



## Modul

---

# AMAN BERMEDIA DIGITAL

---

### Kata Pengantar:

Johnny G. Plate (Menteri Kominfo)

### Editor:

Gilang Jiwana Adikara & Novi Kurnia

### Penulis:

Gilang Jiwana Adikara, Novi Kurnia, Lisa Adhrianti,  
Sri Astuty, Xenia Angelica Wijayanto, Fransiska Desiana &  
Santi Indra Astuti

# **MODUL**

## **AMAN BERMEDIA DIGITAL**

### **Kata Pengantar:**

Johnny G. Plate (Menteri Kominfo)

### **Editor:**

Gilang Jiwana Adikara & Novi Kurnia

### **Penulis:**

Gilang Jiwana Adikara, Novi Kurnia, Lisa Adhrianti, Sri Astuty,  
Xenia Angelica Wijayanto, Fransiska Desiana Setyaningsih, Santi Indra  
Astuti

**Kementrian Komunikasi dan Informatik Republik Indonesia,**

**Japelidi, Siberkreasi**

**2021**

# Modul Aman Bermedia Digital

## **Kata Pengantar**

Johnny G. Plate (Menteri Kominfo)

## **Editor**

Gilang Jiwana Adikara

Novi Kurnia

## **Penulis**

Gilang Jiwana Adikara

Novi Kurnia

Lisa Adhrianti

Sri Astuty

Xenia Angelica Wijayanto

Fransiska Desiana Setyaningsih

Santi Indra Astuti

## **Penanggung jawab**

Dirjen Aplikasi Informatika, Kementerian KOMINFO

## **Dewan Pengarah**

Yosi Moku (Ketua GNLD Siberkreasi),

Tim Riset GLND Siberkreasi

## **Koordinator**

Koordinator Literasi Digital Kementerian KOMINFO

Tim Literasi Digital Kementerian KOMINFO

## ***Proofreader***

Febriansyah Kulau

## **Infografik**

Tegar Satria Yudha Leksana

## **Periset**

Syarifah Nur Aini

Tegar Satria Yudha Leksana

## **Desainer Sampul, Grafik, dan Tata Letak**

Tim Desain dan Konten Literasi Digital Kementerian KOMINFO

## **Penerbit**

Direktorat Jenderal Aplikasi Informatika

Jl. Medan Merdeka Barat no. 9, Jakarta 10110

(021) 3452841

humas@mail.kominfo.go.id

**Ukuran: 15,5 x 23 cm; ix + 200 hlm**

**E-ISBN: 978-602-18118-7-0**

**ISBN: 978-602-18118-7-0**

**Cetakan Pertama: April 2021**

Hak atas Kekayaan Intelektual © 2021 Kementerian Komunikasi dan Informatika



Setiap orang boleh menggunakan, mengutip dan mendistribusikan materi pada dokumen ini dengan wajib menyebutkan sumbernya serta hanya untuk keperluan pendidikan dan/atau non-komersial.



## KATA PENGANTAR

### **Menteri Komunikasi dan Informatika Republik Indonesia** **Modul Literasi Digital – Aman Bermedia Digital** **April 2021**

Pemanfaatan Tol Langit, berupa jaringan infrastruktur digital, guna mendorong pengembangan ekosistem digital melalui pemutakhiran penguasaan teknologi digital oleh anak bangsa menjadi salah satu pokok arahan Bapak Presiden Joko Widodo dalam peluncuran Program Konektivitas Digital pada Februari 2021 lalu. Keamanan ruang digital menjadi salah satu unsur utama pemanfaatan serta pengembangan ekosistem digital. Keberadaan talenta digital yang mampu melindungi diri di ruang digital, serta mewujudkan inovasi yang dapat menjaga keamanan ruang digital tentu menjadi semakin mendesak.

Merespon hal tersebut, Kementerian Komunikasi dan Informatika (Kominfo) menjalankan kebijakan perluasan infrastruktur digital yang diikuti adopsi teknologi baru, dan dibarengi penyelesaian roadmap transformasi digital, peningkatan kapasitas talenta digital, serta penyiapan regulasi pendukung dan pendanaan. Secara khusus, dalam hal penyiapan talenta digital, Kementerian Kominfo bersama pemangku kepentingan terkait telah menyelesaikan Peta Jalan Literasi Digital Nasional yang dikoordinasi oleh Gerakan Nasional Literasi Digital (GNLD) Siberkreasi yang diturunkan menjadi seri Modul Literasi Digital.

Lebih lanjut, sebagai hasil kolaborasi antara Kementerian Kominfo, Jaringan Pegiat Literasi Digital (Japelidi), dan GNLD Siberkreasi seri Modul Literasi Digital meliputi empat nilai utama literasi digital, yaitu: (i) Cakap Bermedia Digital; (ii) Budaya Bermedia Digital; (iii) Etis Bermedia Digital; dan (iv) Aman Bermedia Digital. Secara spesifik, **Modul Literasi Digital – Aman Bermedia Digital** ini bertujuan untuk meliterasi publik terhadap keamanan dalam bermedia digital, antara lain pengenalan terhadap pentingnya menjaga data pribadi, cara melindungi diri dari kekacauan informasi, hingga pentingnya menjaga jejak digital.

Keberadaan modul ini diharapkan mampu mewujudkan peningkatan kemampuan masyarakat untuk mengoperasikan teknologi digital secara aman, serta menjadi sarana untuk meliterasi 12,4 juta masyarakat Indonesia di tahun 2021. Melalui modul ini masyarakat diharapkan dapat menyiapkan diri untuk bersama-sama mewujudkan inovasi, serta mengembangkan ekosistem yang aman dan produktif untuk Indonesia maju.

Indonesia Terkoneksi: Semakin Digital, Semakin Maju

#MakinCakapDigital!

**Menteri Komunikasi dan Informatika Republik Indonesia**  
Johnny G. Plate

## KATA PENGANTAR JAPELIDI

Tantangan utama masyarakat modern dewasa ini adalah penggunaan internet dan media digital yang tak hanya memberikan manfaat bagi penggunanya, namun juga membuka peluang terhadap beragam persoalan. Kurangnya kecakapan digital dalam menggunakan perangkat keras dan perangkat lunak menimbulkan penggunaan media digital yang tidak optimal. Lemahnya budaya digital bisa memunculkan pelanggaran terhadap hak digital warga. Rendahnya etika digital berpeluang menciptakan ruang digital yang tidak menyenangkan karena terdapat banyak konten negatif. Rapuhnya keamanan digital berpotensi terhadap kebocoran data pribadi maupun penipuan digital.

*Roadmap Literasi Digital 2021-2024* yang disusun oleh Kominfo, Siberkreasi, & Deloitte pada tahun 2020 memberikan panduan untuk mengatasi persoalan tersebut dengan merumuskan kurikulum literasi digital yang terbagi atas empat area kompetensi: kecakapan digital, budaya digital, etika digital, dan keamanan digital. Keempat area kompetensi ini menawarkan beragam indikator dan subindikator yang bisa digunakan untuk meningkatkan kompetensi literasi digital masyarakat Indonesia melalui berbagai macam program yang ditujukan pada berbagai kelompok target sasaran.

Dalam rangka menerjemahkan peta jalan dan empat area kompetensi tersebut, Kominfo bekerja sama dengan Jaringan Pegiat Literasi Digital (Japelidi) dan Siberkreasi, menyusun empat modul sebagai langkah awal: Modul *Cakap Bermedia Digital*, Modul *Budaya Bermedia Digital*, Modul *Etis Bermedia Digital*, dan Modul *Aman Bermedia Digital*. Keempat modul ini disusun oleh 22 tim penulis dari Japelidi yang 8 diantaranya juga menjalankan peran sebagai editor dengan dukungan 8 asisten riset dan 4 *proofreader* dalam menyelesaikan penulisan dalam jangka waktu kurang lebih hanya 3 minggu. Tim penyusun modul tentu saja mendapatkan dukungan dan fasilitasi dari Kominfo dan Siberkreasi sebagai mitra kolaborasi.

Meskipun 4 modul dari Seri Modul Literasi Digital Kominfo, Japelidi, & Siberkreasi ini mempunyai fokus yang berbeda dan ditulis oleh tim penyusun yang tak sama, namun keempatnya menyajikan modul yang utuh. Tak hanya memaparkan konsep, problematika, dan strategi yang bisa digunakan baik pengguna media digital maupun pengajar atau pegiat literasi digital, keempat modul ini juga dilengkapi dengan rekomendasi solusi dan evaluasi untuk mengukur kompetensi literasi digital. Namun sebagai upaya awal dan singkat menerjemahkan *Roadmap Literasi Digital 2021-2024* tentu masih terdapat kelemahan di sana sini yang akan diperbaiki di waktu mendatang berdasarkan masukan dari pembaca maupun pengguna modul ini.

Semoga modul ini bermanfaat sebagai salah satu alat pembelajaran untuk meningkatkan kompetensi literasi digital masyarakat Indonesia dalam empat tahun dari sekarang, bahkan mungkin di masa mendatang.

Yogyakarta, 21 Februari 2021

Koordinator Nasional Japelidi  
Novi Kurnia

## DAFTAR ISI

|   |      |
|---|------|
| <b>Kata Pengantar Kementerian Kominfo</b>   | i    |
| <b>Kata Pengantar Japelidi</b>  | ii   |
| <b>Daftar Isi</b>   | iii  |
| <b>Daftar Bagan</b>   | v    |
| <b>Daftar Gambar</b>  | vi   |
| <b>Daftar Tabel</b>   | viii |
| <b>BAB I: Amankan Diri dan Sesama di Ruang Digital</b>                              | 1    |
| <i>Gilang Jiwana Adikara, Novi Kurnia, Santi Indra Astuti</i>                       |      |
| Pengantar   | 1    |
| Keamanan Digital  | 4    |
| Memahami Kompetensi Literasi Digital  | 5    |
| Peta Kompetensi Keamanan Digital  | 13   |
| Sistematika Modul   | 15   |
| Penggunaan Modul  | 17   |
| Daftar Pustaka  | 18   |
| <b>BAB II: Memproteksi Perangkat Digital</b>  | 21   |
| <i>Lisa Adhrianti</i>   |      |
| Urgensi Melindungi Perangkat Digital  | 21   |
| Memproteksi Perangkat Digital   | 22   |
| Jenis-jenis Fitur Proteksi Perangkat Digital  | 26   |
| Simpulan dan Rekomendasi  | 35   |
| Evaluasi Kompetensi Proteksi Perangkat Digital                                      | 45   |
| Contoh Bentuk Evaluasi untuk Aspek Konatif Praktik Proteksi Perangkat Digital       | 49   |
| Daftar Pustaka  | 52   |
| <b>BAB III: Perlindungan Identitas Digital dan Data Pribadi di Platform Digital</b> | 54   |
| <i>Novi Kurnia</i>  |      |
| Urgensi Perlindungan Identitas Digital dan Data Pribadi                             | 54   |
| Memahami dan Melindungi Identitas Digital   | 55   |
| Memahami dan Melindungi Data Pribadi  | 58   |
| Memahami dan Melindungi <i>Personal Identification Number</i>                       | 65   |
| Kemampuan memahami dan melindungi <i>Two Factor</i>                                 | 68   |
| Kemampuan memahami dan melindungi <i>One Time Passwords</i>                         | 71   |
| Simpulan dan Rekomendasi  | 73   |
| Evaluasi Kompetensi Perlindungan Identitas Digital dan Data Diri                    | 79   |
| Contoh Bentuk Evaluasi untuk Aspek Konatif Praktik Perlindungan Data Diri           | 81   |
| Daftar Pustaka  | 83   |
| <b>BAB IV: Memahami dan Menghindari Penipuan Digital</b>                            | 86   |
| <i>Sri Astuty</i>   |      |
| Urgensi Memahami Penipuan Digital   | 86   |

|   |     |
|---|-----|
| Mengenali dan Memahami Penipuan Digital                               | 88  |
| Memahami Aspek Aturan dan Hukum                                       | 105 |
| Simpulan dan Rekomendasi  | 110 |
| Evaluasi Kompetensi Menghindari Penipuan Digital                      | 113 |
| Contoh Instrumen Evaluasi Pengetahuan Dasar mengenai Penipuan Digital | 114 |
| Daftar Pustaka  | 115 |
| <b>BAB V: Melindungi Rekam Jejak Digital</b>                          | 120 |
| <i>Xenia Angelica Wijayanto</i>                                       |     |
| Urgensi Perlindungan Rekam Jejak Digital                              | 120 |
| Mengetahui Bentuk Rekam Jejak Digital                                 | 121 |
| Dua Sisi Jejak Digital  | 128 |
| Rekam Jejak Digital Sulit Dihilangkan                                 | 131 |
| Simpulan dan Rekomendasi  | 136 |
| Evaluasi Kompetensi Perlindungan Rekam Jejak Digital                  | 139 |
| Contoh Bentuk Evaluasi Kemampuan Perlindungan Rekam Jejak Digital     | 139 |
| Daftar Pustaka  | 139 |
| <b>Bab VI: Keamanan Anak di Platform Digital</b>                      | 142 |
| <i>Fransiska Desiana Setyaningsih Setyaningsih</i>                    |     |
| Urgensi Memahami Pentingnya Keamanan Anak                             | 142 |
| Aspek-Aspek Keselamatan Anak di Media Digital                         | 147 |
| Mencegah dan Mengatasi Ancaman Keselamatan Anak Melalui Media Digital | 161 |
| Saran dan Rekomendasi Literasi Keamanan Digital                       | 174 |
| Evaluasi Kompetensi Mengenali dan Meningkatkan Keamanan Digital       | 179 |
| Contoh Instrumen Evaluasi   | 180 |
| Daftar Pustaka  | 180 |
| <b>BAB VII: Tantangan Keamanan Digital</b>                            | 185 |
| <i>Gilang Jiwana Adikara &amp; Novi Kurnia</i>                        |     |
| Internet dan Keamanan Digital   | 184 |
| Kompetensi Keamanan Digital   | 186 |
| Tantangan Keamanan Digital  | 188 |
| Pengembangan Modul Keamanan Digital                                   | 190 |
| Daftar Pustaka  | 192 |
| Daftar Istilah  | 193 |
| Daftar Indeks   | 196 |
| Tentang Penulis   | 199 |

## DAFTAR BAGAN

|             |  |    |
|-------------|--|----|
| Bagan I.1   | Peta kompetensi keamanan digital                                   | 14 |
| Bagan II.1  | Jenis-jenis fitur proteksi perangkat keras dan perangkat lunak     | 27 |
| Bagan II.2  | Cara aman menggunakan kata sandi                                   | 28 |
| Bagan III.1 | Jenis identitas digital  | 56 |
| Bagan III.2 | Langkah-langkah melindungi identitas digital                       | 57 |
| Bagan III.3 | Jenis data pribadi   | 59 |
| Bagan III.4 | Berbagai tips melindungi data pribadi                              | 60 |
| Bagan III.5 | Faktor yang biasa digunakan dalam <i>two-factor authentication</i> | 69 |
| Bagan III.6 | Perlindungan terhadap penggunaan OTP                               | 73 |
| Bagan IV.1  | Modus penipuan digital di media sosial                             | 90 |
| Bagan IV.2  | Beberapa contoh modus <i>scam</i>                                  | 93 |

## DAFTAR GAMBAR

|              |   |     |
|--------------|---|-----|
| Gambar I.1   | Jumlah kasus kejahatan siber di indonesia                             | 3   |
| Gambar I.2   | Komposisi modul literasi digital kominfo-japelidi-siberkreasi         | 12  |
| Gambar II.1  | <i>Screenshot</i> posting viral teknisi servis ponsel                 | 25  |
| Gambar II.2  | Tampilan aplikasi <i>file shredder</i>                                | 32  |
| Gambar III.1 | Poster digital ‘tips melindungi data pribadi di internet’             | 61  |
| Gambar III.2 | Poster digital ‘bersama jaga data pribadi’                            | 62  |
| Gambar III.3 | Poster digital ‘lindungi data pribadi pasien covid-19’                | 63  |
| Gambar III.4 | Poster digital ‘data pribadi harus dilindungi’                        | 64  |
| Gambar III.5 | Poster digital ‘langkah hukum penyalahgunaan data pribadi’            | 65  |
| Gambar III.6 | Poster digital ‘seberapa aman pin anda?’                              | 67  |
| Gambar III.7 | Poster digital ‘autentikasi dua tahap’                                | 70  |
| Gambar III.8 | Poster digital ‘OTP: rahasia antara anda & yang di atas sana          | 72  |
| Gambar IV.1  | Jumlah laporan daring per tahun                                       | 87  |
| Gambar IV.2  | Kerugian dari kejahatan dunia maya yang dilaporkan 2014-2018          | 90  |
| Gambar IV.3  | Jumlah kejahatan siber di Indonesia                                   | 91  |
| Gambar IV.4  | Poster digital ‘waspada penipuan daring shop via medsos’              | 96  |
| Gambar IV.5  | Poster digital ‘penipuan daring’                                      | 95  |
| Gambar IV.6  | Jenis panggilan telepon spam di indonesia tahun 2020                  | 96  |
| Gambar IV.7  | Panggilan spam  | 97  |
| Gambar IV.8  | Sms spam penipuan   | 98  |
| Gambar IV.9  | Infografis mengenal apa itu sms spam dan bagaimana cara melaporkannya | 99  |
| Gambar IV.10 | Phishing ancaman serius pelaku industri indonesia                     | 101 |
| Gambar IV.11 | Akun populer di instagram jadi sasaran serangan <i>phishing</i>       | 102 |
| Gambar IV.12 | Waspada penipuan <i>web phishing</i>                                  | 102 |
| Gambar IV.13 | Contoh akibat tindakan <i>hacking</i>                                 | 103 |
| Gambar IV.14 | Virus <i>hacking</i>  | 104 |
| Gambar IV.15 | <i>Realtime news</i> jelang pilkada hacker serang situs web kpu yogya | 104 |
| Gambar IV.16 | Mengenal alur kerja si lapor  | 108 |
| Gambar IV.17 | Cara lapor jika akun WhatsApp kena <i>hack</i>                        | 109 |
| Gambar V.1   | Poster rekam jejak digital  | 122 |
| Gambar V.2   | Contoh saran digital  | 124 |

|              |  |     |
|--------------|--|-----|
| Gambar V.3   | Cookie di halaman website Ikea indonesia dan Springer  | 125 |
| Gambar V.4   | Jejak digital yang kita tinggalkan   | 126 |
| Gambar V.5   | Persentase data pribadi yang diunggah di internet  | 127 |
| Gambar V.6   | Poster rekam jejak digital   | 132 |
| Gambar VI.1  | Saring baru <i>sharing</i>   | 144 |
| Gambar VI.2  | Poster digital “penggunaan media sosial pada anak”   | 145 |
| Gambar VI.3  | Infografis “ini jenis hinaan dan kata-kata yang sering digunakan oleh para pelaku bullying di media sosial | 149 |
| Gambar VI.4  | Infografis “magang palsu di luar negeri”   | 151 |
| Gambar VI.5  | Infografis “dugaan pembobolan data sepanjang 2020”   | 153 |
| Gambar VI.6  | Infografis “lindungi anak dari bahaya pornografi daring  | 155 |
| Gambar VI.7  | Infografis “pelecehan daring”  | 156 |
| Gambar VI.8  | Pencurian daring zaman now   | 157 |
| Gambar VI.9  | Infografis “anak & kekerasan digital”  | 158 |
| Gambar VI.10 | Infografis “tipe-tipe kecanduan gadget pada anak”  | 160 |
| Gambar VI.11 | Infografis “dampingi anak dalam dunia digital”   | 163 |
| Gambar VI.12 | Karakteristik media sosial   | 165 |
| Gambar VI.13 | Poster digital “10 tips cegah anak terpapar pornografi”  | 166 |
| Gambar VI.14 | Tips membuat konten yang populer   | 168 |
| Gambar VI.15 | Poster digital “konten aduan Kominfo”  | 170 |
| Gambar VI.16 | Laman depan situs “forum anak nasional”  | 172 |
| Gambar VI.17 | Laman depan situs “sahabat anak”   | 173 |
| Gambar VI.18 | Aman bermedia digital  | 174 |
| Gambar VI.19 | Perundungan anak berkebutuhan khusus   | 175 |
| Gambar VI.20 | Pola <i>scammer love</i>   | 176 |

## DAFTAR TABEL

|             |  |     |
|-------------|--|-----|
| Tabel I.1   | Kompetensi Literasi Digital  | 6   |
| Tabel I.2   | 10 Kompetensi Literasi Digital Japelidi  | 7   |
| Tabel I.3   | Area dan Indikator Kompetensi Literasi Digital menurut Koinfo, Siberkreasi & Deloitte                                  | 10  |
| Tabel II.1  | Matriks rekomendasi program literasi digital untuk meningkatkan kecakapan proteksi perangkat digital                   | 38  |
| Tabel II.2  | Evaluasi Kecakapan Proteksi Perangkat digital  | 46  |
| Tabel II.3  | Evaluasi Kecakapan Proteksi Perangkat Digital dilihat dari Aspek Konatif ( <i>Behavioral</i> )                         | 49  |
| Tabel III.1 | Matriks rekomendasi program literasi digital untuk meningkatkan kecakapan perlindungan identitas digital dan data diri | 75  |
| Tabel III.2 | Evaluasi Kecakapan Perlindungan Identitas Digital dan Data Diri  | 80  |
| Tabel III.3 | Evaluasi Kecakapan Perlindungan Data Diri dilihat dari Aspek Konatif ( <i>Behavioral</i> )                             | 82  |
| Tabel IV.1  | Matriks Rekomendasi Program Literasi Digital untuk Meningkatkan Pengetahuan mengenai Penipuan Digital                  | 111 |
| Tabel IV.2  | Evaluasi Pengetahuan Dasar Mengenai Penipuan Digital   | 113 |
| Tabel IV.3  | Evaluasi Pengetahuan Dasar Mengenai Penipuan Digital (aspek Kognitif)  | 114 |
| Tabel V.1   | Matriks rekomendasi program literasi digital untuk meningkatkan kecakapan perlindungan rekam jejak digital             | 136 |
| Tabel V.2   | Evaluasi Kemampuan Perlindungan Rekam Jejak Digital  | 137 |
| Tabel V.3   | Evaluasi Kemampuan Perlindungan Rekam Jejak Digital  | 139 |
| Tabel VI.1  | Matriks rekomendasi program literasi digital untuk meningkatkan kecakapan keamanan digital                             | 177 |
| Tabel VI.2  | Evaluasi Kemampuan Mengenali dan Meningkatkan Keamanan Digital   | 179 |





# **BAB I**

---

## Amankan Diri dan Sesama di Ruang Digital

# **BAB I**

## **AMANKAN DIRI DAN SESAMA DI RUANG DIGITAL**

*Gilang Jiwana Adikara, Novi Kurnia & Santi Indra Astuti*

### **PENGANTAR**

Teknologi internet dan perangkat untuk mengakses jaringan internet sudah bukan hal yang asing lagi di kalangan masyarakat Indonesia. Teknologi ini semakin akrab ketika 2020 lalu dunia menghadapi pandemi yang memaksa manusia untuk mengurangi kegiatan di luar rumah dan memanfaatkan internet untuk melaksanakan kegiatan sehari-hari, baik untuk bekerja, sekolah, belanja, maupun sekadar mencari hiburan dan bersosialisasi. Kita pun semakin mengenal berbagai layanan teknologi digital yang membantu aktivitas keseharian.

Sejak awal abad 21, perkembangan teknologi informasi di dunia terus berkembang secara masif. *Hootsuite* dan *We Are Social* pada Januari 2020 sebanyak 59% penduduk dunia sudah dapat mengakses Internet. Fenomena serupa terjadi juga di Indonesia. Dalam survei yang sama, *Hootsuite* memperkirakan internet sudah dapat diakses oleh 64% warga Indonesia atau sekitar 175,4 juta jiwa. Sedangkan survei yang dilakukan Asosiasi Penyedia Jasa Internet Indonesia (APJII) kuartal kedua 2020 menunjukkan penetrasi internet di Indonesia mencapai 73,7% atau sudah dapat diakses oleh 196,71 juta penduduk Indonesia (APJII, 2020). Tingginya jumlah pengakses digital berdampak pada semakin tinggi juga pengguna layanan digital dan perubahan gaya hidup masyarakat.

Perubahan gaya hidup menjadi serba digital menawarkan sejumlah keuntungan, salah satu yang paling utama adalah kemudahan dan kepraktisan dalam melakukan berbagai aktivitas. Untuk berbelanja misalnya, saat ini kita tidak perlu lagi secara fisik mendatangi toko untuk mendapatkan barang yang kita inginkan. Cukup dengan sentuhan jari melalui perantara gawai yang terkoneksi internet kita sudah bisa memilih barang, membandingkan harga, melakukan negosiasi dengan penjual sampai menyelesaikan pembelian dan melakukan transaksi keuangan.

Gaya hidup baru ini belakangan menjadi semakin populer di kalangan masyarakat Indonesia.

Data *We Are Social* menunjukkan pada 2019 88% pengguna Internet yang berusia di atas 15 tahun melakukan pembelian secara daring. 80% diantaranya mengaku melakukan pembelian melalui ponsel pintar (We Are Social, 2020). Sementara pada 2020, Google dan Termasuk mencatat peningkatan konsumen mengakses layanan digital sebesar 37% dibandingkan pada 2019. Sektor loka-pasar (*e-commerce*) mencatat peningkatan jumlah transaksi yang cukup besar.

Pada 2020 total transaksi secara digital mencapai sekitar Rp621 triliun, naik 11% dibandingkan tahun sebelumnya meskipun dari sisi belanja pariwisata dan transportasi mengalami penurunan (Goole & Temasek, 2020). Hal ini menunjukkan masyarakat semakin nyaman dan percaya dalam melakukan aktivitas keuangan yang selama ini dianggap berisiko tinggi melalui teknologi digital. Perkembangan penggunaan layanan digital ini juga dibarengi dengan peningkatan penggunaan layanan digital di sektor yang lain, termasuk untuk urusan administrasi pemerintahan.

Semakin tingginya aktivitas masyarakat dalam mengakses berbagai layanan di Internet menjadi angin segar karena aktivitas ini dapat membuka peluang masyarakat untuk lebih berdaya. Namun di sisi lain tingginya aktivitas digital juga membuka potensi buruk. Teknologi digital merupakan teknologi baru bagi sebagian besar masyarakat Indonesia. Meskipun berbagai penyedia layanan teknologi digital sudah mempersiapkan fitur keamanan digital yang tinggi, namun celah untuk pencurian data digital masih sangat berpeluang besar terjadi, terutama dari sisi pengguna.

Kasus terkait dengan keamanan digital yang cukup sering terjadi misalnya penipuan dan pencurian akun yang terjadi pada berbagai *platform* layanan digital. Sejumlah cara sebenarnya sudah dilakukan para penyedia layanan digital seperti memberikan fitur autentikasi dua arah hingga menyarankan untuk selalu *log out* dan mengganti kata sandi secara rutin. Berbagai sosialisasi untuk tidak mudah percaya pada tautan yang menggiurkan juga sering diumumkan. Namun kasus kejahatan digital yang menyasar perorangan masih sering terjadi.

Direktorat Tindak Pidana Siber Bareskrim Polri mencatat pada periode Januari hingga November 2020 terjadi sebanyak 4.250 laporan kejahatan *siber*. Dari ribuan kasus, 1.158 kasus di antaranya merupakan kasus penipuan dan 267 kasus akses ilegal. Sementara dari tahun ke tahun jumlah tindak pidana *siber* juga mengalami peningkatan (CNN, 2020).



Gambar I.1.

### Jumlah Kasus Kejahatan Siber di Indonesia

Sumber Direktorat Tindak Pidana Siber Bareskrim Polri (CNN, 2020).

Grafik di atas menggambarkan keamanan digital dari satu konteks, yaitu keamanan akun. Dalam kehidupan digital, keamanan digital memiliki spektrum yang luas, tidak hanya terbatas pada keamanan akun maupun persoalan penipuan digital serta akses ilegal, namun juga berbagai aspek lainnya. Apa saja aspek lain keamanan digital? Apakah yang sebenarnya disebut dengan keamanan digital itu? Apa urgensi kita sebagai pengguna media digital untuk memahami keamanan digital? Pertanyaan-pertanyaan ini akan di jawab di bagian berikut ini.

## KEAMANAN DIGITAL

Secara umum, keamanan digital dapat dimaknai sebagai sebuah proses untuk memastikan penggunaan layanan digital, baik secara daring maupun luring dapat dilakukan secara aman

dan nyaman (Sammons & Cross, 2017). Tidak hanya untuk mengamankan data yang kita miliki melainkan juga melindungi data pribadi yang bersifat rahasia.

Persoalan keamanan digital ini mencuat sejak pertama kali internet lahir. Sifatnya yang menghubungkan antara pengguna secara langsung dan bersifat global membuat keamanan data menjadi salah satu perhatian serius karena kontrol keamanan data pengguna otomatis berada di tangan masing-masing pengguna internet. Penyedia layanan internet maupun *platform* digital hanya bisa menyediakan fasilitas untuk membantu mengamankan data, tetapi kontrol utama tetap ada pada masing-masing pengguna. Bagi pihak yang berniat buruk, celah ini lah yang seringkali diincar. Alih-alih berusaha melakukan peretasan pada sistem penyedia layanan, melakukan penipuan dengan strategi penipuan yang memanfaatkan kelengahan pengguna jauh lebih mudah dilakukan dan seperti data yang sudah diungkapkan di atas, menjadi salah satu metode kejahatan digital yang cukup sering terjadi.

Persoalan lain yang muncul dalam bermedia digital adalah sifat internet juga menghubungkan antarpengguna secara luas dan anonim. Kita bisa melihat nama pengguna yang berinteraksi melalui media digital, namun kita tidak pernah bisa benar-benar yakin apakah di balik nama pengguna itu adalah orang yang bisa kita percaya. Hal ini dikarenakan identitas digital pengguna internet dan *platform* digital bisa sama dengan identitas di dunia nyata, bisa juga tidak. Siapa saja bisa menjadi sosok yang berbeda di internet. Kita pun rentan berinteraksi dengan orang yang tidak kita kenal yang kita tidak benar-benar pahami apa maksud dan tujuan interaksi tersebut.

Persoalan keamanan digital ini semakin rumit ketika interaksi digital tidak hanya melibatkan orang dewasa yang secara psikis lebih matang. Interaksi digital tidak jarang melibatkan anak-anak dan orang berusia lanjut yang masuk ke dalam golongan pengguna rawan. *Resiliensi* mereka di dunia maya semakin ditantang ketika penggunaan internet mulai *intrusif* ke kehidupan personal yang dapat berdampak pada gangguan kesehatan terutama kesehatan mental. Karena sifatnya yang menyeluruh dan kompleks, maka kompetensi literasi digital di tingkat yang lebih lanjut mutlak dibutuhkan.

## **MEMAHAMI KOMPETENSI LITERASI DIGITAL**

Secara umum, literasi digital sering kita anggap sebagai kecakapan menggunakan internet dan media digital. Namun begitu, acap kali ada pandangan bahwa kecakapan penguasaan teknologi adalah kecakapan yang paling utama. Padahal literasi digital adalah sebuah konsep dan praktik yang bukan sekadar menitikberatkan pada kecakapan untuk menguasai teknologi.

Lebih dari itu, literasi digital juga banyak menekankan pada kecakapan pengguna media digital dalam melakukan proses mediasi media digital yang dilakukan secara produktif (Kurnia & Wijayanto, 2020; Kurnia & Astuti, 2017). Seorang pengguna yang memiliki kecakapan literasi digital yang bagus tidak hanya mampu mengoperasikan alat, melainkan juga mampu bermedia digital dengan penuh tanggung jawab.

Untuk bisa mengetahui sejauh mana pengguna mempunyai kecakapan dalam memediasi media digital, maka diperlukan alat ukur yang tepat. Berbagai gagasan mengenai kompetensi literasi digital pun kemudian ditawarkan oleh beragam organisasi baik komunitas maupun instansi pemerintah yang menaruh perhatian pada pengembangan literasi digital di Indonesia.

Tabel 1.1 memetakan empat kerja besar dalam mendeskripsikan area kompetensi dan kompetensi literasi digital yang bisa digunakan sebagai kerangka berpikir dalam melakukan penelitian, perumusan kurikulum, penulisan modul dan buku, maupun beragam program literasi digital lainnya.

Tabel I.1  
Kompetensi Literasi Digital

| Japelidi (2018)  | Tular Nalar (2020)   | Badan Siber dan Sandi Negara (BSSN) (2020)  | Kominfo, Siberkreasi & Deloitte (2020)  |
|--|--|---|---|
| <b>10 kompetensi</b>   | <b>8 kompetensi</b>  | <b>5 kompetensi</b>   | <b>4 area kompetensi</b>  |
| <ul style="list-style-type: none"> <li>• Akses</li> <li>• Paham</li> <li>• Seleksi</li> <li>• Distribusi</li> <li>• Produksi</li> <li>• Analisis</li> <li>• Verifikasi</li> <li>• Evaluasi</li> <li>• Partisipasi</li> <li>• Kolaborasi</li> </ul> | <ul style="list-style-type: none"> <li>• Mengakses</li> <li>• Mengelola Informasi</li> <li>• Mendesain Pesan</li> <li>• Memproses Informasi</li> <li>• Berbagi Pesan</li> <li>• Membangun Ketangguhan Diri</li> <li>• Perlindungan Data</li> <li>• Kolaborasi</li> </ul> | <ul style="list-style-type: none"> <li>• Kelola Data Informasi</li> <li>• Komunikasi dan Kolaborasi</li> <li>• Kreasi Konten</li> <li>• Keamanan Digital</li> <li>• Partisipasi dan Aksi</li> </ul> | <ul style="list-style-type: none"> <li>• <i>Digital Skills</i></li> <li>• <i>Digital Culture</i></li> <li>• <i>Digital Ethics</i></li> <li>• <i>Digital Safety</i></li> </ul> |

Sumber: diolah dari Kurnia dkk, 2018; Kurnia & Wijayanto, 2020;  
Monggilo, Kurnia & Banyumurti, 2020; Kominfo, Siberkreasi & Deloitte (2020);  
Astuti, Mulyati & Lumakto (2020)

Jaringan Pegiat Literasi Digital (Japelidi) merumuskan 10 kompetensi literasi digital Japelidi pada tahun 2018 sebagai kerangka berpikir untuk merumuskan panduan penulisan seri literasi digital Japelidi. Kesepuluh kompetensi literasi digital Japelidi tersebut dijelaskan dalam tabel berikut ini:

Tabel I.2  
10 kompetensi literasi digital Japelidi

| No | Kompetensi       | Definisi  |
|----|------------------|---|
| 1  | Mengakses        | Kompetensi dalam mendapatkan informasi dengan mengoperasikan media digital  |
| 2  | Menyeleksi       | Kompetensi dalam memilih dan memilah berbagai informasi dari berbagai sumber yang diakses dan dinilai dapat bermanfaat untuk pengguna media digital       |
| 3  | Memahami         | Kompetensi memahami informasi yang sudah diseleksi sebelumnya   |
| 4  | Menganalisis     | Kompetensi menganalisis dengan melihat plus minus informasi yang sudah dipahami sebelumnya  |
| 5  | Memverifikasi    | Kompetensi melakukan konfirmasi silang dengan informasi sejenis   |
| 6  | Mengevaluasi     | Kompetensi dalam mempertimbangkan mitigasi risiko sebelum mendistribusikan informasi dengan mempertimbangkan cara dan <i>platform</i> yang akan digunakan |
| 7  | Mendistribusikan | Kompetensi dalam membagikan informasi dengan mempertimbangkan siapa yang akan mengakses informasi tersebut  |
| 8  | Memproduksi      | Kompetensi dalam menyusun informasi baru yang akurat, jelas, dan memperhatikan etika  |
| 9  | Berpartisipasi   | Kompetensi untuk berperan aktif dalam berbagi informasi yang baik dan etis melalui media sosial maupun kegiatan komunikasi daring lainnya                 |
| 10 | Berkolaborasi    | Kompetensi untuk berinisiatif dan mendistribusikan informasi yang jujur, akurat dan etis dengan bekerja sama pemangku kepentingan lainnya                 |

Sumber: Dokumentasi Japelidi 2018 (dalam Kurnia & Wijayanto, 2020)

Hingga akhir tahun 2020, sudah 13 buku seri panduan literasi digital Japelidi diterbitkan dengan tema beragam: Bijak Berbagai Informasi Bencana Alam (Kurnia dkk., 2018), Literasi *Game* (Yuwono dkk., 2018; Wirawanda & Setyawan, 2018), Pengasuhan Digital (Herlina dkk., 2018; Wenerda & Sapanti, 2019), Muslim Ramah Digital (Astuti dkk., 2018), Lawan Hoaks Politik (Adiputra dkk., 2019), Kewarganegaraan (Widodo & Birowo (editor), 2019), Jurnalis Warga (Nurhajati dkk., 2019), Perdagangan orang (Sukmawa dkk., 2019), Perempuan dan Transaksi Daring (Kurnia dkk., 2020), dan Perempuan dan Media Sosial (Monggilo dkk.,



2020). Melalui buku-buku tersebut, pembaca diajak menggunakan 10 kompetensi Japelidi untuk digunakan secara praktis dalam kehidupan sehari-hari. Selain itu, dengan bekerja sama dengan Siberkreasi, buku-buku tersebut bisa diunduh secara gratis melalui situs web literasidigital.id.

Selain menggunakan 10 kompetensi Japelidi dalam menyusun buku panduan, 10 kompetensi literasi digital Japelidi ini juga digunakan sebagai kerangka kerja untuk melakukan berbagai kegiatan lainnya seperti riset maupun kampanye melawan hoaks COVID-19 (Kurnia & Wijayanto, 2020).

Terkait penerapannya dalam riset, 10 kompetensi Japelidi sudah digunakan untuk mengukur skor kompetensi literasi digital masyarakat Indonesia, baik laki-laki maupun perempuan, dalam menggunakan media digital (Japelidi, 2019). Menggunakan kerangka berpikir yang sama, riset yang dilakukan Kurnia dkk (2020) bertujuan mengukur skor kompetensi literasi digital perempuan Indonesia dalam menggunakan aplikasi percakapan. Dalam kedua penelitian tersebut tampak bahwa kompetensi fungsional (akses, seleksi, paham, distribusi, dan produksi) memiliki skor lebih tinggi dibandingkan dengan kompetensi kritis (analisis, verifikasi, evaluasi, partisipasi dan kolaborasi).

Sedangkan dalam kampanye lawan hoaks COVID-19, 10 kompetensi Japelidi juga digunakan sebagai landasan bekerja Japelidi dalam melakukan kampanye baik secara daring maupun luring (Kurnia & Wijayanto, 2020). Kampanye yang menghasilkan 28 konten yang satu konten diproduksi dalam 44 bahasa (42 bahasa daerah, bahasa Mandarin dan bahasa Indonesia) ini mendapatkan dukungan dari warga, komunitas, instansi pemerintah maupun media.

Dengan tujuan serupa untuk meningkatkan literasi digital masyarakat Indonesia, Kurikulum Tular Nalar yang diusung oleh MAFINDO, Maarif Institute dan Love Frankie merumuskan 8 kompetensi yang digunakan sebagai indikator pengguna media digital dengan penekanan pada berpikir kritis (*critical thinking*). Kompetensi yang mengelaborasi berbagai model ini terdiri dari mengakses, mengelola informasi, mendesain pesan, memproses informasi, berbagi pesan, membangun ketangguhan diri, perlindungan data, dan kolaborasi.

Kompetensi literasi digital Tular Nalar tersebut dikembangkan menjadi tiga jenjang, yaitu Tahu, Tanggap, dan Tangguh. Tahu merujuk pada kemampuan dasar, Tanggap merujuk pada kemampuan menengah, sedangkan Tangguh merujuk pada kemampuan lanjut. Ketiga jenjang dan delapan kompetensi literasi media digital ini kemudian dikembangkan oleh kurikulum Tular Nalar ke dalam delapan isu, mencakup literasi dasar (Berdaya Internet), kesehatan (Internet dan Kesehatan), pengajaran di dalam kelas (Internet dan Ruang Kelas), mitigasi bencana (Internet dan Siaga Bencana), kewarganegaraan (Menjadi Warga Digital), keberagaman (Internet Damai), keluarga/keayahbundaan (Internet dan Keluarga), serta disabilitas (Internet Merangkul Sesama) (Astuti, Mulyati & Lumakto, 2020).

Sementara itu, Badan Siber dan Sandi Negara (BSSN) menawarkan lima kompetensi literasi digital yang terdiri dari: kelola data informasi, komunikasi dan kolaborasi, kreasi konten, keamanan digital, serta partisipasi dan aksi (Monggilo, Kurnia & Banyumurti, 2020). Kelola data informasi adalah kemampuan mengakses dan mengevaluasi data dan informasi secara cermat dan bijak. Komunikasi dan kolaborasi merupakan kemampuan berkomunikasi dan berkolaborasi secara etis dengan warganet lainnya. Kreasi konten adalah kemampuan menyunting dan memproduksi konten digital untuk tujuan baik. Keamanan digital merupakan kemampuan untuk melindungi privasi dan keamanan diri dari berbagai ancaman digital. Partisipasi dan aksi merupakan kemampuan untuk memanfaatkan media digital untuk berdaya dan bernilai lebih secara bersama-sama.

Kelima kompetensi ini dirumuskan sebagai kerangka berpikir dan kerangka kerja dalam meningkatkan kompetensi literasi media digital dan keamanan siber yang lebih baik di Indonesia. Oleh BSSN, kelima kompetensi ini kemudian dikembangkan secara khusus dalam sebuah buku panduan yang ditargetkan pada kaum muda terutama mereka sebagai pelajar yang masih duduk di bangku sekolah lanjutan atas dan sebagai mahasiswa di perguruan tinggi. Meskipun begitu, panduan ini bisa digunakan secara umum oleh pengguna media digital baik yang berprofesi sebagai guru, dosen, aktivis, jurnalis, wiraswasta, aparatur sipil negara, dan aneka profesi lainnya (Monggilo, Kurnia & Banyumurti, 2020).

Berbeda dengan perumusan kompetensi literasi digital yang dilakukan oleh Japelidi, Tular Nalar dan BSSN yang berfokus pada kompetensi; Kominfo, Siberkreasi & Deloitte (2020) memberikan kerangka yang lebih besar dengan menawarkan empat area kompetensi yang terdiri dari *Digital Skills*, *Digital Culture*, *Digital Ethics* dan *Digital Safety*.

*Digital Skills* adalah kemampuan individu dalam mengetahui, memahami, dan menggunakan perangkat keras dan piranti lunak TIK serta sistem operasi digital. *Digital Culture* merupakan kemampuan individu dalam membaca, menguraikan, membiasakan, memeriksa, dan membangun wawasan kebangsaan, nilai Pancasila dan Bhinneka Tunggal Ika dalam kehidupan sehari-hari). *Digital Ethics* adalah kemampuan individu dalam menyadari, mencontohkan, menyesuaikan diri, merasionalkan, mempertimbangkan, dan mengembangkan tata kelola etika digital (*netiquette*) dalam kehidupan sehari-hari. *Digital Safety* merupakan kemampuan individu dalam mengenali, mempolakan, menerapkan, menganalisis, dan meningkatkan kesadaran keamanan digital dalam kehidupan sehari-hari.

Masing-masing area kompetensi ini mempunyai beragam indikator atau kompetensi yang dapat dilihat pada tabel di bawah ini.

Tabel I.3

Area dan Indikator Kompetensi Literasi Digital menurut Kominfo, Siberkreasi & Deloitte

| <b><i>Digital Skills</i></b>   | <b><i>Digital Culture</i></b>  | <b><i>Digital Ethics</i></b>             | <b><i>Digital Safety</i></b>                              |
|--|--|--|---|
| Pengetahuan Dasar Mengenai Lanskap Digital – Internet dan Dunia Maya | Pengetahuan dasar akan nilai-nilai Pancasila dan Bhinneka Tunggal Ika sebagai landasan kecakapan digital dalam kehidupan berbudaya, berbangsa, dan bernegara | Etika Berinternet ( <i>Nettiquette</i> ) | Pengetahuan dasar mengenai fitur proteksi perangkat keras |

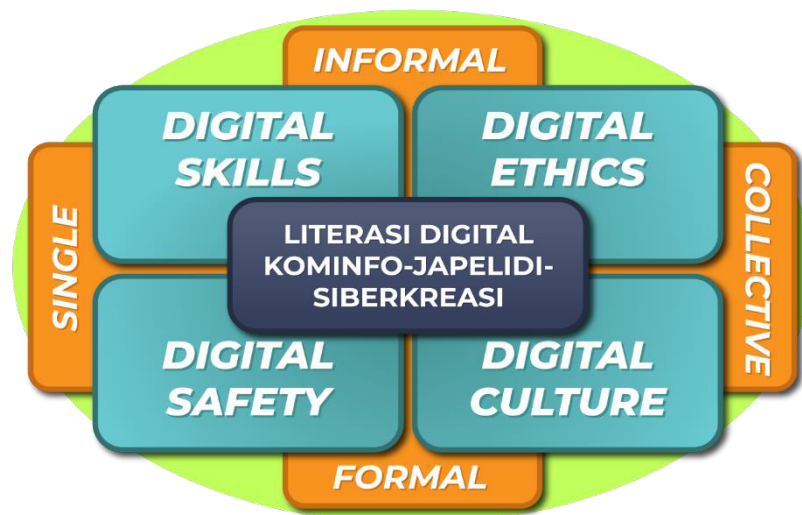
|  |  |   |   |
|--|--|---|---|
| Pengetahuan Dasar mengenai Mesin Pencarian Informasi, cara penggunaan dan pemilahan data                     | Digitalisasi Kebudayaan melalui pemanfaatan TIK  | Pengetahuan mengenai informasi yang mengandung hoaks, ujaran kebencian, pornografi, perundungan dan konten negatif lainnya.                     | Pengetahuan dasar mengenai proteksi identitas digital dan data pribadi di <i>platform</i> digital |
| Pengetahuan Dasar mengenai Aplikasi Percakapan, dan Media Sosial   | Pengetahuan dasar yang mendorong perilaku mencintai produk dalam negeri dan kegiatan produktif lainnya | Pengetahuan dasar berinteraksi, partisipasi, dan kolaborasi di ruang digital yang sesuai dengan kaidah etika digital dan peraturan yang berlaku | Pengetahuan dasar mengenai penipuan digital   |
| Pengetahuan Dasar mengenai Aplikasi dompet digital, lokapasar ( <i>market place</i> ), dan transaksi digital | <i>Digital Rights</i>  | Pengetahuan dasar berinteraksi dan bertransaksi secara elektronik di ruang digital sesuai dengan peraturan yang berlaku                         | Pengetahuan dasar mengenai rekam jejak digital di media (mengunduh dan mengunggah)                |
|  |  |   | <i>Minor safety (catfishing)</i>  |

Sumber: Kominfo, Siberkreasi & Deloitte (2020)

Mencermati area dan indikator literasi digital yang telah ditampilkan dalam Tabel 3, terlihat bahwa literasi digital adalah subjek yang sangat kompleks dan multidimensi. Perbedaan

mengenai cara menyusun kurikulum dan memaknai titik berangkat literasi digital berbeda-beda, tergantung pada perspektif pengguna maupun pihak yang mengembangkan kurikulum tersebut. Literasi digital Siberkreasi yang disusun ke dalam 4 subyek dan 17 indikator ini terdiri dari kompetensi, isu/area tematik, dan kasus. Misalnya, pengetahuan dasar mengenai lanskap digital dalam indikator Internet dan Dunia Maya terkategori area tematik, sementara pencarian informasi, cara penggunaan dan pemilihan data di area *Digital Skills* terkategori sebagai kompetensi. Pada area '*Digital Safety*' terdapat indikator pengetahuan dasar mengenai penipuan digital, yang terkategori dalam 'kasus'. Adanya kategorisasi yang berbeda-beda dalam satu paket subyek literasi digital ini memang tidak terhindarkan, ketika kita berhadapan dengan berbagai isu yang perlu diselesaikan segera. Terlebih lagi, materi literasi digital ini tidak semata-mata bergerak pada level gagasan/ide/pemikiran, tetapi juga diorientasikan pada kemampuan pengguna dalam mengaplikasikan pengetahuan dasar yang mereka peroleh pada kasus-kasus di lapangan yang sifatnya urgen.

Tidak dapat dihindarkan, antara satu modul dan modul lain juga terdapat keterkaitan yang erat, sehingga terkesan ada sedikit tumpang tindih. Peta berikut ini akan menjelaskan posisi masing-masing modul dan isu yang dibawa.



Gambar 1.2

Komposisi Modul Literasi Digital Kominfo-Japelidi-Siberkreasi

Sumber: olahan tim penulis

Terdapat dua poros yang membagi area setiap domain kompetensi. Poros pertama, yaitu domain kapasitas 'single – kolektif' memperlihatkan rentang kapasitas literasi digital sebagai kemampuan individu untuk mengakomodasi kebutuhan individu sepenuhnya hingga kemampuan individu untuk berfungsi sebagai bagian dari masyarakat kolektif/*societal*. Sementara itu, poros berikutnya adalah domain ruang 'informal – formal' yang memperlihatkan ruang pendekatan dalam penerapan kompetensi literasi digital. Ruang informal ditandai dengan pendekatan yang cair dan fleksibel, dengan instrumen yang lebih menekankan pada kumpulan individu sebagai sebuah kelompok komunitas/masyarakat. Sedangkan ruang formal ditandai dengan pendekatan yang lebih terstruktur dilengkapi instrumen yang lebih menekankan pada kumpulan individu sebagai 'warga negara digital.' Blok-blok kompetensi semacam ini memungkinkan kita melihat kekhasan setiap modul sesuai dengan domain kapasitas dan ruangnya.

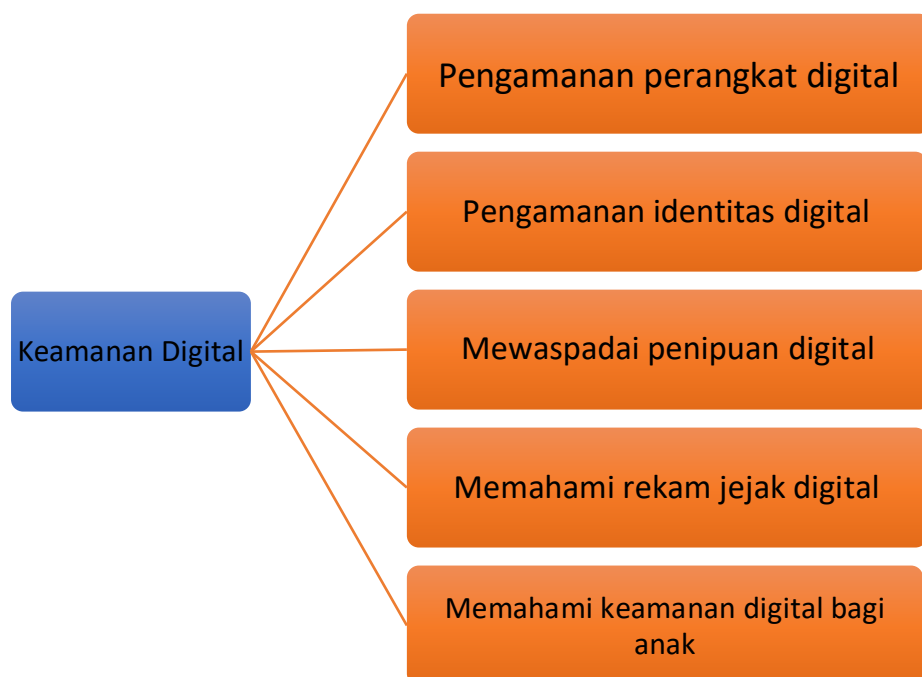
*Digital Skills* merupakan dasar dari kompetensi literasi digital, berada di domain 'single, informal'. *Digital Culture* sebagai wujud kewarganegaraan digital dalam konteks keindonesiaan berada pada domain 'kolektif, formal' di mana kompetensi digital individu difungsikan agar mampu berperan sebagai warga negara dalam batas-batas formal yang berkaitan dengan hak, kewajiban, dan tanggung jawabnya dalam ruang 'negara'. *Digital Ethics* sebagai panduan berperilaku terbaik di ruang digital membawa individu untuk bisa menjadi bagian masyarakat digital, berada di domain 'kolektif, informal'. *Digital Safety sebagai* panduan bagi individu agar dapat menjaga keselamatan dirinya berada pada domain 'single, formal' karena sudah menyentuh instrumen-instrumen hukum positif.

## **PETA KOMPETENSI KEAMANAN DIGITAL**

Membahas tentang keamanan digital berarti membahas berbagai aspek keamanan, mulai dari menyiapkan perangkat yang aman hingga menyediakan panduan untuk berperilaku di media digital yang rendah risiko. Modul ini bertujuan untuk memberikan panduan dan pemahaman untuk meningkatkan kemampuan individu dalam mengenali pentingnya keamanan digital, mengenali faktor-faktor risiko di dunia digital, mempolakan berbagai potensi dan ancaman yang biasa muncul dalam kehidupan digital serta menerapkan

keterampilan literasi digital untuk bisa mendukung aktivitas bermedia digital yang aman dan nyaman. Terdapat tiga aspek kecakapan keamanan digital yakni aspek kognitif, afektif dan konatif atau *behavioral* yang dikembangkan agar pengguna digital mampu mengembangkan keterampilan kritis dalam menganalisis, menimbang serta meningkatkan kesadaran keamanan digital dalam kehidupan sehari-hari.

Bagan I.1. di bawah ini menunjukkan lima indikator atau kompetensi yang perlu ditingkatkan dalam membangun area kompetensi keamanan digital.



Bagan I.1.

Peta Kompetensi Keamanan Digital

Sumber: modifikasi dari Kominfo, Siberkreasi & Deloitte (2020)

Secara umum pembahasan modul ini akan selain menggunakan kurikulum literasi digital yang dirumuskan oleh Kominfo, Siberkreasi & Deloitte (2020) terutama dalam area kompetensi keamanan digital, modul ini juga menggunakan 10 kompetensi literasi digital Japelidi. Dimulai dari kompetensi fungsional yakni mengakses, menyeleksi, memahami, mendistribusikan informasi, dan memproduksi konten, hingga kompetensi kritis yakni

menganalisis, memverifikasi, mengevaluasi, berpartisipasi dan berkolaborasi (Kurnia & Wijayanto, 2020).

Pada kompetensi proteksi perangkat digital, penekanan terletak pada keterampilan fungsional perangkat dan layanan digital. Sedangkan pada kompetensi lainnya yakni melindungi identitas digital, mewaspadaikan penipuan digital, melindungi rekam jejak digital, dan meningkatkan keamanan digital bagi anak-anak, keterampilan yang dibangun tak hanya fungsional melainkan juga kritis.

Dengan tujuan memberikan penguatan keterampilan kognitif, afektif dan konatif atau *behavioral*, modul ini mengajak pengguna media digital maupun pengajar atau pegiat literasi digital untuk memastikan keamanan digital baik bagi diri sendiri maupun sesama warga digital lainnya.

## **SISTEMATIKA MODUL**

Modul ini merupakan bagian dari Seri Modul Literasi Digital Kominfo, Japelidi dan Siberkreasi. Dalam seri modul ini terdapat empat tema besar, yaitu Keterampilan Digital, Budaya Digital, Etika Digital dan Keamanan Digital. Masing-masing modul membahas tema besar yang berbeda dan menyentuh komponen literasi digital yang berbeda pula. Sebagai bagian dari seri literasi digital yang menyeluruh maka beberapa bagian pembahasan pada modul ini akan dibatasi sehingga pemaparannya tidak terlalu jauh keluar dari perspektif keamanan digital. Sedangkan untuk mendapatkan perspektif lain dari topik yang sama kita dapat merujuk pada modul lain pada seri modul literasi digital ini.

Secara spesifik, pada modul mengenai keamanan digital yang berjudul 'Aman Bermedia Digital' ini, kita akan menemui lima bab yang membahas secara detail berbagai aspek seputar pengamanan dan keamanan digital yang kemudian diakhiri dengan bab penutup.

Bab I, pengantar, bab ini ditulis oleh Gilang Jiwana Adikara, Novi Kurnia, dan Santi Indra Astuti menjelaskan pentingnya penulisan modul mengenai keamanan digital yang disusun berdasarkan kompetensi literasi digital Kominfo, Siberkreasi & Deloitte yang kemudian



dikembangkan oleh Japelidi. Bab ini juga menjelaskan sistematika modul dan penggunaannya.

Bab II yang disusun oleh Lisa Adhrianti membahas secara detail tentang pengamanan perangkat digital yang kita gunakan sehari-hari. Kita akan mempelajari pentingnya mengamankan perangkat digital agar terhindar dari berbagai upaya pengambilalihan akses oleh orang-orang yang tidak bertanggung jawab. Bagian ini juga akan mengulas tentang bagaimana cara mencadangkan data berharga kita dan menghapus sepenuhnya data digital sebelum memindahtangankan atau menjual ke orang lain.

Bab III yang membahas tentang perlindungan identitas digital data pribadi ditulis oleh Novi Kurnia. Pada bab ini, kita akan mencoba mengenali bagaimana strategi mengamankan identitas pribadi kita di dunia digital dan menghindari data pribadi kita bocor ke pihak yang berniat buruk. Bab ini akan membahas secara detail strategi mengamankan akun-akun digital kita sehingga tidak mudah diambil paksa oleh orang lain. Bab ini juga membahas strategi untuk membangun kewaspadaan agar tidak mudah memberikan data diri kita pada pihak lain sebelum kita memahami betul risiko dan keuntungannya.

Bab IV yang mengulas seluk beluk penipuan digital secara menyeluruh dipaparkan oleh Sri Astuty. Mulai dari penipuan paling sederhana seperti *scam* ala “Mama minta pulsa” sampai yang memanfaatkan keterampilan *social engineering* untuk mempengaruhi korbannya dan menyiapkan situs palsu demi mencuri data penting yang berkaitan dengan keuangan digital. Bagian ini cukup penting dipahami karena kasus upaya penipuan digital merupakan hal yang sangat sering kita temui, baik melalui surel maupun SMS dan telepon. Bagian tentang penipuan ini juga membahas strategi untuk memverifikasi informasi yang masuk dan menindaklanjuti upaya penipuan yang datang maupun langkah jika kita menjadi korban penipuan digital.

Bab V yang disusun oleh Xenia Angelica Wijayanto membahas tentang rekam jejak digital. Seperti yang kita tahu, kegiatan kita di media digital selalu tercatat dan menghapusnya bukanlah hal yang mudah. Jika dibandingkan, akan jauh lebih mudah menjaga perilaku di media digital daripada berusaha menghapus jejak digital yang pernah kita tinggalkan. Bab ini

juga mengulas strategi memperindah jejak digital kita agar reputasi dan nama baik kita sebagai warga digital terjaga dengan baik.

Bab VI mengenai *minor safety* terutama terkait proteksi anak-anak di dunia maya ditulis oleh Fransiska Desiana Setyaningsih Setyaningsih. Bab ini memaparkan pentingnya keamanan digital berkaitan dengan tumbuh kembang anak termasuk strategi pengasuhan anak di era digital. Bab ini menekankan strategi melindungi anak-anak dari pengaruh buruk di media digital, mulai dari kecanduan sampai *cyberbullying*. Meskipun demikian, pembahasan di bab ini bukan hanya menekankan pada aspek ancaman. Media digital menawarkan peluang besar untuk menjadi pribadi yang kreatif dan berpengetahuan luas. Bab ini juga menelusuri pembahasan strategi yang dapat digunakan orang tua untuk dapat memaksimalkan potensi media digital untuk merangsang tumbuh kembang anak.

Bab VII atau bab terakhir yang ditulis oleh Gilang Adikara Jiwana dan Novi Kurnia merupakan bab yang menutup dan memberikan simpulan atas pentingnya modul ini. Dalam bab ini juga akan dipetakan limitasi modul ini berikut rekomendasi baik pengembangan modul maupun pengembangan berbagai program digital terkait keamanan digital di masa mendatang. Rekomendasi juga akan dikaitkan dengan beberapa kelompok pengguna media digital yang terpinggirkan yakni perempuan, anak, usia lanjut, masyarakat dari daerah 3 T (Terdepan, Terluar, Tertinggal).

## **PENGUNAAN MODUL**

Modul 'Aman Bermedia Digital' ini secara khusus bisa dimanfaatkan baik oleh pengguna media digital secara langsung maupun pengajar atau pegiat literasi digital dalam mengajarkan atau memfasilitasi peningkatan kompetensi keamanan digital. Modul ini juga bisa digunakan oleh siapa pun yang tertarik pada isu keamanan digital misalnya saja guru, orang tua, penyedia layanan internet, pakar teknologi informasi, wirausaha, dan lain sebagainya.

Bab-bab yang dituliskan dalam modul ini, kami rancang untuk bisa digunakan secara utuh satu modul guna mendapatkan penjelasan yang komprehensif terkait beragam kompetensi keamanan digital. Meskipun begitu, pembaca bisa menggunakan modul ini berdasarkan

kompetensi khusus yang dibahas di masing-masing bab. Apapun pilihannya, modul ini tak hanya memaparkan konsep dan memberikan ilustrasi kasus saja namun juga memperlihatkan strategi untuk meningkatkan keamanan digital baik untuk diri maupun pengguna lain. Selain itu, modul ini juga dilengkapi dengan evaluasi untuk bisa mengukur kompetensi digital yang dibangun di setiap bab. Dengan begitu, pembaca bisa melakukan *self-asessment* (evaluasi diri) untuk mengukur kompetensi keamanan digital yang dimilikinya. Evaluasi juga bisa dilakukan oleh pengajar atau pegiat literasi digital yang ingin mengukur kompetensi keamanan digital dari anak didik maupun peserta program.

## DAFTAR PUSTAKA

- Adiputra, W.M., Kurnia, N., Monggilo, Z.M.Z., Yuwono, A., Rahayu. (2019). *Yuk, lawan hoaks politik, ciptakan pemilu damai*. Yogyakarta: Prodi Magister Ilmu Komunikasi, Departemen Ilmu Komunikasi, Universitas Gadjah Mada.
- APJII (2020). Laporan survei internet APJII 2019-2020 (Q2). Didapat dari <https://apjii.or.id/survei2019x>.
- Astuti, S.I., Mulyati, H., & Lumakto, G., (2020). In Search of Indonesian-Based Digital Literacy Curriculum through TULAR NALAR [paper presentation]. "Islam, media and education in the digital era", Bandung, Indonesia, <https://sores.unisba.ac.id/2020/>
- Astuti, Y.D., Virga, R.L., Nusa, L., Mukti, R.K., Iqbal, F., Setyo, B. (2018). *Muslim milenial ramah digital*. Yogyakarta: Program Studi Ilmu Komunikasi Universitas Islam Negeri Sunan Kalijaga.
- CNN (2020, Desember 1). Polri tangani 4.250 kejahatan siber saat pandemi. Diperoleh dari <https://www.cnnindonesia.com/nasional/20201201141213-12-576592/polri-tangani-4250-kejahatan-siber-saat-pandemi>
- Google, Temasek, Bain & Company (2020). At full velocity: Resilient and racing ahead. Diperoleh dari <https://economysea.withgoogle.com/>
- Herlina, D., Setiawan, B, & Adikara, G.J. (2018). *Digital parenting: Mendidik anak di era digital*. Yogyakarta: Samudra Biru.
- Japelidi (2019). *Pemetaan literasi digital masyarakat Indonesia 2019*. Paper dipresentasikan pada Seminar Nasional Seminar Nasional Literasi Digital Dalam Membangun Perdamaian dan Peradaban Dunia. Diselenggarakan oleh ComTC UIN Sunan Kalijaga, Yogyakarta, 5-6 September.

- Kominfo, Siberkreasi, & Deloitte (2020) *Roadmap literasi digital 2021-2024*. Jakarta: Kominfo, Siberkreasi, & Deloitte.
- Kurnia, N, Wendratama, E., Rahayu, R., Adiputra, W.M., Syafrizal, S., Monggilo, Z.M.Z...Sari, Y.A. (2020). *WhatsApp group and digital literacy among Indonesian women*. Yogyakarta: WhatsApp, Program Studi Magister Ilmu Komunikasi, PR2Media & Jogja Medianet.
- Kurnia, N. & Astuti, S. I. (2017). Peta gerakan literasi digital di Indonesia: Studi tentang pelaku, ragam kegiatan, kelompok sasaran dan mitra. *INFORMASI Kajian Ilmu Komunikasi*, 47(2), 149-166.
- Kurnia, N. & Wijayanto, X.A. (2020) kolaborasi sebagai kunci: Membumikan kompetensi literasi digital japelidi. Dalam N. Kurnia, L. Nurhajati, S.I. Astuti, *kolaborasi lawan (hoaks) COVIDcovid-19: Kampanye, riset dan pengalaman japelidi di tengah pandemi*. Yogyakarta: Program Studi Magister Ilmu Komunikasi, Departemen Ilmu Komunikasi, Universitas Gadjah Mada.
- Kurnia, N., Monggilo, Z.M.Z., & Adiputra, W.M. (2018). *Yuk, tanggap dan bijak berbagi informasi bencana alam melalui aplikasi chat*. Yogyakarta: Program Studi Magister Ilmu.
- Kurnia, N., Sadasri, L.M., Angendari, D.A.A, Yuwono, A.I, Syafrizal, S., Monggilo, Z.M.Z, & Adiputra, W.M. (2020) *yuk, sahabat perempuan bertransaksi daring dengan cermat*. Yogyakarta: Program Studi Magister Ilmu Komunikasi, Departemen Ilmu Komunikasi, Universitas Gadjah Mada.
- Monggilo, Z.M.Z, Fandia, M, Tania, S, Parahita, G.D., Setianto, W.A., Sulhan, M, Rajiyem, R, & Kurnia, N. (2020) *Yyuk, sahabat perempuan bermedia sosial dengan bijak*. Yogyakarta: Program Studi Magister Ilmu Komunikasi, Departemen Ilmu Komunikasi, Universitas Gadjah Mada.
- Monggilo, Z.M.Z, Kurnia, N, Banyumurti, I. (2020) *Ppanduan literasi media digital dan keamanan siber: Muda, kreatif, dan tangguh di ruang siber*. Jakarta: Badan Siber dan Sandi Negara.
- Nurhajati, L., Fitriyani, LR., Wijayanto, XA. (2019). *Panduan Menjadi Jurnalis Warga yang Bijak Beretika*. Jakarta: Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) LSPR.

- Sammons, J. & Cross, M. (2017) *The basics of cyber safety: Computer and mobile device safety made*. Cambridge: Elsevier.
- Sukmawa, A.I., Karim, A.M., Yuwono, A.P., Elsha, D.D., Urfan, N.F., & Andiyansari, P. (2019). *Yuk, cegah tindak pidana perdagangan orang!* Yogyakarta: Penerbit Samudra Biru dan UTY.
- We Are Social & Hootsuite (2020, Februari 18). Digital 2020 Indonesia. Didapat dari <https://datareportal.com/reports/digital-2020-indonesia>
- Wenerda, I. & Sapanti, I.R. (2019) *Literasi digital bagi milenial moms*. Yogyakarta: Penerbit Samudra Biru dan Fakultas Sastra Budaya dan Komunikasi.
- Widodo, Y., Birowo, M.A. (eds.) (2019). *Literasi media & informasi dan citizenship*. Yogyakarta: Program Studi Ilmu Komunikasi, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Atma Jaya Yogyakarta.
- Wijayanto, XA., Fitriyani, LR., Nurhajati, L. (2019). *Mencegah dan mengatasi bullying di dunia digital*. Jakarta: Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) LSPR.
- Wirawanda, Y., Setyawan, S. (2018). *Literasi Game untuk Remaja & Dewasa*. Surakarta: Program Studi Ilmu Komunikasi Universitas Muhammadiyah Surakarta - Lembayung Embun Candikala.
- Yuwono, A.I., Anshari, I.N., Rahayu, Syafrizal, Adiputra, W.M. (2018). *Yuk, jadi gamer cerdas: Berbagi informasi melalui literasi*. Yogyakarta: Program Studi Magister Ilmu Komunikasi, Departemen Ilmu Komunikasi, Universitas Gadjah Mada.



# **BAB II**

---

## Memproteksi Perangkat Digital

## **BAB II**

### **MEMPROTEKSI PERANGKAT DIGITAL**

*Lisa Adhrianti*

#### **URGENSI MELINDUNGI PERANGKAT DIGITAL**

Perangkat digital seperti gawai atau peranti komputer yang kita miliki adalah alat utama yang bisa digunakan untuk mengakses internet dan berselancar di dunia maya. Secara standar perangkat ini sudah dirancang dengan segudang fitur pengaman untuk memastikan aktivitas kita saat bermedia digital aman dan nyaman. Namun setiap teknologi memiliki beragam celah yang bisa dimanfaatkan orang yang tidak bertanggung jawab. Faktanya, salah satu celah terbesar dalam teknologi digital ada pada pengguna, baik karena pengguna lalai dalam mengoperasikan perangkat maupun lupa mengaktifkan fitur pengaman.

Perangkat digital memiliki peran vital dalam melakukan aktivitas digital. Misalnya ketika kita melakukan komunikasi seringkali kita menggunakan gawai yang terkoneksi dengan jaringan internet pada keseharian kita, sehingga dalam menggunakan perangkat digital kita perlu melakukan proteksi terhadap perangkat digital yang kita miliki. Sebuah perangkat digital selalu terdiri dari dua kelompok komponen utama: perangkat keras dan perangkat lunak. Perangkat keras adalah perangkat yang secara fisik bisa kita lihat dan pegang, seperti layar ponsel, monitor, *keyboard*, *hard disk*, dan kartu penyimpanan. Sedangkan perangkat lunak merupakan aplikasi dan program yang ditanamkan di dalam perangkat untuk membuatnya mampu bekerja dengan baik. Kedua komponen ini saling terkait sehingga upaya pengamanannya pun dilakukan secara berkesinambungan.

Mengapa penting melakukan proteksi perangkat digital? Perangkat digital yang kita miliki saat ini menjadi kunci untuk beragam aktivitas digital. Tidak hanya mencari hiburan, melainkan juga bertransaksi secara daring. Di dalam perangkat digital kita tersimpan beragam informasi penting. Mulai dari galeri foto dan video pribadi, daftar kontak, sampai data-data keuangan yang diperlukan bertransaksi termasuk uang digital. Karena pentingnya isi di dalam perangkat digital, teknologi ini sering menjadi incaran upaya peretasan. Jika upaya tersebut berhasil maka pengguna perangkat digital akan mengalami kerugian atas

berbagai kebocoran data pribadi yang bisa mengakibatkan keamanan privasi kita menjadi terganggu. Proteksi perangkat digital juga bertujuan agar perangkat digital yang kita gunakan tidak disalahgunakan oleh orang lain misalnya ketika ponsel pintar kita dilengkapi dengan proteksi seperti kata sandi atau *fingerprint* maka ponsel kita tidak bisa digunakan oleh orang lain.

Bab ini mengajak kita untuk mempelajari keutamaan dan pentingnya proteksi (perlindungan) terhadap perangkat digital serta mengenali jenis-jenis fitur proteksi perangkat digital. Selain itu, melalui bab ini, kita juga akan memahami upaya dan konsekuensi untuk proteksi digital sekaligus mempraktikkan kemampuan ini untuk proteksi perangkat digital melalui lembar evaluasi kerja yang harus dikerjakan di akhir bab. Yang terpenting, bab ini juga mengajak untuk memahami konteks yang lebih luas, bahwa proteksi perangkat digital bukan hanya tanggung jawab individu semata sebagai pengguna melainkan juga sebagai pengajar serta pegiat literasi digital yang sama-sama mempunyai kewajiban untuk menguasai kecakapan proteksi perangkat digital.

Bagi pengajar atau pegiat literasi digital, bab ini bisa dimanfaatkan untuk melakukan berbagai program guna meningkatkan kompetensi *Digital Safety* (keamanan digital) peserta ajar atau target program tersebut. Pada akhir bab juga tersedia panduan evaluasi untuk mengukur kemampuan memahami dan melindungi perangkat digital.

## **MEMPROTEKSI PERANGKAT DIGITAL**

Proteksi perangkat digital pada dasarnya merupakan perlindungan yang bertujuan untuk melindungi perangkat digital dari berbagai ancaman *malware*. *Malware*, singkatan dari *malicious software*, adalah perangkat lunak yang dirancang untuk mengontrol perangkat secara diam-diam, bisa mencuri informasi pribadi milik kita atau uang dari pemilik perangkat. Perangkat lunak perusak telah digunakan untuk mencuri sandi dan nomor akun dari ponsel, komputer, tablet dengan cara membebankan biaya palsu pada akun pengguna, dan bahkan melacak lokasi dan aktivitas pengguna tanpa sepengetahuan mereka (Lookout.com, 2020).



Penelitian status yang dilakukan Lookout menunjukkan bahwa perilaku pengguna dan geografi sangat memengaruhi risiko dalam menghadapi perangkat lunak jahat. Cara paling aman untuk menghindari program semacam itu adalah dengan mengunduh aplikasi yang sudah banyak digunakan, serta terpercaya dengan cara melihat ulasan dari pengunduh aplikasi tersebut. Beberapa aplikasi yang terpercaya tersebut adalah Google Play atau Appstore (Lookout.com, 2020).

Dalam menjalankan upaya penipuan, peretas biasanya menyamarkan *malware* sebagai aplikasi seluler yang tampak aman di toko aplikasi dan situs web. Misalnya kita selama ini mengenal aplikasi permainan *Angry Birds* sebagai aplikasi yang aman. Peretas kemudian berusaha membuat program tiruan yang berisi *malware* dengan iming-iming semua level yang berbayar bisa terbuka secara gratis. Aplikasi tiruan ini biasanya diedarkan di luar toko aplikasi resmi. Ketika pengguna mengunduhnya, tanpa dia sadari pengguna itu tengah memasukkan aplikasi tiruan yang membahayakan perangkat digital dan data yang ada di dalamnya (Lookout.com, 2020).

Meskipun sudah ada upaya untuk menghindari mengunduh perangkat dari luar situs resmi, ternyata, pengunduhan aplikasi yang cermat dan teliti tidak selalu meminimalkan risiko. Hal ini disebabkan karena ada situs-situs yang dengan curang memaksa perangkat untuk melakukan unduh otomatis ketika situs tersebut diakses aplikasi-aplikasi peramban (*browser*) masa kini seperti Google Chrome atau Mozilla Firefox sebenarnya sudah mengantisipasi hal ini dan akan memberikan deteksi bila pengguna masuk ke situs yang berbahaya. Namun kita tetap harus berhati-hati dan tidak disarankan untuk menginstal unduhan secara acak dari pengelola unduhan.

Data menunjukkan bahwa tingkat kasus *malware* di Indonesia termasuk yang tertinggi. Microsoft telah meluncurkan hasil riset Asia Pasifik di edisi terbaru *Security Endpoint Threat Report 2019* yang mengungkapkan bahwa Indonesia memiliki tingkat *malware* tertinggi di kawasan Asia. Temuan ini berasal dari analisis dari beragam sumber data Microsoft, termasuk delapan triliun sinyal ancaman yang diterima dan dianalisis oleh Microsoft setiap hari, mencakup periode 12 bulan, dari Januari hingga Desember 2019 (Microsoft Indonesia, 2019).

Sejak mulainya wabah COVID-19, data *tim Microsoft Intelligence Protection* menunjukkan bahwa setiap negara di dunia telah melihat setidaknya satu serangan digital bertema COVID-19. Volume serangan yang berhasil di negara-negara yang terkena wabah tampaknya naik, karena meningkatnya ketakutan dan keinginan informasi terkini. Dari jutaan pesan penipuan yang ditargetkan secara global setiap harinya, sekitar 60.000 diantaranya bertema COVID-19, dengan lampiran berbahaya atau URL (alamat website) jahat. Penyerang menyamar sebagai entitas mapan seperti Organisasi Kesehatan Dunia (WHO), Pusat Pengendalian dan Pencegahan Penyakit (CDC), dan Kementerian Kesehatan untuk masuk ke kotak inbox (Microsoft Indonesia, 2019). Hal ini menunjukkan bagaimana peretas cerdas dalam melakukan berbagai tipu daya untuk menembus proteksi perangkat digital kita. Salah satunya dengan memanfaatkan naluri alami manusia yang serba ingin tahu dan khawatir jika ada ancaman yang belum dikenali.

Microsoft menjelaskan, penyerang menggunakan infrastruktur yang ada, seperti *ransomware*, *phishing*, dan alat pengiriman *malware* lainnya, dan memasukkan kata kunci COVID-19, untuk memanfaatkan ketakutan massal. Setelah pengguna mengklik tautan berbahaya ini, penyerang dapat menyusup ke jaringan, mencuri informasi, dan mendapatkan uang dari serangan mereka (Microsoft Indonesia, 2020).

Pemahaman mengenai proteksi perangkat digital harus dimiliki oleh pengguna perangkat seperti telepon pintar, tablet, dan komputer karena aktivitas penggunaan perangkat tersebut sangat rentan dan memiliki banyak risiko yang kemudian bisa terjadi dikemudian hari. Risiko lainnya yang mungkin saja terjadi pada perangkat digital yang kita miliki jika tidak diproteksi dengan benar adalah kegiatan mengakses data dan dokumen pribadi yang bisa dilakukan oleh orang yang paham teknologi dan informasi, seperti kasus viral di media sosial yang dihebohkan dengan aksi tukang servis *handphone* yang membongkar galeri pelanggan demi mencari foto dan video bugil terungkap dan kemudian viral. Modus mereka adalah melihat-lihat file foto dan video di telepon pintar yang sudah diperbaiki dengan harapan menemukan foto atau video bugil dari pemiliknya.

Akun Twitter @ndagels pada Jumat (29/1/2021) mengunggah beberapa tangkapan layar akun Facebook yang identitasnya disamarkan. Dalam tangkapan layar tersebut tertulis beberapa pengakuan teknisi servis ponsel yang membuka galeri pelanggan dan menemukan foto serta video bugil (BeritaHits.id, 2021).



Gambar II.1

Screenshot Posting Viral Teknisi Servis Ponsel

Sumber : Twitter @ndagels

Unggahan dengan nama disamarkan kemudian dengan memberi *caption* “penyakit yang tidak kunjung sembuh, selalu penasaran lihat isi galeri, bagaimana dengan para suhu disini?” postingan ini diunggah dalam grup teknisi servis telepon pintar dan laptop selanjutnya muncul komentar dari akun Facebook lainnya yang mengakui pernah melakukan hal serupa.

Kasus tersebut mengingatkan kita akan pentingnya sikap bijak dalam menggunakan perangkat digital, karena seringkali kita menyimpan dokumen sensitif seperti foto diri maupun, video keseharian kita bersama pasangan. Kasus penyebaran video pribadi yang terjadi pada salah satu artis di Indonesia juga bisa menjadi perhatian kita. Berdasarkan penjelasan dari Kabid Humas Polda Metro Jaya Kombes Pol Yusri Yunus mengatakan, artis tersebut sempat mengakui bahwa sebelum beredar video seks tersebut, telepon pintar miliknya rusak dan dititipkan di saudaranya (Kompas.com, 2020). Artis tersebut mengaku telah menghapus video tersebut pada perangkat lainnya kemudian memberikannya ke manajer pribadinya.

Kasus-kasus tersebut memberikan pembelajaran bagi kita pengguna perangkat digital untuk selalu menggunakan perangkat digital untuk hal yang positif. Proses penghapusan dokumen yang tersimpan pada perangkat digital pada dasarnya tidak semuanya akan terhapus secara permanen, meskipun sudah dihapus tetapi dokumen yang berada di perangkat digital belum sepenuhnya terhapus, sehingga pihak yang paham teknologi seperti tukang servis telepon pintar dan laptop dengan mudah dapat mengembalikan *file* yang sudah dihapus di perangkat digital kita.

Seberapa pentingnya proteksi perangkat digital? jawabannya sangat penting karena dengan memahami perlindungan perangkat digital, sebagai pengguna ponsel pintar atau komputer akan menjadikan data-data yang berada di perangkat digital tidak mudah diakses oleh orang lain. Dengan perlindungan perangkat digital yang optimal maka upaya kita untuk tetap dapat menggunakan perangkat digital secara lebih nyaman untuk menunjang aktivitas ataupun pekerjaan sehari-hari pun bisa dilakukan.

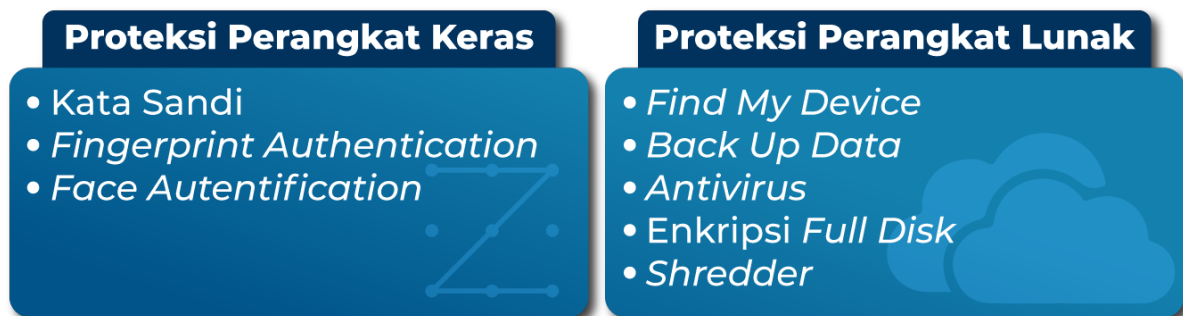
### **JENIS-JENIS FITUR PROTEKSI PERANGKAT DIGITAL**

Perangkat digital yang beredar saat ini sebenarnya sudah dirancang supaya aman meskipun digunakan oleh pengguna yang awam sekalipun. Untuk proteksi perangkat keras, kita mengenal beberapa fitur, seperti kata sandi, autentikasi dengan sidik jari, maupun autentikasi wajah. Sedangkan perangkat lunak dilindungi oleh sistem pengamanan bawah sistem operasi yang ada pada perangkat. Prinsipnya, selama kita selalu menggunakan produk yang asli, sistem operasi ini akan terus memperbarui diri agar mampu mengimbangi berbagai varian *malware* baru.

Namun kita sebagai pengguna seringkali mengabaikan fitur-fitur tersebut dan lebih memilih untuk tidak memasangnya pada perangkat digital yang kita miliki. Bahkan terkadang memilih menggunakan *software* bajakan atau mengunduh aplikasi dari situs yang tidak bisa dipercaya keamanannya. Praktik semacam ini lah yang kerap kali membuat perangkat digital kita menjadi mudah dibobol oleh peretas.

Ketika pertama kali menggunakan perangkat, pastikan menggunakan praktik keamanan terdepan di yang terintegrasi dengan seluruh layanan pendukung produk digital untuk

membantu menjaga keamanan perangkat. Pengamanan berlapis sangat penting untukantisipasi perlindungan data pribadi pengguna sekaligus memberikan fleksibilitas kepada pengguna dalam menggunakan perangkat seluler guna menunjang produktivitas secara aman penting dan menjaga privasi pengguna (Android Open Source Project, 2018). Jika dirasa perlu ditambahkan, kita juga bisa menambahkan fitur proteksi perangkat digital ekstra untuk memperkuat proteksi perangkat digital yang kita miliki. Sebagai contoh, kita bisa menggunakan fitur *remote wipe*, *back up data*, antivirus, enkripsi *full disk* dan *shredder*. Patut diingat, fitur ini bersifat opsional, artinya jika kita tidak terlalu banyak menggunakan perangkat digital untuk aktivitas yang berisiko, perangkat tambahan ini tidak terlalu dibutuhkan.



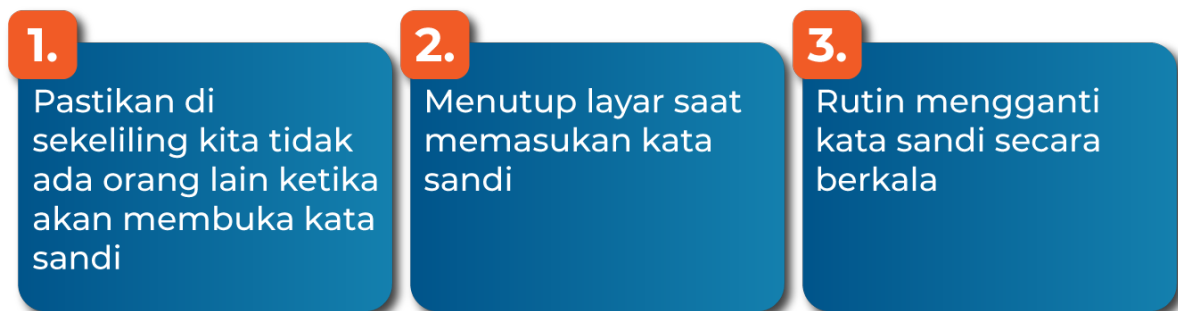
Bagan II.1

Jenis-Jenis Fitur Proteksi Perangkat keras (*kiri*) dan perangkat lunak (*kanan*)

### Memanfaatkan Fitur Kata Sandi

Perangkat digital seperti ponsel pintar, tablet dan komputer tentunya memiliki proteksi berupa fitur kata sandi, yang sering kita gunakan untuk mengamankan perangkat digital yang kita punya. Fitur kata sandi dalam telepon pintar, tablet, laptop, komputer biasanya berupa angka dan ada juga yang berbentuk pola. Fitur kata sandi memang masih memiliki beberapa kelemahan, misalnya kata sandi yang kita gunakan, diketahui oleh orang terdekat, hal ini bisa mengakibatkan telepon pintar, laptop, komputer bisa diakses oleh orang lain. Sehingga ketika kita menggunakan fitur proteksi menggunakan kata sandi harus benar-benar merahasiakan dari orang lain demi keamanan data-data pribadi yang berada di perangkat digital.

Cara pengaturan kata sandi biasanya bisa ditemui pada menu pengaturan pada setiap perangkat. Setiap perangkat digital memiliki pola pengaturan yang berbeda sehingga ada baiknya kita merujuk pada buku panduan pengguna atau mencari solusi di Internet maupun bertanya langsung pada layanan pelanggan. Pastikan kata sandi yang kita buat menggunakan kombinasi angka dan huruf agar kata sandi lebih kuat. Berikut cara aman untuk menghindari kata sandi kita diketahui oleh orang lain.



Bagan II.2

Cara aman menggunakan kata sandi

Ketika kita menggunakan fitur kata sandi, beberapa hal yang perlu diketahui dan diantisipasi yaitu jangan sampai kata sandi yang sudah kita atur diketahui oleh orang lain, cara yang tepat untuk menghindari terjadinya orang lain mengetahui kata sandi kita adalah dengan selalu melihat sekeliling kita ketika akan membuka kata sandi, usahakan ketika kita memasukan kata sandi berupa huruf dan angka, di sekeliling kita tidak ada orang lain, kita juga bisa menutup layar ketika memasukkan kata sandi dengan menggunakan tangan untuk menghindari orang lain mengetahui kata sandi perangkat digital yang kita miliki. Cara selanjutnya usahakan rutin mengubah kata sandi perangkat digital yang kita gunakan, bisa dilakukan seminggu satu kali perubahan kata sandi.

### **Fitur *Fingerprint Authentication***

Fitur Kunci Pencocokan sidik jari (*Fingerprint authentication*) merupakan fitur perlindungan perangkat ponsel dengan sistem deteksi sidik jari. Fitur ini bekerja dengan cara menyesuaikan sidik jari pengguna ponsel agar bisa membuka ponsel, sehingga orang lain tidak mudah untuk membuka ponsel karena sidik jari setiap orang tentunya berbeda. Fitur ini menggunakan *Fingerprint Hardware Interface Description Language* (HIDL) untuk

terhubung ke pustaka khusus vendor dan perangkat keras *fingerprint*, seperti sensor *fingerprint*.

Fitur *fingerprint authentication* merupakan salah satu fitur proteksi perangkat digital yang memiliki proteksi yang cukup baik. Fitur ini memiliki kelebihan dari fitur kata sandi misalnya kita menggunakan fitur sidik jari ini, meskipun orang lain melihat cara kita membuka ponsel tetapi mereka akan tetap tidak bisa untuk membuka ponsel kita karena sidik jari setiap orang memiliki bentuk yang berbeda-beda. Patut diingat, tidak semua perangkat digital dibekali dengan fitur ini sehingga kita perlu untuk melihat buku panduan perangkat yang kita gunakan untuk memastikan apakah perangkat kita sudah mendukung fitur sidik jari atau belum.

#### **Fitur Pencocokan Wajah (*Face Authentication*)**

Pencocokan wajah (*face authentication*) merupakan fitur kunci ponsel dengan menyocokkan wajah pengguna untuk membuka kunci perangkat mereka. Fitur ini bekerja dengan mendeteksi wajah pengguna menggunakan kamera depan ponsel. Ketika wajah terdeteksi cocok dengan data yang sudah diatur maka ponsel akan membuka kuncinya.

Proteksi menggunakan fitur ini memiliki tingkat keamanan yang tinggi karena pada beberapa teknologi terkini fitur ini tidak bisa ditembus dengan foto wajah atau wajah orang yang mirip. Untuk membukanya harus dilakukan dengan paksa dengan membobol sistem operasi perangkat digital secara menyeluruh. Walaupun kuat, fitur *face authentication* memiliki beberapa kelemahan, misalnya dalam langkah membuka kunci menggunakan fitur wajah sistem kunci ini mengharuskan wajah kita tidak terhalang oleh apapun. Oleh karena itu, bagi beberapa orang fitur ini justru merepotkan, terlebih ketika harus digunakan di tempat umum dimana kita biasanya mengenakan masker, kaca mata, maupun aksesoris kepala lainnya.

#### **Fitur Cari Perangkat Saya (*Find My Device*)**

Perangkat digital *mobile* memiliki kelemahan, kita bisa dengan mudah kehilangan baik karena lupa menempatkannya atau menjadi korban kejahatan. Untuk kondisi semacam ini

sejumlah perangkat digital terbaru sudah dibekali fitur *find my device* atau cari perangkat saya.

Fitur Cari Perangkat Saya (*Find My Device*) ini merupakan fitur yang bisa diaktifkan untuk mencari perangkat digital yang hilang, mengunci file, bahkan melakukan *remote wipe*. *Remote wipe* atau penghapusan jarak jauh merupakan langkah yang bisa kita gunakan ketika ponsel kita hilang atau dicuri. *Remote wipe* akan mengatur ponsel kita kembali ke mode pabrik dan menghapus semua data dan aplikasi yang ada di dalamnya. Sehingga ketika ada orang lain yang mendapatkan dan berniat buruk, data pribadi kita akan tetap aman.

Fitur *remote wipe* ini bisa diakses dengan menghubungi pusat bantuan masing-masing perangkat. Harus diingat, beberapa perangkat tipe lama memerlukan langkah tambahan untuk mengaktifkan fitur ini. Seperti fitur-fitur lainnya, pengaturan fitur ini akan berbeda untuk setiap perangkat sehingga merujuk pada panduan pengguna dan menghubungi *customer service* produk adalah langkah yang bijak.

### **Memahami dan Melindungi dengan Fitur *Back-up Data***

*Back-up* data atau membuat cadangan data merupakan langkah yang digunakan untuk mencegah kehilangan data yang ada di telepon pintar, tablet, komputer dan laptop. Seringkali dalam menggunakan perangkat digital, kita memiliki data-data yang penting seperti foto, video, dokumen dan arsip penting. Untuk melindungi data tersebut kita bisa melakukan *back up data* secara rutin ke internet maupun melalui aplikasi yang dapat dipasang di perangkat, seperti *Dropbox*, *OneDrive*, dan *iCloud*. Selain itu sejumlah aplikasi juga memiliki fitur pencadangan otomatis yang mempermudah kita dalam mengelola data. WhatsApp misalnya secara berkala mencadangkan pesan-pesan yang pernah kita buat. Sedangkan aplikasi kontak yang ada di ponsel kita juga dapat diintegrasikan secara otomatis ke pusat penyimpanan data yang sudah ditetapkan oleh produsen ponsel.

Kita dapat mencadangkan dan memulihkan perangkat seluler, serta mengakses dan memulihkan file dari cadangan menggunakan aplikasi seluler. Seperti yang sudah disebutkan sebelumnya, dengan *backup* daring, kita harus selalu memastikan bahwa enkripsi digunakan



untuk mentransfer dan menyimpan data kita, sehingga hanya kita yang dapat mengaksesnya. (Sammons & Cross, 2016). Sedangkan untuk data-data pekerjaan, saat ini layanan penyimpanan *cloud* sudah cukup populer digunakan sebagai penyimpanan data daring yang aman dari potensi kerusakan perangkat keras. Banyak layanan penyedia layanan penyimpanan *cloud*. Beberapa yang cukup familiar adalah Google Drive dan OneDrive milik Microsoft. Tinggal membuat akun dan kita bisa memanfaatkan fitur ini untuk mencadangkan data-data pekerjaan kita. Pastikan menggunakan kata sandi yang aman agar penyimpanan daring ini tidak dibuka orang lain.

### **Kemampuan Memahami dan proteksi perangkat digital dengan Fitur Antivirus “Lookout”**

Pertahanan utama perangkat digital terhadap *malware* adalah menggunakan perangkat lunak yang baik untuk melindungi sistem perangkat digital. Meskipun ada sejumlah program antivirus di pasaran, program yang kita pilih harus memiliki reputasi yang baik. Perangkat lunak harus fokus pada jenis perlindungan ini, dan bukan program yang menyertakan fitur antivirus sebagai pertimbangan. Dalam memilih proteksi antivirus, biaya tidak harus menjadi perhatian (Sammons & Cross, 2016). Antivirus menjadi perlindungan bagi berbagai perangkat komputer, termasuk ponsel pintar. Aplikasi antivirus sangat banyak dan mudah untuk diakses selain itu beberapa ponsel juga sudah memiliki antivirus yang langsung ada tanpa harus menginstal.

Fitur proteksi antivirus pada perangkat digital terkadang diperlukan, karena seringkali virus seperti *malware* bekerja pada sistem perangkat lunak, hal tersebut jika dibiarkan akan mengakibatkan masalah pada perangkat keras yang kemudian bisa menjadikan perangkat digital kita mengalami kerusakan. Untuk memilih antivirus yang cocok, ada baiknya berkonsultasi dengan teknisi komputer atau ponsel yang berpengalaman. Mereka juga dapat merekomendasikan serentan apa perilaku bermedia digital kita dan menentukan apakah kita memerlukan perlindungan virus secara maksimal atau cukup pada level standar.

### **Kemampuan Memahami dan langkah menggunakan fitur Enkripsi *Full Disk***

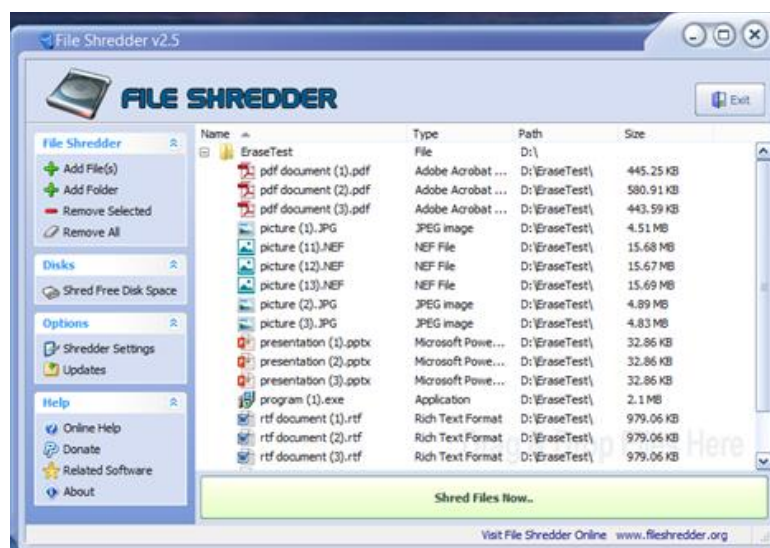
*Full disk encryption* memungkinkan seluruh kapasitas *hard drive computer* untuk dienkripsi, mencakup sistem, program, dan semua data yang tersimpan di dalamnya. Sehingga data

tidak dapat diakses tanpa mengetahui kata kunci yang telah diatur. Enkripsi adalah proses penyandian pesan sehingga hanya mereka yang berwenang untuk melihat data yang dapat membacanya. Tanpa enkripsi, pesan disebut sebagai teks biasa, tetapi ketika algoritma diterapkan, pesan menjadi acak dan disebut teks sandi (Sammons & Cross, 2016).

Bagi pengguna perangkat digital secara umum fitur ini termasuk ke dalam fitur untuk pengguna tingkat lanjut karena memerlukan pemahaman tentang teknik komputer yang cukup sebelum melakukan pengaturan data secara mendalam. Kami merekomendasikan untuk berkonsultasi dengan teknisi komputer yang sudah berpengalaman dan terpercaya untuk menentukan apakah perangkat digital yang kita miliki memerlukan fitur ini. Namun jika merasa cukup yakin dengan keterampilan teknik komputer, kita bisa memanfaatkan aplikasi enkripsi seperti *Bitlocker* yang biasanya sudah tersedia dalam sistem operasi komputer yang kita miliki.

### Kemampuan Memahami dan Menggunakan Fitur *Shredder*

*Shredder* merupakan fitur yang mampu memusnahkan data secara total sehingga tidak dapat dimanfaatkan oleh pihak lain, sebab menghapus data saja tidak menjamin data terhapus sepenuhnya, data tersebut tetap bisa dimunculkan kembali dengan perangkat lunak tertentu. *Shredder* bukanlah fitur untuk mengenkripsi, namun fitur pemusnah data ini biasanya menjadi satu kesatuan di dalam aplikasi enkripsi (wartaekonomi.co.id, 2017)



Gambar II.2

## Tampilan aplikasi File Shredder

Sumber : (r-hComp.com,2016)

Fitur ini menjadi salah satu fitur proteksi perangkat digital yang perlu diketahui karena, ketika kita menggunakan perangkat digital seringkali kita memiliki data-data privasi seperti foto, video dan dokumen yang sangat rahasia. *File Shredder* merupakan program yang bisa kita coba untuk menghapus file secara permanen sehingga data kita benar-benar terhapus dan tidak bisa diakses oleh orang lain. Aplikasi ini tetap mudah untuk digunakan. juga menambahkan pilihan menghapus pada saat kita mengklik kanan pada suatu file atau folder. Berikut situs web resminya bisa digunakan untuk mendownload aplikasi ini yaitu <http://www.files shredder.org/>.

## Mengelola perangkat Digital yang sudah rusak

Mengelola perangkat digital yang rusak sebelum menjual atau memindahtangankan perangkat digital bertujuan agar dokumen pribadi kita tidak disalahgunakan dikemudian hari. Hal ini bisa saja terjadi seperti contoh kasus yang telah dijelaskan di awal mengenai viralnya unggahan penyedia jasa reparasi ponsel yang dengan sengaja melihat dan membuka isi galeri dari pengguna ponsel, bayangkan bahwa di ponsel milik pribadi terdapat koleksi foto video yang berbaur sensitif kemudian kita lupa untuk menghapus datanya secara permanen, apa yang akan terjadi? Kasus video pribadi salah satu artis bisa menjadi salah satu pelajaran bagi kita dalam menggunakan perangkat digital.

Penelitian terbaru oleh para ahli perusahaan antivirus Kaspersky menemukan hampir 90% perangkat yang dijual (*second*) masih menyisakan data sensitif milik penggunanya. Sebagian besar perangkat ini belum dihapus seutuhnya saat akan dijual, sehingga informasi pemilik sebelumnya berisiko dapat diakses oleh pihak ketiga. Data yang ditemukan berkisar dari entri kalender berisi catatan rapat hingga foto dan video pribadi. Bahkan, dokumen pajak, informasi perbankan, kredensial *login* dan informasi medis dimana semua data ini akan berbahaya jika jatuh ke tangan yang salah (Republika.co.id, 2021).

Menurut Kepala Tim Analisis dan Riset Global Kaspersky Lab, Christian Funk, kesalahpahaman yang cukup umum dilakukan pengguna adalah hanya menghapus data

atau melakukan format ulang media penyimpanan. Cara ini hanya menghapus dari tampilan layar namun masih dapat dikembalikan dengan berbagai cara (Republika.co.id, 2021).

Pengelolaan perangkat digital dapat dilakukan dengan berbagai cara, sebelum menjual atau memindahtangankan perangkat digital, pengguna harus waspada. Berikut adalah saran Kaspersky untuk memastikan data telepon pintar benar-benar dihapus sebelum dijual/dipindahtangankan ke pengguna lain (Liputan6.com,2021):

1. Pastikan tempat penyimpanan file harus ditimpa alias *overwritten* agar tak bisa dipulihkan. Beberapa solusi keamanan seperti Kaspersky Total Security memiliki penghapus data jenis ini. Selanjutnya kita juga bisa menghapus data bawaan Windows sendiri, Cipher, yang biasanya dipakai untuk enkripsi, sekaligus digunakan untuk menghapus file dari *hardisk* atau membuatnya tidak dapat digunakan. Prioritas penjual adalah mengeluarkan informasi dan data pribadi dari gawai yang mau dijual sehingga data tetap pribadi. Cadangkan data, baik itu yang ada di gawai, komputer, kartu memori, atau penyimpan lain. Cadangkan dengan aman sebelum menghapus dari gawai yang mau dijual. Lepaskan SIM dan kartu penyimpanan dari telepon. Jika perangkat memakai eSIM, jangan lupa untuk menghapusnya. Aktifkan autentikasi dua faktor (2FA) untuk akun apa pun. Lalu, jangan lupa untuk *log out* dari semua layanan digital (perbankan, email, media sosial, dan lain-lain) dari gawai yang mau dijual. Lakukan reset pabrik (*factory reset*) atau format media.

Bagaimana jika ponsel pintar rusak? pengambilan data pada ponsel yang sudah rusak atau mengalami kerusakan di bagian layar atau komponen lain memiliki cara tersendiri. Apabila layar *smartphone* pecah dan tak nampak gambar apapun alias mati, maka butuh program *Virtual Network Computing* (VNC). Ada banyak pilihan tersedia di toko aplikasi, sebaiknya pilih versi yang dapat diakses secara cuma-cuma dan aman digunakan. VNC merupakan sebuah program yang memindahkan antarmuka Android menuju komputer sehingga segala sesuatu bisa dikendalikan langsung dari layar desktop. Untuk menggunakan salah satu program VNC, setidaknya perlu mengunduh dan memasang terlebih dahulu ke komputer serta perangkat Android. Selain versi cuma-cuma, terdapat versi berbayar yang mengusung lebih banyak fitur. Disarankan memilih program VNC versi berbayar untuk cakupan pemakaian lebih luas (Jalantikus.com, 2016).

### **Upaya dan Konsekuensi Proteksi Perangkat Digital**

Pelanggaran yang sering terjadi terhadap proteksi perangkat digital biasanya mengenai penyebaran data-data privasi pengguna perangkat digital yang sifatnya sensitif seperti video, foto dan dokumen penting, karena seseorang yang dengan sengaja melakukan pencurian data dari perangkat digital pasti memiliki tujuan dan maksud yang kurang baik, dalam kasus penyedia jasa reparasi gawai memperlihatkan bahwa penyedia jasa reparasi tersebut bisa dengan mudah melihat data-data yang bersifat privat dan bisa jadi data tersebut disebarkan kepada orang lain sehingga terjadi penyebaran privasi yang bersifat kesusilaan, jika ditinjau dari aspek hukum sesuai Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah melalui Undang-Undang No. 19 Tahun 2016 (UU ITE) Pasal 45 ayat (1) UU ITE mengatur “Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah).

Pada Rancangan Undang-Undang Perlindungan Data Pribadi, sesuai dengan versi yang dapat diakses pada saat tulisan ini dibuat, BAB XIV KETENTUAN PIDANA Pasal 42 mengatur Setiap orang yang melakukan pencurian dan atau pemalsuan data pribadi dengan tujuan untuk melakukan kejahatan dipidana dengan pidana penjara paling lama 1 (satu) tahun dan/atau denda paling banyak Rp300.000.000,- (tiga ratus juta rupiah) sehingga kejahatan yang dilakukan dengan merujuk pada pencurian data pribadi maka akan dikenakan sanksi. Dengan adanya peraturan tersebut harapannya tidak ada lagi kasus pelanggaran yang terjadi pada perangkat digital yang menyangkut privasi dan data pribadi meski proteksi perangkat digital harus tetap kita tingkatkan.

### **SIMPULAN DAN REKOMENDASI**

Pada akhirnya, proteksi perangkat digital memiliki peran yang sangat penting dalam setiap aktivitas yang menggunakan perangkat digital, dengan melakukan proteksi perangkat digital akan mencegah terjadinya pengambilan data pribadi secara sepihak, pengambilan data

pribadi yang dilakukan oleh pihak yang tidak bertanggung jawab tentunya memiliki risiko kerugian bagi pemilik data pribadi. Kita sebagai pengguna perangkat digital juga harus memahami penggunaan fitur-fitur proteksi perangkat digital sehingga semakin kita dapat mengenali berbagai fitur yang berguna untuk mendukung keamanan perangkat digital yang dimiliki atau dimanfaatkan dalam kehidupan keseharian, maka peranan kita untuk menciptakan lalu lintas yang sehat dalam arus informasi digital semakin nyata kontribusinya.

Berdasarkan uraian yang telah dijabarkan, maka upaya terhadap proteksi keamanan perangkat digital menghasilkan beberapa rekomendasi yang diberikan agar kita dapat secara bijak berperan dalam kepedulian terhadap perangkat digital yang dimiliki atau dimanfaatkan dalam aktivitas keseharian. **Pertama**, pastikan memilih perangkat digital di agen resmi; **Kedua**, sebaiknya teliti sebelum memiliki dengan mengecek kesesuaian kode perangkat yang tertulis di kemasan dan yang tertera di perangkat; **Ketiga**, biasakan untuk membaca buku panduan bagi pemilik perangkat untuk lebih mengenali perangkat; **Keempat**, pilihlah kata sandi dengan tingkatan paling aman dengan kode sandi yang mudah diingat pemilik perangkat; **Kelima**, tidak dengan mudah memperlihatkan atau meminjamkan perangkat digital ke orang lain tanpa pengawasan; **Keenam**, selalu waspada dengan tawaran situs-situs daring yang menggiurkan untuk kebutuhan konsumtif; **Ketujuh**, sebaiknya sterilkan atau kosongkan perangkat digital terlebih dahulu sebelum ingin mengganti dengan perangkat lainnya.

Dalam level pasar, sudah seharusnya pemangku kepentingan yang relevan baik pengusaha perangkat digital maupun pelaku pasar lainnya, bertanggung jawab untuk memberikan proteksi terhadap perangkat digital dengan sistem yang lebih baik lagi sehingga file dokumen pribadi dan data diri pengguna yang ada dalam sistem mereka terjaga dengan baik. Langkah-langkah menjaga keamanan harus diupayakan seoptimal mungkin baik di dalam sistem maupun dengan dimunculkan perangkat-perangkat yang mampu memproteksi perangkat digital dengan baik dan menjaga perangkat digital supaya tidak mudah untuk diambil alih oleh pihak-pihak yang merugikan

Dalam level negara, adalah kewajiban negara untuk melindungi dan menghadirkan keamanan bagi perangkat digital bagi data pribadi warga negaranya melalui kebijakan yang adil dan mengedepankan asas hak asasi manusia terhadap perlindungan diri di dunia maya.

Bab ini masih sangat terbuka untuk dikembangkan agar seluruh pemangku kepentingan mampu bertanggungjawab untuk proteksi perangkat digital. Pengembangan di masa depan bisa dilakukan dengan mempertimbangkan ragam khalayak yang akan disasar melalui pembelajaran maupun variasi program literasi digital. Ragam khalayak ini bisa dilihat dari pendekatan usianya, kelompok terpinggirkan (anak, perempuan, dan difabel), maupun masyarakat di kawasan 3T (terdepan, terluar dan tertinggal). Pertimbangan lain juga bisa dilihat dari langkah aksinya yang bisa bersifat individual atau kolaboratif, pendekatan aksi yang formal melalui kurikulum sekolah atau perguruan tinggi maupun yang informal melalui aneka program, maupun ruang yang akan digunakannya yakni daring atau luring.

Tabel II.1

Matriks rekomendasi program literasi digital  
untuk meningkatkan kecakapan proteksi perangkat digital

| Aspek/<br>Khalayak<br>Sasaran   | Anak dan<br>Remaja  | Perempuan  | Lansia  | 3T   | Difabel  |
|---|---|--|---|--|--|
| <b>Mengetahui<br/>dan<br/>Memahami<br/>proteksi<br/>Perangkat<br/>Digital<br/>dengan<br/>Fitur Kata<br/>Sandi</b> | Program formal melalui kurikulum program formal melalui sekolah terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi guru) | Pelatihan informal yang bisa ditujukan dengan kelompok perempuan tertentu dilihat dari usia maupun pekerjaan. Metode dilakukan dengan diskusi dan studi kasus yang isunya umum | Pembuatan program audio yang sederhana dalam bahasa daerah sehingga mudah dipahami lansia       | Pembuatan konten sederhana, tercetak dan mudah dibawa dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik | Pembuatan konten yang ramah di media yang bisa diakses difabel               |
|   | Program informal melalui ekstrakurikuler terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi)                             | Pelatihan informal yang bisa ditujukan dengan kelompok perempuan tertentu dilihat dari usia maupun pekerjaan. Metode dilakukan   | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat                          | Program diskusi yang sederhana sesuai dengan media yang bisa diakses difabel |



|   |  |  |   |  |  |
|---|--|--|---|--|--|
|   | orangtua)  | dengan diskusi dan studi kasus yang isu khusus tentang perempuan   |   |  |  |
| <b>Mengetahui dan Memahami proteksi perangkat digital dengan Fitur Fingerprint authentication</b> | Program formal melalui sekolah terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi guru) | Pelatihan informal yang bisa ditujukan dengan kelompok perempuan tertentu dilihat dari usia maupun pekerjaan. Metode dilakukan dengan diskusi dan studi kasus yang isunya umum | Pembuatan program audio yang sederhana dalam bahasa daerah sehingga mudah dipahami lansia       | Pembuatan konten sederhana, tercetak dan mudah dibawa dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik | Pembuatan konten yang ramah di media yang bisa diakses difabel               |
|   | program informal melalui ekstrakurikuler terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau        | Pelatihan informal yang bisa ditujukan dengan kelompok perempuan tertentu dilihat dari usia maupun pekerjaan. Metode   | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat                          | Program diskusi yang sederhana sesuai dengan media yang bisa diakses difabel |

|   |  |   |   |  |  |
|---|--|---|---|--|--|
|   | didampingi orangtua)   | dilakukan dengan diskusi dan studi kasus yang isunya umum                               |   |  |  |
| <b>Mengetahui dan menggunakan proteksi perangkat digital dengan Fitur Face Authentication</b> | Belum diperlukan untuk anak dibawah 13 tahun   | Pembuatan konten video yang mudah dipahami sehingga bisa mempraktikkan sendiri          | Pembuatan program audio yang sederhana dalam bahasa daerah sehingga mudah dipahami lansia       | Pembuatan konten sederhana, tercetak dan mudah dibawa dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik | Pembuatan konten yang ramah di media yang bisa diakses difabel               |
|   | program informal melalui ekstrakurikuler terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi | Pembuatan konten poster digital yang mudah dipahami sehingga bisa mempraktikkan sendiri | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat                          | Program diskusi yang sederhana sesuai dengan media yang bisa diakses difabel |

|   |   |   |   |  |  |
|---|---|---|---|--|--|
| <b>Mengetahui dan menggunakan proteksi perangkat digital dengan Fitur Remote Wipe</b> | Belum diperlukan untuk anak dibawah 13 tahun  | Pembuatan konten video yang mudah dipahami sehingga bisa mempraktikkan sendiri          | Pembuatan program audio yang sederhana dalam bahasa daerah sehingga mudah dipahami lansia       | Pembuatan konten sederhana, tercetak dan mudah dibawa dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik | Pembuatan konten yang ramah di media yang bisa diakses difabel               |
|   | program informal melalui ekstrakurikuler terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi) | Pembuatan konten poster digital yang mudah dipahami sehingga bisa mempraktikkan sendiri | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat                          | Program diskusi yang sederhana sesuai dengan media yang bisa diakses difabel |

|   |   |   |   |  |  |
|---|---|---|---|--|--|
| <b>Mengetahui dan menggunakan proteksi perangkat digital dengan Fitur Back-up Data</b>        | Belum diperlukan untuk anak dibawah 13 tahun  | Pembuatan konten video yang mudah dipahami sehingga bisa mempraktikkan sendiri          | Pembuatan program audio yang sederhana dalam bahasa daerah sehingga mudah dipahami lansia       | Pembuatan konten sederhana, tercetak dan mudah dibawa dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik | Pembuatan konten yang ramah di media yang bisa diakses difabel               |
|   | program informal melalui ekstrakurikuler terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi) | Pembuatan konten poster digital yang mudah dipahami sehingga bisa mempraktikkan sendiri | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat                          | Program diskusi yang sederhana sesuai dengan media yang bisa diakses difabel |
| <b>Mengetahui dan menggunakan proteksi perangkat digital dengan Fitur Antivirus "Lookout"</b> | Belum diperlukan untuk anak dibawah 13 tahun  | Pembuatan konten video yang mudah dipahami sehingga bisa mempraktikkan sendiri          | Pembuatan program audio yang sederhana dalam bahasa daerah sehingga mudah dipahami lansia       | Pembuatan konten sederhana, tercetak dan mudah dibawa dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik | Pembuatan konten yang ramah di media yang bisa diakses difabel               |

|  |   |   |   |  |  |
|--|---|---|---|--|--|
|  | program informal melalui ekstrakurikuler terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi) | Pembuatan konten poster digital yang mudah dipahami sehingga bisa mempraktikkan sendiri | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat                          | Program diskusi yang sederhana sesuai dengan media yang bisa diakses difabel |
| <b>Mengetahui dan menggunakan proteksi perangkat digital dengan fitur Enkripsi Full Disk</b> | Belum diperlukan untuk anak dibawah 13 tahun  | Pembuatan konten video yang mudah dipahami sehingga bisa mempraktikkan sendiri          | Pembuatan program audio yang sederhana dalam bahasa daerah sehingga mudah dipahami lansia       | Pembuatan konten sederhana, tercetak dan mudah dibawa dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik | Pembuatan konten yang ramah di media yang bisa diakses difabel               |
|  | program informal melalui ekstrakurikuler terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau             | Pembuatan konten poster digital yang mudah dipahami sehingga bisa mempraktikkan sendiri | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat                          | Program diskusi yang sederhana sesuai dengan media yang bisa diakses difabel |

|  |  |   |   |  |  |
|--|--|---|---|--|--|
|  | didampingi   |   |   |  |  |
| <b>Mengetahui dan menggunakan proteksi perangkat digital dengan Fitur Shredder</b> | Belum diperlukan untuk anak dibawah 13 tahun   | Pembuatan konten video yang mudah dipahami sehingga bisa mempraktikkan sendiri          | Pembuatan program audio yang sederhana dalam bahasa daerah sehingga mudah dipahami lansia       | Pembuatan konten sederhana, tercetak dan mudah dibawa dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik | Pembuatan konten yang ramah di media yang bisa diakses difabel               |
|  | program informal melalui ekstrakurikuler terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi | Pembuatan konten poster digital yang mudah dipahami sehingga bisa mempraktikkan sendiri | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat                          | Program diskusi yang sederhana sesuai dengan media yang bisa diakses difabel |

Dengan pengayaan khalayak maupun program di masa depan, baik di level individu, pasar dan negara, niscaya upaya proteksi perangkat digital akan lebih ditingkatkan, sehingga persoalan-persoalan terkait hal tersebut bisa diminimalisir sekuat mungkin dan keamanan digital bisa diciptakan.

Meskipun begitu, harus juga kita pahami konteks yang lebih luas, bahwa proteksi perangkat digital bukan hanya tanggung jawab individu semata, baik pengguna maupun pengajar serta pegiat literasi digital. Proteksi perangkat digital juga tanggung jawab pemangku kepentingan lainnya seperti pengelola perangkat digital, maupun pemerintah karena kemampuan memahami dan menggunakan fitur-fitur proteksi perangkat digital pada dasarnya harus dimiliki oleh setiap elemen dari para pengguna perangkat digital demi keamanan dokumen yang bersifat pribadi .

## EVALUASI KOMPETENSI PROTEKSI PERANGKAT DIGITAL

Evaluasi Proteksi perangkat digital digunakan untuk melakukan pengukuran terhadap kecakapan pengguna perangkat digital dalam melakukan proteksi perangkat digital, kita bisa melakukan evaluasi dalam tiga area. Pertama, aspek kognitif atau pengetahuan mengenai proteksi perangkat digital. Kedua, aspek afektif atau perasaan yang menunjukkan kesadaran pengguna perangkat digital akan pentingnya proteksi perangkat digital sebagai perwujudan tanggung jawab sebagai warga negara dan warga digital yang baik. Ketiga, aspek konatif atau *behavioral* untuk melihat sejauh mana pengetahuan dan kesadaran melakukan proteksi perangkat digital dalam kehidupan sehari-hari. Untuk memudahkan, tabel III.1 menjelaskan matriks kecakapan proteksi perangkat digital dalam ketiga aspek tersebut.

Tabel II.2

Evaluasi Kecakapan Proteksi Perangkat digital

| No. | Aspek<br>Perlindungan<br>Perangkat<br>digital | Domain Evaluasi             |                         |  |
|-----|---|-----------------------------|-------------------------|--|
|     |   | Kognitif                    | Afektif                 | Konatif/ <i>behavioral</i>                       |
| 1   | Memahami<br>dan                               | Mengetahui<br>konsep, jenis | Menyadari<br>pentingnya | Mempraktikkan proteksi<br>Perangkat digital bagi |

|   |  |  |  |   |
|---|--|--|--|---|
|   | melakukan proteksi Perangkat digital dengan berbagai jenis-jenis fitur                                     | serta konteks perlindungan (individu, pasar dan negara) terkait proteksi Perangkat digital | perlindungan proteksi Perangkat digital untuk diri sendiri, keluarga, maupun orang lain  | diri sendiri, keluarga maupun orang lain  |
| 2 | Memahami dan mengetahui cara penggunaan proteksi Perangkat digital dengan Fitur Kata Sandi                 | Mengetahui arti istilah Fitur Kata Sandi serta cara penggunaannya                          | Menyadari pentingnya penggunaan Fitur Kata Sandi sebagai salah satu cara melakukan proteksi Perangkat digital                        | Mempraktikan proteksi Perangkat digital dengan menggunakan Fitur Kata Sandi dengan benar                        |
| 3 | Memahami dan mengetahui cara penggunaan proteksi perangkat digital dengan Fitur Fingerprint authentication | Mengetahui arti istilah <i>Fitur Fingerprint authentication</i> serta cara penggunaannya   | Menyadari pentingnya penggunaan Fitur <i>Fingerprint authentication</i> sebagai salah satu cara melakukan proteksi perangkat digital | Mempraktikan proteksi perangkat digital dengan menggunakan Fitur <i>Fingerprint authentication</i> dengan benar |
| 4 | Memahami dan mengetahui  | Mengetahui arti istilah Fitur <i>Face Authentication</i>                                   | Menyadari pentingnya penggunaan Fitur  | Mempraktikan proteksi perangkat digital dengan menggunakan Fitur <i>Face</i>                                    |



|   |   |  |  |   |
|---|---|--|--|---|
|   | cara penggunaan proteksi perangkat digital dengan Fitur Face Authentication                         | serta cara penggunaannya   | <i>Face Authentication</i> sebagai salah satu cara melakukan proteksi perangkat digital                                | <i>Authentication</i> dengan benar  |
| 5 | Memahami dan mengetahui cara penggunaan proteksi perangkat digital dengan Fitur Remote Wipe         | Mengetahui arti istilah Fitur <i>Remote Wipe</i> serta cara penggunaannya  | Menyadari pentingnya penggunaan Fitur <i>Remote Wipe</i> sebagai salah satu cara melakukan proteksi perangkat digital  | Mempraktikan proteksi perangkat digital dengan menggunakan Fitur <i>Remote Wipe</i> dengan benar  |
| 6 | Memahami dan mengetahui cara penggunaan proteksi perangkat digital dengan Fitur <i>Back-up Data</i> | Mengetahui arti istilah Fitur <i>Back-up Data</i> serta cara penggunaannya | Menyadari pentingnya penggunaan Fitur <i>Back-up Data</i> sebagai salah satu cara melakukan proteksi perangkat digital | Mempraktikan proteksi perangkat digital dengan menggunakan Fitur <i>Back-up Data</i> dengan benar |
| 7 | Memahami dan mengetahui   | Mengetahui arti istilah Fitur <i>Antivirus</i>                             | Menyadari pentingnya penggunaan Fitur  | Mempraktikan proteksi perangkat digital dengan menggunakan Fitur                                  |

|   |   |  |  |   |
|---|---|--|--|---|
|   | cara penggunaan proteksi perangkat digital dengan Fitur <i>Antivirus "Lookout"</i>                        | <i>"Lookout"</i> serta cara penggunaannya  | <i>Antivirus "Lookout"</i> sebagai salah satu cara melakukan proteksi perangkat digital                                      | <i>Antivirus "Lookout"</i> dengan benar   |
| 8 | Memahami dan mengetahui cara penggunaan proteksi perangkat digital dengan fitur Enkripsi <i>Full Disk</i> | Mengetahui arti istilah fitur Enkripsi <i>Full Disk</i> serta cara penggunaannya | Menyadari pentingnya penggunaan fitur Enkripsi <i>Full Disk</i> sebagai salah satu cara melakukan proteksi perangkat digital | Mempraktikan proteksi perangkat digital dengan menggunakan fitur Enkripsi <i>Full Disk</i> dengan benar |
| 9 | Memahami dan mengetahui cara penggunaan proteksi perangkat digital dengan Fitur <i>Shredder</i>           | Mengetahui arti istilah <i>Fitur Shredder</i> serta cara penggunaannya           | Menyadari pentingnya penggunaan <i>Fitur Shredder</i> sebagai salah satu cara melakukan proteksi perangkat digital           | Mempraktikan proteksi perangkat digital dengan menggunakan <i>Fitur Shredder</i> dengan benar           |

#### CONTOH BENTUK EVALUASI UNTUK ASPEK KONATIF PRAKTIK PROTEKSI PERANGKAT DIGITAL

Isilah form evaluasi di bawah ini berdasarkan pengalaman sehari-hari untuk mengukur kecakapan Proteksi perangkat digital dari aspek konatif (*behavioral*). Kegiatan ini bisa dilakukan sendiri oleh pengguna perangkat digital sebagai pembelajar sebagai sebuah cara

untuk melakukan evaluasi diri (*self-assessment*). Selain itu, kegiatan ini bisa juga dilakukan oleh pengajar atau pegiat literasi digital untuk melakukan evaluasi terhadap anak didik atau peserta ajar atau peserta program literasi digital.

Tabel II.3

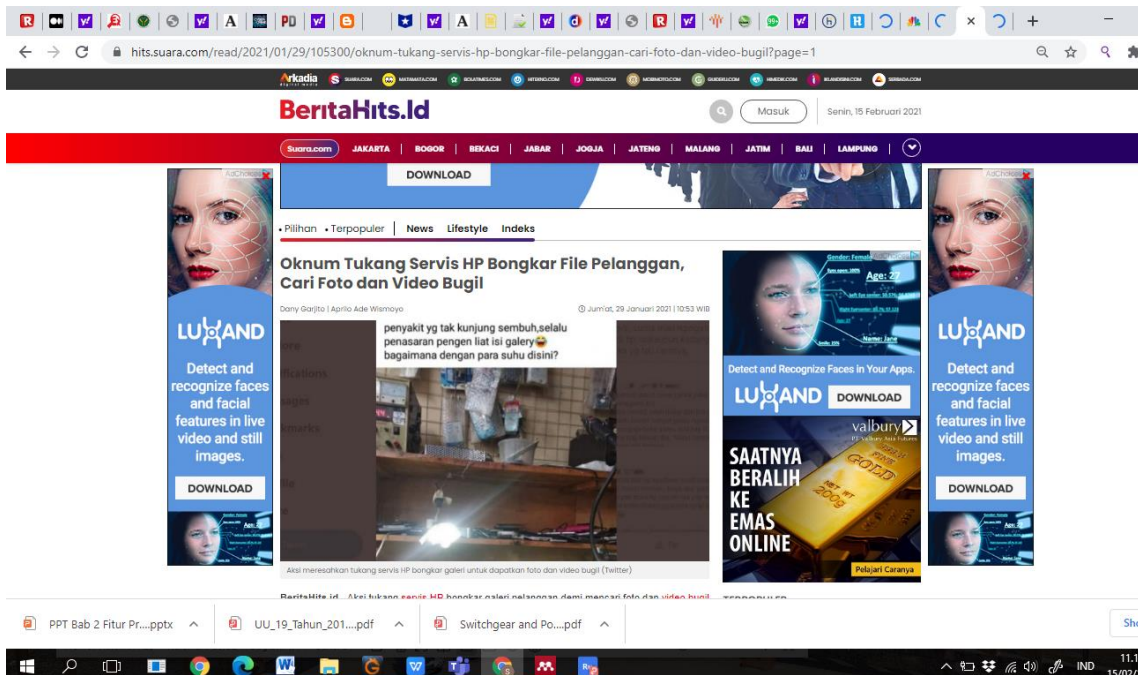
Evaluasi Kecakapan Proteksi Perangkat Digital dilihat dari Aspek Konatif (*Behavioral*)

| No | Pernyataan  | Berilah tanda V (centang) pada salah satu pilihan |        |        |               | Alasan |
|----|---|---|--------|--------|---------------|--------|
|    |   | Sangat Jarang                                     | Jarang | Sering | Sangat Sering |        |
| 1  | Menggunakan Fitur Proteksi perangkat digital lebih dari satu  |   |        |        |               |        |
| 2  | Merubah kata sandi, pola layar secara berkala   |   |        |        |               |        |
| 3  | Melakukan <i>Scan Antivirus</i> secara berkala  |   |        |        |               |        |
| 4  | Melakukan Back Up data agar data memiliki cadangan  |   |        |        |               |        |
| 5  | Menggunakan Fitur <i>Remote Wipe</i> untuk menemukan perangkat digital ketika kehilangan perangkat digital                  |   |        |        |               |        |
| 6  | Melakukan penghapusan data sebelum menjual, atau memberikan perangkat digital kepada orang lain                             |   |        |        |               |        |
| 7  | Menggunakan aplikasi VNC untuk memindahkan file dokumen pada perangkat digital yang rusak sebelum membawa ke tukang service |   |        |        |               |        |
| 8  | Menggunakan fitur Shredder untuk melakukan penghapusan file   |   |        |        |               |        |

|   |  |  |  |  |  |  |
|---|--|--|--|--|--|--|
|   | dokumen di perangkat digital secara permanen   |  |  |  |  |  |
| 9 | Melaporkan pada pengelola perangkat digital jika ada upaya tindakan mencurigakan terkait indikasi penyalahgunaan file dokumen pribadi kita |  |  |  |  |  |

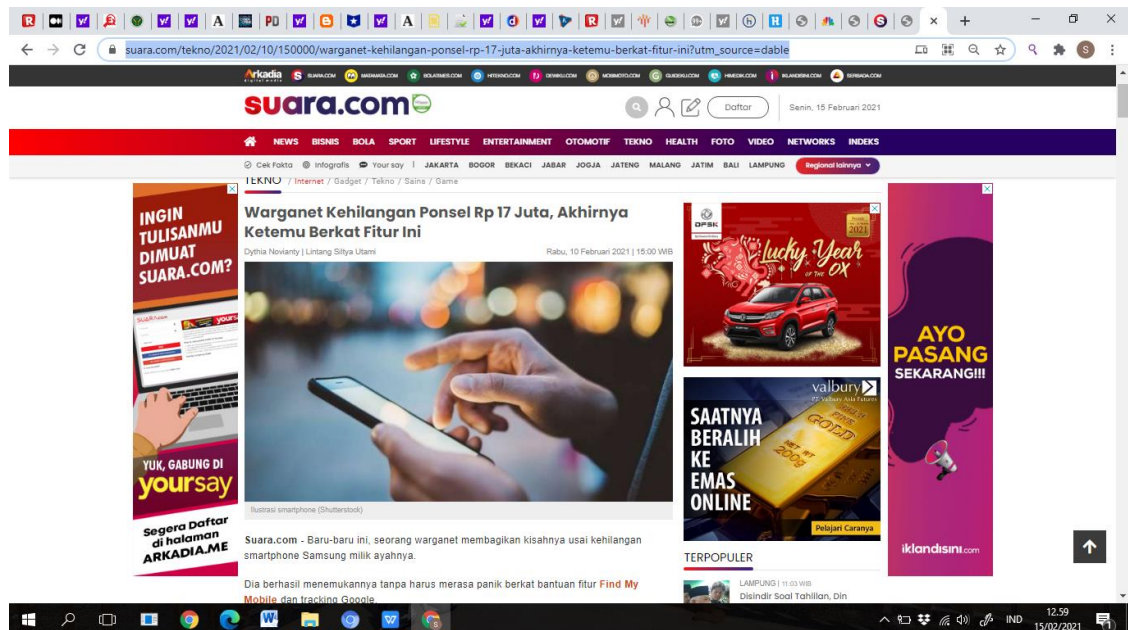
## Lembar Evaluasi

Disajikan kasus-kasus berikut untuk didiskusikan sesuai dengan aspek proteksi perangkat digital.

|   |   |
|---|---|
| 1 | <p>Akses Digital</p> <p><a href="https://www.suara.com/tekno/2021/02/10/150000/warganet-kehilangan-ponsel-rp-17-juta-akhirnya-ketemu-berkat-fitur-ini?utm_source=dable">https://www.suara.com/tekno/2021/02/10/150000/warganet-kehilangan-ponsel-rp-17-juta-akhirnya-ketemu-berkat-fitur-ini?utm_source=dable</a></p>                   |
| 2 | <p>Proteksi Perangkat Digital</p>  <p>Diskusikan kasus ini dari aspek Proteksi Perangkat digital , mengapa data dari perangkat digital bisa dengan mudah diakses orang lain ? Bagaimana cara memproteksinya ?</p> <p>Proteksi Perangkat digital</p> |

## Latihan 1

1. Bacalah Informasi Bergambar Dibawah Ini dengan baik !



Link : [https://www.suara.com/tekno/2021/02/10/150000/warganet-kehilangan-ponsel-rp-17-juta-akhirnya-ketemu-berkat-fitur-ini?utm\\_source=dable](https://www.suara.com/tekno/2021/02/10/150000/warganet-kehilangan-ponsel-rp-17-juta-akhirnya-ketemu-berkat-fitur-ini?utm_source=dable)

1. Setelah membaca Informasi Bergambar diatas isilah tabel berikut !

| No. | Pertanyaan Evaluasi  | Jawaban |       | Alasan |
|-----|--|---------|-------|--------|
|     |  | YA      | Tidak |        |
| 1.  | Apakah perlu menggunakan fitur proteksi digital ?  |         |       |        |
| 1.  | Apakah anda sudah mengaktifkan fitur proteksi digital ?  |         |       |        |
| 1.  | Apakah anda bisa mengoperasikan fitur proteksi perangkat digital sebagai alat pendukung proteksi perangkat ponsel anda ? |         |       |        |
| 1.  | Apakah anda akan memberitahukan kepada teman atau keluarga mengenai pentingnya proteksi perngkat digital ?               |         |       |        |

## DAFTAR PUSTAKA

Android Open Source Project. (2018, September 23). Android enterprise security white paper. *White Paper*.

- [https://source.android.com/security/reports/Google\\_Android\\_Enterprise\\_Security\\_Whitepaper\\_2018.pdf](https://source.android.com/security/reports/Google_Android_Enterprise_Security_Whitepaper_2018.pdf)
- Bustomi, M. I. (2020, Desember 30). Polisi selidiki penyebaran video syur Gisel dan Nobu dari ponsel yang rusak. *Kompas.com*. Diperoleh dari <https://megapolitan.kompas.com/read/2020/12/30/12271211/polisi-selidiki-penyebaran-video-syur-gisel-dan-nobu-dari-ponsel-yang>
- Garjito. D. (2021, Januari 29). Oknum tukang servis HP bongkar file pelanggan, cari foto dan vVdeo bugil. *BeritaHits.id*. Diperoleh dari <https://hits.suara.com/read/2021/01/29/105300/oknum-tukang-servis-hp-bongkar-file-pelanggan-cari-foto-dan-video-bugil?page=1>
- Kusumawardhani. N. Q. (2021, Februari 08). Tips sebelum menjual dan membeli pPerangkat second. *Republika.co.id*. Diperoleh dari
- Lookout.com. (2021) Should You worry about getting a cell phone virus? Diperoleh dari <https://www.lookout.com/know-your-mobile/android-virus>
- Microsoft Indonesia. (2020, Juni 26). Tingkat kasus malware di Indonesia tertinggi di Asia Pasifik: Laporan microsoft security endpoint threat 2019. Diperoleh dari <https://news.microsoft.com/id-id/2020/06/26/tingkat-kasus-malware-di-indonesia-tertinggi-di-asia-pasifik-laporan-microsoft-security-endpoint-threat-2019/><https://www.republika.co.id/berita/qo5uie368/tips-sebelum-menjual-dan-membeli-perangkat-emsecondem>
- r-hcomp.blogspot.com .(2016, Juni 07). Menghapus file secara permanen dengan file shredder. Diperoleh dari <https://rh-comp.blogspot.com/2016/06/menghapus-file-secara-permanen-dengan.html>
- Sammons, J., & Cross, M. (2016). The bBasics of cyber safety: Computer and mobile device safety made easy. In *the basics of cyber safety: Computer and mobile device safety made easy*.
- Prayogo. C. (2017, April 18) Ini 4 metode enkripsi untuk proteksi data digital. *Wartaekonomi.co.id* Diperoleh dari <https://www.wartaekonomi.co.id/read138222/ini-4-metode-enkripsi-untuk-proteksi-data-digital>

Wardani. A. S. (2021, Februari 05). Tips aman sebelum jual beli smartphone bekas. *Liputan6.com*. Diperoleh dari <https://www.liputan6.com/tekno/read/4475749/tips-aman-sebelum-jual-beli-smartphone-bekas>



# **BAB III**

---

## Perlindungan Identitas Digital dan Data Pribadi di Platform Digital



### **BAB III**

## **PERLINDUNGAN IDENTITAS DIGITAL DAN DATA PRIBADI DI *PLATFORM* DIGITAL**

*Novi Kurnia*

### **URGENSI PERLINDUNGAN IDENTITAS DIGITAL DAN DATA PRIBADI**

Sebagai pengguna *platform* digital, kita pasti menyimpan dan mengelola identitas digital dan data pribadi ke dalam *platform* tersebut. Persoalannya, perlindungan terhadap identitas digital dan data pribadi ini masih jadi persoalan di berbagai belahan dunia (Sammons & Cross, 2017). Apalagi, belum semua negara, termasuk Indonesia, mempunyai regulasi yang mengatur perlindungan data pribadi supaya hak warga negara di dunia digital bisa dijamin aspek hukumnya.

Skandal Cambridge Analytica tahun 2014, misalnya, merupakan kasus kebocoran data pribadi 87 juta pengguna Facebook yang menyeret *platform* raksasa ini ranah hukum. Komisi Perdagangan Federal AS (*Federal Trade Commission/FTC*) menjatuhkan denda US\$5 miliar atau sekitar Rp70 triliun sebagai denda terbesar yang pernah dijatuhkan FTC. Facebook juga diwajibkan memperbaiki sistem perlindungan data penggunanya (Kompas 2019, 25 Juli).

Kasus lain adalah bocornya 530.000 data sandi dan detil akun aplikasi Zoom, sebuah *platform video meeting* yang populer di masa pandemi pada April 2020. Kebocoran ini tidak terjadi dari aplikasi Zoom melainkan melalui peretasan sandi yang sama dengan sandi email penggunanya (Cnbcindonesia.com. 2020, April 16).

Di tanah air, bocornya 91 juta data pengguna aplikasi lokapasar (*e-commerce*) Tokopedia ditengarai bulan Juli 2020. Kasus ini diduga sebagai rentetan dari kebocoran yang terjadi pada bulan Mei yang melibatkan 15 juta data pengguna (Bernie 2020).

Data pribadi yang bocor dan akun yang diretas adalah contoh ancaman keamanan digital yang bisa membuat identitas digital dan data pribadi bisa dimanfaatkan pihak lain untuk

beragam kepentingan di luar pengetahuan penggunanya serta ada kemungkinan merugikan penggunanya. Padahal dalam menggunakan *platform* digital yang penggunanya sangat masif, terkumpulnya data pengguna menjadi *big data*, membuka peluang bocornya identitas digital dan data pribadi baik dalam proses penyimpanan maupun pemrosesan (Winarsih & Irwansyah 2020).

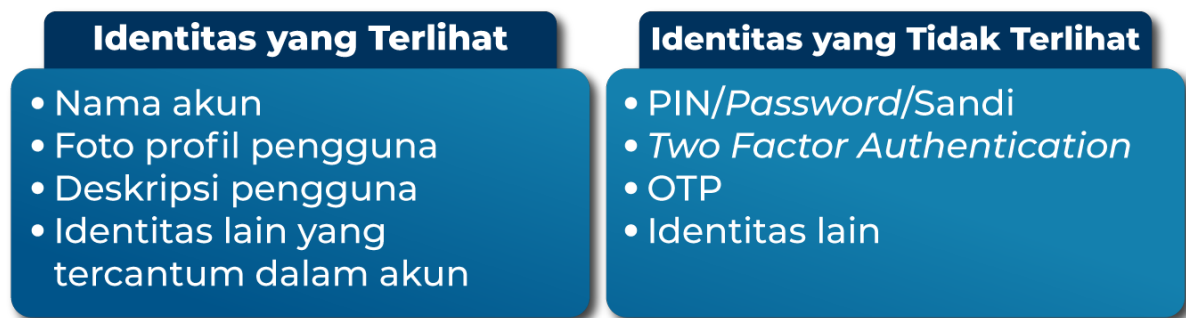
Bab ini disusun dengan tujuan agar pengguna *platform* digital, baik pembelajar maupun pengajar, mempunyai kemampuan untuk memahami dan melakukan perlindungan identitas digital dan data pribadi. Kemampuan ini sangat penting bagi warga negara yang secara individual mempunyai tanggung jawab menjaga keamanan digital bersama dengan memahami aspek hukum yang berlaku. Bab ini juga akan memberikan pemaparan dan panduan menggunakan *Personal Identification Number* (PIN), *Two-Factor Authentication* (2TFA), dan *One-Time Password* (OTP) agar bisa memaksimalkan perlindungan identitas digital dan data pribadi.

Dengan dilengkapi panduan evaluasi untuk mengukur kemampuan memahami dan melindungi identitas digital dan data pribadi pada pengguna media digital, bab ini bisa dimanfaatkan oleh pengajar atau pegiat literasi digital melakukan berbagai program guna meningkatkan kompetensi *Digital Safety* peserta ajar atau target program tersebut.

## **MEMAHAMI DAN MELINDUNGI IDENTITAS DIGITAL**

Kita mungkin pernah mendengar kasus pembajakan akun media sosial yang digunakan untuk penipuan yang melibatkan identitas digital penggunanya. Namun, apakah kita memahami apa yang disebut dengan identitas digital? Apakah kita juga memahami risiko yang mungkin timbul jika kita tidak mampu melindungi identitas digital? Apakah kita tahu, sadar dan mampu mempraktikkan berbagai cara melindungi identitas digital kita?

Identitas digital pada dasarnya adalah identitas seseorang sebagai pengguna *platform* media digital (Monggilo, Kurnia, & Banyumurti 2020). Terdapat dua jenis identitas digital baik yang terlihat maupun tidak terlihat sebagaimana dijelaskan dalam bagan III.1.



Bagan III.1

Jenis identitas digital

Sumber: Monggilo, Kurnia & Banyumurti (2020)

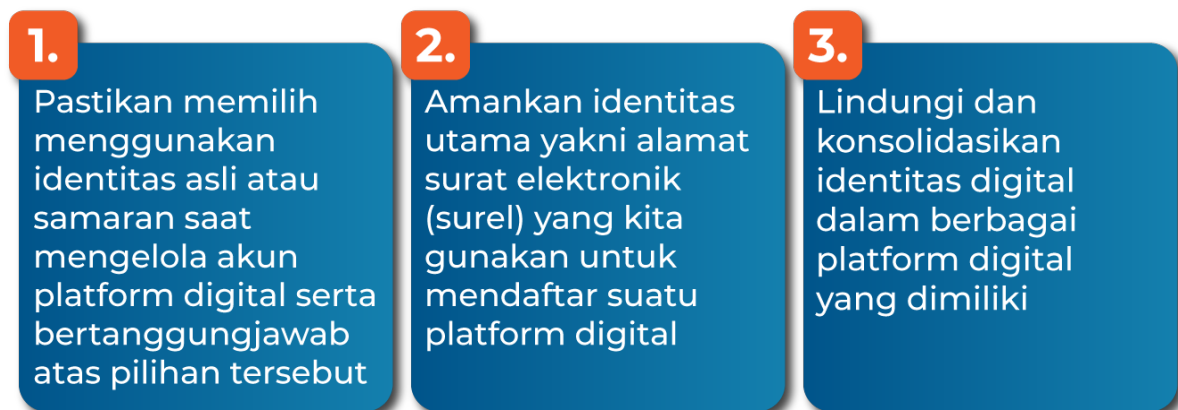
Identitas digital yang terlihat tidak selalu identik dengan identitas kita dalam kehidupan nyata yang merupakan rangkuman karakteristik kita baik yang bersifat tetap maupun tidak tetap (Monggilo, Kurnia & Banyumurti 2020). Identitas tetap berupa nama, tempat lahir, tanggal lahir, jenis kelamin, dan nama orang tua dan biasanya tercatat di berbagai kartu identitas seperti Kartu Keluarga (KK) dan Kartu Tanda Penduduk (KTP). Sedangkan identitas tidak tetap misalnya pekerjaan, alamat tinggal maupun penampilan fisik seperti warna rambut yang bisa berubah dengan cepat dan biasanya jarang tercatat di kartu identitas kecuali alamat tempat tinggal.

Berbeda dengan identitas di dunia nyata, identitas digital bukanlah suatu kesatuan karakteristik melainkan gabungan beragam identitas parsial (Monggilo, Kurnia & Banyumurti 2020). Artinya ada identitas digital yang sama dengan identitas kita di dunia nyata, ada yang berbeda. Misalnya saja, orang bisa mencantumkan nama, alamat, tempat tanggal lahir di *platform* digital sesuai aslinya, ada yang tidak. Bahkan ada yang meramu identitas digitalnya dengan sebagian identitas asli sebagian samaran.

Tak heran jika kemudian kita mendapatkan beberapa akun media sosial yang dimiliki orang yang sama namun dengan identitas yang berbeda, sebab seorang pengguna bisa memiliki banyak persona (Monggilo, Kurnia & Banyumurti 2020). Kondisi seperti ini bisa terjadi karena identitas digital biasanya tidak membutuhkan konfirmasi dengan kartu identitas formal seperti KTP atau KK.

Sementara itu, identitas digital yang tidak terlihat tentu sangat penting untuk kita jaga sebagai ‘kunci rahasia’ penjaga keamanan supaya tidak ada orang yang bisa masuk ke *platform* digital kita, sebagai rumah kita, di dunia maya.

Apa yang harus kita lakukan untuk menjaga identitas digital kita? Bagan III.2 memberikan tiga langkah yang bisa dilakukan dalam melindungi identitas digital kita.



Bagan III.2.

Langkah-langkah melindungi identitas digital

Sumber: diolah dari Monggilo, Kurnia & Banyumurti (2020)

Pertama, sebagai pengguna *platform* digital, kita bisa menggunakan identitas asli atau samaran, namun kita wajib bertanggung jawab atas pilihan tersebut. Pastikan juga hanya menampilkan identitas digital yang “aman”. Hindari untuk menampilkan identitas digital yang seolah aman tapi tidak seperti tanggal lahir kita dan nama ibu kandung. Sebab, identitas tersebut biasanya digunakan dalam transaksi perbankan yang tentu hanya kita saja yang boleh menggunakannya.

Kedua, pastikan keamanan surat elektronik kita sebagai identitas digital utama yang kita gunakan untuk mengakses berbagai *platform* digital dengan secara rutin memastikan sandi diperbaharui. Selain itu, sebelum bergabung dalam *platform* digital tertentu (*application admission*), pastikan kita memahami identitas digital kita akan dikelola dengan baik dan aman. Kita juga wajib membaca syarat yang harus kita sepakati saat mendaftar akun

*platform* digital dengan detail serta sadar akan risikonya. Kita juga harus memastikan memahami seluruh jaminan privasi dan keamanan *platform* tersebut.

Ketiga, pastikan kita melindungi identitas digital kita di berbagai akun *platform* digital yang kita gunakan. Konsolidasikan keamanannya misalnya dengan tidak menggunakan sandi sama namun hubungkan satu akun dengan lainnya dengan perlindungan yang maksimal untuk saling mengunci.

Ketiga langkah di atas penting untuk melindungi identitas digital yang kita miliki agar tidak terjadi kerugian di masa mendatang. Namun begitu, kita juga perlu melindungi identitas digital milik orang lain baik keluarga atau teman maupun orang lain dengan cara menghargai privasi mereka serta tidak melakukan invasi ke dalam sistem keamanan *platform* digital mereka.

## **MEMAHAMI DAN MELINDUNGI DATA PRIBADI**

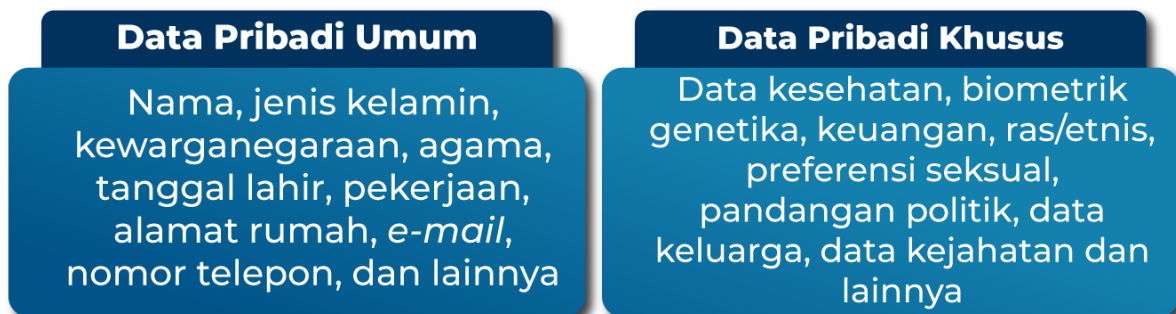
Jika identitas digital adalah karakter kita di *platform* digital baik yang terlihat maupun tidak terlihat, maka data pribadi merupakan konsep yang lebih luas. Data pribadi adalah data yang berupa identitas, kode, simbol, huruf atau angka penanda personal seseorang yang bersifat pribadi (Latumahina, 2014). Data pribadi bisa juga diartikan sebagai data atau informasi perseorangan yang disimpan, dikelola dan dilindungi kerahasiaannya karena bersifat privat.

*General Data Protection Regulation* (GDPR), regulasi perlindungan data pribadi yang disahkan Uni Eropa pada tahun 2016, merumuskan bahwa data pribadi adalah segala informasi yang bisa digunakan sebagai penanda rasional untuk mengenali seseorang. Contoh data pribadi yang biasanya dikaitkan dengan *platform* digital adalah alamat surat elektronik, alamat *Internet Protocol (IP address)*, nomor telepon genggam, dan data lokasi peta.

Di Indonesia, Rancangan Undang-undang Pelindungan Data Pribadi (RUUPDP) mendefinisikan data pribadi sebagai setiap data tentang seseorang yang teridentifikasi dan atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya

baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non elektronik (dalam Monggilo, Kurnia & Banyumurti 2020).

Secara umum, terdapat dua jenis data pribadi yakni sebagaimana terlihat dalam bagan III.3



Bagan III.3

Jenis data pribadi

Sumber: Monggilo, Kurnia & Banyumurti (2020)

Meskipun terdapat dua jenis data pribadi, keduanya dilekatkan dengan konsep privasi yang dianggap sebagai sebuah kondisi di mana terdapat hak seseorang untuk dilindungi dan tidak diganggu kehidupan maupun data pribadinya (Latumahina, 2014).

Dalam penggunaan dan pengelolaan data pribadi di *platform* digital, privasi bisa dianggap sebagai hak kita sebagai pengguna media digital untuk memilih apakah data pribadi kita akan diinformasikan pada pihak lain atau tidak (Monggilo, Kurnia & Banyumurti, 2020). Oleh karena itu, *platform* digital seperti media sosial, aplikasi percakapan, lokapasar maupun *platform* digital lainnya mempunyai tanggung jawab untuk melindungi data diri penggunanya. Sebab tanpa persetujuan kita, data pribadi kita di *platform* digital yang bocor adalah bukti sistem perlindungan data pribadi penggunanya masih belum maksimal.

Nah bagaimana kemudian sebagai pengguna kita bisa melindungi data diri kita di *platform* digital? Secara umum, terdapat beberapa tips agar data diri kita terlindungi seperti terlihat dalam bagan di bawah ini.

## TIPS PERLINDUNGAN DATA PRIBADI

Gunakan *password* (sandi) yang kuat, gunakan secara berbeda di setiap akun platform digital yang dimiliki, dan perbaharui secara berkala

Pahami dan pastikan pengaturan privasi di setiap akun platform digital yang dimiliki sesuai dengan tingkat keamanan yang dibutuhkan

Hati-hati mengunggah data pribadi di platform digital karena keamanan data pribadi kita tidak selalu terjamin

Hindari untuk membagikan data pribadi kita (tempat tanggal lahir, nama ibu kandung, *password* berbagai akun platform digital)

Hindari berbagi data pribadi orang lain baik keluarga, teman, maupun kenalan di dunia maya sebab data mereka adalah privasi mereka

Hindari memasukkan data pribadi yang penting saat berinteraksi dalam platform digital dengan menggunakan Wi-Fi gratis di tempat publik

Pahami dan pilih aplikasi yang dipasang di gawai hanya mengakses data yang dibutuhkan dan bukan data pribadi kita lainnya

Selalu lakukan pembaruan perangkat lunak yang digunakan dalam gawai untuk meminimalisir resiko ada celah kebocoran

Waspada jika ada komunikasi atau aktivitas mencurigakan baik dari akun dengan identitas digital yang kita kenal maupun bukan

Bagan III.4

Berbagai tips perlindungan data pribadi

Sumber: diolah dari Monggilo, Kurnia & Banyumurti (2020), Tirto.id. (2019, Desember 10)

Selain tips umum melindungi data pribadi seperti dijelaskan di atas, dalam kehidupan sehari-hari, perlindungan data pribadi juga bisa diterapkan saat kita melakukan transaksi daring. Dalam transaksi ini, baik penjual maupun pembeli tak hanya mengutamakan kejujuran informasi tapi juga keamanan data pribadi (Kurnia dkk, 2020).

Caranya bagaimana? Tak hanya kemampuan mengakses *platform* dan memahami pengaturan privasi di setiap *platform*, kemampuan melakukan verifikasi sebagai suatu proses untuk membandingkan keamanan *platform* yang digunakan dibandingkan dengan *platform* jual beli lainnya. Pastikan sistem keamanan *platform* kita menjamin data pribadi yang kita titipkan pada *platform* tersebut. Selain melakukan verifikasi pada *platform*, perlu juga melakukan verifikasi pada akun pengguna *platform* yang akan melakukan transaksi dengan kita, baik sebagai penjual maupun pembeli. Jangan lupa, kita harus selalu memastikan transaksi daring yang dimediasi tersebut menggunakan *platform* keuangan

yang mereka sediakan bukan rekening pribadi untuk menghindari penyalahgunaan data pribadi kita. Selain itu, kita juga harus memastikan keamanan perangkat lunak maupun keras yang kita gunakan untuk bertransaksi daring.

Pentingnya perlindungan data pribadi ini juga ditekankan baik oleh instansi pemerintah, korporasi maupun komunitas sebagai bentuk tanggung jawab mereka. Salah satu contoh kampanye perlindungan data pribadi ini dilakukan oleh pemerintah Jawa Barat sebagaimana terlihat dalam Gambar III.1.



Gambar III.1

Poster Digital 'Tips Melindungi Data Pribadi di Internet'

Sumber: Akun Twitter Official Jawa Barat Sapu Bersih Hoaks (2019, 27 Juni)

Dalam poster digital tersebut, pesan utama yang disampaikan adalah ragam tips melindungi data pribadi di internet dari penggunaan sandi yang sulit dan berbeda untuk akun yang berbeda, mengatur privasi, menjaga data pribadi, memastikan tautan, memastikan situs yang dikunjungi, memastikan keamanan jaringan internet, memastikan akses saat bergabung pada aplikasi tertentu, sekaligus juga menghargai privasi pengguna *platform* digital lainnya. Di sini terlihat bahwa perlindungan data pribadi tak hanya tentang data diri



tapi juga data orang lain sebagai tanggung jawab pengguna *platform* sebagai warga digital yang baik dan bertanggung jawab.

Kampanye perlindungan data pribadi juga dilakukan oleh industri yang mengelola *platform* digital misalnya saja Traveloka yang berkolaborasi dengan Tirto.id untuk mengajak penggunanya untuk menjaga data pribadi secara bersama (lihat Gambar III.2)



Gambar III.2

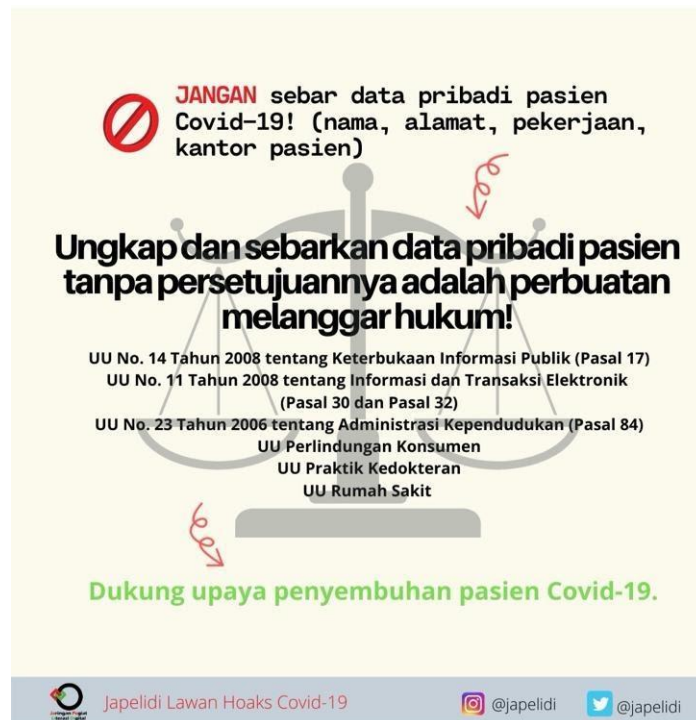
Poster Digital 'Bersama Jaga Data Pribadi'

Sumber: Tirto.id. (2019, Desember 10)

Dalam gambar III.2 tersebut, pesan yang ingin disampaikan adalah soal pentingnya data pribadi untuk kita simpan sendiri dan tidak dibagikan, setiap akun adalah privat sehingga

poin dari Traveloka tidak bisa diperjualbelikan dan ajakan untuk siaga sehingga kalau ada aktivitas mencurigakan segera melaporkan pada *platform*.

Pentingnya untuk tidak menyebarkan data pribadi orang lain juga ditekankan oleh Japelidi dalam kampanyenya melawan hoaks COVID-19 seperti yang terlihat dalam Gambar III.3.



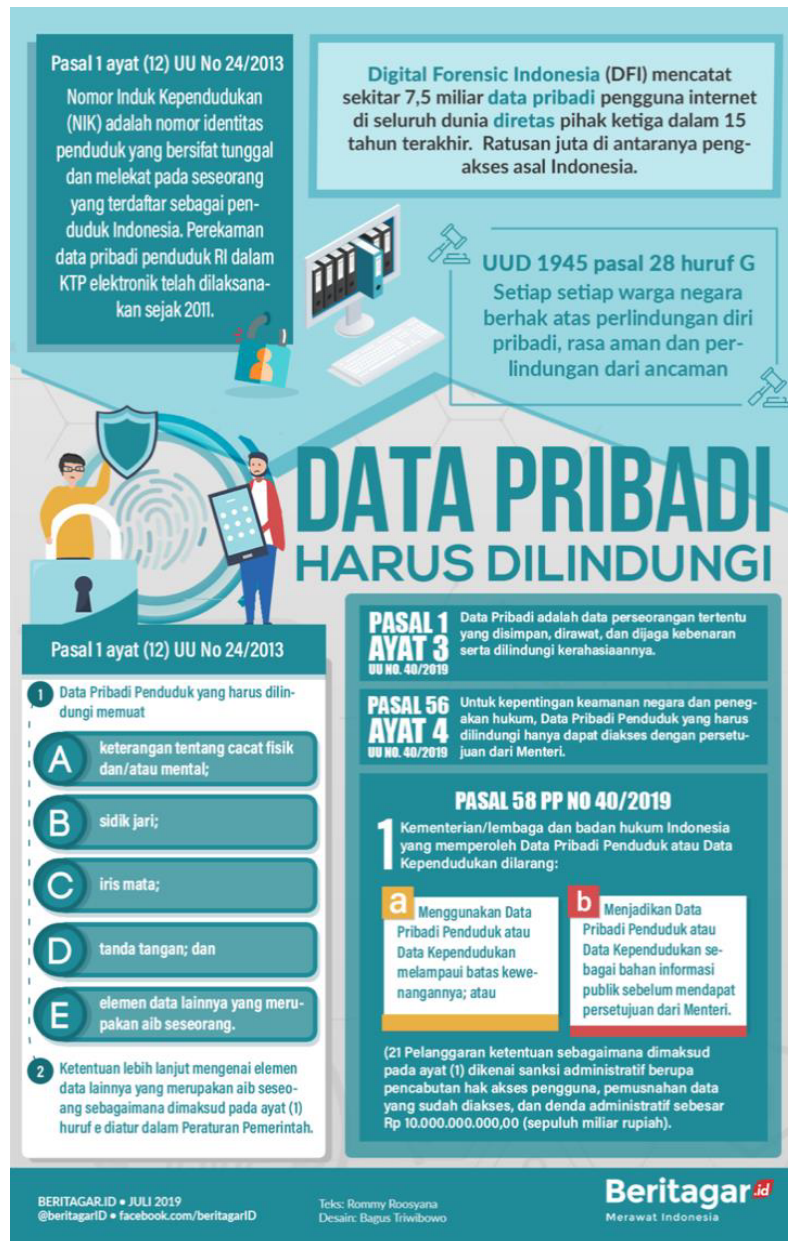
Gambar III.3

Poster Digital 'Lindungi Data Pribadi Pasien COVID-19'

Sumber: Dokumentasi Japelidi dalam Kampanye Lawan Hoaks COVID-19 (2020)

Dalam poster digital di atas, penegasan tentang perlindungan data pribadi, dalam hal ini khususnya pasien COVID-19, dilindungi oleh berbagai produk hukum yang berlaku di Indonesia. Poster ini menekankan pentingnya melindungi data diri orang lain yang dijamin oleh hukum.

Pentingnya aspek hukum ini juga ditegaskan oleh beberapa poster digital seperti bisa dilihat dalam Gambar III.4 dan Gambar III.5.



Gambar III.4

Poster Digital 'Data Pribadi Harus Dilindungi'

Sumber: Lokadata, 2019



Gambar III.5

Poster Digital 'Langkah Hukum Penyalahgunaan Data Pribadi'

Sumber: Hukumonline, 2019

Kedua poster digital di atas menunjukkan pentingnya memahami aspek hukum dalam perlindungan data pribadi supaya kita bisa menjadi warga negara sekaligus warga digital yang bertanggung jawab dalam menjaga keamanan digital bersama.

### MEMAHAMI DAN MELINDUNGI *PERSONAL IDENTIFICATION NUMBER* (PIN)

Seringkali untuk memudahkan kita menggunakan beragam *platform* digital, kita menggunakan angka sandi atau *Personal Identification Number* (PIN) yang sama. Namun, apakah sandi yang sama untuk beragam akun yang berbeda itu aman? Sebelum pertanyaan

tersebut dijawab, mari kita pahami dulu konsep PIN dalam perlindungan data pribadi sebagai salah satu kemampuan keamanan digital.

PIN adalah angka sandi yang hanya diketahui oleh pengguna *platform* digital dan sistem autentikasi *platform* digital tersebut (Raharja & Setyabudi, 2019). Biasanya PIN yang terdiri dari 4 hingga 6 digit angka digunakan sebagai cara sistem melakukan identifikasi terhadap pengguna agar akses ke sistem tersebut terbuka dan pengguna bisa memanfaatkan aneka fitur dan layanan dalam *platform* digital. Selain terkait dengan akses, PIN juga digunakan untuk membedakan pengguna satunya dengan pengguna lainnya.

Biasanya PIN menggunakan kode yang numerik dan biasanya digunakan dalam berbagai macam kegiatan transaksi keuangan daring maupun transaksi lainnya yang menggunakan sistem digital (Investopedia.com. 2020, Juli 31). Sebagai contoh, PIN biasa digunakan untuk melakukan aneka transaksi melalui *internet banking* hingga sistem keamanan pintu rumah. Bahkan, PIN juga digunakan untuk pengaman sepeda motor yang menggunakan sistem pengaman ganda (*double smart lock*) bersamaan dengan *Radio-Frequency Identification* (RFID) (Raharja & Setyonudi, 2019).

Untuk menjaga keamanan identitas digital dan data pribadi kita, kemampuan kita menggunakan PIN adalah kemampuan dasar yang selalu bisa kita asah. Dalam poster digital yang dikeluarkan oleh Ansonalex.com (2012, Oktober 10) sebagaimana terlihat dalam gambar III.6, terlihat sejarah PIN yang biasanya terdiri dari 4 hingga 6 digit sebagai proses autentikasi pengguna saat masuk ke dalam suatu sistem digital.

Bagaimana caranya kita bisa menggunakan PIN dengan baik dan aman? Pertama, hindari memilih kombinasi angka yang mudah ditebak, misalnya tanggal dan tahun lahir. Pilihlah kombinasi angka yang potensi keamanannya tinggi dengan selalu membuat PIN yang susah untuk diprediksi orang lain. Kedua, sebaiknya kita tidak menuliskan PIN di kartu identitas kita ataupun secarik kertas yang ditaruh di dompet. Dengan begitu, jika dompet kita tertinggal atau hilang, tidak ada potensi kerugian yang bisa ditimbulkan. Ketiga, gunakan PIN yang berbeda untuk kepentingan yang berbeda supaya tingkat keamanannya



lebih tinggi. Keempat, jika kita memasukkan PIN di berbagai mesin, misalnya ATM, di tempat terbuka, selalu tutupkan tangan kita supaya tidak ada orang yang melihatnya.



Gambar III.6 di atas adalah contoh kampanye untuk mengajak pengguna *platform* digital untuk selalu memastikan keamanan PIN sebagai salah satu langkah yang penting menjaga keamanan identitas digital dan data pribadi.

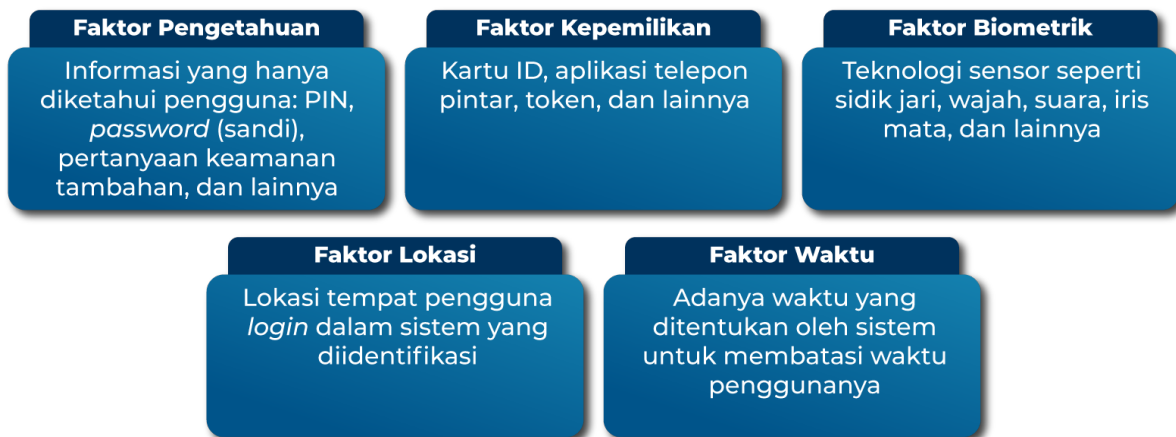
### **KEMAMPUAN MEMAHAMI DAN MELINDUNGI *TWO-FACTOR AUTHENTICATION* (2FA)**

Dalam menggunakan surat elektronik (surel) seringkali kita merasa enggan saat *login*, kita masih diminta untuk melakukan konfirmasi lagi untuk memastikan bahwa kita adalah pengguna yang terdaftar dalam sistem. Autentikasi tahap dua ini kadang dilakukan dengan menjawab pertanyaan tambahan, memasukkan kode yang dikirim melalui *short message service* (SMS) atau kadang dengan melakukan persetujuan ke telepon pintar kita. Sering kita kemudian berucap, ‘Mau masuk akun surat elektronik sendiri kok repot ya?’.

Proses autentikasi seperti ini tak tanya kita temukan saat akan mengakses surat elektronik tapi juga saat melakukan transaksi daring maupun saat menggunakan berbagai akun *platform* digital lainnya. Nah, apa sih yang disebut dengan *Two-Factor authentication* (2FA) tersebut? Bagaimana kemudian kita bisa melindungi 2FA ini?

*Two-factor authentication* (2FA) adalah keamanan penggunaan sistem digital yang membutuhkan dua faktor identifikasi (Susianto & Yulianti, 2015). Dalam bahasa lain bisa dikatakan bahwa 2FA adalah fitur keamanan yang digunakan untuk melakukan autentikasi ulang apakah pengguna yang akan *login* adalah benar-benar pemilik akun tersebut dan terdaftar dalam sistem (Socs.binus.ac.id. 2019, Juni 11).

Proses autentikasi dua faktor ini dilakukan dengan cara identifikasi pengguna berdasarkan dua faktor sebagai komponen informasi yang hanya diketahui oleh pengguna dan sistem. Biasanya langkah pertama adalah pengguna *login* melalui *username* atau email untuk masuk ke sistem. Langkah berikutnya, pengguna dikonfirmasi lagi dengan beberapa faktor sebagai langkah tambahan untuk memastikan. Terdapat beberapa faktor yang biasa digunakan oleh berbagai sistem digital dalam proses 2FA sebagaimana terlihat dalam bagan di bawah ini.



Bagan III.5

Faktor yang biasa digunakan dalam *Two-factor Authentication*

Sumber: diolah dari Socs.binus.ac.id. (2019, Juni 11)

Kedua langkah identifikasi ini harus benar, sebab jika tidak maka pengguna tidak akan bisa masuk ke sistem. Apapun pilihan yang dilakukan oleh sistem, pada dasarnya *Two-factor Authentication* ini adalah upaya dari sistem *platform* digital untuk memastikan keamanan akses akun oleh pengguna yang betul-betul berhak dan terdaftar. Dengan begitu, sangat kecil kemungkinan akun pengguna akan dimanfaatkan oleh pihak yang tidak bertanggung jawab. Meskipun begitu, proses *Two-factor Authentication* tidaklah bisa menjamin 100% keamanan akses akun pengguna. Untuk itu, setiap pengguna wajib untuk selalu berhati-hati dalam menjaga kerahasiaan data pribadi.





Gambar III.7.

Poster Digital 'Autentikasi Dua Tahap'

Sumber: Tirto.id. (2019, Agustus 20)

Dari poster digital diatas, dijelaskan bahwa autentikasi dua tahap merupakan sistem pengamanan akun digital di mana pengguna diwajibkan untuk memasukkan nama pengguna dan sandi yang dikombinasikan dengan tiga cara autentikasi: menggunakan kata kunci,

menggunakan ponsel, dan menggunakan sidik jari. Namun begitu, pengguna harus berhati-hati untuk tidak mudah memberikan nomor telepon genggam baik di dunia maya maupun dunia nyata, sebab nomor telepon genggam sering digunakan sebagai tempat pengiriman konfirmasi terutama SMS dalam mendapatkan pelayanan berbagai *platform* digital.

### **KEMAMPUAN MEMAHAMI DAN MELINDUNGI *ONE-TIME PASSWORDS* (OTP)**

Saat kita melakukan transaksi daring misalnya untuk melakukan pembelian baju di salah satu lokapasar, sering kita mendapatkan SMS yang berisi 6 digit angka yang harus kita masukkan untuk melanjutkan transaksi tersebut. Mungkin kita bertanya, 'Bukankah sudah ada nama akun dan sandi? Mengapa juga harus repot-repot menunggu surat elektronik atau SMS untuk mendapatkan kode untuk melanjutkan transaksi?'

Sebagai pengguna *platform* digital, kita tentu saja harus cermat, penggunaan kode unik yang khas dan difungsikan satu kali dalam satu transaksi inilah yang disebut dengan *One-time Passwords* (OTP). Dalam bahasa lain, OTP adalah sandi yang dimiliki oleh pengguna *platform* digital yang diubah secara teratur oleh sistem sehingga seorang pengguna selalu *login* dengan menggunakan salah satu sandi dari daftar sandi yang dimilikinya. Kelebihan OTP adalah keamanan yang tinggi sehingga kemungkinannya kecil untuk diretas. Sedangkan kelemahannya adalah pengguna harus menjaga agar daftar sandi tersebut selalu aman jangan sampai tercuri atau hilang (Yusuf, 2008).

Dalam praktiknya biasanya OTP hanya dipakai oleh pengguna saat memperoleh layanan digital sehingga sistem tersebutlah yang biasanya mengirimkan 6-8 digit angka melalui SMS atau email yang dijaga hanya digunakan sekali pakai oleh seorang pengguna. Biasanya sistem akan ketat sekali dalam menerima OTP yang dimasukkan oleh pengguna, salah satu nomor saja maka transaksi atau pelayanan akan berhenti atau gagal (Uzone.id 2020, November 6).

Dengan ketatnya sistem OTP ini bahkan bisa dikatakan bahwa bawa OTP adalah "rahasia antara anda dan yang diatas sana" (lihat Gambar III.8). Pesan yang ingin disampaikan oleh poster digital tersebut adalah OTP merupakan salah satu perangkat keamanan yang merupakan kode verifikasi yang disampaikan langsung ke pengguna melalui SMS agar bisa

digunakan sekali pakai. Dengan begitu hanya pengguna dan Tuhan yang tahu, tentu saja selain sistem yang dianggap bukan orang atau pengguna lainnya atau bahkan pengelola *platform* digital.

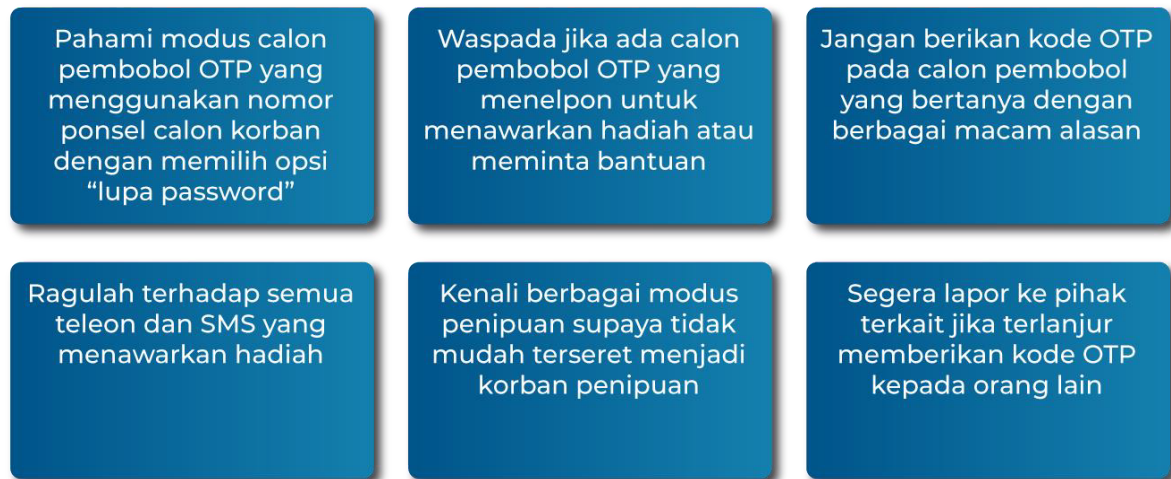


Gambar III.8.

Poster Digital 'OTP: Rahasia antara Anda & Yang Di Atas Sana

Sumber: Tirto.id. (2019, Februari 12)

Meskipun OTP dianggap sebagai sistem keamanan *platform* digital yang canggih, sebagai pengguna yang hati-hati, kita sebaiknya tetap harus waspada dalam menggunakannya dengan mempertimbangkan beberapa hal di bawah ini.



Bagan III.6

#### Perlindungan terhadap Penggunaan OTP

Sumber: diolah dari Tirto.id. (2019, Februari 12)

Keenam strategi di atas pada dasarnya terdiri dari komitmen kita sebagai pengguna media digital yang memegang penuh RAHASIA demi menjaga keamanan digital.

### SIMPULAN DAN REKOMENDASI

Dalam level individu, kemampuan kita sebagai pengguna media digital dalam melindungi identitas digital dan data diri termasuk memahami dan mempraktikkan penggunaan PIN, 2FA dan OTP adalah suatu kecakapan yang sangat penting dan tidak bisa ditinggalkan. Jika dilihat dari konsep 10 kompetensi literasi digital Japelidi, kecakapan tersebut seolah hanya terkait dengan kecakapan akses dan seolah bersifat teknis semata, padahal tidak.

Memang benar, kompetensi akses yang terkait pengaturan identitas digital dan data pribadi di perangkat keras dan lunak yang kita miliki juga di *platform* digital yang kita gunakan penting untuk melindungi identitas digital dan data diri. Namun kompetensi lain juga sama pentingnya. Sebagai pengguna digital yang sadar akan keamanan digital, kita harus bisa melakukan seleksi informasi terkait identitas digital maupun data diri mana yang harus

dilindungi. Kita juga harus memahami konsep perlindungan identitas digital dan data diri berikut ragam perangkatnya seperti PIN, T2FA, dan OTP.

Kita harus memastikan perlindungan identitas digital dan data diri sendiri, keluarga maupun orang lain saat kita membagikan pesan maupun memproduksinya sebelum kita sampaikan ke pengguna media lainnya. Kita wajib terlibat baik secara individual dengan berpartisipasi dan secara kolektif dengan berkolaborasi jika menemukan pelanggaran identitas digital dan data diri di depan mata kita. Partisipasi dan kolaborasi adalah dua kompetensi penting untuk menyelesaikan beragam persoalan masyarakat digital termasuk perlindungan identitas digital dan data diri (Kurnia & Wijayanto, 2020). Seluruh kemampuan ini patut kita miliki agar kita menjadi pengguna media digital yang tangguh menjaga keamanan data diri kita, keluarga dan orang lain di dunia maya.

Dalam level pasar, sudah sepantasnya pemangku kepentingan yang relevan baik pengusaha *platform* digital maupun pelaku pasar lainnya, bertanggung jawab untuk melindungi identitas digital dan data diri pengguna yang ada dalam sistem mereka. Langkah-langkah menjaga keamanan harus diupayakan seoptimal mungkin baik di dalam sistem maupun menjaga supaya tidak mudah dibobol pihak yang mau menyalahgunakan identitas digital dan data pribadi yang disimpan dalam *platform* tertentu.

Dalam level negara, adalah kewajiban negara untuk melindungi identitas digital dan data pribadi warga negaranya melalui kebijakan yang adil dan mengedepankan asas hak asasi manusia terhadap perlindungan diri di dunia maya.

Dengan begitu, bab ini, masih sangat terbuka untuk dikembangkan agar seluruh pemangku kepentingan mampu bertanggung jawab untuk perlindungan identitas digital data diri. Pengembangan di masa depan bisa dilakukan dengan mempertimbangkan ragam khalayak yang akan disasar melalui pembelajaran maupun variasi program literasi digital. Ragam khalayak ini bisa dilihat dari pendekatan usianya, kelompok terpinggirkan (anak, perempuan dan kaum difabel), maupun masyarakat di Kawasan 3T (terdepan, terluar dan tertinggal). Pertimbangan lain juga bisa dilihat dari langkah aksinya yang bisa bersifat individual atau kolaboratif, pendekatan aksi yang formal melalui kurikulum sekolah atau perguruan tinggi

maupun yang informal melalui aneka program, maupun ruang yang akan digunakannya yakni daring atau luring.

Tabel III.1

Matriks rekomendasi program literasi digital  
untuk meningkatkan kecakapan perlindungan identitas digital dan data diri

| <b>Aspek/<br/>Khalayak<br/>Sasaran</b>                           | <b>Anak dan<br/>Remaja</b>  | <b>Perempuan</b>   | <b>Lansia</b>   | <b>3T</b>  | <b>Penyandang<br/>Disabilitas</b>  |
|--|---|--|---|--|--|
| <b>Mengetahui<br/>dan<br/>Memahami<br/>identitas<br/>digital</b> | Program formal melalui kurikulum program formal melalui sekolah terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi guru) | Pelatihan informal yang bisa ditujukan dengan kelompok perempuan tertentu dilihat dari usia maupun pekerjaan. Metode dilakukan dengan diskusi dan studi kasus yang isunya umum | Pembuatan program audio yang sederhana dalam bahasa daerah sehingga mudah dipahami lansia | Pembuatan konten sederhana, tercetak dan mudah dibawa dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik | Pembuatan konten yang ramah di media yang bisa diakses oleh penyandang disabilitas |
|  | Program informal melalui ekstrakurikuler terkait TIK dengan metode belajar interaktif dan kuis yang   | Pelatihan informal yang bisa ditujukan dengan kelompok perempuan tertentu dilihat dari usia maupun   | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau            | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau masyarakat                                | Program diskusi yang sederhana sesuai dengan media yang bisa diakses               |

|   |  |   |   |   |   |
|---|--|---|---|---|---|
|   | menyenangkan<br>(oleh atau<br>didampingi<br>orangtua)  | pekerjaan.<br>Metode<br>dilakukan<br>dengan diskusi<br>dan studi<br>kasus yang isu<br>khusus tentang<br>perempuan   | tokoh<br>masyarakat   |   | oleh<br>penyandang<br>g disabilitas   |
| <b>Mengetahui<br/>dan<br/>Memahami<br/>data pribadi</b> | Program<br>formal melalui<br>sekolah terkait<br>TIK dengan<br>metode belajar<br>interaktif dan<br>kuis yang<br>menyenangkan<br>(oleh atau<br>didampingi<br>guru) | Pelatihan<br>informal yang<br>bisa ditujukan<br>dengan<br>kelompok<br>perempuan<br>tertentu dilihat<br>dari usia<br>maupun<br>pekerjaan.<br>Metode<br>dilakukan<br>dengan diskusi<br>dan studi<br>kasus yang<br>isunya umum | Pembuatan<br>program<br>audio yang<br>sederhana<br>dalam<br>bahasa<br>daerah<br>sehingga<br>mudah<br>dipahami<br>lansia | Pembuatan<br>konten<br>sederhana,<br>tercetak dan<br>mudah dibawa<br>dengan bahasa<br>daerah yang<br>mudah dicerna<br>dan ilustrasi<br>yang menarik | Pembuatan<br>konten<br>yang<br>ramah di<br>media yang<br>bisa<br>diakses<br>oleh<br>penyandang<br>g disabilitas |
|   | program<br>informal<br>melalui<br>ekstrakurikuler<br>terkait TIK<br>dengan<br>metode belajar<br>interaktif dan<br>kuis yang<br>menyenangkan                      | Pelatihan<br>informal yang<br>bisa ditujukan<br>dengan<br>kelompok<br>perempuan<br>tertentu dilihat<br>dari usia<br>maupun<br>pekerjaan.  | Program<br>diskusi yang<br>sederhana<br>dalam<br>bahasa<br>daerah<br>melibatkan<br>tokoh<br>agama atau<br>tokoh         | Program<br>diskusi yang<br>sederhana<br>dalam bahasa<br>daerah<br>melibatkan<br>tokoh agama<br>atau tokoh<br>masyarakat                             | Program<br>diskusi<br>yang<br>sederhana<br>sesuai<br>dengan<br>media yang<br>bisa<br>diakses<br>oleh            |

|                                       |   |   |   |  |  |
|---------------------------------------|---|---|---|--|--|
|                                       | (oleh atau didampingi orangtua)   | Metode dilakukan dengan diskusi dan studi kasus yang isunya umum                        | masyarakat  |  | penyandang disabilitas   |
| <b>Mengetahui dan menggunakan PIN</b> | Belum diperlukan untuk anak dibawah 13 tahun  | Pembuatan konten video yang mudah dipahami sehingga bisa mempraktikkan sendiri          | Pembuatan program audio yang sederhana dalam bahasa daerah sehingga mudah dipahami lansia       | Pembuatan konten sederhana, tercetak dan mudah dibawa dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik | Pembuatan konten yang ramah di media yang bisa diakses oleh penyandang disabilitas               |
|                                       | program informal melalui ekstrakurikuler terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi) | Pembuatan konten poster digital yang mudah dipahami sehingga bisa mempraktikkan sendiri | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat                          | Program diskusi yang sederhana sesuai dengan media yang bisa diakses oleh penyandang disabilitas |
| <b>Mengetahui dan menggunakan 2FA</b> | Belum diperlukan untuk anak dibawah 13 tahun  | Pembuatan konten video yang mudah dipahami sehingga bisa                                | Pembuatan program audio yang sederhana dalam  | Pembuatan konten sederhana, tercetak dan mudah dibawa  | Pembuatan konten yang ramah di media yang  |



|                                       |   |   |   |  |  |
|---------------------------------------|---|---|---|--|--|
|                                       |   | mempraktikkan sendiri   | bahasa daerah sehingga mudah dipahami lansia  | dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik   | bisa diakses oleh penyandang g disabilitas   |
|                                       | program informal melalui ekstrakurikuler terkait TIK dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi) | Pembuatan konten poster digital yang mudah dipahami sehingga bisa mempraktikkan sendiri | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat | Program diskusi yang sederhana dalam bahasa daerah melibatkan tokoh agama atau tokoh masyarakat                          | Program diskusi yang sederhana sesuai dengan media yang bisa diakses oleh penyandang g disabilitas |
| <b>Mengetahui dan menggunakan OTP</b> | Belum diperlukan untuk anak dibawah 13 tahun  | Pembuatan konten video yang mudah dipahami sehingga bisa mempraktikkan sendiri          | Pembuatan program audio yang sederhana dalam bahasa daerah sehingga mudah dipahami lansia       | Pembuatan konten sederhana, tercetak dan mudah dibawa dengan bahasa daerah yang mudah dicerna dan ilustrasi yang menarik | Pembuatan konten yang ramah di media yang bisa diakses oleh penyandang g disabilitas               |
|                                       | program informal melalui ekstrakurikuler terkait TIK  | Pembuatan konten poster digital yang mudah dipahami                                     | Program diskusi yang sederhana dalam bahasa   | Program diskusi yang sederhana dalam bahasa daerah   | Program diskusi yang sederhana sesuai  |

|  |   |                                     |   |  |  |
|--|---|-------------------------------------|---|--|--|
|  | dengan metode belajar interaktif dan kuis yang menyenangkan (oleh atau didampingi | sehingga bisa mempraktikkan sendiri | daerah melibatkan tokoh agama atau tokoh masyarakat | melibatkan tokoh agama atau tokoh masyarakat | dengan media yang bisa diakses oleh penyandang g disabilitas |
|--|---|-------------------------------------|---|--|--|

Dengan pengayaan khalayak maupun program di masa depan, baik di level individu, pasar dan negara, niscaya upaya perlindungan identitas digital dan data pribadi akan lebih ditingkatkan, sehingga persoalan-persoalan terkait hal tersebut bisa diminimalisir sekuat mungkin dan keamanan digital bisa diciptakan.

Meskipun begitu, harus juga kita pahami konteks yang lebih luas, bahwa perlindungan identitas dan data pribadi bukan hanya tanggung jawab individu semata, baik pengguna maupun pengajar serta pegiat literasi digital. Keamanan digital juga tanggung jawab pemangku kepentingan lainnya seperti perbankan, pengelola aneka *platform* digital, maupun pemerintah.

### **EVALUASI KOMPETENSI PERLINDUNGAN IDENTITAS DIGITAL DAN DATA DIRI**

Untuk melakukan pengukuran terhadap kecakapan pengguna *platform* digital dalam melakukan perlindungan identitas dan data diri, kita bisa melakukan evaluasi dalam tiga area. Pertama, aspek kognitif atau pengetahuan mengenai perlindungan identitas digital dan data diri. Kedua, aspek afektif atau perasaan yang menunjukkan kesadaran pengguna *platform* digital akan pentingnya perlindungan identitas digital dan data diri sebagai perwujudan tanggung jawab sebagai warga negara dan warga digital yang baik. Ketiga, aspek konatif atau *behavioural* untuk melihat sejauh mana pengetahuan dan kesadaran melakukan perlindungan identitas digital dan data diri dalam kehidupan sehari-hari. Untuk memudahkan, tabel III.2 menjelaskan matriks kecakapan perlindungan identitas digital dan data diri dalam ketiga aspek tersebut.

Tabel III.2

## Evaluasi Kecakapan Perlindungan Identitas Digital dan Data Diri

| No. | Aspek<br>Perlindungan<br>Identitas<br>digital dan<br>data pribadi | Domain Evaluasi  |   |  |
|-----|---|--|---|--|
|     |   | Kognitif   | Afektif   | Konatif/ <i>behavioral</i>   |
| 1   | Memahami dan melakukan perlindungan identitas digital             | Mengetahui konsep, jenis serta konteks perlindungan (individu, pasar dan negara) terkait identitas digital | Menyadari pentingnya perlindungan identitas digital diri, keluarga, maupun orang lain                                 | Mempraktikkan perlindungan identitas digital, keluarga maupun orang lain |
| 2   | Memahami dan melakukan perlindungan data pribadi                  | Mengetahui konsep, jenis serta konteks perlindungan (individu, pasar dan negara) terkait identitas digital | Menyadari pentingnya perlindungan data diri, keluarga, maupun orang lain  | Mempraktikkan perlindungan data diri, keluarga maupun orang lain         |
| 3   | Memahami dan mengetahui cara penggunaan PIN                       | Mengetahui arti istilah PIN serta cara penggunaannya   | Menyadari pentingnya penggunaan PIN sebagai salah satu cara melakukan perlindungan identitas digital dan data pribadi | Mempraktikkan perlindungan data diri dengan menggunakan PIN dengan benar |

|   |              |  |   |   |
|---|--------------|--|---|---|
| 4 | Memahami 2FA | Mengetahui arti istilah 2FA serta cara penggunaannya | Menyadari pentingnya penggunaan 2FA sebagai salah satu cara melakukan perlindungan identitas digital dan data pribadi | Mempraktikan perlindungan data diri dengan menggunakan 2FA dengan benar |
| 5 | Memahami OTP | Mengetahui arti istilah 2FA serta cara penggunaannya | Menyadari pentingnya penggunaan OTP sebagai salah satu cara melakukan perlindungan                                    | Mempraktikan perlindungan data diri dengan menggunakan OTP dengan benar |

#### **CONTOH BENTUK EVALUASI UNTUK ASPEK KONATIF PRAKTIK PERLINDUNGAN DATA DIRI**

Isilah lembar evaluasi di bawah ini berdasarkan pengalaman sehari-hari untuk mengukur kecakapan perlindungan data diri dari aspek konatif (*behavioral*). Kegiatan ini bisa dilakukan sendiri oleh pengguna *platform* digital sebagai pembelajar sebagai sebuah cara untuk melakukan evaluasi diri (*self-assessment*). Selain itu, kegiatan ini bisa juga dilakukan oleh pengajar atau pegiat literasi digital untuk melakukan evaluasi terhadap anak didik atau peserta ajar atau peserta program literasi digital.

Tabel III.3

Evaluasi Kecakapan Perlindungan Data Diri dilihat dari Aspek Konatif (*Behavioral*)

| No | Pernyataan  | Berilah tanda V (centang) pada salah satu pilihan |        |        |               | Alasan |
|----|---|---|--------|--------|---------------|--------|
|    |   | Sangat Jarang                                     | Jarang | Sering | Sangat Sering |        |
| 1  | Memilih sandi berbeda untuk berbagai akun <i>platform</i> digital berbeda                       |   |        |        |               |        |
| 2  | Melakukan tes kekuatan sandi menggunakan beberapa aplikasi yang tersedia gratis                 |   |        |        |               |        |
| 3  | Memperbarui sandi secara reguler  |   |        |        |               |        |
| 4  | Memperbarui sandi jika ada indikasi akun digunakan oleh orang lain                              |   |        |        |               |        |
| 5  | Melakukan pengaturan privasi akun <i>platform</i> digital secara berkala                        |   |        |        |               |        |
| 6  | Menggunggah hanya data pribadi diri yang relevan diketahui umum                                 |   |        |        |               |        |
| 7  | Menyimpan data pribadi yang bersifat khusus dan rahasia hanya untuk diri sendiri                |   |        |        |               |        |
| 8  | Menghindari berbagi data pribadi orang lain termasuk keluarga kita sendiri                      |   |        |        |               |        |
| 9  | Melaporkan pada pengelola <i>platform</i> jika ada tindakan mencurigakan terkait data diri kita |   |        |        |               |        |
| 10 | Menyimpan nomor-nomor atau kontak penting jika menemukan  |   |        |        |               |        |

|  |   |  |  |  |  |  |
|--|---|--|--|--|--|--|
|  | adanya kebocoran data pribadi diri<br>maupun orang lain |  |  |  |  |  |
|--|---|--|--|--|--|--|

## DAFTAR PUSTAKA

- Bernie, M. (2020, Juli 5). 91 Juta data pengguna tokopedia bocor dan disebar di forum internet. *Tirto.id*. Diperoleh dari <https://tirto.id/91-juta-data-pengguna-tokopedia-bocor-dan-disebar-di-forum-internet-fNH1>
- Clinton. B. (2019, Juli 25). Facebook resmi didenda Rp 70 Triliun, terbesar dalam Sejarah. *Kompas.com*. Diperoleh dari <https://tekno.kompas.com/read/2019/07/25/06510077/facebook-resmi-didenda-rp-70-triliun-terbesar-dalam-sejarah?page=all>
- Cnbcindonesia.com. (2020, April 16). Kacau, 530.000 data akun zoom dijual hacker di dark web. *Cnbcindonesia.com*. Diperoleh dari <https://www.cnbcindonesia.com/tech/20200416082700-37-152270/kacau-530000-data-akun-zoom-dijual-hacker-di-dark-web>
- Hukumonline.com. (2019, November 20). Langkah Hukum Melawan Penyalahgunaan Data Pribadi. *Hukumonline.com*. <https://www.hukumonline.com/klinik/bacagrafis/lt5dd4b7eba91ac/langkah-hukum-melawan-penyalahgunaan-data-pribadi/>
- Investopedia.com. (2020, Juli 31). Personal identification number (PIN). *Investopedia.com*. Diperoleh dari <https://www.investopedia.com/terms/p/personal-identification-number.asp#:~:text=What%20is%20a%20Personal%20identification,required%20to%20complete%20a%20transactio>
- Jabar Saber Hoaks [jabarsaberhoaks]. (2019, Juli 1). Tips melindungi data pribadi di internet [TWEET]. Diakses dari <https://twitter.com/jabarsaberhoaks/status/1145513797454401537/photo/1>
- Kurnia, N, Wendratama, E., Rahayu, R., Adiputra, W.M., Syafrizal, S., Monggilo, Z.M.Z...Sari, Y.A. (2020). *WhatsApp group and digital literacy among Indonesian women*. Yogyakarta: WhatsApp, Program Studi Magister Ilmu Komunikasi, PR2Media & Jogja Medianet.

- Kurnia, N. & Wijayanto, X.A. (2020). Kolaborasi sebagai kunci: Membumikan kompetensi literasi digital Japelidi. Dalam N. Kurnia, L. Nurhajati, S.I. Astuti, *Kolaborasi lawan (Hoaks) COVID-19: Kampanye, riset dan pengalaman Japelidi di tengah pandemi*. Yogyakarta: Program Studi Magister Ilmu Komunikasi, Departemen Ilmu Komunikasi, Universitas Gadjah Mada.
- Kurnia, N., Sadasri, L.M., Angendari, D.A.A, Yuwono, A.I, Syafrizal, S., Monggilo, Z.M.Z, & Adiputra, W.M. (2020). *Yuk, sahabat perempuan bertransaksi daring dengan cermat*. Yogyakarta: Program Studi Magister Ilmu Komunikasi, Departemen Ilmu Komunikasi, Universitas Gadjah Mada.
- Latumahina, R. E. (2014). Aspek hukum perlindungan data pribadi di dunia maya. *Jurnal Gema Aktualita*, 3(2), 14–25.
- Monggilo, Z.M.Z, Kurnia, N, Banyumurti, I. (2020). *Panduan literasi media digital dan keamanan siber: Muda, kreatif, dan tangguh di ruang siber*. Jakarta: Badan Siber dan Sandi Negara.
- Raharja, G.Y.M. & Setyobudi, P. (2019). Rancang bangun sistem keamanan sepeda motor menggunakan RFID dan Personal Identification Number (PIN) berbasis mikrokontroler Atmega16. *Elkom: Jurnal Elektronika dan Komputer*. Vol. 12, No. 1, Maret, hal. 6-12.
- Roosyana, R & Triwibowo, B. (2019, Juli). Data Pribadi Harus Dilindungi. *Beritagar*. Didapat dari <https://lokadata.id/artikel/infografik-data-pribadi-anda-bisa-terancam>
- Sammons, J. & Cross, M. (2017). *The basics of cyber safety: Computer and mobile device safety made*. Cambridge: Elsevier.
- Socs.binus.ac.id. (2019, Juni 11). Two factor authentication. *Socs.binus.ac.id*. Diperoleh dari <https://socs.binus.ac.id/2019/06/11/two-factor-authentication/>
- Susianto, D. & Yulianti, I. (2015). Mengamankan wireless dengan menggunakan two factor, password, dan mac address filtering. *Expert Jurnal Manajemen Sistem Informasi dan Teknologi*. Vol.5., No.2.,Desember, hal; 31-26.
- Tirto.id. (2019, Desember 10). Karena kini data adalah harta paling berharga. *Tirto.id*. Diperoleh dari <https://tirto.id/karena-kini-data-adalah-harta-paling-berharga-endn>
- Tirto.id. (2019, Februari 2019). Kode rahasia yang cukup diketahui anda dan tuhan. *Tirto.id*. Diperoleh dari <https://tirto.id/kode-rahasia-yang-cukup-diketahui-anda-dan-tuhan-dgKs>

Uzone.idFajrina, H. N. (2020, November 6). Cara kerja pengiriman OTP kode unik yang (hampir) mustahil sama. *Uzone.id*. Diperoleh dari <https://uzone.id/cara-kerja-pengiriman-otp-kode-unik-yang-hampir-mustahil-sama>

Winarsih & Irwansyah .(2020). Proteksi privasi big data dalam media sosial. *Jurnal Audience: Jurnal Ilmu Komunikasi*, Vol. 03, No 1, Hal. 1-33.

Zaenudin, A. (2019, Agustus 20). Nomor telepon, identitas maha penting di zaman digital. *Tirto.id*. Diperoleh dari <https://tirto.id/nomor-telepon-identitas-maha-penting-di-zaman-digital-egrx>





# **BAB IV**

---

## Memahami dan Menghindari Penipuan Digital

## **BAB IV**

### **MEMAHAMI DAN MENGHINDARI PENIPUAN DIGITAL**

*Sri Astuty*

#### **URGENSI MEMAHAMI PENIPUAN DIGITAL**

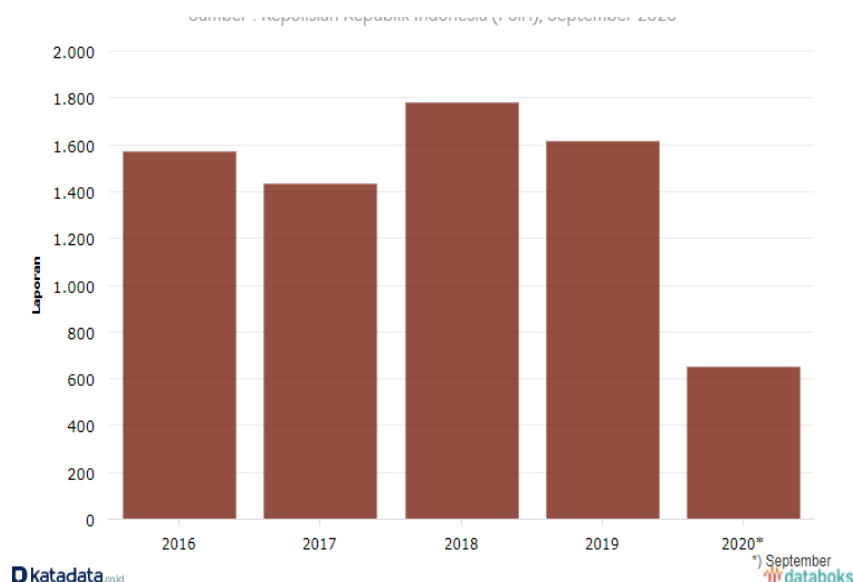
Aktivitas penggunaan internet semakin meningkat bahkan sejak pandemi COVID-19. Mulai dari belajar hingga bertransaksi jual beli pun dilakukan secara daring. Data Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dan Indonesia Survey Center pada semester kedua menyebutkan bahwa penetrasi pengguna internet di Indonesia 196,71 juta jiwa atau sekitar 73,7% dari total populasi penduduk Indonesia. Pengguna internet di Indonesia menggunakan telepon pintar atau *smartphone* untuk mengakses internet mencapai 95,4% (APJII & Indonesia Survey Center, 2020).

APJII juga mencatat aktivitas yang paling banyak dilakukan para pengguna internet di Indonesia adalah berinteraksi dengan aplikasi pesan instan (29,3%) dan melalui media sosial (24,7%). Alasan aktivitas lain menggunakan internet adalah untuk mengakses berita, layanan perbankan, mengakses hiburan, belanja daring, jualan daring, layanan informasi barang/jasa, layanan publik, layanan informasi pekerjaan, transportasi daring, *game*, *e-commerce*, layanan informasi pendidikan, dan layanan informasi Kesehatan. Meningkatnya angka pengguna internet berdampak pada meningkatnya pengguna media sosial dan transaksi daring. Salah satu aktivitas penggunaan internet yang paling banyak kita lakukan adalah melakukan belanja daring.

Ragam alasan penggunaan internet tersebut di atas, justru masyarakat akan dihadapkan pada berbagai kemungkinan risiko kejahatan pada dunia digital. Kepolisian Republik Indonesia sepanjang Januari s.d September 2020 menyebutkan bahwa terdapat 2.259 laporan, di mana ragam laporan kasus kejahatan digital ini seperti penyebaran konten provokatif, penipuan daring, pornografi, akses ilegal, manipulasi data, pencurian data/identitas, perjudian, intersepsi ilegal, pemerasan, peretasan sistem elektronik, pengubahan tampilan situs dan gangguan sistem. Dari data ini sebanyak 649 kasus yang dilaporkan merupakan kasus penipuan daring, dengan posisi urutan kedua terbanyak

kasusnya. Kasus ini adalah yang terdata dan dilaporkan untuk penipuan digital, sementara ada juga yang tertipu tetapi tidak melaporkan bahkan kadang mengikhhlaskan saja, dianggap sebagai musibah.

Pada data lima tahun terakhir, Kepolisian Republik Indonesia menyebutkan sejak 2016 sampai dengan September 2020 ribuan kasus penipuan daring telah dilaporkan. Pada 2016 terjadi laporan kasus penipuan daring sebanyak 1.570 kasus; tahun 2018 sebanyak 1.430; tahun 2019 sebanyak 1.781; dan tahun 2019 sebanyak 1.617 kasus; dan sampai dengan September 2020 telah ada 649 kasus yang dilaporkan. Seluruh kasus dalam 5 tahun terakhir berkisar 7.047 kasus.



Gambar IV.1

Jumlah Laporan Penipuan Daring Per Tahun

Sumber : Kepolisian Republik Indonesia, September 2020

Penipuan digital yang dilaporkan banyak menyasar ketika kita melakukan aktivitas belanja dan bertransaksi secara daring melalui beragam layanan lokapasar (*e-commerce*) seperti Shopee, Tokopedia, Bukalapak, Lazada, Blibli, Orami, Bhinneka, Ralali, JD.ID atau Sociolla. Kenapa belanja daring menjadi target dalam penipuan digital? Berdasarkan data, belanja daring saat ini menjadi salah satu aktivitas tren warga digital. Aktivitas ini semakin populer dilakukan karena dianggap memberikan kemudahan bagi konsumen (Kurnia dkk., 2020).

Pada bab ini, kita mendiskusikan berbagai jenis penipuan digital yang saat ini kasusnya semakin meningkat di Indonesia. Bab ini juga akan memberikan pengenalan dasar mengenai penipuan digital yang terjadi dalam berbagai motif, mulai dari penawaran publikasi ilmiah, salah kirim pulsa, transfer palsu, kuota gratis, penipuan berkedok hadiah/menang undian, informasi lowongan pekerjaan, informasi bantuan, pelelangan barang dengan mengatasnamakan lembaga resmi, kredit murah/pinjaman *daring*, investasi, teknisi palsu, dan sebagainya. Dari pengenalan dasar penipuan ini diharapkan dapat menjadi panduan bagi kita di dalam mengembangkan pengetahuan dan kompetensi literasi digital tentang penipuan digital dengan fokus penguatan pada kompetensi menganalisis, memverifikasi dan mengevaluasi hal-hal yang berkaitan dengan penipuan digital.

Bab ini juga mengantarkan kita untuk memahami berbagai aspek hukum yang dapat kita jadikan dasar ketika terjadi kasus penipuan digital, baik yang berkaitan dengan ketentuan teknis maupun ketentuan pidana diantaranya seperti yang tertuang dalam Undang-Undang No.11 Tahun 2008 tentang Informasi Transaksi Elektronik yang diubah sebagian oleh Undang-Undang No.19 Tahun 2016 tentang Perubahan atas Undang-Undang No.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik; Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen; Undang-Undang No. 7 Tahun 2014 tentang Perdagangan serta aturan hukum lainnya yang terkait dalam penipuan digital.

## **MENGENALI DAN MEMAHAMI PENIPUAN DIGITAL**

Kemajuan teknologi internet memudahkan berbagai hal mulai dari berbagi informasi hingga proses jual beli barang atau jasa melalui berbagai macam aplikasi. Namun demikian, terdapat oknum-oknum yang memanfaatkan kemajuan teknologi tersebut dengan melakukan kejahatan siber/kejahatan digital. Berbelanja daring rentan menjadi incaran para pelaku kejahatan digital karena aktivitas ini memiliki beragam celah yang bisa dimanfaatkan, terutama dengan memanfaatkan kelengahan pengguna teknologi digital.

Penipuan daring memanfaatkan seluruh aplikasi pada *platform* media internet untuk menipu para korban dengan berbagai modus. Penipuan jenis ini menggunakan sistem elektronik (komputer, internet, perangkat telekomunikasi) yang disalahgunakan untuk

menampilkan upaya menjebak pengguna internet dengan beragam cara. Strateginya biasanya dilakukan secara bertubi-tubi tanpa diminta dan sering kali tidak dikehendaki oleh korbannya (Sitompul, 2012; Elsina, 2015).

Modus penipuan digital lebih mengarah pada penipuan yang menimbulkan kerugian secara finansial. Salah satu contoh yang sering terjadi adalah penipuan produk secara daring. Modusnya dengan mengirimkan barang yang berbeda dengan yang dijanjikan saat transaksi dilakukan atau bahkan tidak mengirimkan barang sama sekali. Penipuan digital ini tidak hanya menimbulkan kerugian pada pembeli saja, karena terdapat pula bentuk penipuan yang merugikan penjual. Misalnya pembeli yang melakukan transfer fiktif dan penjual lalai melakukan pengecekan kembali sehingga tertipu dengan mengirimkan produk yang dijualnya. Jika dipetakan, maka setidaknya terdapat dua kerugian yang dialami konsumen seperti digambarkan dalam bagan di bawah ini.

Modus penipuan digital dilakukan dengan target awal adalah melakukan pencurian data digital, sehingga perlindungan terhadap identitas digital dan data pribadi menjadi bagian yang penting pada berbagai dunia (Sammons & Cross, 2017). Identitas digital ini tentu saja tidaklah selalu sama dengan identitas kita dalam kehidupan nyata yang merupakan rangkuman karakteristik kita baik yang bersifat tetap maupun tidak tetap (Monggilo, Kurnia & Banyumurti, 2020). Informasi lebih detail tentang hal ini dapat dibaca di Bab III tentang perlindungan identitas digital dan data pribadi.

Selanjutnya pencurian data pribadi menjadi target dalam melakukan penipuan digital dan umumnya berkaitan dengan keuangan data-data yang dijual, biasanya didapat dari perusahaan maupun bank, dengan berisikan nama lengkap, tempat tinggal, tanggal lahir, Nomor Induk Kependudukan (NIK), nomor telepon rumah, email, alamat kantor, jabatan, hingga nama ibu kandung (Nurdiani, 2020). Penipuan digital ini marak terjadi melalui media sosial. Modusnya pun berbeda-beda, mulai dari rekayasa sosial (*social engineering*), menjual produk di bawah harga pasar hingga membatasi komentar pada unggahan terkait.

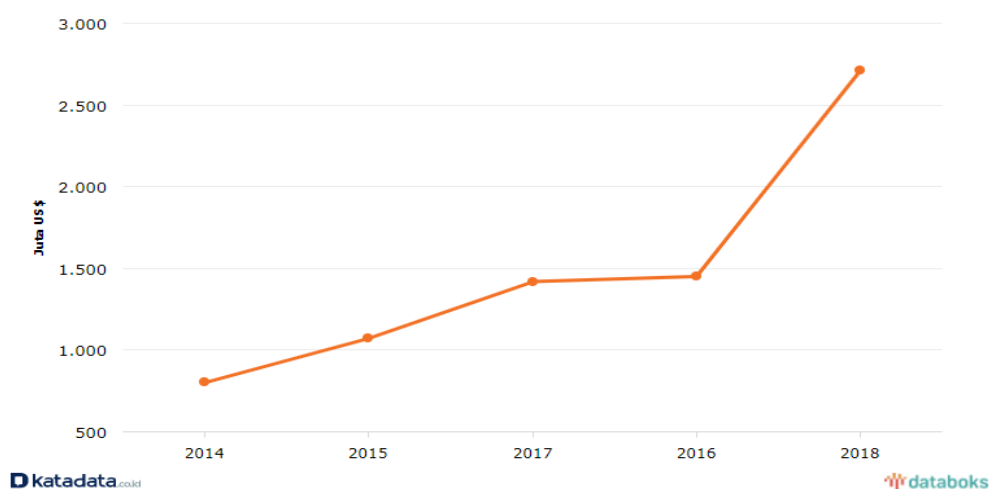


Bagan IV.1

Modus penipuan digital di media sosial

Sumber: olahan penulis

Kita juga dapat memperhatikan bahwa cukup banyak kerugian yang dimunculkan dari kejahatan digital ini dengan kriteria penipuan digital yang mana dalam lima tahun terakhir sejak 2014 sampai dengan 2018 bahwa kerugian yang ditimbulkan kejahatan digital ini mencapai US\$7.450,6 juta dengan rincian kerugian pada tahun 2014 sebesar US\$800,49 juta. Pada tahun 2015 kerugian mencapai US\$1070,71 juta, kemudian pada tahun 2016 kerugian mencapai US\$1450,7 juta, tahun 2017 kerugian mencapai US\$1418,7 juta, dan pada tahun 2018 kerugian mencapai US\$2.710 juta.



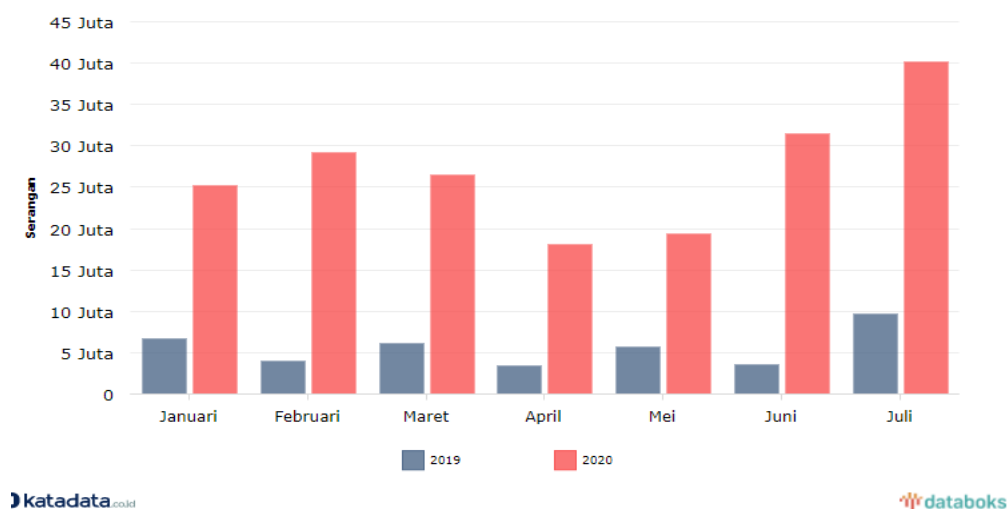
Gambar IV.2

Kerugian dari Kejahatan Dunia Maya yang Dilaporkan IC3 2014-2018

Sumber: Statista, 9 Juli 2019

Untuk menangkal kejahatan digital khususnya penipuan digital dengan berbagai modus sebagaimana tersebut di atas, maka kita perlu pemahaman dan peningkatan literasi digital dalam kerangka ketahanan keamanan digital dengan minimal kompetensi yang dimiliki adalah **kemampuan analisis, kemampuan verifikasi dan kemampuan evaluasi**.

Kemampuan analisis, verifikasi, dan evaluasi berkaitan dengan pemahaman awal mengapa terjadi penipuan digital, apa pengertian penipuan digital sebagaimana yang telah dijelaskan pada bagian awal di atas. Selanjutnya apa saja jenis dari penipuan digital termasuk mengenali dan memahami cara kerja penipuan digital. Setidaknya pemahaman tentang penipuan digital dengan berbagai kerugian serta aspek dan aturan hukum yang berkaitan dengan penipuan digital sebagaimana tersebut di atas dapat membantu kita semua untuk tahu secara dasar mengenai penipuan digital. Tren serangan siber pada berbagai *platform* media digital semakin meningkat, bahkan pada masa pandemi COVID-19. Hal ini menuntut ketahanan kita agar mampu menangkal kejahatan pada dunia maya ini. Serangan siber merupakan serangan yang berdampak dan membahayakan. Serangan siber dapat dilakukan oleh individu, kelompok, organisasi bahkan negara dengan cara meretas akun dengan menyasar keamanan sistem informasi pada perangkat digital, jaringan infrastruktur maupun perangkat pribadi dengan sumber anonim. Serangan siber ini bertujuan untuk mencuri, mengubah, merugikan serta menghancurkan sasaran yang menjadi target mereka. Serangan siber yang membahayakan inilah yang kita sebut sebagai kejahatan siber.



### Gambar IV.3

#### Jumlah Kejahatan Siber di Indonesia

Sumber: Badan Siber dan Sandi Negara (BSSN, November 2020)

Tren serangan siber di Indonesia meningkat dari tahun ke tahun, dengan tipe dan variasi serangan yang berbeda dari tahun sebelumnya, namun ada juga yang masih sama. Hal ini terjadi karena beberapa sebab, antara lain adanya pelaku kejahatan, modus kejahatan, kesempatan untuk melakukan kejahatan, korban kejahatan, reaksi sosial atas kejahatan, dan hukum. Rata-rata yang menjadi pelaku kejahatan adalah mereka yang lebih menguasai teknologi ini dan menggunakan kemampuannya itu untuk melakukan akses yang tidak sah ke jaringan komputer orang lain. Jadi tren pelaku kejahatan siber cukup jelas yaitu mereka yang paham dan mahir dalam dunia digital ini (Danuri & Suharnawi, 2017).

#### Ragam Penipuan Digital

Dalam berbagai kasus serangan siber di atas, penipuan digital menjadi salah satu bentuk kejahatan digital yang cukup rentan dan banyak dialami oleh masyarakat. Setidaknya ada empat bentuk penipuan digital, yaitu *scam*, *spam*, *phising*, dan *hacking*.

Secara teknis, penipuan dapat bersifat *social engineering* dengan ragam bentuk yang kita terima mulai dari SMS, telepon, email bahkan dalam bentuk virus serta pembajakan/peretasan akun dan *cloning platform* yang kita miliki.

#### Kemampuan Memahami dan Tips Mengendalikan *Scam*

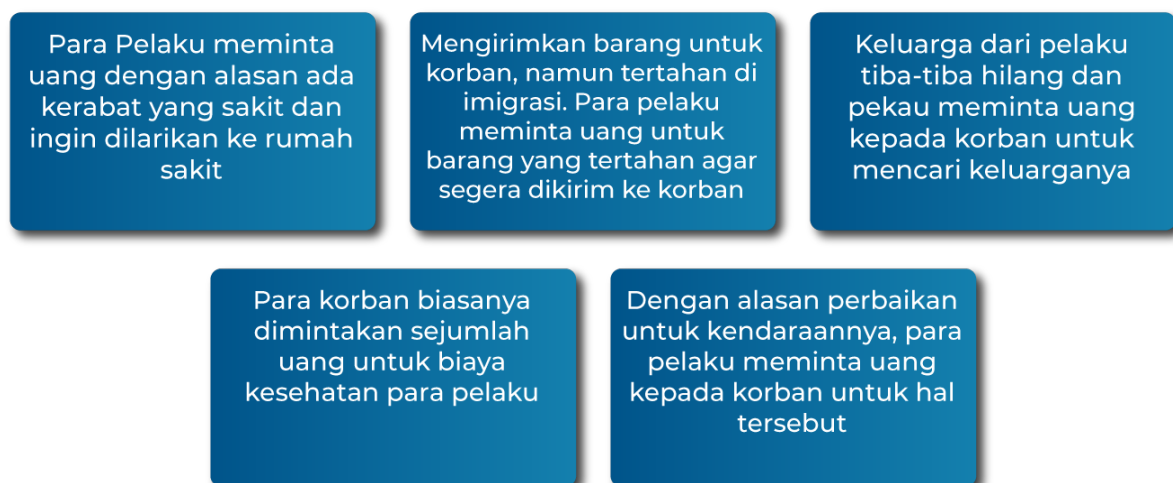
*Scam* merupakan bentuk penipuan digital yang paling umum. Pelaku kejahatan ini disebut *scammer*. Strateginya dengan memanfaatkan empati dan kelengahan pengguna. Metodenya beragam, bisa menggunakan telepon, SMS, WhatsApp, email, maupun surat berantai. Beberapa varian *scam* diantaranya *romance scam* yang dikembangkan dari *Nigerian Scam*. Istilah *nigerian scam* lahir karena penipuan ini awalnya tersebar melalui email dengan modus seorang pengusaha kaya mencari partner untuk memindahkan kekayaannya ke negeri tersebut. Jika kasusnya di Indonesia, maka sang *scammer* akan berdalih ingin memindahkan kekayaan ke Indonesia. Korban *scam* akan diperlakukan secara telaten hingga meyakini bahwa si *scammer* betul-betul serius. Ujung dari penipuan ini



adalah *scammer* akan meminta sejumlah uang sebagai biaya transfer untuk memindahkan kekayaannya lintas negara.

*Romance scam* menggunakan prinsip yang sama dengan *Nigerian Scam*. Bedanya, pada *Romance scam* pelaku berpura-pura mencari pasangan dan memanfaatkan empati korban yang dirayu untuk mau membantunya membiayai ongkos pindah negara. Tentu saja semua rayuan itu hanyalah tipuan agar korbannya percaya. Pelaku penipuan *romance scam* akan menggunakan profil palsu atau dikenal dengan istilah *profile cloning*. Hal tersebut bertujuan agar menarik perhatian calon korban (Salsabilah, Mulyadi & Agustanti 2021).

Terdapat beberapa modus *scam* dengan memainkan emosi korban sebagai berikut:



Bagan IV.2

Beberapa contoh modus scam

Sumber: olahan penulis

Untuk melihat bagaimana penipuan dengan kategori *scam* ini, berikut beberapa hal berkaitan dengan bagaimana teknis terjadinya *scam*, ciri-ciri *scam*, dan tips aman menghindari *scam* untuk menghindari penipuan digital terutama sebagai contoh pada saat melakukan belanja secara daring.



Gambar IV.4

Poster digital 'Waspada Penipuan Daring Shop via Medsos'

Sumber: Liputan6. Com (2020).

Scam sebagai penipuan digital merupakan kejahatan yang paling kerap terjadi. Pada era digital ini scam menjadi ancaman jika kita tidak waspada terhadap berbagai trik yang dilakukan oleh scammer. Scam selain berupa *romance scam* juga dapat berupa manipulasi psikologis, di mana pelaku akan memperdaya kita dengan memainkan trik

psikologis. Pelaku akan meminta informasi kode PIN/OTP yang kita miliki dan selanjutnya meminta transfer uang. Hal yang harus dihindari dari penipuan scam adalah kita dapat menjaga identitas pribadi kita, tidak memberitahukan siapa pun kode PIN/OTP yang kita miliki serta kita juga harus lebih selektif ketika menggunakan aplikasi untuk bertransaksi daring. Berikut kampanye yang dilakukan oleh Gopay dalam memberikan tips pada penggunaanya untuk menghindari *scam*.



Gambar IV.5

Poster Digital 'Penipuan Daring'

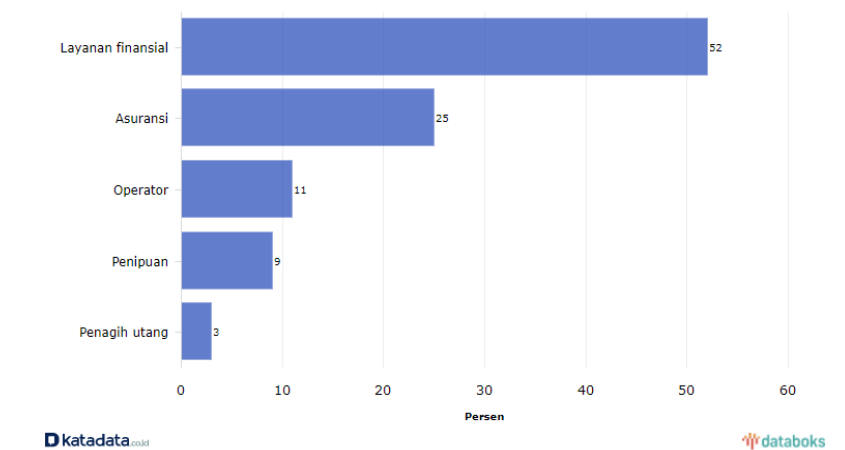
Sumber : Tirto.id (2020)

### Kemampuan Memahami dan Tips Mengendalikan *Spam*

*Spam* bisa terjadi dalam beragam bentuk, informasi mengganggu yang berbentuk iklan secara halus, informasi yang menjadi titik masuk bagi kejahatan siber seperti pemalsuan data, penipuan atau pencurian data (Alazab dan Broadhurst, 2015). Aktivitas *spam* pada dasarnya relatif mudah apabila melihat definisinya yang merupakan tindakan yang dilakukan bertubi-tubi atau berulang-ulang. Artinya pengirim informasi yang dikatakan melakukan *spam* yang disebut sebagai *spammer* bisa berada pada dua ciri yang memang dengan sengaja mengirimkan *spam* untuk berbuat kejahatan atau pengirim *spam* yang tidak mengetahui bahwa dirinya telah melakukan *spam*.

Email *spam*, selain berisi informasi tidak penting atau tidak relevan, tak jarang pula email *spam* menggiring penerima untuk mengklik tautan atau URL (*Unique Related Location*) tertentu. Ketika di klik URL ini akan mengarah kepada situs web yang mengandung *malware* atau virus yang dapat merusak sistem komputer penerima email atau mencuri data penerima email (lihat Bab I). Sisipan *malware* atau virus ini biasanya berbentuk pesan atau informasi dalam email *spam* tersebut yang bersifat sosial atau kode-kode rumit (Putra, 2016).

*Spam* selain berupa email juga berupa panggilan telepon. Umumnya panggilan telepon ini beraneka ragam mulai dari layanan finansial, penawaran asuransi, operator, penipuan, dan penagih utang. Berdasarkan data Truecaller (2020) sampai dengan 8 Desember 2020 tercatat kurang lebih terdapat 100 panggilan *spam* yang dilaporkan.



Gambar IV.6 Jenis Panggilan Telepon Spam di Indonesia Tahun 2020

Sumber : Truecaller, 8 Desember 2020

Bahkan data terkait *spam* dalam bentuk panggilan spam sepanjang tahun 2018 berupa *telemarketing*, perusahaan penagih hutang, penipuan uang, dan iklan agresif mencapai 17.983 panggilan dengan nomor-nomor yang tidak diketahui.



Gambar IV.7

Panggilan Spam

Sumber : Tirto.id (2020)



Selain *spam* berupa email, panggilan, *spam* juga berbentuk SMS. SMS *spam* biasanya dikirim secara bertubi-tubi tanpa kita kehendaki yang dikirim oleh pelaku secara terus menerus yang berisi bahwa kita memperoleh hadiah, mencatut nama perusahaan-perusahaan dan menyebutkan mewakili dari nama perusahaan terkenal, bahkan menyertakan tautan palsu. Umumnya SMS *spam* memiliki tujuan ada juga yang bertujuan untuk melakukan promosi, menawarkan produk, namun yang perlu diwaspadai adalah yang bertujuan untuk melakukan penipuan.



Gambar IV.8

SMS Spam Penipuan

Sumber: Dokumentasi Penulis, 2021

Adapun cara untuk menghindari email, telepon maupun SMS *spam* dapat dilakukan dengan memanfaatkan fitur-fitur yang terdapat dalam perangkat kita, misalnya dengan melakukan blokir. Berikut kampanye yang dilakukan oleh Badan Regulasi Telekomunikasi Indonesia (BRTI) dalam hal memperoleh telepon maupun SMS *spam*.

# Kesal Dapat SMS Spam Terus? Laporin Aja!

Spam SMS atau pesan spam yang sering sekali kita terima, ternyata tanpa disadarisudah berada di tahap mengganggu loh

## Apa Itu SMS Spam?

SMS spam adalah bentuk pengiriman pesan secara bertubi-tubi tanpa kehendak penerimanya

## Apa Sih Tujuan dari SMS Spam?

Biasanya SMS spam bertujuan untuk promosi, menawarkan suatu produk dan bahkan bisa juga untuk modus penipuan

## Aneka Modus SMS Spam

- Menawarkan promo seperti hadiah hingga kupon
- Menyebut nomor anda memenangkan suatu hadiah
- Mencatut nama perusahaan-perusahaan besar
- Kadang turut menyertakan link palsu

## Hentikan dengan Fitur Filter atau Block

Hampir di semua tipe ponsel saat ini dilengkapi fitur filter SMS atau juga blokir nomor yang kerap mengirim kita SMS spam

## Laporkan SMS spam ke Badan Regulasi Telekomunikasi Indonesia (BRTI) dengan cara:

Kirim screenshot SMS spam dan nomor pengirim dengan menyertakan nomor ponsel kalian yang teregistrasi NIK dan KK

Kirim aduan ke Twitter BRTI @aduanBRTI melalui Direct Message (DM)

Belum cukup dpt Rp38jt dr Tebar Uang? JANGAN SEDIH km bsa nambah Rp10jt di \*500\*200 skrng!

Selamat Anda mndptkn hadiah dari PT. Mana Tau dgn kode ADEADEAJALU untuk info klik [www.bit.ly](http://www.bit.ly)

Pantau.com

Dirangkum dari berbagai sumber  
Naskah & Grafis: Amin H. Al Bakki

Gambar IV.9

Infografis Mengenai Apa Itu SMS Spam dan Bagaimana Cara Melaporkannya

Sumber : Pantau (2020)

### **Kemampuan Memahami dan Tips Mengendalikan *Phishing***

*Phishing* merupakan kejahatan digital yang kerap ditemui oleh masyarakat Indonesia. *Phishing* adalah istilah penipuan yang menjebak korban dengan target menysar kepada orang-orang yang percaya bahwa informasi yang diberikannya jatuh ke orang yang tepat. Biasanya, *phishing* dilakukan dengan menduplikat situs web atau aplikasi bank atau *provider*. Ketika kita memasukkan informasi rahasia, uang kita akan langsung dikuras oleh *cracker* tadi. Kejahatan *phishing* ini dilakukan oleh oknum dengan menghubungi kita sebagai calon korbannya melalui email, telepon, atau pesan teks dengan mengaku dari lembaga sah. Biasanya oknum-oknum yang melakukan *phishing* akan menanyakan beberapa data sensitif seperti identitas pribadi, detail perbankan, kartu kredit, dan juga kata sandi. Bagi kita yang terjebak dalam kejahatan ini, informasi yang diperoleh pelaku dapat ia gunakan untuk mengakses akun penting yang kita miliki dan mengakibatkan pencurian identitas hingga kerugian finansial. Selain melalui email dan situs web, *phishing* juga bisa dilakukan melalui suara (*vishing*), SMS (*smishing*) dan juga beberapa teknik lainnya yang terus-menerus akan diperbarui oleh para penjahat dunia maya. Dan berdasarkan data serangan *phishing* situs, surel, dan seluler mencapai pada kuartal II tahun 2020 mencapai kurang lebih 100, dimana serangan dominan ke situs sebanyak 61, surel sebanyak 24, dan seluler 15 (Check Point, 2020)

*Phishing* selama masa pandemi COVID-19 juga terus meningkat. Serangan *siber* ini menjadi kategori yang berbahaya. Proses kerja *phishing* umumnya bermaksud untuk menangkap informasi yang sangat sensitif seperti *username*, sandi dan detail kartu kredit dalam bentuk meniru sebagai sebuah entitas yang dapat dipercaya atau *legitimate organization* dan biasanya berkomunikasi secara elektronik (Rachmawati, 2014). Pada masa COVID-19 sampai dengan Agustus 2020 serangan *siber* tertinggi berupa *phishing* mencapai 58 kasus (Interpol, 2020).

Cara kerja *phishing* ini juga biasanya ditujukan kepada pengguna *internet banking*, karena menggunakan isian data (ID) pengguna dan kata sandi, dan tidak menutup kemungkinan untuk ditujukan ke pengguna lainnya. Pelaku *phishing* akan membuat sebuah



situs web yang menyerupai halaman utama layanan perbankan, lengkap dengan kolom isian nama pengguna dan sandi. Korban yang tidak cermat akan mengisi kolom tersebut karena mengira situs web tersebut adalah situs web asli. Ketika data diisikan, pelaku *phishing* tinggal mengambil rekaman data yang berhasil dicurinya melalui situs web *phishing* tersebut.

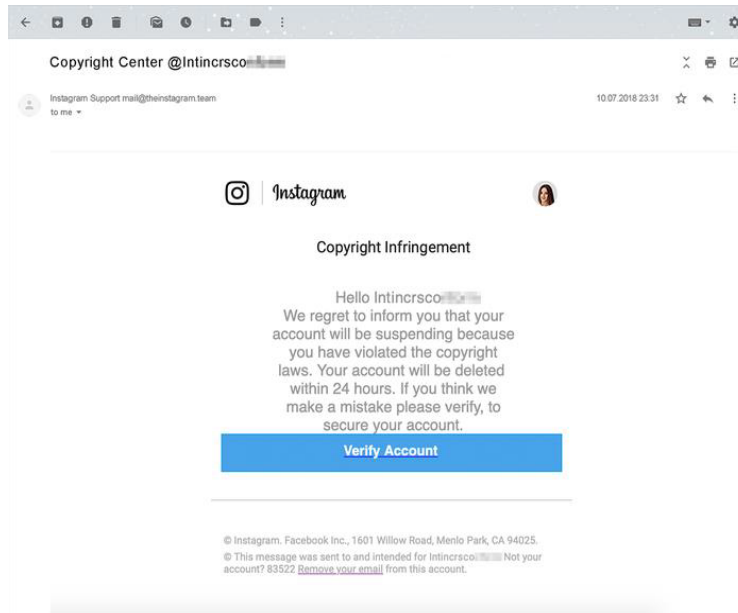
Selain itu *phishing* ini juga biasanya dilakukan melalui media-media sosial yang terhubung ke jaringan internet seperti melalui email/SMS dan situs web. Modus perbuatannya yang melalui email/SMS mengirimkan pesan. Kita mungkin pernah mendapatkan telepon dari orang yang mengaku teman lama. Mungkin juga telepon dari orang yang mengaku pegawai bank dan menyatakan bahwa kita sudah menerima hadiah. Setelah itu korban akan dipandu sehingga tanpa sadar membocorkan data pribadinya sendiri. Hal semacam ini juga lumrah dalam praktik *phishing* (Gulo dkk., 2020).



Gambar IV.10. Phishing Ancaman Serius Pelaku Industri Indonesia

Sumber: Bacapikirshare.org. (2013)

Selain itu *phishing* saat ini juga telah menyerang pada berbagai *platform* media sosial. Salah satu contoh Instagram yang terkena *phishing*.



Gambar IV. 11. Akun Populer di Instagram Jadi Sasaran Serangan Phishing

Sumber: Infokomputer.grid.id. (2019, Maret 19)

Berikut juga merupakan contoh serangan phishing berupa *web phishing*:



Gambar IV.12. Waspada Penipuan Web Phishing

Sumber: Mediaindonesia.com. (2020, Februari 21)

Jadi *phishing* dapat kita bedakan sesuai dengan tanda-tanda yang umum sering terjadi diantaranya adanya email *phishing* yang biasanya berisi tautan situs *web phishing* atau kata kunci seperti permintaan sandi, *login*, dan lain-lain. Setidaknya ada beberapa hal yang dapat dilakukan untuk mendeteksi *phishing* yaitu melalui kesadaran kita untuk mengenali email/SMS/situs web *phishing* atau melalui piranti lunak yang tersedia seperti *PhiGARo* maupun *Honeypot* yang memang telah dipasang untuk mendeteksi adanya serangan *phishing* pada perangkat digital kita, di mana piranti lunak ini tentu saja akan terus dikembangkan oleh para ahli *siber* untuk mendeteksi serangan *phishing* yang semakin waktu semakin canggih cara dan modusnya.

### **Kemampuan Memahami dan Tips Mengendalikan *Hacking***

*Hacking* merupakan tindakan dari seorang yang disebut sebagai *hacker* yang sedang mencari kelemahan dari sebuah sistem komputer. Di mana hasilnya dapat berupa program kecil yang dapat digunakan untuk masuk ke dalam sistem komputer ataupun memanfaatkan sistem tersebut untuk suatu tujuan tertentu tanpa harus memiliki *user account* (Murti, 2005: 38). Umumnya cara kerja para *hacker* adalah dengan melakukan pembobolan/peretasan sampai dengan percobaan keamanan situs situs web dan komputer dapat mereka lakukan. Berikut beberapa contoh kasus akun diretas hack dengan berbagai cara, dari tokopedia yang dibobol *hacker*, pemberitahuan virus yang dapat membobol akun, *hack* situs web KPU Yogyakarta:



Gambar IV.13

Contoh akibat tindakan *hacking*

Sumber: Cnbcindonesia.com. (2020, Mei 5).



Gambar IV.14

*Virus Hacking*

Sumber : Dokumentasi Penulis, 2021



Gambar IV.15

*Realtime News* Jelang Pilkada Hacker Serang Situs web KPU Yogya

Sumber: Jogja.tribunnews.com. (2017, Oktober 2)

Pada sisi yang lain seorang *hacker* yang memiliki sisi baik, jika menemukan hal-hal indikasi penyimpangan/peretasan/pembobolan akan memberitahu sistem administrator, bahwa sistem komputer yang dimasukinya telah terdapat kelemahan yang mungkin berbahaya bagi sistem komputer tersebut. Jika hasil dari *hacking* ini dimanfaatkan oleh orang yang tidak baik, maka tindakan tersebut digolongkan ke dalam kejahatan siber.

## MEMAHAMI ASPEK ATURAN DAN HUKUM

Selain itu, transaksi dalam elektronik ini mengandung banyak aspek hukum yang harus diperhatikan, baik dari segi perdata maupun pidana, diantaranya tentang perlindungan hukum bagi konsumen yang dirugikan, cara penyelesaian sengketa antara pelaku usaha dan konsumen, keabsahan kontrak secara elektronik yang dapat dilihat pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang diubah sebagian dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (Rudiastari, 2015).

Contoh kasus pengenaan sanksi hukum kejahatan siber dalam bentuk *phishing* di Indonesia dapat dikenakan UU ITE No.11 Tahun 2008 Pasal 35 “Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, perubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik” jo Pasal 51 ayat (1) “Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah)”, karena *phishing* merupakan kejahatan siber yang membuat situs yang menyerupai situs asli yang resmi, padahal situs tersebut adalah situs palsu. *Cybercrime* dalam bentuk *phishing* ini juga dapat dikenakan Pasal 28 ayat (1), Pasal 45A ayat (1) karena *phishing* juga melakukan kebohongan untuk menyesatkan orang lain di mana mengarahkan orang yang dibohongi untuk mengakses sebuah tautan yang di mana tautan tersebut ditujukan ke situs palsu dan memberikan suatu perintah untuk memperbarui informasi pribadinya yang rahasia ke dalam situs palsu yang telah dibuat oleh pelaku *phishing*, sehingga informasi pribadinya yang rahasia tersebut diketahui oleh pelaku *phishing* dan menyebabkan orang tersebut mengalami kerugian (Gulo dkk., 2020)

Jadi ketentuan hukum untuk pelaku kejahatan *spam*, *scam*, *phishing* dan *hacking* juga ini dapat dikenakan:

Pasal 28 (1) UU ITE mengatur “Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian

konsumen dalam Transaksi Elektronik”. Pasal 45A ayat (1) UU ITE yang mengatur Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik, sebagaimana dimaksud dalam Pasal 28 ayat (1) UU ITE, dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)

Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang pada Pasal 3, Pasal 4, Pasal 5 ayat (1) mengatur “Setiap Orang yang menerima atau menguasai penempatan, pentransferan, pembayaran, hibah, sumbangan, penitipan, penukaran, atau menggunakan Harta Kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana sebagaimana dimaksud dalam Pasal 2 ayat (1) dipidana dengan pidana penjara paling lama 5 (lima) tahun dan denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah)” dan/atau Pasal 82 dan/atau Pasal 85 Undang-Undang Nomor 3 Tahun 2011 tentang Tindak Pidana Transfer Dana dan/atau 378 KUHP, dengan ancaman hukuman penjara 6-20 tahun

Dari penjelasan di atas, nampak bahwa sanksi hukum yang dikenakan pada pelaku penipuan digital sudah jelas diatur dalam perundangan. Dengan begitu, penting bagi kita untuk mempunyai kesadaran untuk melaporkan penipuan digital sebagaimana akan dijelaskan di bagian berikut.

### **Memahami Pelaporan Penipuan Digital**

Penipuan digital dengan berbagai kategori *scam*, *spam*, *phishing* maupun *hacking* yang masuk dalam perangkat digital kita seperti email, telepon, maupun SMS selain dapat kita antisipasi dengan menggunakan fitur-fitur perlindungan yang ada pada perangkat kita, misalnya dengan melakukan blokir atau kita dapat melakukan cek rekening penipu dan melakukan pelaporan. Berikut beberapa hal yang berkaitan dengan pelaporan penipuan digital baik melalui situs resmi maupun pelaporan secara langsung ke kepolisian terdekat. Adapun pelaporan dan pengecekan secara digital diantaranya:

1. Langkah yang dapat dilakukan adalah Laporkan kejahatan *siber* di sekitar kita melalui [www.patrolisiber.id](http://www.patrolisiber.id)
2. Laporkan SMS spam ke Badan Regulasi Telekomunikasi Indonesia (BRTI) dengan cara melakukan tangkapan layar pada SMS *spam* dan nomor pengirim dengan menyertakan identitas ponsel kita yang telah teregistrasi NIK dan KK atau kirim aduan ke Twitter BRTI @aduanBRTI melalui *direct message* (DM).
3. Kita dapat melakukan pengecekan dan pelaporan rekening penipu mulai dari nama pemilik, nama bank, hingga rekaman transaksi sehingga nomor rekening penipu dapat dibekukan melalui:
  - a. [CekRekening.id](http://CekRekening.id) yang merupakan situs yang dimiliki oleh Kementerian Komunikasi dan Informatika dengan cara buka situs, pilih bank, masukkan nomor rekening dan klik periksa tombol rekening. Jika terindikasi melakukan penipuan klik "tambah laporan" dan isi kolom-kolom yang diperlukan. [CekRekening.id](http://CekRekening.id) juga merupakan situs yang dapat kita gunakan untuk melaporkan jika terdapat investasi palsu maupun kejahatan lainnya.
  - b. [Kredibel.co.id](http://Kredibel.co.id) yang merupakan situs untuk mengecek rekam jejak nomor rekening dan kredibilitas nomor rekening.
  - c. Melalui Otoritas Jasa Keuangan (OJK) melalui layanan pengaduan ke 1-500-655 atau email ke [konsumen@ojk.go.id](mailto:konsumen@ojk.go.id).
4. Kita juga dapat melapor ke situs [Lapor.go.id](http://Lapor.go.id) merupakan situs Kepolisian Republik Indonesia dengan cara kita membuat akun terlebih dahulu dan laporkan penipuan yang kita alami. Selain situs resmi [Lapor.go.id](http://Lapor.go.id) dapat juga mengadu melalui SMS ke 1708, aplikasi LAPOR! atau melalui akun Twitter @LAPOR1708 dengan menyematkan #lapor.
5. Kita juga dapat melapor ke CS KK maupun CS penyedia layanan produk/CS e-commerce seperti CS Shopee, CS Bukalapak, CS Tokopedia dan seterusnya.
6. Jika kita mengalami penipuan digital melalui Instagram, kita dapat melaporkan ke akun Instagram @indonesiablacklist.



Gambar IV.16

Mengenal Alur Kerja SI LAPOR

Sumber: Indonesiabaik.id. (2019).





Gambar IV.17

Cara Laporkan Jika Akun WhatsApp Kena Hack

Sumber: Kompas.com (2020, September 27)

## SIMPULAN DAN REKOMENDASI

Penipuan digital termasuk tipe kejahatan digital tertinggi di Indonesia. Setidaknya terdapat 4 kategori penipuan digital yaitu *spam*, *scam*, *phishing*, *hacking*. Penipuan digital tertinggi terdapat pada kasus berbelanja daring, namun demikian pada berbagai hal juga terdapat ragam modus dan motif penipuan digital, karena itu kompetensi literasi digital dengan kemampuan analisis, verifikasi dan evaluasi menjadi elemen penting dalam diri kita untuk melindungi keamanan diri dan perangkat digital yang kita miliki dari penipuan digital.

Selain memahami berbagai jenis penipuan digital dan mengenal cara kerja yang mereka buat, kita juga memiliki kemampuan untuk proteksi terhadap berbagai kemungkinan peretasan akun yang kita miliki, setidaknya memanfaatkan fitur-fitur dalam perangkat digital kita dapat mencegah kejahatan digital. Kemampuan lain juga yang harus ada pada diri kita adalah mampu mengaplikasikan kompetensi literasi digital dengan tidak mendiamkan jika terdapat indikasi penipuan digital, yaitu dengan cara melakukan pelaporan penipuan digital ke situs-situs resmi serta memahami berbagai ketentuan hukum yang berlaku berkaitan dengan penipuan digital.

Kompetensi literasi digital tidak hanya terbatas pada 4 komponen pada kejahatan digital di atas. Melakukan gerakan kampanye komprehensif kepada masyarakat agar memiliki kesadaran dalam hal bertransaksi digital ada baiknya melakukan kelayakan pengecekan harga, tidak tergiur dengan diskon atau harga miring yang ditawarkan untuk meminimalisir tindak pidana penipuan yang dapat terjadi. Selain itu kesadaran kita sebagai pengguna untuk terus ditingkatkan untuk membedakan antara berbagai jenis penipuan digital dan meningkatkan keamanan melalui piranti lunak yang kita miliki terutama mendeteksi *scam*, *spam*, *phishing*, dan *hacking*. Perlu penajaman konteks penipuan digital seperti *pharming*, *social engineering yang massif*, *sniffing*, *money mule*, di mana pada beberapa bagian terdapat *overlapping* konsep dalam *spam*, *phishing* dan *social engineering* itu sendiri serta mengingat konsep tersebut menjadi bagian kerangka penting dalam daya tahan keamanan digital kita dari penipuan digital ke depan serta pentingnya mempertajam interpretasi kategori penipuan digital dalam aturan hukum.

Pada bab ini, juga memberikan pertimbangan dalam kerangka keamanan digital dari modus penipuan digital bagi masyarakat dengan kriteria pendekatan usia, kelompok terpinggirkan (anak, perempuan dan kaum difabel), maupun masyarakat di Kawasan 3T (terdepan, terluar dan tertinggal), di mana dalam perlindungan diri dari penipuan digital seluruh pemangku kepentingan secara bersama-sama perlu baik dari pendekatan untuk memperoleh minimal pengetahuan modus penipuan digital serta keterampilan dalam mendeteksi adanya indikasi penipuan digital.

Tabel IV.1

Matriks Rekomendasi Program Literasi Digital  
untuk Meningkatkan Pengetahuan mengenai Penipuan Digital

| Aspek/<br>Khalayak<br>Sasaran   | Anak dan<br>Remaja  | Perempuan  | Lansia  | 3T  | Penyandang<br>Disabilitas   |
|---|---|--|---|---|---|
| Mengetahui<br>dan<br>Memahami<br>Konsep<br>Penipuan<br>Digital <i>Scam</i><br>dan cara<br>pencegahannya | Pembuatan<br>program<br>maupun<br>konten yang<br>menyenangkan mengenai<br>ragam<br>penipuan<br>digital <i>scam</i><br>dan<br>modusnya | Pembuatan<br>program<br>maupun<br>konten<br>pelatihan<br>mengenali<br>penipuan<br>digital <i>scam</i><br>dan<br>modusnya | Pembuatan<br>konten yang<br>sederhana<br>untuk<br>mengenali<br>penipuan<br>digital <i>scam</i><br>dan<br>modusnya | Pembuatan<br>konten<br>sederhana<br>untuk<br>mengenali<br>penipuan<br>digital <i>scam</i><br>dan modusnya | Pembuatan<br>konten<br>tentang<br>penipuan<br>digital <i>scam</i><br>dengan<br>metode yang<br>ramah bagi<br>penyandang<br>disabilitas |
| Mengetahui<br>dan<br>Memahami<br>Konsep<br>Penipuan<br>Digital <i>spam</i><br>dan cara<br>pencegahannya | Pembuatan<br>program<br>maupun<br>konten yang<br>menyenangkan mengenai<br>ragam<br>penipuan   | Pembuatan<br>program<br>maupun<br>konten<br>pelatihan<br>mengenali<br>penipuan<br>digital <i>spam</i>                    | Pembuatan<br>konten yang<br>sederhana<br>untuk<br>mengenali<br>penipuan<br>digital <i>spam</i><br>dan             | Pembuatan<br>konten<br>sederhana<br>untuk<br>mengenali<br>penipuan<br>digital <i>spam</i><br>dan modusnya | Pembuatan<br>konten<br>tentang<br>penipuan<br>digital <i>spam</i><br>dengan<br>metode yang<br>ramah bagi                              |

|   |   |  |   |   |  |
|---|---|--|---|---|--|
| ya  | digital <i>spam</i><br>dan<br>modusnya  | dan<br>modusnya  | modusnya  |   | penyangang<br>disabilitas  |
| Mengetahui<br>dan<br>Memahami<br>Konsep<br>Penipuan<br>Digital<br><i>Phishing</i> dan<br>cara<br>pengcegahann<br>ya | Pembuatan<br>program<br>maupun<br>konten yang<br>menyenangk<br>an mengenai<br>ragam<br>penipuan<br>digital <i>phishi</i><br><i>ng</i> dan<br>modusnya | Pembuatan<br>program<br>maupun<br>konten<br>pelatihan<br>mengenali<br>penipuan<br>digital <i>phishi</i><br><i>ng</i> dan<br>modusnya | Pembuatan<br>konten yang<br>sederhana<br>untuk<br>mengenali<br>penipuan<br>digital<br><i>phishing</i> dan<br>modusnya | Pembuatan<br>konten<br>sederhana<br>untuk<br>mengenali<br>penipuan<br>digital <i>phishing</i><br>dan modusnya   | Pembuatan<br>konten<br>tentang<br>penipuan<br>digital<br><i>phishing</i><br>dengan<br>metode yang<br>ramah bagi<br>penyangang<br>disabilitas             |
| Mengetahui<br>dan<br>Memahami<br>Konsep<br>Penipuan<br>Digital <i>Hacking</i><br>dan cara<br>pengcegahann<br>ya     | Pembuatan<br>program<br>maupun<br>konten yang<br>menyenangk<br>an mengenai<br>ragam<br>penipuan<br>digital <i>hackin</i><br><i>g</i> dan<br>modusnya  | Pembuatan<br>program<br>maupun<br>konten<br>pelatihan<br>mengenali<br>penipuan<br>digital <i>hackin</i><br><i>g</i> dan<br>modusnya  | Pembuatan<br>konten yang<br>sederhana<br>untuk<br>mengenali<br>penipuan<br>digital <i>hacking</i><br>dan<br>modusnya  | Pembuatan<br>konten<br>sederhana<br>untuk<br>mengenali<br>penipuan<br>digital<br><i>hacking</i> dan<br>modusnya | Pembuatan<br>konten<br>tentang<br>mengenali<br>penipuan<br>digital<br><i>hacking</i><br>dengan<br>metode yang<br>ramah bagi<br>penyangang<br>disabilitas |
| Mengetahui<br>dan<br>Memahami<br>Aturan Hukum<br>yang terkait<br>dengan<br>penipuan<br>digital                      | Pembuatan<br>program<br>maupun<br>konten yang<br>menyenangk<br>an mengenai<br>aturan<br>hukum   | Pembuatan<br>program<br>maupun<br>konten<br>pelatihan<br>mengenai<br>aturan<br>hukum   | Pembuatan<br>konten yang<br>sederhana<br>untuk<br>mengenai<br>aturan hukum<br>terkait penipu<br>an digital            | Pembuatan<br>konten<br>sederhana<br>untuk<br>Mengenai<br>aturan hukum<br>terkait penipu<br>an digital           | Pembuatan<br>konten<br>tentang<br>penipuan<br>digital<br><i>hacking</i><br>dengan<br>metode yang   |

|  |                                |                                |  |  |   |
|--|--------------------------------|--------------------------------|--|--|---|
|  | terkait<br>penipuan<br>digital | terkait<br>penipuan<br>digital |  |  | ramah bagi<br>penyandang<br>disabilitas |
|--|--------------------------------|--------------------------------|--|--|---|

## EVALUASI KOMPETENSI PENIPUAN DIGITAL

Untuk mengukur kemampuan literasi digital yang kita miliki berkaitan dengan pengetahuan dasar mengenai penipuan digital, setidaknya dapat diukur dengan aspek kognitif, afektif dan konatif, yang mana pada akhir modul ini, diharapkan kita mampu memiliki pengetahuan dan kesadaran bahwa transaksi digital yang kita lakukan rentan dengan berbagai kejahatan digital dalam hal ini adalah penipuan digital

Tabel IV.2

Evaluasi Pengetahuan Dasar Mengenai Penipuan Digital

| No | Aspek<br>Pengenalan Dasar<br>Penipuan Digital | Domain Evaluasi                              |  |  |
|----|---|--|--|--|
|    |   | Kognitif                                     | Afektif  | Konatif  |
| 1. | Memahami <i>Scam</i>                          | Mengetahui konsep dan pola kerja <i>scam</i> | Mengetahui dan menyadari cara mengatasi penipuan digital <i>scam</i> | Mempraktikkan perlindungan keamanan dari penipuan digital dengan kriteria <i>scam</i> kepada diri kita |
| 2. | Memahami <i>Spam</i>                          | Mengetahui konsep dan pola kerja <i>spam</i> | Mengetahui dan menyadari cara mengatasi penipuan digital <i>spam</i> | Mempraktikkan perlindungan keamanan dari penipuan digital dengan kriteria <i>spam</i> kepada diri kita |
| 3. | Memahami <i>Phishing</i>                      | Mengetahui konsep dan                        | Mengetahui dan menyadari   | Mempraktikkan perlindungan keamanan  |

|    |   |   |  |  |
|----|---|---|--|--|
|    |   | pola kerja<br><i>phishing</i>                                       | cara mengatasi<br>penipuan digital<br><i>phishing</i>  | dari penipuan digital<br>dengan kriteria<br><i>phishing</i> kepada diri kita,<br>keluarga dan orang lain                               |
| 4. | Memahami <i>Hacking</i>   | Mengetahui konsep dan pola kerja<br><i>hacking</i>                  | Mengetahui dan menyadari cara mengatasi penipuan digital <i>hacking</i>                            | Mempraktikkan perlindungan keamanan dari penipuan digital dengan kriteria <i>hacking</i> kepada diri kita, keluarga, dan orang lain    |
| 5. | Memahami berbagai ketentuan aturan hukum yang berkaitan dengan penipuan digital | Mengetahui apa saja ketentuan hukum terkait dengan penipuan digital | Mengetahui dan menyadari bahwa adanya ketentuan hukum sebagai pencegahan tindakan penipuan digital | Mempraktikkan aturan hukum sebagai bentuk perlindungan dan pencegahan dari penipuan digital kepada diri kita, keluarga, dan orang lain |

#### CONTOH INSTRUMEN EVALUASI PENGETAHUAN DASAR MENGENAI PENIPUAN DIGITAL

Contoh instrumen ini hanya berkaitan dengan aspek kognitif dari penipuan digital, di mana pengetahuan menjadi fondasi dasar untuk mencegah dan mengatasi penipuan digital yang saat ini sedang marak dengan beragam modus dan beragam teknik yang dilakukan oleh para pelaku untuk meretas/membobol akun yang kita miliki. Kegiatan ini sebagai bentuk evaluasi diri berkaitan dengan ketahanan keamanan digital kita.

Tabel IV.3

Evaluasi Pengetahuan Dasar Mengenai Penipuan Digital (aspek Kognitif)

| No | Pernyataan | Berilah tanda V (centang) pada salah satu | Alasan |
|----|------------|---|--------|
|----|------------|---|--------|

|    |   | pilihan       |        |        |              |  |
|----|---|---------------|--------|--------|--------------|--|
|    |   | Sangat Sering | Sering | Jarang | Tidak Pernah |  |
| 1  | Menerima pesan berantai tentang pengumuman berhadiah/bantuan, dsb.  |               |        |        |              |  |
| 2  | Meneruskan pesan berantai tentang pengumuman berhadiah/bantuan, dsb |               |        |        |              |  |
| 3. | Menerima email <i>spam</i>  |               |        |        |              |  |
| 4. | Menerima SMS <i>spam</i>  |               |        |        |              |  |
| 5. | Menerima panggilan <i>spam</i>                                      |               |        |        |              |  |
| 6. | Mengklik tautan pada email/SMS <i>spam</i>                          |               |        |        |              |  |
| 7. | Mengalami peretasan akun dengan menggunakan profil                  |               |        |        |              |  |
| 8. | Melakukan pelaporan jika menemui adanya penipuan digital            |               |        |        |              |  |

## DAFTAR PUSTAKA

- Alazab, Mamoun, dan Roderic Broadhurst.(2015). Spam and criminal activity, trends and issues (Australian Institute of Criminology). *RegNet Research Paper*, No. 2014/44.
- Annur, C. M. (2020, Agustus September 28). Serangan siber covid-19 secara global. *Databoks.katadata.co.id*. Diperoleh dari <https://databoks.katadata.co.id/datapublish/2020/09/28/phishing-dan-malware-serangan-siber-paling-banyak-selama-pandemi>
- APJII dan Indonesia Survey Center. (2020). Laporan Survei Internet APJII 2019 – 2020 (Q2).
- Bacapikirshare.org. (2013, Agustus 27). Phishing ancaman serius pelaku industri indonesia. *Bacapikirshare.org*. Diperoleh dari <https://www.bacapikirshare.org/phishing-ancaman-serius-pelaku-industri-indonesia/>.

- Badan Siber dan Sandi Negara. (2020, November). Jumlah kejahatan siber di indonesia. *Databoks.katadata.co.id*. Diperoleh dari <https://databoks.katadata.co.id/datapublish/2020/11/20/tren-serangan-siber-meningkat-selama-pandemi-covid-19>
- Bakki, A. H. (2020). Infografis mengenal apa itu sms spam dan bagaimana cara melaporkannya. *Pantau.com*. Diperoleh dari <https://www.pantau.com/topic/visual/infografis-mengenal-apa-itu-sms-spam-dan-bagaimana-cara-melaporkannya>
- Briantika, Adi. (2020, Juni 8). Siber polri bekuk tiga penipu penjualan masker murah lewat medsos. *tirto.id*. Diperoleh dari [https://tirto.id/siber-polri-bekuk-tiga-penipu-penjualan-masker-murah-lewat-medsos-F6K?utm\\_source=Tirtoid&utm\\_medium=Terkait](https://tirto.id/siber-polri-bekuk-tiga-penipu-penjualan-masker-murah-lewat-medsos-F6K?utm_source=Tirtoid&utm_medium=Terkait)
- Check Point. (2020). Serangan phishing berdasarkan mediaum (Kuartal II, 2020). *Databoks.katadata.co.id*. Diperoleh dari <https://databoks.katadata.co.id/datapublish/2020/08/13/situs-internet-target-utama-serangan-phishing>
- Danuri, M., & Suharnawi. (2017). Trend cyber crime dan teknologi informasi di indonesia. *Infokam*, 13(2), 55–64. Diperoleh dari <http://amikjtc.com/jurnal/index.php/jurnal/article/view/133/118>.
- Elsina, L. R. .(2015). Aspek-aspek hukum dalam transaksi perdagangan secara elektronik. *Jurnal GEMA AKTUALITA*, Vol 4, Nomor 1, Juni 2015.
- Grahanurdian.com. (2020). E-commerce indonesia tahun 2020. *Grahanurdian.com*. Diperoleh dari <https://grahanurdian.com/e-commerce-indonesia-tahun-2020/>
- Gulo, A.S. ,Lasmadi, S., Nawawi, K. (2020). Cyber crime dalam bentuk *phishing* berdasarkan undang-undang informasi dan transaksi elektronik. *PAMPAS: Journal Of Criminal* Volume 1 Nomor 2, 2020 ( ISSN 2721-8325 )68-81.
- Indonesiabaik.id. (2019). Mengenal alur kerja si lapor!. *Indonesiabaik.id*. Diperoleh dari <http://indonesiabaik.id/infografis/mengenal-alur-kerja-si-lapor>
- Infokomputer.grid.id. (2019, Maret 19). Waspadalah, akun populer di instagram jadi sasaran serangan *phishing*. *Infokomputer.grid.id*. Diperoleh dari



- <https://infokomputer.grid.id/read/121670535/waspadalah-akun-populer-di-instagram-jadi-sasaran-serangan-phishing?page=a>
- iPrice. (2021, Februari, 10). 10 e-commerce dengan pengunjung terbesar pada kuartal IV 2020. *Databoks.katadata.co.id*. Diperoleh dari <https://databoks.katadata.co.id/datapublish/2021/02/11/10-e-commerce-dengan-pengunjung-terbesar-pada-kuartal-iv-2020>
- JakPat. (2021, Februari 2). Alasan konsumen berbelanja daring. *Databoks.katadata.co.id*. Diperoleh dari <https://databoks.katadata.co.id/datapublish/2021/02/09/efisien-dan-diskon-jadi-alasan-konsumen-belanja-daring>
- Jogja.tribunnews.com. (2017, Oktober 2). Realtime news jelang pilkada hacker serang situs web KPU Yogya. *Jogja.tribunnews.com*. Diperoleh dari <https://jogja.tribunnews.com/2017/02/10/realtime-news-jelang-pilkada-hacker-serang-situs-web-kpu-yogya>
- Kepolisian Republik Indonesia. (2020, September). Jumlah laporan penipuan online per tahun. *Databoks.katadata.co.id*. Diperoleh dari <https://databoks.katadata.co.id/datapublish/2020/09/11/ribuan-penipuan-online-dilaporkan-tiap-tahun>
- Kominfo, Siberkreasi, & Deloitte .(2020). *Roadmap Literasi Digital 2021-2024*. Jakarta: Kominfo, Siberkreasi, & Deloitte.
- Kurnia, N., Sadasri, L.M., Angendari, D.A.D., Yuwono, A.I., Syafrizal., Monggilo, Z.M.Z., Adiputra,W.M. (2020). Yuks, kita bertransaksi daring dengan cermat. Seri literasi digital Jjapelidi. Yogyakarta Program Studi Magister Ilmu Komunikasi UGM.
- Kurnia, N., Wendratama, E., Rahayu, R., Adiputra, W.M., Syafrizal, S., Monggilo, Z.M.Z...Sari, Y.A. (2020). *WhatsApp group and digital literacy among Indonesian women*. Yogyakarta: WhatsApp, Program Studi Magister Ilmu Komunikasi, PR2Media & Jogja Medianet.
- Laraspati, A. (2021, Januari 19). *Awas 5 modus penipuan online di indonesia*. *Detik.com*. Diperoleh dari <https://inet.detik.com/cyberlife/d-5338367/awas-5-modus-penipuan-online-ini-marak-di-indonesia>
- Monggilo, Z.M.Z, Kurnia, N, Banyumurti, I. (2020) *panduan literasi media digital dan keamanan siber: Muda, kreatif, dan tangguh di ruang siber*. Jakarta: Badan Siber dan Sandi Negara.

- Nurdiani, Iftah. P.utri (2020). Pencurian identitas digital sebagai bentuk cyber related crime. *Jurnal Kriminologi Indonesia*, 16 (2), 1-10.
- Peraturan Pemerintah No. 82 Tahun 2012 Tentang Penyelenggaraan Sistem Dan Transaksi Keuangan
- Peraturan Presiden No 74 Tahun 2017 Tentang Peta Jalan Sistem Perdagangan Nasional Berbasis Elektronik
- Putra, E. N. (2016). Pengiriman email spam sebagai kejahatan cyber di indonesia. *Jurnal Cakrawala Hukum*, 7(2), 169–182. Diperoleh dari <http://jurnal.unmer.ac.id/index.php/jch/article/view/1906>.
- Rachmawati, Dian. (2014). *Phishing* sebagai salah satu bentuk ancaman dalam dunia cyber. *Jurnal Saintkom*, Vol. 13, No. 3.
- Rudiastari, E. (2015). “Perlindungan hukum terhadap konsumen dalam perjanjian jual beli melalui e-commerce di indonesia”, *Jurnal Sosial dan Humaniora*, Vol 5, No.1. , Maret 2015
- Salsabilah, T., Mulyadi, & Agustanti, R. D. (2021). Tindak pidana romance scam dalam situs kencan online di indonesia. *Jurnal Kertha Semaya*, 9(3), 387–403. Diperoleh dari <https://ocs.unud.ac.id/index.php/kerthasemaya/article/view/68457>.
- Sammons, J. & Cross, M. (2017) *The basics of cyber safety: Computer and mobile device safety made*. Cambridge: Elsevier .
- Smartphone GSMA Intelligence., Internet., Global Web Index., Media Sosial Platform Periklanan Media Sosial. (2020, Januari). Pertumbuhan E-Commerce Indonesia Tahun 2019. *grahanurdian.com* Diperoleh dari <https://grahanurdian.com/e-commerce-indonesia-tahun-2020/>
- Sitompul, J. (2012). *Cyberspace, cybercrimes, cyberlaw: Tinjauan aspek hukum pidana*. Jakarta: Tatanusa.
- Sukmawa, A.I., Karim, A.M., Yuwono, A.P., Elsha, D.D., Urfan, N.F., & Andiyansari, P. (2019). *Yuk, cegah tindak pidana perdagangan orang!* Yogyakarta: Penerbit Samudra Biru dan UTY.
- Suwandi, C. (2020, Februari 21). Waspada penipuan web *phishing* saat pandemi korona. *Mediaindonesia.com*. Diperoleh dari <https://mediaindonesia.com/nusantara/308419/waspada-penipuan-web-phishing-saat-pandemi-korona>

- Tirto.id. (2020, Januari 9). Penipuan Kejahatan Paling Populer di Era Digital. *Tirto.id*.  
Diperoleh dari <https://tirto.id/penipuan-kejahatan-paling-populer-di-era-digital-exio>
- Truecaller. (2020, Desember 8). Jenis Panggilan Telepon Spam di Indonesia Tahun 2020.  
*Databoks.katadata.co.id* Diperoleh dari  
<https://databoks.katadata.co.id/datapublish/2020/12/14/dari-mana-saja-asal-panggilan-telepon-spam-di-indonesia>
- Tamtomo, A. B. (2020, September 27). Cara lapor jika akun WhatsApp kena hack.  
*Kompas.com*. Diperoleh dari  
<https://www.kompas.com/tren/read/2020/09/27/093000565/infografik--cara-lapor-jika-akun-WhatsApp-kena-hack>
- Undang-Undang No. 8 Tahun 1999 Tentang Perlindungan Konsumen
- Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
- Undang-Undang No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang
- Undang-Undang No. 3 Tahun 2011 tentang Tindak Pidana Transfer Dana
- Undang-Undang No. 7 Tahun 2014 Tentang Perdagangan
- Undang-Undang No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik
- Wardani, A. S. (2020, Januari 17). Marak penipuan online shop di medsos, hati-hati modus makin canggih. *Liputan 6*. Diperoleh dari  
<https://www.liputan6.com/tekno/read/4157301/headline-marak-penipuan-online-shop-di-medsos-hati-hati-modusnya-makin-canggih>
- Wardoyo, S. (2020, Mei 5). Soal data tokopedia bocor, bos idea: Ada hacker mau pamer. *Cnbcindonesia.com*. Diperoleh dari  
<https://www.cnbcindonesia.com/tech/20200505152323-37-156478/soal-data-tokopedia-bocor-bos-idea-ada-hacker-mau-pamer>
- Zaenudin, A. (2019, Maret 6). Panggilan dari Nomor Tidak Dikenal yang Meresahkan. *Tirto.id*. Diperoleh dari <https://tirto.id/panggilan-dari-nomor-tidak-dikenal-yang-meresahkan-dix5>



# **BAB V**

---

## Melindungi Rekam Jejak Digital

## **BAB V**

### **MELINDUNGI REKAM JEJAK DIGITAL**

*Xenia Angelica Wijayanto*

#### **URGENSI PERLINDUNGAN REKAM JEJAK DIGITAL**

Dunia digital saat ini memberikan masyarakat tempat dan teknologi yang memudahkan kita dalam beraktivitas. Sebagai pengguna teknologi, tidak dapat kita pungkiri bahwa salah satu aspek yang harus kita perhatikan adalah keamanan kita di dunia digital (*Digital Safety*). Dalam aktivitas sehari-hari, setiap dari kita secara sadar atau tidak sadar telah meninggalkan banyak jejak di dunia maya. Penggunaan teknologi yang melekat dengan kehidupan sehari-hari kita juga telah meningkatkan kejahatan di dunia maya dengan mengakses perangkat lunak, gawai, dan terlebih menyambungkan diri kita dengan internet, kita telah memberikan akses pada pihak lain untuk mengetahui kebiasaan kita sehari-hari.

Teknologi yang semakin canggih dapat membaca dan memetakan kebiasaan kita hanya dengan membaca jejak yang kita tinggalkan. Mulai dari hal sederhana seperti penggunaan peta digital seperti Waze dan Google Maps, pola kita sehari-hari menjadi mudah untuk dipelajari oleh pihak lain. Kemudahan teknologi pun ternyata memiliki sisi yang perlu kita waspadai, yakni jejak-jejak kita di dunia maya. Jejak-jejak inilah yang disebut dengan jejak digital (*digital footprints*).

Jejak digital ini pula yang membentuk dan mengabadikan gambaran tentang siapa kita di dunia digital, yang bisa jadi lebih detail dari yang kita bayangkan. Apa pun yang kita lakukan saat melakukan aktivitas daring, penting bagi kita untuk mengetahui jenis jejak yang kita tinggalkan, dan apa efeknya bagi kita di kemudian hari ([internetsociety.org](http://internetsociety.org), 2021).

Bab Jejak Digital ini disusun untuk membantu kita dalam mempelajari lebih lanjut tentang jejak digital dan juga membantu kita menentukan cara yang tepat untuk melindungi privasi kita di dunia digital. Dengan mengetahui bentuk rekam jejak digital, contoh kasus tentang rekam jejak digital serta memahami bahwa rekam jejak digital sulit dihilangkan, maka

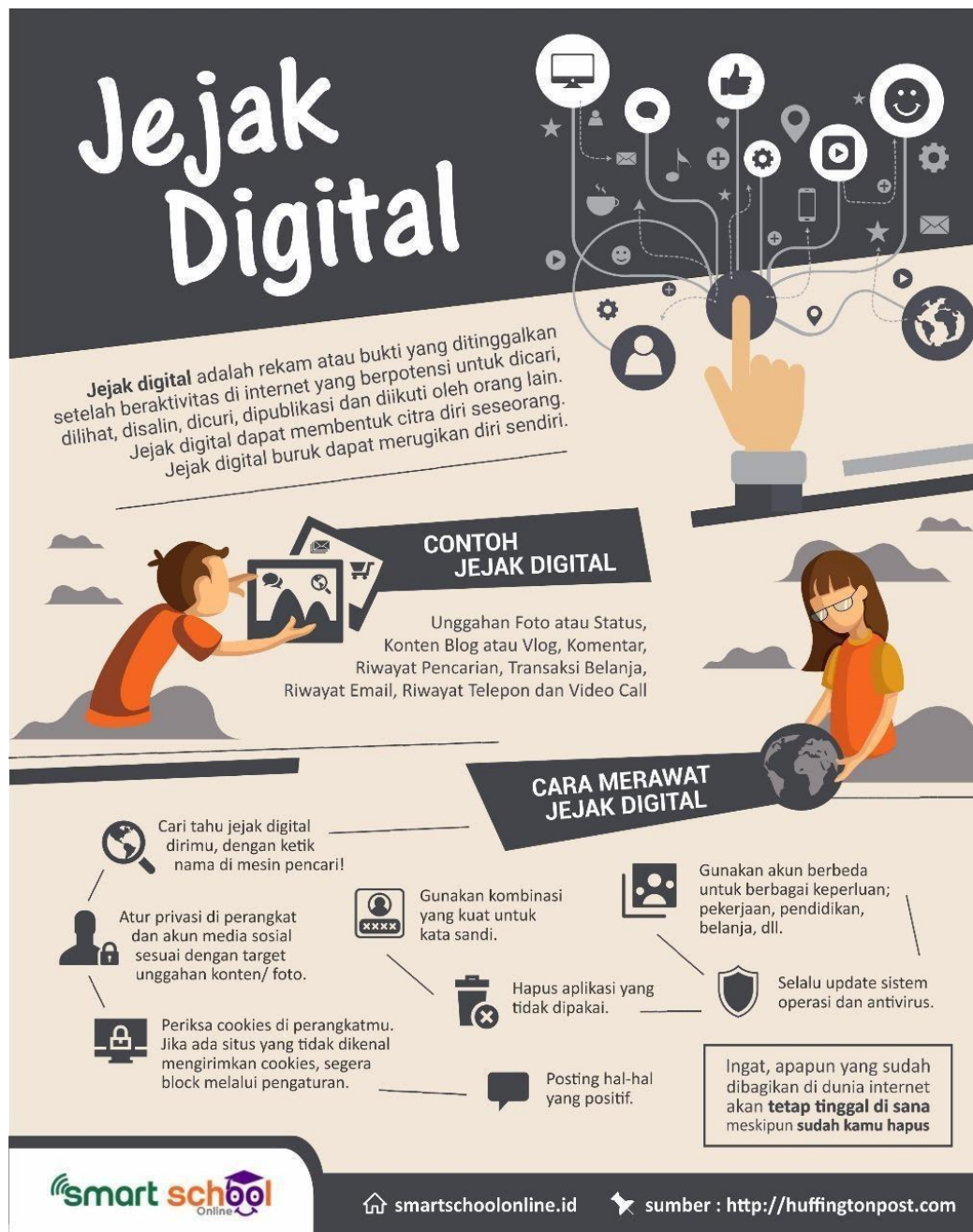
diharapkan kita dapat mengembangkan kemampuan kita untuk melindungi diri sendiri, dan juga orang lain dalam ranah digital.

Penting pula bagi kita untuk memahami bahwa setiap tindakan yang kita lakukan memiliki konsekuensi, terlebih di ranah digital yang kita seringkali luput untuk memperhatikan dan berhati-hati. Konsekuensi hukum juga perlu kita pahami, karena beberapa kasus menunjukkan bahwa tidak hanya pelaku yang dapat dihukum namun juga korban penyalahgunaan rekam jejak digital dapat menjadi sasaran empuk.

Selain menjelaskan konsep, memberikan ilustrasi kasus dan menyampaikan langkah-langkah untuk melindungi jejak digital, bab ini juga akan memberikan penjelasan mengenai evaluasi untuk mengukur keterampilan perlindungan jejak digital. Evaluasi ini bisa digunakan secara langsung oleh pengguna media digital sebagai *self-assessment* (evaluasi diri) maupun oleh pengajar atau pegiat literasi digital untuk mengukur kompetensi perlindungan jejak digital peserta didik atau peserta program jejak digital. Penguatan kompetensi perlindungan jejak digital sangat penting untuk menjaga keamanan digital supaya tidak terseret dalam penyalahgunaan identitas digital dan data diri kita maupun pengguna media digital lainnya.

## **MENGETAHUI BENTUK REKAM JEJAK DIGITAL**

Secara umum, jejak digital adalah jejak data yang kita buat dan kita tinggalkan saat menggunakan perangkat digital (dictionary.com, 2021). Salah satu ancaman terbesar bagi kaum muda di situs media sosial adalah jejak digital dan reputasi masa depan mereka (O'Keeffe & Clarke-Pearson, 2011). Tidak hanya perangkat digital, namun termasuk pula situs web yang kita kunjungi, email yang kita kirim, komentar yang kita tinggalkan pada media sosial, foto yang kita unggah, transaksi kita pada situs atau *platform* belanja daring, dan segala informasi yang kita kirimkan ke berbagai layanan daring yang ada.



Gambar V.1

Poster rekam jejak digital

Sumber: Smartschoolonline.id, 2018)

Ketika kita mengunjungi berbagai situs web, melalui menu *history* pada *browser* kita dapat melihat bukti situs mana saja yang telah kita kunjungi. Rekaman aktivitas web yang kolektif dan saling berhubungan ini yang dikatakan sebagai jejak digital (O'Keeffe & Clarke-Pearson, 2011). Setiap kali kita mengunjungi situs web, kita telah mengungkapkan beberapa informasi tentang diri kita kepada pemilik situs web seperti alamat IP, lokasi geografis, jenis

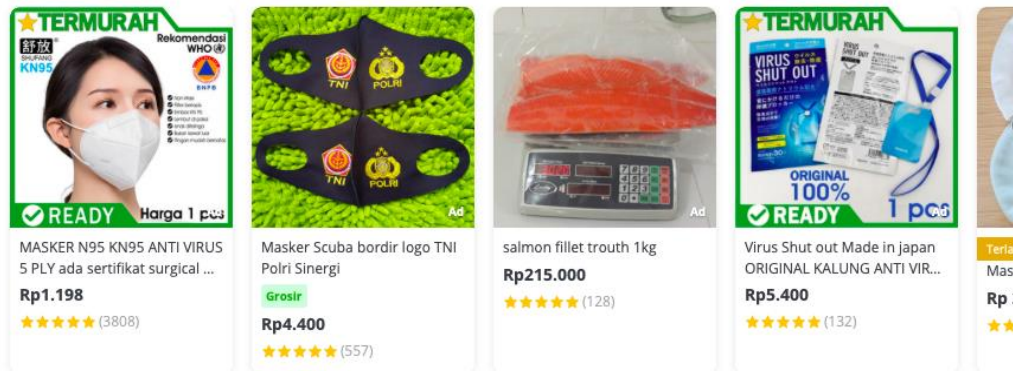
peramban (*browser*) web dan sistem operasi, dan seringkali juga situs web yang terakhir kali kita kunjungi. Potongan-potongan informasi yang tampak relatif tidak berbahaya dan bahkan cukup anonim ini pun adalah jejak digital kita (internetsociety.org, 2021).

Jejak digital memiliki sisi positif dan juga sisi negatif yang perlu kita waspadai. Jejak digital dan keberadaan fisik orang-orang sekarang dapat dilacak dengan mudah sehingga seseorang kini harus melindungi anonimitas mereka secara daring dan juga luring dengan lebih menyeluruh (Madden, 2012). Riset yang dilakukan oleh The Pew Research Center's Internet & American Life Project pada 2011 menyatakan bahwa Sekitar dua pertiga dari pengguna situs jejaring sosial menaikkan keamanan dari akun jejaring sosial mereka. 63% dari mereka telah menghapus orang dari daftar "teman" mereka, 44% telah menghapus komentar yang dibuat oleh orang lain di profil mereka, dan 37% telah menghapus nama mereka dari foto yang diberi *tag* untuk mengidentifikasi diri mereka (Madden, 2012).

Kekhawatiran atas pelanggaran privasi ini berawal dari temuan bahwa dunia digital telah merekam setiap gerak gerik kita. Cara termudah mengetahui jejak digital kita adalah dengan mengetikkan nama kita pada *search engine*/mesin pencari digital seperti Google, Yahoo, Altavista, Yandex, dan sebagainya. Berapa banyak informasi yang kita temukan dan terhubung dengan kita dari hasil tersebut?

Cara lain adalah dengan melakukan pencarian barang pada situs belanja daring. Meskipun kita telah menutup halaman toko daring tersebut, situs itu tetap akan memberikan kita referensi hasil pencarian yang cocok dengan pencarian kita sebelumnya. Atau, bahkan hasil pencarian kita akan terhubung dengan media sosial kita sehingga kita akan melihat iklan-iklan yang berhubungan dengan pencarian kita tersebut bertebaran di *timeline*. Hal ini memperlihatkan bahwa jejak penelusuran kita terekam di internet.



Terlaris untukmu [Lihat Semua](#)

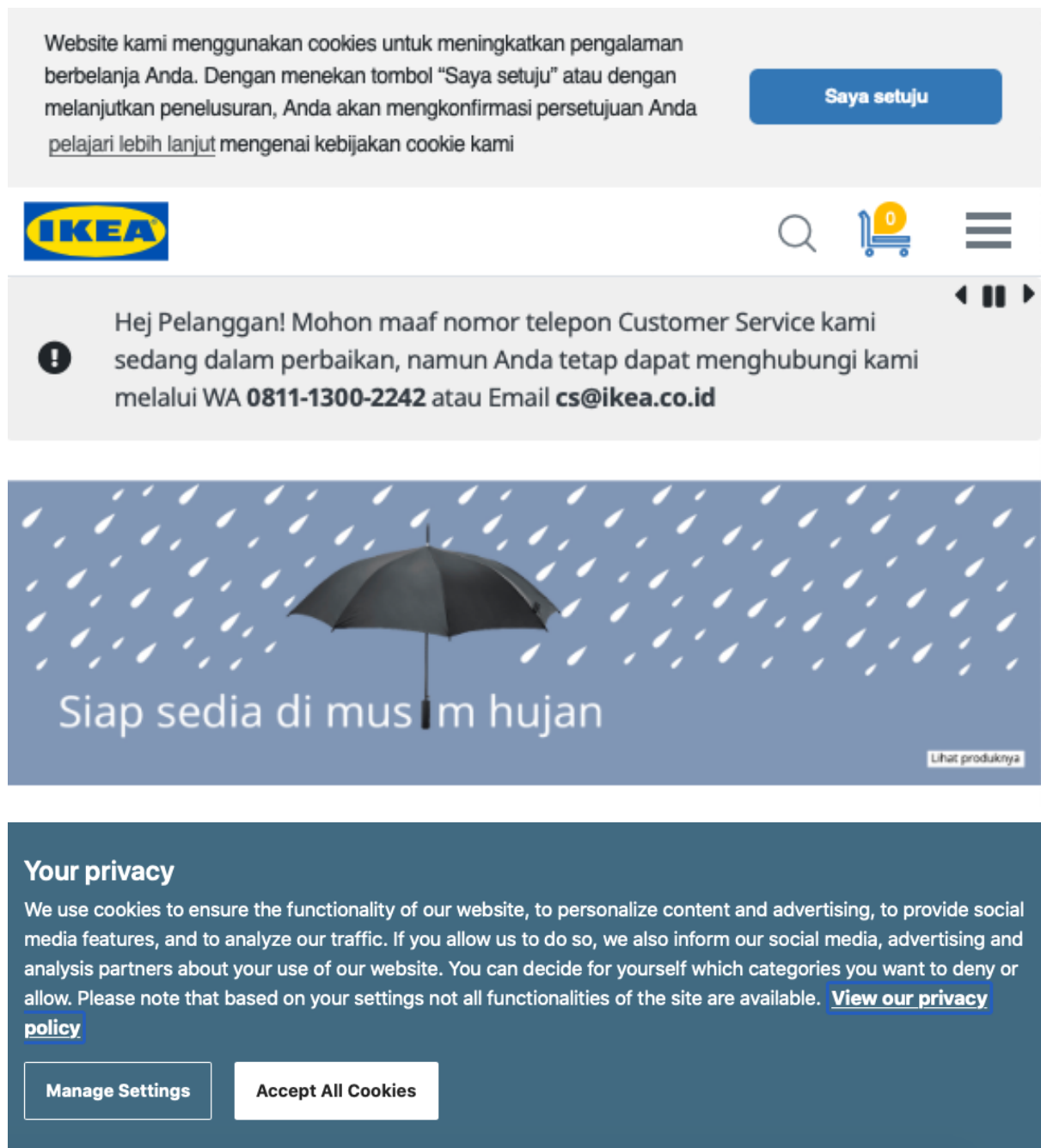
Gambar V.2

Contoh saran digital

Sumber : Dokumentasi pribadi penulis, 2021.

Jejak digital dikategorikan dalam dua jenis, yakni jejak digital yang bersifat pasif dan jejak digital yang bersifat aktif. Mengetahui kedua jenis jejak digital ini penting untuk meminimalisir dampak yang ditimbulkan dari tercecernya jejak digital kita.

**Jejak digital pasif** adalah jejak data yang kita tinggalkan secara daring dengan tidak sengaja dan tanpa sepengetahuan kita. Biasanya digunakan untuk mencari tahu profil pelanggan, target iklan, dan lain sebagainya. Jejak digital pasif ini tercipta saat kita mengunjungi situs *web* tertentu dan *server web* mungkin mencatat alamat IP kita, yang mengidentifikasi penyedia layanan Internet dan perkiraan lokasi. Meskipun alamat IP kita dapat berubah dan tidak menyertakan informasi pribadi apa pun, itu masih dianggap sebagai bagian dari jejak kita. Aspek yang lebih pribadi dari jejak digital adalah riwayat penelusuran kita, yang disimpan oleh beberapa mesin telusur saat kita masuk. Biasanya data ini diakses melalui *cookie* (Vonbank, 2019).



Gambar V.3.

*Cookie di website IKEA Indonesia dan Springer*

Sumber : ikea.co.id, springer.com 2021.

Pada dasarnya, jejak digital pasif ini tidak berbahaya, tetapi data jejak ini bisa menjadi masalah besar dalam beberapa keadaan. Masalah yang timbul dari jejak digital pasif ini antara lain adalah penjualan data aktivitas pelanggan oleh perusahaan pengelola website kepada pihak-pihak lain.

**Jejak digital aktif** mencakup data yang dengan sengaja kita kirimkan di internet atau di *platform* digital (Vonbank, 2019). Contohnya seperti mengirim email, mempublikasikan di media sosial, mengisi formulir daring, dan lain sebagainya. Hal-hal tersebut berkontribusi pada jejak digital aktif kita karena kita memberikan data untuk dilihat dan/atau disimpan oleh orang lain. Semakin banyak email yang kita kirim, semakin banyak jejak digital kita. Saat ini, banyak orang bahkan tidak berpikir sebelum mereka mempublikasikan sesuatu. Jejak digital aktif kita dapat mempengaruhi berbagai hal seperti ketika kita melamar pekerjaan baru. Perusahaan saat ini gemar untuk melihat profil media sosial calon pekerjanya sehingga kita perlu untuk berhati-hati dalam mengelola jejak digital aktif ini. Komentar kasar di Twitter atau foto yang pelanggaran aturan di Instagram sudah cukup untuk merusak peluang kerja dan reputasi kita.

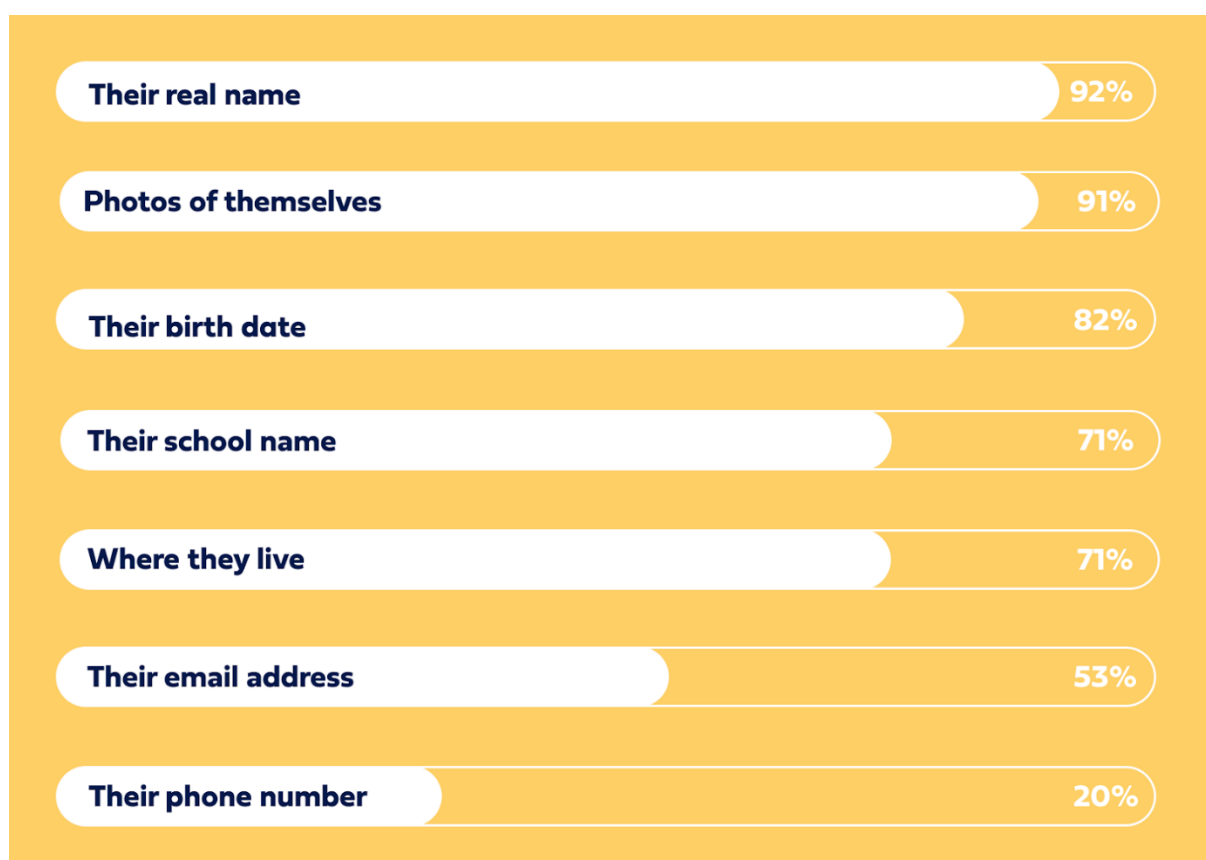


Gambar V.4

Jejak digital yang kita tinggalkan

Sumber: olahan penulis

Penting untuk berhati-hati dengan apa yang kita unggah di internet karena hal tersebut dapat digunakan untuk merugikan kita. Semua yang kita publikasikan dapat dilihat oleh semua orang: calon pemberi kerja, guru, dan universitas. Namun, di masa penuh keterbukaan seperti sekarang ini, sudah seperti tidak ada Batasan tentang apa saja yang boleh dibagikan di media sosial. Survei yang dilakukan terhadap anak-anak di Amerika menunjukkan bahwa anak muda cenderung membagikan hal-hal yang privat di internet. Berikut adalah statistik tentang apa saja yang diungkapkan kebanyakan anak muda tentang diri mereka secara daring (Vonbank, 2019).



Gambar V.5

Persentase data pribadi yang diunggah di Internet

Sumber : Medium.com

Jejak digital yang kita tinggalkan pada dasarnya adalah hal yang netral. Akan tetapi, kenetralan tersebut dapat menjadi positif atau negatif tergantung dari bagaimana kita atau pihak lain memanfaatkan data tersebut. Untuk membuat jejak digital yang positif, sangat

penting bagi kita untuk memahami implikasi, baik positif maupun negatif, dari tindakan kita di dunia maya.

## DUA SISI JEJAK DIGITAL

**Penyalahgunaan jejak digital** adalah pemanfaatan jejak digital secara negatif. Netsafe mencatat beberapa hal negatif yang muncul dari penyalahgunaan jejak digital yang paling sering dilaporkan oleh pengguna internet, antara lain: mempublikasikan informasi pribadi yang mengarah ke penindasan atau pelecehan daring, serta menerbitkan informasi pribadi atau bisnis yang digunakan untuk serangan manipulasi psikologis.

Modus penyalahgunaan jejak digital lain yang juga sering dilakukan adalah menerbitkan atau berbagi informasi yang merusak reputasi, seperti kehilangan pekerjaan. Perilaku membocorkan informasi pribadi atau biasa disebut Selain ketiga modus tersebut, Netsafe juga mencatat modus lain dengan menerbitkan atau berbagi gambar atau video yang digunakan untuk *sexting*, pemerasan, pelecehan berbasis gambar (terkadang disebut *revenge porn*) atau insiden pemerasan. Untuk perilaku semacam ini ancaman hukumnya bisa berlapis dan menyentuh hukum tentang pencemaran nama baik bahkan juga pemerasan.

Pemanfaatan jejak digital adalah penggunaan jejak digital secara positif. Jejak digital yang ditinggalkan seringkali digunakan oleh aparat penegak hukum. Bagi mereka, jejak digital tersebut akan sangat membantu dalam mengungkap kasus-kasus kriminal, baik yang berbasis dunia daring (*cybercrime*) maupun yang terjadi di dunia luring Bentuknya beragam. Mulai dari aktivitas sinyal seluler pada ponsel, riwayat *login* akun media sosial, sampai dengan jejak pengiriman SMS atau panggilan telepon. Bahkan, jika seseorang meretas sebuah situs web atau aplikasi berbasis Internet, sejatinya jejak digital itu akan tertinggal dan bisa dilacak (Kumparan.com, 2017).

Kita pun sebenarnya bisa merancang jejak digital yang baik. Misalnya dengan meninggalkan catatan karya atau prestasi di berbagai *platform* digital seperti media sosial maupun blog pribadi. Jejak-jejak digital positif yang kita tinggalkan ini di kemudian hari akan menjadi catatan diri kita di media digital. Harapannya ketika seseorang mengetikkan nama kita di

mesin pencari maka seluruh karya berkualitas yang pernah kita buat bisa muncul dan menjadi catatan nama baik.

***Data is the new oil.*** Terminologi mengenai data sebagai tambang baru nampaknya dipahami betul oleh perusahaan-perusahaan yang menggunakan internet sebagai basisnya. Saat ini data menjadi hal yang diperjual belikan (Tirto.id, 2019). Kita pasti pernah menerima telepon atau SMS tentang informasi togel, jual nomor HP yang mirip dengan nomor kita, penawaran asuransi, dan lain sebagainya. Pernahkah kita bertanya, dari mana mereka mendapatkan nomor ponsel kita? Hal ini memberikan kita gambaran, bahwa jejak digital kita yang tertinggal seringkali disalahgunakan oleh orang lain. Mungkin ketika kita masuk ke sebuah web, dan mendaftarkan akun, atau ketika kita masuk ke situs belanja daring dan mengisi data diri. Website pun semakin canggih sehingga saat ini website telah dapat membaca kebiasaan kita.

*Cookie* adalah salah satu cara untuk menghubungkan beberapa tindakan oleh satu pengguna ke dalam satu aliran yang terhubung. *Cookie* berupa rangkaian huruf dan angka yang berubah-ubah sesuatu tanpa makna yang melekat yang dikirimkan situs web ke *browser* web kita. Jejak digital dalam bentuk *cookie* digunakan untuk membuat Internet lebih bermanfaat, dan juga dapat membantu membuat transaksi individu lebih aman karena situs tersebut telah mendapatkan informasi spesifik tentang perilaku kita. Keputusan keamanan transaksi bergantung pada kombinasi beberapa faktor, termasuk *cookie*. Pengembang web telah menetapkan *cookie* sebagai salah satu cara paling nyaman untuk menambahkan ketekunan dan keamanan pada pengalaman web Anda, itulah mengapa *cookie* ada di mana-mana (internetociety.org, 2021).

Saat ini banyak website dan aplikasi yang tanpa kita sadari mengumpulkan jejak digital kita untuk kemudian mereka jual pada pihak lainnya. Mengapa data jejak digital kita menjadi komoditas? Bayangkan bila situs tempat kita bertransaksi daring merekam perilaku belanja para penggunanya. Mulai dari benda apa yang kita beli, berapa banyak, kemana pengirimannya, jenis kelamin yang membeli, ulasan terhadap barang tersebut, dan banyak hal lainnya. Tentu data ini dapat digunakan untuk menganalisa pasar, dan sangat bermanfaat bagi para produsen barang yang diperjual belikan.

Untuk memastikan bahwa situs dan aplikasi yang kita gunakan tidak membahayakan jejak digital kita, maka ada baiknya bila kita memeriksa dan membandingkan sistem keamanan situs web, aplikasi, dan metode transaksi elektronik yang ditawarkan oleh perorangan, toko, perusahaan, dan penyedia jasa perantara sebelum melakukan transaksi daring (Kurnia, dkk., 2021).

Selain dimanfaatkan oleh situs dan aplikasi daring, jejak digital juga banyak dimanfaatkan dalam dunia kerja. Banyak perusahaan baik skala besar dan kecil, yang saat ini menggunakan teknologi internet untuk mencari tahu tentang latar belakang karyawan yang akan dipekerjakan atau pun informasi tentang karyawan yang sedang bekerja. Pepatah lama 'Pilih teman Anda dengan bijak' sangatlah relevan dengan konteks jejaring sosial daring saat ini. Semakin banyak individu harus berhati-hati dalam menggunakan jaringan secara umum karena perusahaan semakin senang menggunakan informasi yang dikumpulkan dari jaringan sosial untuk menilai calon karyawan mereka (Peluchette & Karl, 2010).

Keberadaan dan tingkah laku kita semakin besar kemungkinannya untuk diketahui oleh orang lain melalui jejak digital yang kita tinggalkan. Dengan mempelajari rekam jejak digital kita melalui media sosial dan internet, perusahaan dapat memutuskan apakah mereka akan mempekerjakan kita atau tidak. Hal ini tentu menguntungkan bagi sebagian dari kita, dan merugikan bagi sebagian yang lain. Perlu diingat bahwa apa pun yang masuk ke internet dapat ditemukan hanya dalam waktu beberapa menit.

Meskipun media sosial seseorang tidak selalu menggambarkan keadaan sebenarnya dari orang tersebut, namun seringkali media sosial menjadi patokan untuk menilai. Banyak orang mengambil kesimpulan tentang orang lain hanya berdasarkan unggahan yang ia tinggalkan pada media sosialnya. Dalam dunia kerja, berdasarkan artikel yang di unggah oleh Linovhr.com (2018), terdapat beberapa parameter yang bisa dipakai menilai calon karyawan melalui media sosialnya antara lain kalimat yang sering diunggah di media sosial, foto-foto di media sosial, interaksi yang dilakukan, serta lingkaran pertemanan calon pelamar.

Anggota Asosiasi Digital Forensik Indonesia, Mukhlis Prasetyo Aji, dalam sebuah kesempatan menyatakan bahwa orang bisa terganjal dan susah mendapatkan pekerjaan karena jejak digitalnya. Mukhlis menuturkan, saat ini jejak digital sudah menjadi rujukan banyak lembaga atau perusahaan untuk merekrut tenaga kerja. Hal ini dapat terlihat dari salah satu syarat dimana pelamar wajib mencantumkan identitas media sosial mereka. Bukan tanpa alasan, perusahaan atau lembaga tersebut akan menelusuri kepribadian calon pekerjanya melalui rekam jejak di media sosial. Jika sang pelamar santun dan bijak dalam bermedia sosial, besar kemungkinan akan berdampak positif (Fahmi, 2018).

Oleh karena itu, menyampaikan sebuah pernyataan di media sosial haruslah berhati-hati. Apabila yang kita tuliskan dianggap merugikan pihak lain, maka sangat mungkin kita menjadi tersangka atas dakwaan perbuatan tak menyenangkan, ujaran kebencian, dan lainnya. Pada sisi yang lain, jejak digital kita pun dapat digunakan untuk meningkatkan kinerja kita di dunia kerja. Ada empat jenis motivasi utama penggunaan media sosial dengan jejak digital mereka. Keempat hal tersebut adalah memperkuat jaringan sosial, mencari teman yang cocok dan matang, mengembangkan usaha dan mencari koneksi bisnis (Benson & Filippaios, 2010).

### **REKAM JEJAK DIGITAL SULIT DIHILANGKAN**

Beberapa dari kita pasti bertanya, bagaimana cara menghapus jejak digital? Jawabannya adalah, tidak ada. Kita bisa saja meminta penyedia *platform* media digital untuk menghapus data yang kita miliki. Kita juga bisa menghapus atau menutup akun. Namun, dalam konteks kehidupan digital, kita tidak pernah hidup sendiri. Di luar sana ada orang-orang yang mungkin sudah menangkap tampilan layar atau mengarsipkan dokumen pribadi yang pernah kita unggah. Jika kejadiannya seperti ini, maka hampir mustahil untuk menghapus jejak ini secara utuh.

Untuk itu, kita harus berhati-hati ketika melakukan sesuatu di dunia digital. Di masa sekarang, dengan media sosial yang sudah menjadi keseharian, kita menjadi sangat mudah memberikan komen dan mempublikasikan sesuatu. Pepatah mengatakan, Mulutmu harimaumu. Sedikit di modifikasi untuk masa sekarang, Jarimu Harimaumu. Kadang kita tidak dapat mengerem apa yang kita komentarkan. (CNN Indonesia, 2019). Lalu apakah yang



sudah kita publikasikan dapat kembali kita tarik? Bisa, namun tidak semua data kita menjadi hilang. Masih ada data cadangan yang tersisa di digital, sehingga data tersebut dapat sewaktu-waktu ditarik kembali. Hal itu bisa terjadi meskipun kita telah menghapus seluruh informasi yang kita sebarakan sebelumnya. Ingat, jejak digital kita terekam selamanya dan secara otomatis tersimpan di berbagai belahan dunia.



Gambar V.6

Poster Rekam Jejak Digital

Sumber: Indonesiabaik.id, 2020

Di era penggunaan teknologi dan internet yang semakin maju, cara-cara dalam mencari informasi pun semakin beragam dan praktis sehingga sangat mudah bagi orang untuk mengorek informasi tentang kita di internet. Seperti dalam kasus-kasus *cyberbullying*, dapat dilihat bahwa *cyberbullying* banyak terungkap setelah ditelusuri dari rekam jejak digital korban dan pelakunya. Secara umum konten *cyberbullying* bisa dikirimkan oleh individual

maupun kelompok secara berulang kali yang isinya bisa tentang individu maupun kelompok lainnya dengan unsur konten yang bersifat kejam, vulgar, mengancam, mempermalukan, melecehkan, menakut-nakuti dan atau yang sesuatu yang berbahaya (Wijayanto, Fitriyani & Nurhajati, 2019). Jejak ini lah yang tertinggal ketika kita mempublikasikan sesuatu.

Terdapat banyak cara untuk meminimalisir terjadinya hal-hal yang tidak diinginkan serta cara melindungi jejak digital kita. Salah satu yang paling sederhana adalah dengan selalu menyempatkan untuk membaca syarat dan ketentuan aplikasi, media sosial dan juga situs web yang kita akses. Bagian ini memang terasa menjemukan untuk dibaca, tetapi mencermatinya bisa berguna di kemudian hari. Jika ada pilihan untuk tidak merekam jejak digital dan membagikannya ke pihak ketiga, kita bisa memilih opsi tersebut sehingga jejak digital kita aman. Kebiasaan lain yang patut diasah adalah kebiasaan untuk membatasi jenis data yang Anda bagikan. Jangan mengunggah informasi sensitif atau data pribadi seperti KTP, SIM, Paspor, PIN dan lainnya di media sosial.

Berbicara tentang berbagai kasus dan juga cara-cara melindungi rekam jejak digital, kita juga perlu mengetahui di mana posisi kita berdiri dalam dunia digital. Perlindungan terhadap rekam jejak seharusnya diberikan oleh pemerintah dan menjadi tanggung jawab normatif sebagai pengayom. Pada praktiknya, melalui kasus-kasus di atas dapat kita lihat dan temukan bahwa peraturan yang kini disediakan oleh pemerintah tidaklah ideal untuk melindungi. Alih-alih melindungi, sering kali peraturan ini malah menjebak dan menjerat masyarakat. Hingga saat ini, yang ada hanyalah perihal perlindungan data pribadi dalam UU ITE pasal 26 ayat 1 dan ayat 2, PP No 71/2019 (PSTE) dan PM Kominfo No 20/2016. Keduanya menjadi dasar dalam melindungi jejak digital yang juga menjadi bagian dari data pribadi kita. Namun, perlu kita ketahui bahwa kedua ini saja tidak cukup untuk menanggulangi. Dibutuhkan instrumen hukum secara spesifik yang mengadopsi perihal rekam jejak digital ini secara komprehensif. Selama aturan spesifik belum ada, maka kita harus mencari melalui aturan-aturan lain yang dapat dikaitkan dengan jejak digital.

Cara lain untuk mengelola jejak digital kita adalah dengan mempelajari dan menerapkan prinsip-prinsip literasi digital. Japelidi (Jaringan Pegiat Literasi Digital), telah mengembangkan 10 Kompetensi Digital untuk memudahkan kita mengelola jejak digital.

**Pertama**, kemampuan mengakses sudah melekat pada setiap orang yang secara aktif menggunakan sarana internet dalam kehidupannya sehari-hari. Setiap saat, setiap detik ketika kita membuka internet, maka di saat itu pula kita sudah meninggalkan jejak kita di dunia digital, tanpa terkecuali.

**Kedua**, setelah kita memiliki kemampuan kompetensi mengakses media digital, maka pemahaman kita harus lebih diasah. Di sinilah tahapan kompetensi memahami kita jalankan. Apabila sebelumnya kita hanya mengetahui sedikit tentang rekam jejak digital, maka kompetensi memahami ini membawa kita untuk mendalami dan mencari tahu lagi lebih banyak tentang jejak digital. Apabila kita telah memahami, maka akan lebih mudah bagi kita untuk mengetahui apa yang harus dilakukan selanjutnya.

**Ketiga**, mengetahui bentuk-bentuk rekam jejak digital merupakan salah satu tahapan dari kompetensi menganalisis dalam literasi digital. Kita harus cermat dan jeli menganalisis setiap kegiatan daring kita yang pasti meninggalkan jejak digital. Menerbitkan blog dan mengunggah pembaruan media sosial adalah cara populer lainnya untuk memperluas jejak digital kita. Setiap tweet yang kita posting di Twitter, setiap pembaruan status yang kita publikasikan di Facebook, dan setiap foto yang kita bagikan di Instagram berkontribusi pada jejak digital kita. Semakin banyak kita menghabiskan waktu di situs jejaring sosial, semakin besar jejak digital kita. Bahkan mengklik "menyukai" halaman atau kiriman Facebook menambah jejak digital kita, karena datanya disimpan di server Facebook.

**Keempat**, setelah kemudian kita tahu dan memahami lebih dalam tentang jejak digital, maka kita harus mulai menyeleksi apa saja yang kita unggah. Proses ini harus dilakukan agar kita waspada atas setiap jejak digital yang kita tinggalkan. Setiap orang yang menggunakan Internet memiliki jejak digital, jadi itu bukan sesuatu yang perlu dikhawatirkan. Namun, sebaiknya pertimbangkan jejak data apa yang hendak kita tinggalkan. Misalnya, dengan menyeleksi, kita dapat mencegah mengirim email yang kurang sopan, yang terlalu "pedas", dan lain sebagainya, karena pesan tersebut mungkin tetap daring selamanya. Ini juga dapat membuat kita lebih berhati-hati dengan apa yang kita publikasikan di situs web serta media sosial. Meskipun kita sering kali dapat menghapus konten dari situs media sosial, setelah

data digital dibagikan secara daring tidak ada jaminan bahwa kita dapat menghapusnya dari Internet.

**Kelima**, verifikasi harus kita lakukan untuk memastikan apakah Langkah yang akan kita lakukan dapat berpotensi meninggalkan jejak digital yang berdampak buruk atau tidak. Dengan memverifikasi informasi yang keluar dan masuk, kita dapat memastikan bahwa informasi yang kita sebar adalah informasi yang baik. Selain itu, perlu juga dilakukan verifikasi terhadap situs atau aplikasi yang kita gunakan. Hal ini diperlukan untuk menghindari kita menggunakan website atau aplikasi yang telah disusupi sehingga jejak digital kita dicuri atau bahkan digunakan untuk kejahatan.

**Keenam**, evaluasi atas berbagai kegiatan daring kita menjadi bagian tak terpisahkan ketika kita membahas beragam contoh kasus yang berkaitan erat dengan jejak digital di media daring. Tak bisa dipungkiri, seringkali orang cenderung abai atau menganggap remeh kegiatan daring yang sangat umum dan sehari-hari kita lakukan. Seolah kita lupa bahwa setiap Langkah kita mengklik apapun di internet akan meninggalkan jejak yang menetap dan sulit dihapus begitu saja. Evaluasi secara berkala terhadap data-data yang kita tinggalkan, akun yang kita miliki dan hal-hal lain terkait dengan keberadaan digital kita dapat melindungi kita dari penyalahgunaan jejak digital oleh pihak yang tidak bertanggung jawab.

**Ketujuh**, saat ini, ketika kita mendistribusikan informasi dengan menggunakan perangkat digital, kita juga telah meninggalkan jejak digital. Contohnya ketika kita meneruskan pesan di WhatsApp, muncul tanda panah yang menandakan kita meneruskan pesan. Atau proses mencuitkan kembali di Twitter, *repost* di Instagram dan lain-lain. Untuk itu, kita perlu mengetahui bahwa proses distribusi yang kita lakukan pun tidak terlepas dari jejak digital kita sehingga kita dapat berhati-hati dalam melakukan proses distribusi.

**Kedelapan**, kemampuan kita dalam memproduksi rekam jejak digital yang baik perlu untuk ditingkatkan. Tidak dapat dipungkiri bahwa jejak berupa data yang telah kita produksi akan tertinggal lama di internet. Meskipun kita telah menghapusnya, internet telah menduplikasi jejak kita dan membuatnya tetap ada. Oleh karenanya, kita perlu memperhatikan serta waspada akan jejak yang kita hasilkan.

**Kesembilan**, pengetahuan yang telah kita dapatkan tentang rekam jejak digital ini akan semakin bermanfaat bila dapat kita bagikan pada orang lain. Kompetensi partisipasi mengajak kita untuk dapat turut serta dalam melindungi jejak digital kita dan juga orang lain. Tidak hanya melindungi, namun juga memperindah jejak digital kita. Partisipasi dapat dilakukan dengan tidak turut menyebarkan jejak digital orang lain, tidak menyalahgunakan jejak digital, serta melakukan pengecekan jejak digital kita masing-masing secara berkala.

**Kolaborasi**, adalah kompetensi yang paling akhir dicapai dalam 10 kompetensi literasi digital Japelidi. Sangat sederhana, kolaborasi yang dimaksud adalah bagaimana kita sebagai orang-orang yang memiliki rekam jejak digital, berkolaborasi dengan berbagai pihak dalam rangka partisipasi kita menjaga rekam jejak digital kita. Banyak hal dapat kita kerjakan sendirian. Namun akan semakin besar dampaknya bila kita mengerjakannya Bersama-sama. Untuk itu diperlukan kolaborasi.

## **SIMPULAN DAN REKOMENDASI**

Dalam pengembangannya, bab ini sangat terbuka untuk menerima masukan dan saran dari pihak-pihak terkait mengenai perlindungan dan pemanfaatan rekam jejak digital. Diharapkan bahwa pada pengembangan kedepan, bab ini dapat memperoleh masukan dengan mempertimbangkan macam-macam pembaca dan pengguna yang merupakan target dari bab ini. Tentunya segmentasi pembaca akan sangat beragam, seiring dengan beragamnya pengguna ranah digital saat ini. Sebagai perhatian khusus, pengembangan diperlukan terutama bagi kelompok terpinggirkan (anak, perempuan dan kaum difabel), masyarakat di Kawasan 3T (terdepan, terluar dan tertinggal), serta juga berdasarkan kategori usia. Seluruhnya adalah mereka yang pernah bersinggungan dengan perangkat digital, apa pun itu. Untuk itu, perlu dilakukan pendekatan-pendekatan spesifik agar dapat menjangkau seluruh lapisan, terutama bagi lapisan masyarakat yang rentan penyalahgunaan rekam jejak digital. Selain itu, banyak hal dapat dilakukan, terutama bila kita mengelaborasi 10 kompetensi literasi digital Japelidi.

Untuk itu, berikut adalah beberapa rekomendasi hal-hal yang perlu dilakukan untuk meningkatkan kecakapan dan pengetahuan tentang rekam jejak digital ini.

Tabel V.1

Matriks rekomendasi program literasi digital  
untuk meningkatkan kecakapan perlindungan rekam jejak digital

| Aspek/<br>Khalayak<br>Sasaran  | Anak dan<br>Remaja   | Perempuan  | Lansia  | 3T<br>(Terdepan,<br>Terluar,<br>Tertinggal)   | Penyandang<br>Disabilitas   |
|--|--|--|---|---|---|
| <b>Mengetahui<br/>dan<br/>Memahami<br/>rekam jejak<br/>digital</b>                 | Mulai dikenalkan kepada anak-anak sejak usia awal melalui kegiatan sekolah dengan pendampingan guru  | Melalui pelatihan dan <i>talkshow</i> , dikenalkan mengenai bahaya rekam jejak digital (dengan pendekatan kasus KBGO)  | Memberikan pendampingan bagi lansia untuk memahami tentang rekam jejak digital, melalui kegiatan rutin khusus seperti di RT atau lingkungan sekitar | Penjangkauan kepada kelompok 3T, dengan informasi yang disederhanakan sesuai dengan bahasa daerah atau dengan konten spesifik yang mudah mereka cerna | Konten-konten yang mudah untuk digunakan, dengan cara dan bahasa yang sesuai perlu untuk dibuat |
| <b>Mengelola<br/>dan<br/>memproduksi<br/>rekam jejak<br/>digital yang<br/>baik</b> | Sejak dini melalui sekolah, diberikan pengetahuan tentang cara mengelola rekam jejak digital (dalam kurikulum atau dapat juga sebagai <i>insert</i> kegiatan), serta orang tua turut | Melalui pelatihan dan <i>talkshow</i> , serta konten sosial yang memberikan cara-cara serta panduan untuk mengelola, serta memproduksi rekam jejak digital yang baik | Melalui pendampingan rutin yang dilakukan dari lingkup yang dekat. Selain memberikan aktivitas, juga memberikan informasi baru bagi mereka.         | Penjangkauan kepada kelompok 3T, dengan informasi yang disederhanakan sesuai dengan bahasa daerah atau dengan konten spesifik yang mudah mereka cerna | Konten-konten yang mudah untuk digunakan, dengan cara dan bahasa yang sesuai perlu untuk dibuat |

|  |   |                                    |  |  |  |
|--|---|------------------------------------|--|--|--|
|  | serta memantau penggunaan saluran digital | dan tidak membahayakan bagi mereka |  |  |  |
|--|---|------------------------------------|--|--|--|

Untuk menutup bagian ini, mari kita pikirkan kembali. Jenis informasi apa yang ingin kita temukan tentang diri kita secara daring dalam 10 tahun mendatang?

Kita memiliki kendali atas jejak digital kita. Pada sisi lainnya, jejak digital juga adalah hal yang tidak dapat kita kendalikan karena berada pada pihak lain. Namun, kita dapat membuat keputusan tentang apa yang kita publikasikan di internet, media sosial, *platform* pesan dan sebagainya, meskipun kita tidak dapat mengontrol bagaimana orang lain mempersepsikan diri kita. Penting bagi kita untuk dapat membentuk dan menjaga jejak digital kita, sebaik-baiknya sejauh yang kita dapat lakukan.

## EVALUASI KOMPETENSI PERLINDUNGAN REKAM JEJAK DIGITAL

Tabel V.2  
Evaluasi Kemampuan Perlindungan Rekam Jejak Digital

| No. | Aspek Perlindungan Rekam Jejak Digital | Domain Evaluasi   |  |   |
|-----|--|---|--|---|
|     |  | Kognitif  | Afektif  | Konatif/ <i>behavioral</i>  |
| 1   | Bentuk rekam jejak digital             | Mengetahui konsep serta bentuk rekam jejak digital                                  | Menyadari pentingnya perlindungan rekam jejak digital bagi diri sendiri, orang lain, maupun keluarga | Mempraktikkan perlindungan rekam jejak digital dalam keseharian   |
| 2   | Kasus-kasus jejak digital di Indonesia | Mengetahui dan dapat mengidentifikasi kasus-kasus rekam jejak digital di sekeliling | Menyadari pentingnya untuk tetap update mengenai berita kasus-kasus rekam jejak digital              | Mempraktikkan perlindungan rekam jejak digital terutama setelah mengetahui contoh kasus                             |
| 3   | Rekam jejak digital sulit dihilangkan  | Mengetahui bahwa rekam jejak digital sulit dihilangkan                              | Menyadari bahwa perlindungan rekam jejak digital harus diutamakan                                    | Mempraktikkan kehati-hatian dalam kegiatan digital untuk menjaga rekam jejak digital diri sendiri maupun orang lain |

## CONTOH *BENTUK* EVALUASI KEMAMPUAN PERLINDUNGAN REKAM JEJAK DIGITAL

Isilah lembar evaluasi di bawah ini berdasarkan pengalaman sehari-hari untuk mengukur kemampuan perlindungan rekam jejak digital berdasarkan aspek perilaku. Form ini dapat diisi oleh pengguna *platform* digital sebagai lembar evaluasi diri. Isian ini juga dapat diisi oleh pengajar atau pegiat literasi digital dalam mengevaluasi peserta didik, dan juga digunakan dalam program-program literasi digital.

Tabel V.3  
Evaluasi Kemampuan Perlindungan Rekam Jejak Digital

| No | Pernyataan   | Berilah tanda V (centang) pada salah satu pilihan |        |        |               | Alasan |
|----|--|---|--------|--------|---------------|--------|
|    |  | Sangat Jarang                                     | Jarang | Sering | Sangat Sering |        |
| 1  | Saya mengunggah konten positif saja                                |   |        |        |               |        |
| 2  | Saya dapat membedakan rekam jejak digital yang baik dan yang buruk |   |        |        |               |        |
| 3  | Saya menjaga rekam jejak digital yang saya tinggalkan              |   |        |        |               |        |
| 4  | Saya membatasi data yang saya bagikan                              |   |        |        |               |        |
| 5  | Saya selalu mengecek kembali jejak digital yang saya tinggalkan    |   |        |        |               |        |
| 6  | Saya dapat menciptakan jejak digital yang baik untuk diri sendiri  |   |        |        |               |        |

## DAFTAR PUSTAKA

Azucar, D., Marengo, D., & Settanni, M. (2018). Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis. *Personality and individual differences*, 124, 150-159.

Benson, V., & Filippaios, F. (2010). Effects of digital footprint on career management: evidence from social media in business education. In *World Summit on Knowledge Society* (pp. 480-486). Springer, Berlin, Heidelberg.

CNNIndonesia. (2018, Juni 5). Jejak digital sulit dihapus, hati-hatilah berucap di internet.

cnnindonesia.com

Diperoleh

dari



- <https://www.cnnindonesia.com/teknologi/20180604203115-185-303426/jejak-digital-sulit-dihapus-hati-hatilah-berucap-di-internet>
- Digital Footprint (def.1) (n.d). dalam Dictionary Online. Diperoleh dari <https://www.dictionary.com/browse/digital-footprint>
- ELSAM. (2018, Agustus 18). Kasus Penyalahgunaan Data Pribadi Sepanjang 2013 Sampai Dengan 2017. *ELSAM Multimedia*. Diperoleh dari <https://multimedia.elsam.or.id/infografis-kasus-penyalahgunaan-data-pribadi-sepanjang-2013-2017/>
- Fahmi, M.I. (2018, Agustus 8). Tak kunjung dapat kerja? Coba cek media sosial anda. Kompas.com Diperoleh dari <https://regional.kompas.com/read/2018/08/03/21200431/tak-kunjung-dapat-kerja-coba-cek-media-sosial-anda>.
- Internet Society .(2016). Why Did We Start Leaving Such Big Footprints. Diperoleh dari [https://www.internetsociety.org/wp-content/uploads/tutorials/Why\\_did\\_we\\_Start\\_Leaving\\_such\\_Big\\_Footprints/presentation\\_content/external\\_files/Why\\_Did\\_We\\_Start\\_Leaving\\_Such\\_Big\\_Footprints.pdf](https://www.internetsociety.org/wp-content/uploads/tutorials/Why_did_we_Start_Leaving_such_Big_Footprints/presentation_content/external_files/Why_Did_We_Start_Leaving_Such_Big_Footprints.pdf)
- Kresna, M. (2019, Maret 2020) bagaimana data nasabah kartu kredit diperjualbelikan. Titro.id. Diperoleh dari <https://tirto.id/bagaimana-data-nasabah-kartu-kredit-diperjualbelikan-djSv>
- Kurnia, N., Sadasri, L.M., Angendari, D.A.D., Yuwono, A.I., Syafrizal, Monggilo, Z.M.Z., & Adiputra, W.M., (2021). *Yuk, sahabat perempuan bertransaksi daring dengan cermat*. Program Studi Magister Ilmu Komunikasi UGM.
- Linovhr.com. (2018, Juli 2013). Trend HR: Menerawang calon karyawan melalui media sosial. *Linovhr.com*. Diperoleh dari <https://www.linovhr.com/trend-hr-menerawang-calon-karyawan-melalui-media-sosial/>
- Mardiastuti, A. (2018, Agustus 7). Luna Maya-Cut Tari etap tersangka, ini jejak 8 tahun kasusnya. Detik.com. Diperoleh dari <https://news.detik.com/berita/d-4153964/luna-maya-cut-tari-tetap-tersangka-ini-jejak-8-tahun-kasusnya>
- Nawi A., Hussin Z., Ren C.C., Norsaidi N.S., Mohd Pozi M.S. (2020) Identifying the types of digital footprint data used to predict psychographic and human behaviour. In: Ishita E., Pang N.L.S., Zhou L. (eds) *Digital Libraries at Times of Massive Societal Transition*.

- ICADL 2020. Lecture Notes in Computer Science, vol 12504. Springer, Cham.  
[https://doi.org/10.1007/978-3-030-64452-9\\_26](https://doi.org/10.1007/978-3-030-64452-9_26)
- Netsafe. (2019, Juli 22). What is a digital footprint?. netsafe.org. Diperoleh dari  
<https://www.netsafe.org.nz/digital-footprint>.
- O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. *Pediatrics*, 127(4), 800-804.
- Peluchette, J., & Karl, K. (2009). Examining students' intended image on Facebook: "What were they thinking?!" . *Journal of education for business*, 85(1), 30-37.
- Shahlihah. N. F. (2020, Juni 29). Heboh twit dirut TVRI Iman Brotoseno soal film porno, ini klarifikasinya. Kompas.com. Diperoleh dari  
<https://www.kompas.com/tren/read/2020/05/29/191555365/heboh-twit-dirut-tvri-iman-brotoseno-soal-film-porno-ini-klarifikasinya?page=all>
- Smartschoolonline.id. (2018, November 21). Jejak digital. *Smartschoolonline.id*. Diperoleh dari <https://smartschoolonline.id/materi/detail/65/Jejak-Digital>
- Society. (2016, Januari 12) Your digital footprint paints a picture of who you are. Internetociety.org. Diperoleh dari <https://www.internetsociety.org/tutorials/your-digital-footprint-matters/>
- Vonbank, C. (2019, September 2). Your digital footprint: What is it exactly? <https://medium.com/global-citizen-foundation/your-digital-footprint-what-is-it-exactly-a8c49737af2b>
- Wijayanto, X.A., Fitriyani, L.R., & Nurhajati, L. (2019). *Mencegah dan Mengatasi Bullying di Dunia Digital*. Penerbit LP3M LSPR.
- Zebua, D.J. (2017, Juni 16). Hina polisi di Facebook usai ditilang, seorang PNS dijerat UU ITE. Kompas.com. Diperoleh dari  
<https://regional.kompas.com/read/2017/06/16/07040051/hina.polisi.di.facebook.usai.ditilang.seorang.pns.dijerat.uu.ite>.



# BAB VI

---

## Keamanan Anak di Platform Digital

## **BAB VI**

### **KEAMANAN ANAK DI *PLATFORM* DIGITAL**

*Fransiska Desiana Setyaningsih Setyaningsih*

#### **URGENSI MEMAHAMI PENTINGNYA KEAMANAN ANAK**

Teknologi komunikasi dan informasi berkembang sangat cepat. Kemunculan media baru dalam hal ini internet, semakin memudahkan kita dalam mengakses informasi. Tentu banyak diantara kita tidak asing lagi dengan Facebook, Instagram, Twitter, WhatsApp dan sebagainya. Nama-nama tadi merupakan sebagian aplikasi yang disediakan untuk memudahkan kita agar dapat berkomunikasi dengan banyak orang. Dengan memiliki salah satu atau lebih aplikasi tersebut, kita sudah dapat terhubung dengan dunia luar yang sangat luas. Kita dengan mudahnya dapat mengakses berbagai informasi dan dengan mudahnya membagikan informasi.

Itulah mengapa, era ini dikenal juga sebagai era digital, yakni era di mana informasi semakin mudah dan cepat diperoleh, selanjutnya disebarluaskan menggunakan teknologi digital. Teknologi digital sendiri adalah teknologi yang menggunakan sistem komputerisasi yang terhubung dengan internet. Penggunaan teknologi digital yang tepat tentu saja akan membawa dampak positif, sebaliknya jika digunakan dengan tidak tepat maka akan membawa dampak negatif bagi penggunanya. Di Indonesia, pengguna teknologi digital cukup tinggi, terutama penggunaan gawai untuk mengakses internet, khususnya media sosial. Berdasarkan data tahun 2017, tercatat 92,82% pengguna media sosial di Indonesia, didominasi oleh generasi milenial, yakni sebanyak 97,4% (indonesiabaik.id, 2017).

Dalam media digital, setidaknya ada empat hal yang perlu mendapat perhatian dari kita semua, yakni pembuat pesan, sifat pesan, cara penyebaran pesan dan dampak pesan. Pertama, pembuat pesan, semua orang dapat membuat pesan sehingga anak-anak pun tertarik memiliki akun sendiri, menampilkan diri dan berinteraksi dengan orang lain yang tidak dikenal. Hal ini menimbulkan ancaman sekaligus kesempatan terutama berkaitan dengan privasi dan keselamatan anak-anak. Kedua, sifat pesan media digital, sangat beragam karena bersumber dari seluruh penjuru dunia, terlebih sebagian besar tidak

disaring oleh pekerja media profesional. Hal ini membuat anak-anak menerima aneka pesan yang sangat mungkin tidak sesuai dengan nilai-nilai agama dan budaya keluarga mereka. Ketiga, penyebaran pesan, penyedia layanan media digital ingin mendapatkan keuntungan ekonomi maka mereka merancang medianya agar menarik. Keempat, dampak pesan, jika digunakan secara baik media digital adalah sumber pengetahuan tak terbatas. Pengguna dapat menggunakannya untuk belajar hal-hal praktis hingga rumit. Kita dapat lebih produktif jika mampu memanfaatkan media digital ini dengan baik. Namun, konten negatif yang berdampak buruk juga banyak bertebaran di dunia maya seperti berita palsu, kekerasan, pornografi dan sebagainya.

Saat kita berinteraksi dengan pengguna media digital lainnya, kita harus memperhatikan bahwa apa yang kita lakukan akan berdampak bagi mereka. Karena pengguna media digital tidak terbatas, mencakup semua orang termasuk difabel, perempuan, anak, lansia dan juga berasal dari beragam wilayah termasuk kawasan 3T (Tertinggal, Terluar, Terdepan). Oleh karena itu, ada banyak faktor yang sebaiknya kita pertimbangkan sebelum berbagi informasi dengan pengguna media digital lainnya. Pertama, kita harus memastikan informasi tersebut bisa dipercaya. Kedua, kita juga harus mempertimbangkan nilai manfaat informasi tersebut jika dibagikan. Tak heran jika untuk mengingatkan pentingnya berhati-hati dalam berbagi informasi, banyak kampanye literasi digital dilakukan oleh berbagai organisasi atau komunitas, misalnya saja dengan slogan yang jamak digunakan: *saring sebelum sharing* (Monggilo, Kurnia, & Banyumurti, 2020).



Gambar VI.1

Saring Baru *Sharing*

Sumber: indonesia.go.id (2019, Januari 22)

Secara umum, meskipun aplikasi media digital mempunyai ketentuan usia penggunaanya, tapi dalam praktiknya, yang lumrah saat ini ketika anak-anak dari berbagai usia, pendidikan, latar belakang sosial maupun wilayah, juga lincah berselancar di media sosial dengan gawai yang mereka miliki. Penggunaan aplikasi media sosial pada anak-anak hingga saat ini masih menjadi perhatian tersendiri bagi para penggiat literasi digital. Karena kelompok anak-anak merupakan kelompok yang rentan terhadap berbagai kejahatan digital di dunia maya. Banyak kasus yang mengancam keselamatan terhadap anak di bawah umur yang terjadi

karena disebabkan oleh ketidaktahuan dan ketidakmampuan menggunakan media sosial dengan baik dan benar.



Gambar VI.2

Poster Digital "Penggunaan Media Sosial pada Anak"

Sumber: newslab.uajy.ac.id (2017, Desember 7)

Gambar di atas menunjukkan mengenai beberapa aspek positif dan aspek negatif dari penggunaan media sosial pada anak. Selanjutnya dari gambar tadi kita juga bisa mengetahui bahwa sejumlah besar anak-anak dan remaja telah terekspos konten pornografi terutama yang muncul tidak dengan sengaja saat mengakses media sosial.

Kebanyakan anak-anak tidak terlalu memahami atau bahkan tidak peduli akan bahaya yang dapat mengancam mereka. Selain itu, anak-anak dapat dengan mudahnya saling berbagi informasi termasuk data yang sifatnya pribadi, bahkan dengan orang yang baru dikenalnya. Lalu apa yang dimaksud dengan informasi pribadi? Segala hal yang dapat mengidentifikasi kita itulah informasi pribadi, contohnya nama lengkap, alamat rumah, nomor kartu

identitas, nama ibu kandung, riwayat kesehatan, nomor telepon dan sebagainya (Monggilo, Kurnia, & Banyumurti, 2020).

Selain untuk saling bertukar informasi, media digital juga menawarkan hiburan secara daring. Salah satu hiburan yang digemari hampir sebagian besar pengguna gawai adalah bermain *game*, baik perorangan maupun tim. *Game* memiliki konten yang mirip dengan produk media hiburan pada umumnya. Konten dalam *game* bisa memiliki konsekuensi efek yang positif maupun negatif, efek yang sesuai dengan norma dan regulasi di Indonesia maupun yang tidak. Kekerasan, pornografi, adalah sedikit dari banyak muatan konten dalam *game* yang harus dapat disikapi dengan bijak oleh para pemainnya, termasuk di Indonesia (Yuwono dkk, 2018).

Melihat kenyataan seperti ini, maka perlu adanya kesadaran terhadap keselamatan digital anak-anak terutama mereka yang masih di bawah umur. Sehingga literasi digital menjadi hal yang penting. Hal ini juga didukung oleh riset Japelidi tahun 2017, dimana kegiatan yang berkaitan dengan literasi digital di Indonesia masih lebih banyak berfokus di lembaga pendidikan, bukan di masyarakat secara langsung.

Untuk itulah maka bab terakhir dalam Modul *Digital Safety* ini menekankan pada anak-anak saat beraktivitas menggunakan media digital. Sebab sebagai pribadi pengguna media digital, anak-anak perlu membekali dirinya agar dapat terhindar dari berbagai ancaman keselamatan yang mengintai saat beraktivitas menggunakan media digital. Beberapa pertanyaan berikut akan memandu kita dalam menggunakan modul ini. Pertama, Apa saja aspek keselamatan anak di media digital? Kedua, Bagaimana cara mencegah dan mengatasi ancaman keselamatan pada anak saat menggunakan media digital berikut contoh kasus? Ketiga, Rekomendasi apa yang dapat diberikan untuk meningkatkan pemahaman terhadap ancaman keselamatan anak bermedia digital? Keempat, Proteksi keamanan seperti apa yang ditawarkan kepada anak-anak terutama yang berkebutuhan khusus (penyandang disabilitas), perempuan dan mereka yang berada di wilayah 3T (Tertinggal, Terdepan dan Terluar)?



Modul ini juga dilengkapi dengan evaluasi dan lembar evaluasi pada bagian akhir, untuk menguji pemahaman kita berkaitan dengan keamanan dan keselamatan anak-anak dalam dunia digital. Sehingga pada akhirnya, kita bisa membantu anak-anak agar memiliki kemampuan untuk melindungi diri saat menggunakan media digital.

### **ASPEK-ASPEK KESELAMATAN ANAK DI MEDIA DIGITAL**

Keterarikan anak-anak terhadap media digital memang sudah tidak diragukan. Berbagai kemudahan dan kesenangan yang ditawarkan menjadi salah satu daya tarik. Apalagi saat ini, saat pandemi COVID-19 sedang melanda dunia, termasuk Indonesia, di mana banyak aktifitas tatap muka yang dibatasi, maka ketergantungan akan gawai menjadi sangat besar.

Berdasarkan survei yang penulis lakukan terhadap beberapa anak, terlihat bahwa hampir sebagian besar waktu mereka dihabiskan dengan bermain gawai. Saat menunggu atau setelah menyelesaikan tugas sekolah, adalah waktu di mana kebanyakan mereka menghabiskan waktu dengan bermain gawai. Aktivitas dengan gawai yang biasa dilakukan adalah bermain *game*, berselancar di dunia maya melalui akun media sosial yang dimiliki hingga menggunakan berbagai aplikasi yang ditawarkan seperti TikTok. Semua itu mereka lakukan untuk mengisi waktu luang yang banyak kosong karena harus beraktivitas dari rumah dan juga untuk menunjukkan eksistensi mereka.

Sebenarnya tidak ada larangan penggunaan gawai oleh anak-anak, meskipun patut diperhatikan bahwa orangtua sebaiknya mendampingi mereka. Sebab, anak-anak belum sepenuhnya paham akan ancaman yang mengintai keselamatannya. Ancaman tersebut bisa muncul tiba-tiba tanpa mereka sadari. Berikut ini beberapa aspek keselamatan anak yang disebabkan oleh penggunaan media digital.

**Pertama, perundungan (*bullying*)** yang terjadi secara daring sering memanfaatkan berbagai fasilitas pesan singkat, email hingga media sosial. Perundungan dapat diartikan sebagai perilaku tidak menyenangkan baik secara verbal, fisik maupun sosial yang diterima seseorang atau sekelompok orang. Korban perundungan tidak terbatas, bisa anak-anak maupun dewasa, berasal dari berbagai latar belakang sosial, pendidikan, ekonomi bahkan

hingga mereka yang berkebutuhan khusus atau difabel. Pelaku perundungan juga bisa beragam, seusia atau lebih tua, dikenal atau bahkan tidak dikenal sama sekali.

Kasus perundungan di media digital terjadi karena unggahan konten yang sifatnya pribadi. Konten tersebut kemudian viral lalu dibagikan berkali-kali oleh banyak orang ke berbagai media sosial. Berbagai komentar bermunculan, mulai dari isi konten sampai ke keluarga, teman, sekolah, tempat kerja dan sebagainya. Korban perundungan biasanya menjadi depresi, mengurung diri, kehilangan kepercayaan diri hingga keinginan untuk mengakhiri hidup. Seperti kasus perundungan yang menimpa Zara Adhisty, salah satu artis Indonesia, yang mengunggah video dengan kekasihnya di Instagram menjadi sorotan publik. Dalam kasus ini Zara kemudian memilih untuk menghilang (Samsoerizal, 2020). Infografis berikut bisa membantu kita untuk mengetahui bentuk perundungan yang biasa terjadi melalui media digital.



Gambar VI.3

Infografis “Ini Jenis Hinaan dan Kata-kata yang Sering Digunakan oleh Para Pelaku Bullying di Media Sosial. Sumber: femina.co.id (2017, Oktober 13)

**Kedua, perdagangan orang.** Tindak Pidana Perdagangan Orang (TPPO) berupa perekrutan, pengangkutan, penampungan, pengiriman, pemindahan atau penerimaan seseorang disertai dengan ancaman dan intimidasi bertujuan untuk eksploitasi baik dalam negeri maupun luar negeri (Sukmawati dkk, 2019). Tindak perdagangan orang seperti ini bukan saja menasar orang dewasa namun dengan maraknya media sosial, tindak ini juga menasar terutama perempuan dan anak-anak. Salah satu bentuk kasus perdagangan orang yang berhasil diungkap adalah praktik perdagangan anak di Surabaya yang dilakukan melalui media sosial instagram (Rianda, 2018). Tindak perdagangan orang seringkali dilatarbelakangi oleh kesulitan secara ekonomi, kemiskinan dan rendahnya tingkat pendidikan. Kehadiran media digital seperti saat ini sering dimanfaatkan oleh para pelaku untuk membujuk korbannya. Oleh karena itu, kemampuan memanfaatkan media secara cerdas adalah suatu keharusan guna mencegah tindak pidana perdagangan orang. Infografis di bawah ini dapat kita gunakan sebagai salah satu pedoman untuk menghindari tindak perdagangan orang.



Gambar VI.4

Infografis “Magang Palsu di Luar Negeri”

Sumber: akurat.co (2018, April 05)

**Ketiga, pencurian data pribadi.** Pencurian data pribadi melalui media digital menjadi sorotan banyak pihak karena rentan digunakan untuk pelanggaran lain seperti penipuan

akun, pemalsuan dokumen, perdagangan orang hingga terorisme. Pencurian identitas terutama secara digital merupakan kegiatan ilegal pengambilan informasi pribadi seseorang melalui internet yang biasanya akan dipergunakan untuk melakukan kejahatan lain dan akan sangat merugikan korban (Nurdiani, 2020). Berbagai macam masalah yang sering ditemukan dalam hal keamanan informasi antara lain penyadapan pasif, penyadapan aktif, penipuan dan lain-lain. Dalam prakteknya, pencurian data dapat berwujud dalam pembacaan suatu data *file* teks oleh pihak yang tidak berwenang, memanipulasi data *file* teks, kerusakan data akibat buruknya konektivitas fisik ataupun keamanan dari data tersebut (Putra & Garuda, 2017). Berikut ini adalah gambar modus pencurian yang saat ini marak di media daring.





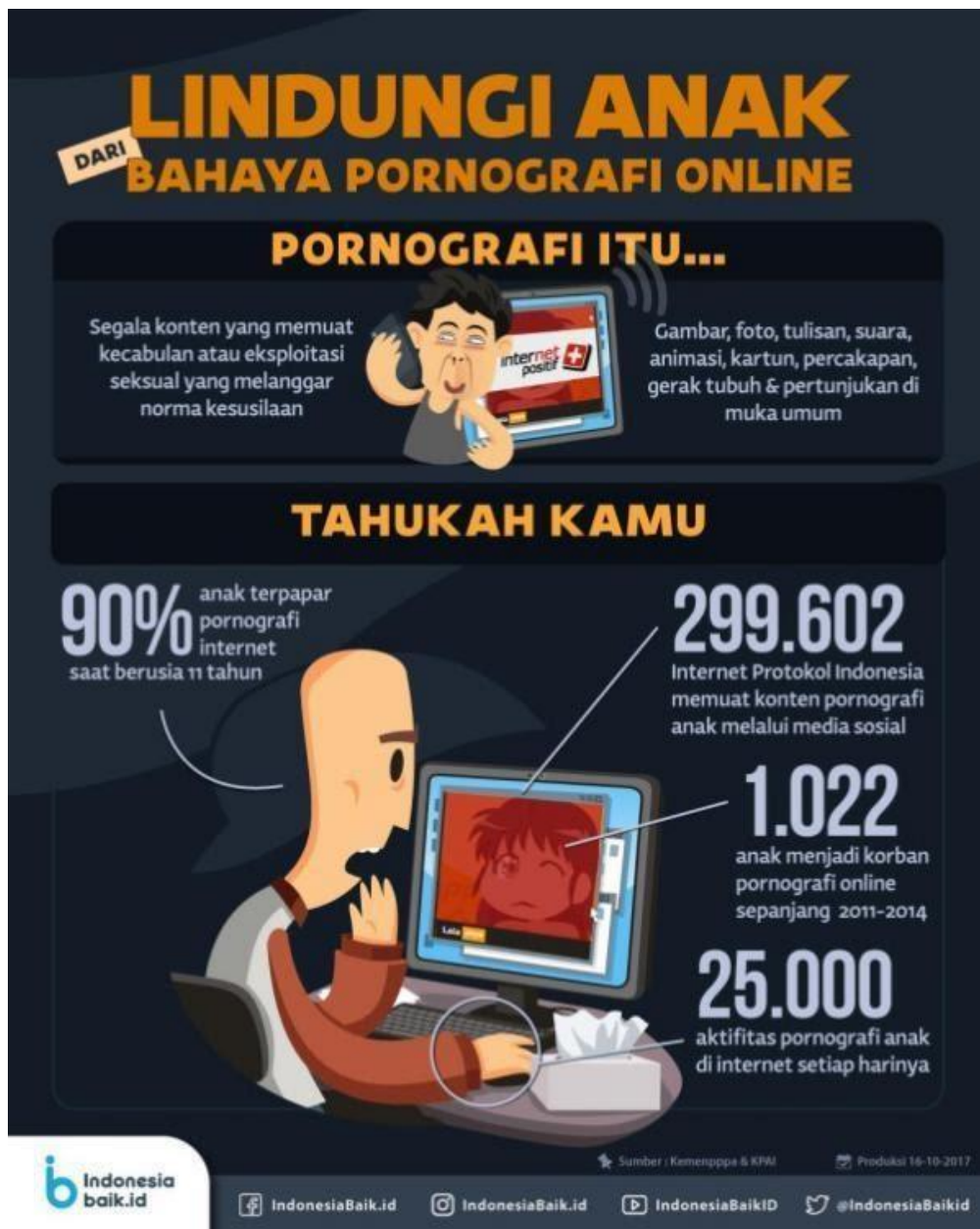
Gambar VI.5

Infografis “Dugaan Pembobolan Data Sepanjang 2020”

Sumber: republika.co.id (2020, September 02)

**Keempat, pelecehan seksual dan pornografi.** Pelecehan seksual adalah perilaku yang terkait dengan seks yang tak diinginkan, perilaku yang dianggap melanggar norma kesopanan dan kesusilaan. Pornografi bisa diartikan sebagai segala konten yang memuat eksploitasi seksual yang melanggar norma kesusilaan. Pelecehan seksual dapat terjadi kapan saja dan di mana saja, termasuk secara daring demikian juga dengan pornografi. Pelecehan seksual dan pornografi secara daring melalui media digital kerap menimpa perempuan dan anak-anak, dengan beragam bentuk, mulai dari tulisan, pesan suara, animasi, percakapan baik dalam bentuk gambar, foto maupun video. Salah satu kasus munculnya pelecehan ini bisa dimulai dari hal yang sederhana, misalnya berkenalan melalui media digital. Hubungan yang terjalin bisa berlanjut hingga tahap di mana kedua belah pihak mulai saling mengirimkan informasi, biasanya foto atau video yang sifatnya pribadi/intim. Suatu saat korban (biasanya perempuan) akan diancam foto atau video pribadi tadi akan disebar jika tidak menuruti keinginan pelaku (Ramadhan, 2020). Agar anak dapat terhindar dari pelecehan seksual secara daring, maka kita perlu mengoptimalkan pengasuhan digital, pengasuhan yang bertujuan untuk menghindarkan anak dari ancaman dan memaksimalkan potensi digital.

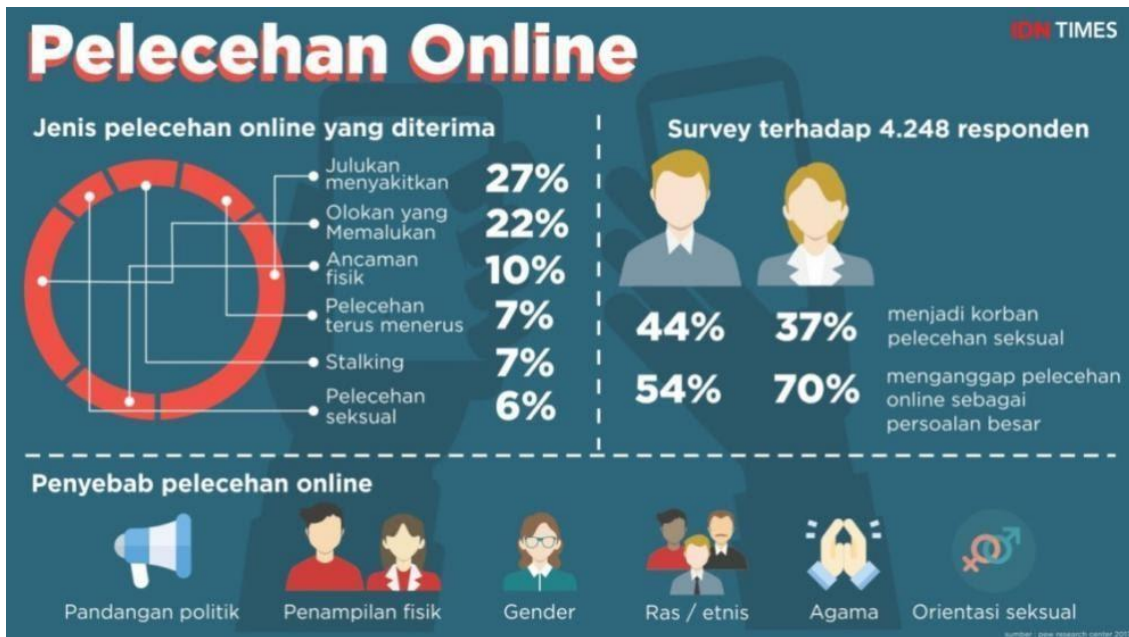




Gambar VI.6

Infografis “Lindungi Anak Dari Bahaya Pornografi Online”

Sumber: literasidigital.id



Gambar VI.7

Infografis “Pelecehan *Online*”

Sumber: IDN Times (2017, Juli 18)

**Kelima, penipuan.** Kemudahan mengakses informasi menggunakan media digital juga memudahkan seseorang melakukan tindak penipuan atau terjebak dalam kasus penipuan. Apalagi belakangan ini aktivitas penggunaan media secara daring juga meningkat. Sepanjang 2019, Direktorat Tindak Pidana Siber Bareskrim mencatat 1.617 kasus penipuan secara daring. Rinciannya, sebanyak 534 kasus terjadi di Instagram, 413 kasus di WhatsApp dan sisanya 304 kasus terjadi di Facebook (liputan6). Umumnya modus yang digunakan adalah dengan memberikan penawaran yang mengatasnamakan perusahaan ataupun perorangan, dengan iming-iming hadiah baik berupa uang maupun jasa lainnya. Jika tidak waspada maka kita akan terjebak dan mengambil penawaran tersebut. Seperti kasus yang menimpa hampir 400 orang yang tergiur lelang sepatu merek tertentu di Instagram. Pelaku setelah melakukan lelang, selanjutnya meminta pemenang lelang untuk mengirim uang, tetapi sepatu tadi tidak dikirimkan kepada pemenang (Wamad, 2021). Gambar berikut ini dapat membantu kita untuk berhati-hati terutama bertransaksi secara daring.



Gambar VI.8

Infografis “Ini Cara Pencuri *Online* Zaman Now”

Sumber: liputan6.com (2017, November 18)

**Keenam, kekerasan.** Kekerasan dapat diartikan sebagai tindakan spontan emosional dari sebagian individu dan kelompok yang marah karena terpengaruh isu yang berlanjut menjelma menjadi tindak kekerasan (Hufad, 2003). Konten kekerasan mudah dijumpai di dunia digital. Data yang ditunjukkan pakar media Sonia Livingston menyimpulkan bahwa 1 dari 3 anak melihat muatan kekerasan dan kebencian secara daring. Hal ini menunjukkan bahwa potensi anak untuk terpengaruh konten media sangat besar. Salah satu penyebab kekerasan melalui media digital adalah melalui *game*. Kemudahan seseorang untuk mengakses berbagai bentuk *game* secara daring, sangat didukung oleh teknologi saat ini.



Berbagai konten *game* yang ditawarkan, tidak hanya bersifat positif tetapi banyak juga yang bersifat negatif. Konten *game* yang bersifat negatif tentu memiliki dampak negatif juga seperti pornografi, perilaku menyimpang, kekerasan dan perjudian. Adanya Peraturan Menteri Komunikasi dan Informatika No. 11 Tahun 2016 mengenai Klasifikasi Permainan Interaktif Elektronik dianggap belum cukup mampu dalam mengatasi dampak negatif *game* terhadap para pemainnya. Sebagai contoh, seorang gadis berusia 15 tahun tega membunuh seorang anak berusia lima tahun, dengan alasan karena terpengaruh film dan *game* (Mutmainah, 2020).



Gambar VI.9

Infografis “Anak & Kekerasan Digital”

Sumber: akurat.co (2020, Maret 10)

**Ketujuh, kecanduan.** Gawai saat ini menjadi salah satu alat yang wajib dibawa kemana-mana. Banyak hal yang dapat diselesaikan melalui gawai, karena dengan sekali klik kita bisa mendapatkan apa yang diinginkan. Kemudahan inilah yang membuat kita tidak bisa dipisahkan dari gawai, karena ada orang yang bisa lupa bawa uang tetapi tidak melupakan gawainya. Ketergantungan akan gawai dengan segala kemudahan yang ditawarkan pada akhirnya menimbulkan kecanduan. Ada yang kecanduan belanja, kecanduan main *game*, kecanduan menggunakan aplikasi TikTok, kecanduan berselancar di media sosial dan sebagainya. Sindrom kecanduan gawai ini dinamakan *nomophobia* yang berasal dari istilah "*no-mobile-phone-phobia*". Seperti yang dialami oleh seorang pemuda yang nekat mencuri karena tidak memiliki uang untuk bermain *game* secara daring (pontianak.kompas.com). untuk lebih jelasnya, kita bisa lihat infografis berikut yang menginformasikan mengenai beberapa tipe anak-anak yang kecanduan pada gawai.



Gambar VI.10

Infografis “Tipe-Tipe Kecanduan Gadget pada Anak”

Sumber: detik.com (2016, Oktober 31)

Beberapa aspek-aspek keselamatan anak terutama di dunia digital harus menjadi perhatian kita bersama baik sebagai orang tua, guru maupun pendamping anak dan pegiat literasi digital yang tertarik pada isu anak. Terutama karena anak-anak biasanya hanya tahu menggunakan tanpa tahu dampak lanjutan dari penggunaannya.

### **MENCEGAH DAN MENGATASI ANCAMAN KESELAMATAN ANAK MELALUI MEDIA DIGITAL**

Anak-anak di bawah umur adalah anak-anak yang masih berada dalam pengawasan orang tua. Secara umum, definisi anak-anak dilekatkan pada anak-anak yang berusia 0 hingga 18 tahun. Pada rentang usia ini, menurut Potter (2008) dalam Herlina dkk (2018), seorang anak sedang berada pada masa pertumbuhannya, baik secara fisik, kognitif, maupun moral. Artinya, seorang anak dinilai belum memiliki kemampuan untuk membentengi diri dari berbagai efek buruk, termasuk dalam mengonsumsi pesan yang disiarkan melalui berbagai media. Kondisi tersebut juga membuat anak menjadi khalayak yang paling berisiko terpapar dampak negatif penggunaan media termasuk media digital karena mereka belum sepenuhnya mempunyai keterampilan berpikir kritis.

Sebagaimana yang sudah disinggung sebelumnya di bagian awal bab ini, pengalaman anak-anak berhadapan dengan layar gawai, komputer, laptop dan berbagai perangkat yang terhubung dengan jaringan internet terutama di masa pandemi COVID-19 seperti sekarang ini sangatlah tinggi. Untuk itu, kita perlu mengalihkan perhatian mereka dari perangkat-perangkat tadi atau istilahnya kita melakukan diet gawai untuk anak-anak. Lalu, apa yang perlu kita lakukan?

Upaya yang paling awal yang bisa dilakukan adalah menanamkan tiga nilai penting dalam menggunakan media digital, yakni pertama, mengembangkan kreativitas di era digital melalui berbagai pengalaman menggunakan media digital. Pengalaman itu meliputi keterampilan mengolah kata, suara, angka, gambar, dan sebagainya. Pengalaman juga didapat melalui pengenalan berbagai bentuk media digital seperti website, media sosial, piranti lunak, dan aplikasi layanan. Kemampuan dan kreativitas untuk menjelajahi berbagai sudut dan potensi media digital sangat penting dalam menunjang kehidupan generasi di masa depan. Kedua, kolaborasi, yakni nilai yang dibawa oleh media digital karena

cakupannya yang nyaris tak terbatas, dari sisi isi maupun penggunaannya. Media digital memungkinkan kita untuk berkomunikasi dan berinteraksi dengan banyak orang dengan mudah. Agar tak tersesat, anak-anak perlu belajar berinteraksi dan bekerjasama dengan orang dari beragam latar belakang budaya dan keterampilan. Oleh karena itu keterampilan berkomunikasi, bernegosiasi, menghargai pendapat orang lain, hingga membagi tugas harus dikuasai oleh anak. Orang tua perlu merancang kegiatan di luar sekolah yang tidak berfokus pada kompetisi tapi kolaborasi untuk mengembangkan kemampuan ini. Ketiga, kritis dalam berpikir penting diajarkan pada anak-anak. Mereka menghadapi media digital yang memuat berbagai konten dan pesan dari seluruh penjuru dunia dengan nilai-nilai yang berbeda. Maka setiap keluarga perlu menanamkan nilai-nilai kehidupan yang diafirmasi setiap keluarga pada anak-anaknya. Jika hal itu berhasil dilakukan orang tua maka anak-anak akan mengembangkan pola pikir dan sikap kritis dalam bermedia dan mampu memanfaatkan fasilitas media yang serba canggih untuk kegiatan-kegiatan positif (Herlina dkk, 2018)





Gambar VI.11

Infografis “Dampingi Anak dalam Dunia Digital”

Sumber: literasidigital.id

Selain ketiga hal di atas, kita juga harus memiliki kompetensi yang memadai dalam mengarahkan anak-anak sehingga dapat mencegah mereka menjadi pelaku atau korban dari penggunaan media digital. Kompetensi sendiri diartikan sebagai kemampuan seseorang dalam melakukan sesuatu. Kompetensi dapat dipelajari dan dikuasai oleh individu. Kompetensi juga merupakan keterampilan yang bertahap dan penguasaan kompetensi yang

lebih mendasar diperlukan untuk menguasai kompetensi selanjutnya. Merujuk pada hal di atas, maka ada beberapa kompetensi yang perlu diketahui dan diajarkan kepada anak dalam upaya mencegah dan mengatasi ketika terjadi situasi yang mengancam keselamatan, yakni:

### **Mengakses media digital**

Kemampuan mengakses media digital perlu ditanamkan sejak awal, sebagai pedoman bagi anak-anak saat mereka menggunakan media digital tersebut. Kemampuan mengakses ini tidak terbatas pada keterampilan teknis saat mereka berinteraksi dengan media digital, melainkan juga cara mereka memperoleh dan menyebarkan informasi. Kita memiliki kewajiban untuk memberikan pemahaman kepada anak-anak, informasi seperti apa yang layak untuk dicari dan layak untuk disebarluaskan. Jika memungkinkan, ada pembatasan dalam penggunaan media digital pada anak. Hal lain yang juga dapat kita lakukan adalah dengan menutup beberapa konten atau laman yang tidak sesuai dengan kebutuhan anak

Beberapa tips yang dapat kita terapkan untuk meningkatkan kemampuan dalam mengakses media digital adalah:

**Pertama, kemampuan memilih media sosial** – mendampingi anak-anak saat mereka baru memulai mencoba menggunakan media sosial adalah keputusan yang bijak. Pilihlah media sosial yang cocok dengan usia dan kebutuhannya. Jika anak-anak sudah memiliki media sosial, kita perlu mendampingi mereka untuk memastikan bahwa media sosial yang telah dipilih memang benar-benar sesuai dengan usia dan kebutuhannya. Mintalah anak-anak untuk sedapat mungkin mematuhi kebijakan yang dikeluarkan oleh masing-masing media sosial sebagai syarat bagi para penggunanya demikian pula dengan berbagai perubahan dalam layanan yang diberikan. Gambar berikut ini bisa kita gunakan untuk memberikan pemahaman kepada anak-anak berkaitan dengan karakteristik dari media sosial.

## Karakteristik Media Sosial



Gambar VI.12

### Karakteristik Media Sosial

Sumber: Banyumurtui (2019, Juli 12)

**Kedua, kemampuan menyaring informasi** – beragam informasi dapat dengan mudah diperoleh sekaligus dibagikan secara daring. Tugas kita di sini adalah mengajarkan kepada anak-anak cara untuk mendeteksi dan menyaring informasi yang layak diterima. Lalu, seperti apa informasi yang layak diterima itu? Informasi yang layak diterima adalah informasi yang berasal dari sumber yang kredibel, sumber yang dapat dipercaya. Selain itu kita juga perlu menanamkan nilai-nilai kekerasan dan pornografi sehingga mereka dapat menolak konten sejenis itu yang tiba-tiba muncul saat mengakses media digital. Berikut beberapa tips yang dapat kita gunakan untuk mencegah anak-anak terpapar konten negatif terutama pornografi.



Gambar VI.13

Poster Digital “10 Tips Cegah Anak Terpapar Pornografi”

Sumber: literasidigital.id

**Ketiga, kemampuan mengatur waktu.** Kemampuan mengakses media digital perlu kita imbangi dengan kemampuan mengatur waktu penggunaan. Oleh karena itu kita perlu memastikan bahwa waktu penggunaan media digital tidak mengganggu aktivitas penting sehari-hari anak-anak seperti belajar, beristirahat, beribadah, berinteraksi langsung dengan keluarga dan lainnya. Pastikan anak-anak bisa membagi waktu tersebut dengan baik, salah

satu yang dapat dilakukan adalah membuat kesepakatan berapa lama waktu yang dapat digunakan dan kapan mereka bisa mengakses media digital.

### **Mendistribusi informasi melalui media digital**

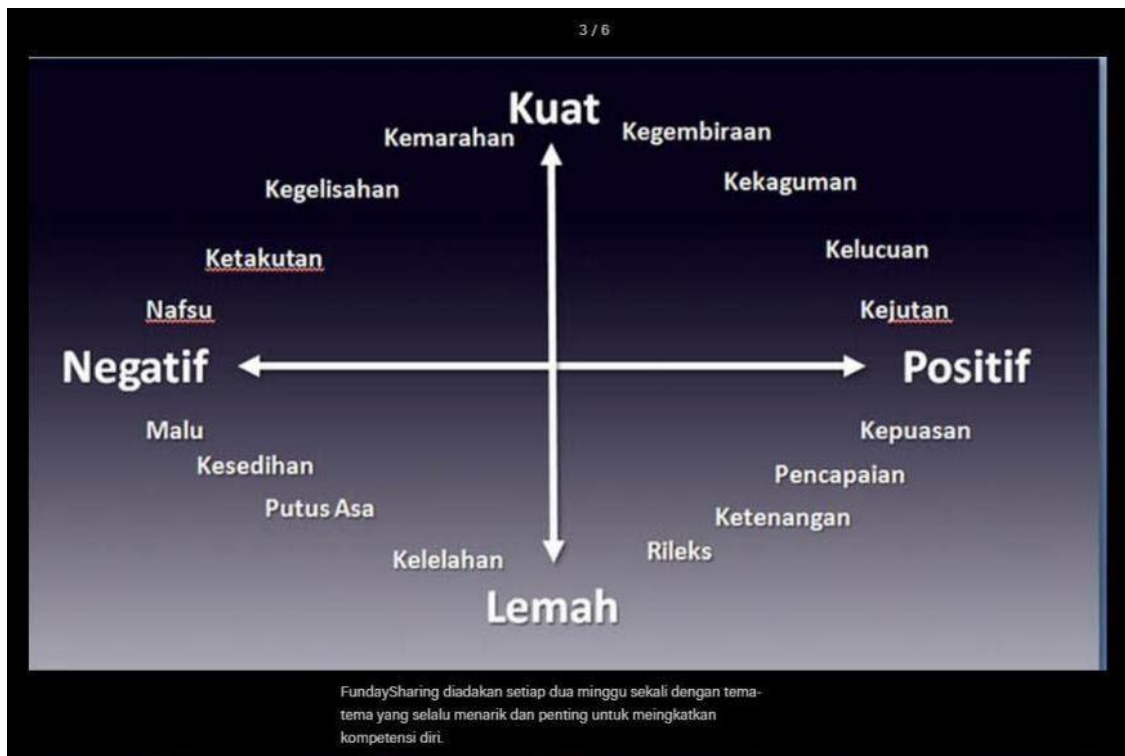
Kemampuan mendistribusi berbagai informasi juga perlu dilakukan, karena biasanya kesalahan dalam mendistribusi inilah yang menjadi salah satu sumber ancaman keselamatan anak-anak di dunia digital. Anak-anak perlu kita ajarkan untuk tidak dengan gegabah mendistribusikan informasi terutama informasi pribadi melalui media digital baik berupa tulisan, gambar maupun video. Disamping itu, kita juga perlu memberikan pemahaman mengenai cara-cara menyampaikan pesan dengan baik. Karena seringkali maksud baik ditanggapi keliru karena cara penyampaian yang kurang tepat.

Beberapa tips yang dapat kita terapkan untuk meningkatkan kemampuan dalam mendistribusikan informasi melalui media digital adalah:

**Pertama, kemampuan membagi informasi.** Pemahaman bahwa tidak setiap informasi yang kita peroleh, harus dibagikan kepada orang lain perlu diberikan sejak awal kepada anak-anak. Biasakan anak-anak untuk membaca dan memahami terlebih dahulu seluruh informasi yang diperoleh. Mintalah anak-anak untuk terlebih dahulu mempertimbangkan apakah informasi tersebut dapat dibagikan kepada orang lain, atau berhenti sampai diri sendiri. Pertimbangkan juga apakah informasi yang akan kita bagikan itu adalah informasi yang valid, yang dapat dipercaya sumbernya. Salah satu yang bisa kita jadikan sebagai pertimbangan adalah manfaat dari informasi tadi, jika bermanfaat maka bisa dibagikan, tetapi kalau tidak, sebaiknya tidak perlu dibagikan.

**Kedua, kemampuan mengemas informasi.** Berbagai informasi yang kita peroleh melalui media digital tidak sepenuhnya dapat dipercaya, karena ada beberapa informasi yang sifatnya hoaks. Anak-anak juga perlu dibekali dengan kemampuan mengolah informasi yang ingin mereka bagikan, seperti pemilihan bahasa atau kata-kata, pemilihan gambar atau foto. Karena kemasan pesan juga menjadi salah satu hal yang perlu diperhatikan sebelum mereka membagikannya. Gaya penyampaian ini bisa berupa pilihan atas informasi atau data yang ingin ditekankan, visualisasi penyerta informasi serta penyesuaian dengan karakter media

sosial yang digunakan. Sedangkan bahasa berkaitan dengan pilihan kata dan hubungan antarparagraf yang membentuk keseluruhan makna pesan. Dengan demikian, distribusi konten yang dilakukan dapat menarik perhatian warganet lainnya guna mendukung tercapainya tujuan yang diinginkan. Gambar berikut merupakan salah satu cara yang dapat membantu kita mengemas informasi yang dapat membawa dampak positif bagi mereka yang menerimanya.



Gambar VI.14

Tips Membuat Konten yang Populer

Sumber: liputan6.com (2014, November 06)

Ketiga, Kemampuan mengenal teman dan lingkungan, ketika kita ingin mendistribusikan pesan kepada orang lain melalui media digital, sebaiknya juga perlu mengenal siapa saja teman yang akan menerimanya. Dengan mengetahui siapa penerima pesan maka akan meminimalisir kesalahan dalam pengemasan pesan, karena beda penerima pesan maka beda juga cara pesan dikemas. Selain perlu mengetahui siapa penerima pesan, perlu juga mengetahui di lingkungan seperti apa pesan tersebut akan kita sebar. Jangan sampai,

setelah kita membagikan pesan tersebut, ternyata respon yang kita terima tidak seperti yang kita harapkan.

### **Partisipasi terkait media digital**

Berpartisipasi dalam dunia digital berarti bersama-sama turut dalam menyampaikan berbagai informasi berkaitan dengan aspek keselamatan pengguna media digital itu sendiri. Membagikan informasi berkaitan dengan aspek-aspek kekerasan yang bisa muncul yang dapat mengancam keselamatan diri sendiri maupun orang lain, proaktif mengingatkan teman-teman sebaya agar berhati-hati ketika menggunakan media digital, aktif menolak perilaku perundungan, pelecehan, penipuan sebagainya merupakan beberapa hal terkait kemampuan berpartisipasi. Beberapa tips yang dapat kita terapkan untuk meningkatkan kemampuan dalam partisipasi terkait media digital adalah:

**Pertama, kemampuan menyampaikan informasi yang baik dan etis.** Kemudahan berbagi informasi juga perlu didukung dengan kemampuan memberi masukan secara konstruktif atas pendapat orang lainnya dalam *platform* tertentu. Kemampuan dalam menyampaikan informasi seperti berkomentar menanggapi informasi orang lain, perlu kita lakukan dengan baik dan etis. Salah satunya dengan cara menyertakan tautan berita yang benar untuk memperkuat bukti berita yang kita bagikan. Sebab, walaupun kita tidak berhadapan secara langsung dengan lawan bicara, namun ada etika yang perlu dipatuhi oleh pengguna media digital.

**Kedua, kemampuan menggunakan media digital secara produktif.** Selain saling berbagi informasi, anak-anak bisa kita dorong untuk menggunakan media digital untuk hal-hal yang sifatnya produktif, seperti belajar bahasa, melukis atau menggambar, belajar berbagai kerajinan tangan, memasak, merakit robot hingga keterampilan mengolah data. Jika sejak dini anak-anak sudah kita ajak untuk memanfaatkan media digital secara efektif, maka kelak mereka akan memiliki pengetahuan dan keterampilan yang bisa dimanfaatkan untuk masa depan.

**Ketiga, kemampuan melaporkan pelanggaran dalam penggunaan media digital.** Kita perlu mengajarkan anak-anak untuk berani melaporkan berbagai pelanggaran yang mereka



jumpai atau bahkan alami selama menggunakan media digital. Pemerintah dalam hal ini Kementerian Komunikasi dan Informasi sudah menyediakan sistem aduan terkait konten-konten negatif tersebut. Ada 12 kategori konten negatif yang bisa dilaporkan, yakni pornografi/pornografi anak, perjudian, pemerasan, penipuan, kekerasan/kekerasan anak, fitnah/pencemaran nama baik, pelanggaran kekayaan intelektual, produk dengan aturan khusus, provokasi SARA, berita bohong, terorisme/radikalisme, dan informasi/dokumen elektronik melanggar UU (kominfo.go.id)



Gambar VI.15

Poster Digital “Konten Aduan Kominfo”

Sumber: twitter.com

**Keempat, kemampuan berkata ‘tidak’ terhadap ajakan negatif.** Walaupun kelompok anak-anak merupakan kelompok yang belum sepenuhnya mampu berpikir kritis, namun kita perlu memberikan pemahaman mengenai apa yang boleh dan apa yang tidak boleh dilakukan dengan menggunakan media digital. Kita perlu mengajarkan kepada anak-anak agar mampu berkata ‘tidak’ terhadap berbagai ajakan yang bersifat negatif yang nantinya akan menimbulkan ancaman kekerasan terhadap diri mereka.



### **Kolaborasi melalui media digital**

Kemampuan kolaborasi merupakan kemampuan yang unik, karena dimulai dari diri sendiri. Berkolaborasi melalui media digital artinya bekerja sama dengan banyak pihak untuk menghasilkan konten yang sifatnya positif. Sehingga kemampuan kolaborasi tidak saja berguna bagi individu tetapi juga berguna secara kolektif. Anak-anak bisa memulainya dengan selalu saling mengingatkan diantara mereka agar bisa terhindar dari terpaan konten-konten negatif. Bisa juga dengan bergabung dalam suatu forum atau komunitas di mana di dalamnya mereka bisa merancang konten-konten kreatif sendiri untuk mereka bagikan kepada anak-anak seusia. Beberapa tips yang dapat kita terapkan untuk meningkatkan kemampuan dalam melakukan kolaborasi melalui media digital adalah:

**Pertama, kemampuan untuk bergabung dalam forum atau komunitas.** Adalah tugas kita sebagai orangtua, guru, pendamping anak atau pegiat untuk mengajak anak-anak agar mau bergabung dalam salah satu komunitas yang sesuai dengan keinginan mereka. Melalui komunitas yang dipilih itu, diharapkan anak-anak bisa mengasah keterampilan dan kemampuan mereka. Misalnya, jika mereka ingin agar hak anak itu diperhatikan maka salah satu wadah yang menyediakannya adalah Forum Anak Nasional (FAN). FAN adalah sebuah organisasi anak yang dibina oleh Pemerintah Republik Indonesia, melalui Kementerian Pemberdayaan Perempuan dan Perlindungan Anak. Anak-anak yang tergabung dalam forum ini bisa bebas berekspresi, berkomunikasi dan berinteraksi dalam rangka pemenuhan hak partisipasi anak.



Gambar VI.16

Laman Depan Situs “Forum Anak Nasional”

Sumber: [forumanak.id](http://forumanak.id)

**Kedua, kemampuan menciptakan pertemanan.** Media digital memudahkan kita untuk kembali menjalin hubungan dengan teman-teman lama atau saudara yang sudah lama tidak berjumpa. Media digital juga bisa menjadi tempat untuk mendapatkan teman baru, teman yang bisa saja memiliki pandangan yang sama dengan kita mengenai suatu topik. Anak-anak bisa mencoba untuk persoalan yang berada di sekitar mereka dan memberi solusi nyata dengan berkolaborasi bersama teman-temannya, misalnya menggalang dana untuk anak-anak yang kurang mampu. Tentu saja, kolaborasi ini perlu didampingi oleh orangtua atau pendamping anak.



Gambar VI.17

Laman Depan Situs “Sahabat Anak”

Sumber: [sahabatanak.org](http://sahabatanak.org)

Selanjutnya, mari kita cermati contoh kasus berikut ini.

Kasat Reskrim Polres Bogor, Ajun Komisaris Benny Cahyadi mengatakan bahwa duel ala gladiator itu **bermula karena saling ejek di media sosial Facebook (FB)** kemudian berlanjut hingga janji untuk berkelahi pada Kamis 14 Maret 2019 malam. **"Iya di FB, keduanya AH dan MR saling ejek sehingga berkelahi didampingi masing-masing kelompok,"** katanya di Mapolres Bogor, Senin (18/3/2019). **"Ini bukan tawuran tapi lebih ke individu dan mereka tidak saling mengenal,"** tambahnya. Atas perbuatannya, MR akan **dikenakan Pasal 80 ayat 3 UU No 35/2014 perubahan atas UU No 23/2002, tentang Perlindungan Anak dan atau Pasal 184 ayat 4 KUHP dengan ancaman pidana penjara 15 tahun** (sumber: [kompas.com](http://kompas.com))

Berita di atas merupakan kutipan berita yang dimuat di [kompas.com](http://kompas.com) tanggal 18 Maret 2019. Penulis sengaja memberikan penekanan dengan menebalkan beberapa kalimat untuk menunjukkan salah satu dari 4 kemampuan yang sudah dikemukakan sebelumnya. Kemampuan yang dimaksud adalah kemampuan mendistribusikan pesan. Dari berita tersebut kita bisa belajar bahwa pertama, tidak semua orang suka dengan pesan yang kita

bagikan apalagi jika pesan tersebut berupa ejekan; kedua, tidak semua orang di media sosial itu kita kenal dengan baik bahkan ada yang tidak kita kenal sama sekali; ketiga, ketika kita emosional menanggapi suatu pesan, hal buruk akan terjadi; dan keempat, konsekuensi hukum atas tindakan gegabah sudah menunggu. Sehingga sekali lagi, berhati-hatilah dalam menggunakan media digital. Kuasailah minimal 4 kemampuan tersebut (akses, distribusi, partisipasi dan kolaborasi) agar kita aman bermedia digital.

## SARAN DAN REKOMENDASI LITERASI KEAMANAN DIGITAL

Tidak dipungkiri bahwa kehadiran media digital membawa perubahan baik positif maupun negatif dalam kehidupan kita sehari-hari. Kemampuan para pengguna, termasuk anak-anak, dalam mengoperasikan dan kepatuhan mereka akan aturan bermedia digital menjadi salah tuntutan yang tidak tertulis. Kita memahami bahwa anak-anak lebih cepat mengetahui perkembangan teknologi namun itu bukan berarti mereka juga memahami cara menggunakan teknologi tersebut dengan baik. Untuk itulah pendampingan tetap kita berikan kepada anak-anak agar mereka bisa terhindar dari berbagai aspek ancaman keselamatan dalam penggunaan media digital. Selain itu, peningkatan kompetensi literasi digital pada anak-anak juga harus terus dilakukan, terutama berkaitan dengan kompetensi mengakses, kompetensi mendistribusi, kompetensi partisipasi dan kompetensi kolaborasi.

Anak-anak sebagai pengguna media digital perlu kita beri pemahaman mengenai berbagai ancaman keselamatan yang mengintai saat mereka menggunakan media digital. Berikut rekomendasi yang bisa diberikan terkait keamanan digital, khususnya bagi anak-anak.

| Batasi Informasi Pribadi   | Batasi Penggunaan Gawai  | Kenali Ancaman Keselamatan   | Saring Sebelum Sharing  |
|--|--|--|---|
| Ingatkan anak-anak agar tidak gegabah saat memberikan informasi yang sifatnya pribadi ketika berinteraksi di media digital. Berhati-hati ketika berbagai nomor kontak, alamat rumah, sekolah atau informasi lain yang memungkinkan orang-orang yang tidak bertanggungjawab melacaknya. | Beri batasan waktu yang tegas kepada anak-anak saat menggunakan media digital. Dengan adanya pembatasan waktu, dapat meminimalisir berbagai ancaman keselamatan bagi anak-anak | Ajak dan tunjukkan kepada anak-anak berbagai potensi ancaman termasuk modus yang biasa digunakan. Biasakan anak-anak terbuka. Latih anak untuk mengendalikan emosinya dan bila memungkinkan mengalihkan emosi tadi pada kegiatan yang positif. | Pikirkan dengan baik sebelum berbagi pesan, karena sekali tersebar, sulit dihapus. Biasakan anak-anak untuk tidak begitu saja membuka pesan termasuk tautan yang diterima, pastikan dahulu kejelasan pengirimnya. |

Gambar VI.18 Aman Bermedia Digital. Sumber: olahan penulis.

Untuk difabel, kita perlu memperjuangkan kesetaraan dalam penggunaan media digital. Ancaman keselamatan yang paling sering diterima oleh difabel adalah perundungan, sebagaimana tampak pada gambar berikut.



Gambar VI.19

Perundungan Anak Berkebutuhan Khusus

Sumber: tirtod (2017, Juli 17)

Perundungan yang diterima oleh difabel di dunia nyata maupun media digital sama buruknya. Oleh karena itu, berilah motivasi kepada difabel bahwa mereka setara dengan semua orang dalam segala bidang. Kita juga bisa melatih difabel untuk tidak takut bersuara, menceritakan atau melaporkan perlakuan yang kurang menyenangkan yang mereka terima terutama melalui media digital.

Untuk perempuan, kita perlu menyadari bahwa perempuan baik dewasa maupun anak-anak, merupakan kelompok yang paling rentan mendapatkan kekerasan melalui media digital. Perempuan biasanya lebih mengedepankan emosi atau perasaan, apalagi jika sudah berhubungan dengan romantisme atau asmara, sebagaimana contoh pada gambar berikut. Informasi serupa juga dapat dibaca pada Bab IV.



Gambar VI.20 Pola Scammer Love

Sumber: jeyjingga.com (2020, Juli 21)

Oleh karena itu kita perlu memberikan pemahaman bahwa apa yang tampak di media digital tidak selamanya sesuai kenyataan. Kewaspadaan perempuan perlu ditingkatkan saat menerima informasi. Biasakan untuk selalu melakukan pengecekan ketika menerima pesan terutama yang menawarkan sesuatu, terutama terhadap pesan-pesan yang mencurigakan.

Untuk masyarakat di kawasan 3T, kita perlu memberikan sosialisasi mengenai berbagai macam dampak positif dan negatif berkaitan dengan penggunaan media digital. Perlu juga diberikan penekanan pada berbagai aspek ancaman keselamatan bagi penggunanya. Selain itu, kita juga bisa mengadakan berbagai pelatihan untuk meningkatkan keterampilan terutama kemampuan untuk mengakses, mendistribusi, berpartisipasi dan berkolaborasi melalui media digital.

Berdasarkan rekomendasi yang sudah diberikan, maka bab mengenai keamanan anak di platform digital ini masih dapat dikembangkan lagi, terutama berkaitan dengan keselamatan pengguna media digital bagi difabel, perempuan dan masyarakat di Kawasan 3T. Selain pengelompokan khalayak, modul ini juga bisa dikembangkan untuk menyasar keselamatan anak-anak yang didasarkan pada pengelompokan usia (anak, remaja, dewasa). Karena disadari atau tidak, kehadiran teknologi digital juga menyentuh mereka sehingga perlu ada variasi literasi digital terkait perlindungan keamanan digital yang khusus ditujukan kepada kelompok-kelompok tersebut.

Tabel VI.1

Matriks rekomendasi program literasi digital  
untuk meningkatkan kecakapan keamanan digital

| <b>Aspek/<br/>Khalayak<br/>Sasaran</b>      | <b>Anak dan<br/>Remaja</b>                            | <b>Perempuan</b>  | <b>Lansia</b>                                     | <b>3T</b>                                    | <b>Difabel</b>                              |
|---|---|---|---|--|---|
| <b>Keselamatan<br/>di Media<br/>Digital</b> | Program formal menambahkan materi tentang keselamatan | Pelatihan pada komunitas perempuan yang bisa dilanjutkan dengan | Pembuatan konten dengan bahasa dan ilustrasi yang | Pembuatan konten yang mudah dipahami tentang | Pembuatan konten sederhana melalui beberapa |

|   |  |  |  |   |   |
|---|--|--|--|---|---|
|   | dalam penggunaan media digital dalam kegiatan belajar mengajar khususnya TIK di sekolah  | diskusi dan studi kasus  | sederhana yang mudah dipahami oleh lansia  | keselamatan di media digital dilengkapi dengan gambar yang menarik  | media yang disesuaikan dengan kebutuhan difabel   |
|   | Program informal dengan menambahkan materi terkait keselamatan dalam penggunaan media digital dalam kegiatan ekstrakurikuler terkait TIK   | Pelatihan informal pada komunitas perempuan yang bisa dilanjutkan dengan diskusi dan studi kasus | Program sosialisasi yang kontennya disesuaikan dengan kebutuhan lansia dengan bahasa dan ilustrasi yang sederhana yang mudah | Program diskusi atau sosialisasi yang melibatkan tokoh masyarakat dan tokoh agama                               | Program diskusi yang dilengkapi contoh kasus disesuaikan dengan kebutuhan difabel           |
| <b>Mencegah dan Mengatasi Ancaman Kekerasan Melalui Media Digital</b> | Program formal menambahkan materi tentang ancaman kekerasan melalui media digital dalam kegiatan belajar mengajar khususnya TIK di sekolah | Pelatihan pada komunitas perempuan yang bisa dilanjutkan dengan diskusi dan studi kasus          | Pembuatan konten dengan bahasa dan ilustrasi yang sederhana yang mudah dipahami oleh lansia                                  | Pembuatan konten yang mudah dipahami tentang keselamatan di media digital dilengkapi dengan gambar yang menarik | Pembuatan konten sederhana melalui beberapa media yang disesuaikan dengan kebutuhan difabel |



|  |   |  |  |   |   |
|--|---|--|--|---|---|
|  |   |  |  |   |   |
|  | Program informal dengan menambahkan materi terkait ancaman kekerasan melalui media digital dalam kegiatan ekstrakurikuler terkait TIK | Pelatihan informal pada komunitas perempuan yang bisa dilanjutkan dengan diskusi dan studi kasus | Program sosialisasi yang kontennya disesuaikan dengan kebutuhan lansia dengan bahasa dan ilustrasi yang sederhana yang mudah | Program diskusi atau sosialisasi yang melibatkan tokoh masyarakat dan tokoh agama | Program diskusi yang dilengkapi contoh kasus disesuaikan dengan kebutuhan difabel |

### EVALUASI KOMPETENSI MENGENALI DAN MENINGKATKAN KEAMANAN DIGITAL

Setelah menyelesaikan modul ini, kita diharapkan memiliki kemampuan untuk mengetahui, mengenali dan menerapkan keamanan digital terutama bagi anak-anak. Dengan kata lain, ada tiga aspek yang hendak disasar dalam evaluasi ini yakni berkaitan dengan aspek kognitif, afektif dan konatif. Untuk lebih jelaskan dapat dilihat pada table VI.1 berikut ini.

Tabel VI.2

Evaluasi Kemampuan Mengenali dan Meningkatkan Keamanan Digital

| No | Keamanan Anak di Platform Digital       | Domain Evaluasi  |  |   |
|----|---|--|--|---|
|    |   | Kognitif   | Afektif  | Konatif   |
| 1  | Aspek keselamatan anak di media digital | Mengetahui dan mengenali berbagai aspek keselamatan di media digital | Mampu menilai berbagai aspek keselamatan anak di media digital | Menerapkan kesadaran terhadap keselamatan anak di media digital |
| 2. | Mencegah dan                            | Memahami cara  | Menyadari  | Mempraktikkan   |

|  |   |   |  |  |
|--|---|---|--|--|
|  | mengatasi ancaman keselamatan anak di melalui media digital | mencegah dan mengatasi ancaman keselamatan anak melalui media digital | pentingnya mencegah dan mengatasi ancaman keselamatan anak melalui media digital | kesadaran keamanan digital terkait upaya mencegah dan mengatasi keselamatan anak melalui media digital |
|--|---|---|--|--|

### CONTOH INSTRUMEN EVALUASI

Untuk menguji pemahaman berkaitan dengan keamanan anak di platform digital, maka salah satu contoh instrumen evaluasi (kegiatan) yang dilakukan adalah berkaitan dengan mencegah dan mengatasi ancaman keselamatan anak di bawah umur dalam penggunaan media digital, dilihat dari aspek konatif. Dalam bab ini, telah diuraikan mengenai beberapa aspek keselamatan digital yang dihadapi ketika kita menggunakan media digital. Peserta diminta menceritakan pengalamannya berkaitan aspek-aspek keselamatan tersebut. Selanjutnya peserta memberikan caranya mencegah dan mengatasi kondisi yang dialaminya tersebut.

Ingat, bahwa cara kita memperlakukan orang lain di dunia digital merupakan gambaran cara yang sama kita memperlakukan orang lain di dunia nyata.

### DAFTAR PUSTAKA

- Bailey, Diane. (2008). *Cyber ethics: Cyber citizenship & cyber safety*. The Rosen Publishing Grup Inc.
- Banyumurti, I. (2019, Juli 12). Materi untuk tot literasi digital untuk guru, bagian li dari 4 serial. Diperoleh dari <https://www.slideshare.net/banyumurti/materi-1-tot-literasi-digital-internet-media-sosial-dan-literasi-digital>
- Cipta, H. (2020, Agustus 03). Kecanduan game online, remaja 18 tahun nekad curi sepeda di tengah keramaian. *Kompas.com*. Diperoleh dari <https://pontianak.kompas.com/read/2020/08/03/14153731/kecanduan-game-online-remaja-18-tahun-nekat-curi-sepeda-di-tengah-keramaian?page=all>

- Femina.co.id. (2017, Oktober 13). Infografis: Ini jenis hinaan dan kata-kata yang sering digunakan oleh para pelaku bullying media sosial. *Femina.co.id*. Diperoleh dari <https://www.femina.co.id/trending-topic/infografis-ini-jenis-hinaan-dan-kata-kata-yang-sering-digunakan-oleh-para-pelaku-bullying-di-media-sosial>
- Forum Anak Nasional. Tangkapan Layar Laman *forumanak.id*. Diperoleh dari <https://forumanak.id>
- Herlina, D., Benni, S., & Gilang J.A. (2018). *Digital parenting: Mendidik anak di era digital*. Yogyakarta: Samudra Biru.
- Hidayatulloh, T. (2018, April 05). Infografis: Magang palsu di luar negeri jadi modus baru eksploitasi anak. *Akurat.co*. Diperoleh dari <https://akurat.co/id-189011-read-magang-palsu-di-luar-negeri-jadi-modus-baru-eksploitasi-anak>
- Hufad, A. (2003). Perilaku kekerasan: Analisis menurut sistem budaya dan implikasi edukatif. *Jurnal Mimbar Pendidikan*, No. 2/XXII/2003.
- IDN Times. (2017, Juli 18). (Infografis) Pelecehan online, sisi gelap perkembangan internet. *Idntimes.com*. Diperoleh dari <https://www.idntimes.com/news/world/rosa-folia/infografis-menimbang-perkara-pelecehan-online-1>
- Ikhsan, A. (2019, Maret 18). Saling ejek di media sosial berujung maut, satu pelajar tewas. *Kompas.com*. Diperoleh dari <https://bogor.kompas.com/read/2019/03/18/12272721/saling-ejek-di-media-sosial-berujung-maut-satu-pelajar-tewas>
- Indonesia.go.id. (2019, Januari 22). Tangkapan layar laman indonesia.go.id. Diperoleh dari <http://indonesiabaik.id/infografis/pengguna-media-sosial-di-indonesia-19>
- Jeyjingga. (2020, Juli 21). Scammer love. 10 fakta cinta dalam dunia maya. Diperoleh dari <https://jeyjingga.com/scammer-love-cinta-dalam-dunia-maya/>
- Liputan6.com. (2014, November 06). 6 tips membuat konten yang populer. *Liputan6.com*. Diperoleh dari <https://www.liputan6.com/citizen6/read/2129929/6-tips-membuat-konten-yang-populer>
- Literasidigital.id. Tangkapan layar infografis dari laman literasidigital.id. Diperoleh dari <http://literasidigital.id/infografis-literasi-digital/>
- Maria, S. Y. N. (2017, November 18). (Cek fakta) Maling zaman now incar transaksi online. *Liputan6.com*. Diperoleh dari <https://www.liputan6.com/cek-fakta/read/3289267/cek-fakta-maling-zaman-now-incar-transaksi-online>

- Monggilo, Z.M.Z, Novi, K., & Indriyatno, B. (2020). Panduan literasi media digital dan keamanan siber: Muda, kreatif dan tangguh di ruang siber. Direktorat Pengendalian Informasi, Investigasi dan Forensik Digital, Badan Siber dan Sandi Negara.
- Mutmainah, N. (2020, Maret 18). Melindungi anak-anak dan remaja dari kekerasan di media. Diperoleh dari <https://theconversation.com/melindungi-anak-anak-dan-remaja-dari-kekerasan-di-media-133794>
- Nurdiani, I.P. (2020, November). Pencurian identitas digital sebagai bentuk cyber related crime. *Jurnal Kriminologi Indonesia*, Vol.16 No.2.
- Putra, D.I. & Garuda, G. (2017, Juli). Perancangan aplikasi penyandian data text menggunakan metode symmetric stream cipher. *Jurnal Pelita Informatika*, Vol.6 No.1.
- Ramadhan, A.S. (2020, Desember 02). Waspada! Ada ancaman kekerasan seksual baru berbasis online. *Jabar.suara.com*. Diperoleh dari <https://jabar.suara.com/read/2020/12/02/153202/waspada-ada-ancaman-kekerasan-seksual-baru-berbasis-online?page=all>
- Ramadhani, P.I. (2020, September 29). Bareskrim catat ada 1.617 kasus penipuan online pada 2019, paling banyak di instagram. *Liputan6.com*. Diperoleh dari <https://www.liputan6.com/bisnis/read/4369038/bareskrim-catat-ada-1617-kasus-penipuan-online-pada-2019-paling-banyak-di-instagram>
- Rinanda, H. M. (2018, Oktober 09). Perdagangan anak via medsos dibongkar, 1 anak dijual Rrp. 22 juta. Diperoleh dari <https://news.detik.com/berita-jawa-timur/d-4249465/perdagangan-anak-via-medsos-dibongkar-1-anak-dijual--rp-22-juta>
- Robota.co.id. Tangkapan layar dari laman *robota.co.id*. Diperoleh dari <http://robota.co.id/kursus-robotik>
- Sahabat Anak. Tangkapan layar dari laman *sahabatanak.org*. Diperoleh dari <https://sahabatanak.org>
- Sammons, J., & Michael, C. (2017). *The basic of cyber safety: Computer and mobile device safety made easy*. Elsevier. Inc
- Samsoerizal, D. (2020, Agustus 24). Kasus Zara: UU pornografi, moralitas dan budaya cyberbullying. *Insertlive*. Diperoleh dari <https://www.insertlive.com/hot-gossip/20200824132046-7-158339/kasus-zara-uu-pornografi-moralitas-dan-budaya-cyberbullying>

- Saputro, F. A. & Nugroho, A. S. (2020, September 02). Ada harapan RI segera punya UU perlindungan data pribadi. *Republika.co.id*. Diperoleh dari <https://republika.co.id/berita/qg0hk6409/ada-harapan-ri-segera-punya-uu-perindungan-data-pribadi>
- Sulaiman, M. R. (2016, Oktober 31). Infografis: Perlu tahu, tipe-tipe kecanduan gadget yang bisa dialami anak. *Detik.com*. Diperoleh dari <https://health.detik.com/anak-dan-remaja/d-3333597/infografis-perlu-tahu-tipe-tipe-kecanduan-gadget-yang-bisa-dialami-anak>
- Sukmawati, A.I., Al Musa, K., Andri, P.Y., Debby, D.E., Noverti, F.U., & Popi, A. (2019). Yuk, cegah tindak pidana perdagangan orang!. Yogyakarta: Samudra Biru.
- Surono, A. (2020, Maret 10). Infografis: Anak dan kekerasan digital. *Akurat.co*. Diperoleh dari <https://akurat.co/news/id-1040232-read-anak-dan-kekerasan-digital>
- Tirto.id. (2017, Juli 17). Bullying di gunadarma dan hak pendidikan bagi difabel. Diperoleh dari <https://tirto.id/bullying-di-gunadarma-dan-hak-pendidikan-bagi-difabel-csQ8>
- Twitter.com. Tangkapan Layar [twitter.com](https://twitter.com/aduankonten/status/995865135590731776/photo/1) (Foto Twitter). Diperoleh dari <https://twitter.com/aduankonten/status/995865135590731776/photo/1>
- Uajy.ac.id (2017, Desember 07). Media sosial dan anak. Diperoleh dari <http://newslab.uajy.ac.id/2017/12/07/media-sosial-dan-anak/>
- Wijayanto, X.A., Lomria, R.F., & Lestari, N. (2019). Mencegah dan mengatasi bullying di dunia digital. Lembaga Penelitian, Publikasi dan Pengabdian kepada Masyarakat, London School of Public Relations Jakarta
- Yuwono, A.I., Irham, N.A., Rahayu, S., & Wisnu, M.A. (2018). Yuk, jadi gamer cerdas: Berbagi informasi melalui literasi. Program Studi Magister Ilmu Komunikasi, Departemen Ilmu Komunikasi, Universitas Gadjah Mada
- Wamad, S. (2021, Januari 01). 400 orang tertipu pria cirebon yang lelang sepatu via medsos. *Detik.com*. Diperoleh dari [https://news.detik.com/berita-jawa-barat/d-5317556/400-orang-tertipu-pria-cirebon-yang-lelang-sepatu-via-medsos?\\_ga=2.4778618.83269806.1612529609-1882349041.1607901181](https://news.detik.com/berita-jawa-barat/d-5317556/400-orang-tertipu-pria-cirebon-yang-lelang-sepatu-via-medsos?_ga=2.4778618.83269806.1612529609-1882349041.1607901181)
- Winarsih & Irwansyah. (2020). Proteksi privasi big data dalam media sosial. *Jurnal Audience: Jurnal Ilmu Komunikasi*, Vol.3 No.1.

## **BAB VII**

### **TANTANGAN KEAMANAN DIGITAL**

*Gilang Adikara Jiwana & Novi Kurnia*

#### **INTERNET DAN KEAMANAN DIGITAL**

Internet dan media digital lahir dari harapan bahwa dunia maya ini akan membuka dimensi baru yang menghapus sekat ruang dan waktu di dunia nyata. Tujuannya mulia, memberikan kebebasan bagi manusia untuk berkreasi dengan sumber daya yang terjangkau dan meningkatkan kualitas hidup manusia dengan memberikan akses yang luas dan merata bagi setiap penggunanya untuk mencari informasi, memperoleh pengetahuan, dan berkontribusi dengan menghasilkan karya-karya yang dapat dinikmati oleh pengguna digital yang lain.

Namun, suatu penciptaan selalu memiliki dua sisi, peluang dan ancaman. Dalam peluang yang besar untuk berkreasi, lahir pula ancaman dari kebebasan berkreasi dan berekspresi ini. Ancaman-ancaman yang dibuat oleh orang yang tidak bertanggung jawab ini bertujuan memanfaatkan kelengahan pengguna digital yang tidak sadar akan besarnya harga atas informasi yang dimilikinya. Maka dari itu, kesadaran untuk mengamankan diri, keluarga, dan sesama pengguna digital adalah salah satu kompetensi literasi digital yang penting untuk dimiliki.

Menghadirkan keamanan digital adalah proses yang mencakup berbagai dimensi. Mulai dari menyiapkan perangkat yang aman untuk melindungi dan menjalankan kegiatan bermedia digital, menjaga data-data pribadi, menghindari upaya penipuan, menjaga perilaku saat bermedia digital hingga membangun ketahanan diri sejak usia dini. Pada bab-bab sebelumnya kita sudah membahas berbagai upaya untuk menghadirkan lingkungan digital yang aman dan nyaman. Prosesnya memang tidak mudah, diperlukan upaya yang serius untuk bisa mewujudkan lingkungan digital yang aman. Namun, ketika semua sudah tertata dengan baik maka pengamanan digital ini pada dasarnya ada untuk membantu kita untuk menjadi lebih produktif.



# BAB VI

---

## Keamanan Anak di Platform Digital

Dengan lingkungan yang aman untuk beraktivitas di dunia digital, kita tidak perlu lagi khawatir akan adanya ancaman yang datang dan mengganggu produktivitas kita. Aktivitas mencari informasi, berinteraksi di dunia maya, berkreasi dan berkolaborasi dengan para pengguna digital lainnya akan membantu kita untuk mengaktualisasi diri dan meninggalkan jejak-jejak digital positif yang juga bisa dinikmati pengguna digital yang lain.

Pada akhirnya, mengulas dan mendiskusikan teknologi digital merupakan sebuah proses belajar tanpa ujung. Teknologi digital, baik dalam konteks piranti digital maupun perkembangan medium di dalam dunia digitalnya berkembang dengan sangat pesat. Gordon E. Moore, *co-founder* Intel yang merupakan perusahaan produsen “otak komputer” terlaris di dunia pada 1965 menawarkan teori menarik. Menurutnya perkembangan jumlah transistor dalam sebuah mikrochip yang menjadi inti teknologi digital berkembang secara eksponensial. Setiap dua tahun, jumlah transistor bertambah dua kali lipat. Artinya setiap dua tahun teknologi digital yang ada di sekitar kita setidaknya berkembang dua kali lipat lebih canggih. Teori ini awalnya hanya digunakan untuk memproyeksikan perkembangan teknologi komputasi pada era 1960-an. Namun, ternyata pola tersebut masih konsisten terjadi sampai saat ini (Ourworldindata, 2020)

Perkembangan komputer yang semakin cepat berpengaruh juga pada perkembangan berbagai hal yang berkaitan dengan teknologi digital, baik perangkatnya, *platform* di dunia digitalnya, maupun peluang dan tantangannya. Lima tahun yang lalu kita mungkin belum membayangkan akan menikmati fasilitas ojek yang dipanggil kapan pun kita butuhkan. Kita juga mungkin dulu belum mampu membayangkan teknologi yang memungkinkan membeli seporsi martabak di pinggir jalan tanpa harus membayar dengan uang tunai. Hal yang beberapa tahun lalu tak lazim dilakukan saat ini menjadi hal yang biasa saja.

Hal yang sama terjadi pada konteks keamanan digital. Perkembangan teknologi juga berarti membuka peluang lahirnya beragam modus kejahatan baru yang mengancam keamanan digital kita. Namun, pada saat yang bersamaan, tindakan pengamanan digital, baik yang bersifat teknis seperti pengamanan perangkat digital maupun yang bersifat penguatan ketahanan diri, dalam menghadapi tantangan dunia digital juga turut berkembang mengikuti tren yang terjadi.



## KOMPETENSI KEAMANAN DIGITAL

Modul ini merupakan modul dasar yang memetakan area kompetensi keamanan digital yang diturunkan dari kurikulum literasi digital dalam Peta Jalan Literasi Digital 2021-2024 (Kominfo, Siberkreasi & Deloitte, 2020). Kurikulum ini kemudian diinterpretasikan dan dikembangkan oleh Japelidi dengan melakukan elaborasi terhadap 10 kompetensi literasi digital Japelidi yang sudah dibumikan dalam berbagai kegiatan dari penulisan seri buku panduan literasi digital, riset kompetensi literasi digital masyarakat hingga melakukan kampanye melawan hoaks COVID-19 (Kurnia & Wijayantom 2020).

Modul dengan tema keamanan digital ini merupakan salah satu modul dari empat seri modul kolaborasi Kominfo, Japelidi dan Siberkreasi dengan tema keterampilan digital, budaya digital, etika digital, dan keamanan digital. Modul ini dirancang untuk bisa digunakan sebagai media pembelajaran guna membangun ketangguhan pengguna internet agar celah terbukanya kebocoran identitas digital maupun data pribadi bisa tertutup rapat. Tak hanya memahami berbagai istilah terkait keamanan digital, pembaca modul diajak memahami berbagai strategi, langkah maupun tips untuk meningkatkan keamanan digital baik untuk dirinya sendiri maupun orang lain. Dengan begitu, pembaca modul ini - baik pengguna media digital maupun pengajar atau pegiat literasi digital bisa mengasah kompetensi keamanan digital mereka.

Kompetensi keamanan digital dalam modul ini didefinisikan sebagai kecakapan individual yang bersifat formal dan mau tidak mau bersentuhan dengan aspek hukum positif. Secara individual, terdapat tiga area kecakapan keamanan digital yang wajib dimiliki oleh pengguna media digital.

**Pertama**, kecakapan keamanan digital yang bersifat kognitif untuk memahami berbagai konsep dan mekanisme proteksi baik terhadap perangkat digital (lunak maupun keras) maupun terhadap identitas digital dan data diri. Hanya dengan penguasaan pengetahuan yang memadai maka pengguna media digital bisa melindungi diri beragam ancaman keamanan digital. Misalnya dengan memiliki pengetahuan yang memadai tentang berbagai

strategi untuk melakukan proteksi terhadap perangkat keras maupun lunak akan membantu meningkatkan keamanan perangkat digital yang kita gunakan.

**Kedua**, kecakapan keamanan digital yang bersifat afektif pada dasarnya bertumpu pada empati agar pengguna media digital punya kesadaran bahwa keamanan digital bukan sekadar tentang perlindungan perangkat digital sendiri dan data diri sendiri. Keamanan digital juga merupakan perlindungan perangkat digital media digital lainnya agar sistem keamanan digital yang ada di “rumah” kita maupun “rumah” orang lain dan “rumah-rumah” di sekitar kita aman dan tidak kemasukan pembobol yang bisa jadi merusak “rumah” tapi juga mengambil “barang-barang” kita. Rumah bisa di sini bisa dianalogikan sebagai sistem keamanan digital kita, sedangkan barang-barang bisa diartikan sebagai identitas digital dan data diri di *platform* digital. Jika perasaan, empati dan kesadaran kita untuk menjaga dunia maya kita bersama agar aman, maka kita adalah warga digital yang bertanggung jawab.

**Ketiga**, kecakapan keamanan digital yang bersifat konatif atau *behavioral* yang merupakan langkah-langkah praktis untuk melakukan perlindungan identitas digital dan data diri. Misalnya saja selalu memastikan menggunakan sandi yang kuat dan memperbaharuinya secara berkala.

Kecakapan yang bertumpu pada perilaku ini bisa dipandu dengan 10 kompetensi literasi digital Japelidi. Pertama, pastikan akses perangkat digital dan *platform* yang digunakan aman, dengan sandi yang kuat, selalu baru dan dijaga kerahasiaannya. Kedua, bersikap selektif saat menerima atau mencari informasi. Tidak semua informasi yang beredar di dunia digital atau kita terima layak dipercaya kebenarannya. Ketiga dengan memahami berbagai peluang dan ancaman di media digital. Hal ini termasuk juga memahami bagaimana strategi melindungi diri dan orang-orang di sekitar kita. Keempat dengan mengasah keterampilan analisis terhadap berbagai situasi. Keterampilan analisis yang baik akan membuat kita jauh lebih aman ketika bermedia digital karena kita akan terbiasa membedakan mana informasi yang berkualitas dan mana saja yang lebih baik diabaikan.

Kompetensi kelima adalah kemampuan untuk memverifikasi. Keterampilan ini sangat erat kaitannya dalam pengamanan diri karena verifikasi akan menghilangkan keraguan atas

suatu informasi. Memilih tempat yang tepat dalam memverifikasi data juga menjadi tantangan tersendiri. Keenam, mengevaluasi informasi-informasi yang kita dapatkan dan membuat kesimpulan tindak lanjut atas informasi tersebut. Kompetensi berikutnya merupakan kompetensi untuk mendistribusikan informasi yang sudah kita pastikan tidak akan membahayakan diri sendiri atau orang lain. Diperlukan kejelian agar distribusi informasi ini tidak justru menjadi bumerang. Hal yang sama juga berlaku pada kompetensi kedelapan, yaitu keterampilan untuk memproduksi konten yang tidak membahayakan diri sendiri dan tidak membahayakan orang lain. Patut kita hindari konten-konten yang berisiko membongkar data pribadi diri dan orang lain karena ada ancaman serius dari perilaku tersebut.

Bila pada tahapan-tahapan tersebut sudah dikuasai, maka kompetensi berikutnya adalah berpartisipasi. Partisipasi dalam konteks keamanan digital bisa kita lakukan dalam membuat sebuah lingkungan digital yang aman. Baik di dunia maya maupun di dunia nyata. Kita bisa ikut melakukan pengawasan konten, melakukan pelaporan atau sekadar aktif dalam upaya sosialisasi keamanan digital. Puncak dari kompetensi literasi digital adalah kolaborasi. Pada tahapan ini kita bisa berperan aktif sebagai kolaborator dalam menciptakan suasana yang aman dan nyaman. Menjadi penggerak bagi masyarakat sekitar maupun komunitas di dunia maya.

Meskipun kesepuluh kompetensi tersebut dapat dibedakan secara terpisah, namun dalam pelaksanaannya seluruh kompetensi itu sebenarnya saling berkesinambungan. Untuk bisa berkolaborasi dengan baik maka kita perlu menguasai kompetensi lain yang lebih sederhana dan bertahap semakin kompleks.

## **TANTANGAN KEAMANAN DIGITAL**

Modus-modus tindakan yang mengancam keamanan digital serta berbagai strategi penguatan diri untuk menghindari ancaman keamanan yang dituliskan pada modul ini relevan untuk menjawab tantangan yang ada pada dalam rentang waktu saat ini. Namun, pada dua tahun mendatang bisa jadi tantangannya berubah menjadi semakin kompleks dan berbahaya. Kelima tantangan yang kita bahas pada modul ini juga akan mengalami perubahan menjadi semakin menantang.

**Pertama**, fitur proteksi yang semakin beragam demikian juga *platform* yang semakin berkembang termasuk juga ancamannya. Jika kita adalah pengguna yang hanya menggunakan perangkat digital untuk kegiatan sehari-hari dan setia dengan produk-produk asli, perubahan ini sebenarnya tidak terlalu menjadi kendala. Para pakar yang membangun perangkat digital setiap saat juga selalu melakukan pembaruan sistem pengamanan sehingga penggunaannya selalu terlindungi. Namun ada baiknya kita juga selalu membuka mata atas beragam isu keamanan digital yang mengintai proteksi perangkat digital.

**Kedua**, kompleksitas identitas digital dan data pribadi yang tak mudah untuk dilindungi. Seperti yang sudah dibahas pada bab-bab sebelumnya, celah digital terbesar sebenarnya justru ada pada pengguna digital. Penyedia layanan digital sudah menyiapkan sederet strategi untuk mencegah pembobolan. Namun, terkadang pengguna yang abai akan pentingnya data digital dan ceroboh saat melakukan aktivitas di dunia digital. Kecerobohan ini selalu menjadi cara paling efektif bagi peretas untuk menembus sistem keamanan. Di masa mendatang, akan makin banyak strategi digunakan untuk mengelabui pengguna sehingga kecerobohan yang kecil sekalipun berpotensi mengancam keamanan data kita.

**Ketiga**, ragam penipuan digital yang semakin banyak. Jika dilihat trennya, jumlah kejahatan digital dalam bentuk penipuan juga semakin meningkat seiring semakin aktifnya kita di dunia digital. Para penipu seakan tidak pernah lelah untuk mencoba menipu dengan beragam cara. Lagi-lagi, keterampilan pengguna menjadi kunci pengamanan utama yang dapat memblokir serangan penipu.

**Keempat**, rekam jejak yang dimanfaatkan lebih banyak negatifnya dari positifnya. Data kita adalah sebuah komoditas yang sangat berharga. Semakin banyak kalangan yang menyadari nilai data kita dan nilai rekam jejak manusia. Maka menjaga rekam jejak saat ini menjadi sebuah langkah yang harus dilakukan agar kita tak sampai merugi di kemudian hari.

Yang terakhir, **kelima**, *minor safety* untuk anak yang semakin menantang terutama saat pandemi. Kecanduan, layanan digital untuk anak yang semakin menarik, dan semakin kecilnya ruang bermain akan semakin mengancam tumbuh kembang anak di masa

mendatang. Para orang tua, kerabat, dan saudara terdekat harus mulai sadar akan hal ini. Anak-anak adalah masa depan kita sehingga menjaga mereka sebaik-baiknya menjadi tugas lingkungan di mana anak itu tinggal.

Untuk menjawab tantangan ini, kolaborasi antara individu pengguna perangkat digital, industri digital, dan regulasi yang kuat harus terjalin dengan baik. Hanya mengandalkan salah satu komponen saja tidak akan menghasilkan lingkungan digital yang aman dan nyaman karena setiap komponen menjadi kunci dalam pengamanan digital.

### **PENGEMBANGAN MODUL KEAMANAN DIGITAL**

Sebagai sebuah upaya literasi digital yang tidak pernah berhenti, modul ini akan mempertahankan pola yang saat ini sudah ada. Seperti penyusunan dengan pendekatan yang praktis dari kurikulum yang sudah disusun, melengkapi modul dengan konsep, strategi dan tips-tips praktis, dan dukungan kasus-kasus empiris yang bisa menjadi pembelajaran bersama. Bentuk modul yang diperkaya dengan ilustrasi dan visualisasi juga akan menjadi kekuatan karena melalui penyampaian visualisasi yang menarik dan menyederhanakan, konsep yang sulit akan lebih mudah dipahami.

Materi-materi seputar penjelasan aspek hukum juga menjadi fokus pada masa mendatang. Modul ini juga akan mempertahankan rekomendasi untuk kelompok minoritas dan mengembangkannya menjadi lebih komprehensif pada pembaruan berikutnya. Sedangkan sebagai sarana mempermudah pengguna modul untuk merefleksikan diri, modul ini juga memperkaya diri dengan evaluasi dan lembar evaluasi untuk diri sendiri atau anak didik maupun peserta program literasi digital.

Modul **Aman Bermedia Digital** ini rencananya akan terus mengalami pembaharuan atau pengembangan setiap tahun agar bisa merespons perubahan lanskap dunia digital yang terjadi tidak hanya di Indonesia, melainkan juga secara global. Untuk mendukung pembaharuan atau pengembangan tersebut, tim penyusun juga akan terus mengevaluasi berbagai kajian yang mendasari penyusunan modul ini, termasuk mengevaluasi ulang kurikulum literasi digital yang ada dan menimbang apakah kurikulumnya masih bisa relevan dengan kondisi terbaru.

Kurikulum-kurikulum literasi digital yang digunakan pada modul ini merupakan hasil refleksi dan kajian ilmiah atas beragam fenomena yang terjadi di sekitar kita. Modul ini menggabungkan beragam perspektif yang dipakai dalam kurikulum-kurikulum tersebut untuk dapat disarikan dalam wujud panduan praktis. Berbeda dengan kajian ilmu alam yang bersifat pasti, kajian literasi digital masuk dalam ranah ilmu sosial yang juga tidak pernah berhenti bergerak dan tidak bisa digeneralisasi. Perlu ada peninjauan ulang secara berkala berdasarkan fenomena yang terjadi serta berbagai saran dan masukan yang diberikan.

Tim penyusun juga menyadari walaupun modul edisi ini sudah disusun dengan mempertimbangkan beragam konteks dan kepentingan, modul ini masih jauh dari sempurna. Modul ini baru membahas keamanan digital yang ditujukan bagi masyarakat yang sudah cukup memiliki kemampuan untuk mengakses media digital dengan fasilitas yang memadai. Modul ini juga

Namun, modul ini belum banyak menyentuh kalangan masyarakat yang masih mengalami hambatan dalam mengakses teknologi digital dengan lancar. Sebagai contoh, modul ini belum menyentuh upaya literasi digital bagi warga yang berada di kawasan tertinggal, terdepan, dan terluar (3T) yang masih mengalami kendala teknis maupun kendala secara pribadi. Modul ini juga belum banyak membahas strategi pengembangan literasi digital bagi masyarakat disabilitas, mereka yang berusia lanjut, kelompok minoritas, perempuan, dan anak. Kekurangan-kekurangan itu menjadi catatan dan akan menjadi pekerjaan rumah yang harus dituntaskan di kemudian hari karena akses internet yang sehat dan aman adalah hak seluruh warga negara tanpa terkecuali.

#### **DAFTAR PUSTAKA**

- Kominfo, Siberkreasi, & Deloitte (2020) *Roadmap literasi digital 2021-2024*. Jakarta: Kominfo, Siberkreasi, & Deloitte.
- Kurnia, N. & Wijayanto, X.A. (2020) Kolaborasi sebagai kunci: Membumikan kompetensi literasi digital Japelidi. Dalam N. Kurnia, L. Nurhajati, S.I. Astuti, *Kolaborasi lawan (hoaks) COVID-19: Kampanye, riset dan pengalaman japelidi di tengah*

*pandemi*. Yogyakarta: Program Studi Magister Ilmu Komunikasi, Departemen Ilmu Komunikasi, Universitas Gadjah Mada.

Ourworldindata (2020). Technological Progress. *Ourworldindata.org*. Diperoleh dari <https://ourworldindata.org/technological-progress>.

## DAFTAR ISTILAH

|                                   |  |
|-----------------------------------|--|
| <i>Algoritma</i>                  | Prosedur sistematis untuk pemecahan masalah  |
| <i>Antivirus</i>                  | Perangkat lunak perlindungan virus   |
| <i>Autentikasi</i>                | Proses verifikasi identitas dalam sistem   |
| <i>Back Up data</i>               | Langkah untuk mencegah kehilangan data   |
| <i>Back-Up</i>                    | Proses membuat data cadangan   |
| <i>Biometrics</i>                 | Teknologi keamanan berbasis tubuh individu   |
| <i>Bluetooth</i>                  | Perangkat teknologi komunikasi data tanpa kabel                                      |
| <i>Cookie</i>                     | Kumpulan informasi berisi rekam jejak dan aktivitas ketika menelusuri sebuah website |
| <i>Daring</i>                     | Dalam jaringan   |
| <i>Data digital</i>               | Data yang berisikan angka untuk sistem perhitungan tertentu                          |
| <i>Data Pribadi</i>               | Data mengenai ciri diri individu   |
| <i>Digital</i>                    | Berhubungan dengan angka untuk sistem perhitungan tertentu                           |
| <i>Distribusi informasi</i>       | Proses penyampaian mengenai kabar atau berita  |
| <i>Dompot Digital</i>             | Aplikasi elektronik untuk pembayaran secara daring                                   |
| <i>Double Smart Lock</i>          | Kunci untuk pengaman ganda yang praktis  |
| <i>Dropbox</i>                    | Aplikasi Penyimpanan data di internet  |
| <i>Email</i>                      | Sarana bertukar surat menggunakan jaringan internet                                  |
| <i>Enkripsi</i>                   | Proses penyandian data   |
| <i>Etika Digital</i>              | Aturan beretika saat berinteraksi di dunia maya                                      |
| <i>Face authentication</i>        | Pencocokan wajah untuk autentikasi sistem  |
| <i>Face Recognition</i>           | Fitur pengenalan wajah   |
| <i>Fingerprint authentication</i> | Pencocokan sidik jari untuk autentikasi sistem                                       |
| <i>Fitur</i>                      | Karakteristik khusus pada suatu alat   |
| <i>Gadget</i>                     | Telepon pintar   |
| <i>Game</i>                       | Permainan  |
| <i>Gawai</i>                      | Peranti kecil berteknologi dengan fungsi praktis                                     |
| <i>Hacker</i>                     | Individu yang mengakses data secara tidak sah  |
| <i>Hardware</i>                   | Perangkat keras computer   |
| <i>Hoaks</i>                      | Berita bohong atau palsu   |
| <i>Identitas digital</i>          | Cara elektronik untuk mengidentifikasi seseorang                                     |
| <i>Internet Protocol</i>          | Protokol lapisan jaringan untuk pengalamatan   |
| <i>Internet</i>                   | Jaringan komunikasi antarmedia   |
| <i>Jejak digital</i>              | Jejak data saat individu menggunakan internet  |
| <i>Jejak digital aktif</i>        | Data yang secara sengaja ditinggalkan oleh pengguna di dunia maya                    |
| <i>Jejak digital pasif</i>        | Data yang secara tidak sengaja ditinggalkan oleh pengguna di dunia maya              |
| <i>Kejahatan siber</i>            | Tindakan kriminal yang dilakukan dengan memanfaatkan media internet                  |
| <i>Keselamatan digital</i>        | Kondisi aman atas tindakan penggunaan perangkat tertentu                             |



|                                   |   |
|-----------------------------------|---|
| <i>Kode File</i>                  | Penomoran pada identitas data   |
| <i>Layanan daring</i>             | Membantu suatu hal melalui dalam jaringan   |
| <i>Literasi digital</i>           | Kemampuan untuk memahami dan menggunakan informasi melalui teknologi                                |
| <i>Log Out</i>                    | Proses keluar untuk memutus akses pada sistem   |
| <i>Lokapasar</i>                  | Website atau aplikasi yang memfasilitasi proses jual beli dari berbagai took                        |
| <i>Malware</i>                    | Perangkat lunak dirancang untuk mengontrol perangkat secara diam-diam                               |
| <i>Massif</i>                     | Kuat, kukuh, utuh   |
| <i>Media</i>                      | Alat sarana komunikasi  |
| <i>Media digital</i>              | Media yang dikodekan dalam format yang dapat dibaca oleh mesin                                      |
| <i>Media sosial</i>               | Media daring untuk berinteraksi tanpa batas ruang dan waktu   |
| <i>Microsoft</i>                  | Perusahaan sistem operasional pada computer   |
| <i>Minor Safety</i>               | Keamanan anak   |
| <i>Mobile Ad Fraud</i>            | Penipuan iklan seluler  |
| <i>Money mule</i>                 | Metode pencurian dengan mentransfer uang secara illegal   |
| <i>Nomor OTP</i>                  | Nomor verifikasi sekali pakai   |
| <i>OneDrive</i>                   | Aplikasi penyimpanan data Microsoft   |
| <i>One-Time Password</i>          | Kata kunci yang berlaku hanya untuk satu sesi   |
| <i>Partisipasi dunia digital</i>  | Aktivitas di dalam penggunaan teknologi dan internet  |
| <i>Password</i>                   | Kata kunci atau sandi   |
| <i>Pelanggaran privasi daring</i> | Penyalahgunaan akses data pribadi seseorang   |
| <i>Pelecehan seksual</i>          | Pendekatan terkait seks yang tidak diinginkan salah satu pihak                                      |
| <i>Pencurian data pribadi</i>     | Tindakan ilegal dalam mendapatkan data individu melalui internet                                    |
| <i>Penipuan</i>                   | Tindakan seseorang dengan tipu muslihat kebohongan  |
| <i>Penipuan digital</i>           | Tindakan tipu muslihat kebohongan melalui teknologi dan internet                                    |
| <i>Perdagangan orang</i>          | Segala transaksi jual beli terhadap manusia   |
| <i>Peretasan</i>                  | Tindakan untuk memperoleh data secara tidak sah   |
| <i>Perlindungan identitas</i>     | Tindakan untuk mengamankan informasi diri   |
| <i>Perundungan</i>                | Tindakan menyakiti atau mengintimidasi orang lain   |
| <i>Pharming</i>                   | Serangan dunia maya dengan pengalihan situs sah ke situs palsu                                      |
| <i>Phishing</i>                   | Penipuan dengan mengelabui target untuk mencuri akun  |
| <i>PIN</i>                        | <i>Personal Identification Number</i> (PIN) Angka sandi rahasia untuk otentikasi pengguna ke sistem |
| <i>Platform</i>                   | Rencana kerja sebagai dasar bagi berjalannya sebuah sistem  |

|                                       |   |
|---------------------------------------|---|
| <i>Pornografi</i>                     | Hal berbau seksual berupa gambar, tulisan, video, atau pesan                |
| <i>Privasi</i>                        | Kerahasiaan pribadi   |
| <i>Proteksi</i>                       | Perlindungan  |
| <i>Radio-Frequency Identification</i> | Metode identifikasi untuk menyimpan dan mengambil data jarak jauh           |
| <i>Ransomware</i>                     | Malware yang digunakan peretas mengenkripsi data korban                     |
| <i>Recovery Key</i>                   | Kunci Pemulihan   |
| <i>Remote Wipe</i>                    | Cara untuk menghapus data pada ponsel yang hilang atau dicuri               |
| <i>Rooting</i>                        | Proses mendapatkan hak akses yang lebih tinggi                              |
| <i>Router</i>                         | Perangkat keras untuk menghubungkan beberapa jaringan                       |
| <i>Sarana internet</i>                | Sesuatu yang digunakan dalam menghubungkan antar media elektronik           |
| <i>Seleksi informasi</i>              | Aktivitas untuk memilih pesan tertentu                                      |
| <i>Shredder</i>                       | Fitur pemusnah data   |
| <i>Siber</i>                          | Sistem komputer dan informasi   |
| <i>Sistem Elektronik</i>              | Serangkaian perangkat dan prosedur dengan alat bantu perkembangan teknologi |
| <i>Sistem Non Elektronik</i>          | Serangkaian perangkat dan prosedur dengan alat bantu benda dan manusia      |
| <i>Situs jejaring sosial</i>          | Komunitas virtual untuk melakukan interaksi social                          |
| <i>Smartphone</i>                     | Ponsel cerdas   |
| <i>Sniffing</i>                       | Tindak kejahatan penyadapan dengan internet untuk mengambil data            |
| <i>Social Engineering</i>             | Rekayasa Sosial   |
| <i>Sosial media</i>                   | Media daring untuk berinteraksi dalam dunia maya                            |
| <i>Surel</i>                          | Surat elektronik  |
| <i>Teknologi digital</i>              | Fasilitas pendukung berbasis sinyal elektrik computer                       |
| <i>Teknologi informasi</i>            | Fasilitas pendukung kualitas hasil informasi secara cepat dan berkualitas   |
| <i>Teknologi komunikasi</i>           | Fasilitas pendukung dalam proses pertukaran informasi                       |
| <i>Transaksi daring</i>               | Pembelian barang dan jasa melalui media internet                            |
| <i>Two-factor Authentication</i>      | Proses keamanan dengan dua sarana identifikasi                              |
| <i>Update</i>                         | Pembaruan   |
| <i>Warganet</i>                       | Individu yang aktif menggunakan internet                                    |
| <i>WhatsApp</i>                       | Aplikasi bertukar pesan pada ponsel cerdas                                  |

## DAFTAR INDEKS

### 3

3T, 46, 47, 83, 84, 120, 145, 147, 153, 156, 187, 201

### A

Akses, 16, 59  
Algoritma, 203  
Aman, ii, ix, 25, 27, 184  
anak, ix, 14, 25, 26, 27, 28, 46, 49, 50, 51, 52, 53, 58, 83, 86, 87, 90, 120, 136, 145, 147, 152, 153, 154, 155, 156, 157, 160, 164, 167, 169, 171, 172, 173, 174, 175, 176, 177, 179, 180, 181, 182, 184, 186, 187, 189, 190, 191, 192, 193, 199, 200, 201, 204  
Antivirus, 37, 40, 41, 51, 57, 58, 203  
Aspek hukum, 93  
Autentikasi, 77, 79, 203

### B

Back-up, 40, 51, 56

### C

Cadangan, 43  
Cadangan data, 43  
Cookie, ix, 134, 138, 203

### D

Daring, 17, 96, 103, 104, 203  
Data digital, 203  
Data Pribadi, v, 67, 70, 71, 72, 73, 74, 92, 93, 150, 203  
Difabel, 47, 84, 120, 147, 187  
Distribusi, 16, 203  
Dokumen, 44, 114  
Dompot Digital, 203

### E

Enkripsi, 37, 41, 52, 57, 203  
Etika Digital, 25, 203  
Evaluasi, v, vi, x, 16, 27, 54, 55, 58, 59, 61, 88, 89, 91, 122, 123, 130, 144, 148, 149, 189

### F

Face authentication, 39, 203  
Face Recognition, 203  
File, 42, 204  
film, 151, 168, 209  
Fingerprint authentication, 38, 203  
Fitur, v, 37, 38, 39, 40, 41, 42, 47, 48, 49, 50, 51, 53, 55, 56, 57, 58, 203, 205  
foto, 31, 34, 35, 39, 40, 42, 43, 44, 61, 130, 132, 135, 139, 143, 164, 177

### G

gambar, 44, 71, 75, 137, 155, 162, 164, 171, 177, 185, 186, 187, 188, 205  
game, 95, 156, 157, 167, 169, 190  
Game, 17, 30, 156, 203  
Gawai, 169, 203

### H

Hoaks, 17, 70, 72, 92, 93, 203, 210

### I

Identitas digital, 64, 65, 89, 98, 203  
Informasi, 16, 17, 21, 44, 60, 61, 93, 97, 98, 114, 128, 175, 180, 186, 192  
Internet Protocol, 67, 203

### J

Jejak digital, ix, 129, 132, 133, 135, 136, 137, 138, 150, 151, 203

### K

Kampanye, 18, 29, 71, 72, 93, 201  
Keamanan, v, vi, x, 16, 19, 24, 25, 88, 189, 197, 204  
Keamanan digital, 19, 88, 197  
Kebocoran, 63  
Kecakapan, x, 55, 58, 88, 91, 197  
kecanduan, ix, 27, 169, 190, 193  
Kejahatan, 13, 99, 100, 109, 127, 203  
Kejahatan siber, 203

kekerasan, ix, 153, 167, 175, 179, 180,  
186, 188, 189, 191, 192, 193  
kekerasan digital, ix, 193  
keselamatan, 23, 152, 154, 156, 157, 171,  
174, 177, 179, 184, 185, 187, 188, 189,  
190  
kesetaraan, 185  
Kolaborasi, 16, 93, 145, 181, 201, 210  
Kompetensi, v, vi, x, 16, 17, 18, 19, 20, 24,  
119, 142, 145, 173, 196, 197  
Komputer, 93  
Komunikasi, 2, 16, 19, 28, 29, 30, 92, 93,  
94, 116, 126, 150, 168, 180, 193, 201,  
208, 209, 210  
Komunitas, 205  
Konsumen, 97, 114, 128  
Konten, 16, 147, 156, 158, 167, 178, 180  
Kunci, 38, 39, 203, 205

## L

Lansia, 47, 84, 120, 147, 187  
Layar, 191, 193  
literasi digital, ii, viii, x, 14, 15, 16, 17, 18,  
19, 21, 23, 24, 25, 28, 29, 46, 47, 58, 82,  
83, 84, 90, 93, 97, 100, 119, 122, 126,  
142, 143, 145, 147, 149, 153, 154, 156,  
184, 187, 190, 194, 196, 197, 198, 200,  
201, 208, 209  
Literasi digital, 22, 204  
Lokapasar, 204

## M

Malware, 32, 204, 205  
Maya, 20, 22, 99, 150  
Media digital, 27, 172, 182, 204  
Media sosial, 193, 204  
minor safety, 26, 187, 190, 199  
Modul, 2, ii, v, vi, 22, 23, 25, 27, 156, 196,  
200, 201  
Modus, vii, 34, 98, 99, 110, 137, 198

## O

orang tua, 27, 147, 171, 172

## P

Paham, 16

Partisipasi, 16, 19, 83, 145, 179, 198, 204  
pegiat literasi digital, ii, 25, 27, 28, 32, 54,  
58, 64, 88, 90, 130, 149, 171, 196  
Pelecehan seksual, 164, 204  
pembaca, ii, 18, 27, 145, 196  
Pencocokan, 38, 39, 203  
Pencurian data, 161, 204  
pengajar, ii, 25, 27, 28, 32, 54, 58, 64, 88,  
90, 130, 149, 196, 209, 210  
pengguna media digital, ii, 13, 15, 17, 18,  
19, 25, 27, 64, 68, 82, 83, 130, 153, 156,  
179, 184, 187, 196, 197  
Penipuan, v, vi, x, 96, 97, 98, 101, 103,  
104, 107, 111, 115, 119, 120, 121, 122,  
123, 127, 204  
Penipuan daring, 97  
Penipuan digital, 96, 98, 115, 119, 204  
Perangkat digital, x, 31, 36, 37, 39, 47, 55,  
60  
Perangkat keras, 31, 37, 203, 205  
Perangkat lunak, 32, 41, 203, 204  
Perdagangan orang, 17, 204  
Perempuan, 17, 47, 84, 120, 147, 181,  
186, 187  
Peretas, 33  
Peretasan, 204  
Perlindungan, v, vi, vii, x, 16, 45, 55, 67,  
82, 88, 89, 91, 97, 114, 127, 128, 142,  
148, 149, 181, 183, 204, 205  
Perlindungan identitas, 204  
perundungan, 21, 157, 158, 179, 185  
Perundungan, ix, 157, 185, 186, 204  
pesan, 18, 34, 40, 41, 70, 71, 83, 95, 105,  
109, 110, 123, 124, 143, 144, 148, 152,  
157, 164, 171, 172, 177, 178, 183, 187,  
205  
Pharming, 204  
*Phishing*, 109, 122, 127, 204  
PIN, 64, 74, 75, 76, 77, 82, 86, 89, 92, 93,  
104, 142, 204  
Platform, v, vi, 127, 204, 210  
Pornografi, 164, 165, 176, 205  
Privasi, 205  
Produksi, 16  
Proteksi, v, x, 32, 37, 39, 44, 54, 55, 58, 59,  
60, 94, 156, 193, 205

## **R**

Rekam jejak, 149

Rekam jejak digital, 149

## **S**

Sandi, 16, 19, 29, 37, 47, 55, 93, 100, 124, 126, 192

Seleksi, 16, 205

Seleksi informasi, 205

Siber, 12, 13, 16, 19, 29, 93, 100, 124, 125, 126, 166, 192, 205

Sistem, 93, 126, 205

Sniffing, 205

Social Engineering, 205

strategi, ii, 14, 26, 27, 82, 196, 197, 198, 199, 200, 201

## **T**

Teknologi digital, 12, 152, 195, 205

Teknologi informasi, 205

Teknologi komunikasi, 152, 205

Transaksi, 17, 97, 114, 126, 128, 205

Transaksi daring, 205

tulisan, 164, 177, 205, 209

Two-factor Authentication, 78, 205

## **V**

Verifikasi, 16

video, 31, 34, 35, 40, 42, 43, 44, 49, 50, 51, 52, 53, 61, 63, 86, 87, 137, 158, 164, 177, 205

## **W**

Warganet, 205

WhatsApp, viii, 28, 40, 92, 101, 118, 126, 128, 144, 152, 166, 205, 209

## TENTANG PENULIS

### **Gilang Jiwana Adikara**

Dosen di Jurusan Ilmu Komunikasi Universitas Negeri Yogyakarta. Aktif sebagai anggota Jaringan Pegiat Literasi Digital (Japelidi) sejak 2017 dan terlibat dalam berbagai kegiatan literasi digital baik di tingkat nasional maupun daerah termasuk sebagai tim penyusunan kurikulum literasi digital Tular Nalar yang diinisiasi Mafindo, Maarif Institute, Love Frankie dan Google. Salah satu bukunya yang berkaitan dengan literasi digital berjudul *Digital Parenting: Mendidik Anak di Era Digital* dapat diunduh gratis di literasidigital.id. Facebook: Gilang Adikara, website: [www.gilangadikara.com](http://www.gilangadikara.com), dan email: [gilang.ja@uny.ac.id](mailto:gilang.ja@uny.ac.id).

### **Novi Kurnia**

Staf pengajar Program Studi Magister Ilmu Komunikasi di Fisipol UGM. Selain menjadi salah satu dewan redaksi JSP (Jurnal Ilmu Sosial dan Ilmu Politik), ia adalah pendiri dan koordinator Jaringan Pegiat Literasi Digital (Japelidi) dari tahun 2017 hingga sekarang. Doktor lulusan Flinders University (South Australia) ini menekuni kajian literasi digital, sinema Indonesia, serta gender dan media. Ia dan timnya memenangkan *WhatsApp Misinformation and Social Research Award* yang hasilnya diterbitkan dalam buku berjudul *WhatsApp Group and Digital Literacy among Indonesian Women* pada tahun 2020. Berbagai karyanya di bidang literasi digital, gender dan media serta kajian film Indonesia diterbitkan di berbagai publikasi lainnya level nasional dan internasional. Ia bisa dihubungi melalui: [novikurnia@ugm.ac.id](mailto:novikurnia@ugm.ac.id).

### **Santi Indra Astuti**

Dosen di Fakultas Ilmu Komunikasi, Universitas Islam Bandung (UNISBA), Bidang Kajian Ilmu Jurnalistik. Saat ini tengah menempuh studi PhD di School of Communication, Universiti Sains Malaysia, Pulau Pinang Malaysia. Minatnya merentang mulai dari kajian media hingga media/digital literacy. Selain mengajar, ybs terlibat dalam sejumlah aktivitas lapangan, di antaranya dalam kampanye anti rokok, gerakan anti hoaks, dan tentunya, literasi media/literasi digital di tengah public. Bergabung memperkuat Mafindo sebagai Presidium Pengampu Riset, ybs mendirikan Jaringan Pegiat Literasi Digital (Japelidi). Terlibat dalam gerakan literasi media Bersama Yayasan Pengembangan Media dan Anak (YPMA) sejak 2007, dan selama 5 tahun menggagas gerakan Hari Tanpa TV di Bandung Raya. Dapat dihubungi melalui alamat *email*: [santi.indraastuti@gmail.com](mailto:santi.indraastuti@gmail.com) dan [santi@unisba.ac.id](mailto:santi@unisba.ac.id).

### **Lisa Adhrianti**

Staf Pengajar Jurusan Ilmu Komunikasi FISIP Universitas Bengkulu (UNIB). Lahir di Bengkulu, 30 September 1982. Menempuh pendidikan S1 di Fakultas Ilmu Komunikasi di Universitas Islam Bandung, S2 dan S3 Ilmu Komunikasi FISIP UI Jakarta. Saat ini menjabat sebagai Ketua Jurusan Ilmu Komunikasi FISIP UNIB dan aktif di ASPIKOM Wilayah Bengkulu sebagai Koordinator bidang Kerjasama, Organisasi dan Kelembagaan. Konsisten di bidang Kehumasan dan termasuk anggota Jaringan Pegiat Literasi Digital (Japelidi) ini juga merupakan trainer *Public Speaking* dan Konsultan *Branding*. Selain itu memiliki riwayat menulis buku ontologi memoar dan fiksi yang telah dipublikasikan : *It's Me, Tidak Pernah Ada yang Sia-sia, dan Yang Paling Membuat Kita Bahagia* (2019). Karya ilmiah yang terkait dengan keilmuannya adalah: *Digitalisasi PR bagi Penguatan Citra Pemerintah Daerah* (2016), *The Islamic Political Participation through the Relationship Persuasive*

*Communication (2017), Infografis Penguatan Reputasi Kehumasan Pemerintah melalui Narasi Tunggal Sosialisasi Paket Kebijakan Ekonomi (2018), Digital Infographics for Strengthening Bengkulu's Regional Tourism Promotions (2019), Komunikasi Pengurangan Resiko Bencana Berbasis Keluarga dan Kolaborasi Lawan Hoaks COVID-19 (2020).* Ia dapat dihubungi melalui FB: Lisa Adhrianti, IG @lisaadhrianti, Email: lisaadhrianti@unib.ac.id.

### **Sri Astuty**

Bekerja sebagai staf pengajar pada FISIP ULM. Terlibat berbagai penelitian diantaranya bekerjasama dengan AGB Nielsen, KPI, Dewan Pers, Perusahaan, Pemerintah Daerah Kalselteng. Menulis pada beberapa bagian buku nasional maupun internasional, media maupun jurnal diantaranya *Kisah Pilu Petani di Lahan Gambut* (Agustus, 2014), *Memberdayakan Orang Jejangkit* (Desember, 2015), *Komunikasi Digital: Kreativitas dan Interkonektivitas* (September, 2016), *Bunga Rampai Komunikasi Indonesia* (Oktober, 2017), *Komunikasi Pemasaran dan Pengembangan Potensi Daerah* (November, 2017), *Multiple Platform In Transformative Public Relations, Cultural and Tourism* (November, 2018), *Dinamika Komunikasi & Kearifan Lokal Seri 1 dan Seri 2* (September, 2018), *Public Relations dan Periklanan : Menghadapi Revolusi Industri 4.0 Kongres V AspiKOM* (Mei, 2019) *Kolaborasi Lawan Hoax Covid-19 bersama Japelidi Indonesia* (Desember, 2020), *Kebijakan Publik pada Pandemi Covid-19* (2020). Aktivitas organisasi lainnya di ASPIKOM, Japelidi, dsb. Ia dapat dihubungi melalui astutysri30@yahoo.co.id.

### **Xenia Angelica Wijayanto**

Peneliti dan pengajar di Institut Komunikasi dan Bisnis LSPR, desainer grafis serta konsultan ini adalah alumnus jurusan Hukum Lingkungan, Fakultas Hukum UGM dan juga Corporate Communication dari LSPR Jakarta. Bergabung dengan Japelidi pada 2019, Xenia terlibat dalam beberapa kampanye Japelidi. Karyanya di Japelidi antara lain adalah buku Panduan Menjadi Jurnalis Warga yang Bijak Beretika (2019), serta buku Mencegah dan Mengatasi Bullying di Dunia Digital (2019). Saat ini dipercaya sebagai Kepala Pusat Publikasi LP3M LSPR, Kepala Pusat Hak Kekayaan Intelektual, serta mengelola Penerbit LP3M di IKB LSPR. Minat risetnya antara lain tentang media, lingkungan hidup, keberagaman, pop culture dan hukum. Tulisan-tulisan non-akademis-nya yang lain dapat dibaca di [www.lokatanya.com](http://www.lokatanya.com). Komunikasi dapat melalui instagram @xenipi dan Twitter @XeniAngeli.

### **Fransiska Desiana Setyaningsih Setyaningsih**

Staf pengajar sekaligus Sekretaris Program Studi Ilmu Komunikasi (S-1) FISIP Universitas Katolik Widya Mandira, Kupang. Menjadi anggota Jaringan Pegiat Literasi Digital (Japelidi) dari tahun 2019 hingga sekarang, sejak 2018 dipercaya sebagai auditor dan asesor internal universitas. Magister lulusan Universitas Indonesia ini menekuni kajian komunikasi dan media, beberapa tulisannya telah diterbitkan di Jurnal Nasional. Terakhir di tahun 2020, berhasil mengantarkan Tim PKM Unwira dari Prodi Ilmu Komunikasi lolos Pekan Ilmiah Mahasiswa Nasional (PIMNAS) ke-33 sebagai juara Favorit. Email: fransiskadesiana@unwira.ac.id.



Kominfo | Siberkreasi | Japelidi  
**2021**