



Kolaborasi *Pentahelix*

dalam Perlindungan Data Pengguna Layanan *E-Commerce* dan Perbankan Digital di Indonesia

**Penulis**

Janitra Haryanto
Amelinda Pandu Kusumaningtyas
Anaq Duanaiko

Editor

Dewa Ayu Diah Angendari

Desain dan Tata Letak

Masgustian

Pendahuluan

Perkembangan teknologi telah memungkinkan digitalisasi dalam pelbagai ranah strategis. Salah satunya adalah ranah ekonomi, khususnya dalam bidang penyedia pasar (*e-commerce*) dan jasa perbankan (perbankan digital). Digitalisasi kedua sektor tersebut mendorong perubahan kebiasaan masyarakat, dari konvensional menuju digital. McKinsey & Company memperkirakan terdapat 30 juta pelanggan *e-commerce* di tahun 2017 dan akan bertambah seiring tahun.¹ Data lain dari We Are Social menyebutkan bahwa setidaknya 86% dari total pengguna internet di Indonesia pernah melakukan pembelian produk atau jasa secara daring.² Jumlah ini diprediksi akan terus bertambah seiring dengan bertambahnya angka pengguna internet di Indonesia.

Fenomena digitalisasi ini tentunya diikuti oleh munculnya fenomena pertukaran data di ranah daring. Perkembangan teknologi menempatkan data sebagai inti dari layanan penyedia jasa. Teknologi komputasi awan dan perkembangan analisis *big data* memungkinkan pengoperasian sistem dan penyimpanan data yang lebih efisien, serta pengolahan data dalam jumlah yang besar untuk memberikan gambaran yang lebih akurat. Di satu sisi, hal ini merupakan bentuk inovasi yang sangat penting dalam pelayanan konsumen. Namun di sisi lain, pertukaran data juga membuka ruang bagi kejahatan siber.

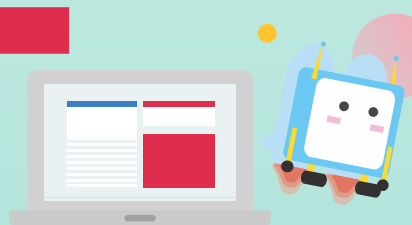
Menurut data yang dikeluarkan oleh Bareskrim Polri (sebagaimana dijelaskan dalam Rahmadiani dkk., 2018), kasus kejahatan siber yang menasar pengguna layanan *e-commerce* dan perbankan digital pada tahun 2018 sejumlah 1.507 kasus.³ Dari jumlah tersebut, 1.404 kasus merupakan kasus penipuan berbasis daring dan sisanya merupakan kasus intrusi ilegal ke dalam surel pengguna layanan.⁴ Pada tahun 2019, beberapa kasus kejahatan siber terhadap pengguna layanan *e-commerce* dan perbankan digital juga mencuat ke publik. Polri mencatat 3.429 kasus kejahatan siber sejak bulan Januari hingga Agustus dengan kasus penipuan di *e-commerce* sebagai jumlah kasus terbanyak.⁵

Di sisi lain, perlindungan data pribadi yang mencakup data pengguna layanan belum diformulasikan dengan komprehensif. Pemerintah dan penyedia jasa layanan seringkali didapuk sebagai pihak yang paling bertanggungjawab dalam kasus kejahatan

siber terhadap data pengguna. Padahal, perlindungan data pengguna sejatinya merupakan tanggungjawab bersama yang melibatkan pelbagai aktor, termasuk pengguna, akademisi, dan komunitas terkait.

Berangkat dari permasalahan tersebut, studi kasus ini berupaya menganalisis pendekatan terhadap perlindungan data pribadi yang efektif guna menghindari kejahatan siber. Menggunakan metode studi literatur, studi ini berargumen bahwa kolaborasi *Pentahelix* merupakan salah satu pendekatan yang efektif untuk menjaga keamanan data pengguna oleh karena peran dan kapabilitas aktor yang beragam sehingga masing-masing sektor dapat saling melengkapi perlindungan data pengguna layanan *e-commerce* dan perbankan digital.

Digitalisasi dan Transformasi menuju Masyarakat Digital



Seiring dengan pesatnya pertumbuhan moda produksi yang berimplikasi pada pertumbuhan ekonomi, gaya hidup masyarakat pun bertransformasi dengan cepat pula. Fenomena ini menjadi kekhasan yang muncul di negara-negara berkembang, termasuk Indonesia. Hal ini terlihat lebih kentara di tetangga Indonesia, Singapura, di mana gaya hidup masyarakat kini 30% lebih cepat dibandingkan era tahun 90-an.⁶ Menurut Psikolog Dr Stephanie Brown yang berasal dari *Silicon Valley*, apa yang berbahaya dari gaya hidup masyarakat yang serba cepat adalah bagaimana kecepatan memberikan sebuah rasa semu, dikarenakan kunci dari pembentukan hubungan antar manusia berada di dalam aksi bukan akumulasi interaksi seperti yang diberikan sekarang.⁷

Jasa yang memudahkan adanya interkoneksi antar fungsi pun muncul untuk menawarkan efektivitas yang lebih dalam tujuan jual-beli di dunia digital (*e-tailing*). Layanan seperti digital banking pun merupakan inovasi perbankan yang memudahkan transaksi daring. Dari pilihan transfer melalui *Virtual Account* hingga kartu debit virtual muncul agar masyarakat dapat membayar tanpa harus mengunjungi ATM untuk transfer. Layanan perbankan yang canggih ini sering juga disebut *Digital Banking* karena penggunaan akses internet saat melakukan aktivitas perbankan. Kini, kata-kata baru seperti '*Online Shopping dan Online Payment*' bukan lagi istilah asing bagi sebagian besar pengguna internet. Dunia digital memungkinkan pengguna berubah menjadi konsumen hanya dengan jari mereka.

Fenomena ini menunjukkan bahwa *e-commerce* telah mengakomodasi masyarakat modern yang bertujuan mengejar efektivitas dalam mencapai tujuan. Schiff menjelaskan dalam bukunya yang berjudul *How an Economy Grows and Why It Crashes*, bahwa masyarakat telah menjadi lebih rumit dalam kondisi pertumbuhan ekonomi.⁸ *Digital banking* dan *e-commerce* menjadi saling terkait di dunia yang serba cepat ini karena kemudahan pembayaran daring dalam melakukan transaksi daring. Hal yang cepat dan instan ini pun dapat mengubah pola konsumsi seseorang dalam melakukan kegiatan jual beli.

Gaya Hidup Digital dan Kejahatan Siber

Penggunaan teknologi digital di Indonesia sangatlah tersegmentasi. Posisi sosial atau fisik seseorang dalam lanskap geopolitik Indonesia sangat berpengaruh pada kedekatan individu tersebut dengan dunia digital.⁹ Kesenjangan digital tidak hanya masalah tingkat akses ke teknologi dan infrastruktur material, tetapi juga berbagai faktor yang membentuk peluang orang untuk mengadopsi media digital, seperti gender, pendidikan, status sosial ekonomi, usia, dan bahkan geografis.¹⁰ Bahkan bagi mereka yang telah memiliki akses terhadap dunia digital, tidak serta merta diikuti dengan adanya pengetahuan dan kompetensi yang memadai terhadap dunia digital itu sendiri. Akibatnya, masyarakat yang memiliki akses digital yang cukup ini juga merupakan masyarakat yang rentan terkena permasalahan yang sering muncul dalam dunia digital. Laporan yang dikeluarkan oleh *World Economic Forum* di tahun 2019 bahkan mengungkapkan bahwa penyalahgunaan data pribadi dan kejahatan siber kini menjadi salah satu risiko global. Hal ini disebabkan karena kecepatan perkembangan teknologi nyatanya tidak selalu diikuti oleh cepatnya respon pemerintah dan kecakapan serta tingkat pengetahuan pengguna.

Dalam konteks *e-commerce* dan jasa layanan *online* lainnya, kecepatan akses dan besaran jumlah pengguna memiliki dampak yang besar pula. Meningkatnya *e-commerce* yang digunakan untuk menunjang gaya hidup pun telah memancing para kriminal siber untuk melakukan aksinya kepada kelompok yang mampu mengakses gaya hidup digital ini.



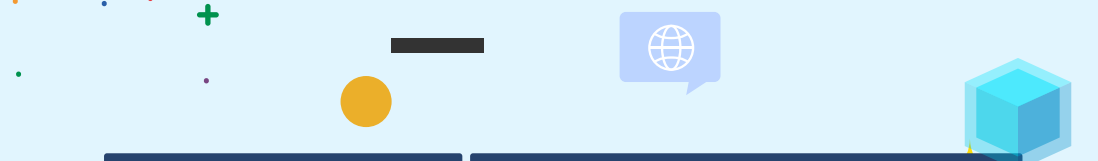


Kejahatan Siber terhadap Pengguna Layanan *E-Commerce* dan Perbankan Digital

Mengacu pada hasil Konvensi Kejahatan Siber Komite Eropa (sebagaimana dijelaskan pada ITU, 2012), kejahatan siber didefinisikan berdasarkan tipologinya sebagai: (1) serangan terhadap integritas, ketersediaan dan kerahasiaan data dan sistem komputer, (2) serangan yang berkaitan dengan komputer, (3) serangan yang berkaitan dengan konten, (4) serangan yang berkaitan dengan hak cipta.¹¹ Dalam tipologi kejahatan siber tersebut, kejahatan siber terhadap pengguna layanan *e-commerce* dan perbankan digital dapat dikategorikan dalam tipologi (1) dan (2). Kejahatan siber terhadap pengguna layanan *e-commerce* dan perbankan digital biasanya merupakan penipuan dengan motif ekonomi dan pelbagai metode.

Hingga saat ini, belum ada istilah yang disepakati secara internasional dalam menyebutkan tipe kejahatan ini. Tipe kejahatan siber memiliki sebutan yang beragam: penipuan berbasis komputer (*computer fraud*, berdasarkan UU Penipuan dan Penyalahgunaan Komputer Amerika Serikat)¹², penipuan berbasis internet (*internet fraud*, berdasarkan Kepolisian Federal Australia)¹³, dan lain sebagainya. Di kawasan Uni Eropa, penipuan terhadap pengguna layanan *e-commerce* dan perbankan digital dilakukan dengan sejumlah kategori teknik seperti manipulasi lokasi (*location manipulation*), penipuan identitas (*identity fraud*), penipuan perangkat (*device spoofing*), bot (*threats and bots*) dan penipuan pembayaran (*payment fraud*).¹⁴

Kategori Teknik	Teknik	
<i>Location Manipulation</i>	• <i>IP Spoofing</i> • <i>Geo Spoofing</i> • <i>Rotating IP</i> • <i>ProxyAnon</i>	• <i>VPN Anon</i> • <i>TOR Dropbox</i> • <i>Shipping Package Pickup</i>
<i>Identity Fraud</i>	• <i>Social Engineering</i> • <i>Documentation Forgery</i> • <i>Call Center Fraud</i> • <i>Credential Testing</i> • <i>Recipient Fraud</i> • <i>Synthetic Identity</i> • <i>Credential Replay</i>	• <i>Salary Staging</i> • <i>Phishing</i> • <i>Mules</i> • <i>Account Validation</i> • <i>Card Testing</i> • <i>Ghost Broker</i> • <i>Identity Farms</i> • <i>Identity Marketplace</i>



Kategori Teknik	Teknik
Device Spoofing	• Malicious Apps • App Tampering • Jailbreak • Session Hijack • Root Cloaking • SMShijacking • Device Cloning • Session Replay • Device Posting Ghosting • Mobile App Vulnerability • Cookie Wiping • Remote Desktop • Fraudfox/Antidetect
Threats and Bots	• Insider Recruitment • Man in the Browser • Banking Malware • Keylogging • Low and Slow BOTS • Man in the Mobile • DDoS • Adv Persistent Threat • Ransomware • Remove Access Trojan • Simple/Mobile BOTS • Spyware • Trojan Horse • Network Hacks • Compromised Email Session • Tampering
Payment Fraud	• Payment Fraud • Fake Policy Application • Fake Loan Application • New Card Application • Illegal Money Transfer • Identity Takeover • Seller Fraud • OFAC/AML • Loan Stacking • Gift Card Fraud • Fraudulent Claims • Tax Fraud • Bustout (Loan) • Fake Listing • Loyalty Fraud • Content Access • Bonus Abuse



Tabel 1. Tren metode penipuan di kawasan UE tahun 2019

Namun demikian, oleh karena penipuan terhadap pengguna *e-commerce* dan perbankan digital di setiap kawasan dilakukan oleh penyerang dan terhadap target dengan kelemahan yang berbeda, setiap kawasan memiliki teknik serangannya sendiri. Menurut pemaparan Direktorat Tindak Pidana Siber Bareskrim Polri (sebagaimana ditulis oleh Rahmadiani dkk., hal. 4), setidaknya terdapat tujuh teknik penipuan siber yang marak digunakan di Indonesia: *cracking*, *diddling*, *leaking*, *distributed denial of service* (DDoS), *email forgery and threat*, *piggybacking*.¹⁵ Penjelasan lebih lanjut mengenai teknik tersebut adalah sebagai berikut:



1. Cracking

Cracking atau peretasan adalah sebuah metode peretasan sistem komputer dengan tujuan mengakses informasi pribadi seseorang.¹⁶ Peretasan seringkali dilakukan dengan secara berulang (teknik *brute-force*), berupaya memasuki suatu sistem dengan cara mencoba satu-per-satu kemungkinan celah dalam sistem tersebut. Mengenai teknik *cracking* dan kaitannya dengan keamanan akun perbankan, Robitzski berargumen bahwa peretasan melalui celah sistem keamanan bank biasanya digunakan untuk mengidentifikasi akun-akun bank yang memiliki jumlah uang yang besar sebagai calon target penipuan.¹⁷

2. Diddling

Berkaitan dengan integritas data, *diddling* dapat didefinisikan sebagai kegiatan modifikasi data dalam sebuah sistem komputer. Zakaras menjelaskan lebih lanjut bahwa *diddling* (atau yang seringkali disebut dengan *tampering*) akan sangat berbahaya apabila dilakukan terhadap akses utama (*root access*) dari suatu sistem komputer yang memiliki kapasitas mengubah, menerima, memerintahkan dan menghapus suatu data dari sistem.¹⁸ Akses terhadap akses utama akan memungkinkan penyerang untuk juga menempatkan *malware* berupa Trojan untuk memanipulasi sistem. Teknik ini digunakan pada kasus peretasan akun Citibank oleh penyerang yang berasal dari Rusia pada tahun 1994, dimana uang sejumlah sepuluh juta dolar dimanipulasi agar dikirimkan melalui empat puluh transaksi di akun bank yang tersebar di tujuh negara berbeda.¹⁹



3. Leaking

Leaking adalah eksploitasi data pengguna secara non-konsensual kepada aktor-aktor tertentu. Pembocoran data pengguna tidak harus melalui intrusi dalam sebuah sistem komputer secara ilegal. Kasus yang terjadi terhadap raksasa *e-commerce* Amazon di Tiongkok membuktikan bahwa dengan lemahnya pengawasan dalam sebuah organisasi, karyawan yang berperan sebagai pengelola data dapat menyalahgunakan otoritasnya untuk menerima suap dari perusahaan tertentu dan membeberkan informasi pelanggan untuk kepentingan perusahaan tersebut.²⁰

4. Distributed Denial of Service (DDoS)

DDoS adalah serangan yang dilakukan secara bersamaan oleh sejumlah perangkat komputer untuk melumpuhkan akses pengguna terhadap perangkat/sistem komputer.²¹ Menurut Innab dan Alamri, DDoS memiliki tiga tipe penyerang: *masquerader* (penyerang merupakan aktor yang tidak memiliki izin dan berupaya masuk ke sistem milik aktor lain), *misfeasor* (penyerang merupakan aktor yang memiliki izin namun menyalahgunakan izin tersebut) dan *clandestine user* (penyerang merupakan aktor yang tidak memiliki izin dan berupaya mengontrol maupun mencuri data aktor yang berizin).²² Terlepas dari tipe penyerangannya, DDoS dapat berdampak besar bagi keberlangsungan layanan *e-commerce* dan perbankan digital. Kasus serangan DDoS yang dikombinasikan dengan teknik *phishing*²³ terhadap perusahaan *e-commerce* E-bay menyebabkan kerugian waktu dan finansial, serta meningkatnya keuntungan kompetitif dari perusahaan lain akibat menurunnya reputasi E-bay.²⁴

5. Email Forgery and Threat

Email forgery and threat adalah kegiatan penipuan dan peretasan terhadap surel individu maupun organisasi dengan tujuan kriminal. *Email forgery* pada dasarnya merupakan serangan *spoofing*, dimana penyerang meniru individu maupun organisasi yang terpercaya dan berupaya menipu target untuk melakukan kegiatan tertentu melalui surel.²⁵ Dalam kasus serangan terhadap perbankan digital, Alsayed dan Bilgrami menyebut taktik ini sebagai *deceptive phishing attack* dimana penyerang menyamar sebagai perwakilan dari bank yang digunakan oleh target, lalu melakukan 'call action' - penyerang menyertakan urgensi yang tinggi untuk mengakses *link* yang mengarahkan target dalam alamat web yang berbahaya.²⁶

6. Piggybacking

Piggybacking adalah upaya penyusupan penyerang terhadap sebuah sistem komputer/jaringan dengan memanfaatkan kelalaian aktor-aktor yang memiliki akses terhadap sistem tersebut.²⁷ Teknik ini tidak selalu membutuhkan kemampuan peretasan, mengingat penyerang dapat menggunakan teknik *socio-engineering* untuk memancing target memberikan akses terhadap penyerang. Namun demikian, *piggybacking* juga dapat direferensikan sebagai *piggyback-entry wiretapping* yang didefinisikan oleh Kim dan Solomon sebagai upaya penyerang untuk memotong jaringan dan memodifikasi pesan dalam jaringan komunikasi dengan merubah jaringan komunikasi dan mengarahkannya kepada komputer lain yang dikehendaki penyerang.²⁸

Teknik-teknik di atas seringkali digunakan oleh penyerang siber di Indonesia guna melakukan penipuan. Dalam melakukan serangan siber, penyerang bisa mendapatkan informasi awal dari aktivitas jual-beli data pribadi ilegal di dalam *dark web*. Informasi yang didapatkan meliputi nama pengguna hingga nomor kartu kredit/debit maupun rekening pengguna layanan.²⁹

Saat ini, kesulitan penanggulangan permasalahan data pengguna jasa layanan *e-commerce* dan perbankan digital ditengarai oleh tiga karakteristik kejahatan siber; (1) melewati batasan antar negara, (2) anonimitas penyerang, dan (3) pengorganisasian serangan.³⁰ Apalagi dalam konteks serangan siber terhadap sistem komputer apapun, serangan dapat dilakukan secara diam-diam dan memanfaatkan kelemahan sistem yang tidak diketahui oleh pengguna maupun pengelola. Serangan seperti ini seringkali disebut sebagai *zero-day attack*.³¹



Kolaborasi *Pentahelix* sebagai Upaya Pengamanan Data Pengguna Layanan *E-Commerce* dan Perbankan Digital

Dunia digital, termasuk *e-commerce* dan perbankan digital, dapat diibaratkan sebagai sebuah sistem yang melibatkan berbagai aktor yang memiliki peranannya masing-masing. Setidaknya terdapat lima aktor penting dalam mewujudkan perlindungan data pengguna layanan *e-commerce* dan perbankan digital. Aktor-aktor tersebut adalah; (1) pemerintah (*Government*), (2) penyedia jasa layanan *e-commerce* dan perbankan digital (*Companies*), (3) akademisi (*Academicians*), (4) komunitas (*Community*), dan (5) pengguna layanan *e-commerce* dan perbankan digital (*Users*).³² Meski memiliki perannya masing-masing, kelimanya melakukan upaya dengan tujuan yang sama: meningkatkan keamanan data pengguna layanan *e-commerce* dan perbankan digital. Oleh sebab itu, meski tidak selalu dilakukan dalam suatu kerangka kerja yang terorganisir, studi ini mempersepsikan upaya dari masing-masing tersebut sebagai sebuah kolaborasi antar aktor yang dilakukan untuk memastikan keamanan data pengguna layanan *e-commerce* dan perbankan digital.

Studi ini juga melihat bahwa kolaborasi antar aktor merupakan salah satu upaya yang efektif karena adanya keberagaman peran serta kemampuan sumber daya setiap aktor dalam menangani permasalahan digital yang bersifat saling melengkapi. Sebagai contoh, pemerintah memiliki peran sebagai institusi yang mendapatkan legitimasi dari masyarakat untuk menjaga keteraturan sosial. Pemerintah dengan



aparatur sipil memiliki kapabilitas dalam menyusun dan menetapkan yang dapat memastikan keamanan data pengguna. Di sisi lain, penyedia layanan *e-commerce* dan perbankan digital sebagai badan usaha memiliki kuasa sumber daya dalam melindungi konsumen. Sumber daya ini dapat berupa inovasi teknologi yang mumpuni serta kompetensi sumber daya manusia dalam organisasi tersebut.

Dalam konteks Indonesia, kolaborasi *pentahelix* dapat menjadi sebuah strategi yang dapat ditempuh untuk mewujudkan perlindungan data pengguna seutuhnya. Kolaborasi *pentahelix* merupakan sebuah pendekatan yang menekankan pada sinergi para aktor secara holistik.³³ Kolaborasi antar aktor dilakukan sesuai dengan peran dan kapabilitas masing-masing aktor. Pemerintah, penyedia jasa layanan *e-commerce* dan perbankan digital, akademisi, komunitas, dan pengguna layanan *e-commerce* dan perbankan digital mengupayakan perlindungan data pengguna sebagai berikut:

Pemerintah

Sebagai lembaga negara yang dimandatkan oleh konstitusi untuk melindungi warga negaranya, pemerintah memiliki kewajiban untuk meregulasi penyelenggaraan layanan *e-commerce* dan perbankan digital. Dalam konteks perlindungan data pengguna oleh pemerintah, pendekatan telah dilakukan, baik secara regional (berbasis kawasan) maupun domestik (berbasis negara).

Secara regional, UE adalah satu-satunya organisasi regional yang memiliki regulasi mengenai perlindungan data pribadi, termasuk data pengguna layanan *e-commerce* dan perbankan digital. Pendekatan regulatif perlindungan data pribadi tersebut dikodifikasikan dalam *General Data Protection Right* (GDPR) yang mengikat seluruh organisasi (baik negara maupun badan usaha) yang beroperasi di dalam kawasan UE untuk melakukan serangkaian kebijakan guna memastikan keamanan data pribadi masyarakat UE.³⁴ Dalam hal perlindungan data pengguna, penyedia jasa layanan memastikan adanya penggunaan perangkat lunak enkripsi untuk menyimpan dan mengirimkan data pengguna, serta mematuhi kebijakan Teknologi Informasi Komunikasi (TIK) yang sudah diterapkan oleh pemerintah setempat.³⁵

Dalam tataran negara, regulasi perlindungan data pribadi telah diterapkan baik sebagai sebuah regulasi yang berdiri sendiri, seperti UU Perlindungan Data (*Data Protection Act*) di Inggris; maupun secara terpisah pada sektor tertentu, seperti the UU Komisi Perdagangan Federal (*Federal Trade Commission/FTC Act*) dan UU Privasi Konsumen Kalifornia (*California Consumer Privacy Act/CCPA*) di AS.³⁶ Apabila telah diterapkan, CCPA akan memiliki dampak terhadap penyedia jasa layanan berupa peningkatan penyimpanan data dan pemetaan definisi penjualan data pribadi, pemberian izin pemilik data untuk mengakses dan menghapus data pribadinya, pemberian izin pemilik data untuk tidak berpartisipasi dalam kegiatan penjualan data pribadinya, pembaruan persetujuan tingkat layanan dengan pihak ketiga yang mengelola data pribadi pengguna, penyelesaian celah keamanan informasi dan kelemahan sistem.³⁷

Selain itu, pemerintah juga menyiapkan panduan yang digunakan sebagai standar kebijakan TIK yang diterapkan oleh penyedia jasa layanan, seperti *National Cyber Security Center Cyber Assessment Framework (NCSC CAF guidance)* milik pemerintah Inggris. Panduan seperti NCSC CAF mewajibkan perusahaan di Inggris untuk memiliki kerangka dalam mengelola infrastruktur siber dan mencapai resiliensi siber. Hal ini termasuk: mengelola resiko siber, melindungi sistem dari serangan siber, mendeteksi peristiwa serangan dan meminimalisir dampak insiden keamanan siber.³⁸

Meski di tataran regional ASEAN belum memiliki kerangka regulasi serupa, pemerintah Indonesia telah memiliki beberapa regulasi yang ditujukan untuk melindungi data pengguna. Saat ini, pengawasan *e-commerce* mengacu pada Undang-Undang No.7 tahun 2014 tentang Perdagangan, Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dan Undang-Undang No.8 Tahun 1999 Tentang Perlindungan Konsumen. Walaupun belum terdapat peraturan yang secara



husus mengatur *e-commerce*, pemerintah RI melalui Otoritas Jasa Keuangan (OJK), telah menetapkan Peraturan Otoritas Jasa Keuangan Nomor 12/ POJK.03/Tahun 2018 Tentang Penyelenggara Layanan Perbankan Digital oleh Bank Umum.

Langkah yang telah diambil pemerintah menetapkan PJOK patut diapresiasi. Akan tetapi menjadi lebih baik bila pemerintah mampu menetapkan kebijakan yang secara khusus mengatur *e-commerce*. Sebetulnya sejak tahun 2015 pemerintah mulai menyusun Rencana Peraturan Pemerintah (RPP) *e-commerce*, namun belum kunjung disahkan. Keberadaan regulasi yang secara khusus mengatur *e-commerce* menjadi penting agar tercipta landasan hukum yang kuat untuk memfasilitasi sinergi yang lebih optimal dalam mewujudkan perlindungan data pengguna. Selain itu, tinjauan terhadap UU yang dianggap masih lemah dalam melindungi data pribadi, seperti Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik di Indonesia, perlu dilakukan. Tinjauan ini diperlukan untuk memastikan bahwa regulasi tersebut berhasil mencegah pelanggaran data pengguna layanan dan memastikan adanya efek jera terhadap pelaku kejahatan siber terhadap pengguna layanan *e-commerce* dan perbankan digital. Untuk menuntaskan permasalahan perlindungan data pengguna, pemerintah juga dapat mempertimbangkan pembentukan regu khusus pengawasan layanan *e-commerce* dan perbankan digital.

Penyedia Jasa Layanan *E-Commerce* dan Perbankan Digital

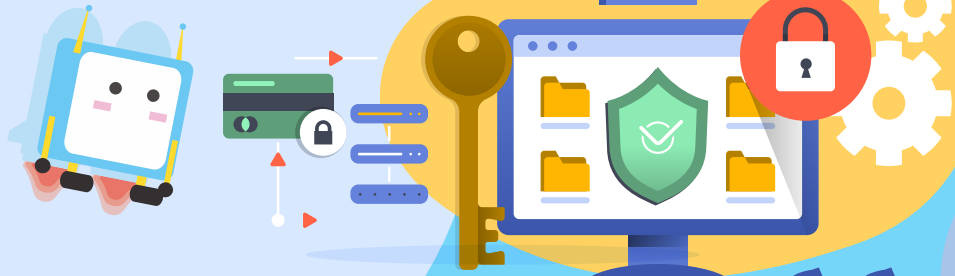
Keamanan data pengguna dalam *e-commerce* dan perbankan digital turut menjadi tanggung jawab penyedia jasa. Penyedia jasa layanan *e-commerce* dan perbankan digital, sesuai dengan regulasi yang berlaku di basis operasi penyedia layanan tersebut, dituntut untuk mampu menjamin keamanan data penggunanya. Oleh sebab itu, penyedia jasa layanan *e-commerce* dan perbankan digital memiliki standar keamanan yang disesuaikan dengan kebutuhan penggunanya. Saat *Prime Day*, sebagai contoh, *e-commerce* AS Amazon melengkapi situsnya dengan perlindungan seperti *Secure Socket Layer* (SSL), informasi *header* dan *cookie* yang aman, perlindungan surel dan *Domain Name System* (DNS) dan peningkatan integritas karyawan dan tingkat kepatuhan *Chief Executive Officer* (CEO).³⁹ Pengamanan tersebut berguna dalam melindungi serangan yang biasanya dilakukan dengan teknik yang



beragam. Pengamanan SSL yang berbasis teknik kriptografi terbaru, misalnya, akan memungkinkan jaringan komunikasi antar pengguna layanan *e-commerce* dan pengelola situs *e-commerce*. Dengan demikian, potensi serangan dengan strategi *Man in the Middle* (MITM) akan berkurang akibat ketidakmampuan pihak ketiga untuk mengintrusi jaringan. Sedangkan, *cookie* dengan sistem keamanan tertentu akan menghindarkan diri dari serangan siber yang dilakukan dengan teknik *spoofing*.

Perlindungan teknis yang disediakan oleh penyedia jasa layanan *e-commerce* dan perbankan digital menjadi penting dan merupakan tanggung jawab penyedia jasa layanan. Selain perlindungan teknis yang hanya melibatkan penyedia jasa layanan, langkah perlindungan jasa layanan yang melibatkan pengguna layanan juga bersifat krusial. Bagi penyedia jasa layanan *e-commerce* dan perbankan digital, langkah keamanan seperti ketersediaan mekanisme *second factor authentication* (2FA) yang memungkinkan autentikasi berupa kata kunci satu kali (*one-time password*/OTP) yang dikirimkan melalui SMS kepada pengguna akan membantu pengamanan transaksi yang dilakukan.⁴⁰

Dalam konteks penyedia jasa layanan *e-commerce* dan perbankan digital di Indonesia, sejumlah langkah pengamanan telah diterapkan untuk menjaga keamanan data pengguna layanan. Meski informasi mengenai langkah teknis mandiri yang telah dilakukan penyedia jasa layanan *e-commerce* dan perbankan digital tidak banyak dipublikasikan, langkah teknis yang dilakukan dengan melibatkan pengguna telah dilakukan oleh pelbagai penyedia layanan *e-commerce*, seperti Blibli⁴¹, Tokopedia⁴², Bukalapak⁴³; serta perbankan digital, seperti Jenius Banking⁴⁴. Beberapa dari fitur tersebut didapatkan oleh penyedia jasa layanan tersebut oleh karena adanya kerjasama dengan mitra yang memiliki andil dalam pengamanan data pengguna, seperti Jenius yang bekerjasama dengan Visa (dengan standar *Verified by Visa*).⁴⁵ Selain itu, penyedia jasa layanan *e-commerce* dan perbankan digital juga mendorong pengguna untuk menjaga keamanan data, misalnya saja melalui pemberian himbauan rutin untuk mengganti kata sandi akun secara berkala.





Akademisi

Akademisi juga berperan penting dalam penanggulangan kejahatan siber di Indonesia. Peran akademik dalam penanggulangan isu kejahatan siber terhadap pengguna jasa layanan adalah mengkaji isu penipuan terhadap pengguna layanan e-commerce dan perbankan digital yang menghasilkan masukan bagi aktor-aktor lain. Salah satu contoh komunitas akademik yang mendukung penelitian isu tersebut adalah *OpenNet Initiatives* (ONI) yang merupakan proyek bersama dari the Citizen Lab milik Munk School of Global Affairs di Universitas Toronto, AS; the Berkman Center for Internet and Society dari Universitas Harvard, AS; dan SecDev Group dari Ottawa, Kanada.⁴⁶ ONI berfokus pada kajian kebijakan pemerintah yang berkaitan dengan pembatasan akses dan pengawasan ruang siber.

Di Indonesia, terdapat beberapa komunitas akademisi yang berfokus pada isu penanggulangan kejahatan siber. Pusat penelitian seperti Center for Digital Society (CfDS) UGM dan Cyber for Law Center UNPAD adalah beberapa dari pusat penelitian di Indonesia yang tak hanya berkontribusi dalam tataran gagasan semata, melainkan juga memainkan peran sebagai representasi sipil yang dapat menyelaraskan keseimbangan relasi kuasa dalam mewujudkan pengamanan data pengguna. CfDS UGM, sebagai contoh, berupaya memberikan rekomendasi bagi pemerintah melalui kajian-kajian, seperti CfDS Case Study dan CfDS Digitimes, serta berupaya menyediakan ruang diskusi antar pengambil kebijakan mengenai isu keamanan siber dalam acara, seperti CfDS Convention on Cybersecurity.⁴⁶ Akademisi dapat mengkaji dampak serta berbagai kebijakan yang berhubungan dengan kejahatan siber dan keamanan data pengguna, terlibat aktif dalam perumusan kebijakan terkait isu-isu tersebut, serta mengedukasi masyarakat untuk meningkatkan kesadaran pengguna melalui pengarusutamaan isu keamanan data pengguna.

Komunitas

Komunitas turut memiliki peranan penting dalam dalam penanggulangan kejahatan siber di Indonesia. Peran komunitas dalam penanggulangan isu kejahatan siber terhadap pengguna jasa layanan adalah meningkatkan kesadaran masyarakat terkait isu kejahatan siber dan keamanan data, memastikan regulasi berlaku hingga ke level akar rumput, dan berkontribusi pada penyusunan regulasi. Tak hanya itu, komunitas juga menjadi representasi sipil yang mampu menyelaraskan keseimbangan relasi kuasa dalam mewujudkan pengamanan data pengguna.

Beberapa contoh komunitas yang gencar mengawal isu kejahatan siber dan keamanan data antara lain adalah; European Digital Rights (EDRi)⁴⁸, Electronic Frontier Foundation (EFF), dan Defenders Protection Initiative. Sebagai contoh, EFF berupaya menyuarakan perubahan pada UU Penipuan dan Penyalahgunaan Komputer AS (*Computer Fraud and Abuse Act/CFAA*) yang dianggap bermasalah dan berpotensi melanggar hak asasi manusia setelah salah satu aktivis *hacking* AS, Aaron Schwartz, meninggal dunia secara tragis.⁴⁹ Upaya pengawalan kebijakan pemerintah maupun penyedia jasa layanan *e-commerce* dan perbankan digital menjadi penting untuk menjaga agar kebijakan tersebut menasar objek yang benar.

Sedangkan itu beberapa komunitas di Indonesia juga menyuarakan isu kejahatan siber dan keamanan data. Komunitas yang berbasis nasional, seperti Indonesia Cyber Security Forum (ICSF) dan Information Communication Technology Watch (ICT Watch); maupun yang berbasis daerah, seperti Info Cegatan Jogja (ICJ),⁵⁰ turut serta dalam upaya perlindungan data pengguna. Mengenai permasalahan kejahatan siber terhadap pengguna *e-commerce* dan perbankan digital, Ardi Sutedja selaku Ketua ICSF sempat mengingatkan para penyedia jasa layanan *e-commerce* untuk



tidak meremehkan isu peretasan data mengingat pelbagai kasus serupa telah kerap terjadi di luar Indonesia.⁵¹ Di tingkat daerah, ICJ menyediakan forum (melalui media sosial Facebook) bagi masyarakat untuk saling berbagi mengenai pelbagai isu, termasuk isu kejahatan siber yang melibatkan *platform e-commerce* dan perbankan digital.

Dengan demikian, secara garis besar, komunitas-komunitas berkontribusi terhadap perlindungan data pengguna layanan *e-commerce* dan perbankan digital dengan meningkatkan kesadaran masyarakat mengenai perlindungan data pribadi dengan mensosialisasikan perilaku yang bijak mengenai data pribadi, mendorong pemerintah dan penyedia jasa layanan *e-commerce* dan perbankan digital untuk melindungi data pengguna, serta mengawasi kebijakan pemerintah dan penyedia jasa layanan *e-commerce* dan perbankan digital.

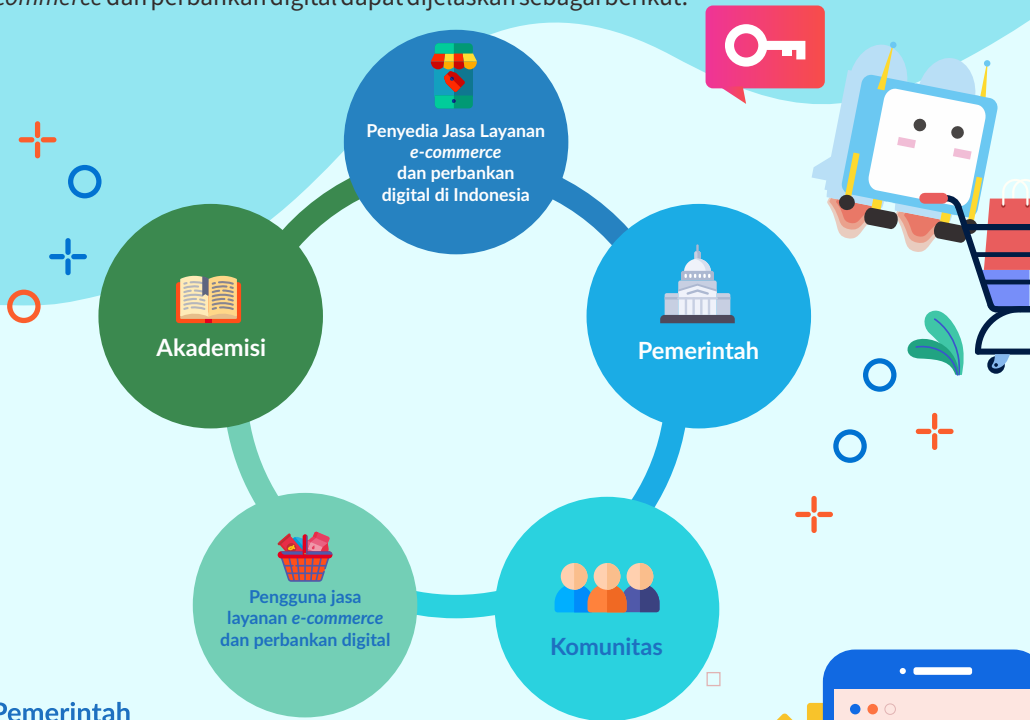
Pengguna Layanan E-Commerce dan Perbankan Digital

Pengamanan data pengguna merupakan hak pengguna layanan *e-commerce* dan perbankan digital. Hak tersebut telah dijamin melalui serangkaian regulasi yang telah ditetapkan pemerintah. Penyedia jasa layanan *e-commerce* dan perbankan digital pun telah mengakomodasi hak tersebut melalui penerapan berbagai sistem pengamanan data pengguna yang terus diperbaharui agar pengamanan yang diberikan semakin optimal. Namun, segala upaya tersebut akan menjadi sia-sia bila tidak disertai dengan peran serta pengguna dalam menjaga keamanan data pribadinya.

Menurut sebuah survei yang dilakukan pada tahun 2016 tentang *Data Breaches and Customer Loyalty*, 70% pengguna merasa bahwa keamanan data pengguna merupakan tanggung jawab penyedia jasa layanan.⁵² Cara pandang demikian membuat pengguna merasa tidak perlu ambil bagian dan menyerahkan tindakan pengamanan data pribadi kepada penyedia jasa sepenuhnya. Pengguna dapat menjadi abai mengikuti protokol pengamanan data pribadi yang disediakan oleh penyedia jasa layanan, mengakibatkan upaya pengamanan data pengguna menjadi tidak optimal.

Berdasarkan pemaparan di atas, maka sudah sepatutnya pengguna layanan *e-commerce* dan perbankan digital turut terlibat aktif dalam melindungi keamanan data pribadi. Sebagai contoh, sebagian kecil tindakan yang dapat dilakukan oleh pengguna adalah dengan tidak menggunakan satu *email* untuk pelbagai kepentingan, menjaga kerahasiaan data pribadi,⁵³ meningkatkan keamanan kata sandi dengan secara rutin melakukan penggantian kata sandi secara berkala, membuat kata sandi yang rumit dan unik (serta bila perlu menggunakan manajemen kata sandi) dan selalu waspada dan berhati-hati tatkala menggunakan layanan *e-commerce* dan perbankan digital.

Secara ringkas, peran setiap aktor dalam perlindungan data pengguna *e-commerce* dan perbankan digital dapat dijelaskan sebagai berikut:



Pemerintah

- Penetapan regulasi *e-commerce*.
- Menetapkan regulasi panduan bagi penyedia jasa layanan untuk mencapai resiliensi siber.
- Membentuk *task force* pengawasan layanan *e-commerce* dan perbankan digital.
- Menyusun regulasi yang memberikan efek jera terhadap para pelaku kejahatan siber pengguna layanan *e-commerce* dan perbankan digital.

Penyedia Jasa Layanan *e-commerce* dan perbankan digital di Indonesia

- Inovasi teknologi untuk keamanan pengguna
- Memenuhi standar keamanan yang diakui secara internasional.
- Mematuhi peraturan yang ditetapkan oleh Pemerintah Indonesia.
- Bekerjasama dengan mitra terpercaya dalam memberikan layanan jasa kepada pelanggan.
- Mendorong pengguna untuk menjaga keamanan data, misalnya saja melalui pemberian himbauan rutin untuk mengganti kata sandi akun secara berkala.

Akademisi

- Mengkaji kebijakan dan dampak kejahatan siber terkait pengguna layanan *e-commerce*, perbankan digital, dan keamanan data pengguna.
- Terlibat aktif dalam perumusan kebijakan, sehingga tercipta kebijakan terkait layanan *e-commerce*, perbankan digital, dan keamanan data pengguna yang komprehensif.
- Meningkatkan kesadaran masyarakat melalui pengarusutamaan isu keamanan data pengguna.

Komunitas

- Membantu sosialisasi mengenai data pribadi masyarakat.
- Meningkatkan kesadaran masyarakat mengenai perlindungan data pribadi.
- Melakukan advokasi isu perlindungan data pengguna. Memantau dan mengawasi penerapan kebijakan pemerintah, baik di tingkat nasional maupun hingga akar rumput.
- Mendorong penyedia jasa layanan *e-commerce* dan perbankan digital dalam melakukan perlindungan data pengguna yang optimal.

Pengguna jasa layanan *e-commerce* dan perbankan digital

- Lebih waspada terhadap keamanan datanya, misalnya dengan a) tidak menggunakan satu email untuk pelbagai kepentingan, b) menjaga kerahasiaan data pribadi, c) meningkatkan keamanan kata sandi dengan rutin melakukan penggantian kata sandi secara berkala, d) membuat kata sandi yang rumit dan unik, serta e) bila perlu menggunakan manajemen kata sandi.
- Selalu waspada dan berhati-hati tatkala menggunakan layanan *e-commerce* dan perbankan digital.

Kesimpulan

Mempertimbangkan berbagai penjelasan sebelumnya, studi ini berargumen bahwa perlindungan data pengguna layanan *e-commerce* dan perbankan digital di Indonesia dapat diupayakan dengan kolaborasi *pentahelix* yang terdiri dari pemerintah, penyedia jasa layanan *e-commerce* dan perbankan digital, akademisi, komunitas, serta pengguna layanan. Pemerintah memiliki peran besar di tataran regulasi dan edukasi, penyedia jasa bertanggung jawab untuk inovasi teknologi keamanan, akademisi dan komunitas dapat berkontribusi melalui advokasi isu, formulasi kebijakan, serta pendekatan edukasi kepada masyarakat, dan pengguna memiliki tanggung jawab untuk menjadi lebih sadar dan berhati-hati dalam menjaga keamanan datanya.

Studi ini juga melihat bahwa kerjasama yang dilakukan antar aktor juga diperlukan untuk menyediakan perlindungan yang lebih kuat. Kerjasama menjadi penting untuk dilakukan dalam konteks perlindungan data pengguna oleh karena adanya keterbatasan yang dimiliki oleh setiap aktor. Sebagai contoh, meski memiliki

kajian yang memiliki validitas akademik yang mumpuni, akademisi barangkali memiliki kesulitan dalam mempublikasikan penelitiannya pada tingkat keluasaan tertentu. Meskipun memiliki teknologi inovasi yang mumpuni, penyedia jasa layanan mungkin tidak akan mampu melakukan edukasi secara menyeluruh kepada masing-masing penggunaannya. Dengan demikian, studi lanjutan mengenai perlindungan data konsumen dapat mencoba merumuskan tingkat kesadaran pengguna atas keamanan datanya serta kerangka kerjasama yang mendukung upaya perlindungan data pengguna layanan e-commerce dan perbankan digital di Indonesia.

Referensi

¹Das, K., Tamhane, T., Vatterott, B., Wibowo, P., & Wintels, S. (2018). The digital archipelago: ²How online commerce is driving Indonesia's economic development. McKinsey & Company, August. We Are Social. (2019). Digital 2019 Indonesia. Tersedia di https://datareportal.com/digital-in-indonesia?utm_source=Reports&utm_medium=PDF&utm_name=Digital_2019&utm_content=Country_Link_Slide [diakses pada 31 Oktober 2019]

³Rahmadiani A., Mantovani, A. P. K., Hariz, S. U., Haryanto, J., dan Aidad, F. F., (2018). Strategi Keamanan Siber Indonesia. CfDS Digitimes [daring] Vol. 21. Hal. 4. Tersedia di <http://cfds.fisipol.ugm.ac.id/publications/3-2473>. [Diakses pada 31 Oktober 2019].

⁴Ibid.

⁵CNN Indonesia, (2019). Polri Catat 3.000 Kasus Kejahatan Siber Hingga Agustus 2019. CNN Indonesia [daring] Tersedia di <https://www.cnnindonesia.com/teknologi/20191029183819-185-443890/polri-catat-3000-kasus-kejahatan-siber-hingga-agustus-2019>. [Diakses pada 31 Oktober 2019].

⁶Macrae, F. (2007). Pace of life speeds up as study reveals we're walking faster than ever. Daily Mail [daring] Tersedia di <http://www.dailymail.co.uk/sciencetech/article-452046/Pace-life-speeds-study-reveals-walking-faster-ever.html> [Diakses pada 30 Okt 2019].

⁷Brown, D. S. (2014). Society's self-destructive addiction to faster living. NY Post [daring] Tersedia di <http://nypost.com/2014/01/04/societys-addiction-to-faster-living-is-destroying-us-doctor/> [Diakses pada 30 Okt. 2019].

⁸Schiff, P. D., & Schiff, A. (2010). How an economy grows and why it crashes: a tale. Hoboken, New Jersey: Wiley.

⁹Jurriëns, E., & Tapsell, R. (Eds.). (2017). Digital Indonesia: connectivity and divergence. ISEAS-Yusuf Ishak Institute.

¹⁰Ibid.

¹¹ITU, (2012). Understanding cybercrime: Phenomena, challenges and legal response. [daring] Tersedia di <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf>, hal. 12.

¹²Lebih lanjut mengenai penipuan berbasis komputer di AS, lihat

¹³Lebih lanjut mengenai penipuan berbasis internet di Australia, lihat Police.act.gov.au. (n.d.).

Internet Fraud [daring] Tersedia di <https://police.act.gov.au/sites/default/files/PDF/bizsafe-internet-fraud-factsheet.pdf>.

¹⁴ Lebih lanjut mengenai tipe penipuan terhadap pengguna layanan e-commerce dan perbankan digital, lihat NETS, (2019). European Online Fraud Report 2019. NETS [daring] Tersedia di <https://www.nets.eu/solutions/fraud-and-dispute-services/Documents/Nets-Fraud-Report-2019.pdf>, hal. 36.

¹⁵ Rahmadiani, A., hal. 4.

¹⁶ Avast.com. (2019). Cracking [daring] Tersedia di <https://www.avast.com/c-cracking> [Diakses pada 4 Nov. 2019].

¹⁷ Robitzski, D. (2019). HACKERS ARE CRACKING ONLINE BANKING SITES TO STEAL YOUR CASH. Futurism [daring] Tersedia di <https://futurism.com/the-byte/hackers-cracking-online-banking-systems-steal> [Diakses pada 4 Nov. 2019].

¹⁸ Zakaras, M. R. (2001). International computer crime. International Review of Penal Law [daring] Vol. 72(3-4) Tersedia di <https://www.cairn.info/revue-internationale-de-droit-penal-2001-3-page-813.htm#>, hal. 818

¹⁹ Lebih lanjut mengenai kasus peretasan Citibank pada tahun 1994, lihat Goldstone, D., dan Shave, B. (1999). International Dimensions of Crime in Cyberspace. Fordham International Law Journal [daring] Vol. 22(5) Tersedia di <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1638&context=ilj>.

²⁰ Lebih lanjut mengenai kasus leaking di Amazon, lihat Emont, J., Stevens, L., dan McMillan, R. (2018). Amazon Investigates Employees Leaking Data for Bribes. Wall Street Journal [daring] Tersedia di <https://www.wsj.com/articles/amazon-investigates-employees-leaking-data-for-bribes-1537106401>.

²¹ Kementerian Pertahanan AS, (2018). Security Tip (ST04-015) Understanding Denial-of-Service Attacks [daring] Tersedia di <https://www.us-cert.gov/ncas/tips/ST04-015> [Diakses pada 4 Nov. 2019].

²² Innab, N., dan Alamari, A. (2018). The Impact of DDoS on E-Commerce. Dalam 2018 21st Saudi Computer Society National Computer Conference (NCC) [daring] Tersedia di DOI: 10.1109/NCG.2018.8593125., hal. 2.

²³ Lebih lanjut mengenai phishing, lihat Kim, D., dan Solomon, M. G. (2018). Fundamentals of Information Systems Security. Burlington: Jones & Bartlett Learning, p. 97.

²⁴ Ibid., hal. 3.

²⁵ Lihat Zakaras, hal. 819.

²⁶ Alsayed, A. O., dan Bilgrami, L. (2017). E-Banking Security: Internet Hacking, Phishing Attacks, Analysis and Prevention of Fraudulent Activities. International Journal of Emerging Technology and Advanced Engineering [daring] Vol. 7(1), ISSN 2250-2459, hal. 110.

²⁷ Lord, N. (2019). Social Engineering Attacks: Common Techniques & How to Prevent an Attack. Digital Guardian [daring] Tersedia di <https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack> [Diakses pada 5 Nov 2019].

²⁸ Kim dan Solomon, hal. 85.

²⁹ Berdasarkan pemaparan Kombes Polri Ricky pada CfDS Convention on Cybersecurity pada tahun 2018, lihat Ricky. (2018). Bareskrim Polri Tindak Pidana Siber.

³⁰ Ibid.

³¹ Lebih lanjut mengenai zero-day attack, lihat Kello, L. (2017). *The Virtual Weapon and International Order*. New Haven: Yale University Press, hal. 48.

³² Yunas, N. S., (2019). Implementasi Konsep Penta Helix dalam Pengembangan Potensi Desa melalui Model Lumbung Ekonomi Desa di Provinsi Jawa Timur. *Matra Pembaruan: Jurnal Inovasi Kebijakan*, 3(1), pp.37-46.

³³ Ibid.

³⁴ Mengenai informasi lebih lanjut terkait GDPR, lihat EU, (n.d.). EU GDPR. ORG. [daring] Tersedia di <https://eugdpr.org/>.

³⁵ Microsoft 365 Team. (2019). GDPR compliance and small business [daring] Tersedia di <https://www.microsoft.com/en-us/microsoft-365/growth-center/resources/gdpr-compliance-and-small-business> [Diakses pada 5 Nov. 2019].

³⁶ Lihat Chabitsky, S., dan Pittman, F. P., (2019). *The ICLG to: Data Protection Laws and Regulations*. ICLG [daring] Tersedia di <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa>.

³⁷ Lebih lanjut mengenai dampak CCPA terhadap perusahaan yang berada di area Kalifornia serta perbandingannya dengan GDPR, lihat PwC. (2019). *Your readiness roadmap for the California Consumer Privacy Act (CCPA)*. [daring] Tersedia di <https://www.pwc.com/us/en/services/consulting/cybersecurity/california-consumer-privacy-act.html>.

³⁸ Lebih lanjut mengenai NCSC CAF Inggris, lihat National Cyber Security Center (NCSC), (2019). *NCSC CAF guidance*. [daring] Tersedia di <https://www.ncsc.gov.uk/collection/caf/cyber-assessment-framework>.

³⁹ Lebih lanjut mengenai upaya Amazon mengamankan situsnya pada saat Prime Day, lihat UpGuard, (2019). *Prime Day: How Amazon Handles Cybersecurity*. [daring] Tersedia di <https://www.upguard.com/blog/prime-day-how-amazon-handles-cybersecurity>.

⁴⁰ Lebih lanjut mengenai 2FA dan OTP, lihat DBS Vickers Security, (n.d.) *2FA Implementation FAQ (Singapore Accounts)*. [daring] Tersedia di <https://www.dbs.com.sg/vickers/en/resources/faq/second-factor-authentication-2fa>.

⁴¹ Lebih lanjut mengenai keamanan akun di BliBli, lihat BliBli.com, (n.d.). *Pusat Bantuan*. [daring] Tersedia di <https://www.blibli.com/faq/topic/registrasi-info/keamanan-akun/>

⁴² Lebih lanjut mengenai keamanan akun di Tokopedia, lihat Tokopedia.com, (n.d.) *Pusat Bantuan Tokopedia*. [daring] Tersedia di <https://www.tokopedia.com/help/search?q=OTP&refid=pg-11>

⁴³ Lebih lanjut mengenai keamanan akun di Bukalapak, lihat Bukalapak.com, (n.d) *Tanya Jawab*. [daring] Tersedia di <https://www.bukalapak.com/bantuan>

⁴⁴ Lebih lanjut mengenai OTP Jenius Banking, lihat Isabella, C. (2019). *Pahami Pentingnya Merahasiakan Kode OTP. Jenius* [daring] Tersedia di <https://www.jenius.com/highlight/detail/pahami-pentingnya-merahasiakan-kode-otp>.

⁴⁵ Lebih lanjut mengenai Verified by Visa Jenius, lihat Isabella, C. (2017). *Aman Bertransaksi Online dengan Kartu Debit Jenius Visa. Jenius* [daring] Tersedia di <https://www.jenius.com/highlight/detail/aman-bertransaksi-online-dengan-kartu-debit-jenius-visa>.

⁴⁶ Lebih lanjut mengenai ONI, lihat About ONI, (n.d.) *OpenNet Initiatives* [daring] Tersedia di <https://opennet.net/about-oni>.

⁴⁷ Lebih lanjut mengenai CfDS UGM, lihat Home, (n.d). *Center for Digital Society UGM* [daring] Tersedia di <https://www.cfds.fisipol.ugm.ac.id>.

⁴⁸Lebih lanjut mengenai EDRi lihat About, (n.d.) European Digital Rights [daring] Tersedia di <https://edri.org/about/>.

⁴⁹Lebih lanjut mengenai upaya EFF dalam mengubah CFAA, lihat EFF, (n.d.) Computer Fraud And Abuse Act Reform. [daring] Tersedia di <https://www.eff.org/issues/cfaa>.

⁵⁰Info Cegatan Jogja (ICJ) merupakan sebuah komunitas masyarakat yang berbasis di Facebook, dan merupakan salah satu komunitas terbesar di Yogyakarta. ICJ kerap menjadi tempat masyarakat mengadukan tindak kejahatan siber dan penyalahgunaan data pribadi yang menyimpannya. Namun dalam beberapa kesempatan ICJ turut menyebarkan data pribadi secara tidak konsensual.

⁵¹Syarizka, D. (2019). Perusahaan Dagang-El Diminta Jangan Remehkan Isu Peretasan Data. Bisnis.com [daring] Tersedia di <https://teknologi.bisnis.com/read/20190324/84/903638/perusahaan-dagang-el-diminta-jangan-remehkan-isu-peretasan-data> [Diakses pada 5 Nov. 2019].

⁵²Gemalto. (2017). Consumers vs Businesses Consumers are increasingly aware of online security risks, but hold businesses responsible for data breaches. Gemalto.

⁵³Oleh karena Indonesia masih merumuskan UU Perlindungan Data Pribadi yang akan menjadi tolak ukur bagi terminologi data pribadi, data pribadi dapat dirujuk sebagai Personal Data yang digunakan pemerintah UE, atau Personally Identifiable Information (PII) digunakan oleh pemerintah AS.





Center for Digital Society

Faculty of Social and Political Sciences
Universitas Gadjah Mada
Room BC 201-202, BC Building 2nd Floor,
Jalan Socio Yustisia 1
Bulaksumur, Yogyakarta, 55281, Indonesia

Phone : (0274) 563362, Ext. 116

Email : cfds.fisipol@ugm.ac.id

Website : cfds.fisipol.ugm.ac.id

 facebook.com/cfdsugm

 Center for Digital Society (CfDS)

 [cfds_ugm](https://www.instagram.com/cfds_ugm)

 [@cfds_ugm](https://twitter.com/cfds_ugm)

 [@cfds_ugm](https://twitter.com/cfds_ugm)

 CfDS UGM