

Digitimes #40
Maret 2023

LANSKAP KEAMANAN SIBER SEKTOR LAYANAN PERBANKAN DAN FINANSIAL DI INDONESIA 2022



CfDS
CENTER FOR DIGITAL SOCIETY

Room BC 201-203
Faculty of Social and Political Sciences
Universitas Gadjah Mada
Jalan Socio Yustisia 1, Bulaksumur, Yogyakarta
(0274) 563362, Ext. 116 | cfds.fisipol@ugm.ac.id



Peneliti dan Kontributor

Penulis

M. Perdana Karim
Archandra Viryasatya Sugama

Penyunting

Annisa Pratita Kirana Mantovani

Desainer dan Penata Layout

Hanny Handayani

Daftar Isi

2	Pendahuluan
5	Keamanan Siber Dalam Layanan Perbankan Dan Finansial di Indonesia
9	Keamanan Siber Dalam Layanan Perbankan Dan Finansial Di Indonesia Oleh Pemerintah Beserta Tantangannya
12	Keamanan Siber Dalam Layanan Perbankan dan Finansial di Indonesia
14	Kesimpulan
15	Referensi





PENDAHULUAN

Teknologi dan arus informasi mengalami perkembangan yang pesat dalam satu dekade ini. Pandemi COVID-19 membuat perkembangan tersebut menjadi semakin cepat, sebagaimana manusia harus terpaksa beradaptasi dengan keadaan dan menggantikan kegiatan-kegiatan yang dapat dilakukan secara luring menjadi secara daring. Akibat hal tersebut, berbagai sektor industri mulai mengalami transformasi digital dengan perkembangan pesat, sebagaimana mereka harus mengakomodasi jumlah pengguna yang meningkat di masa pandemi. Namun, tidak semua sektor industri mengalami perkembangan yang sama selama pandemi, sebagaimana sektor industri yang lebih kuat menghadapi pandemi cenderung merupakan sektor industri yang memiliki kehadiran kuat dalam ranah perkembangan teknologi dan informasi. Salah satu sektor yang kuat menghadapi pandemi dan terus berkembang adalah sektor perbankan dan layanan finansial.

Istilah layanan finansial di sini mengacu pada layanan yang diberikan oleh industri yang bergerak dalam sektor-sektor finansial dan perbankan. Menurut Investopedia, layanan-layanannya meliputi perbankan, hipotek, kartu kredit, layanan pembayaran, persiapan dan perencanaan pajak, akuntansi, dan investasi. Pendapat lain mengatakan bahwa asuransi termasuk dalam layanan finansial.¹ Dari sini dapat diartikan bahwa layanan finansial merupakan layanan yang berfokus pada manajemen dan transaksi keuangan yang dilakukan oleh industri terkait. Pada Digitimes kali ini, bahasan layanan finansial akan difokuskan pada tiga kasus utama yang menjadi pusat perhatian dalam *Focus Group Discussion* yang diadakan oleh *Center for Digital Society (CfDS)* UGM bersama Google Cloud Indonesia dengan menghadirkan pembicara serta peserta dari berbagai lembaga di sektor finansial dan perbankan. Tiga layanan utama tersebut yaitu, *e-payment*, *digital bank*, dan *peer-to-peer (P2P) lending* yang ada di Indonesia.

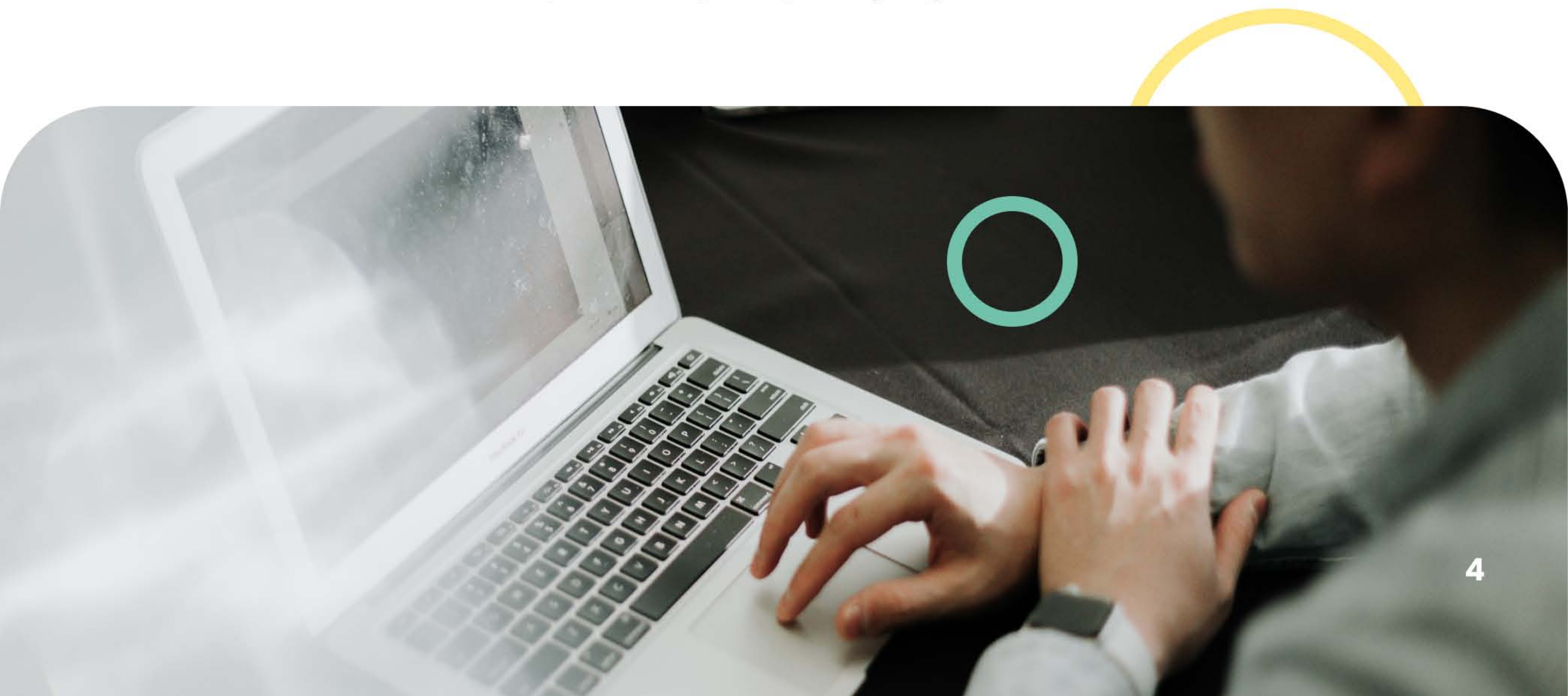
Meskipun COVID-19 membuat masyarakat pada umumnya terpaksa untuk mulai mengadopsi dan menggunakan alternatif-alternatif daring, pada kenyataannya, Indonesia merupakan salah satu negara dengan jumlah populasi masyarakat dewasa yang mayoritas belum terdaftar atau menggunakan fasilitas perbankan dan finansial. Dari 181 juta orang dewasa terdapat sebanyak 51% yang tidak menggunakan layanan perbankan dan finansial Indonesia.² Alasan atas adanya kesenjangan pengguna layanan perbankan dan finansial ini bervariasi, namun, pada dasarnya disebabkan oleh ketidakpercayaan dan ketakutan masyarakat terhadap industri layanan finansial, serta infrastruktur dan ketersediaan layanan finansial yang kurang memadai lanskap Indonesia yang luas.³ Guna mengecilkan kesenjangan *unbanked population* di Indonesia ini, penting untuk adanya kolaborasi antara pemerintah dan industri untuk mendorong minat dan kepercayaan masyarakat. Serta meningkatkan infrastruktur dan ketersediaan luas terhadap layanan perbankan dan finansial di Indonesia. Salah satu aspek penting dalam layanan perbankan dan finansial yang perlu ditingkatkan adalah aspek keamanan siber.

Keamanan siber merupakan salah satu aspek penting dalam menjaga kepercayaan nasabah terhadap layanan perbankan dan finansial. Sebagaimana sektor perbankan dan finansial merupakan sektor yang sangat rawan untuk mendapatkan serangan siber.⁴ Untuk menjaga keamanan siber dalam layanan perbankan dan keuangan di Indonesia, beberapa tindakan yang biasanya dilakukan adalah sebagai berikut⁵ :

- **Penerapan sistem keamanan siber yang kuat:** Lembaga keuangan biasanya menerapkan sistem keamanan siber yang kuat untuk melindungi data nasabah dan transaksi yang dilakukan. Sistem keamanan siber yang digunakan biasanya meliputi firewall, sistem deteksi serangan, dan sistem enkripsi data. Selain itu, penerapan standar keamanan seperti ISO 27001:2013 juga merupakan suatu keharusan yang membantu lembaga perbankan untuk melindungi aset teknologinya. Sebagian bank saat ini mulai menerapkan standar tersebut untuk semakin meningkatkan sistem keamanan siber mereka.
- **Penyediaan akses terbatas:** Lembaga keuangan biasanya memberikan akses terbatas ke sistem perbankan dan keuangan hanya kepada pegawai yang memiliki kewenangan yang sesuai. Hal ini bertujuan untuk mencegah terjadinya akses yang tidak sah ke sistem.

- **Pelatihan dan sosialisasi keamanan siber:** Lembaga keuangan biasanya melakukan pelatihan dan sosialisasi keamanan siber kepada pegawai dan nasabah agar mereka dapat menyadari pentingnya keamanan siber dan cara-cara untuk menjaganya.
- **Penyediaan layanan bantuan keamanan siber:** Lembaga keuangan biasanya menyediakan layanan bantuan keamanan siber bagi nasabah yang mengalami masalah keamanan siber, seperti lupa password atau terjadi serangan siber.
- **Kerjasama dengan pihak-pihak terkait:** Lembaga keuangan biasanya juga bekerjasama dengan pihak-pihak terkait, seperti lembaga pemerintah, badan keamanan siber nasional, dan perusahaan keamanan siber, untuk menjaga keamanan siber dalam layanan perbankan dan keuangan di Indonesia.

Namun, meskipun telah dilakukan berbagai tindakan untuk menjaga keamanan siber dalam layanan perbankan dan keuangan di Indonesia, masih ada kemungkinan terjadinya serangan siber atau kebocoran data. Di samping karena infrastruktur keamanan siber negara yang masih kurang matang (akan dibahas lebih lanjut lebih lanjut pada bagian-bagian selanjutnya), peningkatan jenis-jenis ancaman baru yang melibatkan sentuhan manusia seperti *social engineering* dan *phishing* juga berperan besar dalam terjadinya kebocoran data.⁶ Oleh karena itu, selain industri yang harus meningkatkan sistem keamanan sibernya, nasabah juga harus memahami pentingnya keamanan siber dan melakukan tindakan pencegahan yang tepat, seperti menggunakan password yang kuat dan tidak memberikan informasi pribadi kepada pihak yang tidak dikenal.



KEAMANAN SIBER DALAM LAYANAN PERBANKAN DAN FINANSIAL DI INDONESIA

A Pemanfaatan dalam Upaya Peningkatan Kesejahteraan Masyarakat

Saat ini, Indonesia sedang mengalami lonjakan yang besar dalam transformasi digital di sektor perbankan dan finansial. Terjadi peningkatan dalam transaksi digital yang diakibatkan oleh semakin banyaknya orang yang menggunakan sistem perbankan digital dan *e-wallet* dalam kurun waktu 3 tahun ke belakang.⁷ Dengan 179 juta orang sudah menggunakan pembayaran digital, semakin banyak orang yang terkoneksi dengan internet dan menjadi subjek dalam ruang digital.⁸ Keamanan siber diperlukan untuk mengawal transformasi digital serta transaksi elektronik yang ada di dalamnya. Dr. Edit Prima, M.hum (Direktur Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata Badan Siber dan Sandi Negara RI) mengatakan bahwa di era pandemi terdapat lebih dari 1.2 miliar *anomaly traffic* yang dipersepsikan sebagai serangan siber kepada stakeholder di Indonesia.⁹ Pada tahun ini, hingga bulan September 2022 sendiri, sudah ditemukan lebih dari 1.1 juta anomali yang terjadi khusus di sektor keuangan saja. Mengingat semakin tingginya jumlah masyarakat yang terlibat dalam aktivitas elektronik, hal tersebut dapat membahayakan para nasabah yang bergantung pada sistem keamanan digital dari bank atau platform yang digunakannya.

Upaya peningkatan keamanan siber dianggap sebagai sebuah kunci dalam memastikan kesejahteraan masyarakat yang menggantungkan arus keuangannya pada teknologi digital. Sebagaimana pemerintah melalui Bank Indonesia dengan sistem pembayaran digitalnya yang dikenal dengan nama *Quick Response Code Indonesia Standard* (QRIS) menargetkan terwujudnya *Cashless Society*, jumlah transaksi digital ke depannya pun juga diprediksi akan semakin meningkat. Bilamana target untuk mengajak 65 juta pelaku Usaha Mikro, Kecil, dan Menengah (UMKM) menggunakan sistem pembayaran tanpa uang tunai tersebut terwujud, dapat dikatakan bahwa kesejahteraan mereka akan bergantung pada sistem keamanan digital dari platform yang akan mereka gunakan nantinya.



KEAMANAN SIBER DALAM LAYANAN PERBANKAN DAN FINANSIAL DI INDONESIA

A Pemanfaatan dalam Upaya Peningkatan Kesejahteraan Masyarakat

Saat ini, Indonesia sedang mengalami lonjakan yang besar dalam transformasi digital di sektor perbankan dan finansial. Terjadi peningkatan dalam transaksi digital yang diakibatkan oleh semakin banyaknya orang yang menggunakan sistem perbankan digital dan *e-wallet* dalam kurun waktu 3 tahun ke belakang.⁷ Dengan 179 juta orang sudah menggunakan pembayaran digital, semakin banyak orang yang terkoneksi dengan internet dan menjadi subjek dalam ruang digital.⁸ Keamanan siber diperlukan untuk mengawal transformasi digital serta transaksi elektronik yang ada di dalamnya. Dr. Edit Prima, M.hum (Direktur Keamanan Siber dan Sandi Keuangan, Perdagangan dan Pariwisata Badan Siber dan Sandi Negara RI) mengatakan bahwa di era pandemi terdapat lebih dari 1.2 miliar *anomaly traffic* yang dipersepsikan sebagai serangan siber kepada stakeholder di Indonesia.⁹ Pada tahun ini, hingga bulan September 2022 sendiri, sudah ditemukan lebih dari 1.1 juta anomali yang terjadi khusus di sektor keuangan saja. Mengingat semakin tingginya jumlah masyarakat yang terlibat dalam aktivitas elektronik, hal tersebut dapat membahayakan para nasabah yang bergantung pada sistem keamanan digital dari bank atau platform yang digunakannya.

Upaya peningkatan keamanan siber dianggap sebagai sebuah kunci dalam memastikan kesejahteraan masyarakat yang menggantungkan arus keuangannya pada teknologi digital. Sebagaimana pemerintah melalui Bank Indonesia dengan sistem pembayaran digitalnya yang dikenal dengan nama *Quick Response Code Indonesia Standard* (QRIS) menargetkan terwujudnya *Cashless Society*, jumlah transaksi digital ke depannya pun juga diprediksi akan semakin meningkat. Bilamana target untuk mengajak 65 juta pelaku Usaha Mikro, Kecil, dan Menengah (UMKM) menggunakan sistem pembayaran tanpa uang tunai tersebut terwujud, dapat dikatakan bahwa kesejahteraan mereka akan bergantung pada sistem keamanan digital dari platform yang akan mereka gunakan nantinya.

B**Posisi Indonesia dalam Penjaminan Keamanan Infrastruktur Digital Layanan Perbankan dan Finansial di Tataran Global**

Untuk menjamin keamanan siber, infrastruktur digital masih menjadi salah satu hal yang paling dibutuhkan. Kesiapan infrastruktur keamanan digital yang matang dapat mempermudah rangkaian proses menghadapi serangan siber yang dimulai dari antisipasi hingga penanganan ketika serangan tersebut sudah masuk ke suatu jaringan. Dari segi kewanaman sibernya, Indonesia menduduki peringkat 84 dari 161 negara di tahun 2022 berdasarkan *National Cybersecurity Index* yang mengukur kesiapan keamanan siber suatu negara dimulai dari aspek-aspek seperti pengembangan kebijakan, perlindungan data dan layanan digital, hingga penanganan kejahatan siber.

Di sisi lain, walaupun dalam lima tahun terakhir sudah terdapat peningkatan secara konsisten pada Indeks Pembangunan Teknologi Informasi dan Komunikasi (IP-TIK) atau *ICT Development Index*, Indonesia masih perlu mengejar ketertinggalannya setelah menempati posisi ke-68 dari 132 negara dalam hal pembangunan infrastruktur IP-TIK berdasarkan peringkat dalam *Global Innovation Index* (GII) 2022. Peringkat ini masih di bawah negara-negara ASEAN lainnya seperti Brunei Darussalam (61), Thailand (54), Malaysia (51), dan Singapura (11). East Ventures dalam laporannya mengenai *Digital Competitiveness Index* (2022) yang juga berfokus pada penggunaan ICT dalam meningkatkan perekonomian di daerah-daerah di Indonesia menunjukkan bahwa masih terdapat kesenjangan di antara wilayah-wilayah di Indonesia. Walaupun sudah cukup menurun, kesenjangan tingkat kompetitif masih cukup nampak antara provinsi-provinsi di Jawa-Bali dan lainnya.

Sebagai negara yang memegang peranan penting dalam perekonomian digital di wilayah ASEAN dengan total *Gross Merchandise Value* (GMV) sebesar US\$70 miliar, Indonesia berperan aktif dalam berkolaborasi dengan negara-negara lain untuk meningkatkan keamanan siber.¹⁰

Salah satu bentuk kerja sama Indonesia dengan negara-negara lain adalah pembentukan *Computer Emergency Response Team* (CERT) di ASEAN, Asia Pasifik, dan negara-negara OKI yang ditujukan untuk mengatasi serangan-serangan siber serta memperkuat pembangunan infrastruktur wilayah pada sektor-sektor seperti telekomunikasi, perbankan, dan finansial. Sebagai bagian dari tim tersebut, Indonesia turut berkontribusi dalam pertukaran pengetahuan serta peningkatan upaya respon terhadap serangan-serangan siber yang ditujukan pada negara-negara anggota wilayah tersebut.



C Identifikasi Tantangan Keamanan Siber dalam Layanan Finansial dan Perbankan di Indonesia

Infrastruktur siber layanan perbankan dan finansial di Indonesia saat ini menghadapi beberapa permasalahan yang harus diatasi agar layanan tersebut dapat berjalan dengan lancar. Menurut laporan *Asean Cyberthreat Assesment* yang diterbitkan oleh *Interpol*, Indonesia merupakan salah satu negara dengan tingkat serangan siber tertinggi di Asia Tenggara.¹¹ Tantangan keamanan siber dalam layanan finansial dan perbankan di Indonesia dapat kami identifikasi sebagai tiga tantangan: dari segi infrastruktur, regulasi dan sumber daya manusia.

Jika dilihat dari segi infrastruktur, sistem keamanan siber Indonesia masih tergolong rendah, sebagaimana Indonesia masih sering mengalami serangan siber kepada sektor-sektor industri vital dan dimana serangan tersebut berhasil.¹² Serangan siber yang sering terjadi di Indonesia yang dialami oleh bank dan sektor finansial antara lain *compromised attacker* dan *advanced persistent threat* (APT).¹³ *Compromised attacker* adalah serangan siber yang dilakukan dengan menggunakan komputer atau jaringan yang telah terinfeksi *malware*. Serangan ini dapat menyebar dengan cepat ke komputer atau jaringan lain yang terhubung dengan komputer atau jaringan yang terinfeksi, sehingga menyebabkan kerusakan yang lebih luas. Sedangkan *Advanced Persistent Threat* (APT) adalah serangan siber yang dilakukan dengan cara yang terencana dan terorganisir untuk menginfeksi sistem dan merusak data dengan tujuan tertentu. Serangan ini biasanya dilakukan oleh kelompok atau individu yang memiliki keahlian dan sumber daya yang cukup untuk melakukan serangan tersebut.

Dalam konteks regulasi, Indonesia telat dalam menghadapi isu-isu keamanan siber dan data pribadi. Sebagaimana pengesahan Undang-undang Pelindungan Data Pribadi hanya baru dilakukan pada Oktober 2022. Sedangkan konseptualisasi dan perumusan dari UU PDP ini sudah dilakukan sejak tahun 2019.¹⁴ Mengingat urgensi dari kebutuhan akan adanya suatu UU komprehensif yang mengatur mengenai keamanan siber dan pelindungan data pribadi, keterlambatan dalam pengesahan UU PDP menunjukkan bahwa keamanan siber dan pelindungan data pribadi tidak selalu merupakan fokus utama dari Pemerintah Indonesia. Meskipun Indonesia sudah memiliki beberapa regulasi yang mengatur mengenai keamanan siber dan pelindungan data pribadi, seperti UU ITE maupun Peraturan Presiden No 82/2022 tentang Pelindungan Infrastruktur Informasi Vital, regulasi-regulasi tersebut terpecah antara beberapa instansi pemerintah, tidak merupakan suatu hal yang konklusif dan menyeluruh.¹⁵¹⁶ Hal tersebut menjadikan lanskap keamanan siber dan pelindungan data pribadi di Indonesia seolah-olah terfragmentasi dan sporadis dalam sifatnya.

Selain tantangan dari segi infrastruktur dan regulasi, salah satu permasalahan yang kerap dihadapi adalah kurangnya talenta digital atau digital-skilled labour di Indonesia. Hingga saat ini, Indonesia tercatat memiliki kekurangan talenta digital sebesar 55% dibandingkan dengan kebutuhan pasar.¹⁷ Kurangnya talenta digital di Indonesia menyebabkan lembaga keuangan kesulitan dalam mencari talenta yang memiliki kemampuan digital yang baik untuk membantu menjaga keamanan siber layanan perbankan dan finansial di Indonesia serta mengembangkan layanan baru yang menggunakan teknologi informasi.

Tantangan dari segi keamanan siber serta kurangnya talenta digital dalam pasar ketenagakerjaan dapat terjadi karena kurangnya anggaran yang dikeluarkan dan digunakan guna peningkatan infrastruktur layanan siber di Indonesia. Sebagian besar lembaga keuangan di Indonesia hanya mengalokasikan sekitar 2% dari total anggaran teknologi informasi untuk keamanan siber.¹⁸ Anggaran yang rendah ini dapat menyebabkan lembaga keuangan kesulitan dalam membeli perangkat keamanan siber yang memadai, seperti firewall dan antivirus, serta kesulitan dalam memberikan pelatihan keamanan siber bagi pegawai.





KEAMANAN SIBER DALAM LAYANAN PERBANKAN DAN FINANSIAL DI INDONESIA OLEH PEMERINTAH BESERTA TANTANGANNYA

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

Peraturan ini dikeluarkan pada tahun 2020 dengan tujuan untuk mengatur dan mengendalikan kegiatan penyelenggaraan layanan keuangan berbasis teknologi informasi di Indonesia. Peraturan ini mengatur tentang pengaturan, pengawasan, dan pengendalian kegiatan penyelenggaraan layanan keuangan berbasis teknologi informasi yang dilakukan oleh Bank Indonesia, bank umum, bank perkreditan rakyat, bank syariah, dan lembaga keuangan lainnya yang memiliki izin untuk melakukan kegiatan usaha layanan keuangan berbasis teknologi informasi. Peraturan ini juga mengatur tentang prinsip-prinsip yang harus diikuti oleh penyelenggara layanan keuangan berbasis teknologi informasi, seperti prinsip kehati-hatian, prinsip kepastian hukum, prinsip transparansi, dan prinsip keadilan.

Selain itu, terdapat beberapa persyaratan yang harus dipenuhi oleh penyelenggara layanan keuangan berbasis teknologi informasi yang diatur dalam peraturan ini, seperti persyaratan teknis, persyaratan keuangan, dan persyaratan manajemen risiko. Sebagian manfaat yang dirasakan dari adanya Peraturan BI No 22/23/PBI/2020 ini dapat diuraikan sebagai berikut¹⁹ :



- **Meningkatkan kepercayaan nasabah:** Peraturan ini membantu meningkatkan kepercayaan nasabah terhadap layanan keuangan berbasis teknologi informasi yang ada di Indonesia, karena penyelenggara layanan keuangan berbasis teknologi informasi harus memenuhi persyaratan yang telah ditetapkan oleh BI.
- **Mengurangi risiko kegagalan sistem:** Peraturan ini juga membantu mengurangi risiko kegagalan sistem yang mungkin terjadi pada layanan keuangan berbasis teknologi informasi, karena penyelenggara layanan harus memenuhi persyaratan teknis yang telah ditetapkan oleh BI.
- **Mengurangi risiko penyalahgunaan data nasabah:** Peraturan ini juga membantu mengurangi risiko penyalahgunaan data nasabah oleh penyelenggara layanan keuangan berbasis teknologi informasi, karena penyelenggara layanan harus memenuhi persyaratan keamanan data yang telah ditetapkan oleh BI.
- **Meningkatkan efisiensi layanan keuangan:** Peraturan ini juga dapat meningkatkan efisiensi layanan keuangan yang disediakan oleh penyelenggara layanan keuangan berbasis teknologi informasi, karena penyelenggara layanan harus memenuhi persyaratan yang telah ditetapkan oleh BI.
- **Mendorong inovasi layanan keuangan:** Peraturan ini juga dapat mendorong inovasi layanan keuangan yang disediakan oleh penyelenggara layanan keuangan berbasis teknologi informasi, karena penyelenggara layanan harus selalu menyesuaikan layanan yang disediakanannya dengan perkembangan teknologi yang ada.



Meskipun demikian, peraturan ini juga mengalami beberapa tantangan, baik dari segi implementasi maupun sebagai upaya untuk mengajak masyarakat untuk merasa aman dan mau untuk menggunakan layanan keuangan berbasis teknologi yaitu:

- **Tingkat literasi digital masyarakat Indonesia yang masih rendah:** Salah satu tantangan terbesar yang kerap dialami oleh Indonesia dalam hal pengimplementasian kebijakan-kebijakan berbasis teknologi adalah tingkat literasi digital masyarakat Indonesia yang masih rendah. Meskipun Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dalam survei penelitian mereka menyebutkan bahwa tingkat penetrasi internet di Indonesia telah mencapai 77,02% pada tahun 2022, hal tersebut tidak merefleksikan tingkat literasi digital masyarakat Indonesia.²⁰²¹ Melainkan, hanya menunjukkan persentase masyarakat Indonesia yang kini sudah 'melek' digital, namun masih belum 'cakap' digital.
- **Kurangnya kepercayaan terhadap layanan keuangan berbasis teknologi informasi:** Beberapa orang mungkin masih kurang percaya terhadap keamanan dan kepercayaan layanan keuangan berbasis teknologi informasi, sehingga mungkin ragu untuk menggunakannya. Hal ini dapat dibuktikan dengan jumlah masyarakat Indonesia yang masih belum menggunakan menggunakan maupun terdaftar dalam sistem perbankan Indonesia. Laporan dari World Bank melaporkan bahwa jumlah masyarakat dewasa Indonesia yang masih belum bergabung dalam bank adalah sebanyak 51% dari 181 juta.²²

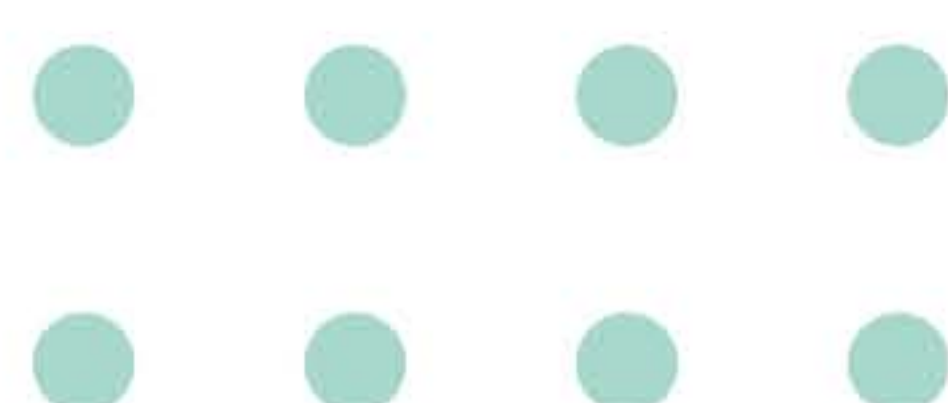




B Undang-Undang Pelindungan Data Pribadi

UU Pelindungan Data Pribadi (PDP) bersifat mengayomi dalam konteks pelindungan data pribadi masyarakat Indonesia senada dengan *General Data Protection Regulation* yang dimiliki oleh Uni Eropa. UU PDP bertujuan untuk melindungi hak-hak individu terkait dengan penggunaan, pengolahan, dan penyebaran data pribadi, seperti contohnya penjaminan terhadap hak individu untuk mengontrol penggunaan data pribadi mereka, serta penjaminan bahwa data pribadi tidak akan digunakan secara tidak sesuai atau tidak sah. UU PDP yang baru disahkan pada Oktober 2022 masih memiliki jalan yang panjang.

Pasalnya, selain mengingat usianya yang masih sangat baru di Indonesia sehingga perlu adanya penyesuaian dari berbagai sektor untuk mene-rapkannya, kekosongan lembaga yang independen juga membuat UU PDP masih mudah untuk ditumpangi kepentingan kelompok tertentu. Selain itu, perbedaan kesiapan sistem dari masing-masing lembaga yang juga berpeluang menghambat pengimplementasiannya di masing-masing lembaga. Misalnya saja, beberapa platform atau lembaga masih sangat bergantung pada data pribadi penggunanya untuk menjalankan model bisnis mereka.





UU PDP memberikan kewajiban bagi pengolah data pribadi untuk meminta persetujuan dari individu sebelum menggunakan atau memproses data pribadi mereka, serta memberikan hak kepada individu untuk mengakses, memperbaiki, atau menghapus data pribadi mereka yang disimpan oleh pengolah data. UU PDP juga menetapkan sanksi-sanksi bagi pengolah data yang melanggar ketentuan yang berlaku, seperti denda atau pidana penjara. Sanksi-sanksi ini bertujuan untuk memberikan efek jera bagi pengolah data yang tidak mematuhi ketentuan perlindungan data pribadi, sekaligus memberikan perlindungan bagi individu yang hak-haknya telah dilanggar.

Dari sini, kembali lagi salah satu tantangan terbesar yang akan dihadapi adalah mengenai kepatuhan bagi para penyelenggara sistem elektronik terhadap UU tersebut. Melihat kejadian terkait implementasi dan kepatuhan terhadap Peraturan Menteri Komunikasi dan Informatika No. 5 Tahun 2020, kepatuhan para penyelenggara sistem elektronik merupakan tantangan. Sebagaimana menjelang masa akhir dari tenggat waktu adopsi. Permenkominfo No. 5 Tahun 2020, masih terdapat banyak penyelenggara sistem elektronik privat yang tidak mengadopsi Permenkominfo No. 5 Tahun 2020, sehingga pemerintah terpaksa memblokir akses platform mereka di Indonesia hingga mereka mengadopsi Permenkominfo No. 5 Tahun 2020.²³ Hal serupa dapat terjadi dengan UU PDP jika para penyelenggara sistem elektronik tidak segera mengadopsi UU PDP dalam batas waktu 2 tahun.





KEAMANAN SIBER DALAM LAYANAN PERBANKAN DAN FINANSIAL DI INDONESIA: PERSPEKTIF INDUSTRI

A Tantangan Keamanan Infrastruktur Siber

Sebagai salah satu sektor yang menjadi target utama dalam serangan siber, industri-industri dalam sektor perbankan dan finansial menghadapi sejumlah tantangan yang berkaitan dengan infrastruktur siber mereka. Di antara jenis-jenis serangan yang menargetkan sektor tersebut, *ransomware* merupakan salah satu jenis serangan tertinggi yang ditemukan dalam beberapa tahun terakhir. Dengan jumlah sebanyak 1.3 juta serangan *ransomware* yang menyasar ke seluruh sektor, Indonesia menempati posisi pertama di negara ASEAN yang mendapati serangan dengan jenis ini.²⁴ Perkembangan teknologi membuat serangan *ransomware* menjadi ancaman yang paling sering dilakukan oleh para pelaku. Serangan ini biasanya menyebar melalui penipuan *phishing* atau dengan mengeksploitasi kerentanan dalam perangkat lunak atau sistem, dan dapat menimbulkan konsekuensi serius bagi individu dan organisasi yang menjadi korban serangan ini.²⁵

Untuk menangani serangan *ransomware*, sektor perbankan dan finansial di Indonesia perlu menerapkan sistem keamanan yang kuat, memberikan edukasi keamanan siber bagi nasabah dan pegawai, serta bekerjasama dengan pihak-pihak terkait untuk menjaga keamanan siber.

Benny Sadwiko (Chief Information Security Officer, Koordinator Task Force Ketahanan dan Keamanan Siber Bank Indonesia) mengatakan bahwa beberapa tantangan utama dalam kerentanan industri menghadapi serangan siber adalah kurangnya sistem *prevention and detection* yang dapat menghalau serangan ini masuk, ketidaksiapan *urgent management* dan *physical security*, kurangnya kesadaran dan supervisi dalam penanganan serangan siber, serta kurangnya edukasi terhadap nasabah mengenai serangan siber itu sendiri.²⁶ Selain itu, kurangnya *cyber-talent* juga merupakan isu penting yang perlu diatasi oleh para *stakeholders* di sektor ini.

Di sisi lain, beberapa peserta FGD lain juga menyampaikan bahwa tantangan yang mereka hadapi juga datang dari semakin maraknya *social engineer* yang menipu dan bertujuan untuk mengambil data-data pribadi dari penggunaanya. Walaupun ancaman ini tidak serta merta meliputi ancaman yang diakibatkan oleh infrastruktur, ancaman ini juga dapat diminimalisasi dengan peningkatan infrastruktur keamanan seperti penggunaan sistem keamanan *multifactor authentication* serta penerapan *zero-trust policy*.



B Pola Hubungan Industri dan Pemerintah

Dalam konteks keamanan siber dalam layanan perbankan dan finansial di Indonesia, industri dan pemerintah memiliki hubungan yang saling terkait dan bergantung. Industri perbankan dan finansial di Indonesia bergantung pada pemerintah untuk memberikan regulasi yang memadai dan menjamin keamanan siber layanan keuangan, sementara pemerintah bergantung pada industri untuk menjalankan layanan keuangan dengan aman dan terpercaya.

Pemerintah di Indonesia telah menerbitkan beberapa peraturan dan kebijakan yang berkaitan dengan keamanan siber dalam layanan perbankan dan finansial, seperti Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran, serta Undang-undang Pelindungan Data Pribadi. Peraturan-peraturan tersebut bertujuan untuk menjaga keamanan siber layanan keuangan di Indonesia dan melindungi hak-hak nasabah.

Industri perbankan dan finansial di Indonesia harus mematuhi peraturan-peraturan yang dikeluarkan oleh pemerintah, serta terus berupaya meningkatkan sistem keamanan siber mereka untuk menjaga kepercayaan nasabah dan menghindari terjadinya serangan siber. Pemerintah juga harus terus memantau perkembangan industri perbankan dan finansial, serta memberikan dukungan dan fasilitas yang diperlukan agar industri tersebut dapat beroperasi dengan aman dan terpercaya.

Meskipun demikian, pola hubungan industri dan pemerintah hanya dapat berjalan jika kedua belah pihak bersifat transparan dalam menjalani hubungan kerja sama ini. Benny Sadwiko (Chief Information Security Officer, Koordinator Task Force Ketahanan dan Keamanan Siber Bank Indonesia) mengatakan bahwa salah satu tantangan dari hubungan kerja sama industri dan pemerintah adalah kurangnya transparansi dari pihak industri.²⁷ Pihak industri perlu lebih transparan terhadap pemerintah dalam hal pelaporan informasi sampai kepada detail sekecil apapun, agar pemerintah dapat mengetahui langkah efektif apa yang dapat dilakukan guna membantu sektor industri. Namun kecenderungan yang terjadi adalah sektor industri masih kurang bersifat transparan kepada pihak pemerintah.



C Keterlibatan dan Inisiatif Industri

Dalam mengatasi tantangan-tantangan serta menghadapi ancaman serangan siber, sektor industri berperan besar untuk menciptakan sistem yang tepat di lembaga masing-masing. Sejumlah bank telah menerapkan strategi masing-masing dalam membangun infrastruktur mereka. Berdasarkan laporan dari *Communication & Information System Security Research Center (CISSReC)*, ditunjukkan bahwa beberapa Bank memiliki tingkat keamanan siber yang justru lebih tinggi dibanding lembaga negara lainnya. Bank Tabungan Pensiunan Nasional misalnya menempati posisi pertama dengan poin 92 sedangkan Badan Siber dan Sandi Negara (BSSN) mendapatkan poin sebesar 82. Bank Indonesia juga menunjukkan inisiatifnya dengan membentuk tim respons atas insiden komputer terkait keamanan keuangan yang membuatnya meraih penghargaan *Cyber Resilience Initiative* dalam *Central Banking's FinTech RegTech Global Awards* oleh *Central Banking Publication (CBP)* pada tahun 2022.²⁸ Angela Wanodya Sawangi (Assistant Vice President Bank Central Asia) mengatakan bahwa BCA telah secara mandiri mengikuti standar oleh BI, BSSN, dan OJK serta standar-standar internasional yang diterapkan oleh badan internasional seperti ISO. BCA juga menggunakan 10 persen dari total anggaran dana atau sebesar Rp500 Miliar untuk meningkatkan keamanan sibernya.²⁹

Di sisi lain, industri-industri di sektor perbankan dan finansial juga turut berinisiatif dalam mengedukasi nasabahnya mengenai ancaman siber termasuk penipuan digital. Lembaga-lembaga seperti OJK, BI, BCA, dan AFTECH turut mengupayakan kampanye serta sosialisasi yang menargetkan kepada para nasabah dan pengguna layanan sektor perbankan dan finansial untuk menjadi lebih sadar dan terampil dalam mengatasi ancaman siber. AFTECH misalnya, menciptakan sebuah situs bernama CEKFINTECH.ID yang dapat digunakan untuk mengecek apakah sebuah platform fintech legal atau tidak.³⁰ Inisiatif-inisiatif seperti ini terus digalakkan oleh industri-industri untuk meningkatkan keamanan siber dan meminimalisasi ancamannya.

KESIMPULAN

Pandemi COVID-19 yang telah merubah tatanan dunia selama dua tahun ini juga berpengaruh terhadap perkembangan teknologi. Akibat dari pandemi ini, semakin banyak orang bergantung kepada teknologi yang mengakibatkan industri untuk terus berinovasi agar dapat memenuhi permintaan masyarakat. Salah satu industri yang terpengaruhi oleh transformasi digital pandemi adalah industri layanan perbankan dan finansial. Industri layanan perbankan dan finansial selama masa pandemi mengalami disrupsi besar, baik dari segi jumlah pengguna yang meningkat maupun kerentanan yang dialami industri tersebut akibat nilai yang dimilikinya.

Dengan disahkan dan diberlakukannya Peraturan Bank Indonesia Nomor 22/23/PBI/2020 tentang Sistem Pembayaran, layanan perbankan dan finansial Indonesia menjadi semakin dapat dipercaya dan mudah digunakan baik dari segi industri maupun nasabah. Di samping itu, dengan adanya POJK Nomor 4/POJK.05/2021 Tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Lembaga Jasa Keuangan Non-Bank, dan POJK Nomor 11/POJK.03/2022 Tentang Penyelenggaraan Teknologi Informasi Oleh Bank Umum para penyelenggara layanan perbankan dan finansial juga diwajibkan untuk meningkatkan kapasitas TI nya untuk menghindari ancaman-ancaman siber di masa depan. Tidak hanya itu saja, disahkannya Undang-undang Pelindungan Data Pribadi menjadi lapisan tambahan dalam upaya pemerintah Indonesia untuk terus memperbaiki regulasi keamanan siber dan pelindungan data pribadi di Indonesia. Terlepas dari serangkaian instrumen yang mengatur sistem elektronik lembaga-lembaga perbankan dan finansial yang ada, isu keamanan siber masih akan menjadi aspek penting bagi keberlangsungan dan keberlanjutan layanan perbankan dan finansial Indonesia yang ke depannya terus akan menjadi perhatian baik bagi pemerintah maupun sektor industri.

Dalam FGD dan penulisan Digitimes ini, salah satu aspek penting yang dapat dilakukan baik oleh pemerintah maupun industri adalah untuk terus berkolaborasi. Guna mengurangi dampak yang dapat dirasakan dari lemahnya keamanan siber dan nilai yang dimiliki oleh industri perbankan dan finansial. Dengan adanya kolaborasi antara pemerintah dan industri, kedua entitas tersebut akan saling mampu melengkapi dalam aspek-aspek yang mereka kurang. Industri dapat bertindak lebih transparan dan melaporkan detail sekecil apapun. Sebaliknya, dengan informasi yang didapatkan oleh industri, pemerintah akan mampu untuk memformulasikan kebijakan-kebijakan yang menguntungkan kedua belah pihak.

REFERENCES

- ¹Bedaiwy, S., & Peter, D. (2022). Microfinance Regulation and Consumer Socio-Economic Security. In E. Alaverdov, & M. Bari (Ed.), *Regulating Human Rights, Social Security, and Socio-Economic Structures in a Global Perspective* (pp. 194-210). IGI Global. <https://doi.org/10.4018/978-1-6684-4620-1.ch012>
- ²The Global Findex Database 2021, The World Bank. <https://www.worldbank.org/en/publication/globalfindex>
- ³The Global Findex Database 2021
- ⁴The Global Findex Database 2021
- ⁵Dirangkum dari laporan The Global Cyber Threats to Financial System (IMF,2020) <https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm>
- ⁶Verizon Business 2021 Data Breach Investigations Report
- ⁷Ahdiat, A. (2022). "Tren Transaksi QRIS Meningkat Pesat sejak Awal Pandemi." Databoks, 1 November 2022. <https://databoks.katadata.co.id/datapublish/2022/11/01/tren-transaksi-qrisk-meningkat-pesat-sejak-awal-pandemi>.
- ⁸Data dari laporan Statista berjudul "Number of digital payment users in Indonesia from 2017 to 2021, with forecasts to 2027" (2022).
- ⁹Dalam FGD Lanskap Keamanan Siber dalam Layanan Perbankan dan Finansial di Indonesia bersama CfDS UGM pada tanggal 22 November 2022.
- ¹⁰Menteri Keuangan, Sri Mulyani Indrawati dalam 3rd Indonesia Fintech Summit 2021, 11 Desember 2021
- ¹¹ASEAN Cyberthreat Assessment 2021, Interpol
- ¹²ASEAN Cyberthreat Assessment 2021, Interpol
- ¹³Dalam FGD Lanskap Keamanan Siber dalam Layanan Perbankan dan Finansial di Indonesia bersama CfDS UGM pada tanggal 22 November 2022.
- ¹⁴CNN Indonesia, 2022. Deadlock RUU PDP, Kominfo Ungkap Alasan Belum Sepakat dengan DPR [WWW Document]. URL <https://www.cnnindonesia.com/teknologi/20220611042603-185-807654/deadlock-ruu-pdp-kominfo-ungkap-alasan-belum-sepakat-dengan-dpr>
- ¹⁵Presiden Terbitkan Perpres 82/2022 tentang Pelindungan Infrastruktur Informasi Vital [WWW Document], 2022. . Sekretariat Kabinet Republik Indonesia. URL <https://setkab.go.id/presiden-terbitkan-perpres-82-2022-tentang-pelindungan-infrastruktur-informasi-vital/>
- ¹⁶PwC Indonesia, 2020. Indonesia's Progress on Data Protection (No. 02), Digital Trust News-Flash. PwC Indonesia.
- ¹⁷Skills for the future in Indonesia in 2030, AlphaBeta Advisors. URL <https://alphabeta.com/our-research/skills-for-the-future-in-indonesia-in-2030/>

¹⁸ASEAN Cyberthreat Assessment 2021

¹⁹Dirangkum dari halaman Bank Indonesia mengenai Peraturan BI No 22/23/PBI/2020 tentang Sistem Pembayaran. https://www.bi.go.id/id/publikasi/peraturan/Pages/P-BI_222320.aspx

²⁰Asosiasi Penyelenggara Jasa Internet Indonesia, 2022. Laporan Survei Internet APJII 2022.

²¹adminsiberkreasi, 2020. Status Literasi Digital Indonesia 2020 (Hasil Survei di 34 Provinsi). literasi digital. URL http://literasidigital.id/sdm_downloads/status-literasi-digital-indonesia-2020-hasil-survei-di-34-provinsi/ (accessed 4.26.21).

²²The Global Findex Database 2021

²³Yusuf, 2022. Dirjen Aptika: Pendaftaran PSE Bertujuan untuk Ciptakan Ruang Digital Kondusif. Ditjen Aptika. URL <https://aptika.kominfo.go.id/2022/08/dirjen-aptika-pendaftaran-pse-bertujuan-untuk-ciptakan-ruang-digital-kondusif/> (accessed 8.20.22).

²⁴ASEAN Cyberthreat Assessment 2021

²⁵Gendre, A. (2022). "Ransomware Attacks: Why Email Is Still the #1 Delivery Method." Vade, 16 Juni 2022.

²⁶Dalam FGD Lanskap Keamanan Siber dalam Layanan Perbankan dan Finansial di Indonesia bersama CfDS UGM pada tanggal 22 November 2022.

²⁷Dalam FGD Lanskap Keamanan Siber dalam Layanan Perbankan dan Finansial di Indonesia bersama CfDS UGM pada tanggal 22 November 2022.

²⁸Publikasi Bank Indonesia. (2022). Bank Indonesia Perkuat Prakarsa Ketahanan Siber. https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_2415822.aspx

²⁹Dalam FGD Lanskap Keamanan Siber dalam Layanan Perbankan dan Finansial di Indonesia bersama CfDS UGM pada tanggal 22 November 2022.

³⁰Pertiwi, W.K., n.d. Cek Legalitas Pinjol dan Fintech di Situs Cekfintech.id Halaman all - Kompas.com [WWW Document]. KOMPAS.com. URL <https://tekno.kompas.com/read/2021/11/19/19425877/cek-legalitas-pinjol-dan-fintech-di-situs-cekfintechid?page=all>



ABOUT CFDS

Center for Digital Society (CfDS) is the research center established by the Faculty of Social and Political Sciences, Universitas Gadjah Mada. The institution is created under the concern over the contemporary dynamics of socio-political condition of the world that is accentuated by the impeccable influence of information technology. The phenomenon triggers the new patterns and complexities in the society, and thus requires new approaches in managing such complexities.

CfDS pledged to delve more on the study of contemporary digital society, including related issues surrounding the topic; such as the issues of smart city and urban development. The emphasis is then put on the utilization of technology to shape the society in becoming digitalized, as well as to bring solvency to social issues.

VISION

Solving Social Problem and Accelerating Prosperity through Indonesia Digital Society

ACTIVITIES

- Research and development
- Dissemination and Publication
- Educational and Policy Advocacy



 facebook.com/cfds.ugm

 @cfds_ugm

 Center for Social Society (CfDS)

 @cfds_ugm

 Cfds_ugm

 CfDS UGM