TENGGARA STRATEGICS

Kajian kebijakan teknis turunan UU No. 1/2024
tentang Informasi & Transaksi Elektronik

Menakar Pengamanan Tepat Sasaran & Inklusi Keuangan dalam Transaksi Elektronik

September 2025

Didukung oleh:

Centre for Strategic and International Studies · TheJakartaPost · Universitas Prasetiya Mulya

Kajian kebijakan teknis turunan UU No. 1/2024
tentang Informasi & Transaksi Elektronik

Menakar Pengamanan Tepat Sasaran & Inklusi Keuangan dalam Transaksi Elektronik

Penelitian dari Tenggara Strategics.

Galby R. Samhudi
Bayo Andhika Putra
Rayhan Kalevi Barung
Dananjaya Rijaluzaman

Kajian kebijakan ini bertujuan memperkaya diskursus mengenai pengaturan transaksi elektronik di Indonesia yang tengah menyambut regulasi teknis terbaru, turunan dari UU No. 1/2024. Tim penulis menyampaikan apresiasi kepada semua pihak yang telah berkontribusi dalam penyelesaian naskah ini.

Pandangan yang disampaikan di sini sepenuhnya merupakan milik tim penulis dan Tenggara Strategics.

Penaggung jawab:
Riyadi Suparno

Desain dan tata letak:
Ferdinand Phoe
Andreas Meidyan
Shifa Rafida Fitri

Daftar isi

1. Ringkasan eksekutif

- Layanan transaksi keuangan digital, tengah mengalami pertumbuhan di Indonesia dan berpotensi mengalami disrupsi akibat kebijakan mengenai tanda tangan elektronik tersertifikasi (TTET) sebagai mandat UU No.1/2024 tentang Informasi dan Transaksi Elektronik (ITE). Pada peraturan tersebut transaksi digital yang dilakukan tidak dengan tatap muka didefinisikan sebagai transaksi risiko tinggi yang menggunakan TTET. Meski demikian, pengaturan transaksi keuangan tersebut masih bersifat terlalu umum dan masih memerlukan penjelasan lebih lanjut, khususnya mengenai risiko tinggi yang berbeda-beda di tiap sektor, apalagi pada transaksi digital yang seluruhnya dilaksanakan tanpa tatap muka secara fisik.
- Indonesia pada dasarnya sudah memiliki paket kebijakan pengamanan transaksi digital yang relatif lengkap, dengan setiap jenisnya memiliki derajat dasar hukum yang berbeda-beda. Berbagai skema pengamanan telah diimplementasikan pada sektor jasa keuangan digital, mulai dari verifikasi tahap awal melalui *One Time Password* (OTP) dan pertautan kata sandi (*password),* pembubuhan lapisan keamanan biometrik atau verifikasi nomor identifikasi personal (*Personal Identification Number*, PIN), verifikasi kartu identitas (melalui mekanisme *Know Your Customer*, KYC), dan lapisan keamanan lainnya, khususnya ketika terjadi transaksi anomali.
- Keberadaan mekanisme pengamanan yang sudah digunakan di Indonesia telah tumbuh secara organik sebagai bagian dari inovasi industri dalam merespons risiko keamanan siber, dengan tetap mempertimbangkan aspek inklusi keuangan. Penerapan kewajiban TTET justru berpotensi kontraproduktif karena dapat menghambat ruang inovasi sektor keuangan digital dan memperlambat perkembangan ekosistem ekonomi digital yang inklusif.
- Kesuksesan platform Indonesia Anti-Scam Centre (IASC) merupakan refleksi upaya para pelaku industri menekan *fraud* melalui pengamanan sistem dan kolaborasi dengan regulator. Model tersebut menunjukkan bahwa ketika diberi ruang, pelaku pasar mampu membentuk mekanisme anti-penipuan yang efisien tanpa intervensi regulasi yang relatif mengikat dan prosedural.
- Meski regulasi pelindungan data pribadi sudah ada, titik paling rentan justru berada pada sisi konsumen karena rendahnya literasi digital sehingga masih terdapat risiko kebocoran data dan penipuan.
- Kajian ini menghasilkan beberapa rekomendasi kebijakan, di antaranya:
    1. Definisi "Transaksi Elektronik yang memiliki risiko tinggi" perlu diperjelas dengan peraturan teknis turunan dari UU No. 1/2024 tentang ITE, yang pada saat ini masih memiliki definisi yang terlalu luas.
    2. Regulator sektor keuangan digital perlu terus mendorong inovasi aktor bisnis untuk menciptakan mekanisme pengamanan yang paling andal dan tepat dengan keadaan pasar, termasuk kolaborasi antar pelaku bisnis yang tercermin dari IASC yang turut mendorong diciptakannya upaya anti penipuan tanpa mekanisme regulasi yang kecenderungannya mengikat, prosedural, dan teknologi-spesifik.
    3. Perlindungan data pribadi masyarakat, khususnya para pengguna jasa transaksi digital, perlu menjadi perhatian regulator dalam rangka menciptakan ekosistem ekonomi digital yang menjunjung tinggi kepentingan perlindungan konsumen.
    4. Dalam rangka memastikan keseimbangan antara pengendalian risiko dan keberlanjutan inovasi di sub-sektor transaksi digital, pengaturan teknis terkait transaksi berisiko tinggi sebaiknya ditetapkan oleh regulator yang betul-betul memiliki kewenangan dan kekhususan pada area ini, seperti Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK).

2. Latar belakang

Dalam era digital yang berkembang pesat, transaksi elektronik semakin menjadi bagian tak terpisahkan dari kehidupan sehari-hari. Kegiatan transaksi elektronik merupakan buah dari adopsi teknologi pembayaran digital yang dibuat oleh para penyelenggara sistem elektronik yang bergerak dalam bidang keuangan digital, atau yang kerap disebut perusahaan *financial technology* (fintech). Saat ini, layanan fintech telah terintegrasi dengan sektor keuangan secara keseluruhan, sehingga baik bank maupun lembaga keuangan lainnya turut menyediakan layanan mereka secara digital.

Data dari Bank Indonesia (BI) menunjukkan bahwa nilai transaksi uang elektronik meningkat 34,62 persen dari Rp 1,85 kuadriliun di tahun 2023 menjadi Rp 2,5 kuadriliun pada tahun 2024. Pada Q1 2025, nilai transaksi uang elektronik mencapai Rp 739,41 triliun.[1] Salah satu faktor yang memengaruhi cepatnya pertumbuhan transaksi elektronik di Indonesia, terutama dalam beberapa tahun ke belakang, adalah pengadopsian mekanisme *Quick Response Code Indonesian Standard* (QRIS), yakni standar kode QR nasional yang dikembangkan oleh BI untuk memfasilitasi pembayaran digital lintas penyedia jasa sistem pembayaran secara mudah. Nilai transaksi QRIS di Indonesia meningkat dari hanya Rp 8,21 triliun dari 124,11 juta transaksi di tahun 2020 hingga mencapai Rp 659,93 triliun dari 6,24 miliar transaksi di tahun 2024.[2]

Peningkatan ini didukung oleh adopsi teknologi pembayaran digital yang semakin luas, seperti dompet digital (*e-wallet*) dan layanan perbankan digital. Perkembangan ini tidak hanya memudahkan masyarakat dalam bertransaksi, tetapi juga mendorong inklusi keuangan dan pertumbuhan ekonomi digital di Indonesia. Dengan infrastruktur yang terus berkembang dan regulasi yang mendukung, transaksi elektronik di Indonesia diproyeksikan akan terus tumbuh sehingga memberikan kontribusi positif bagi perekonomian nasional secara umum.

Kemudahan dan kenyamanan dalam transaksi elektronik ditengarai sebagai salah satu faktor penting bertumbuhnya jumlah kegiatan dengan metode ini yang dipilih oleh masyarakat luas. Sebagai contoh, QR Code dapat digunakan sebagai metode pembayaran yang efisien dan mudah diakses karena pelanggan dapat langsung melakukan transaksi dengan cepat tanpa perlu verifikasi identitas yang merepotkan. Selain itu, penggunaan dompet digital seperti GoPay, OVO, dan DANA, atau *virtual account* perbankan turut mempercepat proses transaksi elektronik dengan memasukkan PIN atau sidik jari untuk pengamanannya.

Tidak hanya sederhana dalam penggunaan dan kemudahan yang dirasakan oleh para pengguna, ada beberapa mekanisme yang dibuat oleh para perusahaan fintech dalam rangka menghadirkan proses transaksi elektronik yang aman dan andal sebagaimana yang diwajibkan oleh pemerintah selaku regulator sektor keuangan digital. Beberapa mekanisme pengamanan transaksi elektronik yang sudah ada meliputi; *Know Your Costumer* (KYC), autentikasi dua faktor (*two factor authentication,* 2FA), *One-Time Password* (OTP), biometrik, dan *smart contract blockchain*. Beberapa sistem autentikasi tersebut dapat meningkatkan keamanan transaksi dengan relatif sederhana sehingga dapat menjaga kemudahan bagi penggunanya. Selain itu, ada juga sertifikasi keamanan seperti ISO 27001 atau PCI DSS yang dapat meningkatkan kepercayaan pelanggan.

---

[1] Bank Indonesia, "Statistik Sistem Pembayaran dan Infrastruktur Pasar Keuangan (SPIP) Juni 2025," 17 Juli 2025. https://tinyurl.com/mpk28mzz

[2] Alfathi, "Penggunaan QRIS Terus Meningkat, Nominal Transaksi Capai Rp659 Triliun," GoodStats, 14 Apr. 2025. https://tinyurl.com/787e3abx

Dalam rangka menjaga kesinambungan perkembangan fintech, pemerintah telah menetapkan beberapa kebijakan pada beberapa aspek bisnis fintech, terutama aspek pengamanan, agar para pelaku bisnis dan konsumen yang terdampak dapat terus melaksanakan kegiatan mereka dengan aman dan nyaman. Namun demikian, pada tatanan implementasi kebijakan keamanan transaksi digital terdapat beberapa isu yang perlu menjadi perhatian para pembuat kebijakan agar tata kelola transaksi elektronik tetap bisa berkontribusi terhadap pertumbuhan ekonomi dan kesejahteraan masyarakat secara umum, dan menghindari hambatan yang mengganggu inovasi bisnis fintech yang telah turut berkontribusi pada pertumbuhan ekonomi dan inklusi keuangan di Indonesia.

Indonesia memiliki beberapa pengaturan, salah satunya adalah Undang-Undang (UU) No. 11/2008 tentang Informasi dan Transaksi Elektronik (ITE), yang telah direvisi dua kali, yaitu pada tahun 2016 dan 2024. Undang-undang ini dibuat dalam rangka memberikan dasar hukum dan pengamanan kegiatan transaksi elektronik. Tujuan utama dari UU ini adalah untuk menghindari penyalahgunaan informasi elektronik, dokumen elektronik, teknologi informasi, dan/atau transaksi elektronik sebagaimana yang menjadi inti bisnis dari fintech. Sebagai contoh, mengacu pada UU ITE Pasal 17 Ayat (2a), setiap Transaksi Elektronik yang memiliki risiko tinggi bagi para pihak wajib menggunakan tanda tangan elektronik yang tersertifikasi (TTET). Ketentuan ini dimaksudkan menjadi dasar hukum untuk memastikan keaslian, integritas, serta prinsip tidak dapat disangkal (*non-repudiation*) atas transaksi yang dilakukan secara elektronik, khususnya pada sektor atau aktivitas yang mengandung potensi risiko tinggi bagi pihak-pihak terkait.

Pada saat ini, setiap institusi keuangan, baik bank maupun penyedia jasa pembayaran (PJP) atau jasa pinjaman fintech lain, sudah diwajibkan oleh otoritas terkait, seperti BI dan Otoritas Jasa Keuangan (OJK), untuk memenuhi kewajiban membuat skema pengamanan dalam bisnis mereka. Beberapa skema seperti pelindungan data pribadi, verifikasi KYC, dan otorisasi transaksi guna perlindungan konsumen. Selain kedua lembaga tersebut, ada juga Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) yang mendapatkan amanat UU untuk menjadi ujung tombak pengawasan transaksi keuangan guna mencegah dan memeriksa tindakan melawan hukum pada transaksi elektronik.

Di sisi lain, kebijakan perlindungan konsumen di sektor jasa keuangan Indonesia masih mempertahankan pendekatan berbasis pasar (*market-based approach*) yang memberikan ruang bagi pelaku usaha menyesuaikan mekanisme verifikasi dan otorisasi sesuai dengan profil risiko layanan yang ditawarkan. Prinsip ini perlu dijaga dalam pengembangan kebijakan ke depan agar tetap mendorong kompetisi bisnis yang sehat.

Eksistensi, perkembangan, dan dinamika pengaturan yang ada pada bisnis transaksi elektronik di Indonesia tampak perlu penanganan yang tepat, khususnya pada segi perlindungan konsumen yang berlandaskan asas *market-based*. Dalam rangka mewujudkan visi tersebut, kiranya pemerintah selaku regulator sekaligus eksekutor kebijakan pada sektor bisnis fintech perlu mempertimbangkan beberapa faktor penting agar kepentingan pengamanan transaksi elektronik tidak perlu mengorbankan kemudahan dalam penggunaannya. Pertimbangan kesederhanaan operasional kegiatan transaksi elektronik yang mudah dilaksanakan oleh para pengguna, atau yang sesuai dengan prinsip *market-based,* penting untuk tetap dikedepankan dalam rangka menjaga jumlah transaksi elektronik yang dari padanya aktor fintech bisa berkontribusi kepada pertumbuhan ekonomi dan inklusi keuangan di Indonesia secara umum.

3. Tujuan penelitian

Naskah kebijakan ini dimaksudkan untuk turut serta berkontribusi terhadap proses pembuatan kebijakan yang berkaitan dengan peningkatan kontribusi fintech terhadap pertumbuhan ekonomi dan inklusi keuangan di Indonesia. Selain itu, naskah kebijakan ini bertujuan untuk:

a. Menganalisis struktur dan dinamika tata kelola mekanisme perlindungan konsumen yang *least disruptive* di perbankan dan sektor keuangan digital;
b. Menganalisis kebijakan mitigasi risiko transaksi elektronik dan dampaknya terhadap operasional industri keuangan digital; dan
c. Memformulasikan rekomendasi kebijakan bagi pemerintah untuk merancang kebijakan mitigasi risiko transaksi elektronik dalam rangka meningkatkan kontribusi positif fintech terhadap industri keuangan digital.

4. Metode penelitian

Terdapat tiga metode pengumpulan data yang digunakan dalam penelitian ini, termasuk studi literatur, wawancara mendalam, dan *focus group discussion* (FGD). Studi literatur merupakan kegiatan kajian mengenai latar belakang masalah dan gambaran umum mengenai bagaimana sektor fintech berkembang di Indonesia. Kegiatan ini bertujuan untuk menganalisis struktur dan dinamika tata kelola fintech yang tengah dilaksanakan oleh pemerintah dan menelaah mekanisme perlindungan konsumen yang *least disruptive* di sektor fintech. Kegiatan studi literatur meliputi:

a. Penelusuran produk kebijakan dan perspektif pembuat kebijakan terkait fintech;
b. Kajian regulasi yang berkenaan dengan pengaturan fintech, baik dari segi teknologi informasi maupun urusan keuangan; dan
c. Inventarisasi data yang berkenaan dengan perkembangan dan kontribusi fintech terhadap pertumbuhan ekonomi.

Wawancara mendalam merupakan metode riset kualitatif melengkapi temuan dari studi literatur dan mencakup kegiatan tanya jawab yang dilakukan antara pewawancara dan narasumber terkait topik spesifik yang menjadi objek penelitian dalam rangka mendapatkan informasi tertentu. Kegiatan ini bermaksud untuk menganalisis dampak perluasan kewajiban penggunaan jasa sertifikasi dalam setiap transaksi elektronik terhadap keberlangsungan usaha penyedia layanan pembayaran. Wawancara dilaksanakan dengan narasumber dari kalangan pemerintah yang meliputi Kementerian Komunikasi dan Digital (Komdigi), BI, dan representasi Asosiasi Digital Trust Indonesia (ADTI).

Adapun FGD melibatkan diskusi kelompok terarah guna menggali pandangan, pengalaman, dan ide dari para peserta terkait pengelolaan urusan fintech. Kegiatan ini dimaksudkan untuk melengkapi data yang didapat dari studi literatur dan wawancara. Selain itu, kegiatan ini menyasar pada dua klaster peserta FGD yang akan berpartisipasi pada dua kesempatan yang terpisah, yakni pelaku bisnis penyelenggara fintech dan pengguna jasa fintech.

5. Analisis regulasi

Menurut Peraturan Bank Indonesia (PBI) No. 23/2021 tentang Penyedia Jasa Pembayaran, terdapat beberapa entitas yang dapat diklasifikasikan sebagai aktor di dalam bisnis fintech, yang meliputi Bank,[3] Penyedia Jasa Pembayaran (PJP),[4] dan Penyelenggara Infrastruktur Sistem Pembayaran (PIP).[5] Terminologi yang berbeda diatur oleh Peraturan Otoritas Jasa Keuangan (POJK) No. 21/2023 tentang Layanan Digital oleh Bank Umum dan POJK No. 22/2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan yang meliputi Bank Umum,[6] Lembaga Jasa Keuangan,[7] Lembaga Jasa Keuangan (LJK),[8] dan Pelaku Usaha Jasa Keuangan (PUJK).[9]

Selain itu, UU No. 11/2008 tentang ITE dikenal sebagai pilar penting regulasi mengenai transaksi elektronik yang menjadi kegiatan bisnis utama dari fintech. Melalui UU tersebut, pemerintah selaku regulator berupaya untuk menghadirkan panduan bagi pelaku bisnis fintech dan pemangku kepentingan terkait untuk menciptakan mekanisme kegiatan bisnis yang aman. UU ini telah direvisi dua kali, yakni pada tahun 2016 dan 2024. Pada revisi kedua dengan UU No. 1/2024, terdapat penambahan pengaturan baru mengenai sertifikat elektronik yang patut diperhatikan oleh para pemangku kepentingan dan kebijakan terkait fintech. Pada UU No.1/2024 Pasal 17(2a) berbunyi "Transaksi Elektronik yang memiliki risiko tinggi bagi para pihak menggunakan tanda tangan elektronik yang diamankan dengan Sertifikat Elektronik." Pada bagian penjelasan, yang dimaksud dengan Transaksi Elektronik risiko tinggi adalah "transaksi keuangan yang tidak dilakukan dengan tatap muka secara fisik."

Sebelumnya pada peraturan lain, yakni PBI No. 22/23/PBI/2020 tentang Sistem Pembayaran, pada pasal 54, terdapat penjelasan mengenai gradasi risiko, mulai dari risiko rendah, sedang, dan tinggi. Adapun yang dimaksud dengan risiko tinggi, yang terdapat pada Pasal 54(2c), adalah yang dapat "mengakibatkan perubahan dengan skala tinggi pada model bisnis, sistem, dan/atau infrastruktur." Meski demikian, konteks gradasi dan definisi risiko tinggi di dalam peraturan tersebut berada dalam konteks pengembangan aktivitas, pengembangan produk, dan/atau kerja sama, bukan transaksi elektronik sebagaimana yang dimaksud oleh UU No. 1/2024 tentang ITE.

---

[3] Bank adalah bank umum dan bank perkreditan rakyat sebagaimana dimaksud dalam Undang-Undang mengenai perbankan, termasuk kantor cabang bank asing di Indonesia, dan bank umum syariah serta bank pembiayaan rakyat syariah sebagaimana dimaksud dalam Undang-Undang mengenai perbankan syariah.

[4] Penyedia Jasa Pembayaran yang selanjutnya disingkat PJP adalah Bank atau Lembaga Selain Bank yang menyediakan jasa untuk memfasilitasi transaksi pembayaran kepada pengguna jasa.

[5] Penyelenggara Infrastruktur Sistem Pembayaran yang selanjutnya disebut PIP adalah pihak yang menyelenggarakan infrastruktur sebagai sarana yang dapat digunakan untuk melakukan pemindahan dana bagi kepentingan anggotanya.

[6] Bank Umum yang selanjutnya disebut Bank adalah bank yang melaksanakan kegiatan usaha secara konvensional atau melaksanakan kegiatan usaha berdasarkan prinsip syariah, yang dalam kegiatannya memberikan jasa dalam lalu lintas pembayaran, termasuk kantor cabang dari bank yang berkedudukan di luar negeri dan unit usaha syariah.

[7] Lembaga Jasa Keuangan yang selanjutnya disingkat LJK adalah lembaga yang melaksanakan kegiatan di sektor perbankan, pasar modal, perasuransian, dana pensiun, modal ventura, lembaga keuangan mikro, lembaga pembiayaan, dan lembaga jasa keuangan lainnya.

[8] Lembaga Jasa Keuangan yang selanjutnya disingkat LJK adalah lembaga yang melaksanakan kegiatan di sektor perbankan, pasar modal, perasuransian, dana pensiun, modal ventura, lembaga keuangan mikro, lembaga pembiayaan, dan lembaga jasa keuangan lainnya.

[9] Pelaku Usaha Jasa Keuangan yang selanjutnya disingkat PUJK adalah:

a. LJK dan/atau pihak yang melakukan kegiatan usaha penghimpunan dana, penyaluran dana, dan/atau pengelolaan dana di sektor jasa keuangan; dan
b. pelaku usaha jasa keuangan lainnya, baik yang melaksanakan kegiatan usaha secara konvensional maupun berdasarkan prinsip syariah sesuai dengan ketentuan peraturan perundang-undangan di sektor jasa keuangan.

Selain itu, ada juga POJK No. 8/2023 tentang Penerapan Program Anti Pencucian Uang, Pencegahan Pendanaan Terorisme, dan Pencegahan Pendanaan Proliferasi Senjata Pemusnah Massal di Sektor Jasa Keuangan yang turut memberikan penjelasan mengenai beberapa potensi ancaman keamanan pada sektor keuangan. Pada peraturan tersebut, terdapat identifikasi mengenai Nasabah Berisiko Tinggi,[10] Negara Berisiko Tinggi,[11] dan Transaksi Keuangan Mencurigakan.[12] Selain itu, peraturan tersebut juga mewajibkan Penyedia Jasa Keuangan (PJK) untuk melakukan identifikasi dan verifikasi Calon Nasabah dengan berbagai prinsip dan ketentuan yang sudah diatur di dalam peraturan tersebut dalam rangka mengantisipasi berbagai ancaman keamanan potensial dalam transaksi.

Akan tetapi, peraturan-peraturan tersebut juga belum memberikan penjelasan mengenai Transaksi Elektronik risiko tinggi sebagaimana yang dimaksud oleh UU No.1/2024 tentang ITE, padahal pada saat ini, banyak sekali transaksi elektronik dengan jumlah nilai transaksi yang bermacam-macam yang dilaksanakan tanpa tatap muka secara fisik, dan hal tersebut sudah menjadi hal yang lumrah dilaksanakan oleh masyarakat Indonesia yang mulai terbiasa dengan berbagai layanan transaksi digital, termasuk menggunakan dompet digital. Pada pelaksanaannya, para aktor bisnis juga turut serta secara aktif memberikan makna pada transaksi elektronik risiko tinggi sebagai transaksi yang melibatkan nilai nominal besar, transaksi yang dilakukan oleh pihak yang tidak dikenal, transaksi dalam jumlah besar atau sering berulang yang dilakukan melintasi batas negara, dan transaksi yang dilakukan pada platform digital yang belum terverifikasi.

Lebih lanjut lagi, paket regulasi yang ada sebetulnya juga telah mengatur mekanisme pengamanan lainnya dalam rangka mengamankan kegiatan transaksi elektronik, yang tidak hanya terpaku pada Transaksi Elektronik risiko tinggi. Terdapat beberapa mekanisme pengamanan yang sudah diatur, yang meliputi sertifikasi dan TTET, KYC, 2FA, identifikasi dan verifikasi, kewajiban pembuatan unit khusus yang menangani pengamanan layanan digital, dan mekanisme pengamanan lainnya.

UU No. 11/2008 tentang ITE memberikan skema Sertifikat Elektronik[13] dan TTET[14] sebagai salah satu metode pencegahan terhadap tindakan kejahatan yang menggunakan dokumen dan/atau informasi elektronik. Menurut POJK No. 21/2023 tentang Layanan Digital oleh Bank Umum Pasal 22(1), "Bank dapat memanfaatkan penggunaan TTET dalam penyelenggaraan Layanan Digital sesuai dengan ketentuan peraturan perundang-undangan."[15] Namun demikian, meskipun UU No. 11/2008 tentang ITE hanya menjadikan sertifikasi elektronik sebagai salah satu alternatif, Peraturan Pemerintah (PP) No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Pasal 42(1) menyatakan bahwa "Penyelenggaraan Transaksi Elektronik wajib menggunakan Sertifikat Elektronik yang diterbitkan oleh Penyelenggara Sertifikasi Elektronik Indonesia." Ketentuan yang ada pada PP

[10] Nasabah Berisiko Tinggi adalah Nasabah yang berdasarkan latar belakang, identitas, riwayatnya, dan/atau hasil penilaian risiko yang dilakukan PJK
memiliki risiko tinggi melakukan kegiatan terkait TPPU, TPPT, dan/atau PPSPM.
[11] Negara Berisiko Tinggi adalah negara atau teritori yang potensial digunakan sebagai tempat terjadinya atau sarana kejahatan atau tindak pidana asal, TPPU, TPPT, dan/atau PPSPM.
[12] Transaksi Keuangan Mencurigakan adalah transaksi keuangan mencurigakan terkait TPPU, TPPT, dan/atau PPSPM.
[13] Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat *E-signing* dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
[14] *E-signing* adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
[15] Yang dimaksud dengan Layanan Digital adalah "produk Bank dalam bentuk layanan yang diberikan oleh Bank dengan pemanfaatan TI melalui media elektronik untuk memberikan akses bagi nasabah dan/atau calon nasabah terkait produk Bank maupun produk dan/atau layanan dari mitra Bank, serta dapat dilakukan secara mandiri oleh nasabah dan/atau calon nasabah."

No. 71/2019 tersebut, yang merupakan peraturan turunan dari UU No. 11/2008, berpotensi menimbulkan pertentangan hukum dengan peraturan induknya.

Pada dasarnya, jauh sebelum adanya pengaturan mengenai pengamanan transaksi elektronik, terdapat UU No. 8/2001 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang yang mengatur tentang mekanisme KYC untuk memastikan para pelaku bisnis fintech memiliki informasi yang akurat mengenai para pengguna jasa. Verifikasi data pengguna tersebut penting dilakukan untuk mencegah dan memberantas tindak pidana yang biasanya terjadi di sektor keuangan, khususnya tindak pidana Pencucian Uang (TPPU). Selain itu, pada Pasal 1(5) pada UU tersebut juga turut menjelaskan mengenai beberapa kegiatan dalam sektor fintech yang patut dikategorikan sebagai kegiatan yang mencurigakan, yang selanjutnya menjadi rujukan bagi peraturan turunan di bawahnya, termasuk POJK No. 8/2023. Lebih lanjut lagi, UU No. 8/2001 juga mengamanatkan secara spesifik PPATK sebagai ujung tombak penting mengawasi berbagai kegiatan keuangan yang dilakukan oleh aktor bisnis fintech, atau yang di dalam UU tersebut disebut sebagai Pihak Pelapor.[16] [17]

Selain itu, POJK No. 21/2023 tentang Layanan Digital oleh Bank Umum mengatur pula skema verifikasi transaksi keuangan dalam rangka menghadirkan transaksi yang aman. Peraturan tersebut dituangkan di dalam Pasal 9(1) yang berbunyi "Bank wajib menerapkan paling sedikit 2 (dua) faktor autentikasi (*two factor authentication*) untuk verifikasi transaksi keuangan." Selain itu, pada Pasal 9(2) selanjutnya diatur bahwa "Penerapan 2 (dua) faktor autentikasi (*two factor authentication*) sebagaimana dimaksud pada Ayat (1) dapat dilakukan untuk setiap transaksi keuangan secara individu maupun dengan pembatasan tertentu sesuai dengan analisis risiko yang dilakukan Bank serta persetujuan nasabah."

Pada dasarnya, POJK No. 21/2023 Pasal 5 mewajibkan bank untuk melakukan identifikasi dan verifikasi nasabah dalam hal Penyelenggaraan Layanan Digital dalam rangka mencegah terjadinya pelanggaran hukum yang memanfaatkan layanan tersebut. Selanjutnya, Pasal 18(1) mengatur bahwa "Bank yang menyelenggarakan Layanan Digital wajib membentuk unit atau fungsi yang bertugas menangani penyelenggaraan Layanan Digital."[18] Lalu pada Pasal 23(1) dan (2) dijelaskan pula prinsip-prinsip pengamanan bagi bank yang mengadopsi teknologi informasi dalam penyelenggaraan layanan digital. Bahkan pada Pasal 24(1) dan (2) peraturan tersebut turut

[16] Pihak Pelapor adalah Setiap Orang yang menurut Undang-Undang ini wajib menyampaikan laporan kepada PPATK.

[17] Pihak Pelapor meliputi penyedia jasa keuangan yang termasuk 1. bank; 2. perusahaan pembiayaan; 3. perusahaan asuransi dan perusahaan pialang asuransi; 4. dana pensiun lembaga keuangan; 5. perusahaan efek; 6. manajer investasi; 7. kustodian; 8. wali amanat; 9. perposan sebagai penyedia jasa giro; 10. pedagang valuta asing; 11. penyelenggara alat pembayaran menggunakan kartu; 12. penyelenggara *e-money* dan/atau *e-wallet*; 13. koperasi yang melakukan kegiatan simpan pinjam; 14. pegadaian; 15. perusahaan yang bergerak di bidang perdagangan berjangka komoditi; atau 16. penyelenggara kegiatan usaha pengiriman uang. Selain itu, penyedia barang dan/atau jasa lain yang meliputi: 1. perusahaan properti/agen properti; 2. pedagang kendaraan bermotor; 3. pedagang permata dan perhiasan/logam mulia; 4. pedagang barang seni dan antik; atau 5. balai lelang.

[18] Lalu pada ayat selanjutnya, Pasal 18(2), menjelaskan "unit atau fungsi yang menangani penyelenggaraan Layanan Digital sebagaimana dimaksud pada Ayat (1) memiliki tugas paling sedikit:

a) menyusun kebijakan, standar, dan prosedur penyelenggaraan Layanan Digital;
b) memastikan kesesuaian antara penyelenggaraan Layanan Digital dengan rencana strategis kegiatan usaha Bank;
c) memantau pelaksanaan kerja sama dengan mitra Bank dalam penyelenggaraan Layanan Digital;
d) memantau data transaksi keuangan Layanan Digital;
e) memastikan efektivitas langkah yang digunakan dalam menyelenggarakan Layanan Digital;
f) memantau kendala dan permasalahan yang muncul dari penyelenggaraan Layanan Digital; dan
g) memastikan kecukupan dan alokasi sumber daya terkait Layanan Digital yang dimiliki Bank."

mengatur ancaman sanksi bagi bank yang melanggar ketentuan pengamanan teknologi informasi dalam penyelenggaraan layanan digital.

Surat Edaran OJK No. 29/2022 tentang Ketahanan dan Keamanan Siber Bagi Bank Umum selanjutnya memberikan panduan teknis kepada bank untuk melakukan pelindungan aset. Pada ketentuan tersebut, Bank menerapkan manajemen pelindungan terhadap akses dan pengguna untuk mencegah tindakan tidak terotorisasi pada perangkat, infrastruktur jaringan, dan komponen sistem yang dikelola oleh Bank. Dalam menerapkan manajemen pelindungan terhadap akses dan pengguna, Bank paling sedikit:

a. mengimplementasikan identifikasi dan autentikasi pengelolaan akses terhadap seluruh perangkat lunak dan perangkat keras;
b. melakukan kendali terhadap akses pengguna, termasuk kompleksitas kata sandi, pembatasan percobaan dan penggunaan kembali kata sandi, serta permintaan kata sandi setelah perangkat tidak aktif untuk beberapa saat;
c. menerapkan pengamanan *endpoint* antara lain dengan menggunakan web URL *filtering*, *device control*, dan aplikasi kontrol pada seluruh perangkat *endpoint* pengguna termasuk *endpoint* yang terhubung ke *Virtual Private Network* (VPN);
d. menggunakan verifikasi *One Time Password* (OTP) untuk transaksi yang berisiko tinggi;
e. menerapkan IP *reputation* untuk memverifikasi Alamat IP yang diizinkan dalam proses transaksi;
f. memastikan batasan akses pada *database*, misalnya menerapkan akses *read-only* bagi pengguna selain admin *database*;
g. menggunakan *Multi-Factor Authentication* (MFA) untuk akses data sensitif atau akses terhadap seluruh jaringan apabila diperlukan;
h. menonaktifkan komunikasi antar *workstation* untuk mencegah terjadinya serangan siber dan *disabled peer to peer* pada *wireless client* di perangkat;
i. memastikan seluruh pegawai menggunakan fitur *wireless* hanya untuk kepentingan Bank;
j. menonaktifkan fitur *auto-run content* terhadap perangkat yang terhubung ke sistem atau perangkat di Bank; dan
k. menerapkan metode autentikasi melalui saluran terenkripsi, baik untuk *login* ke jaringan maupun aplikasi.

Dengan kata lain, paket regulasi yang dimiliki oleh Indonesia telah memberikan beberapa alternatif mekanisme pengamanan layanan digital bagi pelaku fintech di Indonesia, yang menjadi langkah positif bagi perkembangan inovasi pada industri ini. Meski ada beberapa peraturan yang masih memerlukan penjelasan legal formal yang penting bagi interpretasi dan pelaksanaan peraturan tersebut, seperti transaksi elektronik yang memiliki risiko tinggi, paket kebijakan dan regulasi yang ada di Indonesia relatif cukup akomodatif terhadap beberapa alternatif pengamanan layanan digital yang beragam bagi pelaku fintech. Beberapa opsi skema pengamanan yang ada telah memiliki dasar hukum melalui beragam regulasi yang dibuat oleh lembaga keuangan terkait sesuai dengan kewenangan spesifik mereka masing-masing.

Selain itu, Dewan Perwakilan Rakyat Republik Indonesia (DPR RI) tengah menggodok wacana pembuatan UU Keamanan Siber yang keberadaannya dianggap sangat penting setelah

memperhatikan beberapa permasalahan di ruang siber Indonesia, seperti dugaan kuat peretasan Pusat Data Nasional Sementara (PDNS) hingga lumpuhnya seluruh layanan imigrasi yang sempat terjadi pada tahun 2024 lalu. Namun demikian, para pemangku kepentingan terkait belum menemui titik temu kapan UU tersebut dapat diproses secara formal di tingkat panitia kerja (panja) DPR RI dan pemerintah. Nantinya UU semacam ini akan turut serta berpengaruh signifikan terhadap layanan digital yang diciptakan oleh aktor-aktor usaha dalam bidang fintech.

6. Signifikansi pelindungan data pribadi

Dalam era digital saat ini, data pribadi memiliki peran yang sangat signifikan dalam setiap transaksi elektronik. Keberadaan data pribadi menjadi fondasi utama dalam proses autentikasi dan verifikasi identitas pengguna. Tanpa adanya data tersebut, sistem tidak akan mampu memastikan bahwa pihak yang melakukan transaksi benar-benar adalah orang yang memiliki hak atas akun atau identitas yang digunakan. Oleh karena itu, data pribadi berperan penting dalam menjaga keabsahan dan keamanan transaksi digital, serta mencegah berbagai bentuk penipuan atau penyalahgunaan identitas.

Lebih dari sekadar alat verifikasi, data pribadi juga berfungsi untuk menciptakan pengalaman digital yang lebih personal dan relevan. Informasi seperti nama, lokasi, riwayat pembelian, dan preferensi individu digunakan oleh penyedia layanan untuk menawarkan produk, layanan, atau konten yang disesuaikan dengan kebutuhan dan minat pengguna. Personalisasi ini menjadi elemen kunci dalam membangun loyalitas pelanggan dan meningkatkan kepuasan pengguna dalam ekosistem digital.

Namun, penting juga disadari bahwa penggunaan data pribadi dalam transaksi digital tidak lepas dari risiko. Kebocoran data, penyalahgunaan informasi, dan pelanggaran privasi menjadi ancaman yang nyata jika tidak disertai dengan pengelolaan dan perlindungan yang memadai. Oleh sebab itu, Indonesia telah memiliki UU No. 27/2022 tentang Pelindungan Data Pribadi (PDP) yang mengatur pelindungan data pribadi milik subjek data sebagai bagian dari pemenuhan hak asasi manusia dan bagaimana data pribadi tersebut harus dikelola oleh pengendali dan pemroses data. Selain itu, UU tersebut juga mengamanatkan presiden untuk membuat sebuah otoritas independen yang menjadi ujung tombak pemerintah dalam hal pelindungan data pribadi, meski sampai saat ini lembaga tersebut belum dibentuk bahkan setelah dua tahun batas pembuatan otoritas pelindungan data pribadi dari peraturan tersebut diundangkan.

Salah satu tujuan dari pelindungan data pribadi adalah untuk mencegah penyalahgunaan informasi oleh pihak yang tidak berwenang, termasuk dalam bentuk penipuan dan pemalsuan identitas (*impersonation*) untuk kegiatan kriminal. Ketika data pribadi seperti nomor identitas, alamat, nomor telepon, atau informasi rekening tersebar tanpa kendali, pelaku kejahatan digital dapat dengan mudah memanfaatkannya untuk melakukan berbagai modus penipuan, mulai dari pembukaan rekening fiktif hingga pengajuan pinjaman atas nama korban.

Dalam konteks ini, kualitas data pribadi menjadi aspek yang tidak kalah penting dari menjaga kerahasiaannya. Data pribadi yang tidak akurat, tidak mutakhir, atau tercatat secara keliru dapat menimbulkan risiko tambahan dalam proses verifikasi identitas. Misalnya, ketika lembaga keuangan menggunakan data yang salah sebagai acuan, proses verifikasi bisa gagal membedakan antara individu yang sah dengan pelaku penipuan, sehingga membuka celah bagi *impersonation* untuk lolos

tanpa terdeteksi. Sebaliknya, jika data yang digunakan terlalu ketat atau keliru, individu yang sah justru bisa tertolak, menciptakan friksi yang tidak perlu dalam layanan.

Kesadaran akan pentingnya perlindungan dan kualitas data inilah yang mendorong negara-negara seperti Singapura dan kawasan Uni Eropa untuk menerapkan regulasi pelindungan data yang komprehensif, seperti *Personal Data Protection Act* (PDPA) di Singapura dan *General Data Protection Regulation* (GDPR) di Uni Eropa. Regulasi-regulasi tersebut tidak hanya menekankan pada aspek keamanan dan persetujuan, tetapi juga mewajibkan akurasi dan kejelasan dalam pengelolaan data pribadi. Hal ini menjadi landasan penting dalam mencegah penipuan digital berbasis identitas dan membangun ekosistem digital yang lebih aman dan terpercaya.

Meski Indonesia telah memiliki pengaturan pelindungan data pribadi dan pemanfaatan data tersebut untuk kepentingan kependudukan dan verifikasi pengguna layanan keuangan digital, literasi teknologi dan digital masyarakat Indonesia juga masih cenderung belum siap mengantisipasi potensi kejahatan digital. Kecenderungan kejahatan siber di Indonesia bukan hanya berbentuk *impersonation*, tapi juga *social engineering* dan *scam* yang mengelabui korbannya yang dengan kesadaran penuh melakukan *authorized payment*. Dengan kata lain, kejahatan siber semacam ini, yang biasa disebut sebagai *authorized push payment fraud* (APP), terjadi bukan hanya dikarenakan adanya penyalahgunaan data pribadi pengguna, tapi juga absensi literasi digital yang sangat menentukan keberhasilan upaya penipuan yang banyak terjadi di Indonesia. Kendala literasi digital semacam ini tidak bisa ditanggulangi dengan membuat sistem pelindungan data pribadi dan pengamanan pembayaran digital, tapi perlu dilakukan adanya edukasi yang dilakukan oleh seluruh pemangku kepentingan di sektor keuangan digital, yang melibatkan regulator dan kalangan bisnis dalam rangka menciptakan ekosistem pembayaran elektronik yang aman dan andal.

7. Kajian perbandingan

Salah satu faktor yang mempersulit proses penyusunan mekanisme keamanan siber di sektor fintech adalah sensitivitas para pelaku usaha terkait terhadap intervensi melalui regulasi. Dengan kata lain, para pemangku kebijakan perlu memperhatikan sensitivitas pengembangan teknologi sebagai inti dari bisnis fintech agar tidak menghambat inovasi pada sektor ini.

Pertama-tama, mekanisme keamanan siber apa pun akan menimbulkan biaya bagi para aktor bisnis, dari PJP sampai para pengguna jasa pembayaran elektronik, sehingga perlu dipastikan bahwa biaya implementasi skema pengamanan tidak terlalu memberatkan pengguna. Kedua, terdapat risiko penerapan pengamanan yang berlebihan—seperti penolakan transaksi berdasarkan dugaan aktivitas mencurigakan yang ternyata tidak akurat (*false flag*), baik karena kesalahan teknis maupun kesalahan manusia (*human error*). Hal ini berpotensi melanggar prinsip keadilan dalam akses keuangan.

Untuk memberikan gambaran yang lebih utuh, bagian ini akan mengkaji perbandingan terhadap implementasi kebijakan keamanan siber di berbagai negara yang menjadi pengaturan payung bagi peraturan teknis bagi layanan keuangan digital. Beberapa studi kasus digunakan untuk menggambarkan konsekuensi nyata dari penerapan sistem deteksi penipuan atau anti-pencucian uang (*anti-money laundering*/AML) yang tidak tepat, termasuk risiko tindakan yang terlalu represif maupun beban biaya yang berlebihan terhadap transaksi keuangan. Selain itu, bagian ini juga akan mengulas praktik terbaik dalam penerapan keamanan siber pada transaksi keuangan yang berhasil

menjaga keseimbangan antara efektivitas perlindungan, efisiensi ekonomi, dan inklusivitas digital, guna memberikan rekomendasi kebijakan yang konstruktif dan aplikatif bagi Indonesia.

7.1. Kajian perbandingan risiko

Risiko *False Flag*

Sebagian besar mekanisme pengamanan siber, termasuk sertifikasi elektronik, umumnya digunakan sebagai upaya untuk mencegah *fraud*, tetapi mekanisme ini memiliki beberapa risiko. Dalam beberapa kasus, sistem justru akan menolak transaksi yang khas akibat pengaturan deteksi yang terlalu sensitif. Implementasi mekanisme ini juga menjadi semakin kompleks ketika bertemu dengan sistem keamanan lain. Padahal, setiap lembaga keuangan sudah memiliki sistem keamanan tersendiri yang berlapis karena sektor keuangan pada dasarnya sangat sensitif terhadap tindakan *fraud*.

Dalam konteks mendeteksi potensi *fraud*, terdapat beberapa jenis anomali transaksi yang menjadi indikasi awal potensi *fraud* yang memerlukan mekanisme pemantauan yang berbeda. Namun, ketika berbagai protokol keamanan dari institusi yang berbeda—seperti bank, penyedia layanan autentikasi, dan pihak ketiga seperti penyelenggara sertifikasi elektronik (PSrE)—berinteraksi dalam satu ekosistem transaksi, gesekan bisa terjadi. Misalnya, sistem A mendeteksi pola transaksi tertentu sebagai mencurigakan, padahal sistem B menganggapnya wajar. Ketidaksinkronan ini dapat memicu alarm palsu (*false flags*) dan menyebabkan transaksi sah malah ditolak.

Kondisi semacam ini bukan sekadar gangguan teknis, tetapi masalah keseragaman antar entitas berbeda hingga dapat berdampak besar pada pengalaman pengguna, terutama dalam konteks transaksi elektronik yang mengandalkan kecepatan dan keandalan. Dengan kata lain, banyaknya lapisan deteksi yang tidak terkoordinasi dapat meningkatkan tingkat penolakan pembayaran secara tidak semestinya.

Kasus Monzo di Inggris

Salah satu contoh ekstrem dari kegagalan sistem deteksi penerapan sistem keamanan digital adalah kasus yang menimpa bank digital asal Inggris, Monzo. Dalam upayanya memperketat pengawasan terhadap aktivitas pencucian uang, Monzo mengandalkan sistem otomatis yang sangat sensitif untuk mendeteksi pola transaksi yang dianggap mencurigakan. Akibatnya, ribuan pengguna sah mengalami pembekuan akun secara mendadak tanpa penjelasan yang memadai. Insiden ini menyebabkan banyak pengguna tidak bisa mengakses akun mereka.[19]

Insiden tersebut menggambarkan salah satu risiko terbesar dari penerapan langkah keamanan siber yang terlalu agresif: munculnya *false positive*, yaitu situasi ketika sistem secara keliru mengidentifikasi pengguna yang sah sebagai ancaman. Ketika sistem keamanan tidak mampu membedakan antara aktivitas abnormal yang sah (seperti bepergian ke luar negeri, menggunakan VPN, atau perubahan perangkat) dengan aktivitas yang benar-benar mencurigakan, hasilnya adalah penolakan transaksi atau pembekuan akun yang tidak semestinya.

[19] The Guardian "Monzo bank freezing accounts for no apparent reason'" Jan. 18, 2020 https://tinyurl.com/muf84kv2

Dalam konteks Indonesia, pemerintah memiliki alternatif perluasan pengamanan transaksi elektronik dengan menerapkan penggunaan layanan sertifikasi elektronik atau TTET sebagaimana diatur di dalam UU No.1/2024 tentang ITE. Dalam konteks transaksi elektronik, sertifikasi elektronik berfungsi sebagai alat verifikasi identitas. Artinya, sebelum suatu transaksi disahkan, sistem sertifikasi elektronik akan berupaya memastikan bahwa orang yang melakukan transaksi tersebut benar-benar adalah pemilik sah akun, bukan pihak yang menyamar.

Secara garis besar, mekanisme kerja sertifikasi elektronik di Indonesia mencakup pengumpulan dan pencocokan sejumlah data teknis—seperti perilaku pengguna, jenis transaksi, lokasi geografis (*geolocation*), perangkat yang digunakan, serta alamat IP koneksi internet—dengan data kependudukan yang tercatat di Direktorat Jenderal Kependudukan dan Pencatatan Sipil (Dukcapil), Kementerian Dalam Negeri. Sistem ini mencari kecocokan antara pola aktivitas transaksi elektronik dengan identitas resmi pengguna untuk meminimalkan risiko penipuan dan penyalahgunaan identitas.

Namun, dalam praktiknya, banyak skenario sah yang justru sering memicu sistem untuk mengeluarkan *false positive*. Beberapa contoh yang umum terjadi antara lain:

1. Perjalanan ke luar negeri, ketika pengguna melakukan transaksi dari negara yang berbeda dari lokasi biasanya.
2. Penggantian perangkat, seperti menggunakan ponsel baru atau laptop kantor yang belum dikenali oleh sistem.
3. Penggunaan VPN, baik untuk alasan privasi maupun karena keperluan pekerjaan lintas negara.
4. *Remote working*, ketika seseorang bisa melakukan *login* dari berbagai tempat, termasuk *co-working space*, hotel, atau area dengan jaringan publik.
5. Perjalanan domestik atau dinas, ketika transaksi dilakukan dari kota yang berbeda dalam waktu singkat.

Untuk meminimalisir risiko *false positive*, pihak PSrE cenderung memberikan toleransi terhadap tingkat tertentu dari perilaku yang dianggap tidak biasa (*abnormal behavior*) guna mengakomodasi kondisi-kondisi yang dapat dijelaskan secara wajar. Misalnya, jika seorang pengguna tiba-tiba melakukan transaksi dari lokasi geografis yang berbeda atau menggunakan perangkat baru, sistem tidak serta-merta menolak transaksi tersebut. Sebaliknya, sistem akan menilai apakah perubahan tersebut masih berada dalam batas kewajaran berdasarkan pola perilaku sebelumnya, seperti frekuensi *login*, riwayat perjalanan, atau pola penggunaan jaringan.

Mekanisme toleransi ini penting untuk menjaga kenyamanan pengguna sah agar tidak terhambat dalam melakukan aktivitas digitalnya. Akan tetapi, ruang kelonggaran tersebut secara tidak langsung juga menciptakan celah yang bisa dimanfaatkan oleh pelaku kejahatan siber. Jika pelaku berhasil meniru secara meyakinkan pola perilaku pengguna, mereka berpotensi lolos dari deteksi karena sistem menganggap aktivitas tersebut masih dalam batas wajar.

Dengan demikian, ada *trade-off* yang tidak bisa dihindari antara mencegah penipuan dan mempertahankan kelancaran transaksi sah. Jika terlalu ketat, sistem akan menolak banyak transaksi legal; terlalu longgar, sistem akan memberi peluang lebih besar bagi tindakan penyalahgunaan. Oleh karena itu, efektivitas sistem keamanan dalam transaksi elektronik sangat bergantung pada pendekatan yang adaptif.

Risiko skalabilitas TTET

Risiko lain dari stipulasi penggunaan sertifikasi elektronik dalam transaksi adalah perbedaan skala pada TTET. Pada saat ini, verifikasi TTET cenderung digunakan untuk aktivitas seperti registrasi di platform *e-commerce*, modifikasi akun, masuk akun (*login*), atau korespondensi dengan pemerintah. Serangkaian aktivitas tersebut memiliki frekuensi yang sangat rendah. Sementara itu transaksi elektronik memiliki frekuensi yang sangat tinggi, bisa berkali-kali dalam satu hari.

Dalam konteks ini, muncul tantangan baru terkait dengan kapasitas sistem penyelenggara sertifikasi elektronik. Penggunaan berlebihan sertifikasi elektronik tanpa penyesuaian terhadap skala dan kebutuhan frekuensi transaksi dapat mengakibatkan penurunan performa sistem, *bottleneck* proses autentikasi, dan membebani biaya operasional platform serta pengguna secara tidak proporsional. Hal ini berpotensi menimbulkan resistensi dari pelaku industri dan memperlambat adopsi digital secara menyeluruh.

Kasus Aadhar e-KYC di India

Masalah skalabilitas ini sudah sering kali menjadi perhatian di berbagai negara. Salah satu contoh paling menonjol adalah ketika India melakukan mewajibkan penggunaan program Aadhaar sebagai standar e-KYC nasional. Aadhaar merupakan sistem identitas digital berbasis biometrik terbesar di dunia yang awalnya dirancang untuk keperluan sosial dan administratif, seperti distribusi subsidi pangan, bantuan langsung tunai, dan pelayanan publik lainnya. Sistem ini memungkinkan pemerintah untuk menyalurkan bantuan secara lebih tepat sasaran kepada masyarakat berpenghasilan rendah dengan memverifikasi identitas penerima melalui data biometrik seperti sidik jari dan pemindaian iris.

Namun, pemerintah India kemudian memperluas penggunaannya secara agresif ke sektor keuangan dan layanan digital, termasuk dalam proses e-KYC dan TTET. Sistem ini kemudian diwajibkan untuk berbagai aktivitas seperti pembukaan rekening bank, aktivasi kartu SIM, hingga transaksi elektronik. Perluasan ini menimbulkan berbagai tantangan skalabilitas karena sistem Aadhaar tidak dirancang untuk menangani verifikasi dalam skala dan frekuensi tinggi. Akibatnya, sering terjadi *bottleneck*, kesalahan verifikasi biometrik, pemblokiran akses layanan bagi individu yang sah, dan dalam beberapa kasus, bocornya data pribadi akibat celah dalam sistem.[20]

Hal ini akhirnya mendorong Mahkamah Agung India pada tahun 2018 menghapus penggunaan program Aadhaar dalam sektor perbankan dan telekomunikasi sebagai standar e-KYC, mengingat risiko pelanggaran privasi dan eksklusi digital yang terlalu besar. Akan tetapi, program Aadhar dipertahankan di program bantuan sosial, mengingat besarnya dampak program ini sebelum penggunaannya di sektor lain.[21]

[20] EPW Engage "Aadhaar Failures: A Tragedy of Errors" April 2019 https://tinyurl.com/mrueutmz
[21] Reuters "India's top court imposes curbs on biometric identity system" Sep. 26, 2018 https://tinyurl.com/2drzetn8

7.2. Kajian perbandingan praktik terbaik

Setelah memahami lanskap regulasi yang ada di Indonesia serta tantangan-tantangan yang dihadapi India dan Inggris, bagian ini akan memberikan gambaran praktik terbaik regulasi pelindungan data pribadi dan transaksi elektronik dari Uni Eropa dan Singapura sebagai tolok ukur bagi Indonesia. Aturan dan regulasi dari kedua yurisdiksi ini digunakan sebagai perbandingan mengenai bagaimana negara-negara dengan standar perlindungan data yang tinggi telah merespons dinamika dan pertumbuhan lanskap digital untuk melindungi warganya dengan lebih baik. Kedua yurisdiksi tersebut telah mengembangkan kerangka hukum yang memadai untuk mengatur pengumpulan dan pemrosesan data pribadi, serta regulasi yang rinci terkait penggunaan TTET sebagai bagian dari pengamanan transaksi.

7.2.1. Uni Eropa

a. Standar pelindungan data pribadi

Diakui sebagai regulasi pelindungan data paling ketat di dunia, Uni Eropa, yang terdiri dari 27 negara, menerapkan *General Data Protection Regulation* (GDPR) tahun 2016 untuk melindungi data pribadi warganya. Dalam suatu fenomena yang disebut "*Brussels effect,*" yang menyiratkan bahwa undang-undang yang dibuat oleh Uni Eropa cenderung ditiru oleh negara lain di seluruh dunia, GDPR telah menjadi standar pelindungan data secara internasional ketika banyak negara telah mengadopsi ketentuan-ketentuan hukum ini ke dalam regulasi pelindungan data mereka masing-masing. Negara-negara seperti Brasil, Australia, Kanada, Jepang, Selandia Baru, dan banyak lainnya telah menerapkan undang-undang privasi yang mirip dengan GDPR sehingga menjadikan GDPR sebagai standar global.

Standarisasi GDPR juga meluas ke sektor swasta, khususnya perusahaan teknologi seperti Meta, Microsoft, dan Apple yang semuanya mematuhi ketentuan GDPR. Kepatuhan ini mencakup langkah-langkah seperti memperoleh persetujuan eksplisit dari pengguna, memberikan hak akses dan penghapusan data, serta menerapkan protokol pelaporan pelanggaran data yang ketat. Dengan menyesuaikan diri terhadap GDPR, perusahaan-perusahaan ini tidak hanya mendapatkan akses ke pasar Eropa, tetapi juga menunjukkan komitmen GDPR memperkenalkan dua istilah kunci: *Data Subject* dan *Data Controller*. *Data Subject* adalah individu yang data pribadinya dikumpulkan. Sedangkan *Data Controller* adalah organisasi yang mengumpulkan dan menentukan tujuan serta cara pemrosesan data pribadi dari *Data Subject* tersebut.

Di dalam GDPR, data pribadi didefinisikan sebagai informasi apa pun yang berkaitan dengan individu yang teridentifikasi atau dapat diidentifikasi. Ini dapat mencakup nama, nomor identifikasi, data lokasi, pengenal daring seperti alamat IP, atau faktor-faktor yang berkaitan dengan identitas fisik, fisiologis, genetik, mental, ekonomi, budaya, atau sosial dari individu tersebut. Regulasi ini juga memperkenalkan konsep *Data Processor*, yaitu pihak ketiga yang memproses data pribadi atas nama *Data Controller*, yang semakin memperjelas peran dan tanggung jawab dalam ekosistem pengelolaan data.[22] Penegakan GDPR dilakukan secara desentralisasi, dengan setiap negara anggota Uni Eropa memiliki otoritas pelindungan data nasional (DPA) masing-masing untuk memastikan kepatuhan terhadap GDPR.

[22] Intersoft Consulting, "Art. 4 GDPR; Definitions", https://tinyurl.com/ym9p2jk4

Pasal 58 GDPR mengategorikan kewenangan DPA ke dalam tiga bidang utama: penyelidikan, korektif, dan konsultatif. Kewenangan penyelidikan memungkinkan DPA melakukan audit pelindungan data, dengan meminta akses terhadap data dan lokasi, serta meminta informasi dari organisasi pengendali data yang sedang diperiksa. Kewenangan ini bertujuan untuk menentukan apakah telah terjadi pelanggaran terhadap GDPR, serta untuk menilai ruang lingkup, sifat, dan konsekuensi dari pelanggaran tersebut.[23]

Jika ditemukan pelanggaran, DPA dapat menggunakan kewenangan korektif mereka. Ini termasuk memberikan peringatan, teguran, atau memberlakukan pembatasan sementara atau permanen terhadap aktivitas pemrosesan data. DPA dapat memaksa organisasi untuk memenuhi permintaan *Data Subject* atau menyesuaikan operasional mereka agar sesuai dengan regulasi dalam jangka waktu tertentu. Mereka juga dapat menghentikan transfer data ke negara ketiga, mencabut sertifikasi, atau melarang badan sertifikasi untuk mengeluarkan sertifikasi. Salah satu alat terkuat yang dimiliki DPA adalah kemampuan untuk menjatuhkan denda administratif. Denda ini dapat mencapai hingga €10 juta atau 2 persen dari omzet tahunan untuk kegagalan prosedural, dan hingga €20 juta atau 4 persen untuk pelanggaran yang lebih serius, seperti pemrosesan data yang melanggar hukum atau pelanggaran terhadap hak *Data Subject*.[24]

Terakhir, DPA juga memiliki fungsi konsultatif. Mereka bertanggung jawab untuk melakukan edukasi dan meningkatkan kesadaran masyarakat nasional mereka mengenai risiko, aturan, perlindungan, dan hak-hak terkait pemrosesan data pribadi. Mereka juga memberikan panduan kepada *Data Controller* melalui mekanisme seperti konsultasi sebelumnya (*prior consultation*) sebagaimana diatur dalam Pasal 36, dan dapat memberikan opini kepada parlemen nasional, pemerintah negara anggota Uni Eropa, atau institusi dan badan lain yang terkait dengan usulan legislasi tentang pelindungan data. DPA juga berperan dalam menyetujui kode etik dan mengakreditasi mekanisme sertifikasi guna mempromosikan praktik terbaik lintas sektor, memastikan transparansi dan kepercayaan bagi individu yang data pribadinya diproses di dalam Uni Eropa.[25]

Salah satu bagian penting dari GDPR adalah kewajiban pemberitahuan pelanggaran data pribadi. Berdasarkan Pasal 33, *Data Controller* diwajibkan untuk memberi tahu DPA dari Negara Anggota terkait dalam waktu tidak lebih dari 72 jam sejak menyadari terjadinya pelanggaran data pribadi. Jika *Data Controller* tidak dapat memberikan pemberitahuan dalam waktu 72 jam, mereka harus melampirkan alasan keterlambatan tersebut bersama dengan pemberitahuan. *Data Controller* tidak wajib melaporkan pelanggaran data jika dianggap "tidak mungkin menimbulkan risiko terhadap hak dan kebebasan individu."[26]

Selain pemberitahuan pelanggaran data, *Data Controller* juga wajib menanggapi permintaan *Data Subject* untuk mengakses data pribadi mereka. Berdasarkan Pasal 15, *Data Subject* memiliki hak untuk dengan mudah mengakses data pribadi mereka yang disimpan oleh *Data Controller*.[27] Lebih lanjut, berdasarkan pasal 16, *Data Subject* juga berhak memperbaiki data pribadi mereka apabila mereka merasa data tersebut diproses secara tidak akurat atau tidak lengkap oleh *Data Controller*.[28]

---

[23] European Data Protection Board, "Data Protection Authority & you", https://tinyurl.com/2xwmbw5y
[24] Ibid
[25] Ibid
[26] Intersoft Consulting, "Art. 33 GDPR; Notifications of a personal data breach to the supervisory authority", https://tinyurl.com/2afmhzvw
[27] Intersoft Consulting, "Art. 15 GDPR; Right of access by the data subject", https://tinyurl.com/4xnt5vac
[28] Intersoft Consulting, "Art. 16 GDPR; Right to rectification", https://tinyurl.com/3t9rpd29

Permintaan ini, menurut Pasal 12(3), harus diproses oleh *Data Controller* tanpa penundaan yang tidak semestinya, paling lambat dalam waktu satu bulan sejak diterimanya permintaan. Perpanjangan waktu hingga dua bulan tambahan (tiga bulan total) diperbolehkan jika diperlukan, namun *Data Controller* wajib memberi tahu *Data Subject* mengenai penundaan tersebut beserta alasan keterlambatannya.[29]

Hal penting yang juga perlu diketahui bahwa penegakan hukum GDPR bersifat terdesentralisir sehingga setiap negara anggota Uni Eropa memiliki desain DPA mereka sendiri. Kondisi ini menciptakan *trade-off* antara tingkat regulasi yang tinggi dan potensi kelonggaran dalam implementasinya. Di satu sisi, GDPR menetapkan standar kepatuhan yang sangat ketat bagi para pengendali dan pemroses data. Namun di sisi lain, karena penegakannya terdesentralisir melalui DPA di masing-masing negara anggota, terdapat ruang diskresi dalam menentukan tingkat sanksi, kecepatan respons, maupun bentuk peringatan yang diberikan kepada pelaku pelanggaran. Artinya, meskipun standar GDPR bersifat seragam secara hukum, pendekatan penegakan dapat berbeda tergantung pada yurisdiksi masing-masing DPA.

Meskipun demikian, model ini justru ideal bagi Uni Eropa. Tingginya standar regulasi yang diterapkan secara harmonis di seluruh wilayah Uni Eropa memungkinkan adanya interoperabilitas yang efisien antarnegara anggota, mempermudah aliran data lintas batas tanpa perlu negosiasi bilateral tambahan. Dengan demikian, GDPR tidak hanya memperkuat pelindungan data pribadi bagi warga Uni Eropa, tetapi juga menciptakan ekosistem digital terpadu yang mendukung pertumbuhan ekonomi digital di kawasan tersebut.

b. Standar keamanan transaksi elektronik

Uni Eropa memiliki sejumlah regulasi dan pedoman yang bertujuan untuk mengatur ekosistem transaksi digital. *EU Payment Services Directive 2* (PSD2) didirikan untuk membentuk ekonomi digital Eropa yang terintegrasi serta melindungi konsumen dan pelaku usaha dalam melakukan pembayaran daring yang aman dan terlindungi. Penting untuk dicatat bahwa PSD2 adalah sebuah *directive* Uni Eropa, artinya ketentuan-ketentuannya bersifat mengikat secara hukum, tetapi pelaksanaannya diserahkan kepada negara-negara anggota untuk mengatur melalui legislasi nasional. Hal ini berbeda dengan GDPR yang merupakan regulasi supranasional Uni Eropa, yang berarti negara-negara anggota wajib mematuhi aturan yang ditetapkan langsung oleh Uni Eropa.

Berdasarkan Pasal 97 PSD2, negara-negara anggota diwajibkan untuk menerapkan *Strong Customer Authentication* (SCA) guna memberikan perlindungan yang lebih baik terhadap konsumen dalam transaksi digital. Direktif ini mewajibkan bahwa individu harus memverifikasi identitas mereka dengan menggunakan setidaknya dua dari tiga kategori faktor otentikasi yang berbeda: sesuatu yang mereka ketahui (*knowledge*) seperti kata sandi atau PIN, sesuatu yang mereka miliki (*possession*) seperti ponsel, dan sesuatu yang melekat pada diri mereka (*inherence*) seperti sidik jari atau pengenalan wajah.

European Banking Authority (EBA) juga menyediakan kerangka regulasi melalui *EBA Guidelines on ICT and security risk management*. Dalam Pedoman 3.4.2 mengenai keamanan logis, lembaga keuangan diwajibkan untuk menerapkan dan secara berkala menilai mekanisme otentikasi yang aman. Mekanisme ini harus selaras dengan prinsip-prinsip yang ditetapkan dalam PSD2 dan mencakup

[29] Intersoft Consulting, "Art. 12 GDPR; Transparent information, communication and modalities for the exercise of the rights of the data subject", https://tinyurl.com/5ct3cbs5

setidaknya otentikasi multi-faktor (*multi factor authentification*, MFA) yang berbasis pada faktor *knowledge*, *possession*, dan *inherence*.

Lebih lanjut, karena Uni Eropa terdiri dari berbagai negara dengan sistem hukum yang beragam, TTET menjadi alat penting untuk memfasilitasi transaksi digital lintas batas yang aman, dapat dioperasikan, dan diakui secara hukum. Regulasi eIDAS (EU No. 910/2014)[30] menetapkan kerangka hukum terpadu untuk identifikasi elektronik dan layanan kepercayaan, termasuk TTET. Regulasi ini mendefinisikan tiga tingkat TTET.

Pertama, *Simple Electronic Signatures* (SES) atau TTET standar didefinisikan dalam Pasal 3(10) sebagai "data dalam bentuk elektronik yang dilampirkan atau dikaitkan secara logis dengan data elektronik lainnya, dan digunakan oleh penandatangan untuk menandatangani." TTET ini memiliki keabsahan hukum tetapi menawarkan tingkat jaminan terendah. SES biasanya digunakan untuk aktivitas berisiko rendah seperti menandatangani bukti pengiriman, menyetujui syarat dan ketentuan secara daring, atau proses administratif rutin di bidang SDM.

Kedua, *Advanced Electronic Signatures* (AdES), sebagaimana didefinisikan dalam Pasal 26, mengharuskan TTET untuk memiliki keterkaitan yang unik dengan penandatangan, mampu mengidentifikasi penandatangan, dan terkait erat dengan data sehingga setiap perubahan setelah penandatanganan dapat dideteksi. AdES umumnya digunakan dalam transaksi dengan risiko menengah hingga tinggi, seperti penandatanganan kontrak bisnis, perjanjian kerahasiaan (*non-disclosure agreement*, NDA), pembukaan rekening bank, dan polis asuransi. TTET ini memberikan tingkat kepercayaan yang lebih tinggi karena adanya verifikasi identitas dan mekanisme integritas bawaan, meskipun tidak secara otomatis memiliki kedudukan hukum yang sama seperti tanda tangan basah.[31]

Ketiga, *Qualified Electronic Signatures* (QES) adalah subtipe dari AdES yang didukung oleh sertifikat digital yang dikeluarkan oleh *Qualified Trust Service Provider* (QTSP) dan dibuat menggunakan *Qualified Signature Creation Device* (QSCD). Berdasarkan Pasal 25(2), QES diberikan kedudukan hukum yang sama dengan tanda tangan basah di seluruh wilayah Uni Eropa. Karena jaminan tinggi dan kesetaraannya dengan tanda tangan tulisan tangan, QES digunakan dalam transaksi bernilai tinggi yang mengikat secara hukum, seperti pengajuan dokumen ke pengadilan, akta notaris, pengadaan publik, kontrak lintas negara, perjanjian pinjaman, dan pengajuan regulasi lainnya ketika otentikasi, integritas data, dan daya berlaku hukum sangat penting.

Definisi yang dikelompokkan semacam ini dapat memastikan kejelasan penggunaan TTET dalam ekonomi digital Uni Eropa, ketika TTET dengan jaminan rendah dapat mempercepat interaksi berisiko rendah, sementara TTET dengan jaminan tinggi memastikan keamanan dan daya laku hukum saat dibutuhkan.

Pendekatan Uni Eropa dalam mengatur TTET mencerminkan keseimbangan antara kebutuhan akan keamanan hukum dan efisiensi operasional. Meskipun eIDAS mewajibkan penggunaan TTET dalam sejumlah konteks tertentu—terutama yang berkaitan dengan layanan publik dan transaksi lintas

[30] eIDAS adalah regulasi yang mengatur *electronic identification, authentication and trust services* atau identifikasi elektronik, autentikasi, dan layanan kepercayaan di kawasan Uni Eropa.

[31] Official Journal of the European Union, "REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC", Agu. 28, 2014, https://tinyurl.com/4puz3rh5

negara—regulasi ini juga menyediakan tingkat-tingkat TTET yang berbeda untuk disesuaikan dengan tingkat risiko masing-masing transaksi. Dengan tidak mewajibkan penggunaan QES di setiap transaksi, Uni Eropa menghindari beban proses yang tinggi dan penggunaan sumber daya yang berlebihan.

Sebaliknya, penggunaan SES atau AdES pada aktivitas berisiko rendah hingga menengah memungkinkan sistem tetap ringan dan responsif. Pendekatan bertingkat ini menjadikan TTET lebih *scalable*, sehingga mampu mendukung adopsi yang lebih luas di sektor publik maupun swasta. Skalabilitas ini sangat penting, khususnya bagi negara-negara yang tengah mengembangkan infrastruktur TTET mereka, karena memungkinkan integrasi yang bertahap namun tetap sesuai dengan prinsip keamanan dan akuntabilitas.

7.2.2. Singapura

a. Standar pelindungan data pribadi

Di Singapura, perlindungan informasi pribadi diatur secara ketat melalui *Personal Data Protection Act* (PDPA). Undang-undang ini menetapkan kerangka hukum yang jelas terkait pengumpulan, penggunaan, dan pengungkapan data pribadi oleh pengendali data. PDPA berfungsi untuk memastikan bahwa data pribadi diproses secara aman dan hanya untuk tujuan yang telah disetujui oleh subjek data.

PDPA mendefinisikan data pribadi sebagai segala bentuk informasi, baik benar maupun tidak, yang dapat digunakan untuk mengidentifikasi seseorang, seperti detail kontak, alamat rumah, atau pengenal langsung lainnya. Selain itu, data pribadi juga mencakup informasi tidak langsung yang dimiliki oleh suatu organisasi yang, jika digabungkan dengan data lain, dapat mengarah pada identifikasi seseorang, seperti catatan transaksi elektronik, alamat IP, atau catatan karyawan. Melalui PDPA, individu memiliki hak untuk mengakses, mengoreksi, menarik persetujuan, memastikan akurasi, perlindungan, hak tindakan pribadi dan hak untuk diberitahu terkait informasi pribadi.

Standar-standar dari regulasi ini mencerminkan peraturan yang serupa dengan GDPR yang dibuat oleh Uni Eropa. Baik PDPA maupun GDPR mencerminkan prinsip bahwa semua individu pribadi memiliki kendali penuh atas data pribadi mereka yang diproses oleh pengendali data.

Menurut PDPA, ketika individu meminta akses atau perubahan data pribadi mereka, pengendali data wajib memenuhi permintaan tersebut sesegera mungkin. Meskipun tidak ada batas waktu yang spesifik, praktik umum bagi pengendali data untuk menanggapi permintaan akses maupun perubahan adalah 30 hari sejak permintaan tersebut diterima. Jika pengendali data tidak dapat memenuhi permintaan tersebut, mereka harus memberitahu individu tersebut dalam waktu 30 hari sejak permintaan diajukan.[32]

Selain itu, amandemen PDPA pada tahun 2020 memperkenalkan kewajiban pelaporan pelanggaran data. Jika terjadi insiden pelanggaran data yang dapat menyebabkan kerugian signifikan bagi individu atau melibatkan volume data besar, pengendali data wajib melaporkan insiden tersebut kepada *Personal Data Protection Commission* (PDPC) dan korban bocor data dalam waktu 72 jam. Secara spesifik, PDPA mengharuskan pengendali data untuk melaporkan pelanggaran data kepada korban setelah menentukan bahwa pelanggaran data tersebut wajib dilaporkan. Jadi bukan setelah

[32] PDPC, "ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PDPA", Okt. 9 2019, https://tinyurl.com/43znahj4

pelanggaran data ditemukan. Hal ini memberikan waktu yang cukup bagi pengendali data untuk mengevaluasi situasi dengan informasi yang jelas tanpa harus terburu-buru mengirimkan laporan kepada PDPC.[33]

PDPC sendiri adalah sebuah *statutory body* atau badan pengatur yang ditetapkan oleh undang-undang untuk mengawasi pelaksanaan ketentuan PDPA. Mereka memastikan bahwa pelaku bisnis mematuhi PDPA dan bertanggung jawab untuk menangani masalah kepatuhan terhadap undang-undang tersebut. Selain itu, komisi tersebut juga bertanggung jawab atas beberapa inisiatif lain yang berkaitan dengan pelindungan data pribadi. Mereka meningkatkan kesadaran publik tentang topik tersebut, berfungsi sebagai badan penasihat bagi sektor publik, dan memimpin kemajuan di sektor tersebut melalui inisiatif R&D.[34]

Singapura juga menerapkan *Data Protection Trustmark* (DPTM), sebuah sertifikasi sukarela bagi perusahaan yang ingin menunjukkan komitmen mereka dalam melindungi informasi pribadi sesuai standar PDPA. Sertifikasi ini meningkatkan kredibilitas perusahaan di mata klien dan mitra bisnis, sekaligus menjadi indikator keandalan perusahaan dalam menangani data pribadi. Pendekatan ini menjadikan Singapura sebagai negara yang mengutamakan pelindungan data pribadi dan secara efektif menekan risiko penyalahgunaan data melalui kerangka hukum yang komprehensif.

Dengan strategi pengaturan pelindungan data pribadi tersebut di atas, Singapura mampu menciptakan ekosistem keamanan siber yang menyeluruh, ketika perusahaan dan individu didorong untuk secara proaktif mengadopsi praktik terbaik dalam menjaga keamanan data pribadi. Pendekatan Singapura terhadap pelindungan data pribadi dianggap sebagai praktik terbaik karena menggabungkan kerangka hukum yang kuat, kejelasan dalam hak-hak individu, dan mekanisme penegakan hukum yang mudah dimengerti.

Peraturan PDPA menguraikan tanggung jawab pengendali data pribadi di kegiatan operasional sehari-hari dan keadaan darurat, seperti di kasus kebocoran data. Di lain sisi, mekanisme sertifikasi DPTM mempermudah proses *onboarding* pelaku bisnis untuk dapat menjadi pengendali data pribadi yang sah. Pendekatan Singapura tersebut menciptakan lingkungan yang mendorong transparansi, akuntabilitas, dan kepercayaan publik.

b. Standar keamanan transaksi elektronik

Untuk beradaptasi dengan dunia digitalisasi yang terus berkembang, Singapura menerapkan regulasi untuk menjaga keamanan aliran uang di ruang digital. Di Singapura, *Technology Risk Management Guidelines* (TRMG) yang diterbitkan oleh *Monetary Authority of Singapore* (MAS) berfungsi sebagai kerangka kerja utama dalam mengidentifikasi, mengelola, dan mengurangi risiko pada transaksi elektronik. Pedoman ini diperbarui secara berkala dalam rangka penyesuaian dengan ancaman siber terbaru dan tren digitalisasi di sektor keuangan. TRMG telah menjadi kerangka penting dalam memastikan bahwa semua transaksi elektronik dilakukan dengan aman, efektif, dan terlindungi dari potensi ancaman siber.

Untuk menjaga keamanan transaksi elektronik, TRMG menetapkan langkah teknis dan operasional yang wajib diterapkan oleh lembaga keuangan. Untuk transaksi bernilai tinggi atau akses sistem

[33] Kennedys, "Singapore introduces mandatory data breach notification requirements", Mar. 4, 2021, https://tinyurl.com/e4k7hyhd
[34] Singapore Statutes Online, "Personal Data Protection Act 2012; PERSONAL DATA PROTECTION COMMISSION AND ADMINISTRATION", https://tinyurl.com/apaabbfh

yang sensitif, lembaga keuangan diwajibkan untuk menerapkan autentikasi multi-faktor. Standar keamanan siber dilaksanakan melalui dua atau lebih faktor yang dapat dibedakan, seperti *knowledge* (apa yang Anda ketahui), *possession* (apa yang Anda miliki), dan *inherence* (siapa Anda).[35] Mekanisme tersebut dapat mencakup kombinasi kata sandi, OTP, biometrik, atau perangkat autentikasi fisik. MFA bertujuan untuk mencegah akses tidak sah dan meminimalkan risiko pencurian identitas atau pengambilalihan akun.

Penggunaan TTET dalam transaksi elektronik di Singapura merupakan salah satu metode yang digunakan untuk menjamin langkah-langkah keamanan tambahan. Di dalam TRMG, TTET dianjurkan penggunaannya dalam transaksi yang dilabelkan sebagai aktivitas berisiko tinggi (*high-risk activities*).

Pada Pasal 14.2.3 dalam pedoman tersebut, aktivitas berisiko tinggi mencakup perubahan data konsumen yang sensitif, seperti alamat rumah, surel, dan detail kontak. Selain itu, aktivitas berisiko tinggi juga meliputi registrasi detail penerima pihak ketiga, transfer dana bernilai tinggi, serta perubahan batas transfer dana. Pedoman ini bertujuan untuk memastikan bahwa transaksi yang bersifat sensitif dilengkapi dengan langkah-langkah autentikasi yang memadai untuk menghindari risiko penipuan atau penyalahgunaan data.[36]

Meskipun pedoman TRMG tidak memiliki kekuatan hukum yang mengikat, MAS memiliki kewenangan untuk mengeluarkan pemberitahuan (*notice*) atas ketidakpatuhan yang dilakukan oleh lembaga keuangan. Pemberitahuan tersebut bersifat mengikat secara hukum, sehingga lembaga keuangan yang tidak mematuhi pedoman ini dapat dikenakan sanksi atau tindakan lebih lanjut oleh MAS.

Di sisi lain, landasan hukum TTET di Singapura pertama kali ditetapkan melalui *Electronic Transactions Act* (ETA) pada tahun 1998. Berdasarkan undang-undang ini, legalitas TTET diakui dan penggunaannya dapat diberlakukan secara sah dalam transaksi elektronik. Meskipun ETA tidak mewajibkan penggunaan TTET, undang-undang ini mengakui dan memberikan landasan hukum bagi penerapannya dalam transaksi elektronik, terutama dalam sektor komersial, pemerintahan, dan perdagangan internasional.

Walaupun Singapura memiliki salah satu sektor keuangan terbesar di dunia, tingkat ketaatan dan beban keamanan siber pada transaksi elektronik di negara tersebut terpaut tidak terlalu jauh dari rata-rata dunia. Hal ini dikarenakan efisiensi dari mekanisme MFA dalam mencegah sebagian besar dari risiko *fraud* dalam transaksi digital. Penggunaan TTET dibatasi pada aktivitas berisiko tinggi dan apa yang dimaksud dengan 'risiko tinggi' didefinisikan dengan jelas, sehingga tidak ada ambiguitas dalam kewajiban keamanan para aktor bisnis di sektor transaksi digital.

[35] Monetary Authority of Singapore, "Technology Risk Management Guidelines", Jan. 18, 2021, https://tinyurl.com/4aux5te5
[36] Ibid

7.3. Tabel perbandingan regulasi pelindungan data pribadi dan metode autentikasi antar negara

Jenis pengaturan	Indonesia	Singapura	Uni Eropa
Pelidungan data pribadi	• Diatur dengan Undang-Undang Pelindungan Data Pribadi (UU PDP) No. 27/2022. • Mengatur kewajiban pengendali data pribadi jenis publik dan swasta, termasuk organisasi internasional. • Otoritas Pelindungan Data Pribadi bertanggung jawab langsung kepada presiden. • Pengendali data pribadi wajib merespons permintaan subjek data dan memberitahukan kegagalan pelindungan data pribadi paling lambat 3 x 24 jam. • Pengaturan teknis dan otoritas pelindungan data pribadi masih disusun oleh pemerintah.	• Diatur oleh *Personal Data Protection Act* (PDPA). • Hanya mengatur kewajiban pengendali data pribadi jenis swasta. • Menekankan persetujuan, akses, koreksi, dan pelaporan kebocoran data. • Badan pengawas: *Personal Data Protection Commission* (PDPC). • Sertifikasi sukarela: *Data Protection Trustmark* (DPTM). • Pelaporan insiden wajib dalam 72 jam jika signifikan.	• Diatur oleh *General Data Protection Regulation* (GDPR). • Hak luas bagi subjek data: akses, koreksi, penghapusan, dan portabilitas. • Mengatur kewajiban pengendali data pribadi jenis publik dan swasta, selain aparat penegak hukum. • Penegakan oleh *Data Protection Authorities* (DPA) tiap negara. • Denda hingga €20 juta atau 4 persen omzet. • Pelaporan pelanggaran wajib dalam 72 jam.
Metode autentikasi	• Detail pengaturan menjadi kewenangan BI dan OJK. • Terdapat kewajiban penggunaan 2FA untuk verifikasi transaksi keuangan.	• Diatur oleh *Technology Risk Management Guidelines* (TRMG) dari *Monetary Authority of Singapore* (MAS). • *Multi-Factor Authentication* (MFA) berbasis kombinasi faktor *knowledge*, *possession*, *inherence*. • TRMG bersifat tidak mengikat, namun MAS dapat mengeluarkan tindakan *notice* yang bersifat mengikat secara hukum.	• Diatur melalui PSD2 dan *EBA Guidelines on ICT and Security Risk Management*. • Wajib *Strong Customer Authentication* (SCA). • MFA berbasis kombinasi faktor *knowledge*, *possession*, dan *inherence*. • Berlaku lintas sektor pembayaran digital. • Kepatuhan bersifat mengikat secara hukum melalui regulasi nasional.

8. Kebijakan sertifikasi elektronik

Industri sertifikasi elektronik domestik telah beroperasi di Indonesia sejak PSrE lokal pertama kali menawarkan jasa sertifikasi terhadap situs web dengan spesifikasi *secure socket layer* (SSL) untuk memverifikasi validitasnya. Di sisi lain, UU No. 1/2024 tentang ITE telah mewajibkan PSrE memberikan garansi sertifikat. TTET di Indonesia dibagi dua jenis, yaitu TTET yang tersertifikasi dan yang tidak tersertifikasi. Dalam pelaksanaannya, TTET tersertifikasi yang diselenggarakan oleh PSrE di Indonesia menggunakan standar *qualified* TTET dari eIDAS di Uni Eropa yang merupakan strata tertinggi TTET. Persamaan standar tersebut mengimplikasikan bahwa PSrE tersertifikasi yang dimiliki Indonesia mempunyai tingkat derajat keamanan tertinggi jika dibandingkan dengan standar Uni Eropa yang mendefinisikan dua tipe PSrE lainnya yang mempunyai standar keamanan yang lebih rendah dan anjuran pemakaian yang berbeda. Hal tersebut berarti bahwa tipe PsrE yang digunakan di Indonesia seharusnya hanya dipakai untuk aktivitas risiko tertinggi seperti pengajuan dokumen ke pengadilan, akta notaris, kontrak lintas negara, atau transaksi keuangan yang mempunyai implikasi hukum yang tinggi seperti asuransi atau pinjaman.

Setelah memperhatikan beberapa model pengaturan dan kebijakan mitigasi risiko pada sektor keuangan digital yang ada di negara lain, ada beberapa sisi yang perlu diperhatikan dan diantisipasi dalam memberlakukan sertifikasi elektronik pada transaksi digital di Indonesia. Sertifikasi elektronik dapat memberikan lapisan keamanan tambahan, meski skema pengamanan tersebut dapat juga berpotensi menghambat penerapan prinsip netral teknologi yang diusung oleh UU No. 1/2024 tentang ITE untuk mendorong fleksibilitas inovasi perbankan. Selain itu, implementasi sertifikasi elektronik perlu mendapatkan perhatian lebih dalam manajemen risiko keuangan digital mengingat mekanisme ini telah memiliki dasar hukum pada tatanan UU, tapi belum memiliki pengaturan teknis turunan, sehingga detail efek dari penggunaan sertifikasi elektronik perlu dianalisis lebih lanjut.

8.1. Tabel perbandingan regulasi sertifikasi elektronik antar negara

Indonesia	Singapura	Uni Eropa
• Diatur dengan revisi kedua UU ITE No. 1/2024. • Digunakan untuk transaksi elektronik yang memiliki risiko tinggi. • Pengaturan teknis lebih lanjut mengenai penggunaan sertifikasi elektronik, termasuk definisi transaksi elektronik risiko tinggi, masih disusun oleh pemerintah.	• Diatur dalam *Electronic Transactions Act* (ETA). • TTET sah secara hukum untuk transaksi. • Digunakan terutama dalam aktivitas berisiko tinggi, seperti: perubahan data sensitif, registrasi detail penerima pihak ketiga, transfer dana bernilai tinggi, serta perubahan batas transfer dana. • Tidak ada stratifikasi tingkat TTET.	• Diatur dalam regulasi eIDAS. • Terdapat tiga tingkat TTET: 1. *Simple Electronic Signature* (SES): untuk aktivitas risiko rendah seperti: Menandatangani bukti pengiriman, menyetujui syarat dan ketentuan secara daring, atau proses administratif rutin. 2. *Advanced Electronic Signature* (AdES): untuk aktivitas risiko menengah seperti: Penandatanganan kontrak bisnis, perjanjian kerahasiaan (NDA), atau pembukaan rekening bank. 3. *Qualified Electronic Signature* (QES): untuk aktivitas risiko tinggi seperti: Pengajuan dokumen ke pengadilan, akta notaris, pengadaan publik, atau kontrak lintas negara.

9. Analisis solusi *market-based* pada kebijakan pengamanan transaksi elektronik

Dalam merancang kebijakan di era digital, prinsip netralitas teknologi menjadi krusial untuk memastikan bahwa regulasi tidak menghambat inovasi, tidak membatasi pilihan pasar, dan tidak menciptakan ketergantungan pada teknologi atau penyedia tertentu. Ketika sebuah regulasi secara eksplisit atau implisit mewajibkan penggunaan satu jenis teknologi, maka akan terbentuk monopoli sebagai konsekuensinya.

Potensi ketidaknetralan ini pada akhirnya membuat kekuatan pasar hanya berkonsentrasi pada segelintir penyedia layanan yang memenuhi kriteria teknis tertentu, tanpa mendorong mereka untuk terus berinovasi atau menurunkan biaya layanan dalam tatanan kompetisi pasar yang sehat. Dalam jangka panjang, hal ini merugikan ekosistem digital secara keseluruhan, terutama pelaku usaha kecil dan menengah yang mungkin tidak mampu mengakses teknologi yang diwajibkan oleh peraturan perundang-undangan. Selain itu, regulasi yang terlalu spesifik pada satu pendekatan teknologi juga akan menjadi usang dengan cepat seiring perubahan lanskap teknologi yang sangat dinamis.

9.1. Pendekatan *market-based* dalam sektor ekonomi digital

Salah satu alasan utama yang kerap dikemukakan dalam penggunaan TTET adalah untuk mencegah penipuan digital. Namun, solusi terhadap *fraud* tidak seharusnya ditentukan secara sepihak oleh regulator. Sebaliknya, mekanisme pencegahan penipuan yang paling efektif seharusnya lahir melalui pendekatan berbasis pasar ketika pelaku usaha secara mandiri memilih dan mengembangkan teknologi yang paling sesuai dengan model bisnis dan profil risikonya masing-masing. Dalam kerangka ini, pemerintah cukup menetapkan standar minimum hasil (misalnya, tingkat keberhasilan verifikasi atau tingkat perlindungan konsumen), bukan metode teknisnya, apalagi di tatanan UU yang bersifat prinsip.

Dengan membuka ruang bagi pendekatan yang lebih fleksibel dan kompetitif, berbagai solusi teknologi anti-penipuan—baik berbasis biometrik, MFA, ataupun teknologi berbasis *digital trust* lain—dapat tumbuh dan berkembang sesuai kebutuhan pasar. Prinsip netralitas teknologi memungkinkan ekosistem digital berkembang secara organik dan berkelanjutan, tanpa intervensi berlebihan yang justru berisiko memperlambat inovasi dan memperbesar kesenjangan teknologi.

Berangkat dari prinsip tersebut, penting untuk menyadari bahwa mayoritas transaksi di Indonesia saat ini dilakukan secara digital, dan transaksi digital tersebut hadir dalam berbagai bentuk—mulai dari belanja kebutuhan sehari-hari hingga pengajuan pinjaman hipotek atau klaim asuransi. Dengan keragaman bentuk, nilai, dan risiko yang menyertai masing-masing transaksi, menjadi sangat sulit untuk menerapkan satu kebijakan menyeluruh yang mewajibkan penggunaan teknologi tertentu secara seragam. Sebagai contoh, terasa janggal ketika pembayaran belanjaan sehari-hari yang dilakukan melalui dompet digital diperlakukan secara regulatif sama dengan transaksi bernilai tinggi seperti pengajuan KPR atau pencairan klaim asuransi, hanya karena keduanya dilakukan tanpa tatap muka fisik.

Selain itu, konsumen dan mitra pedagang yang menggunakan layanan transaksi digital masih memiliki pemahaman yang minim mengenai konsep dan cara kerja TTET. Kurangnya pemahaman

ini menciptakan rasa ragu, bahkan ketakutan, terhadap penggunaan teknologi tersebut. Mereka cenderung mengira bahwa TTET akan melibatkan tindakan fisik seperti menggambar tanda tangan di layar sentuh, atau membuka halaman tambahan untuk menyatakan persetujuan, asumsi yang wajar mengingat istilah "tanda tangan elektronik" sendiri terdengar seperti proses yang rumit dan formal.

Dari pemahaman yang terbatas tersebut, muncul pula ekspektasi negatif bahwa TTET akan menambah proses administratif dalam setiap transaksi. Kekhawatiran ini sangat kuat terutama di kalangan pengguna yang terbiasa dengan transaksi cepat dan praktis. Selain itu, para pengguna tersebut menyatakan penolakan terhadap kemungkinan adanya langkah tambahan, terutama jika dianggap tidak memberikan manfaat nyata bagi mereka sebagai pengguna. Bagi pedagang, kekhawatiran ini bahkan lebih besar karena mereka khawatir pemasukan mereka akan berkurang.

Masalah ini semakin diperparah dengan fakta bahwa sosialisasi mengenai TTET di kalangan masyarakat umum masih sangat terbatas. Terlihat belum ada upaya terpadu dari pemerintah atau otoritas terkait untuk menjelaskan fungsi, manfaat, maupun tata cara penggunaan TTET secara luas dan mudah dipahami. Dalam kondisi seperti ini, mewajibkan penggunaan TTET secara menyeluruh justru berisiko menimbulkan resistensi dari pengguna, bukan karena mereka menolak prinsip keamanannya, melainkan karena mereka tidak memahami bentuk dan cara kerjanya, serta menganggapnya sebagai beban tambahan yang tidak perlu. Dengan kata lain, tanpa edukasi yang memadai, regulasi ini justru kontra produktif dalam adopsi transaksi digital.

Pada sisi akar rumput, konsumen sering menjadi titik terlemah dalam rantai keamanan digital. Dalam banyak kasus, pelanggaran keamanan tidak terjadi karena kegagalan sistem teknis, melainkan karena data pribadi konsumen berhasil dicuri melalui teknik rekayasa sosial yang semakin kompleks. Penjahat siber saat ini tidak hanya mengandalkan peretasan sistem, tetapi juga memanfaatkan manipulasi psikologis untuk mengelabui konsumen agar membocorkan informasi penting, seperti kode OTP, PIN, atau kredensial akun.

Kondisi kompleks di tatanan pengguna ini menunjukkan bahwa, pada akhirnya diperlukan tingkat keterlibatan dan tanggung jawab tertentu di sisi konsumen. Upaya mitigasi risiko tetap membutuhkan partisipasi aktif dari pengguna, baik melalui peningkatan wawasan, kewaspadaan, maupun kepatuhan terhadap protokol keamanan yang diterapkan.

Memang, otoritas dan pelaku industri secara berkala melakukan sosialisasi terkait risiko keamanan digital dan modus kejahatan siber terbaru. Namun demikian, jangkauan dan efektivitas upaya ini masih terbatas, terutama di kalangan masyarakat yang belum melek digital atau kurang mendapatkan informasi resmi dari regulator terkait. Oleh karena itu, meski tanggung jawab perlindungan tidak boleh sepenuhnya dialihkan ke konsumen, realitas di lapangan menuntut adanya keseimbangan antara perlindungan regulatif dan kesadaran individual.

Studi Kasus: Peran Indonesia Anti-Scam Centre (IASC)

Indonesia merupakan salah satu negara dengan tingkat penipuan digital yang sangat tinggi. Sepanjang tahun 2023 hingga pertengahan 2024, OJK mencatat sekitar 166.000 laporan *fraud* digital, dengan total kerugian yang ditaksir mencapai Rp 3,4 triliun.[37] Jumlah kasus dan tingginya nilai kerugian dari laporan tersebut mencerminkan betapa masifnya aktivitas kejahatan keuangan yang terus berkembang, seiring dengan meningkatnya adopsi layanan digital di tengah masyarakat.

Melihat kondisi tersebut, pemerintah melalui otoritas terkait merasa perlu membentuk sebuah pusat koordinasi nasional yang mampu merespons laporan dengan cepat dan efektif. Inilah yang melatarbelakangi pembentukan Indonesia Anti-Scam Center (IASC) pada November 2024—sebuah inisiatif bersama untuk memperkuat perlindungan konsumen, mempercepat proses penanganan penipuan, dan menindak pelaku kejahatan keuangan digital lintas platform secara terintegrasi.

IASC merupakan suatu platform bagi para pelaku penyedia jasa keuangan dan pembayaran untuk berbagi informasi secara *real-time*, yang memainkan peran vital dalam upaya pencegahan penipuan. Melalui pertukaran data yang cepat dan terkoordinasi, para penyedia jasa dapat segera membekukan rekening diduga pelaku penipuan begitu laporan diterima, sehingga peluang untuk memulihkan dana korban menjadi lebih besar.

Selain itu, platform IASC memungkinkan para lembaga keuangan untuk saling berbagi daftar hitam atas rekening atau identitas yang terindikasi terlibat dalam aktivitas penipuan guna mencegah pelaku yang sama membuka rekening baru di lembaga keuangan lainnya dalam rangka mengulangi aksinya tersebut. IASC juga menjadi wadah diseminasi praktik-praktik terbaik dalam pencegahan *fraud*, termasuk teknologi deteksi dini dan sistem verifikasi yang terbukti efektif sehingga mampu memperkuat ketahanan industri jasa keuangan terhadap ancaman kejahatan digital yang semakin kompleks dari waktu ke waktu.

Di tengah berbagai upaya penanggulangan penipuan digital, pendekatan kolaboratif yang diusung melalui IASC menunjukkan efektivitas yang semakin nyata. Berbeda dengan pendekatan yang lebih normatif dan bersifat satu arah—seperti kewajiban penerapan mekanisme tertentu secara seragam, misalnya penggunaan TTET—model IASC memungkinkan respons yang lebih cepat, berbasis data lapangan, dan dapat beradaptasi dengan dinamika modus kejahatan yang terus berubah.

Melalui koordinasi langsung antar pelaku industri, pembekuan rekening dan pelacakan dana dapat dilakukan dalam hitungan jam, bukan hari. Selain itu, berbagi daftar hitam dan praktik terbaik juga memperkuat upaya pencegahan yang proaktif, bukan sekadar kepatuhan administratif. Pendekatan ini menunjukkan bahwa perlindungan konsumen yang efektif tidak selalu bergantung pada instrumen regulasi yang kaku, melainkan pada kemampuan ekosistem untuk bekerja secara terintegrasi dan responsif.

[37] CNBCIndonesia "OJK: Ada 166 Ribu Laporan Scam, Kerugian Rp 3,4 T! Ini Modus Utamanya " Juli 8, 2025 https://tinyurl.com/2z9yu69u

9.2. Potensi efek sertifikat elektronik terhadap tindakan pemalsuan

Penerapan sertifikasi elektronik yang melibatkan PSrE ditujukan untuk meningkatkan keamanan dalam aktivitas transaksi elektronik dari tindakan pemalsuan yang dapat merugikan pengguna dan PJP. Akan tetapi, masih terdapat beberapa celah keamanan di dalam mekanisme sertifikasi elektronik dengan PSrE yang menimbulkan kerentanan terhadap pemalsuan. Kerentanan tersebut memiliki implikasi skala yang besar bila kewajiban sertifikasi elektronik berisiko tinggi memiliki definisi risiko tinggi yang terlalu luas.

Sertifikasi elektronik, dan berbagai alat pengaman digital lain, menggunakan teknologi kriptografi dengan model otorisasi *public key interface* (PKI). PKI ini merupakan suatu model berbasis kriptografi yang menjamin keaslian dari suatu kontrak dengan proses verifikasi lintas perangkat. Dokumen atau *website* yang memuat kontrak akan terenkripsi dengan *public key*, sementara modifikasi kontrak tersebut akan memerlukan *private key* yang hanya dimiliki oleh pihak memiliki otorisasi. Model PKI memiliki beberapa kerentanan, seperti berikut:[38]

1. **Model otorisasi PKI yang kurang ketat dapat mengancam keamanan data pengguna;**

Setiap PSrE dapat menggunakan pendekatan mereka masing-masing dalam desain kriptografi. Model otorisasi PKI yang kurang ketat, baik pada elemen enkripsi, algoritma TTET, kunci enkripsi, dan fungsi *one-way hash*, akan mengancam keamanan data pengguna.

2. **Enkripsi yang tidak efisien jadi celah bagi *timing attack*;**

Kapasitas komputasi perangkat keras dan algoritma perangkat lunak yang menggenerasi *public key* dapat menjadi faktor penghambat, sehingga menciptakan celah dari sisi enkripsi. Enkripsi yang tidak efisien membuat celah bagi *timing attack*, suatu metode untuk menebak *private key* suatu proses berdasarkan waktu enkripsi oleh *public key* dan waktu dekripsi *private key*.

3. **Panjang bit *public* dan *private key* perlukan komputasi besar;**

Beberapa PC level komersial mampu mengurai sertifikasi digital hingga 1024 bit. Tapi sertifikasi digital yang sangat panjang, contohnya hingga 2014 bit, membutuhkan kekuatan komputasi sangat besar yang akan memberatkan proses pertukaran data;

4. **Risiko kegagalan penghapusan data pasca proses enkripsi;**

Data yang dienkripsi oleh *public* dan *private key* diamankan aplikasi dalam bentuk *plain text*. Aplikasi tersebut dapat gagal menghapus data pasca proses enkripsi, sehingga bisa ditemukan, didekripsi, dan digunakan peretas untuk keperluan kejahatan;

5. **Risiko data *private key* tetap tersimpan di RAM;**

Besar kemungkinan data *private key* yang dihasilkan dari *public key* saat proses pertukaran data dalam PKI tetap tersimpan di RAM selama komputer atau gawai belum dimatikan. Data *private key* tersebut dapat ditemukan dan dimanfaatkan oleh pelaku kejahatan;

6. **Kerentanan *private key* yang sering digunakan;**

Suatu *private key* akan lebih mudah diretas bila digunakan untuk dalam banyak proses deskripsi data, dan dampak penyalahgunaannya akan mempengaruhi seluruh data-data tersebut;

[38] Abdulla dan Rana, "Vulnerabilities in Public Key Cryptography," Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security, 2021, Hal. 628-629. https://doi.org/10.2991/ahis.k.210913.079

7. Risiko kerawanan penyimpanan *private key;*

Private key yang tidak disimpan di alat manajemen sertifikasi elektronik, dan malah disimpan di alat yang sama dengan data yang diterima, akan membahayakan keamanan data;

8. Bahaya dari *ransomware*

Serangan *ransomware* dapat "menyandera" data dengan enkripsi yang dibuat oleh peretas juga dapat berdampak pada sistem PKI.

Selain itu, ada lagi risiko yang disebabkan jenis verifikasi TTET sekadar klik, dibandingkan verifikasi TTET dengan metode lain seperti verifikasi informasi IP sampai verifikasi dengan perangkat khusus. Untuk verifikasi dengan klik, ada celah yang berpotensi dieksploitasi melalui *dynamic interface* yang merupakan elemen standar dari semua *browser*, sehingga bahasa *programming* apa pun yang sering digunakan untuk pembuatan *website*, seperti JavaScript, mampu memanipulasi elemen visual secara dinamis. Tindakan tersebut akan memungkinkan tampilan *file* yang disertifikasi tanpa menyebabkan dibatalkannya penerapan TTET ketika *file* yang disertifikasi memiliki muatan dinamis.[39]

Contohnya, suatu *file* kontrak memiliki instruksi makro yang mengacu pada tanggal di sistem komputer dan mengubah harga yang ditampilkan berdasarkan perubahan tanggal. Serangan siber dapat menerapkan perubahan *font* di dokumen yang juga mengubah bentuk karakter huruf, dan contoh dampak perubahan *font* tersebut adalah perubahan nama penerima pembayaran di kontrak tersebut.[40]

Penggunaan TTET dapat diperkuat dengan adanya *interface* khusus, seperti *smart card* dan tablet TTET. Contohnya, PSrE di Indonesia yang diwajibkan melakukan generasi *public key* dengan perangkat keras yang mengacu kepada *Federal Information Processing Standards* (FIPS) dari Amerika Serikat. Akan tetapi, penggunaan alat ini masih dapat dieksploitasi jika perangkat keras tablet tersebut sudah terinfeksi *malware*. Dalam kasus tersebut, TTET pengguna dapat digunakan oleh pihak ketiga untuk transaksi yang tidak sah.[41]

9.3. Pelimpahan biaya tambahan kepada konsumen

Tarif sertifikasi elektronik paket *enterprise* dari sebuah PSrE adalah Rp 2,1 juta per tahun per akun pegawai bagi perusahaan yang menjadi pengguna jasa sertifikasi elektronik.[42] Selanjutnya, jumlah transaksi dan nasabah atau pengguna PJP yang tinggi akan menyebabkan perusahaan tersebut perlu berlangganan paket *enterprise* PSrE dengan jumlah akun per pegawai yang besar untuk mengakomodasi kewajiban sertifikasi elektronik atas transaksi elektronik berisiko tinggi, dengan definisi risiko tinggi yang belum ditentukan. Oleh karena itu, kewajiban sertifikasi elektronik untuk transaksi elektronik dengan definisi risiko tinggi yang luas berpotensi menjadi beban operasional tambahan bagi PJP sehingga, peningkatan beban operasional dapat memaksa PJP melimpahkan sebagian beban tersebut ke konsumen mereka.

[39] Lax, Buccafuri, dan Caminiti, "Digital Document Signing: Vulnerabilities and Solutions," Vol. 6, No. 1-3, Hal. 7-8, 2015. https://doi.org/10.1080/19393555.2014.998843
[40] Ibid.
[41] Lax, Buccafuri, dan Caminiti, "Digital Document Signing: Vulnerabilities and Solutions," Information and Security Journal: A Global Perspective, Vol. 6, No. 1-3, Hal. 5, 2015. https://doi.org/10.1080/19393555.2014.998843
[42] Privy for Business, Enterprise Plan. https://tinyurl.com/3kyacc3r

Di sisi lain, PJP juga perlu beradaptasi dengan ketentuan tersebut dengan mengubah proses bisnis menjadi lebih panjang, mengingat adanya keterlibatan pihak lain, yakni PSrE, dalam proses transaksi. Perubahan tersebut dapat menimbulkan biaya tambahan bagi PJP. Meski pada dasarnya PSrE bersedia menjalankan servernya di lokasi milik PJP demi alasan keamanan dan efisiensi, alternatif tersebut tetap memerlukan modal tambahan bagi PJP.

Pada dasarnya, BI telah memberikan ketentuan penetapan biaya yang dapat dibebankan kepada konsumen sebagaimana yang dimuat di PBI No. 23/6/PBI/2021 tentang PJP. Menurut PBI No. 23/6/PBI/2021 Pasal 170(1), komponen biaya transaksi elektronik yang diperbolehkan dikenakan PJP kepada konsumen adalah biaya pembelian media uang elektronik pertama kali atau penggantian media instrumen uang elektronik, biaya pengisian ulang, biaya tarik tunai melalui kanal pihak lain, biaya transaksi transfer dana antar pengguna ke penerima yang menggunakan jasa PJP berbeda, serta biaya lain yang ditetapkan oleh BI.[43]

Namun demikian, pada Pasal 52 peraturan tersebut juga melarang penyedia barang dan/atau jasa mengenakan biaya tambahan (*surcharge*) kepada pengguna atas biaya layanan yang dikenakan PJP kepada penyedia barang dan jasa tersebut.[44] Sementara Pasal 168 melarang pengenaan biaya pengakhiran penggunaan (*redemption*) uang elektronik.[45] Dengan kata lain, terdapat celah hukum yang memperbolehkan PJP membebankan ongkos tambahan kepada pengguna dalam konteks PBI No. 23/6/PBI/2021 Pasal 170(1) jika kiranya PJP perlu mengatur kembali struktur biaya operasionalnya untuk mengakomodasi sertifikasi elektronik di dalam layanan pembayaran digitalnya.

Selain itu, tidak menutup kemungkinan bagi PJP untuk melimpahkan sebagian beban operasional yang disebabkan kebijakan kewajiban sertifikasi elektronik pada jasa-jasa yang tidak spesifik transaksi elektronik yang diatur skema harganya melalui PBI No. 23/6/PBI/2021 Pasal 54. Contoh jasa-jasa yang diatur skema harganya oleh BI tersebut mencakup biaya pengisian ulang saldo uang elektronik, biaya tarik tunai, biaya transfer, *capping* suku bunga, *merchant discount rate*, biaya transaksi *online* dari PJP kepada penyedia barang, *terminal usage fee* antar PJP, biaya *sharing infrastructure* antar PJP.[46]

Penetapan kebijakan skema harga tersebut di atas dimaksudkan untuk mendorong perluasan akseptasi, layanan, dan inovasi; meningkatkan efisiensi dan kompetisi; dan/atau memperhatikan kepentingan publik dan pelaku industri secara seimbang.[47] Dengan menimbang potensi disrupsi pada operasional model bisnis PJP yang sudah berjalan dengan diberlakukannya TTET, maka terdapat pula potensi pengaruh negatif kepada keseimbangan inovasi bisnis PJP dan inklusi keuangan digital masyarakat Indonesia sebagai objek yang dilindungi di dalam PBI No. 23/6/PBI/2021.

[43] Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran Pasal 170(1)
[44] Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran Pasal 52(1) berbunyi, "Penyedia Barang dan/atau Jasa dilarang mengenakan biaya tambahan (surcharge) kepada Pengguna Jasa atas biaya yang dikenakan oleh PJP kepada Penyedia Barang dan/atau Jasa."
[45] Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran Pasal 168(3)
[46] Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran Pasal 54(2)
[47] Peraturan Bank Indonesia Nomor 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran Penjelasan Pasal 54(3)

9.4. Pengaruh kebijakan sertifikasi elektronik terhadap PJP dan PSrE

Pada dasarnya, sektor keuangan menjadi area yang secara ketat diregulasi oleh pemerintah. Selain itu, aspek perlindungan konsumen di sektor ini juga banyak yang perlu diakomodasi oleh PJP sebagai kepanjangan tangan dari regulator. Dengan kata lain, PJP memiliki tugas besar untuk menginterpretasikan regulasi ketat tersebut ke dalam pesan yang lebih sederhana kepada pengguna dari kalangan masyarakat umum. Oleh karena itu, ketika ada kebijakan sertifikasi elektronik yang berpotensi meliputi transaksi digital yang sehari-hari dilaksanakan oleh para pengguna, maka PJP sedikit banyak perlu beradaptasi dengan kebijakan tersebut dengan sangat hati-hati agar tidak serta merta berimbas kepada para penggunanya.

Selain itu, pemberlakuan TTET sebagai standar pengamanan transaksi elektronik secara kaku juga berpotensi mengurangi ruang inovasi bagi PJP dalam pengembangan mekanisme pencegahan *fraud*. Sebagaimana diketahui, berbagai skema pengamanan yang sudah ada seperti OTP dan MFA, yang sudah sangat umum diimplementasikan pada sektor jasa keuangan digital, tidak ada satu pun di antaranya yang diatur secara eksplisit melalui UU. Keberadaan mekanisme pengamanan tersebut di atas tumbuh secara organik sebagai bagian dari inovasi industri dalam merespons risiko keamanan siber sehingga memungkinkan fleksibilitas dan penyesuaian terhadap dinamika ancaman yang terus berkembang. Dengan kata lain, pelaku jasa keuangan berpotensi kehilangan keleluasaan untuk menciptakan metode otorisasi pembayaran digital yang lebih adaptif, efisien, atau kontekstual sesuai dengan prinsip *market-based*. Hal ini menciptakan tantangan tersendiri dalam menciptakan sistem keamanan yang inklusif namun tetap kuat, terutama dalam ekosistem pembayaran digital yang sangat beragam di Indonesia.

Di sisi lain, jika frekuensi TTET di Indonesia meningkat dalam skala besar dengan adanya perubahan dasar hukum, maka pihak Penyelenggara Sertifikat Elektronik (PSrE) akan harus mengadakan perangkat baru dalam skala besar untuk memenuhi permintaan generasi kriptograf yang meningkat secara eksponensial. Mengikuti logika permintaan dan penawaran pasar, jika permintaan melebihi penawaran, maka harga akan naik dalam rangka penyesuaian diri. Dalam konteks ini, PSrE akan menaikkan biaya langganan jasa TTET untuk menyesuaikan dengan besarnya peningkatan frekuensi generasi kriptografi baru. Dengan demikian, lembaga-lembaga keuangan yang menggunakan jasa TTET akan mengenakan sebagian dari kenaikan biaya tersebut ke kategori pengenaan biaya yang diperbolehkan PBI 23/6/PBI/2021.

Pada dasarnya, model jasa yang disediakan oleh PSrE tidak berhenti pada penyediaan layanan verifikasi, tetapi juga mencakup tanggung jawab finansial dalam bentuk skema jaminan atau *payout guarantee* kepada klien mereka. Artinya, dalam banyak kasus, PSrE memiliki kewajiban untuk menggantikan kerugian jika terjadi insiden penipuan atau pelanggaran yang lolos dari sistem verifikasi mereka. Model seperti ini menempatkan PSrE bukan hanya sebagai penyedia layanan teknis, tetapi juga sebagai entitas yang menanggung risiko dalam setiap transaksi. Konsekuensinya, seiring dengan meningkatnya frekuensi transaksi digital yang harus diverifikasi menggunakan TTET, maka eksposur risiko yang harus ditanggung oleh PSrE juga akan meningkat secara proporsional. Setiap proses verifikasi tambahan adalah satu kemungkinan tambahan ketika kesalahan sistem atau kegagalan deteksi bisa terjadi, dan apabila hal tersebut mengarah pada kerugian bagi pihak klien, PSrE diwajibkan untuk memberikan kompensasi sebagai ganti rugi.

9.5. Potensi stagnasi inklusi keuangan

Inklusi keuangan diposisikan sebagai salah satu elemen strategis pembangunan nasional sebagaimana diatur dalam UU No. 59/2024 tentang Rencana Pembangunan Jangka Panjang Nasional (RPJPN) 2025–2045, yang menetapkan target nasional sebesar 98 persen pada 2045. Selain itu, penjabaran lebih lanjut dalam Rencana Pembangunan Jangka Menengah Nasional (RPJPN) 2025–2029, yang disusun dengan mengintegrasikan visi dan misi Presiden dan kebijakan RPJPN, menempatkan inklusi keuangan sebagai indikator Sasaran Utama Prioritas Nasional dengan target 91 persen pada 2025 dan 93 persen pada 2029.

Kenaikan biaya yang harus ditanggung pengguna jasa transaksi elektronik juga memiliki implikasi negatif terhadap inklusi keuangan bagi masyarakat luas. Menurut Surat Edaran OJK No. 31/SEOJK.07/2017, yang dimaksud dengan inklusi keuangan adalah ketersediaan akses pada berbagai lembaga, produk dan layanan jasa keuangan sesuai dengan kebutuhan dan kemampuan masyarakat dalam rangka meningkatkan kesejahteraan masyarakat. Pada dasarnya, inklusi keuangan yang terbatas atau kurang luas berpotensi mengikis kemampuan adaptasi para entitas usaha di suatu negara dari berbagai disrupsi karena aset yang dapat diakumulasi menurun, sehingga potensi pertumbuhan ekonomi negara secara umum juga akan berkurang.[48]

Selain itu, tingkat inklusi keuangan memiliki pengaruh pada efektivitas transmisi kebijakan moneter. Studi atas hubungan inklusi keuangan dan kebijakan moneter di Vietnam antara tahun 2004 dan 2024 menemukan bahwa inklusi keuangan memiliki hubungan negatif terhadap inflasi, sehingga peningkatan inklusi keuangan dapat mendukung efektivitas kebijakan moneter dengan mendukung stabilitas harga barang dan jasa. Ekspansi inklusi keuangan melalui digitalisasi pasca 2015 yang diakselerasi pandemi COVID-19 meningkatkan cakupan transmisi kebijakan moneter di tengah disrupsi pandemi. Studi tersebut juga menemukan ranah transmisi kebijakan moneter tradisional seperti bunga dan nilai tukar mata uang semakin penting seiring peningkatan inklusi keuangan.[49]

Di sisi lain, peningkatan inklusi keuangan bagi kelompok masyarakat berpenghasilan rendah membutuhkan produk dan jasa keuangan dengan harga atau tarif yang terjangkau.[50] Dengan kata lain, bila terjadi kenaikan biaya yang harus ditanggung pengguna jasa transaksi elektronik, tingkat inklusi keuangan bagi masyarakat umum dapat berkurang sehingga berimbas pada potensi penurunan pertumbuhan ekonomi digital.

Dengan keadaan inklusi keuangan digital di Indonesia yang masih terus tumbuh dan masih terdapat kesenjangan antara daerah perkotaan dengan pedesaan dan antara generasi muda dengan tua, pada dasarnya pembayaran digital masih perlu waktu untuk betul-betul bisa menjangkau kalangan yang masih memiliki keterbatasan literasi digital. Bukan hanya itu, literasi digital juga memerankan peran penting untuk menumbuhkan kesadaran masyarakat akan pentingnya pengamanan data pribadi dan aspek pencegahan kejahatan keuangan digital. Dengan kata lain, keunggulan pembayaran digital yang relatif mudah digunakan oleh masyarakat umum masih rentan terhadap

[48] Ngonyani, "Financial Inclusion: Cost and Implications in Developing Countries: A Review of the Existing Literature," Journal of Economics Education and Entrepreneurship, Vol. 3, No. 2, Okt. 2022, Hal. 124. https://doi.org/10.20527/jee.v3i2.5173
[49] Duy dan Minh, "Financial Inclusion and the Effectiveness of Monetary Policy in Vietnam: an Empirical Analysis," Journal of Lifestyle and SDGs Review Vol. 5 No. 6, Juni 2025. https://tinyurl.com/28jhznx6
[50] Ngonyani, "Financial Inclusion: Cost and Implications in Developing Countries: A Review of the Existing Literature," Journal of Economics Education and Entrepreneurship, Vol. 3, No. 2, Okt. 2022, Hal. 126-127. https://doi.org/10.20527/jee.v3i2.5173

disrupsi kebijakan, termasuk kebijakan pengamanan yang tidak efisien, yang kiranya berimplikasi luas pada penggunaannya, khususnya pada aspek proses dan harga layanan.

9.6. Efek kebijakan sertifikasi elektronik pada ekonomi digital

Penambahan mekanisme sertifikasi elektronik sebagai tambahan lapisan anti-penipuan yang diwajibkan berpotensi mengurangi potensi pendapatan di sektor jasa keuangan dan memiliki implikasi negatif terhadap perkembangan ekonomi digital. Dampak kewajiban sertifikasi elektronik atas transaksi elektronik terhadap ekonomi digital di Indonesia berasal dari implikasi ekonomi dari efek yang telah dijabarkan dari kebijakan tersebut terhadap potensi pelimpahan biaya tambahan kepada konsumen, serta kemungkinan kewajiban sertifikasi elektronik menghambat perkembangan inklusi keuangan di Indonesia.

Temuan dari studi kasus Banxa membuktikan kecurigaan perusahaan infrastruktur transaksi kripto tersebut ketika terjadi penolakan transaksi yang sah oleh sistem anti-penipuan yang diterapkannya. Solusi dari penyedia infrastruktur pembayaran primer yang digunakan Banxa menemukan total nilai sekitar US$7.6 miliar dapat dipulihkan dari transaksi sah tetapi ditolak karena terjaring sistem anti-penipuan Banxa.[51] Kegagalan mendapatkan keuntungan dari transaksi elektronik karena terjaring sistem anti-penipuan semacam ini akan berdampak lebih besar kepada industri fintech dan industri perbankan yang diregulasi jauh lebih ketat jika dibandingkan dengan industri kripto.

Pada kasus lain, survei oleh perusahaan analitik data Fair Isaac Corporation (FICO) menemukan bahwa walau 68 persen pengguna jasa transaksi elektronik waktu nyata (*Real-Time Payment,* RTP) di Indonesia menginginkan perbankan menerapkan sistem anti-penipuan yang lebih baik dalam mendeteksi tindakan penipuan, 93 persen pengguna RTP juga menganggap jumlah tahapan pengecekan untuk keamanan RTP di negara ini sudah cukup banyak. Rasio tersebut jauh melampaui rerata penilaian konsumen RTP global yang mencapai 73 persen. Sementara itu 59 persen konsumen berniat meningkatkan tingkat pemakaian RTP mereka.[52] Dengan kata lain, penambahan tahapan pengecekan untuk keamanan RTP melalui kewajiban sertifikasi elektronik pada transaksi elektronik akan berpengaruh negatif terhadap tingkat pertumbuhan transaksi elektronik, yang selanjutnya turut akan berdampak negatif kepada perkembangan ekonomi digital di Indonesia.

[51] CybersecAsia, “Minimizing false positives in digital payment,“ Okt. 15, 2024. https://tinyurl.com/3uy38vbc
[52] Fair Isaac Corporation, "2024 Scams Impact Survey: Indonesia Investigating the impact of authorized push payment (APP) fraud/scams," Okt. 2024. https://tinyurl.com/2wyxraex

10. Kesimpulan dan rekomendasi

10.1. Kesimpulan

Sisi regulasi

Sektor ekonomi digital, khususnya layanan transaksi keuangan digital, tengah mengalami pertumbuhan di Indonesia dan berpotensi mengalami disrupsi dari kebijakan pemerintah mengenai TTET melalui UU No.1/2024 tentang ITE. Pertumbuhan jumlah nominal dan intensitas transaksi digital tersebut disebabkan oleh kemudahan yang ditawarkan oleh fintech penyedia jasa pembayaran digital. Dengan kata lain, pertumbuhan sektor ini sangat bergantung pada preferensi pasar dan inovasi oleh bisnis fintech sehingga pendekatan yang digunakan dalam pengaturannya perlu memerhatikan *market-based approach.* Di sisi lain, UU No. 1/2024 tentang ITE yang disahkan tahun lalu memuat pengaturan yang berpotensi memengaruhi pertumbuhan sektor keuangan digital, khususnya yang berkaitan dengan penggunaan TTET untuk kegiatan transaksi digital.

Pada UU No. 1/2024 tentang ITE Pasal 17(2a) mengatur bahwa "Transaksi Elektronik yang memiliki risiko tinggi bagi para pihak menggunakan tanda tangan elektronik yang diamankan dengan Sertifikat Elektronik." Pada bagian penjelasan, yang dimaksud dengan Transaksi Elektronik risiko tinggi adalah "transaksi keuangan yang tidak dilakukan dengan tatap muka secara fisik." Pengaturan transaksi keuangan tersebut masih bersifat terlalu umum dan masih memerlukan penjelasan lebih lanjut, khususnya mengenai risiko tinggi yang berbeda-beda di tiap sektor, apalagi pada transaksi digital yang seluruhnya dilaksanakan tanpa tatap muka secara fisik.

Berkaca pada standar regulasi internasional di Uni Eropa dan juga di Singapura yang ketat dan komprehensif, penggunaan TTET diperjelas secara rinci tanpa menghambat efisiensi operasional pasar. Seperti di Uni Eropa yang memiliki tiga klasifikasi TTET (SES, AdES, dan QES) dengan tingkat risiko dan kewajiban penggunaan yang berbeda. Sementara itu, Singapura menerapkan pendekatan yang lebih fleksibel, ketika TTET bersifat opsional dan kepercayaan diberikan pada MFA sebagai jaminan autentikasi yang kuat. Dengan pendekatan tersebut, kedua model tersebut memberi kejelasan dan ruang gerak bagi pelaku pasar untuk tetap berinovasi tanpa terbebani oleh regulasi yang terlalu kaku.

Pada dasarnya, Indonesia telah memiliki paket kebijakan pengamanan transaksi digital yang relatif lengkap, dengan setiap jenisnya memiliki derajat dasar hukum yang berbeda-beda. Di sisi lain, para pelaku bisnis fintech juga pada dasarnya memiliki inisiatif menciptakan dan membuat mekanisme pengamanan transaksi digital yang sesuai dengan karakter pengguna dari kalangan umum masyarakat Indonesia. Hal tersebut perlu dilaksanakan karena mereka memiliki kepentingan untuk menjaga kepercayaan pengguna yang terus meningkat, sehingga kompetisi pasar terus terbentuk dari waktu ke waktu.

Pada akhirnya, dengan menimbang potensi disrupsi pada operasional model bisnis fintech yang bergerak dalam bisnis pembayaran digital yang sudah berjalan, implementasi TTET berpotensi berpengaruh negatif kepada keseimbangan inovasi bisnis fintech PJP dan inklusi keuangan digital masyarakat Indonesia sebagai objek yang dilindungi di dalam PBI No. 23/6/PBI/2021.

Sisi teknis

Meski Indonesia telah memiliki pengaturan pelindungan data pribadi dan pemanfaatan data tersebut untuk kepentingan kependudukan dan verifikasi pengguna layanan keuangan digital, literasi digital masyarakat Indonesia juga masih cenderung belum siap mengantisipasi potensi kejahatan siber. Dengan keadaan inklusi keuangan digital di Indonesia yang masih terus tumbuh dan masih terdapat kesenjangan antara daerah perkotaan dengan pedesaan dan antara generasi muda dengan tua, pada dasarnya pembayaran digital masih perlu waktu untuk betul-betul bisa menjangkau kalangan yang masih memiliki keterbatasan literasi digital, secara khusus literasi finansial digital.

Bukan hanya itu, literasi digital juga memerankan peran penting untuk menumbuhkan kesadaran masyarakat akan pentingnya pengamanan data pribadi dan aspek pencegahan kejahatan keuangan digital. Dengan kata lain, keunggulan pembayaran digital yang relatif mudah digunakan oleh masyarakat umum masih rentan terhadap disrupsi kebijakan, termasuk kebijakan pengamanan yang tidak efisien, yang kiranya berimplikasi luas pada penggunaannya, khususnya pada aspek proses dan harga layanan.

Kecenderungan kejahatan siber di Indonesia bukan hanya berbentuk *impersonation*, tapi juga *social engineering* dan *scam* yang mengelabui korbannya yang dengan kesadaran penuh melakukan *authorized payment*. Dengan kata lain, kejahatan siber semacam ini, yang biasa disebut sebagai APP, terjadi bukan hanya dikarenakan adanya penyalahgunaan data pribadi pengguna, tapi juga absensi literasi digital yang sangat menentukan keberhasilan upaya penipuan yang banyak terjadi di Indonesia. Kendala literasi digital semacam ini tidak bisa ditanggulangi dengan membuat sistem pelindungan data pribadi dan pengamanan pembayaran digital, tapi perlu dilakukan adanya edukasi yang dilakukan oleh seluruh pemangku kepentingan di sektor keuangan digital, yang melibatkan regulator dan kalangan bisnis dalam rangka menciptakan ekosistem pembayaran elektronik yang aman dan andal.

Pada sisi pelaku industri, berbagai skema pengamanan yang sudah ada seperti OTP dan MFA, yang sudah sangat umum diimplementasikan pada sektor jasa keuangan digital, tidak ada satu pun di antaranya yang diatur secara eksplisit melalui UU. Keberadaan mekanisme pengamanan tersebut di atas tumbuh secara organik sebagai bagian dari inovasi industri dalam merespons risiko keamanan siber sehingga memungkinkan fleksibilitas dan penyesuaian terhadap dinamika ancaman yang terus berkembang. Dengan kata lain, pelaku jasa keuangan berpotensi kehilangan keleluasaan untuk menciptakan metode otorisasi pembayaran digital yang lebih adaptif, efisien, atau kontekstual sesuai dengan prinsip *market-based*.

10.2. Rekomendasi

Tujuan dari revisi UU ITE adalah untuk menekan risiko *fraud,* sementara risiko dari penerapan sistem pengamanan digital dalam bentuk apa pun adalah potensi disrupsi terhadap perkembangan ekonomi digital dan inklusi keuangan yang perkembangannya masih sangat rentan. Oleh karena itu, dalam rangka menjaga ekosistem ekonomi digital Indonesia tetap bersahabat dengan perkembangan inovasi bisnis dan kenyamanan pengguna yang lekat kaitannya dengan inklusi keuangan, tanpa harus mengorbankan sisi keamanan serta keandalan transaksi elektronik, maka kiranya beberapa poin rekomendasi di bawah ini perlu diperhatikan oleh para pembuat kebijakan terkait.

1. Definisi "Transaksi Elektronik yang memiliki risiko tinggi" perlu diperjelas dengan peraturan teknis turunan dari UU No. 1/2024 tentang ITE, yang pada saat ini masih memiliki definisi yang terlalu luas. Perumusan definisi tersebut perlu mempertimbangkan *cost and benefit analysis* sehingga pengelompokan jenis transaksi yang diatur oleh klausul tersebut benar-benar tepat sasaran untuk menekan *fraud* dan tidak berimplikasi kontra produktif terhadap manfaat yang ditimbulkan oleh perkembangan ekonomi digital yang sudah ada, khususnya pada pertumbuhan inklusi keuangan.
2. Regulator sektor keuangan digital perlu terus mendorong inovasi aktor bisnis dalam rangka menciptakan mekanisme pengamanan yang paling andal dan tepat dengan keadaan pasar, termasuk kolaborasi antar PJP yang telah tercermin dari operasional IASC yang turut mendorong diciptakannya mekanisme anti *fraud* tanpa mekanisme regulasi yang kecenderungannya mengikat, prosedural, dan teknologi-spesifik. Perspektif dari regulator tersebut perlu dibangun dalam rangka menumbuhkan kolaborasi aktif dari pelaku bisnis sehingga mekanisme mitigasi dan penanggulangan risiko benar-benar sesuai dengan preferensi pengguna.
3. Pelindungan data pribadi masyarakat, khususnya para pengguna jasa transaksi digital, perlu menjadi perhatian regulator yang sebetulnya sudah memiliki dasar hukum melalui UU No. 27/2022 tentang PDP. Otoritas Pelindungan Data Pribadi sebagai ujung tombak pelaksanaan pelindungan data pribadi sebagai bagian dari upaya pelindungan hak asasi manusia perlu segera dibentuk, dan peraturan teknis turunan dari UU tersebut perlu segera diselesaikan dengan mempertimbangkan perspektif *market-based*. Jaminan data pribadi yang diamankan dan digunakan sebagaimana mestinya penting dilaksanakan sebagai dasar kegiatan transaksi elektronik yang terbebas dari potensi kejahatan, seperti *fraud, impersonation*, dan *scam.* Pelaksanaan pengelolaan data pribadi secara efektif dan aman menjadi salah satu kunci dalam menciptakan ekosistem ekonomi digital, termasuk kegiatan transaksi digital, yang menjunjung tinggi kepentingan perlindungan konsumen.
4. Dalam rangka memastikan keseimbangan antara pengendalian risiko dan keberlanjutan inovasi di sub-sektor transaksi digital, pengaturan teknis terkait transaksi berisiko tinggi sebaiknya ditetapkan oleh regulator yang betul-betul memiliki kewenangan dan kekhususan pada area ini, seperti BI dan OJK. Hal ini akan memungkinkan penerapan kebijakan yang lebih kontekstual, selaras dengan dinamika industri, sekaligus tetap menjaga stabilitas dan integritas sistem keuangan digital nasional.

Tenggara Strategics adalah lembaga riset dan konsultasi bisnis dan investasi yang didirikan oleh Centre for Strategic and International Studies (CSIS), *The Jakarta Post*, dan Universitas Prasetiya Mulya. Dengan menggabungkan keunggulan ketiga organisasi tersebut, kami bertujuan untuk membantu komunitas bisnis dengan kajian-kajian yang andal dan komprehensif terkait bidang-bidang yang dapat membantu para pemimpin bisnis mengambil keputusan strategis.

PT Trisaka Wahana Tenggara

The Jakarta Post Building
Jl. Palmerah Barat 142-143
Jakarta 10270

+62 21 5300476/8 ext. 5001

info@tenggara.id

www.tenggara.id