



DOI: <https://doi.org/10.38035/jihhp.v5i6>
<https://creativecommons.org/licenses/by/4.0/>

Perlindungan Konsumen Terhadap Scam Di Era Digital : Studi Komparatif Efektivitas Indonesia Anti Scam Centre Dan Regulasi Singapura

Kiki Anggraeni¹, Yuniar Rahmatiar², Muhamad Abas³

¹Universitas Buana Perjuangan Karawang, Karawang, Indonesia, hk21.kikianggraeni@mhs.ubpkarawang.ac.id.

²Universitas Buana Perjuangan Karawang, Karawang, Indonesia, yuniar@ubpkarawang.com.

³Universitas Buana Perjuangan Karawang, Karawang, Indonesia, muhamad.abas@ubpkarawang.ac.id.

Corresponding Author: muhamad.abas@ubpkarawang.ac.id.³

Abstract: *Consumer protection in the digital era provides many benefits to consumers such as easy access to information, efficiency, and innovation in various fields. However, this development creates new risks such as scams committed by irresponsible parties, and has the potential to cause large financial losses. This research aims to identify and analyze how the effectiveness of legal protection for consumers who are victims of digital scams in Indonesia and Singapore, and to compare the handling mechanisms of the Indonesia Anti Scam Centre and the Singapore Anti Scam Centre. This research uses a qualitative research method with a normative juridical approach where the approach is based on legislation and comparative studies between Indonesia and Singapore. This research concludes that consumer protection and anti-scam centre regulations in handling scams play an important role in minimizing scam victims and protecting consumers from financial losses.*

Keyword: *Consumer Protection, Anti Scam Center, Scam.*

Abstrak: Perlindungan konsumen di era digital memberikan banyak manfaat kepada konsumen seperti kemudahan akses informasi, efisiensi, dan inovasi dalam berbagai bidang. Namun perkembangan ini menimbulkan risiko baru seperti *scam* yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab, dan berpotensi menimbulkan kerugian finansial yang besar. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis bagaimana efektivitas perlindungan hukum terhadap konsumen korban *scam* digital di Indonesia dan Singapura, serta mengetahui perbandingan mekanisme penanganan Indonesia Anti Scam Centre dan *Singapore Anti Scam Centre*. Penelitian ini menggunakan metode penelitian kualitatif dengan pendekatan yuridis normatif yang dimana pendekatan dilakukan berdasarkan peraturan perundang-undangan dan studi perbandingan antara Indonesia dengan Singapura. Penelitian ini menyimpulkan bahwa perlindungan konsumen dan regulasi *anti scam centre* dalam menangani *scam* berperan penting untuk meminimalkan korban *scam* dan melindungi konsumen dari kerugian finansial.

Kata Kunci: Perlindungan Konsumen, Anti Scam Centre, Scam.

PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah mengubah lanskap transaksi ekonomi secara fundamental, menciptakan peluang sekaligus tantangan baru dalam perlindungan konsumen. Beragam kegiatan kini dapat dilakukan secara daring, mulai dari berbelanja, berkomunikasi, bekerja, hingga mengakses pendidikan. Selain itu, informasi terkait transportasi dan kebutuhan lainnya pun semakin mudah dijangkau melalui internet. Meski memberikan kemudahan, masyarakat tetap perlu meningkatkan kewaspadaan terhadap maraknya tindak penipuan yang kian berkembang (Asriansyah, 2023). Di era digital saat ini, kejahatan penipuan mengalami evolusi yang pesat seiring dengan kemajuan teknologi, memanfaatkan kemudahan anonimitas, keterbatasan literasi digital masyarakat, serta sifat lintas batas dari internet. Penipuan digital, atau *scam*, merupakan tindakan manipulatif yang dilakukan secara sengaja demi memperoleh keuntungan pribadi maupun kelompok, dengan cara merugikan orang lain (Wicaksono, 2020). Dalam lanskap digital, *scam* mencakup berbagai bentuk kejahatan siber yang menggunakan media digital sebagai alat utamanya, mulai dari *phishing*, pencurian data pribadi, pemerasan melalui *ransomware*, hingga penipuan keuangan yang semakin kompleks dan sulit dilacak (Force, 2024). Fenomena ini menunjukkan adanya urgensi untuk memperkuat perangkat hukum serta meningkatkan efektivitas implementasi perlindungan terhadap konsumen. Pembentukan pusat *anti scam* menjadi langkah strategis dalam upaya hukum untuk memberikan perlindungan maksimal terhadap masyarakat dari ancaman kerugian finansial yang ditimbulkan oleh kejahatan digital.

Berdasarkan laporan dari Kementerian Komunikasi dan Informatika Republik Indonesia, sepanjang periode 2017 hingga 2024, tercatat sebanyak 572.000 pengaduan terkait penipuan daring. Jumlah tersebut menempatkan Indonesia di jajaran negara dengan laju pertumbuhan kejahatan siber tertinggi di Asia Tenggara (Mandra, 2024). Sumber lain mengungkapkan bahwa pada tahun 2024, sekitar 23% konsumen di Indonesia mengalami kerugian secara finansial akibat praktik scam, naik signifikan dari angka 19% pada tahun sebelumnya, dengan kecenderungan meningkatnya kasus scam yang melibatkan nominal besar (Tech for Good Institute, 2025). Tren serupa juga terjadi di Singapura, di mana Kepolisian setempat mencatat 51.501 laporan kasus penipuan digital sepanjang tahun 2024, naik dari 46.563 laporan pada tahun 2023. Total kerugian ekonomi yang ditimbulkan dari kasus scam di Singapura pada tahun yang sama diperkirakan mencapai S\$1,1 miliar setara dengan Rp. 12,1 triliun rupiah (Wallinda, 2025).

Di Indonesia, Otoritas Jasa Keuangan (OJK) bersama seluruh instansi yang tergabung dalam Satuan Tugas Pemberantasan Aktivitas Keuangan Ilegal (Satgas PASTI) secara resmi membentuk Indonesia Anti Scam Centre (IASC) pada 22 September 2024 sebagai bentuk inisiatif kolektif antar lembaga dalam merespons maraknya penipuan digital secara lebih terstruktur dan terintegrasi. Pendirian Satgas PASTI sendiri berlandaskan pada Keputusan Dewan Komisiner OJK Nomor 1/KDK.08/2023, yang merupakan implementasi dari mandat Pasal 247 Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK). Satgas ini terdiri dari 16 kementerian dan lembaga, termasuk OJK, Kepolisian Republik Indonesia, Kejaksaan Agung, dan Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK). IASC ditetapkan sebagai pusat kendali nasional dalam menangani kejahatan *scam* di sektor jasa keuangan, guna memastikan respons yang lebih cepat, terkoordinasi, dan adaptif (OJK, 2022). Kehadirannya dilandasi oleh kebutuhan yang mendesak akan sebuah mekanisme yang mampu menjawab tantangan kompleksitas kejahatan digital secara efektif dan responsif (Hudiyanto, 2024a). Namun, sebagai institusi yang masih dalam tahap awal pembentukan, IASC masih menghadapi beragam tantangan baik dari sisi

struktur kelembagaan, harmonisasi regulasi, hingga efisiensi operasional. Kondisi ini mencerminkan bahwa sistem perlindungan konsumen di Indonesia belum sepenuhnya terintegrasi dan masih berjalan secara sektoral, yang berdampak pada lambatnya proses penanganan dan rendahnya tingkat pemulihan kerugian korban. Situasi ini semakin diperburuk oleh rendahnya literasi digital di kalangan masyarakat serta hambatan dalam penegakan hukum lintas yurisdiksi, mengingat banyak jaringan sindikat *scam* beroperasi dari luar wilayah Indonesia (United Nation Office on Drugs and Crime, 2024).

Dalam konteks perbandingan sistem perlindungan konsumen, Indonesia dan Singapura menawarkan perspektif yang menarik, mengingat perbedaan sistem hukum keduanya namun memiliki posisi strategis dalam perekonomian global (Wibowo, 2024). Singapura telah lebih dahulu mengimplementasikan pendekatan terintegrasi melalui pembentukan *Anti-Scam Centre* sejak tahun 2019, yang terbukti efektif dalam merespons dan menangani berbagai bentuk kejahatan digital. Inisiatif ini dijalankan di bawah koordinasi *Inter-Ministry Committee on Scams* (IMCS), yang melibatkan lembaga-lembaga kunci seperti *Monetary Authority of Singapore* (MAS), *Singapore Police Force* (SPF) melalui unit khusus *Anti-Scam Command* (ASCom), *Infocomm Media Development Authority* (IMDA), serta *Cyber Security Agency of Singapore* (CSA). Berdasarkan data dari Singapore Police Force, hingga 2024, Anti-Scam Centre berhasil membekukan lebih dari 40.900 rekening bank yang terkait dengan aktivitas penipuan, serta memulihkan dana korban *scam* senilai lebih dari S\$182 juta. Keberhasilan tersebut ditopang oleh kerangka regulasi yang menyeluruh, kolaborasi intensif antar lembaga penegak hukum dan sektor keuangan (Yap, 2024). Serta penerapan inisiatif inovatif seperti *Shared Responsibility Framework* (SRF), yang mengharuskan institusi keuangan dan perusahaan telekomunikasi untuk menerapkan tindakan preventif secara spesifik terhadap serangan phishing (Derry, 2025).

Terdapat sejumlah persamaan dan perbedaan mendasar antara pendekatan penanggulangan penipuan digital yang diterapkan oleh Indonesia Anti Scam Centre (IASC) dan *Singapore Anti Scam Centre* (SASC). IASC di Indonesia memiliki mandat utama untuk menunda transaksi mencurigakan yang terindikasi penipuan, mengidentifikasi pihak-pihak yang terlibat, mengupayakan pengembalian dana korban yang masih tersisa, serta melaksanakan proses penindakan hukum terhadap pelaku (Hudiyanto, 2024b). Sementara itu, SASC di Singapura juga menjalankan fungsi serupa dalam hal penghentian dan pencegahan aktivitas penipuan, serta penegakan hukum melalui identifikasi pelaku. Namun, berbeda dengan IASC, SASC tidak secara langsung memfokuskan diri pada pemulihan dana korban sebagai bagian dari mandat utamanya (Domnic Dass, 2021). Fokus utama dari *unit Anti-Scam Command* (ASCom) di bawah *Singapore Police Force* adalah investigasi mendalam, penindakan tegas, dan intervensi cepat berbasis intelijen, di mana pemulihan dana lebih merupakan konsekuensi dari keberhasilan pembekuan aset hasil kejahatan, bukan layanan pemulihan secara langsung kepada korban sebagaimana dilakukan oleh IASC. Meski demikian, peran SASC tetap signifikan dalam upaya perlindungan konsumen melalui strategi preventif berbasis teknologi, seperti pengembangan aplikasi *ScamShield* serta penerapan kebijakan registrasi identitas pengirim SMS melalui *SMS Sender ID Registry* (SSIR), yang berfungsi sebagai sistem penyaring untuk mencegah pesan penipuan menjangkau pengguna (Monetary Authority of Singapore, 2024).

Penipuan berkedok lowongan kerja, atau *job scam*, telah menjadi salah satu bentuk kejahatan digital yang paling merusak dan meresahkan dalam lanskap dunia maya. Modus ini kerap ditemukan di berbagai platform digital yang memuat informasi peluang kerja, di mana pelaku dengan lihai mengeksploitasi kepercayaan dan minimnya kewaspadaan calon korban. Dalam praktiknya, para penipu sering menyamar sebagai perwakilan dari perusahaan ternama atau individu yang dikenal oleh korban guna memperoleh data pribadi yang bersifat sensitif, atau untuk membujuk korban melakukan tindakan tertentu yang mengarah pada kerugian finansial

maupun pencurian identitas (Wicaksono, 2020). Di Singapura, *job scam* tercatat sebagai salah satu kategori penipuan dengan frekuensi tertinggi, dengan jumlah laporan mencapai 9.043 kasus sepanjang tahun 2024, dan total kerugian yang ditimbulkan mencapai S\$156,2 juta (Force, 2024).

Penelitian ini menawarkan kebaruan melalui fokus khusus terhadap fenomena *scam* yang tengah berkembang pesat di era digital, dengan pendekatan komparatif yang menelaah secara mendalam efektivitas peran Indonesia Anti Scam Centre (IASC) sebagai lembaga perlindungan konsumen, serta membandingkannya dengan *Singapore Anti Scam Centre* (SASC). Keunggulan utama dari penelitian ini terletak pada penekanan analitis terhadap kontribusi IASC dalam memberikan perlindungan hukum bagi konsumen digital, sekaligus mengevaluasi regulasi di Singapura yang telah lebih maju dan terstruktur. Analisis ini mencakup penelaahan kerangka kebijakan seperti *Shared Responsibility Framework* (SRF) serta inovasi teknologi seperti *ScamShield*, yang secara keseluruhan memberikan perspektif yang lebih menyeluruh dan aplikatif guna mendorong reformasi regulasi di Indonesia agar lebih responsif terhadap kejahatan digital yang terus berkembang.

Tujuan dari penulisan ini adalah untuk memperkaya khazanah keilmuan di bidang perlindungan hukum terhadap konsumen yang menjadi korban penipuan digital, khususnya dalam konteks hukum perlindungan konsumen. Pembahasan diarahkan pada analisis terhadap peraturan perundang-undangan yang berlaku di Indonesia sebagai instrumen perlindungan hukum, serta mengkaji secara khusus peran OJK dalam menangani maraknya kasus scam digital. Selanjutnya, kajian ini memperbandingkan mekanisme yang diterapkan oleh IASC dengan sistem yang telah dibangun oleh SASC di Singapura. Penelitian ini bertujuan untuk mengidentifikasi sejauh mana efektivitas perlindungan hukum bagi konsumen korban scam digital di kedua negara, serta mengungkap perbedaan dan persamaan dalam mekanisme penanganan yang dijalankan oleh masing-masing pusat anti scam.

METODE

Penelitian ini menggunakan metode kualitatif dengan pendekatan yuridis normatif, yaitu pendekatan yang bertumpu pada kajian terhadap peraturan perundang-undangan serta analisis perbandingan hukum (komparatif). Data primer yang digunakan berupa peraturan perundang-undangan yang relevan dengan isu perlindungan konsumen dari kejahatan digital, sementara data sekunder meliputi literatur dari buku-buku hukum, jurnal ilmiah, dan sumber-sumber terpercaya dari situs web resmi (Soerjono Soekanto and Sri Mamudji, 2001). Adapun instrumen hukum utama dalam penelitian ini mencakup Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 sebagai perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, serta Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan. Selain itu, penelitian ini juga memuat studi komparatif dengan sistem hukum Singapura, dengan tujuan menelaah efektivitas dan tata kelola dari pembentukan Indonesia Anti Scam Centre (IASC) dibandingkan dengan Singapore Anti Scam Centre (SASC), yang dikenal memiliki pendekatan yang sistematis dan terbukti berhasil. Regulasi-regulasi yang dijadikan rujukan dalam konteks Singapura antara lain *Computer Misuse Act* (CMA), *Cybersecurity Act 2018*, *Shared Responsibility Framework* (SRF), *Personal Data Protection Act* (PDPA), dan *Electronic Transactions Act* (ETA). Melalui evaluasi menyeluruh terhadap kerangka hukum yang ada di kedua negara, penelitian ini diharapkan mampu menghasilkan analisis mendalam yang disusun secara sistematis dalam bentuk naskah jurnal yang komprehensif.

HASIL DAN PEMBAHASAN

1. Efektivitas Perlindungan Hukum Terhadap Konsumen Korban Scam Digital di Indonesia dan Singapura

Berdasarkan data yang dihimpun dari Indonesia Anti Scam Centre (IASC), sejak didirikan, lembaga ini telah menerima puluhan ribu laporan terkait penipuan digital dan berhasil memblokir ribuan rekening yang terindikasi terlibat dalam aktivitas ilegal tersebut. Hingga Maret 2025, tercatat sebanyak 67.866 laporan telah diterima dengan estimasi total kerugian mencapai Rp1,2 triliun, sementara dana sebesar kurang lebih Rp129,1 miliar berhasil dibekukan sebagai langkah preventif terhadap kerugian lanjutan (Kholid Rafsanjani, 2025). Kecepatan respons dan koordinasi antar lembaga, khususnya antara Otoritas Jasa Keuangan (OJK), Satuan Tugas Pemberantasan Aktivitas Keuangan Ilegal (Satgas PASTI), serta penyedia jasa keuangan, menunjukkan adanya kemajuan dalam pemutusan aliran dana yang mengarah pada pelaku scam (Hudiyanto, 2025). Namun demikian, efektivitas regulasi yang ada masih menghadapi sejumlah keterbatasan. Salah satunya adalah waktu penanganan yang relatif lambat jika dibandingkan dengan mekanisme yang dijalankan oleh Singapore Anti Scam Centre, yang telah menerapkan sistem yang lebih terintegrasi dan responsif. Hal ini mengindikasikan perlunya pembaruan serta penguatan implementasi regulasi di Indonesia (Yuyut Prayuti, 2024b). Tantangan utama lainnya mencakup terfragmentasinya saluran pengaduan dan proses penegakan hukum, ditambah fakta bahwa OJK tidak memiliki kewenangan penyidikan terhadap tindak pidana. Selain itu, pelaku scam menunjukkan kemampuan beradaptasi yang sangat cepat terhadap celah hukum dan teknologi, sehingga memperumit proses pemberantasan secara komprehensif (Tech for Good Institute, 2025).

Peran pemerintah dan sektor industri menjadi sangat strategis dalam membangun ekosistem digital yang aman, transparan, dan adil bagi konsumen. Pemerintah memikul tanggung jawab utama dalam menjamin perlindungan konsumen dari praktik bisnis yang merugikan dan tidak etis. Salah satu instrumen utama yang digunakan adalah melalui pembentukan kerangka hukum dan regulasi yang tegas, yang tidak hanya menetapkan hak dan kewajiban konsumen, tetapi juga memberikan sanksi yang proporsional bagi pelaku usaha yang terbukti melakukan pelanggaran (Riana Pratiwi, 2024). Upaya ini bertujuan untuk menciptakan keseimbangan antara kepentingan konsumen dan pelaku usaha, serta mendorong terciptanya praktik bisnis yang berintegritas dan bertanggung jawab di era ekonomi digital.

Di Indonesia Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK), merupakan tiga kerangka hukum utama yang signifikan dalam melindungi konsumen, mengatur transaksi elektronik, dan memperkuat perlindungan konsumen di sektor jasa keuangan, dalam menghadapi tantangan di era digital yang melibatkan kasus penipuan online (*scam*). Undang-Undang Perlindungan Konsumen menegaskan hak konsumen untuk mendapatkan informasi yang jujur dan benar tentang barang/jasa, termasuk dalam transaksi digital, serta memberikan hak privasi dalam pengumpulan, penggunaan, dan pengolahan informasi pribadi oleh penyedia barang/jasa. Selain itu, mengakui transaksi elektronik, UU Perlindungan Konsumen mengatur hak-hak konsumen dalam konteks ini, termasuk memberikan informasi yang jelas dan komprehensif tentang transaksi elektronik, termasuk kebijakan privasi yang diterapkan oleh penyedia layanan (Yuyut Prayuti, 2024a).

Di Indonesia, terdapat tiga pilar regulasi utama yang memiliki peran vital dalam memberikan perlindungan hukum bagi konsumen di tengah dinamika era digital, yaitu Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 sebagai perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), serta Undang-

Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK). Ketiga undang-undang ini membentuk landasan hukum yang komprehensif dalam menangani tantangan kontemporer seperti maraknya kasus penipuan daring (scam).

UU Perlindungan Konsumen secara eksplisit menjamin hak konsumen untuk memperoleh informasi yang akurat, jujur, dan tidak menyesatkan mengenai barang dan/atau jasa, termasuk dalam konteks transaksi digital. Selain itu, undang-undang ini juga memberikan perlindungan terhadap privasi konsumen dalam hal pengumpulan, pemrosesan, dan penggunaan data pribadi oleh pelaku usaha. Dalam kaitannya dengan transaksi elektronik, UU Perlindungan Konsumen menegaskan pentingnya transparansi melalui kewajiban penyedia layanan untuk menyampaikan informasi yang jelas, termasuk kebijakan privasi serta mekanisme perlindungan data yang diterapkan. Sementara itu, UU ITE dan UU P2SK memperkuat aspek penegakan hukum dan pengawasan terhadap penyalahgunaan teknologi informasi serta aktivitas keuangan ilegal, sehingga keseluruhan kerangka ini saling melengkapi dalam menciptakan sistem perlindungan konsumen yang lebih tangguh dan adaptif di era digital (Yuyut Prayuti, 2024b).

Dalam konteks praktik scam, konsumen kerap kali tidak memperoleh informasi yang memadai mengenai risiko, spesifikasi produk, maupun skema pembayaran yang ditawarkan. Penipuan digital terus berevolusi dengan modus operandi yang semakin kompleks dan tersamarkan, sehingga banyak konsumen terperangkap tanpa menyadari bahwa mereka telah menjadi korban. Situasi ini mencerminkan celah serius dalam pelaksanaan penegakan hukum, khususnya terkait kewajiban transparansi informasi yang seharusnya dijamin oleh peraturan perundang-undangan. Penyalahgunaan informasi oleh pelaku scam untuk memanipulasi dan mengecoh konsumen menjadi salah satu bentuk pelanggaran terhadap prinsip perlindungan konsumen sebagaimana diatur dalam Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen. Ketidadaan kontrol dan verifikasi atas informasi yang beredar, serta lemahnya pengawasan digital, membuat mekanisme perlindungan hukum terhadap konsumen menjadi kurang efektif dalam menangkal praktik penipuan yang semakin marak (Jennifer Clarence, 2024).

Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik (UU ITE) hadir sebagai fondasi hukum yang strategis dalam memperkuat perlindungan konsumen di ranah digital, khususnya dalam menghadapi praktik penipuan yang kian marak dalam transaksi elektronik. UU ini dirancang untuk memberikan kepastian hukum yang tegas terhadap pelaku kejahatan siber yang memanfaatkan media elektronik sebagai sarana untuk melakukan tindakan kriminal, termasuk scam. Salah satu ketentuan krusial dalam UU ITE mengatur tentang tanggung jawab penyelenggara sistem elektronik (PSE), yang diwajibkan memastikan seluruh aktivitas transaksi di platform mereka berlangsung sesuai dengan ketentuan hukum dan bebas dari penyebaran informasi palsu yang dapat merugikan konsumen (Irfan Ridha, 2024). Pasal 28 ayat (1) menyatakan bahwa “Setiap orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam transaksi elektronik”, hal ini secara normatif menjerat tindakan pelaku scam sebagai bentuk pelanggaran hukum. Namun, dalam praktiknya, efektivitas penerapan pasal ini masih menghadapi tantangan serius, terutama karena kecanggihan teknologi yang digunakan pelaku membuat pelacakan dan penegakan hukum menjadi sangat kompleks. Jangkauan internet yang lintas batas dan sifat anonim dari aktivitas daring semakin memperlemah daya jangkau pasal tersebut. Kritik terhadap UU ITE juga mencuat karena pendekatannya yang cenderung represif dan reaktif, di mana tindakan hukum umumnya diambil setelah konsumen mengalami kerugian, bukan melalui upaya pencegahan yang sistematis (Syadid Jiddan Alharun, 2025).

Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan (UU P2SK) menjadi salah satu pilar hukum strategis dalam penguatan ekosistem

keuangan nasional, sekaligus sebagai landasan yuridis utama bagi pembentukan Indonesia Anti Scam Centre (IASC). Regulasi ini tidak hanya menekankan pada pembentukan sektor jasa keuangan yang lebih inklusif dan formal, tetapi juga memberikan fokus pada penguatan aspek perlindungan konsumen serta integritas sistem keuangan nasional. Pasal 5 huruf c menegaskan bahwa tujuan utama pengembangan sektor jasa keuangan adalah untuk mendorong pertumbuhan ekonomi nasional yang stabil dan berkelanjutan melalui penguatan sektor jasa keuangan yang efisien, sehat, dan kompetitif. Sementara itu, Pasal 6 huruf e mengatur secara eksplisit fungsi otoritas keuangan dalam melakukan pengawasan dan pengaturan demi menjamin keamanan, stabilitas, dan perlindungan konsumen dalam lingkup keuangan. Ketentuan ini menjadi dasar kewenangan bagi Otoritas Jasa Keuangan (OJK) untuk menjalankan fungsi pengawasan serta menangani dan mencegah tindak pidana di sektor keuangan. Dengan demikian, OJK memiliki legal standing dalam menginisiasi berbagai langkah preventif dan responsif, termasuk intervensi cepat terhadap kasus scam, pemblokiran rekening mencurigakan, identifikasi pihak-pihak yang terlibat, serta koordinasi intensif dengan aparat penegak hukum seperti Kepolisian Republik Indonesia. Lebih lanjut, Pasal 247 UU P2SK secara khusus mengatur pembentukan Satuan Tugas Pemberantasan Aktivitas Keuangan Ilegal (Satgas PASTI) yang diketuai oleh OJK, dengan mandat utama mencegah serta menangani praktik-praktik melawan hukum dalam penghimpunan dana masyarakat dan pengelolaan investasi ilegal, yang turut menjadi kerangka kerja operasional bagi IASC dalam menangani kejahatan siber di sektor jasa keuangan.

Pembentukan Indonesia Anti Scam Centre (IASC) dilatarbelakangi oleh kebutuhan mendesak akan sistem respons yang cepat dan terintegrasi terhadap meningkatnya kasus penipuan di sektor jasa keuangan. IASC berperan sebagai simpul koordinasi antara para penyedia jasa keuangan untuk mempercepat proses penanganan laporan kejahatan finansial digital, dengan fokus pada penundaan transaksi mencurigakan, pemblokiran rekening yang terindikasi terlibat dalam penipuan, identifikasi aktor yang terlibat, upaya pengembalian dana korban yang masih dapat diselamatkan, serta pendampingan dalam proses penegakan hukum. Mekanisme operasional IASC dimulai dari penerimaan laporan masyarakat melalui portal resmi iasc.ojk.go.id, dilanjutkan dengan verifikasi dan penghentian sementara transaksi, pemetaan jaringan pelaku, pemulihan dana, dan fasilitasi proses hukum yang melibatkan aparat penegak hukum. Sebagai bentuk penguatan sistem, OJK juga meluncurkan Sistem Informasi Pelaku di Sektor Keuangan (SIPELAKU) yang mendokumentasikan riwayat individu yang terlibat dalam tindak kecurangan di sektor keuangan. Langkah ini diambil sebagai respons konkret terhadap eskalasi kasus scam dengan kerugian finansial yang terus meningkat. Dalam pelaksanaannya, IASC mendapatkan dukungan luas dari berbagai pemangku kepentingan seperti asosiasi perbankan, penyedia layanan sistem pembayaran, hingga platform e-commerce, yang bersama-sama membentuk ekosistem pertahanan digital terhadap kejahatan finansial (Hudiyanto, 2024a).

Kasus penipuan daring yang terjadi di Singapura maupun Indonesia menunjukkan kemiripan yang signifikan, baik dari segi jumlah maupun pola kejahatannya. Menurut laporan resmi dari *Singapore Police Force* (SPF), ribuan insiden penipuan tercatat setiap tahun, dengan tren yang terus meningkat secara konsisten. Situasi ini menjadi latar belakang utama dibentuknya pusat anti-penipuan di kedua negara, sebagai langkah strategis dalam menangkal ancaman digital yang semakin kompleks dan masif (Force, 2024). Pada tahun 2024, Singapura mencatat sebanyak 51.501 kasus penipuan digital, mengalami kenaikan sebesar 10,6% dibandingkan tahun sebelumnya, dengan total kerugian yang mencapai S\$1,1 miliar. Jenis penipuan yang paling dominan meliputi *e-commerce scams*, *job scams*, dan *phishing scams*, yang menargetkan masyarakat luas secara masif dan sistematis. Untuk menangani fenomena ini, *Singapore Anti-Scam Centre* (SASC), atau lebih tepatnya *Anti-Scam Command* (ASCom), beroperasi di bawah naungan *Singapore Police Force* (SPF) dan menjadi garda terdepan dalam

pemberantasan penipuan daring. SASC menunjukkan tingkat efektivitas yang tinggi dalam respons terhadap ancaman digital berkat struktur operasional yang terkoordinasi serta pemanfaatan teknologi modern secara maksimal. Salah satu inovasi andalannya adalah penggunaan *Robotic Process Automation* (RPA) untuk mengidentifikasi korban secara cepat dan akurat, mempercepat proses intervensi. Selain itu, aplikasi *ScamShield* berfungsi sebagai alat bantu preventif yang memungkinkan masyarakat mengenali potensi penipuan sejak dini melalui fitur deteksi cerdas. Tak hanya itu, kecanggihan sistem berbasis *Artificial Intelligence* (AI) seperti *Scam Analytics and Tactical Intervention System* (SATIS) juga menjadi elemen kunci dalam mendeteksi dan menganalisis pola-pola penipuan serta pelaku di baliknya, memperkuat upaya proaktif negara dalam melindungi warganya dari kejahatan siber yang terus berevolusi (Yap, 2024).

Singapore Anti-Scam Centre (SASC) menunjukkan kemampuan tinggi dalam melakukan pencegahan dan penindakan secara cepat, terstruktur, serta berbasis data, menjadikannya lebih unggul dibandingkan dengan *Indonesia Anti Scam Centre* (IASC) dalam hal respons operasional. Berbeda dengan IASC yang turut memfokuskan upaya pada pemulihan dana korban, SASC tidak menjadikan pengembalian kerugian finansial sebagai layanan utama, melainkan lebih menitikberatkan pada mitigasi dan pencegahan dini terhadap potensi scam. Efektivitas SASC juga ditopang oleh tingkat literasi digital masyarakat Singapura yang relatif tinggi serta dukungan kampanye edukasi publik yang dilakukan secara masif dan konsisten oleh pemerintah maupun sektor swasta. Di sisi lain, sistem pelaporan yang dirancang ramah pengguna dan mudah diakses turut mendorong partisipasi aktif masyarakat dalam melaporkan insiden penipuan secara real-time. Kombinasi antara strategi edukatif, teknologi canggih, dan kesadaran kolektif masyarakat menjadikan perlindungan konsumen di Singapura lebih terintegrasi dan optimal. Hal ini menciptakan kesenjangan nyata dalam efektivitas perlindungan antara Singapura dan Indonesia, yang masih berjuang dalam membangun sistem pelaporan, respons hukum, dan literasi digital yang setara.

Sementara Indonesia memiliki Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen, Singapura mengatur perlindungan konsumen melalui dua undang-undang terpisah, yaitu Consumer Protection (Trade Descriptions and Safety Requirements) Act yang diberlakukan sejak tahun 1975, dan Consumer Protection (Fair Trading) Act (CPFTA) yang mulai berlaku pada tahun 2003 (Luh Widiya Saraswati, 2022). Dalam konteks penipuan atau scam, fokus utama pembahasan tertuju pada Consumer Protection (Fair Trading) Act (CPFTA). Undang-undang ini dirancang untuk menciptakan dan mendorong terciptanya iklim perdagangan yang adil dan transparan, dengan tujuan utama melindungi kepentingan konsumen dari praktik bisnis yang tidak fair dan merugikan. Melalui regulasi ini, perlindungan konsumen dipertegas guna menangkal tindakan curang dan ketidakadilan dalam transaksi, sehingga memberikan jaminan keamanan dan keadilan dalam hubungan perdagangan (Singapore Statutes Online, 2025).

Pasal yang membahas penipuan online (*scam*) dalam *Consumer Protection* (Fair Trading) Act 2003 (CPFTA), terdapat pada (Luh Widiya Saraswati, 2022):

Article 4

- a) *To do or say anything, or omit to do or say anything, if as a result a consumer might reasonably be deceived or misled;*
- b) *To make a false claim;*
- c) *To take advantage of a consumer if the supplier knows or ought reasonably to know that the consumer:*
 - i. *is not in a position to protect his own interests; or*
 - ii. *is not reasonably able to understand the character, nature, language or effect of the transaction or any matter related to the transaction; or*

d) without limiting the generality of paragraphs (a), (b) and (c), to do anything specified in the Second Schedule.

Pasal ini secara jelas menguraikan definisi praktik bisnis yang tidak adil (*unfair practices*), termasuk tindakan penipuan dan penyajian informasi yang menyesatkan dalam kegiatan perdagangan. Larangan tegas diberikan kepada pelaku usaha agar tidak melakukan tindakan yang dapat menyesatkan konsumen, seperti memberikan data palsu atau memanipulasi fakta dalam proses transaksi. Ketentuan ini sangat relevan dalam konteks kasus *scam*, di mana konsumen sering menjadi korban informasi palsu yang disengaja untuk keuntungan pelaku usaha. Selain itu, *Second Schedule* dalam CPFTA mencantumkan daftar rinci mengenai praktik-praktik tidak adil yang umum terjadi, khususnya dalam perdagangan elektronik, sebagai upaya untuk memberikan batasan yang lebih konkret terhadap perilaku yang dilarang.

Lebih lanjut, dalam huruf d disebutkan sejumlah tindakan khusus yang digolongkan sebagai praktik tidak adil yang termaktub dalam *Second Schedule* tersebut. Secara total, terdapat 24 jenis perilaku yang secara eksplisit diidentifikasi sebagai pelanggaran praktik tidak adil. Pasal-pasal berikutnya dalam undang-undang ini juga menguraikan berbagai kondisi dan situasi yang berkaitan erat dengan penerapan aturan mengenai praktik tidak adil tersebut, memberikan kerangka kerja hukum yang komprehensif untuk menangani kasus-kasus penipuan dan manipulasi dalam dunia perdagangan modern (Luh Widiya Saraswati, 2022):

- 1) *An unfair practice may occur before, during or after a consumer transaction.*
- 2) *An unfair practice may consist of a single act or omission.*
- 3) *In determining whether or not a person has engaged in an unfair practice —*
 - a) *the reasonableness of the actions of that person in those circumstances is to be considered; and*
 - b) *an act or omission by an employee or agent of a person is deemed also to be an act or omission of the person if the act or omission occurred in the course of —*
 - i. *the employee's employment with the person; or*
 - ii. *the agent exercising the powers or performing the duties on behalf of the person within the scope of the agent's actual or apparent authority.*

Ketentuan dalam pasal ini secara tegas melarang segala bentuk praktik tidak adil yang dapat terjadi pada setiap tahap transaksi konsumen—baik sebelum, selama, maupun setelah transaksi berlangsung. Larangan ini mencakup tindakan seperti membuat pernyataan yang menyesatkan, melakukan penipuan, atau mengeksploitasi kelemahan konsumen yang berada dalam posisi tidak seimbang, sehingga tidak mampu membela atau melindungi kepentingannya sendiri. Dalam konteks penipuan digital (*scam*), pasal ini berfungsi sebagai instrumen hukum yang penting dalam memberikan perlindungan bagi konsumen dari tindakan curang dan manipulatif yang dapat merugikan mereka, dengan menuntut agar setiap pelaku usaha menjalankan usahanya secara jujur, transparan, dan adil dalam setiap interaksi dan transaksi dagangnya.

Consumer Protection (Fair Trading) Act (CPFTA) di Singapura menyediakan kerangka perlindungan hukum yang memungkinkan korban penipuan digital (*scam*) untuk menempuh jalur perdata guna menuntut ganti rugi atas kerugian yang dialami, sekaligus berfungsi sebagai landasan peraturan yang menetapkan standar praktik perdagangan yang adil di negara tersebut (Singapore Statutes Online, 2025). Walaupun CPFTA tidak secara langsung menyebutkan pembentukan “anti scam centre,” keberadaan Singapore Anti Scam Centre (SASC) yang berada di bawah naungan Singapore Police Force memainkan peran penting sebagai badan eksekutif yang menjalankan pengawasan dan penegakan hukum terhadap pelanggaran yang relevan dengan ketentuan CPFTA, terutama dalam konteks penipuan daring. SASC secara aktif mengoperasionalkan ketentuan hukum dalam CPFTA untuk mengambil tindakan terhadap pelaku *scam*, termasuk bekerja sama dengan lembaga keuangan dan perusahaan

telekomunikasi dalam memblokir transaksi serta akun-akun yang mencurigakan. Sinergi ini menjadikan perlindungan konsumen di Singapura tidak hanya bersifat normatif, tetapi juga aplikatif dan efektif di lapangan.

Di samping itu, Singapura menerapkan Electronic Transactions Act 2010 (ETA) sebagai payung hukum dalam penyelenggaraan transaksi elektronik. Undang-undang ini memberikan kepastian hukum terhadap keabsahan kontrak digital dan tanda tangan elektronik, serta menjamin keamanan dan integritas proses transaksi secara daring. ETA berperan penting dalam menciptakan ekosistem digital yang terpercaya dan terlindungi bagi konsumen maupun pelaku usaha. *Part 2 Electronic Records Signatures And Contracts, Use of automated message systems for contract formation, 15. A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, is not to be denied validity or enforceability solely on the ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.*

Pasal dalam Electronic Transactions Act (ETA) menyatakan bahwa setiap pesan elektronik yang diterima oleh pihak penerima dianggap sebagai pesan yang sah dari pihak pengirim, kecuali terdapat bukti yang menunjukkan sebaliknya. Artinya, begitu pesan elektronik tersebut memasuki sistem informasi milik penerima, pesan tersebut memperoleh legitimasi hukum dan dapat dijadikan alat bukti yang sah dalam transaksi digital, termasuk dalam perkara penipuan online. Ketentuan ini memberikan landasan hukum yang kokoh bagi validitas komunikasi elektronik, sehingga memperkuat posisi korban dalam pembuktian tindakan penipuan digital atau transaksi elektronik lainnya di hadapan hukum.

Lebih lanjut, ETA juga menetapkan batasan tanggung jawab bagi penyedia layanan jaringan (network service providers), di mana mereka tidak bertanggung jawab atas konten yang berasal dari pihak ketiga yang hanya mereka salurkan. Namun demikian, penyedia layanan tetap diwajibkan untuk mematuhi ketentuan hukum dan regulasi yang berlaku. Aturan ini mendukung langkah-langkah operasional Singapore Anti Scam Centre (SASC), yang dapat menjalin kolaborasi erat dengan sektor telekomunikasi dan keuangan dalam mendeteksi, memutus akses, serta mengintervensi aktivitas mencurigakan secara cepat dan efisien. Dengan fondasi hukum dari ETA, SASC memiliki kewenangan yang jelas dalam melakukan penegakan hukum terhadap transaksi digital yang mengandung unsur penipuan, sehingga turut memperkuat sistem perlindungan konsumen dan keamanan dunia maya di Singapura.

Kepolisian Singapura (Singapore Police Force/SPF) berperan sebagai institusi utama dalam penegakan hukum dan pencegahan tindak kriminal di seluruh wilayah negara Singapura. Salah satu inisiatif strategisnya adalah pembentukan *Anti-Scam Centre* (ASC), yang dilandasi oleh *Electronic Transactions Act 2010*—sebuah regulasi yang menetapkan standar keamanan serta pedoman penggunaan sistem transaksi elektronik secara legal dan aman. Selain itu, ASC juga beroperasi berdasarkan *Shared Responsibility Framework* (SRF), sebuah kebijakan nasional yang digagas oleh *Monetary Authority of Singapore* (MAS) bersama *Infocomm Media Development Authority* (IMDA), yang menegaskan pembagian tanggung jawab antara sektor perbankan dan penyedia layanan telekomunikasi dalam menangkal dan menangani kejahatan siber, khususnya penipuan digital (Derry, 2025). Kerangka ini memperkuat mandat ASC untuk melakukan respons cepat terhadap aktivitas keuangan yang mencurigakan, dengan landasan hukum yang jelas dan sistem koordinasi lintas sektor yang efisien. ASC tidak bekerja secara terpisah, melainkan merupakan bagian dari jaringan kolaboratif yang melibatkan berbagai lembaga seperti *Cyber Security Agency of Singapore* (CSA) dalam hal perlindungan infrastruktur digital nasional, serta *Consumers Association of Singapore* (CASE) yang fokus pada perlindungan hak-hak konsumen. Seluruh mekanisme ini berada di bawah koordinasi *Inter-Ministry Committee on Scams* (IMCS), menjadikan upaya pemberantasan penipuan

online di Singapura sebagai pendekatan nasional yang terintegrasi dari sisi hukum, teknologi, dan advokasi publik (Singapore, 2025).

Salah satu strategi utama yang dijalankan oleh Anti-Scam Centre (ASC) adalah menjalin kolaborasi erat dengan tujuh divisi kepolisian Singapura untuk melaksanakan operasi gabungan secara berkala setiap dua minggu. Di samping itu, ASC juga berfokus pada pengembangan kemitraan strategis dengan institusi perbankan serta pelibatan pemangku kepentingan lintas sektor guna memperkuat respons nasional terhadap berbagai modus penipuan. Sebagai bagian dari pendekatan terintegrasi tersebut, ASC meluncurkan *Project FRONTIER* (Funds Recovery Operations and Networks Team, Inspiring Effective Resolutions) pada Mei 2020, yang bertujuan mempercepat pemulihan dana korban penipuan melalui kerja sama langsung dengan bank dan institusi keuangan lainnya. Hingga 1 Agustus 2021, cakupan kemitraan ASC telah meningkat secara signifikan, mencakup 54 mitra yang terdiri dari 14 bank, 15 perusahaan teknologi finansial (fintech), 13 penyedia layanan pembayaran berbasis kartu, 4 operator telekomunikasi domestik, 5 platform e-commerce besar, serta asosiasi perbankan Singapura. Tak hanya itu, jaringan kerja sama ASC juga melibatkan mitra internasional seperti Hong Kong Police Anti-Deception Coordination Centre dan INTERPOL. Kemitraan luas ini memberikan dampak konkret, termasuk dalam pemrosesan sekitar 11.000 laporan penipuan dan pembekuan lebih dari 9.000 rekening bank sepanjang tahun 2020. Menurut data dari National Crime Prevention Council (NCPC), kerugian akibat penipuan lowongan kerja mencapai lebih dari 6,5 juta dolar Singapura hanya dalam enam bulan pertama tahun 2021. Sebagai respons, ASC meluncurkan *Project COMBAT* (Centralised Operational Messaging Bot, Addressing Threats) pada 17 Juli 2021, yang dikerjakan secara kolaboratif bersama unit intelijen, divisi kepolisian wilayah, serta unit internal penanggulangan penipuan. Dalam upayanya untuk terus beradaptasi terhadap dinamika kejahatan digital, ASC juga mengandalkan teknologi terkini dan memperluas jangkauan kemitraan (Dass, 2021). Beberapa inovasi teknologi unggulan yang telah diimplementasikan termasuk aplikasi *ScamShield*, yang hingga Agustus 2024 telah diunduh oleh lebih dari 1,19 juta pengguna, serta *SMS Sender ID Registry (SSIR)* yang terbukti efektif menurunkan angka penipuan melalui SMS hingga 70% (Monetary Authority of Singapore, 2024).

Tingkat efektivitas perlindungan hukum terhadap kejahatan digital di Singapura tergolong tinggi, berkat keberadaan regulasi yang responsif dan adaptif terhadap perkembangan teknologi, seperti *Computer Misuse Act* yang telah mengalami sejumlah amandemen serta *Cybersecurity Act 2018* yang menjadi payung hukum penting dalam menjaga keamanan dunia maya. Keunggulan Singapura juga terletak pada koordinasi lintas sektor yang terstruktur melalui *Inter-Ministry Committee on Scams (IMCS)*, serta kesiapan infrastruktur keamanan siber yang memungkinkan tindakan preventif dan responsif secara cepat dan terintegrasi. Sebaliknya, Indonesia dihadapkan pada tantangan yang menuntut reformasi menyeluruh, termasuk pembaruan kerangka hukum yang relevan dengan dinamika kejahatan digital, penguatan sinergi antarlembaga penegak hukum, serta peningkatan kapasitas aparat dalam mendeteksi dan menangani kasus-kasus scam secara profesional. Selain itu, pengembangan literasi digital di kalangan masyarakat menjadi krusial untuk menciptakan ekosistem digital yang aman, sekaligus memberdayakan individu agar lebih waspada dan terlindungi dari berbagai bentuk penipuan daring. Upaya-upaya tersebut perlu diintegrasikan dalam kebijakan nasional agar perlindungan hukum terhadap korban scam digital dapat berjalan secara efektif, responsif, dan berkelanjutan.

2. Perbandingan Mekanisme Penanganan Indonesia Anti Scam Centre (IASC) dan Singapore Anti Scam Centre (SASC)

Singapura mengimplementasikan pendekatan perlindungan konsumen yang bersifat berlapis dan canggih, dengan memanfaatkan kecerdasan digital, analisis perilaku pengguna, serta evaluasi risiko aliran dana untuk mendeteksi dan mencegah penipuan sejak dini.

Teknologi mutakhir seperti *Artificial Intelligence* (AI) memainkan peran sentral, termasuk sistem SATIS (Suspicious Activity Transaction Identification System) dan teknologi pengenalan wajah yang digunakan untuk mengidentifikasi pola-pola mencurigakan serta modus operandi yang kerap digunakan oleh pelaku kejahatan digital. Di sisi regulasi, Singapura memperkuat posisi konsumen melalui penerapan *Shared Responsibility Framework* (SRF), yang secara tegas menetapkan kewajiban bank dan operator telekomunikasi dalam menangani kasus phishing. Dalam kerangka ini, institusi yang lalai menjalankan tanggung jawabnya diwajibkan untuk memberikan kompensasi atas kerugian yang timbul akibat transaksi ilegal, sehingga menambahkan lapisan perlindungan hukum dan operasional yang konkret bagi masyarakat (Vienna Verzo, 2025).

Sementara itu, di Indonesia, mekanisme penanggulangan penipuan digital tengah dikembangkan melalui kerja sama antara Otoritas Jasa Keuangan (OJK) dan Satgas PASTI, dengan mendorong seluruh perbankan nasional untuk bergabung dalam sistem pendeteksian rekening ilegal yang digunakan oleh pelaku scam. Model koordinasi ini juga melibatkan pelaku industri e-commerce dan penyedia sistem pembayaran dalam upaya kolektif mencegah penipuan daring (Rachel Farahdiba, 2025). Sebagai langkah preventif, Indonesia Anti Scam Centre (IASC) tengah merancang sistem deteksi dini guna mengidentifikasi rekening mule serta mencegah aktivitas mencurigakan sebelum menimbulkan kerugian besar. Sistem ini digagas sebagai versi awal dari teknologi *anti-scam shield* yang telah diadopsi secara luas di Singapura, namun implementasinya di Indonesia masih dalam tahap pengembangan. Selain pendekatan reaktif seperti pemblokiran rekening, IASC juga berkomitmen pada upaya penegakan hukum yang memberikan efek jera serta kampanye edukasi publik secara berkelanjutan. Meskipun demikian, sistem perlindungan Indonesia saat ini belum mencapai tingkat otomatisasi dan efisiensi seperti yang diterapkan di Singapura, khususnya dalam hal deteksi cepat dan notifikasi langsung kepada calon korban.

Tabel 1. Perbandingan Mekanisme Penanganan Antara SASC dan IASC

Aspek	SASC	IASC
Fokus Utama	Pencegahan aktif dan deteksi dengan teknologi otomatis	Deteksi dan pemblokiran rekening, penindakan hukum
Teknologi	RPA, AI, analisis perilaku, aplikasi scamshield	Sistem koordinasi antar bank dan lembaga pengembangan deteksi dini
Respon Waktu	Pembekuan rekening dalam 1 hari, notifikasi SMS cepat	Pemblokiran rekening setelah laporan, proses verifikasi lebih lama
Regulasi dan Akuntabilitas	Shared Responsibility Framework mewajibkan bank bertanggung jawab	Wajib bank bergabung dalam satgas, belum ada kerangka tanggung jawab bank seketat Singapura
Pemulihan Dana	Terbatas, fokus pada pencegahan; korban harus ajukan gugatan	Berupaya mengamankan dan mengembalikan dana korban
Kolaborasi	Kepolisian, bank, telekomunikasi, edukasi masyarakat	OJK, Satgas PASTI, bank, e-commerce, penegak hukum

“Diolah dari berbagai sumber, 2025”

Membandingkan efektivitas mekanisme perlindungan konsumen terhadap scam digital antara Indonesia (dengan fokus pada IASC OJK) dan Singapura memerlukan peninjauan terhadap berbagai aspek, mulai dari struktur kelembagaan hingga hasil nyata di lapangan:

1) Perbandingan Struktur Kelembagaan dan Koordinasi

Dalam struktur kelembagaan dan koordinasi, Indonesia menangani scam, khususnya yang terkait sektor keuangan, melalui Satgas PASTI dengan OJK sebagai ketua, yang merupakan forum koordinasi antar-kementerian/lembaga untuk pemberantasan aktivitas keuangan ilegal, sementara Indonesia Anti-Scam Centre (IASC) dibentuk di bawah OJK sebagai pusat operasional laporan scam keuangan. Singapura, di sisi lain, menerapkan model koordinasi multi-agensi yang lebih terdistribusi melalui *Inter-Ministry Committee on Scams* (IMCS) sebagai payung strategis, dengan peran spesifik untuk MAS (sektor keuangan), SPF melalui ASCom (penegakan hukum), IMDA (telekomunikasi dan informasi), dan CSA (keamanan siber) (Monetary Authority of Singapore, 2024). Koordinasi di Singapura tampak lebih matang dan terstruktur dengan pembagian peran yang jelas, memungkinkan respons komprehensif, sedangkan di Indonesia, kepemimpinan OJK dan fokus pada aktivitas keuangan ilegal memiliki permasalahan koordinasi scam lintas sektoral, terutama karena OJK tidak memiliki yurisdiksi penindakan pidana, sehingga bergantung pada Kepolisian dan Kejaksaan, berbeda dengan ASCom Singapura yang merupakan bagian integral SPF.

2) Perbandingan Regulasi dan Penegakan Hukum

Dari sisi regulasi dan penegakan hukum, kerangka regulasi utama Indonesia seperti UU ITE cenderung lebih represif, menekankan sanksi pidana pasca-pelanggaran, yang dinilai reaktif dan sulit beradaptasi dengan modus kejahatan siber yang cepat berubah (Dzuhriyan, 2024). Sebaliknya, Singapura lebih menekankan pencegahan, mitigasi risiko, dan pembagian tanggung jawab melalui *Cybersecurity Act*, *Computer Misuse Act*, serta *Shared Responsibility Framework* (SRF) yang mengalihkan sebagian tanggung jawab kepada institusi keuangan dan telekomunikasi untuk mencegah phishing dan memberikan kompensasi jika lalai (Force, 2024). Hak ini menunjukkan perbedaan filosofi mendasar dimana Singapura bergerak ke pencegahan proaktif dan akuntabilitas institusional, sementara Indonesia, meski berupaya mencegah dan mengedukasi, masih menekankan penindakan pasca-kejadian.

3) Perbandingan Inisiatif Pencegahan dan Penindakan

Terkait inisiatif pencegahan dan penindakan, Satgas PASTI di Indonesia aktif memblokir ribuan entitas investasi dan pinjaman online ilegal (Kholid Rafsanjani, 2025), sementara IMDA Singapura memblokir jutaan SMS, panggilan scam, dan ribuan situs berbahaya. Dalam pemulihan aset korban, ASCom Singapura berhasil memulihkan lebih dari S\$182 juta pada tahun 2024 (Force, 2024), sedangkan data pemulihan aset IASC Indonesia masih terbatas, dengan Rp129,1 miliar dana diblokir dari total kerugian Rp1,2 triliun yang dilaporkan hingga Maret 2025 (Kholid Rafsanjani, 2025). Kedua negara menyadari pentingnya edukasi publik, namun kondisi Indonesia saat ini menghadapi kendala karena rendahnya literasi digital yang dimiliki oleh masyarakatnya. Singapura telah mengimplementasikan solusi teknologi seperti aplikasi ScamShield dan sistem analisis AI SATIS, sementara Indonesia melalui IASC berupaya meningkatkan pemanfaatan teknologi dan mengusulkan National Hotline terintegrasi. Tingkat pemblokiran entitas/konten ilegal tinggi di kedua negara, namun sifat dinamis scam tetap menjadikan hal tersebut sulit di lakukan. Singapura mencatat pertumbuhan kasus scam +10,6% (2023-2024), dan di Indonesia, laporan konsumen rugi akibat scam meningkat dari 19% (2023) menjadi 23% (2024). IMDA Singapura memblokir 117 juta panggilan & 50 juta SMS scam pada tahun 2024, dan SPF memblokir lebih dari 44.900 situs web terkait scam pada tahun yang sama (Tech for Good Institute, 2025).

4) Keunggulan dan Kekurangan

Dari penjelasan di atas maka dapat disimpulkan bahwa, keunggulan Indonesia adalah komitmen Satgas PASTI dalam pemblokiran entitas keuangan ilegal dan pembentukan IASC sebagai langkah positif sentralisasi pelaporan sektor keuangan, didukung UU P2SK. Kelemahannya meliputi fragmentasi kewenangan penegakan pidana, literasi digital rendah, kapasitas penegakan hukum siber yang perlu ditingkatkan, mekanisme pemulihan aset belum

optimal, dan sifat regulasi yang reaktif. Singapura memiliki keunggulan sistem koordinasi multi-agensi yang kuat (IMCS, MAS, SPF-ASCom, IMDA, CSA), implementasi SRF yang progresif, pemanfaatan teknologi canggih (ScamShield, SATIS), penegakan hukum tegas, dan pemulihan aset sistematis. Namun, tantangannya adalah total kerugian akibat scam yang terus meningkat pada tahun 2024, menunjukkan adaptabilitas pelaku dan bahwa perjuangan melawan scam adalah upaya berkelanjutan, serta miskonsepsi konsumen yang masih ada.

Perbedaan fundamental terletak pada tingkat kematangan sistem perlindungan konsumen digital dan filosofi pendekatan: Singapura telah bergerak ke arah pembagian tanggung jawab dan pencegahan proaktif berbasis teknologi, sementara Indonesia masih dalam tahap penguatan kapasitas dasar penegakan hukum, sentralisasi respons di sektor keuangan, dan peningkatan literasi digital. Indonesia dapat belajar dari model koordinasi, SRF, dan teknologi Singapura, namun setiap solusi perlu diadaptasi dengan cermat sesuai konteks sumber daya, skala geografis, tingkat literasi digital, dan tantangan domestik. Meskipun Satgas PASTI berhasil memblokir ribuan entitas ilegal, peningkatan kerugian di Singapura, meskipun dengan sistem canggih, juga memberi pelajaran bahwa tidak ada solusi tunggal, dan perang melawan scam adalah maraton, bukan sprint.

KESIMPULAN

Analisis terhadap undang-undang dan peraturan yang berlaku menunjukkan bahwa efektivitas perlindungan hukum terhadap konsumen korban scam digital di Indonesia masih terhambat oleh fragmentasi regulasi dan kurangnya sinkronisasi antar lembaga. Meskipun Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen dan Undang-Undang Nomor 1 Tahun 2024 tentang Informasi dan Transaksi Elektronik memberikan kerangka hukum yang penting, implementasinya masih lemah, terutama karena Otoritas Jasa Keuangan (OJK) tidak memiliki yurisdiksi penyelidikan tindak pidana. Sebaliknya, Singapura berhasil menerapkan regulasi yang lebih adaptif melalui Consumer Protection (Fair Trading) Act dan inisiatif teknologi yang mendukung pencegahan scam, dengan Singapore Anti Scam Centre (SASC) yang beroperasi secara terkoordinasi dan mampu memulihkan dana korban secara signifikan. Oleh karena itu, Indonesia perlu memperkuat kerjasama antar lembaga dan memanfaatkan teknologi untuk meningkatkan efektivitas perlindungan konsumen dari scam digital.

Perbandingan mekanisme penanganan antara Indonesia Anti Scam Centre (IASC) dan Singapore Anti Scam Centre (SASC) menunjukkan perbedaan signifikan dalam efektivitas dan pendekatan yang diambil oleh kedua negara. SASC di Singapura beroperasi dengan sistem yang terintegrasi dan terkoordinasi, memanfaatkan teknologi canggih seperti Robotic Process Automation (RPA) dan Artificial Intelligence (AI) untuk mendeteksi dan mencegah scam secara proaktif, serta memiliki kerangka regulasi yang jelas melalui Shared Responsibility Framework (SRF). Sebaliknya, IASC di Indonesia masih menghadapi tantangan dalam hal koordinasi antar lembaga dan waktu respons yang lambat, serta kurangnya yurisdiksi OJK dalam penyelidikan tindak pidana. Hal ini menunjukkan bahwa Indonesia perlu mengadopsi praktik terbaik dari Singapura, termasuk peningkatan kolaborasi antar lembaga dan pemanfaatan teknologi, untuk memperkuat mekanisme penanganan scam dan melindungi konsumen secara lebih efektif.

REFERENSI

- Asriansyah, M. F. (2023). Bahaya Kejahatan Scam. Diambil dari DJKN Kemenkeu: <https://www.djkn.kemenkeu.go.id/kanwil-sumut/baca-artikel/16202/Bahaya-Kejahatan-Scam.html>
- Dass, D. (2021). The Anti-Scam Centre : A Collaborative Approach Against Scams. Diambil dari Singapore Police Force: <https://www.police.gov.sg/Media->

- Room/Police-Life/2021/11/The-Anti-Scam-Centre---A-Collaborative-Approach-Against-Scams
- Derry, L. (2025). Singapore's Scam Surge Strategy: What Enterprises Must Do Now Under the New Shared Responsibility Framework. Diambil dari Memcyco: <https://www.memcyco.com/singapore-shared-responsibility-framework/>
- Domnic Dass. (2021). Dedikasi Untuk Mengganggu Dan Mencegah Operasi Penipuan. Diambil dari Singapore Police Force: [https://www.police.gov.sg/Media-Room/Police-Life/2021/11/The-Anti-Scam-Centre---A-Collaborative-Approach-Against-Scams#:~:text=The Anti-Scam Centre \(ASC\) was set up,Police's nerve centre for investigating scam-related crimes](https://www.police.gov.sg/Media-Room/Police-Life/2021/11/The-Anti-Scam-Centre---A-Collaborative-Approach-Against-Scams#:~:text=The Anti-Scam Centre (ASC) was set up,Police's nerve centre for investigating scam-related crimes)
- Dzuhriyan, A. R. (2024). Consumer Legal Protection in Online Transactions: Challenges and Opportunities in Indonesia's Digital Economy. *Justice Voice*, Volume 3(1).
- Force, S. P. (2024). *Annual Scams and Cybercrime Brief 2024*. Singapore Police Force.
- Hudiyanto. (2024). Tingkat Perlindungan Konsumen, Satgas PASTI Lakukan Soft Launching Indonesia Anti-Sscam Centre. Diambil dari Satgas PASTI Pemberantas Aktivitas Keuangan Ilegal: [https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-Lakukan-Soft-Launching-IASC/SP Satgas Pasti Soft Launching IASC.pdf](https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Documents/Pages/Tingkatkan-Pelindungan-Konsumen-Satgas-Pasti-Lakukan-Soft-Launching-IASC/SP%20Satgas%20Pasti%20Soft%20Launching%20IASC.pdf)
- Hudiyanto. (2025). Waspada Penipuan Website Mengatasnamakan Indonesia Anti-Scam Centre (IASC). Diambil dari Satgas PASTI Pemberantas Aktivitas Keuangan Ilegal: <https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/Waspada-Penipuan-Website-Mengatasnamakan-Indonesia-Anti-Scam-Centre-IASC.aspx>
- Irfan Ridha. (2024). Aspek Hukum Perlindungan Konsumen Digital. *Civilia : Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan*, Volume 3(2).
- Jennifer Clarence. (2024). Perlindungan Hukum Bagi Konsumen Yang Menjadi Korban Perusahaan Investasi Ilegal Berbasis Multi Level Marketing. *Jurnal USM Law Rivew*, Volume 7(3).
- Kholid Rafsanjani. (2025). Satgas PASTI urges extra vigilance against fraud ahead of Eid. Diambil dari IDNFinancials: <https://www.idnfinancials.com/news/53358/satgas-pasti-urges-extra-vigilance-against-fraud-ahead-of-eid>
- Luh Widiya Saraswati. (2022). Studi Komparatif Perlindungan Konsumen Di Indonesia Dan Singapura Terhadap Kenaikan Harga Yang Tidak Wajar. *Justitia : Jurnal Ilmu Hukum Dan Humaniora*, Volume 8(1), hlm. 253.
- Mandra. (2024). Kemenkominfo Terima Ratusan Ribuan Aduan Penipuan Online. Diambil dari Radio Republik Indonesia: <https://rri.co.id/nasional/951055/kemenkominfo-terima-ratusan-ribu-aduan-penipuan-online>
- Monetary Authority of Singapore. (2024). Combatting Scams. Diambil dari Monetary Authority of Singapore: <https://www.mas.gov.sg/regulation/combating-scams>
- Natalia Lorien and Tantimin. (2022). Investasi Bodong Dengan Sistem Skema Ponzi : Kajian Hukum Pidana. *Jurnal Komunitas Yustisia*, Volume 5(1).
- OJK. (2022). Profil Satgas. Diambil dari Otoritas Jasa Keuangan: <https://ojk.go.id/waspada-investasi/id/tentang/Pages/Profil-Satgas.aspx>
- Rachel Farahdiba. (2025). OJK Wajibkan Bank-Bank Gabung Dalam Satgas Anti-Scam Centre, Apa Alasannya. Ddiambil dari Tempo.Co: <https://www.tempo.co/ekonomi/ojk-wajibkan-bank-bank-gabung-dalam-satgas-anti-scam-center-apa-alasannya--31302>
- Riana Pratiwi. (2024). Panduan Anti-Penipuan : Strategi Konsumen Untuk Menghindari Penipuan Dan Praktik Bisnis Yang Curang. Surabaya. CV. Garuda Mas Sejahtera.
- Singapore, M. A. of. (2025). Joint Advisory on Scams Involving Digital Manipulation. Diambil dari Monetary Authority of Singapore: <https://www.mas.gov.sg/news/media->

- releases/2025/joint-pnr-by-spf-mas-and-csa
- Singapore Statutes Online. (2025). Consumer Protection (Fair Trading) Act 2003. Diambil dari Singapore Statutes Online.
- Soerjono Soekanto and Sri Mamudji. (2001). *Penelitian Hukum Normatif, Suatu Tinjauan Singkat*. Rajawali Pers.
- Syadid Jiddan Alharun. (2025). Perbandingan Hukum Tindak Pidana Siber Antara Indonesia Dengan Singapura. *Jurnal Hukum Dan Kewarganegaraan*, Volume 10, 11.
- Tech for Good Institute. (2025). Building Resilience against Scams and Fraud: Spotlight on Indonesia. Diambil dari Tech for Good Institute <https://techforgoodinstitute.org/blog/event-highlights/building-resilience-against-scams-and-fraud-spotlight-on-indonesia/>
- United Nation Office on Drugs and Crime. (2024). Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape. Diambil dari United Nation Office on Drugs and Crime: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf
- Vienna Verzo. (2025). Singapura membutuhkan strategi berlapis untuk melawan penipuan. Diambil dari Banking&Finance: <https://asianbankingandfinance.net/indonesian/exclusive/singapura-membutuhkan-strategi-berlapis-untuk-melawan-penipuan>
- Wallinda, M. F. (2025). Korban Penipuan di Singapura Meningkat Tiap Tahun. Diambil dari Radio Republik Indonesia: <https://www.rri.co.id/internasional/1354277/korban-penipuan-di-singapura-meningkat-tiap-tahun>
- Wibowo, D. E. (2024). The Comparison of Indonesian and American Customer Protection Laws: What and How?. *SASI*, 30(4).
- Wicaksono, S. R. (2020). *Fraud dan Scam di Era Digital : Konsep dan Perkembangan*. CV. Seribu Bintang.
- Yap, A. (2024). *Anti-Scam Centre of the Singapore Police Force: Fighting Scams is a Community Effort*. Diambil dari Singapore Police Force: <https://www.gasa.org/post/anti-scam-centre-of-the-singapore-police-force-fighting-scams-is-a-community-effort>
- Yuyut Prayuti. (2024). Dinamika Perlindungan Hukum Konsumen Di Era Digital: Analisis Hukum Terhadap Praktik E-Commerce dan Perlindungan Data Konsumen Di Indonesia. *Jurnal Interpretasi Hukum*, Volume 5 Nomor 1, 907.
- Yuyut Prayuti. (2024). *Perlindungan Konsumen Di Era Digital*. Literasi Nusantara Abadi Grup.