STRATEGI PENGAMANAN PRIVASI: STUDI PADA PENGGUNA BERAT INTERNET DI MASA PANDEMI COVID-19

Paulus Angre Edvra[1], Birgitta B. Puspita[2]
Universitas Gadjah Mada[1], Universitas Atma Jaya Yogyakarta[2]
Email: paulusangreedvra@mail.ugm.ac.id, birgitta.puspita@uajy.ac.id[*]

Abstrak: Pandemi COVID-19 membuat konsumsi seseorang pada internet meningkat yang menciptakan masalah soal keamanan data pribadi. Semakin banyak konsumsi internet, semakin banyak data yang dipantau dan dikumpulkan oleh sistem Big Data. Peneliti mengeksplorasi langkah-langkah yang dilakukan para pengguna berat internet agar tetap bisa berinternet dengan data aman. Penelitian kualitatif ini menggunakan teknik pengumpulan data wawancara kepada tujuh pengguna berat internet. Hasil menunjukkan bahwa peningkatan konsumsi selama pandemi tak terelakkan. Pengguna internet juga paham tentang adanya pemantauan atas aktivitas daring mereka, dan mereka maklumi karena sudah tertulis di kebijakan privasi aplikasi. Sementara, terkait kebocoran data para pengguna sudah melakukan sejumlah strategi pengamanan.

Kata Kunci: Ancaman privasi; Big Data; pandemi COVID-19; pemantauan daring; pengguna berat internet

Abstract: The COVID-19 pandemic has increased the consumption of the internet which creates problems regarding the security of personal data. The more internet consumption, the more data collected and monitored by the Big Data system. The researcher explores the steps taken by heavy internet users so that they can still surf the internet with safe data. This qualitative research uses interview data collection techniques to seven heavy internet users. The results show that increased consumption during the pandemic is inevitable. Internet users also understand that there is monitoring of their online activity because it is written in the applications' privacy policy. Meanwhile, regarding data leakage, users have taken several safety strategies.

Keywords: Big Data; COVID-19; Heavy internet users; Online surveillance; Privacy threat

PENDAHULUAN

Pertumbuhan penggunaan internet selama pandemi COVID-19 membuat banyak pengguna memasang banyak aplikasi baru di gawai mereka. Hal ini tak terelakkan, mengingat segala kegiatan selama pandemi dilakukan secara daring sehingga pengunduhan aplikasi penting untuk membantu kegiatan seseorang. Salah satu indikasi bahwa pengunduhan aplikasi serta penggunaan aplikasi tersebut bisa ditunjukkan melalui adanya peningkatan penggunaan internet. Staf Khusus Bidang Kebijaksanaan Digital dan Sumber Daya Manusia Kementerian Komunikasi dan Informatika (Kemenkominfo), Dedy Permadi, menyatakan bahwa penggunaan internet di wilayah pemukiman meningkat sekitar 30-40% (Prasetyani, 2021). Hal yang sama diungkapkan juga oleh Pengamat Teknologi Informasi dan Telekomunikasi, Heru Sutadi yang menyebut penggunaan internet di Indonesia meningkat 40% (Salim, 2021). Laporan dari

*Corresponding author

Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) bahkan menyebutkan peningkatan lebih

tinggi, yakni 73,7% pada kuartal II 2020. Peningkatan ini terjadi sebanyak 29,3% pada bidang komunikasi, 24,7% di bidang media sosial, 9,7% untuk hiburan, 7,6% untuk layanan publik, dan 4,8% untuk belanja daring (Prasetyani, 2021).

Dari beberapa kategori yang disebutkan APJII di atas, sektor belanja daring menjadi salah satu yang paling drastis meningkat selama 2020. Staf Ahli Kemenkominfo, Henry Subiakto, menyatakan bahwa belanja daring meningkat 400% dan penggunaan dompet elektronik seperti OVO dan GoPay meningkat 40% selama 2020 (Cindy, 2021).

Selain belanja daring, sejumlah data menyebutkan peningkatan internet di Indonesia juga terjadi di televisi internet dan aplikasi kesehatan. Head of Communication, Hi-Tech, and Media Industry MarkPlus Inc., Rhesa Prabowo, menjelaskan bahwa ada peningkatan konsumsi Pay TV dari 22,7% menjadi 26,4% pandemi COVID-19 (Soenarso, 2020). Pengunduh aplikasi kesehatan seperti Halodoc juga meningkat 10 kali lipat selama pandemi (Fitri, 2020).

Tingginya peningkatan jumlah pengunduh dan pemasang aplikasi ini berimplikasi pada data pengguna yang harus disetorkan untuk registrasi akun. Data-data seperti nama, nomor HP, tanggal lahir, dan alamat email menjadi empat data yang seolah wajib didaftarkan. Data-data ini semestinya dijaga oleh perusahaan, namun fakta di Indonesia tidak menunjukkan keamanan yang baik dari para perusahaan aplikasi. Sudah banyak kasus kebocoran data yang terjadi di aplikasi dan situs di mana warga memasrahkan data mereka.

Salah satu kasus yang terjadi pada pertengahan 12 Mei 2021 adalah bocornya data 279 juta penduduk Indonesia (Roy, 2021). Kasus di atas bukanlah satu-satunya kejadian di mana data warga Indonesia bocor. Ada kejadian lain yang bisa kita lacak di internet soal kebocoran data, seperti bocornya data 91 juta pengguna Tokopedia (Alfianto, 2020), kebocoran 13 juta data pengguna Bukalapak (Kumparan, 2020), dugaan bocornya data di aplikasi PeduliLindungi (Farisa, 2021).

Tak hanya soal data pribadi, di internet semua aktivitas kita juga dipantau dan ada informasi personal kita yang dicatat secara otomatis saat kita beraktivitas di suatu situs atau aplikasi. Terkadang data bisa dipantau dengan sangat mudah saat banyak warga memberi data pribadi secara cuma-cuma di media sosial. Sebagai contoh adalah fitur stiker "Add Yours" di Instagram. Lewat fitur ini, pengguna bisa saling berbalas pesan lewat postingan Insta Story dan belakangan kerap dijadikan challenge oleh para

pengguna. Beberapa tantangan yang muncul antara lain: menunjukkan foto zaman kecil, dan variasi nama panggilan. Netizen yang tertarik untuk menggunakan fitur ini akhirnya menyebar data seputar informasi yang diminta tanpa memahami risikonya. Hasilnya, pada 23 November 2021 ada kasus penipuan menggunakan nama panggilan kecil korban. Nama itu didapat pelaku dari unggahan "Add Yours" korban (CNN Indonesia, 2021).

Melihat paparan data di atas, tampak bahwa ada ancaman privasi yang berbahaya jika pengguna tidak melindungi datanya sendiri. Penelitian ini ingin mengeksplorasi bagaimana aktivitas pengguna internet di Indonesia selama pandemi COVID-19 dan bagaimana strategi pengamanan data pribadi mereka di internet. Pengguna internet yang diteliti adalah pengguna berat. Level pengguna berat ini merujuk pada tulisan Ilakkuvan dan kolega (2019, dalam Hruska dan Maresova, 2020), yakni mereka yang mengonsumsi internet, khususnya media sosial lebih dari tiga jam tiap harinya dan biasanya berusia 18 hingga 29 tahun.

Tujuan dari penelitian ini adalah untuk melihat aktivitas internet para pengguna berat internet selama pandemi, mengeksplorasi pemahaman mereka atas isu-isu privasi dan pemantauan di internet, dan mengeksplorasi cara-cara pengamanan data pribadi yang mereka lakukan di internet. Hal ini berdasar pada kajian-kajian sebelumnya yang menjadi dasar atas penelitian ini. Penelitian oleh Appel (2012) terkait literasi media pada pengguna berat internet lebih berfokus kepada kecenderungan peningkatan kemampuan bermedia atau memanfaatkan media dalam hal ini komputer, tetapi tidak berfokus pada kemampuan literasi tentang privasi. Sementara, internet tidak semata tentang kecakapan menggunakan medianya saja tetapi juga melindungi data pribadi, Sementara itu, penelitian yang dilakukan oleh De Kimpe, Walrave, Verdegen, dan Ponnet (2022) menyatakan bahwa pengguna berat internet di Belgia merasa bahwa mereka well-informed tentang internet dan risikonya, sehingga mereka lebih cenderung kurang merasa rentan atas kemungkinan menjadi korban kejahatan siber dan kurang mengambil langkah-langkah keamanan untuk melindungi dirinya di dunia siber.

Dari penelitian sebelumnya tersebut, penelitian ini akan lebih menggali strategi pengaman digital terkait privasi yang belum dieksplorasi. Selain itu, walauapun pengguna berat cenderung merasa aman di dunia digital karena kecukupan informasi yang mereka miliki, belum tentu mereka tidak memiliki strategi khusus untuk mengamankan data mereka. Maka, penelitian ini bertujuan untuk mengeksplorasi cara pengamanan yang dikembangkan oleh para pengguna berat yang berdomisili di Pulau Jawa untuk melindungi dirinya di dunia siber. Adanya data soal strategi pengamanan ini nantinya bisa direplikasi oleh pengguna lain agar data mereka juga aman.

Internet di Masa Pandemi

Pandemi COVID-19 terjadi di seluruh dunia dan memengaruhi penggunaan internet di seluruh benua. World Economic Forum menjabarkan bahwa penggunaan data seluler global selama 2020 mengalami peningkatan lebih dari 30% dibandingkan 2019, dan pertumbuhannya di 2021 tak jauh berbeda dengan angka di 2020 (Myers, 2021). Internet menjadi sarana yang krusial selama pandemi untuk meningkatkan kualitas hidup seseorang dan memungkinkan adanya interaksi dan transaksi terdesentralisasi selama kebijakan pembatasan sosial berlaku. Transaksi terdesentralisasi terwujud dalam aktivitas belanja daring. Penelitian Shengyu Gu dan kolega menyebutkan bahwa selama pandemi, konsumen berkomitmen menjadikan kegiatan belanja daring seperti

belanja harian (Gu et al., 2021). Di Indonesia, kunjungan di lima situs belanja daring selama 2020 menunjukkan angka yang tinggi, di mana Lazada diakses sebanyak 445,5 juta kali, Shopee 836,1 juta kali, Tokopedia 1,2 miliar kali, Bukalapak 823,5 juta kali, dan Blibli sebanyak 353,2 juta kali (Iriani & Andjarwati, 2020).

Tak hanya belanja daring, penggunaan media sosial juga meningkat selama pandemi. Statista Research Department menyatakan bahwa rata-rata pengguna media sosial di Amerika Serikat menghabiskan waktu sebanyak 65 menit untuk bermedia sosial pada 2020. Rerata ini meningkat dari tahun sebelumnya yakni 54 menit (Statista, 2021). Di satu sisi, media sosial di masa pandemi bisa jadi sarana pertukaran informasi penting di masa darurat, seperti jadi sarana informasi ketersediaan rumah sakit dan oksigen selama krisis pandemi. Di sisi lain, media sosial juga menjadi wadah penyebaran informasi salah seputar pandemi (Yas et al., 2021).

Aktivitas belanja daring dan menggunakan media sosial bisa meninggalkan masalah keamanan data bila tidak berhati-hati. Pengguna situs dan aplikasi belanja daring aktif mendaftarkan diri ke perusahaan belanja daring agar bisa berbelanja daring. Sayangnya, ada catatan buruk soal kebocoran data dari perusahaan belanja daring ini. Belum lagi, pengelolaan kemasan paket belanja yang tidak baik juga bermasalah bagi keamanan data. Di media sosial, adanya tuntutan untuk di rumah saja selama pandemi membuat beberapa orang memproduksi konten dari dalam rumah. Jika tidak hati-hati, kamera akan menangkap informasi seputar tempat tinggal tanpa disadari dan ini bisa dipantau oleh pihak yang tidak diharapkan.

Big Data dan Pemantauan

Boyd dan Crawford (2012) memandang Big Data sebagai fenomena budaya, teknologi, dan ilmiah, yang bertumpu pada interaksi antara: (1) teknologi yang mengumpulkan, menganalisis, menautkan, dan membandingkan sejumlah data; (2) analisis untuk menggambarkan dan mengidentifikasi pola untuk membuat keputusan; dan (3) mitos atau kepercayaan bahwa kumpulan data besar menawarkan bentuk kecerdasan dan pengetahuan baru. Sementara, McKinsey Global Institute (dalam Kubina, Varmus, & Kubinova, 2015) mendefinisikan Big Data sebagai sekumpulan data yang secara jumlah melebihi kemampuan perangkat database biasa yang menangkap, menyimpan, mengelola, dan menganalisis. Lalu, De Mauro, Greco, dan Grimaldi (2015) memandang Big Data sebagai aset informasi yang dicirikan oleh 3V's: volume, kecepatan (velocity), dan variasi yang tinggi sehingga memerlukan teknologi dan metode analisis tertentu untuk mengubahnya menjadi nilai.

Boyd dan Crawford (2012) mempertanyakan lebih lanjut soal kehadiran Big Data. Mereka berargumen bahwa perlu untuk secara kritis mengintrogerasi fenomena Big Data, asumsi, dan bias yang ada di dalamnya. Ada enam poin terkait Big Data yang patut untuk dikritisi, di antaranya menyoal etika dalam mengumpulkan dan mengolah Big Data, dan soal pihak terbatas yang bisa mengakses Big Data.

Perkembangan Big Data juga tidak bisa dipungkiri mengubah pola pemantauan daring yang dilakukan oleh berbagai pihak seperti pemerintah atau sistem pengamanan negara. Gary T. Marx (dalam Fuchs, et al., 2011) menyebut pemantauan daring sebagai penggunaan sarana teknis untuk mengekstrasi atau mengambil data pribadi.

David Lyon (2014) menyatakan bahwa munculnya Big Data membuat sejumlah data menjadi mungkin untuk dikumpulkan. Tak hanya data yang baru, data itu juga dikumpulkan dengan cara baru dan diolah dengan teknik yang baru. David Lyon menyatakan bahwa ada tiga konsekuensi dari

pemantauan daring lewat Big Data, yaitu (Lyon, 2014):

a.Otomatisasi: Big Data dengan sistem algoritmanya menciptakan human-algorithm yang kemudian menciptakan sistem di mana tiap orang diperilakukan dalam sistem pemantauan otomatis. Ini menjadikan pemantauan muncul sebagai prosedur manajeman rutin.

b.Antisipasi: Big Data mampu memberikan rekomendasi antisipatif soal apa yang akan terjadi. Rekomendasi ini muncul dari pengolahan menggunakan kekuatan statistika yang didukung data dalam jumlah sangat besar. Kemampuan ini membuat Big Data dipakai untuk 'meramalkan' masa depan ketimbang fokus pada masa lalu atau saat ini.

c.Adaptasi: Hasil pengolahan Big Data seolah memberi solusi bagi beberapa pihak untuk dapat menyesuaikan diri dengan lingkungan yang dipantau.

Pengamanan Privasi dan Data Pribadi Selama Pandemi

Privasi dan keamanan data pribadi saat pandemi penting untuk dibahas. Pasalnya, pandemi telah membuat kehadiran internet lebih meresap dalam kehidupan manusia (Veliz, 2020). Namun, aktivitas daring di Indonesia belum diimbangi dengan perlindungan hukum terhadap data pribadi setiap orang (Rahmatullah, 2021). Pemantauan yang dilakukan aplikasi seperti PeduliLindungi juga dinilai rawan melanggar privasi. Sementara, warga sulit memahami kebijakan praivasi. Aplikasi sering menggunakan jargon hukum yang rumit dan panjang, sehingga lebih dilihat sebagai tantangan hukum dibanding informasi soal privasi (Boudreaux et al., 2020).

Privasi adalah seseorang atau sesuatu yang tidak diamati atau diganggu oleh orang lain. Privasi merujuk pada hak individu untuk merahasiakan informasi dan hal-hal pribadinya serta hak untuk mengontrol informasi pribadi (Rath & Kumar, 2020, hal. 172). Apa yang dianggap privat oleh seseorang menandakan bahwa hal itu unik dan sensitif untuk mereka. Kekhawatiran seseorang atas isu privasi di dunia digital bisa terjadi pada beberapa domain, di antaranya: domain kesehatan, perbankan, kebijakan, e-commerce, institusi finansial, dan jejaring sosial (Rath & Kumar, 2020, hal. 173).

Lies de Kimpe dan kolega menyatakan bahwa ada dua jenis risiko yang dapat dialami seseorang saat mereka menggunakan internet, yakni risiko terkait konten dan risiko terkait kontak (de Kimpe et al., dalam Hobbs & Mihailidis, 2019). Beberapa risiko daring yang dijabarkan oleh de Kimpe dan kolega termasuk dalam risiko terkait privasi. Tabel 1 di bawah menunjukkan risiko privasi yang mungkin dialami seseorang yang diadaptasi dari kategorisasi risiko yang dibuat oleh de Kimpe dan kolega.

Tabel 1. Deskripsi Kompetensi Keamanan

No.		Risiko Terkait Konten	Risiko Terkait Kontak
1	Agresi	Mendapat kiriman konten kekerasan atau konten yang menyebar kebencian.	Menjadi korban praktik *cyberbullying* atau *cyberstalking.*
2	Seksual	Mendapat kiriman konten pornografi.	Menjadi korban *sexting, sextortion,* atau *online grooming.*
3	Komersial	Mendapat kiriman konten komersial.	Menjadi korban praktik pengumpulan data personal, *spam message*, *phising*, atau pencurian identitas

Adanya risiko atas privasi menandakan perlunya strategi perlindungan privasi bagi para pengguna internet. Perlindungan privasi dan data pribadi seseorang disebut UNESCO

ke dalam salah satu indikator literasi digital. Kemampuan untuk mengamankan privasi masuk dalam kompetensi keempat literasi digital, yakni keamanan. Tabel 2 menunjukkan secara detail kompetensi keamanan yang diperlukan agar seseorang bisa disebut memiliki literasi digital.

Tabel 2. Deskripsi Kompetensi Keamanan

No.	Kriteria	Deskripsi
1	Melindungi gawai pribadi	Kemampuan untuk melindungi perangkat dan konten digital, untuk memahami risiko dan ancaman di lingkungan digital, untuk mengetahui langkah keselamatan dan kemananan, dan untuk memperhatikan privasi.
2	Melindungi personal data dan privasi	Kemampuan untuk melindungi data pribadi dan privasi di lingkungan digital, untuk memahami cara menggunakan dan berbagi informasi pribadi, untuk melindungi diri sendiri dan orang lain dari ancaman privasi, dan untuk memahami bahwa layanan digital menggunakan "kebijakan privasi" untuk menginformasikan bagaimana data pribadi digunakan.
3	Melindungi kesehatan dan kesejahteraan	Kemampuan untuk dapat menghindari risiko kesehatan dan ancaman terhadap kesejahteraan fisik dan psikologis saat menggunakan teknologi digital, untuk dapat melindungi diri sendiri dan orang lain dari kemungkinan bahaya di lingkungan digital (misal *cyberbullying*), dan untuk menyadari fungsi teknologi digital untuk kesejahteraan dan inklusi sosial.
4	Melindungi lingkungan	Kemampuan untuk menyadari dampak lingkungan dari teknologi digital dan penggunaannya.

Sumber: Law, et al., 2018, hal. 24.

Kompetensi pengamanan privasi di atas dapat dijabarkan secara lebih teknis menjadi sebuah strategi pengamanan diri di internet. Misalnya, Penelitian Law dan kolega menemukan bahwa kriteria perlindungan gawai pribadi dapat tercapai jika seseorang mampu untuk mendaftarkan akun di sebuah aplikasi menggunakan password maupun nomor kontak. Sementara, kriteria perlindungan data personal dan privasi dapat dicapai dengan tidak menyebarkan password ke orang lain (Law, et al., 2018). Temuan ini senada dengan penelitian Kumar dan kolega, yang menunjukkan bahwa strategi perlindungan gawai dan privasi di dunia internet yang paling efektif adalah penggunaan password maupun User ID (Kumar, et al., 2018).

METODE

Penelitian ini akan menggunakan jenis penelitian kualitatif. Jenis penelitian kualitatif mendemonstrasikan pendekatan yang berbeda dari penelitian kuantitatif, di mana jenis penelitian ini memiliki keunikan tahap pada analisis dan menggunakan desain penelitian yang beragam (Creswell, 2013a). Sementara, metode yang digunakan dalam penelitian ini adalah deskriptif kualitatif. Tujuan dari penelitian deskriptif kualitatif adalah mendeskripsikan fenomena beserta karakteristik-karakteristiknya. Metode penelitian ini berfokus pada pertanyaan "apa"

dan membutuhkan data yang bersifat natural (Nassaji, 2015).

Peneliti menggunakan teknik pengumpulan data wawancara mendalam (in-depth interview). Peneliti melakukan wawancara mendalam secara daring menggunakan Zoom kepada tujuh informan dalam kurun waktu 10 hingga 27 November 2021. Wawancara secara virtual dipilih mengingat masih adanya pandemi COVID-19. Informan ditentukan lewat purposive sampling. Dengan menggunakan teknik purposive sampling, peneliti dapat dengan sengaja memilih peserta sebagai informan karena mereka telah mengalami fenomena atau konsep kunci yang dieksplorasi dalam penelitian (Creswell & Plano Clark, 2017).

Fenomena yang dicari dari informan adalah pengguna berat internet. Merujuk pada tulisan Ilakkuvan dan kolega (2019, dalam Hruska dan Maresova, 2020), pengguna berat internet adalah mereka yang mengonsumsi internet, khususnya media sosial, lebih dari 3 jam tiap harinya dan biasanya berusia 18 hingga 29 tahun. Dari kriteria ini, peneliti berhasil mengumpulkan tujuh informan berusia 25 hingga 28 tahun, berdomisili di wilayah Pulau Jawa, dan terbagi atas lima informan laki-laki dan dua informan perempuan. Sebagai triangulasi data, peneliti menggunakan studi data sekunder.

Teknik analisis penelitian merujuk pada tahapan analisis kualitatif Cresswell (2013b) yang mencakup organisasi data, Deskripsi, Interpretasi data, dan Representasi dan visualisasi data.

HASIL DAN PEMBAHASAN

Semua informan menghabiskan setidaknya 6 jam berinternet untuk bekerja, dan minimal 3 jam untuk keperluan pribadi. Data lengkap tiap informan bisa dilihat di Tabel 2. Informan bernama Themy dan Pradipta yang mengaku membutuhkan waktu berinternet lebih dari 6 jam untuk bekerja. Hal ini dikarenakan jenis pekerjaan mereka. Themy adalah digital marketing yang harus memantau pergerakan Facebook Ads dan Google Ads tiap waktu dan Pradipta yang bekerja sebagai desainer visual.

“Oh ya nine to five, kalau nggak saya nggak digaji. Hahahaha. Basically karena sudah jadi bagian dari pekerjaan ya emang di jam pekerjaan harus menyentuh internet.” (Niko, wawancara 10 November 2021)

“Waduh. Ya bisa dikatakan setiap hari dari bangun sampai tidur. 24 jam kurangi waktu tidur. Kalau untuk bekerja sekitar 12 jam per hari mungkin.” (Pradipta, wawancara 13 November 2021)

Penggunaan internet untuk kebutuhan pribadi dilakukan informan untuk alasan yang beragam. Advent menggunakan internet untuk pencarian informasi fotografi, film dokumenter, dan gim. Lalu, Pradipta dan Maria lebih suka menggunakan Twitter untuk mencari video lucu. Bram juga menggunakan media sosial untuk mencari video lucu, tapi ia lebih menggunakan platform Facebook. Lalu, Niko yang bermedia sosial untuk mengakstualisasi dirinya. Lalu, Themy menggunakan Discord untuk bersosialisasi dengan teman-teman. Terakhir, Sasa berinternet untuk berbelanja daring.

“Untuk hiburan, sama sekarang cewek mana sih yang nggak suka belanja online? Hahahaha. Kalau untuk aktualisasi diri nggak terlalu sih.” (Sasa, wawancara 12 November 2021)

“Mayoritas sih untuk cari konten fotografi genre street photography dan dokumenter, karena itu hobi saya. Sama cari-cari info tukang dagang kamera analog yang makin ke sini harganya makin kurang ajar.” (Advent, wawancara 11 November 2021).

Tabel 3. Perilaku Berinternet Selama Pandemi

No	Informan	Kebutuhan Internet Selama Pandemi	Penambahan Aplikasi Selama Pandemi
1	Niko	Urusan pekerjaan, ibadah daring, dan belajar.	Aplikasi Investasi, PeduliLindungi, dan Halodoc
2	Advent	Urusan pekerjaan dan Hiburan TV internet.	PeduliLindungi, Strava, OLX, dan Carousel
3	Sasa	Mencari informasi pandemi dan belanja daring.	PeduliLindungi
4	Pradipta	Mengusir kebosanan dengan bermain gim.	TikTok dan gim Vainglory
5	Bram	Urusan pekerjaan dan belanja daring.	Disney+ dan Duolingo
6	Themy	Bersosialisasi dengan teman lewat Discord.	PeduliLindungi, Discord Mobile, Trello Mobile, dan Slack Mobile
7	Maria	Mengusir kebosanan dengan bermain gim.	Aplikasi gim

Sumber: Diolah oleh peneliti.

Soal berbelanja daring, semua informan mengaku melakukannya, seperti terlihat di Tabel 3. Dua aplikasi belanja daring yang banyak disebut oleh informan adalah Shopee dan Tokopedia. Dipta dan Maria mengatakan bahwa kedua aplikasi ini membutuhkan informasi pribadi, termasuk alamat dan nomor HP. Data-data ini diperlukan agar kurir tidak tersesat saat mengantarkan paket. Artinya, informan sudah memasrahkan informasi pribadinya kepada perusahaan aplikasi.

"Saya rasa Shopee ya, karena data saya di sana sangat lengkap. Ada nomor HPnya, ada fotonya, ada foto KTP juga untuk verifikasi ShopeePay." (Maria, wawancara 18 November 2021)

Tabel 4. Kepemilikan Aplikasi Belanja Daring

Aplikasi	Pengguna (2020)	Bram	Maria	Advent	Pradipta	Sasa	Niko	Themy
SHOPEE	1,2 miliar	✓	✓	✓	✓	✓	✓	✓
TOKOPEDIA	836,1 juta	✓	✓	✓	✓	✓	✓	✓
BUKALAPAK	823,5 juta	-	-	✓	-	-	-	-
LAZADA	445,5 juta	-	-	-	-	-	-	-
BLIBLI	353,2 juta	-	-	-	-	-	-	-

Sumber: Diolah dari data penelitian

Peneliti juga menanyakan penanganan data penerima yang ada di kemasan paket belanja daring. Sejumlah informan mengatakan bahwa informasi penerima disobek, dibakar, atau digunting agar tidak bisa terdeteksi. Kemudian, Themy memilih untuk menyimpannya. Ada juga informan seperti Niko yang langsung membuangnya tanpa dirusak.

Isu lain yang peneliti tanya adalah seputar stiker "Add Yours" yang menjadi fitur terbaru di Instagram. Dari tujuh informan, dua informan perempuan mengaku pernah menggunakannya. Sasa menggunakan stiker tersebut dua kali dan dia memilih tantangan yang tidak terlalu menyinggung privasinya. Lalu, Maria menggunakan fitur itu karena merupakan fitur baru dan dia merasa perlu untuk ikut menggunakannya. Sementara, informan lain mengaku belum pernah menggunakan dan mengatakan tidak akan pernah menggunakan.

"Pernah mencoba hanya dua kali. Itu pun yang untuk pertanyaan-pertanyaan yang menurut ku gak terlalu privasi arahnya. Ada beberapa pertanyaan yang privasi juga tapi nggak tak pakai." (Sasa, wawancara 22 November 2021)

Saat memasuki pertanyaan terkait isu Big Data dan pemantauan, semua informan mengatakan bahwa mereka merasa dipantau selama ini (dapat dilihat di Tabel 4). Niko memahami pemantauan dari pelacakan di Google Maps. Themy mulai menyadari ada aktivitas pemantauan saat menjadi asisten laboratorium komputer di kampus. Adapun Sasa dan Maria merasa dipantau saat mereka mendapat rekomendasi iklan yang produknya sama dengan yang cari sebelumnya.

Kemudian, mengenai isu Big Data, Sasa mengaku kurang paham meski sudah pernah mendapat informasinya dari film dokumenter "The Social Dilemma". Informan yang bisa bicara banyak soal Big Data adalah mereka yang bekerja di bagian marketing (Niko dan Themy) dan di bagian data (Advent).

Niko dan Themy mengatakan bahwa Big Data adalah potensi besar bagi periklanan, karena manfaatnya tak terhingga jika bisa memaksimalkan penggunaannya. Sementara, Advent berpendapat bahwa Big Data adalah residu yang tertinggal dari aktivitas pengguna internet. Residu ini kemudian diambil oleh pebisnis digital untuk diolah untuk mengotak-kotakkan pengguna dalam berbagai kelompok konsumen.

"Big Data ini seperti emisi karbon yang bermakna. Kita melakukan kegiatan sehari-hari meninggalkan jejak karbon. Nah pebisnis digital ini mampu mengumpulkan emisi karbon ini lalu mengolahnya berdasarkan sudut pandang dan metode tertentu, sehingga Big Data ini bisa mengotak-ngotakkan kita ini sebagai konsumen produk A, B, dan C." (Advent, wawancara 11 November 2021)

Peneliti juga menanyakan terkait strategi pengamanan data pribadi berdasarkan kompetensi yang ditentukan UNESCO. Pada kompetensi perlindungan data pribadi, semua informan mengaku memasang pengaman password untuk mengakses halaman muka gawai mereka dan menggunakan kombinasi karakter pada password yang digunakan untuk masuk ke aplikasi di dalam gawai.

"Password itu ada sih. Lalu ketika masuk WhatsApp harus masukin password lagi. Dan saya selalu log out semua media sosial saya setelah saya gunakan." (Bram, wawancara 17 November 2021)

Tabel 5. Perilaku Berinternet Selama Pandemi

No	Informan	Pemahaman Soal Big Data	Pemahaman Soal Pemantauan
1	Niko	Big data adalah komoditas yang bernilai sangat mahal.	Pemantauan pelacakan lokasi lewat Google Maps.
2	Advent	Jejak internet yang diolah berdasarkan metode tertentu untuk mengotak-kotakkan pengguna internet.	Pengambilan data fisik (wajah dan sidik jari) dan pengambilan data matriks (input like, subscribe, dll).
3	Sasa	Pernah dengar di film "The Social Dilemma" tapi tidak paham.	Pemantauan riwayat pencarian di gawai.
4	Pradipta	Sistem yang berhubungan dengan Facebook Ads.	Pengambilan data oleh Facebook.
5	Bram	Rekaman dari setiap hal yang kita lakukan di internet yang digunakan oleh penguasa dan *stakeholder* untuk menjalankan suatu agenda.	Data yang terkumpul dari aktivitas klik pengguna internet.
6	Themy	Penggunaan data yang banyak untuk keperluan perusahaan	Pemantauan data perkuliahan mahasiswa lewat sistem *fingerprint*.
7	Maria	Data tentang semua orang di dunia yang jumlahnya sangat banyak	Pemantauan dari fitur perekam suara Google.

Sumber: Diolah oleh peneliti

Pada kompetensi perlindungan data pribadi dan privasi, para informan juga sudah bisa melindungi privasi mereka dengan cara merusak kemasan belanja daring yang berisi informasi seperti nama, alamat, dan nomor kontak mereka. Para informan sadar bahwa adanya informasi seperti alamat, nama, dan kontak yang tersebar dari kemasan belanja daring dapat meningkatkan potensi informan dihubungi atau mendapat kiriman konten yang tidak mereka kehendaki, sehingga mereka merusaknya.

Beberapa informan juga bahkan melakukan tindakan pengamanan agar gawai mereka tidak dibobol dan dicuri datanya oleh pihak lain. Hal ini salah satunya dilakukan oleh Niko. Niko mengatakan bahwa ia selektif dalam menghubungkan gawainya dengan Wi-Fi umum atau tidak asal mencolokkan flashdisk, karena takut ada virus yang mengambil data atau ada pembobol Wi-Fi publik yang bisa masuk ke semua gawai yang terkoneksi.

Pada kompetensi melindungi kesehatan dan kesejahteraan, peneliti mengajak informan bercerita soal gangguan yang dialami saat datanya bocor. Kesemua informan mengatakan gangguan paling sering adalah SMS atau chat pinjaman online (pinjol). Untuk mengatasinya, para informan menggunakan fitur blok yang ada di SMS dan WhatsApp. Semua informan yang mendapat gangguan via WhatsApp mengaku melakukan blok kontak, sementara informan yang mendapat SMS perlakuannya berbeda-beda. Ada informan yang blok semua SMS, dan ada yang memblok sebagian SMS saja seperti Maria.

"Ada yang saya blok nomornya ada yang nggak. Yang saya blok ini yang memang saya rasa sudah sangat mengganggu ya karena mengirimkan SMS banyak sekali." (Maria, Wawancara 18 November 2021)

Terakhir, pada kompetensi melindungi lingkungan sekitar, informan memandang keluarga adalah lingkungan pertama yang harus dilindungi. Orang tua dan adik adalah pihak di keluarga yang merasa perlu dilindungi. Bram misalnya, mengatur aplikasi-aplikasi non-ads pada adik-adiknya yang masih SMP dan mengedukasi orang tuanya untuk tidak asal klik iklan di Facebook karena takutnya ada praktik phishing di sana.

"Saya lebih melakukannya ke adikku yang kembar dan masih SMP. Praktis sejak pandemi kan mereka menghadap layar terus. Saya mengatur aplikasi yang mereka gunakan. Semisal browser hanya menggunakan Opera yang ada fitur ads block nya, lalu Youtube saya gunakan aplikasi yang nggak ada iklannya. Namanya itu YoutubeFence. Ini juga mematikan fitur rekomendasi juga. Ya ini hal konkret yang saya lakukan kepada mereka yang saya nilai masih bisa saya atur. Tapi kalau ke orang tua atau adik yang sudah mahasiswa ya paling cuma saya bilangin saja. Misal jangan sering-sering klik iklan yang muncul secara acak. Kadang link iklan itu kan juga banyak praktik phishing-nya. Ya ini perlu saya beri tahu." (Bram, Wawancara 17 November 2021)

Tabel 6. menunjukkan bagaimana praktik yang dilakukan informan dalam mengamankan gawainya, data pribadinya, kesehatan dan kesejahteraanya, dan lingkungannya.

Informan	Melindungi Gawai pribadi	Melindungi Data Personal dan Privasi	Melindungi Kesehatan dan Kesejahteraan	Melindungi Lingkungan
Niko	*Password* pada gawai dan penggunaan kombinasi karakter pada *password* di aplikasi.	Tidak menggunakan Wi-Fi publik agar terhindar dari peretas.	Blok semua SMS penipuan atau pinjol.	Mengedukasi orang tua agar tidak mudah memfoto sesuatu dan membagikannya.
Advent	*Password* pada gawai dan penggunaan kombinasi karakter pada *password* di aplikasi.	Merusak kemasan paket belanja daring.	Blok semua *chat* penipuan atau pinjol dan blok semua SMS penipuan atau pinjol.	Melanggankan koran orang tuanya untuk sumber informasi.
Sasa	*Password* pada gawai dan penggunaan kombinasi karakter	Merusak kemasan paket belanja daring.	Blok semua SMS penipuan atau pinjol.	Mengingatkan adiknya yang kecanduan Medsos.

	pada *password* di aplikasi.			
Pradipta	*Password* pada gawai *face recognition*, dan penggunaan kombinasi karakter pada *password* di aplikasi.	Merusak kemasan paket belanja daring.	Blok beberapa SMS penipuan atau pinjol.	Membantu orang tua dalam menyaring informasi.
Bram	*Password* pada gawai aktif me-*logout* aplikasi, dan penggunaan kombinasi karakter pada *password* di aplikasi.	Merusak kemasan paket belanja daring.	Blok *chat* penipuan atau pinjol.	Mengatur penggunaan aplikasi adik-adiknya dan mengingatkan orang tua tidak asal klik iklan.
Themy	*Password* pada gawai *finger print,* dan penggunaan kombinasi karakter pada *password* di aplikasi.	Merusak kemasan paket belanja daring dan menerapkan sistem email berjejaring.	Blok *chat* penipuan atau pinjol.	Mengajak orang tua untuk cek informasi lintas-*platform* dan mengurasi materi iklan dari klien.
Maria	*Password* pada gawai, *finger print,* dan penggunaan kombinasi karakter pada *password* di aplikasi.	Merusak kemasan paket belanja daring.	Blok *chat* penipuan atau pinjol dan blok beberapa SMS penipuan atau pinjol.	Membantu orang tua dalam menyaring informasi.

Sumber: Diolah dari data penelitian.

Saat ditanya apakah langkah-langkah yang informan lakukan di empat kompetensi keamanan bisa menghindarkan mereka dari kebocoran data, banyak informan berkata tidak. Themy dan Pradipta misalnya, mengatakan bahwa kebocoran data itu adalah hal yang pasti. Meski demikian, para informan percaya bahwa langkah yang telah dilakukan selama ini bisa meminimalisir data yang tersebar.

PEMBAHASAN

Kehadiran internet selama pandemi semakin tidak terhindarkan. Temuan data menunjukkan bahwa selain urusan pekerjaan yang harus dilakukan daring, peningkatan penggunaan internet dilakukan para informan untuk tujuan berbelanja, hiburan, atau pencarian informasi. Hal ini sejalan dengan data dari World Economic Forum (Myers, 2021) soal adanya peningkatan penggunaan selular.

Pencarian data perkembangan COVID-19 oleh informan menjadi bukti bagaimana media sosial berperan untuk mendukung kesadaran atas pembaruan informasi soal pandemi (Saud et al., 2020). Kemudian, penggunaan internet oleh informan untuk hiburan gim sejalan dengan pernyataan Lukosch dan Phelps (2020, dalam Kriz, 2020), bahwa bermain gim selama pandemi berpotensi untuk menghibur, membuat santai, dan menurunkan stres.

Perihal tujuan belanja, ada informan yang mengatakan bahwa adanya pembatasan sosial membuatnya belanja daring secara aktif sejak 2020. Pernyataan ini sesuai dengan penelitian Gu dan kolega (2021) bahwa pandemi memaksa konsumen untuk berbelanja lewat online marketplace. Aplikasi belanja daring yang digunakan para informan juga merupakan aplikasi yang paling banyak digunakan di Indonesia (Iriani dan Andjarwati, 2020). Sementara, data yang menunjukkan bahwa rata-rata informan memasang dua aplikasi belanja representatif dengan temuan survei Populix (2020), bahwa Generasi Milenial dan Generasi Z adalah generasi yang dekat dengan aplikasi belanja daring.

Pembahasan selanjutnya membahas soal Big Data dan pemantauan. Terkait Big Data, beberapa informan memahami Big Data sebagai data yang banyak yang digunakan untuk keperluan tertentu. Pemahaman informan telah memenuhi satu "V" dari tiga "V" yang menjadi karakteristik Big Data (De Mauro et al., 2015; Sonawane et al., 2018), yakni "Volume", sementara dua "V" lainnya yakni Velocity dan Variety belum dibahas.

Kemudian di pemahaman soal pemantauan, para informan menjelaskan contoh pemantauan yang pernah dialami. Praktik pemantauan mahasiswa yang diceritakan Themy merupakan bentuk dari cheaper surveillance (Schneier, 2015), yakni pemantauan publik yang mungkin terjadi karena biaya alat untuk memantau sudah murah. Kemudian, pemahaman informan lain merujuk pada bentuk automatic surveillance, yakni pengumpulan data yang dikumpulkan secara otomatis. Karakter pemantauan ini juga bisa dipahami dalam konsepsi David Lyon (2014) soal Otomatisasi. Jika pemahaman Themy dan pemahaman keenam informan lainnya soal pemantauan digabungkan, maka akan muncul ubiquitous surveillance. Ubiquitous surveillance adalah pemantauan yang terjadi di mana saja. Biaya pemantauan yang murah menciptakan pemantauan massa dan pemantauan otomatis. Hal ini kemudian menciptakan panopticon digital yang membuat siapapun dipantau kapanpun dan di manapun.

Soal etika pemantauan dan pengolahan Big Data, para informan terpolarisasi dalam dua pendapat. Ada yang berpendapat bahwa pemantauan tidak etis karena melanggar privasi. Namun, ada pernyataan dari Bram yang menarik untuk dianalisis. Pernyataan Bram yang menyebutkan bahwa kebijakan privasi di aplikasi terlalu panjang dan sulit untuk dibaca membuktikan dua hal. Pertama, ia membuktikan bahwa masalah redaksional soal kebijakan privasi terjadi secara global. Pasalnya, Bordeaux dan kolega (2020) juga menemukan isu serupa di Amerika, dengan menyebut bahwa kebijakan privasi menggunakan jargon-jargon hukum yang rumit dan panjang. Kedua, pernyataan Bram juga menunjukkan bahwa di Indonesia belum ada kebijakan atau aturan yang mumpuni soal

pengaturan privasi dan data pengguna internet. Ini sejalan dengan argument Rahmatullah (2021), bahwa di Indonesia belum ada perlindungan hukum terhadap data pribadi, sehingga dasar hukum yang digunakan masih berupa kebijakan privasi dari tiap pengembang aplikasi.

Pembahasan berikutnya lebih fokus pada strategi pengamanan internet yang dilakukan oleh informan. Adanya risiko atas privasi menandakan perlunya strategi perlindungan privasi bagi para pengguna internet. Ada empat kriteria di mana seseorang bisa dikatakan mampu mengamankan dan menjaga privasi mereka, yakni: mampu mengamankan gawai, mampu mengamankan informasi pribadi, mampu melindungi kesehatan dan kesejahteraan, dan mampu melindungi lingkungan sekitar (Law, et al., 2018).

Keempat kriteria pengamanan di atas bisa diturunkan menjadi sejumlah strategi yang bersifat teknis. Strategi melindungi gawai pribadi dapat dilakukan dengan cara mendaftarkan akun di sebuah aplikasi menggunakan password maupun nomor kontak. Lalu, strategi melindungi data personal dan privasi dapat dilakukan dengan tidak menyebarkan password atau informasi privat ke orang lain (Law, et al., 2018). Meski demikian, penelitian Law dan kolega belum memberi contoh teknis untuk kriteria ketiga dan keempat.

Data penelitian menunjukkan bahwa strategi melindungi gawai dan data pribadi yang dilakukan informan senada dengan hasil penelitian Law dan kolega (2018) dan penelitian Kumar dan kolega (2018). Pada strategi mengamankan gawai pribadi, semua informan menggunakan fitur pengamanan password di gawai dan menggunakan password dengan kombinasi karakter untuk masuk ke aplikasi. Password yang kuat yang terdiri dari huruf, angka, huruf kapital, dan karakter spesial ini penting dibuat karena akan membuat orang lain sulit menebak password yang digunakan (Norton, N.D).

Sementara, bentuk pengamanan data pribadi yang dilakukan oleh para informan adalah dengan cara merusak detail informasi penerima di bungkus paket belanja daring. Langkah merusak informasi pribadi di kemasan paket belanja ini sejalan dengan instruksi perlindungan data pribadi oleh Kementerian Komunikasi dan Informatika (Tempo.co, 2021). Dengan adanya aktivitas merusak informasi pribadi yang ada dalam kemasan belanja daring, para informan telah melakukan tindak pencegahan penyebaran informasi privat ke orang lain (Law, et al., 2018).

Temuan data juga menunjukkan bahwa para informan punya strategi unik yang belum ditemukan dalam penelitian Law dan kolega (2018) maupun penelitian Kumar dan kolega (2018). Misalnya, dalam kriteria pengamanan gawai, ada informan yang aktif melakukan log out akun media sosialnya. Kebiasaan log out setelah menggunakan aplikasi media sosial yang dilakukan Bram adalah satu dari enam tips untuk menjaga data pribadi menurut perusahaan antivirus Norton (N.D).

Sementara, strategi unik yang dilakukan untuk melindungi data pribadi yang ditemukan adalah dengan tidak asal menggunakan Wi-Fi publik. Langkah pengamanan ini sejalan dengan argumen Justin Dolly (2018). Dolly menyarankan untuk tidak pernah terhubung dengan jaringan Wi-Fi publik karena sistem keamanannya yang lemah. Sistem keamanan yang lemah dapat membuat para peretas bisa masuk ke gawai yang terhubung dengan Wi-Fi publik tersebut dan mengakses informasi privat yang ada di gawai yang terhubung tersebut.

Pada kriteria perlindungan kesehatan dan kesejahteraan, Law dan kolega belum menurunkannya menjadi strategi teknis.

Namun, bentuk teknis dari kriteria ini dapat diturunkan dari definisinya. Kriteria perlindungan kesehatan dan kesejahteraan merujuk pada kemampuan melindungi diri dari ancaman yang menyerang diri secara fisik ataupun psikis (Law, et al., 2018). Ancaman fisik dan psikis dapat terjadi karena adanya risiko di dunia daring terkait konten atau kontak (de Kimpe, et al., dalam Hobbs & Mihailidis, 2019), misalnya menjadi korban cyberbullying atau mendapat kiriman konten yang tidak dikehendaki. Cara mengatasi ancaman ini salah satunya bisa dilakukan dengan cara memutus hubungan pengguna dengan penyedia risiko, seperti dengan melakukan tindakan blokir.

ketujuh informan menceritakan bahwa dampak dari kebocoran data yang pernah dialami berimbas pada banyaknya penawaran pinjaman daring illegal atau pesan undian berhadiah yang mengganggu. De Kimpe dan kolega memasukkan bentuk ini ke dalam risiko terkait konten komersial (de Kimpe, et al., dalam Hobbs & Mihailidis, 2019). Artinya, informasi nomor kontak para informan bocor sehingga mereka dapat kiriman pesan komersial yang tidak dikehendaki dan hal ini mengganggu mereka.

Langkah perlindungan yang dilakukan informan adalah dengan memblokir kontak yang mengirim SMS atau chat penawaran tersebut. Dengan melakukan blokir, pengiklan tidak bisa lagi mengirimkan SMS atau chat penawaran ke para informan. Dengan demikian, para informan dianggap mampu melindungi kesehatan dan kesejahteraannya dari perilaku di internet yang membahayakan.

Kriteria perlindungan lingkungan juga belum memiliki bentuk strategi teknisnya, sehingga harus dipahami berdasarkan definisinya. Perlindungan lingkungan merujuk pada kemampuan untuk menyadari dampak lingkungan dari teknologi digital dan penggunaannya (Law, et al., 2018). Strategi yang bisa dilakukan pengguna internet untuk melindungi lingkungan dengan demikian adalah dengan mencari informasi terkait risiko internet bagi lingkungan sekitarnya seperti keluarga dan mencari cara untuk melindungi lingkungan sekitarnya dari risiko tersebut.

Dari data penelitian, strategi perlindungan lingkungan bisa tampak dari kasus Bram. Bram melakukan perlindungan terhadap keluarga dan adik-adiknya agar tidak terjerumus praktik phising. Phising adalah bentuk kegiatan yang menjebak seseorang dengan konsep memancing mereka (Wibowo & Fatimah, 2017). Dalam penelitian de Kimpe dan kolega, praktik phising termasuk dalam risiko terkait kontak yang bersifat komersial (de Kimpe, et al., dalam Hobbs & Mihailidis, 2019). Praktik phising ini bisa muncul dalam notifikasi bahwa si pengguna memenangkan hadiah atau dalam bentuk iklan. Setelah link di-klik, seseorang bisa diminta untuk memasukkan data penting seperti nama atau informasi kartu debit kita.

Bram memiliki informasi terkait phising, dan menurutnya praktik ini bisa membahayakan keluarganya. Menurut Bram, adik-adiknya yang masih SMP cenderung tidak bisa membedakan iklan sungguhan dengan iklan phising, sehingga diperlukan langkah agar adik Bram tidak masuk dalam jebakan phising. Akhirnya, ia menggunakan fitur Ads block dan YouTube yang tanpa iklan agar adik-adiknya tidak terhubung dengan pengiklan. Dengan menghindarkan keluarganya dari praktik phising, Bram menunjukkan bahwa dirinya memiliki kompetensi perlindungan lingkungan.

PENUTUP

Selama pandemi, penggunaan internet meningkat untuk bekerja, ibadah daring, belanja daring, mencari informasi, bermain gim, bersosialisasi, mencoba berbagai fitur

baru di media sosial, dan menonton Netflix. Hal tersebut membuka peluang ancaman privasi yang datang dari kegiatan pemantauan dan sistem Big Data. Para pengguna memahami Big Data dari karakteristik volumenya yang besar. Sementara, pengalaman pemantauan yang dialami oleh mereka merujuk pada praktik cheaper surveillance dan pemantauan yang diotomatisasi. Terkait etika, beberapa pengguna berat internet menyatakan aktivitas pemantauan ini etis, sebab sudah ditulis kebijakan privasi. Hanya saja, pengguna menyayangkan redaksional kebijakan privasi yang terlalu panjang dan belum adanya payung hukum terkait sistem Big Data dan surveillance.

Ancaman privasi pengguna berat internet juga berasal dari potensi kebocoran data, baik karena keteledoran pengguna maupun keteledoran perusahaan aplikasi. Jika kebocoran terjadi pada aplikasi, pengguna internet hanya pasrah. Sementara, jika kebocoran berpotensi berasal dari pengguna sendiri, mereka sudah melakukan sejumlah strategi pengamanan berdasarkan empat kriteria dalam kompetensi keamanan. Pada kriteria melindungi gawai, para informan membuat password yang kuat agar tak mudah dibobol, dan aktif me-logout aplikasi seusai digunakan. Pada kriteria melindungi data pribadi, para informan merusak informasi pribadi di kemasan belanja online mereka, dan tidak asal tersambung dengan Wi-Fi publik agar gawai mereka tidak diretas dan informasinya dicuri. Pada kriteria melindungi kesehatan dan kesejahteraan, para informan aktif memblokir nomor yang mengirim konten komersial yang mengganggu. Terakhir, pada kriteria melindungi lingkungan, ada informan yang memasangkan fitur Ads block pada gawai adiknya yang masih SMP guna menghindarkan mereka dari iklan phising yang menjebak.

Dari hasil temuan dalam penelitian ini dapat dikembangkan pada penelitian berikutnya. Peneliti belum memberi fokus khusus terhadap fitur "Add Yours" di Instagram. Akan menarik jika ada penelitian tentang persepsi risiko pengguna media sosial akan stiker "Add Yours" Instagram pasca-kasus penipuan yang bersumber dari fitur ini.

DAFTAR RUJUKAN

Alfianto, R. (2020, Juli 5). 91 Juta data akun Tokopedia bocor dan disebar di forum internet. JawaPos. https://www.jawapos.com/oto-dan-tekno/teknologi/05/07/2020/91-juta-data-akun-tokopedia-bocor-dan-disebar-di-forum-internet/.

Appel, M. (2012). Are heavy users of computer games and social media more computer literate? Computers & Education, 59, 1339-1349. DOI: 10.1016/j.compedu.2012.06.004

Boudreaux, B., Denardo, M. A., Denton, S. W., Sanchez, R., Feistel, K., & Dayalani, H. (2020). Data privacy during pandemics: A scorecard approach for evaluating the privacy implications of COVID-19 mobile phone surveillance programs. Rand Corporation.

Boyd, D., & Crawford, K. (2012). Critical questions for big data. Information, Communication & Society, 15(5), 662-679.

Cindy. (2021, Februari 8). Penggunaan internet semasa pandemic naik 443 persen. Medcom. https://www.medcom.id/nasional/peristiwa/dN6AeYpK-penggunaan-internet-semasa-pandemi-naik-443-persen.

CNN Indonesia. (2021, November 23). Fitur Add Yours Instagram buka celah penipuan dan curi data. CNN

Indonesia. https://www.cnnindonesia.com/teknologi/20211123101840-185-724774/fitur-add-yours-instagram-buka-celah-penipuan-dan-curi-data.

Creswell, J. W. (2013a). Reseach design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). SAGE Publications, Inc.

Cresswell, J. W. (2013b). Qualitative inquiry & research design: Choosing among five approaches. SAGE Publications.

Cresswell, J. W., & Plano Clark, V. L. (2018). Designing and conducting mixed methods research (3rd ed.). SAGE Publications, Inc.

De Kimpe, L., Walrave M., Ponnet, K., & van Ouytsel, J. (2019). Internet safety. Dalam R. Hobbs & P. Mihailidis (Eds.). The international encyclopedia of media literacy. John Wiley & Sons, Inc.

De Kimpe, L., Walrave, M., Verdegem, P. and Ponnet, K. (2022). What We Think We Know About Cybersecurity: An Investigation of the Relationship between Perceived Knowledge, Internet Trust, and Protection Motivation in a Cybercrime Context. Behaviour & Information Technology, 41(8), 1796-1808. DOI: 10.1080/0144929X.2021.1905066

De Mauro, A., Greco, M., & Grimaldi, M. (2015). What is big data? A consensual definition and a review of key research topics. International Conference on Integrated Information, 1644, 97-104. AIP Publishing. Doi: 10.1063/1.4907823.

Dolly, J. (2018, Januari 10). Why you should never, ever connect to public Wi-Fi. CSO Online. https://www.csoonline.com/article/3246984/why-you-should-never-ever-connect-to-public-wi-fi.html.

Farisa, F. C. (2021, September 5). Kebocaran data, aplikasi PeduliLindungi perlu diaudit dan perbaikan. Kompas.com. https://www.kompas.com/tren/read/2021/09/05/163000865/kebocoran-data-aplikasi-pedulilindungi-perlu-diaudit-dan-perbaikan?page=all.

Fitri, A. (2020, April 28). Selama pandemi COVID-19, instalasi Halodoc meningkat 10 kali lipat. Kontan. https://kesehatan.kontan.co.id/news/selama-pandemi-covid-19-instalasi-halodoc-meningkat-10-kali-lipat.

Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M (eds.). (2011). Internet and surveillance: The challenges of web 2.0 and social media. Routledge.

Gu, S., Slusarczyk, B., Hajizada, S., Kovalyova, I., & Sakhbieva, A. (2021). Impact of the COVID-19 pandemic on online customer purchasing behavior. Journal of Theoretical and Applied Electronic Commerce Research, 16, 2263-2281. Doi: https://doi.org/10.3390/jtaer16060125.

Ilakkuvan, V., Johnson, A., Villanti, A. C., Evans, W.D., & Turner, M. (2019) Patterns of Social Media use and their relationship to health risks among young adults. Dalam Hruska, J., dan Maresova, P. (2020). Use of social media platforms among adults in the United States – Behavior on Social Media. Societies, 10(27), 1-14.

Iriani, S. S., & Andjarwati, A. L. (2020). Anaysis of percieived usefulness, perceived ease of use, and perceived risk toward online shopping in the ero of COVID-19 pandemic. Systematic Reviews in Pharmacy, 11(12), 313-320.

Kriz, W. C. (2020). Gaming in the Time of COVID-19. Simulation & Gaming, 5(4), 403-410.

Kubina, M., Varmus, M., & Kubinova, I. (2015). Use of big data for competitive advantage of company. Procedia Economics and Finance, 26, 561-565. Elsevier B.V.

Kumar, T., Porambage, P., Ahmad, I., & Liyanage, M. (2018). Securing the gadget-free digital services. Computer, 51(11).

Kumparan. (2020, Mei 6). Bukalapak akui 13 juta data yang dijual hacker adalah peretasan di Maret 2019. Kumparan. https://kumparan.com/kumparantech/bukalapak-akui-13-juta-data-yang-dijual-hacker-adalah-peretasan-di-maret-2019-1tMRTr1UR0G/full.

Law, N., Woo, D., de la Torre, J., & Wong, G. (2018). A global framework of reference on digital literacy skills for indicator 4.4.2. UNESCO Institute for Statistics.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. Big Data & Society, Juli-December, 1-13. Doi: 10.1177/2053951714541861.

Myers, J. (2021, Agustus 10). This is how much data we're using on our phones. World Economic Forum. https://www.weforum.org/agenda/2021/08/how-the-pandemic-sparked-a-data-boom/.

Nassaji, H. (2015). Qualitative and descriptive research: Data type versus data analysis. Language Teaching Research, 19(2), 129-132.

Norton. (N.D). How to keep your personal information safe on social media. Norton. https://us.norton.com/internetsecurity-how-to-how-to-keep-your-personal-information-safe-on-social-media.html.

Populix. (2020, November 9). Menelusuri lebih jauh tren belanja online masyarakat Indonesia. Populix. https://www.info.populix.co/post/tren-belanja-online-masyarakat-indonesia.

Prasetyani, Y. M. (2021, April 4). Internet sudah jadi napas baru kehidupan di tengah pandemi. Kompas.com. https://nasional.kompas.com/read/2021/04/04/09020061/internet-sudah-jadi-napas-baru-kehidupan-di-tengah-pandemi.

Rahmatullah, I. (2021). Pentingnya perlindungan data pribadi dalam masa pandemi COVID-19 di Indonesia. Adalah: Buletin Hukum & Keadilan, 5(1), 11-16.

Rath, D. K., & Kumar, A. (2020). Information privacy concern at individual, group, organization and societal level – a literature review. Vilakshan – XIMB Journal of Management, 18(2), 171-186.

Roy. (2021, Mei 20). Heboh! Data KTP hingga nomor HP 279 juta Warga RI bocor?. CNBC Indonesia. https://www.cnbcindonesia.com/tech/20210520160626-37-247096/heboh-data-ktp-hingga-nomor-hp-279-juta-warga-ri-bocor.

Salim, H. J. (2021, Februari 26). Selama pandemi COVID-19, pemakaian internet Indonesia naik hingga 40 persen. Liputan6. https://www.liputan6.com/cek-fakta/read/4493427/selama-pandemi-covid-19-pemakaian-internet-indonesia-naik-hingga-40-persen.

Saud, M., Mashud, M., & Ida, R. (2020). Usage of social media during the pandemic: Seeking support and awareness about COVID-19 through

social media platforms. Journal of Public Affairs, 2020;e0247, 1-9. Doi: https://doi.org/10.1002/pa.2417.

Schneier, B. (2015). Data and Goliath: The hidden battles to collect your data and control your world. W. W. Norton & Company.

Soenarso, S. A. (2020, Juni 5). Penggunaan pay TV dan free online streaming meningkat saat pandemi COVID-19. Kontan. https://industri.kontan.co.id/news/pengguna-pay-tv-dan-free-online-streaming-meningkat-saat-pandemi-covid-19.

Sonawane, S., Patel, D., Kevadiya, M., Modi, R., Moradiya, J., & Thomas, A. (2018) Big Data by 3V's and its importance. International Journal of Research in Engineering, Science and Management, 1(12), 11-12.

Statista Research Department. (2021, Mei 19). Social media use during COVID-19 worldwide – Statistics & facts. Statista. https://www.statista.com/topics/7863/social-media-use-during-coronavirus-covid-19-worldwide/#dossierKeyfigures.

Tempo.co. (2021, Juni 7). 3 tips usai terima barang belanja online agar data pribadi tak disalahgunakan. Tempo.co. https://bisnis.tempo.co/read/1469592/3-tips-usai-terima-barang-belanja-online-agar-data-pribadi-tak-disalahgunakan/full&view=ok.

Veliz, C. (2020). Privacy during the pandemic and beyond. The Philosophers Magazine, 107-113.

Wibowo, M., & Fatimah, N. (2017). Ancaman phising terhadap pengguna sosial media dalam dunia cyber crime. Journal of Education and Information Communication Technology, 1(1), 1-5.

Yas, H., Jusoh, A., Streimikiene, D., Mardani, A., Nor, K. M., Alatawi, A., & Umarlebbe, J. H. (2021). The negative role of social media during the COVID-19 outbreak. International Journal of Sustainable Development and Planning, 16(2), 219-228.