

Pelindungan Data Pribadi Nasabah di Era *Open Banking* (Studi Komparasi di Indonesia dan Inggris)

Adinda Rizky Fajri

Faculty of Law, Universitas Sebelas Maret, Surakarta, Indonesia.

**Corresponding author's e-mail: contact.adindarizky@gmail.com*

Article	Abstract
<p>Keywords: Consumer Protection, Open Banking, Personal Data Protection.</p> <p>Artikel History Received: Jun 1, 2024; Reviewed: Sept 28, 2024; Accepted: Oct 26, 2024; Published: Oct 31, 2024.</p> <p>DOI: 10.20961/jolsic.v12i2.87426</p>	<p>This study compares the customer personal data protection in the era of open banking between Indonesia and the United Kingdom. Open banking, which allows banks to share customer financial data and information with third parties via API, offers ease of access and innovation in financial services. In Indonesia, the implementation of open banking is initiated by Bank Indonesia through the National Standard for Open API Payments. Meanwhile, the UK has adopted open banking since 2018 with legal frameworks such as the Payment Service Directives (PSD2) and General Data Protection (GDPR), which emphasize personal data protection and financial market openness. The research method used is normative juridical with regulatory and comparative approaches. The results show that the UK's success in implementing open banking that has specific implementation and supervisory entity namely OBL, can serve as a lesson for Indonesia to create strong legal certainty in personal data protection, which in turn will enhance consumer trust and the development of the digital financial sector.</p>

PENDAHULUAN

Seiring dengan kemajuan teknologi, transformasi digital tidak hanya mengubah sektor perbankan, tetapi juga menciptakan peluang baru dalam bisnis layanan jasa keuangan, salah satunya dengan munculnya *financial technology* (“fintech”) (Kristianti, 2021: 60). Fintech merupakan model bisnis baru yang memberikan kemudahan layanan transaksi keuangan terhadap pengguna yang lebih cepat dan mudah digunakan (Benuf, 2019: 147). Di Indonesia, fintech telah berkembang pesat sejak 2016 dan layanan jasa keuangan yang diselenggarakan terdiri dari sistem pembayaran/penyelesaian transaksi (*digital payment*), pendukung pasar, pinjaman, pembiayaan, dan penyediaan modal/penghimpunan modal, pengelolaan investasi, perasuransian, pendukung keuangan digital lainnya, dan aktivitas jasa keuangan lainnya (Benuf, 2019: 149). Keberadaan fintech melalui aplikasi sistem pembayaran digital seperti GoPay, OVO, dan DANA, oleh perusahaan startup maupun perusahaan besar telah mereduksi tatanan layanan keuangan konvensional sehingga akses masyarakat terhadap layanan keuangan menjadi lebih mudah dan efisien dengan kehadiran fintech (Rahadiyan, 2022: 224).

Pesatnya perkembangan perbankan digital dan fintech menandakan semakin besarnya tuntutan dari konsumen terhadap layanan keuangan yang cepat, mudah, aman, dan nyaman (Omarini, 2018: 4). Hal ini memunculkan adopsi baru dalam penyelenggaraan layanan melalui keterbukaan data antara bank dengan pihak ketiga agar dapat mengakomodasi dan mempercepat layanan terhadap kebutuhan konsumen. Untuk mengoptimalkan keterbukaan data antar bank dan pihak ketiga atas referensi nasabah, maka muncul sebuah inovasi baru yaitu *open banking* atau open API. *Open banking* merupakan pendekatan yang memungkinkan bank membuka data dan informasi keuangan nasabahnya kepada pihak ketiga melalui open API (*Application Program Interface*) (Nathania, dkk, 2023: 250). *Open banking* akan membuka peluang bagi pihak ketiga seperti perusahaan fintech dan layanan jasa keuangan nonbank lain, perusahaan ecommerce, hingga UMKM untuk bekerja sama memberikan layanan. Implementasi *open banking* memberikan manfaat kepada bank, fintech, maupun nasabah. Bagi bank, *open banking* dapat meningkatkan ROE (*return on equity*) yang berkelanjutan, meringankan biaya, mempercepat inovasi, dan pengembangan pelayanan. Bagi fintech, akan terdapat peningkatan profit yang dapat digunakan optimalisasi sistem layanan. Bagi nasabah, manfaat yang dirasakan adalah kemudahan dalam mengakses produk layanan keuangan (Adinegoro, 2020: 94).

Open banking mengecualikan prinsip kerahasiaan bank dalam pemrosesan data nasabah yang tadinya hanya sebagai hubungan tertutup antara bank dengan nasabah, menjadi terbuka dengan adanya *sharing* data dengan pihak ketiga. Pemrosesan data pribadi nasabah didasarkan pada persetujuan nasabah (*consumer consent*) sehingga fokus utama *open banking* akan beralih pada bagaimana nasabah dapat melakukan kontrol dan memaksimalkan manfaat dari penggunaan data perbankan mereka (Leong, M. 2020: 1). Kerangka hukum perlindungan data pribadi nasabah yang memadai diperlukan untuk dapat melindungi nasabah secara efektif di era *open banking*. Kebijakan mengenai pemberitahuan privasi yang mengatur syarat dan ketentuan penggunaan data nasabah yang diwajibkan oleh peraturan dapat menjadi dasar pengawasan dan penegakan hukum terhadap perlindungan data pribadi nasabah. Aturan juga akan bermanfaat bagi regulator serta dapat

menetapkan ekspektasi perilaku industri secara luas terhadap data pribadi nasabah (World Bank Group, 2021: 12).

Inisiasi penerapan *open banking* tertuang dalam “*Blueprint Sistem Pembayaran Indonesia*” 2025 (BSPI 2025) yang menjadikan *open banking* sebagai salah satu visi untuk memaksimalkan digitalisasi perbankan sebagai lembaga utama dalam sektor ekonomi keuangan digital yang berbasis data dan teknologi (Kurniawan, 2021: 14). BI sebagai regulator menginisiasi *open banking* melalui standardisasi Open API yang mencakup standar data, teknis keamanan, dan *governance*. Beberapa regulasi telah dikeluarkan oleh BI mengenai *open banking* di antaranya: Standar Nasional Open API Payment yang disusun BI bersama ASPI (Asosiasi Sistem Pembayaran Indonesia) (“SNAP”) dan Peraturan Anggota Dewan Gubernur Nomor 23/15/PADG/2021 tentang Standar Nasional *Open Application Programming* Pembayaran (“PADG SNAP”). SNAP dan PADG SNAP merupakan peraturan pelaksana dari Peraturan Bank Indonesia Nomor 23/11/PBI/2021 tentang Standar Nasional Sistem Pembayaran. Implikasi dari peraturan tersebut akan berkaitan erat dengan kerangka hukum perlindungan data pribadi yang diatur dalam Undang-Undang Nomor 27 Tahun 2022 tentang Data Pribadi (“UU PDP”) (Fauzan, 2023: 48).

Inggris merupakan salah satu negara penginisiasi *open banking* di dunia yang diawali dengan berlakunya PSD2 (*Second Payment Services Directive*) serta perintah wajib terhadap 9 bank terbesar di Inggris yaitu HSBC, Barclays, RBS, Santander, Bank of Ireland, Allied Irish Bank, Danske, Lloyds, dan Nationwide untuk menyediakan data nasabah secara aman dan terstandardisasi kepada pihak ketiga melalui API (wired.co.uk). Inggris menunjukkan peningkatan positif penerapan *open banking* terhadap perkembangan sektor keuangan nasionalnya. Pay.UK melaporkan bahwa angka pembayaran yang dilakukan melalui *open banking* berada di sekitar 4,5 billion euro, data ini menjadi angka tertinggi sejak Inggris menerapkan *open banking* pada tahun 2018. Angka pengguna *open banking* di Inggris mencapai angka 7 juta pengguna (openbankingexpo.com).

Selain PSD2, Inggris menerapkan GDPR (*General Data Protection Regulation*) dalam kerangka hukum perlindungan data pribadi di era *open banking*. GDPR menekankan pada perlindungan data pribadi, sedangkan, PSD2 menekankan terbukanya pasar *open banking* yang akan berdampak pada sharing data nasabah dengan pihak ketiga (TPPs) meliputi fintech, *ride hilling*, *e-commerce*, dan perusahaan startup untuk mendorong kompetisi dan inovasi. GDPR dan PSD2 menganut prinsip bahwa individu sebagai pemilik data sehingga semua tindakan yang dilakukan terhadap data pnsabah harus didasarkan atas kontrol dan *explicit consent*, meliputi individu harus dapat memilih bagaimana data mereka akan digunakan, dan dengan siapa data mereka akan dibagikan.

Kesuksesan Inggris dalam menerapkan *open banking* patut dijadikan bahan pembelajaran bagi Indonesia (Muqorobin, 2021: 82). Dilansir dari Fintech Times, perkembangan pengaturan menjadi salah satu faktor keberhasilan pertumbuhan *open banking* yang masif di Inggris. Kepastian hukum perlindungan data pribadi nasabah yang aman menjadi faktor keberhasilan karena nasabah mungkin saja ragu untuk membagikan data keuangan kepada pihak ketiga jika keamanan data pribadi

mereka tidak terjamin sehingga regulator perlu memberikan kerangka hukum perlindungan data pribadi nasabah yang sesuai untuk menjaga kepercayaan nasabah bank di era *open banking*.

Inggris dan Indonesia memiliki kecenderungan yang sama dalam menerapkan peraturan mengenai *open banking* dimana kedua negara menerapkan pendekatan *regulatory-driven* (Sugarda, 2022: 170). Adopsi penerapan *open banking* di Indonesia diharapkan mampu meningkatkan perkembangan sektor keuangan, menciptakan inklusi keuangan, selaras dengan peningkatan perekonomian nasional. Hal ini dapat terwujud dengan kepastian hukum dalam perlindungan data pribadi nasabah agar menciptakan kepercayaan kepada nasabah, pihak bank, pihak ketiga, maupun stakeholders untuk ikut serta dalam penerapan *open banking*. Dari uraian di atas, penulis meneliti Pelindungan Hukum Data Pribadi Nasabah di Era *Open Banking* dengan fokus kajian perbandingan hukum antara Indonesia dan Inggris.

METODE PENELITIAN

Penelitian ini adalah penelitian hukum yuridis normatif yang sifatnya preskriptif dan terapan sehingga penelitian hukum ini bertujuan untuk menjawab permasalahan hukum yang dihadapi dan nantinya dapat diterapkan. Pendekatan penelitian ini menggunakan pendekatan perundang-undangan (*statutory approach*) dan pendekatan perbandingan (*comparative approach*). Penelitian ini membandingkan Undang-Undang Nomor 27 Tahun 2022 dan SNAP BI, kemudian dibandingkan dengan UK-GDPR dan Payment Services Regulation di Inggris serta menggunakan aturan lainnya terkait implimentasi *open banking* di kedua negara tersebut. Teknik pengumpulan bahan hukum dalam penelitian ini adalah studi kepustakaan (*library research*) dengan teknik analisis bahan hukum dengan metode silogisme deduktif dengan menarik kesimpulan dari suatu pernyataan atau fakta yang bersifat umum menjadi khusus. (Peter Mahmud Marzuki, 2021: 40).

ANALISIS DAN PEMBAHASAN

1. *Open Banking* di Indonesia

Hukum perlindungan data pribadi di Indonesia secara umum mengacu pada UU PDP. Undang-Undang ini menjadi dasar perlindungan hukum terhadap data pribadi dalam pemrosesan data agar hak konstitusional subjek data pribadi bisa terpenuhi. Rangkaian pemrosesan data pribadi yang diatur dalam UU PDP meliputi: pemerolehan dan pengumpulan; pengolahan dan penganalisisan; penyimpanan; perbaikan dan pembaruan; penampilan, pengumuman, transfer, penyebarluasan, atau pengungkapan; dan atau penghapusan atau pemusnahan. Pemrosesan data pribadi harus dilaksanakan berdasarkan prinsip-prinsip perlindungan data pribadi yang meliputi ketentuan bahwa pemrosesan data pribadi dilakukan secara terbatas dan spesifik, sah secara hukum, dan transparan; sesuai tujuan; menjamin hak subjek data pribadi; akurat, lengkap, tidak menyesatkan, mutakhir, dan dapat dipertanggungjawabkan; dilakukan dengan melindungi keamanan data pribadi dari pengaksesan yang tidak sah, pengungkapan yang tidak sah, penyalahgunaan, perusakan, dan atau penghilangan data pribadi; memberitahukan tujuan dan aktivitas pemrosesan serta kegagalan perlindungan data pribadi; data pribadi dimusnahkan dan/atau dihapus setelah masa retensi berakhir atau berdasarkan permintaan subjek data pribadi; serta pemrosesan data pribadi dilakukan secara bertanggung jawab dan dapat dibuktikan secara jelas (Pasal 16 ayat

(2)). Peraturan mengenai perlindungan data pribadi dapat ditemukan juga dalam beberapa peraturan perundang-undangan, namun dalam konteks perlindungan data pribadi nasabah di era *open banking* tunduk pada UU PDP. UU PDP menentukan dua jenis yaitu data pribadi menjadi dua yaitu data pribadi yang bersifat spesifik dan data pribadi yang bersifat umum. Implementasi *open banking* berkaitan dengan pemrosesan data pribadi nasabah yang termasuk dalam data pribadi spesifik yaitu data keuangan pribadi. (Fauzan, 2023: 49).

Open banking yang diinisiasi Bank Indonesia saat ini masih berada dalam koridor sistem pembayaran, sebagaimana menjadi tugas Bank Indonesia untuk mengatur dan menjaga kelancaran sistem pembayaran berdasarkan UU BI (Asti Rachma Alya, 2021: 170). Bank Indonesia mewujudkan inisiasi *open banking* dengan mengeluarkan “Peraturan Anggota Dewan Gubernur Nomor 23/15/2021 tentang Implementasi Standar Nasional *Open Application Programming Interface* Pembayaran” (“PADG SNAP”). PADG SNAP memberikan aturan standar dalam pelaksanaan *open API* Pembayaran yang dituangkan dalam standar teknis dan keamanan, standar data, spesifikasi teknis SNAP, dan pedoman tata kelola SNAP. (Pasal 4 ayat (3) PADG SNAP).

Open banking erat kaitannya dengan sektor keuangan dan perlindungan data pribadi sehingga lembaga yang mengawasi penyelenggaraan *open banking* adalah Kementerian Komunikasi dan Informasi, Otoritas Jasa Keuangan (OJK), dan Bank Indonesia. Kementerian Komunikasi dan Informasi mengawasi aktivitas dalam bidang komunikasi dan informatika, termasuk penggunaan data pribadi. OJK mengawasi lembaga keuangan. Bank Indonesia mengawasi seluruh alur sistem pembayaran dan kebijakan moneter dalam perbankan. Sebagai lembaga yang mengeluarkan SNAP, penyelenggaraan *open banking* di Indonesia melalui *Open API Payment* menjadi tanggung jawab BI. BI juga bekerja sama dengan *Self-Regulatory Organization* yaitu Asosiasi Sistem Pembayaran Indonesia (“ASPI”) dalam penyelenggaraan *open API payment*. ASPI ditugaskan oleh Bank Indonesia untuk mendukung implementasi kebijakan *open API* Pembayaran; mendukung implementasi proses perizinan, persetujuan, dan pengawasan; menyusun dan menerbitkan ketentuan di bidang Sistem Pembayaran yang bersifat teknis dan mikro berdasarkan persetujuan Bank Indonesia; dan menyusun dan mengelola standar yang ditetapkan oleh Bank Indonesia.

2. *Open Banking* di Inggris

Dasar hukum perlindungan data pribadi nasabah di Inggris didasari pada UK *Data Protection Act* 2018 (“UK DPA”) yang merupakan adaptasi dari *General Data Protection Rules* (GDPR) Uni Eropa ke dalam sistem hukum nasional Inggris. Section 2 UK DPA mengatur enam prinsip dalam perlindungan data pribadi yaitu: (1) pemrosesan data pribadi harus sah dan adil; (2) tujuan pemrosesan data harus ditentukan secara eksplisit dan sah; (3) data pribadi harus memadai, relevan, dan tidak berlebihan; (4) data pribadi harus akurat dan selalu diperbarui; (5) data pribadi disimpan tidak lebih lama dari waktu yang diperlukan; (6) data pribadi diproses secara aman. Lebih lanjut, aturan *open banking* Inggris diatur dalam “Statutory Instruments 2017 Number 752 on The Payment Services Regulations 2017” (PSRs) yang secara umum mengatur mengenai sistem pembayaran untuk mewajibkan penyedia jasa pembayaran membuka sistem mereka kepada pihak ketiga. PSRs mengatur mekanisme keterbukaan data oleh lembaga keuangan sebagai partisipan *open banking* seperti jenis data

apa saja yang dapat dibagikan, dari akun mana data dapat dibagikan, kewajiban standardisasi hingga aturan mengenai lembaga implementasi dan lembaga pengawas implementasi *open banking*.

Inggris membentuk “OBIE” sebagai lembaga independen yang bertujuan untuk menciptakan ekosistem *open banking* yang transparan dan terbuka yang dapat mendukung aksesibilitas, penggunaan, dan inovasi. OBIE merupakan entitas merupakan salah satu bagian dari “*Retail Banking Market Investigation Order 2017*” (CMA Order) yang mewajibkan bank yang termasuk dalam CMA9 untuk membentuk entitas implementasi *open banking*. Hal ini karena CMA memiliki keterbatasan yaitu tidak dapat memberikan standar teknis khusus dalam peraturan yang dikeluarkan sehingga desain dari *open banking* didelegasikan kepada “*The Trustee*” yang bertugas membentuk “OBIE”. OBIE melaksanakan wewenangnya bersama *stakeholders* dalam industri perbankan dan keuangan untuk mengaktualisasikan *open banking*. Pendanaan dari OBIE berasal dari CMA9, sedangkan FCA dan *Her Majesty Treasury* (“*HM Treasury*”) menjalankan peran pengawasan dari sisi Pemerintah. OBIE berperan sebagai penjaga *open banking* berstandar APIs dan memiliki *Directory of Open Banking Participants* yang menyediakan “whitelist” yaitu partisipan yang aktif dalam ekosistem *open banking* Inggris.

Saat ini OBIE telah bertransformasi menjadi “OBL” atau *Open Banking Limited*. OBL memiliki tugas dan wewenang yang sama dengan OBIE dan telah menetapkan kerangka kerja tata kelola untuk mengawasi penyedia layanan pembayaran dan penyedia pihak ketiga untuk mematuhi Standar *Open Banking*, mewajibkan pendaftaran untuk kepatuhan dengan standar teknis dan keamanan dan partisipasi dalam proses pengujian dan sertifikasi berdasarkan CMA Order 2017. Entitas lain yang mengawasi kegiatan *Open Banking* adalah “*Joint Regulatory Oversight Committee (JROC)*” yang terdiri dari *Financial Conduct Authority* dan *Payment Systems Regulator* sebagai ketua bersama, *HM Treasury* dan CMA sebagai anggota, yang mengawasi perkembangan dan memberikan rekomendasi bagi *Open Banking* Inggris di masa depan.

Open banking berkaitan erat dengan kepatuhan terhadap hukum perlindungan data pribadi sehingga implementasinya turut diawasi oleh lembaga independen nonpemerintah yaitu *Information Commissioner’s Office* (“ICO”). Lembaga ini secara khusus pelaksanaan mengawasi perlindungan data pribadi. ICO memiliki kewajiban untuk menegakkan hukum UK GDPR, DPA 2018, “*Freedom of Information Act 2000*” (FOIA), “*the Environmental Information Regulations 2004*” (‘EIR’), dan “*the Privacy and Electronic Communications Regulations 2003*” (‘PECR’). ICO melaksanakan kewajibannya dengan memberikan pedoman kepada individu maupun organisasi, mengatasi masalah, dan mengambil tindakan yang tepat ketika ada pelanggaran hukum.

3. Perbandingan dan Hal yang Dapat Dipelajari oleh Indonesia

Kewenangan mengawasi *Open Banking* di Indonesia dimiliki oleh Kemkominfo, OJK, dan BI. Kemkominfo sebagai lembaga yang mengawasi segala kegiatan yang berada dalam sistem elektronik. OJK berperan sebagai lembaga yang mengawasi segala aktivitas lembaga jasa keuangan. BI mengawasi segala kegiatan yang berkaitan dengan sistem pembayaran. ASPI sebagai SRO yang membantu Pemerintah dalam implementasi *open banking* dan tidak

memiliki kewenangan mengawasi dan memberi sanksi, hanya sebatas lembaga enabler yang menerbitkan standar API untuk kepentingan industri. Belum ada lembaga yang secara khusus mengawasi kegiatan *open banking*.

Sedangkan di Inggris, terdapat beberapa lembaga yang mengawasi kegiatan *open banking*. *Open banking* di Inggris diawasi oleh CMA, FCA, HM Treasury, OBIE/OBL dan JROC. Secara khusus, FCA memberikan mandat kepada OBIE untuk memastikan implementasi *open banking* berjalan sesuai yang diharapkan. Kemudian, OBIE membentuk JROC untuk mengawasi implementasi *open banking* yang anggotanya terdiri HM Treasury, FCA, dan CMA.

Lembaga pengawas *Open Banking* di Inggris lebih mumpuni karena memiliki lembaga khusus dan komite khusus yang mengawasi *open banking*. Spesifikasi kelembagaan ini dapat diterapkan oleh Indonesia karena dengan adanya lembaga yang ditunjuk khusus untuk mengawasi *open banking*, pengawasan akan lebih optimal karena organ yang dibentuk akan memiliki sumber daya yang lebih memahami implementasi *open banking*. Pemerintah juga perlu segera membentuk lembaga independen yang dimandatkan oleh UU PDP sebagai lembaga pengawas dalam sektor perlindungan data pribadi.

Perbedaan lain dari segi lembaga pengawas, implementasi *open banking* di Inggris diawasi oleh *Competition Market Authority* (CMA) yang merupakan lembaga pengawas persaingan usaha. Wewenang CMA terhadap *Open Banking* di Inggris berpusat pada peningkatan persaingan dan inovasi di sektor keuangan dengan memastikan data sharing dan interoperabilitas. Dalam menjalankan tugasnya, CMA didasari atas prinsip keamanan data dan otonomi pengguna yang bertujuan untuk menciptakan pasar keuangan yang lebih kompetitif dan berpusat pada pelanggan (Borgogno & Colangelo, 2020: 40).

Sedangkan, di Indonesia, ruang lingkup kewenangan Komisi Pengawas Persaingan Usaha (“KPPU”) belum secara khusus berperan langsung dalam mengawasi persaingan industri perbankan dan keuangan dalam *open banking*. Tidak seperti CMA yang menginisiasi *open banking*, inisiasi *open banking* di Indonesia diprakarsai oleh Bank Indonesia. Menurut penulis, dalam perkembangan implementasi *open banking* API ke depannya di Indonesia, KPPU dapat mengambil bagian sebagai pengawas. Hal ini karena keterbukaan data akan menimbulkan penguasaan data oleh pelaku usaha sebagai pengendali data yang jika tidak disikapi secara tepat dan hati-hati akan mengarah pada persaingan monopolistik yang berdampak pada kondisi pasar di sektor keuangan.

SIMPULAN

Dari studi komparasi ini, Inggris dan Indonesia memiliki pendekatan yang sama dalam skema *open banking* yaitu *regulatory* atau *mandatory approach* dengan adanya CMA Order 2017 dan PSD2 di Inggris serta PBI SNAP dan PADG SNAP di Indonesia. Inggris berhasil menciptakan ekosistem *open banking* yang aman dan inovatif melalui regulasi dan lembaga implementasi dan lembaga pengawas khusus seperti OBL. Di sisi lain, Indonesia masih dalam tahap pengembangan dengan regulasi yang diinisiasi oleh Bank Indonesia. Untuk meningkatkan kepercayaan dan keamanan data nasabah, Indonesia perlu memperkuat kerangka hukum perlindungan data pribadi dan perlindungan konsumen serta membentuk lembaga pengawas yang khusus mengawasi

implementasi open banking. Pembelajaran dari Inggris terkait lembaga implementasi dan lembaga pengawas khusus *open banking* melalui *Open Banking Limited*, dapat membantu Indonesia dalam mempercepat adopsi *open banking* yang aman, inovatif, dan dapat dipercaya oleh masyarakat.

DAFTAR PUSTAKA

- Kristianti, I. Tulenan, V. M. (2021). Dampak Financial Technology Terhadap Kinerja Keuangan Perbankan. *Kinerja: Journal of Economic and Bussiness Unmul*. 18(1). 57-65.
- Muqorobin. M.M., Anggraini, A., dkk. (2021). Pengaruh Open Banking berbasis Open API terhadap Eksistensi Perbankan. *MAKSIMUM: Media Akuntansi Universitas Muhammadiyah Semarang*. 11(2). 75-84.
- Leong, M. (2020). Open Banking: The Changing Nature of Regulating Banking Data - A Case Study of Australia and Singapore. *Banking & Finance Law Review*. 35(3). 443-469.
- Nathania, S. A., Abubakar, L., & Handayani, T. (2023). Implikasi Hukum Pemanfaatan Open Application Programming Interface Terhadap Layanan Perbankan Dikaitkan Dengan Ketentuan Perbankan Digital. *Jurnal Poros Hukum Padjadjaran*, 4(2), 244-259.
- Omarini, A. (2018). The Digital Transformation in Banking and The Role of FinTechs in the New Financial Intermediation Scenario. *International Journal of Finance, Economics, and Trade (IJFET)*. 1(1). 1-6.
- Rahadiyan, I. (2022). Perkembangan Financial Technology di Indonesia Dan Tantangan Pengaturan Yang Dihadapi. *Mimbar Hukum*. 34(1). 210-236.
- Benuf, K., Mahmudah S., Priyono A. E. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology di Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*. 3(2). 145-160.
- Amalya, R.A. (2021). Perlindungan Data Pribadi Nasabah Perbankan Dalam Implementasi Kebijakan Pembukaan Data Nasabah Perbankan Kepada Pihak Ketiga (Open Banking) Sebagai Upaya Interlink Perbankan Dan Penyelenggara Fintech. Tesis, Fakultas Hukum, Universitas Indonesia.
- Fauzan, P. (2023). Perlindungan Hukum Data Nasabah di Era Open Banking API (Application Programming Interface). Skripsi, Fakultas Hukum, Universitas Sebelas Maret.
- Kurniawan, A. (2021). Pertanggungjawaban Bank Terhadap Risiko Pelanggaran Data Pribadi Nasabah dalam Penyelenggaraan Open Banking. Skripsi, Fakultas Hukum, Universitas Indonesia.
- Peter Mahmud Marzuki. 2021. *Penelitian Hukum Edisi Revisi*. Jakarta: Penerbit Kencana.
- World Bank Group. Ministry of Foreign Affairs of the Netherland. 2021. *Technical Note. The Role of Consumer Consent in Open Banking*.