ISSN (P): (2580-8656)
ISSN (E): (2580-3883)

LEGAL STANDING
JURNAL ILMU HUKUM

Vol.8 No.3a, Desember 2024

PERLINDUNGAN DATA BIOMETRIK DALAM SEKTOR PERBANKAN DI INDONESIA DAN AMERIKA SERIKAT

Ainunnisa Rezky Asokawati
Universitas Indonesia, Jl. Lingkar, Depok, Jawa Barat, Indonesia
ainunnisa.rezky.asokawati@gmail.com

ABSTRACT

This study aims to analyze and compare the regulation and implementation of biometric data protection in the banking sector in Indonesia and the United States. In addition, this study also evaluates the security risks of biometric data and provides policy recommendations to improve its protection. This study uses a doctrinal method using primary and secondary legal sources. The focus of this study is to examine how the Indonesian State protects biometrics as personal data in a legal context and to compare the regulations and implementation related to biometrics in the banking sector in Indonesia and the United States. Based on the results of the study, in general, it was found that both have regulated the financial services sector, especially banking, and the technical management of personal data of customers and/or prospective customers. However, there are no detailed regulations aimed at protecting the biometrics of banking consumers. The absence of specific regulations on biometric data protection in the banking sector requires banks to take proactive steps in securing customer data, such as strengthening security systems and adopting strict internal policies. In addition, the government needs to consider creating more detailed regulations to provide legal certainty and better protection for consumers.

Penelitian ini bertujuan untuk menganalisis dan membandingkan regulasi serta implementasi perlindungan data biometrik dalam sektor perbankan di Indonesia dan Amerika Serikat. Selain itu, penelitian ini juga mengevaluasi risiko keamanan data biometrik dan memberikan rekomendasi kebijakan untuk meningkatkan perlindungannya. Penelitian ini menggunakan metode doktrinal dengan menggunakan sumber hukum primer dan sekunder. Fokus pada penelitian ini adalah meneliti bagaimana upaya Negara Indonesia melindungi biometrik sebagai data pribadi dalam konteks hukum serta membandingkan pengaturan dan penerapan terkait biometrik dalam sektor perbankan pada Negara Indonesia dan Negara Amerika Serikat. Berdasarkan hasil penelitian, secara umum didapati keduanya telah mengatur sektor jasa keuangan, khususnya perbankan, dan teknis pengelolaan data pribadi para nasabah dan/atau calon nasabah. Namun, belum ada pengaturan secara mendetil yang ditujukan untuk melindungi biometrik para konsumen perbankan tersebut. Ketiadaan regulasi khusus tentang perlindungan data biometrik di sektor perbankan mengharuskan bank untuk mengambil langkah proaktif dalam mengamankan data nasabah, seperti memperkuat sistem keamanan dan mengadopsi kebijakan internal yang ketat. Selain itu, pemerintah perlu mempertimbangkan pembuatan regulasi yang lebih rinci untuk memberikan kepastian hukum dan perlindungan yang lebih baik bagi konsumen.

Kata Kunci: *Data Biometrik, Sektor Perbankan, Perlindungan Data.*

A. PENDAHULUAN

Penggunaan biometrik dalam sektor perbankan merupakan salah satu upaya perlindungan nasabah yang diterapkan pada sektor perbankan di Indonesia. Data biometrik menjadi dasar untuk mengidentifikasi keunikan antarindividu yang menjadi bahan verifikasi nasabah (Hukumonline, 2022). Biometrik digunakan sebagai salah satu upaya menjalankan prinsip *Know Your Customer (KYC)* yang umum digunakan dalam sektor perbankan di berbagai belahan dunia. Data merupakan harta berharga pada saat ini, oleh karena itu terdapat istilah bahwa data saat ini adalah kekayaan jenis baru karena sangat bernilai (Supriyadi, 2022). Data pribadi berkaitan dengan informasi pribadi menyangkut orang personal. Penggunaan data ini umum digunakan dalam hal sehari-hari, termasuk dalam sektor perbankan.

Data pribadi atau *personal information* ini dianggap sebagai suatu hal yang harus dijaga sehingga dianggap sebagai sesuatu yang bersifat privat atau rahasia. Oleh karenanya, tidak dapat sembarangan disebarluaskan dan dipergunakan tanpa sepengetahuan dan seizin yang bersangkutan. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik menyatakan dalam Pasal 1 Angka 1 bahwa "Data pribadi adalah informasi spesifik tentang seseorang yang selalu diperbarui, akurat, dan rahasia" (Permenkominfo No. 20, 2016). Oleh karena itu, sudah sepatutnya data pribadi ini diberikan, disimpan, dan dipergunakan secara bijak.

Data pribadi juga termasuk dalam hak privasi. Hak ini telah diatur bahkan dari tingkatan Konstitusi Negara Republik Indonesia, yaitu pada Pasal 28G ayat (1) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (UUD NRI) setiap orang berhak atas perlindungan diri pribadi, yang mencakup kebebasan dari paksaan untuk berbuat atau tidak berbuat sesuatu, termasuk untuk mempertahankan keluarga, kehormatan, martabat, dan harta benda (UUD NRI 28G, 1945). Oleh karena itu, sebagai bagian dari hak atas privasi yang berkaitan dengan dan bahkan berhubungan dengan seseorang, Konstitusi mengharuskan informasi yang disimpan dan termasuk dalam kategori data pribadi ini diberikan rasa aman. Secara umum, pelanggaran mengenai data pribadi dibagi menjadi tiga jenis, yaitu pelanggaran kerahasiaan dengan membuka data pribadi tenpa izin atau secara tidak sah, pelanggaran ketersediaan yang umumnya akibat serangan siber dan mengakibatkan hilang akses atau rusaknya data pribadi, serta pelanggaran integritas yang merupakan perubahan data pribadi secara tidak sah (Deloitte, 2022).

Sektor perbankan merupakan sektor Penyedia Jasa Keuangan yang tergolong berisiko tinggi (*high risk*) berdasarkan *National Risk Assessment (NRA)* atau analisis risiko domestik terhadap Tindak Pidana Pencucian Uang (TPPU) tahun 2015 (PPATK, 2021a), dan secara spesifik bank umum menempati urutan kelima pada NRA tahun

2021 (PPATK, 2021b). Dalam rangka mencegah serta memberantas pencucian uang hingga pendanaan terorisme, *Financial Action Task Force (FATF)* telah mengeluarkan 40+9 rekomendasi sejak tahun 2009. Indonesia menggunakan rekomendasi-rekomendasi tersebut sebagai standar Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU dan PPT). Berdasarkan rekomendasi FATF, diperlukan adanya prinsip KYC atau *Customer Due Diligence (CDD)* (OJK, 2024b).

Melalui adanya perkembangan teknologi, CDD yang dilakukan untuk mengidentifikasi calon nasabah atau nasabah di Indonesia telah menggunakan biometrik. Biometrik yang digunakan pada sektor perbankan di Indonesia adalah biometrik menurut dokumen kependudukan yang tersedia di KTP berupa sidik jari dan iris mata yang didaftarkan pada saat pembuatan KTP (Verihubs, 2023). Namun, untuk memastikan bahwa pihak yang melakukan CDD elektronik adalah pihak asli pemilik identitas tersebut dan mencegah adanya penggunaan data orang lain, maka terdapat teknologi *liveness detection* pada saat verifikasi biometric (Vida, 2022). Perkembangan teknologi saat ini bahkan memungkinkan adanya biometrik suara yang digunakan dalam sektor perbankan (Yudistira, 2018). Maka, pembahasan pada artikel ini berorientasi pada urgensi perlindungan data pribadi terkait dengan biometrik yang digunakan dalam sektor perbankan dan membandingkan dengan Amerika Serikat.

Terdapat dua tujuan yang hendak dicapai. *Pertama*, bagaimana upaya Negara Indonesia melindungi biometrik sebagai data pribadi dalam konteks hukum. *Kedua*, artikel bermaksud untuk menggali bagaimana perbandingan pengaturan dan penerapan terkait biometrik dalam sektor perbankan pada Negara Indonesia dan Negara Amerika Serikat.

Artikel ini memiliki pembaharuan yang didasarkan pada artikel-artikel yang telah terbit sebelumnya. *Pertama*, penelitian oleh Rizki & Salam (2023). Penelitian ini memiliki fokus pada penjabaran mengenai biometrik yang menjadi bagian data pribadi, praktik pengumpulan data biometrik yang dilakukan tidak dengan persetujuan dari pemilik data oleh *Artificial Intelligence* (AI) atau kecerdasan buatan, dan pertanggungjawaban berdasarkan hukum terhadap praktik pengumpulan data biometrik melalui teknologi kecerdasan buatan. Perbedaan artikel yang ditulis dengan artikel milik Rizki & Salam (2023) adalah penelitian ini menekankan pada pembahasan biometrik dan kaitannya dengan sektor perbankan. Terakhir, perbedaan juga ada pada negara yang menjadi bahan pembanding. Kedua, artikel Pramuditha et al. (2023). Artikel ini membahas mengenai perbankan dalam hal penerapan *mobile banking* sebagai bagian dari saluran elektronik yang digunakan dalam sektor perbankan. Persamaan artikel tersebut dengan artikel ini adalah mengenai pembahasan terkait biometrik yang digunakan pada sektor perbankan. Namun, artikel ini tidak mendalami pembahasan mengenai saluran elektronik yang digunakan pada sektor perbankan, dalam hal ini *mobile banking*. Artikel ini hanya berfokus pada pengumpulan data biometrik sebagai

data pribadi yang digunakan pada sektor perbankan pada Negara Indonesia dan Negara Amerika Serikat serta perlindungan terhadap data pribadi.

B. METODE

Pendekatan doktrinal berdasarkan kriteria hukum digunakan dalam penelitian ini (Soekanto & Mamuji, 2013). Teknik penelitian doktrinal, menurut Soetandyo Wignjosoebroto, adalah studi tentang hukum yang dibentuk dan dikonseptualisasikan dengan menggunakan doktrin yang dipilih oleh pembuat atau konseptornya (Efendi & Ibrahim, 2018). Bentuk penelitian hukum doktrinal dipilih karena penelitian ini berfokus pada doktrin-doktrin dan asas-asas hukum, yaitu yang berkaitan dengan perlindungan data pribadi dan pengaturan perlindungan data pribadi yang masih ditemukan secara sporadis di dalam hukum Amerika Serikat. Tujuan dari penelitian ini adalah untuk memberikan jawaban atas permasalahan hukum yang menjadi pokok bahasan dalam penelitian ini. Dalam penelitian ini, digunakan penelitian yuridis normatif, yaitu penelitian yang mengkaji sistem norma hukum. Dengan demikian, aturan-aturan yang berkaitan dengan biometrik dalam industri perbankan di Indonesia dan Amerika Serikat akan dikaji dan dinilai melalui penggunaan jenis penelitian ini.

Kualitas data yang dikumpulkan melalui pengolahan dan analisis data dengan menggunakan metodologi kualitatif dan analitis menjadi sorotan utama dalam penelitian ini. Pendekatan ini menganalisis informasi yang dikumpulkan secara langsung dari informan dan sumber-sumber kepustakaan secara rinci, mendalam, dan lengkap (Emzir, 2014). Metode deduktif menguraikan landasan filosofis berupa asas, teori, dan konsep yang terdapat dalam berbagai peraturan perundang-undangan mengenai data pribadi, serta Undang-Undang Kerahasiaan Bank mengenai pengaturan biometrik sebagai bagian dari data pribadi dan perbankan. Dengan membandingkan fakta-fakta yang luas-seperti ilmu hukum, undang-undang, dan teori-dengan data yang spesifik, kesimpulan dibentuk dengan menggunakan teknik ini.

C. HASIL DAN PEMBAHASAN

1. Upaya Hukum Negara Indonesia dalam Melindungi Biometrik Sebagai Data Pribadi

Dimulai dari tingkat konstitusional, Indonesia memberikan perlindungan hukum terhadap hak-hak dasar masyarakat yang diuraikan dalam Bab XA tentang Hak Asasi Manusia, yang berisi Pasal 28A hingga 28J Undang-Undang Dasar Negara Republik Indonesia Tahun 1945. Hak atas privasi, yang mencakup data pribadi sebagai bagian dari informasi pribadi setiap orang, merupakan komponen penting dari hak asasi manusia yang mendasar. Data pribadi ini memiliki nilai signifikan karena tidak hanya menjadi bagian dari identitas individu tetapi juga mencerminkan hak atas perlindungan diri. Sebagai upaya untuk menjamin perlindungan data pribadi secara

spesifik, Indonesia telah menetapkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UUPDP). Dalam Pasal 1 angka 2 UUPDP ditegaskan bahwa pelindungan data pribadi bertujuan untuk "menjamin hak konstitusional Subjek Data Pribadi (SDP)."

Menurut Pasal 1 Angka 6, seseorang yang memiliki data pribadi dan berhak atas perlindungannya disebut sebagai subjek data pribadi. Pasal 28G ayat (1) UUD 1945 yang menyatakan bahwa setiap orang berhak atas perlindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, secara inheren sejalan dengan hak ini. Sebagai komponen fundamental dari individu, data pribadi adalah komponen penting dari manusia. Oleh karena itu, pelindungannya bukan hanya tanggung jawab individu tetapi juga negara melalui regulasi yang memastikan hak konstitusional setiap warga negara terjamin. Pengaturan dalam UUPDP menegaskan pentingnya perlindungan data pribadi dalam era digitalisasi, di mana informasi personal menjadi rentan terhadap penyalahgunaan. Dengan landasan hukum ini, Indonesia berdedikasi untuk menjunjung tinggi hak-hak warga negara atas privasi sesuai dengan norma-norma hak asasi manusia yang diterima secara luas.

Biometrik merupakan ciri manusia yang didapat berdasarkan karakteristik yang dimilikinya, sehingga dapat digunakan sebagai alat untuk mengidentifikasi dan memastikan keaslian subjek tersebut berdasarkan pembentuk identitasnya (Jasuindo, 2024). Dengan demikian, biometrik berisi informasi mengenai seseorang yang dapat digunakan untuk mengenalinya. Pengumpulan data berdasarkan biometrik masuk dapat dilakukan dengan menggunakan teknologi. Teknologi yang digunakan mengumpulkan informasi berdasarkan ciri khusus yang dimiliki subjek tersebut (Yudanto & Azis, 2019). Ciri khusus manusia yang diambil sebagai data biometrik umumnya adalah sidik jari, retina mata, raut wajah, tanda tangan, suara, iris mata, dan *keystroke* (Yudanto & Azis, 2019).

Biometrik di Negara Indonesia dianggap sebagai data pribadi yang bersifat spesifik (UUPDP 27, 2022), sehingga berdasarkan Penjelasan UUPDP data ini dapat menimbulkan dampak yang besar bagi SDP seperti akan timbulnya dampak tindakan diskriminatif dan potensi kerugian lain. Oleh karena itu, sifatnya tidak seperti nama, jenis kelamin, maupun status perkawinan yang bersifat Data Umum. berbeda dengan Data Pribadi yang bersifat spesifik, Data Umum lebih terbuka untuk diketahui oleh pihak selain daripada SDP. UUPDP tidak membatasi apa saja yang termasuk dalam kategori biometrik. Pada Penjelasan Pasal 4 ayat (1) huruf a, beberapa contoh yang disebutkan adalah sidik jari, retina mata, dan sampel DNA. Sehingga, undang-undang ini telah mengantisipasi apabila perkembangan teknologi semakin pesat dan memungkinkan adanya biometrik yang diambil dari seseorang sebagai cara untuk mengidentifikasi dan melakukan autentifikasi padanya.

Penggunaan biometrik ini merupakan suatu upaya yang dilakukan dengan alasan bahwa biometrik merupakan sistem keamanan yang paling mutakhir saat ini.

Biometrik memiliki beberapa keuntungan seperti akurasi dan kenyamanan, sebab biometrik berkaitan dengan data yang melekat dengan orang pribadi sehingga satu dengan yang lainnya memiliki keunikan masing-masing. Dengan demikian, akurasi keamanan menggunakan biometrik cenderung tinggi. Sebagai suatu upaya untuk mengidentifikasi dan melakukan verifikasi dengan tujuan keamanan, biometrik lebih mudah dibandingkan dengan metode keamanan tradisional yang menggunakan kata sandi (*password*) sehingga memberikan kenyamanan lebih pada pengguna (Nuswantoro, 2023).

Sejak UUPDP ditetapkan, hampir semua aspek data pribadi diatur dan dilindungi oleh undang-undang yang secara tegas dilindungi oleh undang-undang tersebut. UU No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UUITE) terkait erat dengan UUPDP sebagai langkah perlindungan. Pasal 26 ayat (1) UU ITE menyatakan bahwa, " Setiap penggunaan informasi mengenai data pribadi seseorang melalui media elektronik memerlukan persetujuan dari orang yang bersangkutan, kecuali jika peraturan perundang-undangan menentukan lain" Hal ini dikarenakan biometrik menggunakan teknologi elektronik (UUITE 26 (1), 2008).

Sektor keuangan sendiri memiliki pengaturan secara khusus yang diterbitkan oleh Otoritas Jasa Keuangan (OJK) maupun Bank Indonesia (BI). Prinsip-prinsip perlindungan aset, privasi, dan data konsumen digunakan untuk melindungi masyarakat dalam industri jasa keuangan, sesuai dengan peraturan OJK dalam Pasal 2 huruf d Peraturan Otoritas Jasa Keuangan Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat Sektor Jasa Keuangan (POJK 6, 2022). Salah satu perusahaan di industri keuangan yang tercakup dalam POJK ini adalah bank. Pelaku Usaha Jasa Keuangan (PUJK) yang merupakan lembaga yang menaungi industri jasa keuangan wajib menerapkan prinsip KYC untuk menjamin itikad baik dari calon konsumen dan/atau konsumen yang sudah ada. Hal ini dilakukan selain untuk mengumpulkan data konsumen, karena PUJK juga bertanggung jawab atas kerugian konsumen dalam hal PUJK terlibat, melakukan kesalahan, lalai, atau melakukan tindakan lain yang mengakibatkan kerugian, termasuk kerugian yang diakibatkan oleh bocornya informasi pribadi (PJOK 5, 2022).

Mengenai data pribadi yang dilindungi berdasarkan peraturan ini tidak secara eksplisit melindungi data pribadi biometrik konsumen, data dan/atau informasi pribadi dibagi menjadi data milik perseorangan dan korporasi (POJK 11, 2022). Data biometrik merupakan bagian dari kemajuan teknologi informasi. Sehingga, OJK kemudian mengatur dalam POJK Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi. POJK tersebut mengatur teknis bagaimana penyelenggaraan usaha perbankan menggunakan sistem teknologi dan informasi, termasuk dalam pemrosesan, perlindungan, dan pertukaran atas data pribadi nasabah yang dimiliki

oleh bank (PJOK 43-47, 2022). Bank dapat menyelenggarakan digitalisasi usahanya dengan tetap memperhatikan maturitas digital bank, termasuk juga dalam kesiapan dan ketangguhan bank dalam menjaga data pribadi nasabah dalam penyelenggaraan teknologi informasi untuk mendukung transformasi digital (PJOK 66, 2022).

Perihal pengumpulan data dan verifikasi melalui skema KYC dilakukan dalam upaya Uji Tuntas Nasabah (*customer due diligence*) atau pun Uji Tuntas Lanjut (*enhanced due diligence*) terhadap calon nasabah maupun nasabah yang dinilai berisiko tinggi. OJK mewajibkan adanya identifikasi dan verifikasi atas informasi yang diberikan oleh calon nasabah dengan skema pertemuan langsung atau *face to face* (POJK APU&PPT 17 (3), 2017). Namun, diberikan kemudahan untuk melakukan dengan skema elektronik, seperti *video banking* (ibid). Data biometrik yang dikumpulkan digunakan untuk otentifikasi keaslian data dan informasi yang diberikan, maka calon nasabah akan dimintakan kartu identitas seperti KTP elektronik dan sidik jari (POJK APU&PPT 17 (4) b, 2017).

Pengumpulan data biometrik yang menggunakan teknologi berupa media elektronik sebagai alat perekaman butuh adanya kesepakatan dari sang pemilik data. Maka, perlu adanya penyampaian informasi mengenai tujuan pengambilan data, keabsahan pihak yang meminta data, dan jaminan keamanan akan data yang diberikan (UUPDP 5, 2022). Sehingga, terdapat hak yang dilindungi secara undang-undang bagi SDP untuk mengetahui terlebih dahulu mengenai hal yang mendasari tindakannya untuk menyampaikan terkait data pribadi miliknya, terlebih jika hal ini berkaitan dengan data spesifik. Hal inilah yang merupakan keterkaitan antara data pribadi dengan hak privasi seseorang yang dilindungi oleh hukum pada Negara Indonesia. Keduanya saling berkelindan karena berkaitan dengan hak seseorang untuk menentukan apakah akan membuka atau tidak data pribadi miliknya, sebab dengan membuka data tersebut maka telah terjadi penyebaran kepada pihak lain yang harus ia ketahui secara rinci berkaitan dengan pihak penerima data tersebut termasuk pada peruntukannya.

Apabila seseorang tidak menghendaki data pribadi miliknya disebarluaskan atau merasa haknya atas privasi data pribadi terganggu, UUPDP tidak hanya memberikan hak untuk SDP dapat mengakses datanya yang telah diproses, bahkan UUPDP telah memberikan hak bagi pemilik data untuk dapat mengakhiri pemrosesan, menghapus, dan memberikan peluang untuk dapat membatalkan kesepakatan pemrosesan Data Pribadi miliknya (UUPDP 7 8 9, 2022). Sehingga, Penyelenggara Sistem Elektronik harus mengakomodir penghapusan Informasi Elektronik maupun Dokumen Elektronik serta wajib menghapusnya jika sudah tidak relevan atau dimintakan dengan penetapan pengadilan oleh (UUITE 26 (3)(4), 2008). Maka, Pasal 26 ayat (2) UUITE telah memberikan hak gugat yakni, “Gugatan atas kerugian yang diderita berdasarkan undang-undang ini dapat diajukan oleh setiap orang yang hak-haknya dilanggar sebagaimana dimaksud dalam ayat (1)” (UUITE 26 (2), 2008).

Ketentuan pidana juga diakomodasi oleh UUITE dan UUPDP. Sebagai contoh, UUPDP mengatur bahwa pihak yang mendapatkan atau mengumpulkan data pribadi, mengungkapkan data pribadi yang bukan miliknya, atau menggunakan data pribadi yang bukan miliknya untuk menguntungkan diri sendiri secara melawan hukum dapat dipidana penjara dan/atau denda (UUPDP 67, 2022). Dengan demikian, Indonesia secara umum telah mengakomodir adanya perlindungan biometrik sebagai suatu data pribadi melalui adanya UUITE, UUPDP, maupun peraturan teknis yang diatur dengan POJK.

2. Perbandingan Pengaturan dan Penerapan Terkait Biometrik dalam Sektor Perbankan di Indonesia dan Amerika Serikat

Sebagaimana telah dijelaskan sebelumnya, bahwa Indonesia tidak memiliki aturan yang secara khusus mengatur mengenai biometrik. Namun, berdasarkan Pasal 4 ayat (2) huruf b Undang-Undang Perlindungan Data Pribadi, biometrik sering diatur di Indonesia sebagai data pribadi tertentu (UUPDP 4, 2022). Sehingga, Indonesia mengakomodir biometrik ini sebagai suatu data pribadi yang perlindungannya sama dengan jenis lain yang dikategorikan sebagai data pribadi.

Menurut FATF, industri keuangan, termasuk perbankan, harus mematuhi konsep know your customer untuk mengidentifikasi nasabah potensial dan nasabah yang sudah ada, serta mengurangi kemungkinan pencucian uang dan pendanaan teroris. Upaya ini sebagai cara untuk menjalankan rezim anti tindak pidana pencucian uang dan pendanaan terorisme (APU&PPT). Proses identifikasi, verifikasi, dan pemantauan yang dilakukan oleh Bank sebagai Penyedia Jasa Keuangan (PJK) terhadap calon nasabah, nasabah yang sudah ada, atau nasabah yang baru datang untuk memastikan kesesuaian antara profil, karakteristik, dan/atau pola transaksi dikenal dengan istilah KYC atau CDD, atau dalam bahasa Indonesia dikenal dengan istilah Uji Tuntas Nasabah (*customer due diligence*) (POJK APU&PPT 1, 2017). Melalui proses CDD ini, bank sebagai PJK melakukan permintaan atas data pribadi sebagai cara untuk mengidentifikasi calon nasabah orang-perseorangan idengan menggunakan identitas kependudukan seperti KTP, SIM, NPWP, dan sebagainya termasuk juga tujuan pembukaan rekening dan sumber dana (OJK, 2024a). Meskipun CDD tidak berhenti pada proses mengenali calon nasabah, sebab bank sebagai PJK juga harus memantau transaksi jika disinyalir ada transaksi mencurigakan (Wati, 2019). Proses CDD secara konvensional dilakukan langsung antara pegawai bank dengan calon nasabah pada saat onboarding atau pendaftaran (Vida, 2022). Namun, saat ini perkembangan teknologi memungkinkan proses CDD dilakukan tanpa bertatap muka langsung.

Proses CDD saat onboarding dilakukan dengan mencocokan dokumen pribadi dengan individu calon nasabah. Identifikasi dan verifikasi disesuaikan dengan dua dasar, yaitu something you are dan something you have. Pertanyaan pertama dimaksudkan untuk mengetahui data pribadi pendaftar melalui dokumen yang

dimiliki, seperti e-KTP. Kemudian, otentikasi dilakukan dengan mencocokan rekam sidik jari yang tersimpan dalam chip KTP dengan sidik jari yang ditautkan dengan perangkat ponsel (OJK, 2024a). Sehingga, pada saat ini sektor perbankan di Indonesia menggunakan biometrik yang berkaitan dengan data pribadi yang disimpan oleh Kementerian Dalam Negeri Republik Indonesia melalui chip KTP, yaitu iris mata, sidik jari, dan potret wajah (Dukcapil, 2019).

Pasal 21 ayat (2) Peraturan Otoritas Jasa Keuangan telah mengatur beberapa cara untuk melakukan CDD, yakni melalui tatap muka langsung atau pun dilakukan secara elektronik (PJOK 21, 2023). Melalui POJK ini, diatur mengenai informasi data pribadi yang dapat diminta oleh PJK kepada Calon Nasabah atau Nasabah seperti, kartu identitas berupa KTP, tanda tangan, biometrik sebagaimana tersimpan dalam chip KTP, termasuk juga yang dikategorikan sebagai *something you have* seperti username, *password*, *personal identification number* (PIN).

Perlindungan data pribadi merupakan isu bersama bagi seluruh dunia. Informasi mengenai data pribadi yang dimiliki oleh masyarakat dikumpulkan oleh Pemerintah Federal Amerika melalui penggunaan teknologi informasi yang kemudian digunakan untuk keperluan pemerintahan, seperti penegakan hukum dan penyebaran Covid-19, dan juga sektor swasta (U.S. GAO, 2024). Bank menggunakan privacy notice untuk menginfokan kepada calon nasabah/nasabah mengenai informasi pribadi yang akan dikumpulkan dan kepada pihak mana saja informasi tersebut akan dibagi. *The Consumer Financial Protection Bureau* yang dapat memperbaharui mengenai *privacy notice* atau pemberitahuan privasi demi kepentingan transparansi dan edukasi bagi konsumen sektor perbankan.

Amerika memiliki dasar hukum secara umum untuk sektor keuangan dalam Gramm Leach-Billey Act Pasal 6821 tentang Perlindungan Privasi untuk Informasi Nasabah Lembaga Keuangan (*Privacy Protection for Customer Information of Financial Institutions*) (GLBA 6821, 1999). Menurut aturan ini, perlindungan biometrik tidak diatur secara khusus. Hal ini disebabkan oleh fakta bahwa data pribadi sering kali dibatasi dalam situasi ini. Larangan mengumpulkan informasi pelanggan dengan alasan palsu, baik oleh individu atau dengan meminta orang lain mengungkapkan informasi pelanggan dengan alasan palsu, tercakup dalam perlindungan data pribadi Pasal 6821. Setiap negara bagian tunduk pada peraturan tersebut. Setiap institusi yang berwenang untuk meninjau pengaturan dan pedoman lembaga keuangan di masing-masing negara bagian wajib memastikan bahwa lembaga keuangan pada negara tersebut memiliki dan melaksanakan perlindungan atas data pribadi nasabah untuk mencegah kebocoran data dan pengungkapan secara melawan hukum.

Sektor perbankan di Amerika Serikat telah mengatur hal ini dalam *Bank Secrecy Act (BSA)* atau disebut juga dengan *Currency and Foreign Transactions Reporting Act* (BSA, n.d.). Sebagaimana POJK Nomor 8 Tahun 2023, BSA juga mengatur

mengenai biometrik yang dipergunakan dalam sektor perbankan di Amerika Serikat pada electronic banking. Namun, secara khusus, Amerika juga tidak memiliki pengaturan khusus mengenai biometrik. Pada pengaturan ini, otentikasi dilakukan dengan menggunakan PIN dan juga diperkuat dengan biometrik, seperti sidik jari dan iris mata. Namun, pada bank di Amerika Serikat telah menggunakan adanya *voice biometric* atau biometrik suara dalam sektor perbankan (WSJ, 2023). Biometrik menggunakan suara merupakan terobosan terkini dalam sektor perbankan dan memiliki keunikan tersendiri bagi setiap individu. Maka, dengan teknologi terkini dan mutakhir, biometrik suara dapat menjadi pengaman yang ampuh dari peretas (Khan Mk & Aithal, 2024). Biometrik suara merupakan perpaduan kemampuan teknologi dengan biologi yang merupakan hasil kombinasi mulut dan tenggorokan dalam mengeluarkan suara yang unik bagi setiap individu. Maka, secara umum perlindungan atas data pribadi, termasuk penyebarannya, telah memiliki pengaturan tersendiri untuk sektor keuangan dan khususnya perbankan di Amerika. Namun, belum terdapat pengaturan secara spesifik bagaimana melindungi data pribadi dalam bentuk biometrik.

D. SIMPULAN

Negara Indonesia telah mengakomodir adanya peraturan yang melindungi data pribadi yang dalam hal ini adalah biometrik. Perlindungan ini diatur diantaranya dalam Undang-Undang Perlindungan Data Pribadi dan Undang-Undang tentang Informasi dan Transaksi Elektronik. Negara Amerika Serikat maupun Indonesia sendiri sudah mengakomodir pengaturan mengenai penggunaan biometrik ini dalam bidang perbankan. Namun, keduanya belum secara spesifik mengatur bagaimana melindungi biometrik sebagai data pribadi dalam bentuk digital. Negara Indonesia dan Negara Amerika Serikat telah memiliki pengaturan mengenai perbankan dan kaitannya dengan biometrik, namun perkembangan teknologi tetap harus diwaspadai. Sebagaimana dengan berkembangnya kecerdasan buatan, maka perlindungan hukum dan praktik penerapannya juga harus mengimbangi agar data pribadi tetap terlindungi. Perkembangan teknologi yang semakin pesat memaksa dunia untuk dapat melindungi data pribadi dalam bentuk digital termasuk yang diberikan kepada sektor perbankan. Maka, menjadi tanggung jawab bersama, baik pemilik data maupun perbankan sebagai PUJK untuk dapat mengelola, menjaga, dan mengawasi penggunaan dan penyebaran data pribadi nasabah perbankan.

E. DAFTAR RUJUKAN

BSA. (n.d.). *Bank Secrecy Act*. Amerika Serikat.

Deloitte. (2022). *Reforming Indonesia's Personal Data Protection Landscape*. Jakarta: Deloitte.

Dukcapil. (2019). *Dukcapil Beri Solusi Kemudahan e-KYC bagi Perbankan*. Direktorat Jenderal Kependudukan Dan Pencatatan Sipil Kementerian Dalam Negeri Republik Indonesia. https://dukcapil.kemendagri.go.id/phln/read/dukcapil-beri-solusi-kemudahan-e-kyc-bagi-perbankan

Efendi, J., & Ibrahim, J. (2018). *Metode Penelitian Hukum Normatif dan Empiris*. Kencana.

Emzir. (2014). *Metodologi Penelitian Kualitatif Analisis Data*. PT Raja Grafindo Persada.

GLBA 6821. (1999). *Undang-Undang Gramm-Leach-Bliley*. Amerika Serikat.

Hukumonline. (2022). *Peran Sertifikat Elektronik dalam Mendorong Legalitas dan Keamanan Proses e-KYC di Industri Jasa Keuangan*. Hukumonline.Com. https://www.hukumonline.com/berita/a/peran-sertifikat-elektronik-dalam-mendorong-legalitas-dan-keamanan-proses-e-kyc-di-industri-jasa-keuangan-lt62b59e6c19d9a/?page=2

Jasuindo. (2024). *Apa Itu Biometrik?* Jasuindo.Com. https://jasuindo.com/id/2024/03/27/apa-itu-biometrik/

Khan Mk, A., & Aithal, S. (2024). Implementation of Voice Biometric System in the Banking Sector. *International Journal of Applied Engineering and Management Letters*, *8*(1), 120–127. https://doi.org/10.47992/IJAEML.2581.7000.0217

Nuswantoro, S. A. (2023). *Interaksi Manusia dan Komputer: Pengantar dan Prinsip Dasar*. Indramayu: CV Adanu Abimata.

OJK. (2024a). *Kenalan Dulu Yuk Dengan Customer Due Diligence (CDD): Instrumen untuk Memitigasi Risiko-Risiko di Sektor Jasa Keuangan*. Otoritas Jasa Keuangan. http://sikapiuangmu.ojk.go.id/FrontEnd/CMS/Article/40705

OJK. (2024b). *Prinsip Mengenal Nasabah dan Anti Pencucian Uang*. Otoritas Jasa Keuangan. https://ojk.go.id/id/kanal/perbankan/Pages/Prinsip-Mengenal-Nasabah-dan-Anti-Pencucian-Uang.aspx

Permenkominfo No. 20. (2016). *Peraturan Menteri Komunikasi dan Informatika tentang Perlindungan Data Pribadi dalam Sistem Elektronik Nomor 20 Tahun 2016, BN Tahun 2016 No. 1829, Pasal 1 angka 1*.

PJOK 21. (2023). *Peraturan Otoritas Jasa Keuangan tentang Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme dan Pencegahan Pendanaan Proliferasi Senjata Pemusnah Massal di Sektor Jasa Keuangan, POJK Nomor 8 Tahun 2023, LN Tahun 2023 No. 11, Pasal 21 ay*.

PJOK 43-47. (2022). *Peraturan Otoritas Jasa Keuangan tentang Penyelenggaraan Teknologi Informasi, POJK Nomor 11/POJK.03/2022, LN Tahun 2022 No. 5/OJK TLN No. 5/OJK. Pasal 43-Pasal 47*.

PJOK 5. (2022). *Peraturan Otoritas Jasa Keuangan tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan Nomor 6/POJK.07/2022, LN Tahun 2022 No. 99 TLN No. 6788. Pasal 5 dan Pasal 6*.

PJOK 66. (2022). *Peraturan Otoritas Jasa Keuangan tentang Penyelenggaraan*

Teknologi Informasi, POJK Nomor 11/POJK.03/2022, LN Tahun 2022 No. 5/OJK TLN No. 5/OJK. Pasal 66 ayat (1).

POJK 11. (2022). *Peraturan Otoritas Jasa Keuangan tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan Nomor 6/POJK.07/2022, LN Tahun 2022 No. 99 TLN No. 6788. Pasal 11 ayat (2)*.

POJK 6. (2022). *Peraturan Otoritas Jasa Keuangan tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan Nomor 6/POJK.07/2022, LN Tahun 2022 No. 99 TLN No. 6788. Pasal 2 huruf d*.

POJK APU&PPT 1. (2017). *Peraturan Otoritas Jasa Keuangan tentang Perubahan Atas Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan, POJK No. 23 /POJK.01/2019, LN Tahun 20*. Pasal 1 angka 11

POJK APU&PPT 17 (3). (2017). *Peraturan Otoritas Jasa Keuangan tentang Perubahan Atas Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan, POJK No. 23 /POJK.01/2019, LN Tahun 20*. Pasal 17 ayat (3)

POJK APU&PPT 17 (4) b. (2017). *Peraturan Otoritas Jasa Keuangan tentang Perubahan Atas Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.01/2017 tentang Penerapan Program Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme di Sektor Jasa Keuangan, POJK No. 23 /POJK.01/2019, LN Tahun 20*. Pasal 17 ayat (4) huruf b

PPATK. (2021a). *Financial Integrity Rating on Money Laundering and Terrorist Financing*. Jakarta: Pusat Pelaporan dan Analisis Transaksi Keuangan.

PPATK. (2021b). *Penilaian Risiko Indonesia Terhadap Tindak Pidana Pencucian Uang Tahun 2021*. Jakarta: Pusat Pelaporan dan Analisis Transaksi Keuangan.

Pramuditha, P., Harto, B., Parlina, L., Hermawan, I., & Reniawaty, D. (2023). Model E-Channel Design System Dengan Bank Biometric Aplication Pada Bank Di Indonesia. *ATRABIS: Jurnal Administrasi Bisnis (e-Journal)*, *9*(1), 118–129. https://doi.org/10.38204/atrabis.v9i1.1284

Rizki, M. F., & Salam, A. (2023). Pertanggungjawaban Hukum Pengumpulan Data Biometrik Melalui Artificial Intelligence Tanpa Persetujuan Pemilik Data (Studi Kasus Clearview AI Inc. di Yunani dan Inggris). *Lex Patrimonium*, *2*(2), 1–16. https://scholarhub.ui.ac.id/lexpatri/vol2/iss2/9/

Soekanto, S., & Mamuji, S. (2013). *Penelitian Hukum Normatif: Suatu Tinjauan Singkat*. Raja Grafindo Persada.

Supriyadi, D. (2022). *Data Pribadi dan Dua Dasar Legalitas Pemanfaatannya*. Hukumonline.Com. https://www.hukumonline.com/berita/a/data-pribadi-dan-dua-dasar-legalitaspemanfaatannya-lt59cb4b3feba88/

U.S. GAO. (2024). *Protecting Personal Privacy*. U.S. Governement Accountability Office. https://www.gao.gov/protecting-personal-privacy

UUD NRI 28G. (1945). *Undang-Undang Negara Republik Indonesia Tahun 1945, Pasal 28G ayat (1)*.

UUITE 26 (1). (2008). *Undang-Undang Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU Nomor 9 Tahun 2016, LN Tahun 2016 No. 251 TLN No. 5952. Pasal 26 ayat (1)*.

UUITE 26 (2). (2008). *Undang-Undang Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU Nomor 9 Tahun 2016, LN Tahun 2016 No. 251 TLN No. 5952. Pasal 26 ayat (2)*.

UUITE 26 (3)(4). (2008). *Undang-Undang Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU Nomor 9 Tahun 2016, LN Tahun 2016 No. 251 TLN No. 5952. Pasal 26 ayat (3)(4)*.

UUPDP 27. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UUPDP). Pasal 4 ayat (1) huruf a*.

UUPDP 4. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UUPDP). Pasal 4 ayat (2) huruf b*.

UUPDP 5. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UUPDP). Pasal 5 ayat (1)*.

UUPDP 67. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UUPDP). Pasal 67*.

UUPDP 7 8 9. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UUPDP). Pasal 7, Pasal 8, dan Pasal 9*.

Verihubs. (2023). *Apa Itu Sistem Biometrik KTP dan Bagaimana Cara Kerjanya?* Verihubs.Com. https://verihubs.com/blog/biometrik-ktp-adalah/

Vida. (2022). *Peran Verifikasi Identitas Biometrik untuk Pendaftaran Rekening Online*. Vida.Id. https://vida.id/id/blog/the-role-of-biometric-identity-verification-for-online-account-registration

Wati, D. K. (2019). *KYC sebagai Peran Perbankan dalam Pemberantasan TPPU*. Pusat Pelaporan Dan Analisis Transaksi Keuangan. https://www.ppatk.go.id/siaran_pers/read/968/kyc-sebagai-peran-perbankan-dalampemberantasan-tppu.html

WSJ. (2023). *The Wall Street Journal. "I Challenged My AI Clone to Replace Me for 24 Hours"*. https://youtu.be/t52Bi-ZUZjA?si=85Sx_Emv3zq_yREH. Diakses pada tanggal 31 Mei 2024

Yudanto, Y., & Azis, A. (2019). *Pengantar Teknologi Internet of Things (IoT)*. Surakarta: UNS Press.

Yudistira, G. (2018). *Bank Permata Luncurkan Pemindai Suara Biometric Voice ID Untuk Verifikasi Nasabah*. Kontan.Co.Id. https://keuangan.kontan.co.id/news/bank-permata-luncurkan-pemindai-suara-biometric-voice-iduntuk-verifikasi-nasabah