentukan kerangka normatif berupa Standar Nasional Open API Pembayaran (SNAP), yang formalitasnya dituangkan melalui Surat Keputusan Gubernur Bank Indonesia Nomor 23/10/KEP.GBI/2021 tertanggal 16 Agustus 2021. Regulasi ini mewajibkan penerapan bertahap terhadap standar interoperabilitas Open API dalam sistem pembayaran nasional.

Peningkatan Standar Nasional OpenAPI Sebagai Standarisasi Keamanan Transaksi dompet elektronik

Teknologi API memudahkan pengguna dompet elektronik dengan menjembatani bank-bank konvensional untuk berbagi data secara aman kepada pihak ketiga yang diberikan kehendak seperti dompet elektronik sehingga tercipta metode *open banking*.[38] Metode ini berjalan menggunakan bantuan dari API dan peraturan yang dibuat untuk melakukan akses kepada API sehingga menjembatani komunikasi antar pihak.[39]

BI mendirikan SNAP sebagai salah satu upaya dalam mewujudkan industri sistem pembayaran yang kompetitif, sehat, dan juga inovatif di Indonesia.[40] Dengan menerapkan SNAP, penyedia layanan pembayaran dapat meningkatkan keamanan data, transparansi, dan kenyamanan pengguna. SNAP API menetapkan standar keamanan dan teknis, standar data, serta spesifikasi teknis SNAP, jenis arsitektur API, format serta struktur data, *authentication and authorization method*, *communication protocol*, *encryption technique*, ketentuan pengelolaan akses API, serta format data untuk permintaan dan tanggapan. Dokumen pedoman tata kelola SNAP mendukung efisiensi dan keamanan transaksi digital, termasuk perlindungan data pribadi pengguna di sektor pembayaran.[41]

Melalui penerapan SNAP API dari BI, integrasi antar sistem dapat terwujud, sehingga

---

37 Devita Azwi Nurrahma, Nibi Nazwa Quinita Tanjung, Gema Surya Gemilang, dan Nurbaiti, "Persepsi Konsumen Tentang Keamanan Data pada Aplikasi *E-Wallet*: Studi Kasus Dana", *Jurnal Manuhara: Pusat Penelitian Ilmu Manajemen dan Bisnis* Volume 3, Nomor 3, 2025, hlm. 112.

38 Jekaterina Drozdovica, "*Digital Wallets and Open Banking: Future of Payments*", https://noda.live/articles/digital-wallets-and-open-banking, diakses pada 12 Juli 2024.

39 *Ibid.*

40 Developers BRI, "5 Manfaat dan Kegunaan SNAP Bank Indonesia, Mudahkan Pembayaran Masyaraka", https://developers.bri.co.id/id/news/5-manfaat-dan-kegunaan-snap-bank-indonesia-mudahkan-pembayaran-masyarakat, diakses pada 12 Juli 2024.

41 ASPI, "Standar Nasional Open API Pembayaran (Pedoman Tata Kelola)", *Bank Indonesia,* 2021, hlm. 2.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

memungkinkan aplikasi dompet elektronik untuk melakukan transaksi langsung dengan bank dan *merchant*, serta mengelola akun pengguna dengan mengakses saldo, riwayat transaksi, dan informasi akun.[42] Dengan menggunakan SNAP, aplikasi dompet elektronik dapat meningkatkan fungsionalitas dan mempermudah penggunaannya serta tetap mematuhi standar keamanan berdasarkan peraturan yang berlaku. Adanya SNAP diharapkan dapat meningkatkan efisiensi transaksi dalam industri *fintech* dengan memungkinkan akses data nasabah bank sesuai standar tanpa perlu negosiasi tambahan dengan komitmen tetap menjamin keamanan dalam melakukan transaksi. Kemudahan dan keamanan transaksi yang ditawarkan melalui API terbuka berbasis SNAP juga diharapkan meningkatkan peluang masyarakat dalam membuka rekening.[43]

Adanya keamanan data di dalam transaksi menggunakan dompet elektronik menjadi hal yang krusial mengingat dalam penggunaannya diperlukan adanya data pribadi yang dimasukkan oleh pengguna pada aplikasi sebelum melakukan transaksi. Meskipun penyelenggaraan sistem elektronik yang aman menjadi tanggung jawab PSE,[44] pengguna dompet elektronik juga perlu memiliki kesadaran bahwa keamanan data menjadi bagian penting di era digital.[45] Sehingga keterlibatan dari konsumen diperlukan untuk perlindungan data dalam transaksi menggunakan dompet elektronik dan mencegah adanya pembobolan akun oleh pihak yang tidak bertanggung jawab.[46] Hal ini serupa dengan pendapat Dr. Jonas Gross, CEO Hakata, yang menekankan pentingnya penyimpanan data pribadi langsung pada perangkat pengguna.[47] Sayangnya SNAP belum memiliki ketentuan mengenai bagaimana keterlibatan dari pengguna layanan pembayaran termasuk dompet elektronik dalam proses perlindungan data.

Merujuk pada survei Kementerian Komunikasi dan Informatika bersama Katadata Insight pada tahun 2021, dompet elektronik dinilai merupakan produk keuangan yang paling rentan mengalami kebocoran data yakni sebesar 36,6%,[48] sehingga perlu ada upaya perlindungan yang lebih ketat untuk menanggulangi kerentanan tersebut. Dalam menunjang perlindungan data pengguna layanan dompet elektronik di Indonesia, metode ZKP dapat menjadi solusi untuk mengatasi kerentanan kebocoran data dompet elektronik. ZKP merupakan metode kriptografi untuk verifikasi informasi tanpa mengharuskan adanya pengungkapan konten informasi tersebut.[49] Dalam metode ini pihak yang menerima dan melakukan verifikasi informasi (*veriver*) tidak memiliki pengetahuan apa pun dari pemberi bukti (*prover*).[50] ZKP memiliki elemen kunci kelengkapan, tanpa pengetahuan, dan keabsahan.[51] Elemen kelengkapan berarti apabila pernyataan yang diberikan merupakan benar, maka verifikasi akan selalu berhasil dikarenakan pembuktian dan verifikator jujur.[52] Elemen tanpa pengetahuan berarti apabila pernyataan benar maka pemeriksa tidak dapat memperoleh pengetahuan apapun terkait dengan informasi

---

42 Tim Redaksi Jalin, "Open Api: Solusi sistem transaksi Digital", https://www.jalin.co.id/id-id/berita/blog/open-api-solusi-sistem-transaksi-digital, diakses pada 12 Juli 2024.

43 Billiam, Lastuti Abubakar, dan Tri Handayani, "The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for the Advancement of Indonesian Banking," *Padjadjaran Journal of Law,* Volume 9, Nomor 1, 2022, hlm. 84, https://jurnal.unpad.ac.id/pjih/article/view/38685.

44 Pasal 15 ayat (1) Undang-undang (UU) Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

45 Moehammad Ramadhoni dan Handri Santoso, "Zero Knowledge Proof for SNAP (Standar Nasional OPEN API Pembayaran) in Indonesia", Jurnal dan Penelitian Teknik Informatika, Volume 8, Nomor 3, 2023, hlm. 1308, https://repository.pradita.ac.id/id/eprint/264/1/12423-Article%20Text-12154-1-10-20230622.pdf.

46 *Ibid.*

47 Savannah Fortis, "Are ZK-proofs the key to Europe's new digital ID regulations?", https://cointelegraph.com/news/zero-knowledge-proofs-eu-digital-id-wallet-regulation, diakses pada Juli 2024.

48 Annissa Mutia, "Survei: Ini Produk Keuangan yang Dianggap Rentan Kebocoran Data", https://databoks.katadata.co.id/datapublish/2022/10/14/survei-ini-produk-keuangan-yang-dianggap-rentan-kebocoran-data, diakses pada 12 Juli 2024.

49 Ari Budi Santosa, *Loc.cit.*

50 *Ibid.*

51 Sodium Wallet, "Understanding Zero Knowledge Proofs — One of the Key Technical Features of Sodium Wallet", https://medium.com/@sodiums_org/understanding-zero-knowledge-proofs-one-of-the-key-technical-features-of-sodium-wallet-dc9745e526f7, diakses pada 12 Juli 2024.

52 *Ibid.*

P-ISSN : 2407-6546
E-ISSN : 2685-2357

pribadi, kecuali adanya putusan pengadilan atau kebenaran hakim.[53] Elemen keabsahan berarti minimalnya peluang seorang meyakinkan verifikator mengenai pernyataan yang salah.[54]

Adanya penerapan dari ZKP dalam standar praktik dan keamanan dalam SNAP mempersempit data yang dikelola oleh PSE. Penyempitan akses data tersebut dilakukan dikarenakan pihak penyedia layanan dompet elektronik tidak harus untuk memegang data pribadi pengguna terutama yang bersifat sensitif seperti nomor rekening.[55] Metode ZKP memungkinkan seorang *prover* meyakinkan pihak verifikator atas kebenaran suatu pernyataan tanpa harus mengungkapkan informasi secara langsung terkait isi dari bukti tersebut. ZKP memanfaatkan sebuah pernyataan yang disebut sebagai saksi sebagai input untuk menghasilkan bukti ringkas mengenai kebenaran pernyataan tersebut. Dengan begitu, proses pembuktian yang memenuhi kriteria kelengkapan dan *soundness* mampu memberikan jaminan yang kuat bahwa pernyataan tersebut valid meskipun tidak membocorkan informasi yang mendasari pembuatannya.

Dalam konteks teori perlindungan konsumen, penerapan ZKP pada dompet elektronik diharapkan dapat memberikan solusi terhadap lemahnya posisi konsumen yang relatif lebih lemah dalam transaksi jual beli barang atau jasa.[56] Konsumen pun seringkali tidak memahami sepenuhnya bagaimana data pribadi mereka diproses. Konsep ZKP dapat mengurangi kesenjangan informasi ini dengan memberikan transparansi dalam proses verifikasi tanpa mengekspos data sensitif.[57] Sehingga penerapan ZKP juga selaras dengan prinsip perlindungan konsumen seperti diatur dalam Pasal 4 UU Perlindungan Konsumen yang mengatur hak pengguna atas informasi yang benar, jelas, dan jujur mengenai kondisi dan jaminan barang dan/atau jasa.[58]

Hingga saat ini penyedia layanan dompet elektronik masih meminta nomor rekening untuk melakukan penautan akun dompet elektronik dengan kartu debit maupun kredit. Akan tetapi dompet elektronik yang memiliki kerentanan kebocoran data yang cukup tinggi, sehingga diperlukan mekanisme penautan akun dompet elektronik dengan kartu kredit maupun debit tanpa harus adanya pemberian informasi nomor kartu kepada penyedia layanan digital. Dalam implementasi yang penulis usungkan, ZKP dapat digunakan sebagai standar dalam praktik dan keamanan SNAP.

Dengan adanya implementasi ZKP, penyedia layanan dompet elektronik sebagai pihak ketiga diantara pengguna dompet elektronik dan Bank konvensional, ketika pengguna ingin menautkan akun debit maupun kredit pengguna ke dalam dompet elektronik, pengguna tidak perlu mengisi data nomor rekening. Pengguna dapat mengajukan permohonan enkripsi kepada bank konvensional agar data mereka dimasukkan ke dalam dompet elektronik. Bank konvensional kemudian mengenkripsi data pengguna dan mengirimkan kode enkripsi kepada mereka, sehingga hanya pengguna dan pihak bank yang dapat mengakses serta mengetahui data tersebut. Setelah pengguna menerima kode, pengguna mengirimkan data tersebut untuk kemudian digunakan penyedia dompet elektronik untuk melakukan verifikasi kepada bank konvensional untuk menautkan akun dompet elektronik dengan kartu kredit maupun debit pengguna.

Dapat dipahami bahwa dalam melakukan transaksi digital menggunakan sejumlah data sensitif sehingga dalam implementasi perlindungan data pribadi oleh negara diperlukan adanya pendekatan yang holistik dengan menggabungkan payung hukum dan teknologi agar tidak

---

53 *Ibid.*
54 *Ibid.*
55 Moehammad Ramadhoni dan Handri Santoso, *Loc.cit.*
56 I Gede Pasek Adiarta dan Lalu Wira Pria Suharta,"Perlindungan Hukum Pengguna Dompet Digital Menurut Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan konsumen", *Jurnal Commerce Law*, Volume 4, Nomor 2, hlm. 387.
57 *Ibid.*
58 *Ibid.*

P-ISSN : 2407-6546
E-ISSN : 2685-2357

menimbulkan kerugian pada terekseposnya data sensitif yang tidak dikehendaki.[59] Terutama dalam menghadapi praktik pengumpulan data sensitif seperti yang terjadi pada aplikasi dompet elektronik DANA yang meminta pengguna untuk memverifikasi akunnya untuk menjadi DANA premium dengan memasukkan foto KTP dan informasi yang terdapat dalam KTP tersebut,[60] dimana KTP sebagai dokumen kependudukan, memuat data pribadi yang wajib dilindungi oleh negara.[61] Dari segi payung hukum, Undang-Undang Pelindungan Data Pribadi telah mengatur mengenai kewajiban pengendali data untuk menerapkan prinsip minimalisasi data,[62] tujuan terbatas,[63] dan akuntabilitas dalam pemrosesan data kependudukan.[64] Undang-undang tersebut juga telah menetapkan sanksi administratif berupa teguran, penghentian aktivitas pengolahan data, hingga pencabutan izin usaha bagi penyedia layanan yang melanggar dan tidak mampu memberikan perlindungan data pribadi pengguna.[65]

Sebagai upaya dalam meningkatkan perlindungan data pribadi dari segi teknologi, penulis mengusulkan adanya penerapan ZKP secara bertahap terhadap semua jenis data sensitif dengan memperluas cakupan penerapan ZKP dengan menyusun standar pengelolaan data pribadi bersama para *stakeholder*, penyedia jasa pembayaran termasuk dompet elektronik, dan masyarakat. Pelaksanaan dari ZKP sendiri dapat dilaksanakan secara bertahap dari penyusunan skema, standar, hingga penentuan verifikator yang bertanggung jawab. Hal ini diharapkan dapat mengatasi dilema verifikasi identitas tanpa perlu menyimpan atau menunjukkan seluruh data pribadi pengguna, sehingga menghindari risiko kegagalan perlindungan data pribadi yang dapat berimplikasi pada pencurian identitas, penipuan, pelanggaran privasi, hingga kehilangan kepercayaan pemilik data.[66]

Pembaharuan Regulasi Dalam Rangka Penguatan Hukum Perlindungan Data Pribadi Keamanan Transaksi Digital Menggunakan Dompet Elektronik

Tidak dapat dipungkiri, bersamaan dengan kemudahan dalam penggunaan dompet elektronik, terdapat kerentanan kebocoran data pribadi yang perlu untuk ditangani. Sayangnya, hingga saat ini Indonesia belum mengatur perlindungan data pribadi pada transaksi digital secara spesifik, termasuk regulasi terkait dompet elektronik. Kondisi tersebut beresiko menimbulkan kekosongan hukum dan potensi adanya kejahatan siber. Akibatnya, masyarakat menjadi rentan terkena penyalahgunaan data pribadi, penipuan, dan berbagai kejahatan siber lainnya. Untuk itu, perlu dilakukan sejumlah pembaharuan dalam regulasi perlindungan data pribadi untuk keamanan transaksi digital.

Dalam halnya perlindungan data pribadi dengan menerapkan standar ZKP, Uni Eropa melalui Regulasi EU Digital Identity Wallet Nomor 1183 tahun 2024 telah mengatur secara eksplisit mengenai kewajiban bagi negara anggota untuk mengintegrasi berbagai teknologi untuk menjaga privasi seperti ZKP.[67] Penggunaan metode kriptografi seperti ZKP dalam perlindungan data pribadi terutama data identitas pengguna ditujukan untuk memvalidasi "kebenaran pernyataan pengguna" berdasarkan data tersebut tanpa perlu mengungkap data sehingga

---

59 Ugnė Zieniūtė, "Data sensitif dan cara melindunginya", https://nordvpn.com/id/blog/data-pribadi-atau-sensitif/, diakses pada Juli 2024.

60 DANA, "Bagaimana cara menjadi akun DANA Premium?", https://dana.zendesk.com/hc/id-id/articles/360040996114-Bagaimana-cara-menjadi-akun-DANA-Premium, diakses pada Juli 2024.

61 Bernadetha Aurelia Oktavira, "Apakah KTP Merupakan Data Pribadi yang Dilindungi?", https://www.hukumonline.com/klinik/a/apakah-ktp-merupakan-data-pribadi-yang-dilindungi-lt5c8b573e224de/, diakses pada Juli 2024.

62 Pasal 27 Undang-Undang Nomor 27 tahun 2022 Tentang Pelindungan Data Pribadi.

63 Pasal 28 Undang-Undang Nomor 27 tahun 2022 Tentang Pelindungan Data Pribadi.

64 Pasal 16 ayat (2) huruf h Undang-Undang Nomor 27 tahun 2022 Tentang Pelindungan Data Pribadi.

65 Pasal 47 Undang-Undang Nomor 27 tahun 2022 Tentang Pelindungan Data Pribadi.

66 Facit, "*Consequences of a Data Breach*?", https://facit.ai/insights/consequences-of-data-breach#:~:text=Consequences%20of%20a%20Data%20Breach,-The%20consequences%20of&text=Victims%20may%20face%20identity%20theft,of%20dollars/pounds/Euros, diakses pada 23 Juni 2025.

67 Pasal 14 Regulation (EU) 2024/1183 of The European Parliament and of The Council of 11 April 2024.

privasi pengguna tetap terjaga.[68] Selain itu regulasi ini juga diharapkan dapat memberikan warga Uni Eropa untuk memiliki identifikasi daring dan luring yang aman, sehingga memungkinkan akses yang lancar dan terpercaya pada layanan digital publik maupun privat.[69]

Sebagai upaya penguatan hukum perlindungan data pribadi dalam transaksi menggunakan dompet elektronik di Indonesia, penulis mengusulkan beberapa pembaharuan regulasi untuk menunjang penerapan ZKP di Indonesia. Pertama, pemerintah perlu membentuk badan atau otoritas pengawas independen yang bertugas memastikan implementasi UU PDP berjalan secara efektif dan menjamin keamanan data pribadi dalam transaksi digital. [70] Pentingnya keberadaan otoritas pengawas pelindungan data pribadi tersebut juga telah ditekankan pada regulasi internasional, seperti dalam regulasi General Data Protection Regulation Uni Eropa yang disahkan pada 2016 lalu (EU GDPR) dalam Pasal 51 ayat (1).

Hingga kini, badan pengawas otonom belum dibentuk dan pengaturan mengenai hal tersebut juga belum diatur dengan jelas di Indonesia. Dalam Pasal 58 UU PDP diatur mengenai pembentukan Data Protection Authority (DPA), tetapi tidak dijelaskan lebih lanjut terkait batasan dari tugas DPA tersebut. Sebaliknya, negara Uni Eropa, yaitu Inggris dan Norwegia telah lama membentuk DPA.[71] Di Inggris, DPA dikenal sebagai The Data Protection Commissioner, yang bertugas mengendalikan dan memantau arus informasi yang berhubungan dengan data pribadi individu.[72] Sementara di Norwegia terdapat *Supervisory Authority* (The Norwegian Data Protection Authority (NDPA)) di tingkat negara anggota Uni Eropa dan European Data Protection Board di tingkat regional Uni Eropa. Kedua lembaga tersebut memiliki tugas masing-masing dan aturan hukum perlindungan data pribadi di Norwegia.[73]

Di tingkat regional Asia, seperti Hong Kong, Otoritas Perlindungan Data atau *Data Protection Authority* dikenal sebagai Privacy Commissioner for Personal Data (PCPD). Hal tersebut tercantum di dalam Personal Data Privacy Ordinance tahun 1995. Pembentukan PCPD ini bertujuan untuk menjamin keamanan data pribadi serta memastikan bahwa pengelolaan data oleh pengendali data pribadi telah sesuai dengan standar yang ditetapkan.[74] Oleh karena itu, pemerintah Indonesia perlu mempertimbangkan pembentukan DPA sebagai upaya pengawasan dan pengendalian perlindungan data pribadi, terutama pada keamanan transaksi digital. Hal ini penting mengingat potensi penyalahgunaan data pribadi dapat dilakukan oleh berbagai pihak. Keberadaan DPA diharapkan dapat memperkuat perlindungan data pribadi secara lebih optimal, menciptakan pengawasan yang lebih efektif, dan meningkatkan akuntabilitas para pengendali data pribadi.[75]

Kedua, ketentuan dalam Pasal 56 ayat (1) UU PDP terkait transmisi data pribadi ke negara lain perlu ditambahkan dengan kalimat "mendapat persetujuan dari pemilik data pribadi", agar

---

68 *Ibid.*

69 EUR-Lex, "EU Digital Identity Wallet", https://eur-lex.europa.eu/EN/legal-content/summary/the-establishment-of-the-european-digital-identity-framework-including-the-provision-of-european-digital-identity-wallets-and-trust-services.html?fromSummary=31, diakses pada 29 Juni 2025.

70 Made Emy Andayani Citra (et.al.), "Perlindungan Hukum terhadap Data Diri Pribadi di Era Ekonomi Digital: Peluang dan Tantangan (Studi Komparasi Indonesia dan Malaysia)", *Jurnal Hukum Saraswati,* Volume 05, Nomor 2, 2023, hlm. 527, https://e-journal.unmas.ac.id/index.php/JHS/article/download/8238/6120.

71 Azza Fitrahul Faizah (et.al.), "Penguatan Pelindungan Data Pribadi Melalui Otoritas Pengawas Di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura", *Jurnal Ilmu Hukum dan Sosial*, Volume 1, Nomor 3, Agustus 2023, hlm. 3, https://journal.stekom.ac.id/index.php/Hakim/article/view/1222.

72 Hari Sutra Disemandi, "Urgensi Regulasi Khusus dan Pemanfaatan *Artificial Intelligence* dalam Mewujudkan Perlindungan Data Pribadi di Indonesia", *Jurnal Wawasan Yuridika,* Volume 5, Nomor 2, September 2021, hlm. 187, http://ejournal.sthb.ac.id/index.php/jwy/article/view/460.

73 Florianus Yudhi P. A. dan Viona Puspita, "Perlindungan Hukum Atas Data Pribadi (Studi perbandingan Hukum Indonesia dan Norwegia", *Conference on Management, Business, Innovation, Education and Social Sciences* , Volume. 1, Nomor 1, Maret 2021, hlm. 422, https://journal.uib.ac.id/index.php/combines/article/view/4466.

74 Rosalinda Elsina Latumahina, "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya", *Jurnal Gema Aktualita,* Volume 3, Nomor 2, 2014, hlm. 17, https://scholar.google.com/citations?view_op=view_citation&hl=en&user=83m-jIkAAAAJ&citation_for_view=83m-jIkAAAAJ:u5HHmVD_uO8C.

75 *Ibid.*

P-ISSN : 2407-6546
E-ISSN : 2685-2357

pemilik data mendapat pemberitahuan mengenai transmisi tersebut dan memberikan persetujuan secara sukarela. Apabila tidak mendapat izin dari pemilik data, maka berpotensi mengabaikan hak absolutnya (*absolute rights*). Selain itu, hal tersebut juga berdampak negatif terhadap keamanan transaksi digital karena membuka peluang pelanggaran keamanan, seperti pencurian atau penyalahgunaan data untuk penipuan digital. Sebagai perbandingan, regulasi GDPR di Uni Eropa mewajibkan persetujuan secara eksplisit dari pemilik data serta membatasi perpindahan data dengan negara yang tak memenuhi standar perlindungan yang memadai, kecuali pemilik memberikan persetujuan atau ada mekanisme pelindung seperti Binding Corporate Rules (BCRs).[76] Dengan adanya mekanisme ini, pemilik data pribadi lebih percaya terhadap keamanan data mereka, sehingga transaksi digital lebih terlindungi.

Ketiga, perlu adanya pembentukan regulasi yang lebih spesifik terkait pelindungan data pribadi dalam aktivitas transaksi digital, khususnya pada penggunaan dompet elektronik. Hal ini disebabkan pengaturan dalam UU PDP masih bersifat umum, meliputi jenis data pribadi (Pasal 4); hak subjek data pribadi (Pasal 5-Pasal 14); pemrosesan data pribadi (Pasal 16-Pasal 18); kewajiban pengendali dan prosesor data pribadi dalam pemrosesan data pribadi (Pasal 19-Pasal 50); transfer data pribadi (Pasal 55-Pasal 56); sanksi administratif (Pasal 57); kelembagaan (Pasal 58); penyelesaian sengketa dan hukum acara (Pasal 64); larangan dalam penggunaan data pribadi (Pasal 65-Pasal 66); dan ketentuan pidana (Pasal 67-Pasal 73). Namun, ketentuan - ketentuan tersebut belum secara eksplisit menjangkau karakteristik dan risiko yang melekat pada penggunaan dompet elektronik. Padahal, dalam praktiknya, berbagai insiden kebocoran data dan penyalahgunaan informasi pribadi pengguna dompet elektronik menunjukkan urgensi pembentukan regulasi khusus yang bersifat *lex specialis* terhadap UU PDP. Regulasi tersebut dapat berupa peraturan pelaksana dari UU PDP. Pembaruan regulasi ini bertujuan untuk menjamin kepastian hukum dan ketertiban dalam pemanfaatan teknologi, khususnya dalam transaksi digital.

PENUTUP

Kesimpulan

1. Transaksi digital yang meningkat pesat membutuhkan regulasi untuk menjamin keamanan dan kenyamanan pengguna. Bank Indonesia, sebagai lembaga pengawas, memastikan mekanisme transfer uang berjalan dengan baik dan melindungi nasabah. PBI 18/40/PBI/2016 dan PBI 22/20/PBI/2020, memastikan standar keamanan tinggi bagi dompet elektronik. Pemerintah perlu memperkuat regulasi perlindungan data pribadi untuk mencegah kebocoran dan penyalahgunaan data, sebagaimana tercantum dalam UU PDP dan UU ITE. Perlindungan data pribadi sangat penting untuk mencegah dampak negatif seperti pencurian identitas dan penipuan. Dengan demikian diperlukan standarisasi keamanan data, seperti SNAP yang ditetapkan oleh BI dan dikelola oleh ASPI, memastikan semua penyedia layanan mematuhi protokol keamanan ketat, meningkatkan perlindungan konsumen dan transparansi.
2. Bank Indonesia mendirikan SNAP untuk memajukan industri pembayaran Indonesia dengan fokus keamanan, transparansi, dan kenyamanan pengguna. Namun, SNAP belum mengatur secara khusus bagaimana perlindungan data pengguna layanan pembayaran, termasuk dompet elektronik. Penggunaan *Zero Knowledge Proof* (ZKP) dalam SNAP menjadi solusi potensial untuk melindungi data pengguna dompet elektronik. ZKP memungkinkan verifikasi informasi tanpa mengungkapkan konten informasi kepada verifikator, sehingga menjaga keamanan dan privasi. Implementasi ZKP dapat menyempitkan akses terhadap data sensitif seperti nomor rekening, dengan bank konvensional menggunakan enkripsi untuk verifikasi tanpa mengungkapkan informasi sensitif kepada penyedia layanan. Meskipun demikian, perlindungan data sensitif seperti KTP dalam aplikasi dompet elektronik masih menjadi tantangan yang perlu diatasi sesuai

[76] Article 45 (3) General Data Protection Regulation (GDPR).

P-ISSN : 2407-6546
E-ISSN : 2685-2357

regulasi privasi yang berlaku. Penggunaan ZKP dapat diperluas untuk melindungi semua jenis data sensitif dengan melibatkan pihak terkait dalam menyusun standar pengelolaan data yang aman. Implementasi ZKP secara bertahap dengan mempertimbangkan skema, standar, dan verifikator yang handal adalah kunci keberhasilan dalam mengamankan data pengguna layanan digital di masa depan.

3. UU PDP masih bersifat umum dan belum mengatur secara spesifik mengenai perlindungan data pribadi dalam transaksi digital. Kondisi ini memungkinkan terjadinya kekosongan hukum yang berisiko dimanfaatkan oleh oknum yang tidak bertanggung jawab, hal ini berimplikasi pada kerentanan penyalahgunaan data pribadi pengguna dan kejahatan siber pada aplikasi dompet elektronik. Untuk mengatasi permasalahan tersebut, diperlukan langkah nyata dari pemerintah, diantaranya dengan membentuk lembaga pengawas independen sebagaimana telah diterapkan di berbagai negara lain, seperti Inggris, Norwegia, dan Hong Kong. Selain itu, penguatan ketentuan mengenai transmisi data pribadi lintas negara melalui persetujuan eksplisit pemilik data guna menjamin hak-hak individu dan keamanan transaksi digital serta pembentukan regulasi yang lebih spesifik sebagai turunan dari UU PDP dapat memberikan perlindungan yang lebih optimal dan menjamin kepastian hukum bagi masyarakat.

Saran

1. Pemerintah harus melakukan pemantauan dan evaluasi berkala terhadap implementasi regulasi perlindungan data pribadi untuk memastikan efektivitas dan keberlanjutan perlindungan yang diberikan. Di samping itu pemerintah perlu untuk mempelajari praktik terbaik dari negara lain yang telah berhasil menerapkan perlindungan data pribadi, seperti Uni Eropa melalui GDPR. Hal ini bertujuan untuk mewujudkan ekosistem digital yang terpercaya, aman, dan nyaman, serta mendorong perkembangan ekonomi digital yang sehat di Indonesia.
2. BI bersama ASPI harus memperketat standar keamanan data dengan melibatkan seluruh penyedia layanan dalam mematuhi protokol keamanan ketat. Adapun penggunaan teknologi ZKP dalam Standar Nasional Open API Pembayaran (SNAP) dapat dipertimbangkan sebagai upaya tindak lanjut untuk melindungi data pengguna layanan pembayaran digital.
3. Dalam menunjang pelindungan data pribadi di Indonesia, selain adanya penggunaan ZKP, diperlukan adanya pembaharuan regulasi dan juga pembentukan DPA yang independen. Pembaharuan regulasi melalui peraturan pelaksana dari UU PDP dapat meminimalisir celah hukum dan meningkatkan efektivitas PDP, terkhusus pelindungan data pengguna dompet elektronik di Indonesia.

DAFTAR PUSTAKA

Buku

Ahmad M. Ramli dan Tasya Safiranita Ramli, *Hukum sebagai Infrastruktur Transformasi Indonesia: Regulasi dan Kebijakan Digital*, Bandung: Refika Aditama, 2022.

Apriyanto, Bagus Putu Pramana, dan Anggraeni Widya Purwita, *Transformasi Ekosistem Digital,* PT Sonpedia Publishing Indonesia, Jambi, 2025.

Muhaimin, Metode Penelitian Hukum, Ctk. Pertama, Mataram University Press, Mataram, 2020.

M. Rohmadi dan Yakub Nasucha, *Dasar-Dasar Penelitian*, Pustaka Brilliant, 2015.

Wahyudi Djafar (et.al.), *Perlindungan Data Pribadi: Usulan Kebijakan dari Perspektif Hak Asasi Manusia*, ELSAM, 2016.

Jurnal

ASPI, “Standar Nasional Open API Pembayaran (Pedoman Tata Kelola)”, *Bank Indonesia*, 2021.

Billiam (et.al.), "The Urgency of Open Application Programming Interface Standardization in the Implementation of Open Banking to Customer Data Protection for the Advancement of Indonesian Banking”, *Padjadjaran Jurnal Ilmu Hukum*, Volume 9, Nomor 1, 2022.

P-ISSN : 2407-6546
E-ISSN : 2685-2357

Cynthia H., "Registrasi Data Pribadi Melalui Kartu Prabayar Dalam Perspektif Hak Asasi Manusia", *Jurnal HAM*, Volume 9, Nomor 2, 2018.

Damasha Khoiri Clevalda dan Dona Budi Kharisma, "Perlindungan Hukum terhadap Nasabah dompet elektronik Oleh Bank Indonesia", *Privat Law Journal*, Volume 9, Nomor 1, 2021.

Desvronita, "Faktor-faktor yang Mempengaruhi Minat Menggunakan Sistem Pembayaran *E-Wallet* Menggunakan *Technology Acceptance Model", Jurnal Akmenika*, Volume 18 Nomor 2, 2021.

Devita Azwi Nurrahma, Nibi Nazwa Quinita Tanjung, Gema Surya Gemilang, dan Nurbaiti, "Persepsi Konsumen Tentang Keamanan Data pada Aplikasi *E-Wallet*: Studi Kasus Dana", *Jurnal Manuhara: Pusat Penelitian Ilmu Manajemen dan Bisnis*, Volume 3, Nomor 3, 2025.

M. Zulfa Aulia, "Hukum Pembangunan dari Mochtar Kusumaatmadja: Mengarahkan Pembangunan atau Mengabdi pada Pembangunan?" *Undang: Jurnal Hukum*, Volume 1, Nomor 2, 2018.

Moehammad Ramadhoni dan Handri Santoso, "Zero Knowledge Proof for SNAP (Standar Nasional OPEN API Pembayaran) in Indonesia", *Jurnal dan Penelitian Teknik Informatika*, Volume 8, Nomor 3, 2023.

Muhammad Fahri Fauzadeli dan Rani Apriani, "Perlindungan Hukum Terhadap Nasabah E-Wallet Atas Kebocoran Data dan Kehilangan Sejumlah Dana", *Jurnal Ilmiah Ilmu Hukum QISTIE*, Volume 15, Nomor 2, 2022.

Ni Nyoman Anita Candrawati, "Perlindungan Hukum Terhadap Pemegang Kartu E-Money Sebagai Alat Pembayaran Dalam Transaksi Komersial", *Jurnal Magister Hukum Udayana* Volume 3 Nomor 1, 2014.

Nurul Adliyah (et.al.), "Perlindungan Data Pribadi Pengguna dompet elektronik Ovo." Al-Amwal: *Journal of Islamic Economic Law Volume 6*, Nomor 1, 2021.

Purnama Ramadani (et.al.), "Analisis Keamanan Transaksi E-Commerce dalam Mencegah Penipuan Online", Profit: Jurnal Manajemen, Bisnis dan Akuntansi, Volume 1, Nomor 4, 2022.

Ririn Aswandi (et.al.), "Perlindungan Data dan Informasi Pribadi Melalui Indonesia Data Protection System (IDPS)", *LEGISLATIF*, Volume 3, Nomor 2, 2020.

Rosalinda Elsina Latumahina. "Aspek Hukum Perlindungan Data Pribadi Di Dunia Maya." *Jurnal GEMA AKTUALITA*, Volume 3, Nomor 22, 2014.

Dokumen Lain

Almadinah Putri Brilian, "Survei: 71% Orang RI Pakai Dompet Elektronik, Mana yang Paling Laris?", https://finance.detik.com/fintech/d-6433675/survei-71-orang-ri-pakai-dompet-digital-mana-vang-paling-laris, diakses Juni 2024.

Ari Budi Santosa, "Apa Itu Zero-Knowledge dan Bagaimana Cara Kerjanya", https://pintu.co.id/academy/post/apa-itu-zero-knowledge, diakses 13 Juli 2024.

Bernadetha Aurelia Oktavira, "Apakah KTP Merupakan Data Pribadi yang Dilindungi?", https://www.hukumonline.com/klinik/a/apakah-ktp-merupakan-data-pribadi-yang-dilindungi-lt5c8b573e224de/, diakses Juli 2024.

Developers BRI, "5 Manfaat dan Kegunaan SNAP Bank Indonesia, Mudahkan Pembayaran Masyaraka", https://developers.bri.co.id/id/news/5-manfaat-dan-kegunaan-snap-bank-indonesia-mudahkan-pembayaran-masyarakat, diakses pada 12 Juli 2024.

EUR-Lex, "EU Digital Identity Wallet", https://eur-lex.europa.eu/EN/legal-content/summary/the-establishment-of-the-european-digital-identity-framework-including-the-provision-of-european-digital-identity-wallets-and-trust-services.html?fromSummary=31, diakses pada 29 Juni 2025.

Facit, "Consequences of a Data Breach?", https://facit.ai/insights/consequences-of-data-breach#:~:text=Consequences%20of%20a%20Data%20Breach,-

P-ISSN : 2407-6546
E-ISSN : 2685-2357

The%20consequences%20of&text=Victims%20may%20face%20identity%20theft,of%20dollars/pounds/Euros, diakses pada 23 Juni 2025.

FasterCapital, "How Technology is Disrupting Traditional Markets", https://fastercapital.com/content/How-Technology-is-Disrupting-Traditional-Markets.html#:~:text=Traditional%20methods%2C%20such%20as%20cash,online%20transactions%20seamless%20and%20efficient, diakses Juli 2024.

Fitriyani Puspa Samodra, "E-Wallet adalah Dompet Elektronik, Ketahui Jenis dan Kelebihannya", https://www.liputan6.com/hot/read/5439316/e-wallet-adalah-dompet-digital-ketahui-jenis-dan-kelebihannya, diakses Juni 2024.

Gocardless, "Digital Transactions: What Are They?", https://gocardless.com/guides/posts/what-are-digital-transactions/#what-is-a-digital-transaction, diakses Juli 2024.

Jekaterina Drozdovica, "Digital Wallets and Open Banking: Future of Payments", https://noda.live/articles/digital-wallets-and-open-banking, diakses pada 12 Juli 2024.

Nur, "Saldo ShopeePay Hilang Tanpa Kejelasan, CS Shopee Berbelit-belit", https://mediakonsumen.com/2023/04/29/surat-pembaca/saldo-shopeepay-hilang-tanpa-kejelasan-cs-shopee-berbelit-belit, diakses Juni 2024.

Tim Redaksi Jalin, "Open Api: Solusi sistem transaksi Digital", https://www.jalin.co.id/id-id/berita/blog/open-api-solusi-sistem-transaksi-digital, diakses pada 12 Juli 2024.

Rosa Anggreati, "Perkembangan E-wallet di Indonesia dan Manfaat Sehari-hari", https://www.medcom.id/ekonomi/bisnis/ob340X8k-perkembangan-e-wallet-di-indonesia-dan-manfaat-sehari-hari, diakses Juni 2024.

Savannah Fortis, "Are ZK-proofs the key to Europe's new digital ID regulations?", https://cointelegraph.com/news/zero-knowledge-proofs-eu-digital-id-wallet-regulation, diakses Juli 2024.

Sodium Wallet, "Understanding Zero Knowledge Proofs — One of the Key Technical Features of Sodium Wallet", https://medium.com/@sodiums_org/understanding-zero-knowledge-proofs-one-of-the-key-technical-features-of-sodium-wallet-dc9745e526f7, diakses Juli 2024.

Ugnė Zieniūtė, "Data Sensitif dan Cara Melindunginya", https://nordvpn.com/id/blog/data-pribadi-atau-sensitif/, diakses Juli 2024.

Dokumen Hukum

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Peraturan Bank Indonesia Nomor 22/23/PBI/2020 Tahun 2020 tentang Sistem Pembayaran

Peraturan Bank Indonesia Nomor 23/6/PBI/2021 Tahun 2021 tentang Penyedia Jasa Pembayaran.

Regulation (EU) 2024/1183 of The European Parliament and of The Council of 11 April 2024.