BAB III

METODOLOGI PENELITIAN DAN PERANCANGAN

3.1 Metodologi Pengumpulan Data

Dalam perancangan kampanye sosial menjaga data pribadi di internet, penulis akan mengumpulkan data dengan gabungan metode kualitatif dan kuantitatif (*hybrid*). Pengambilan data secara kualitatif akan dilakukan dengan wawancara kepada ahli hukum untuk mengetahui *insight* dari perlindungan data pribadi di Indonesia saat ini dari prespektif hukum, ahli keamanan teknologi informasi dan komunikasi untuk mengetahui lebih mendalam mengenai kejahaatan siber, sikap masyarakat, dan bagaimana cara melindungi data pribadi di internet, ahli media untuk mendapatkan informasi mengenai media dan strategi yang tepat. Selain wawancara, penulis juga melakukan studi literatur dan eksisting melalui pencarian internet, jurnal dan buku yang membahas perlindungan data di internet.

Selain itu, penulis juga menggunakan metode pengumpulan data kuantitatif. Pengambilan data dengan metode ini, dilakukan dengan menyebarkan kuesioner menggunakan Google Form, dengan tujuan mengetahui pemahaman target audiens mengenai perlindungan data pribadi dan bagaimana mereka menjaga data tersebut sampai sekarang.

3.1.1 Metode Kuantitatif

Menurut (Sugiyono, 2017), metode kuantitatif merupakan metode pengumpulan data berlandaskan filsafat positifisme, yang berfungsi untuk meneliti suatu populasi atau sampel tertentu. Data yang dikimpulkan dan dianilisis bersifat statistik.

3.1.1.1 Kuesioner

(Kumar et al., 2011) mengatakan, kuesioner merupakan beberapa pertanyaan yang tertulis dan jawabannya dicatata oleh responden, sehingga pertanyaan yang dibuat harus jelas dan mudah

dimengerti responden. Dalam perancangan ini, penulis ingin mengetahui tingkat pemahaman target audiens terhadap "perlindungan data pribadi" serta bagaimana para responden menjaga data pribadi yang mereka miliki.

Penulis menyusun kuesioner melalui *Google Form*, selanjutnya penulis menerapkan rumus Solvin untuk menghitung jumlah sampel, dengan derajat ketelitian 10%. Sampel yang diambil sesuai dengan target demografis audiens yaitu masyarakat Jabodetabek, dengan populasi jumlah penduduk sebesar 60.141,6 juta orang (Berdasarkan data jumlah penduduk Jawa Barat dan DKI Jakarta tahun 2020, website resmi BPS, (https://www.bps.go.id/indicator/12/1886/1/jumlah-penduduk-hasil-proyeksi-menurut-provinsi-dan-jenis-kelamin.html). Berikut perhitungannya:

$$S = \frac{n}{1 + N.e^2}$$

Keterangan:

S = Jumlah responden

N/n= Jumlah populasi

E = Sampling error/Derajat ketelitian

$$S = \frac{60.141,6}{1 + (60.141,6\,.\,(0.1)^2)} = 99,83$$

$$S = 99,83 \approx 100$$

Setelah mendapaatkan besaran sampel dengan derajat ketelitian 10%, penulis menulis mengumpulkan responden yang berjumlah 100 orang. Kuesioner disebarkan pada tanggal 20 Februari

2021, dan berikut merupakan data hasil kuesioner per 25 Februari 2021, dengan jumlah 100 responden.

Tabel 3.1 Data Demografis Responden

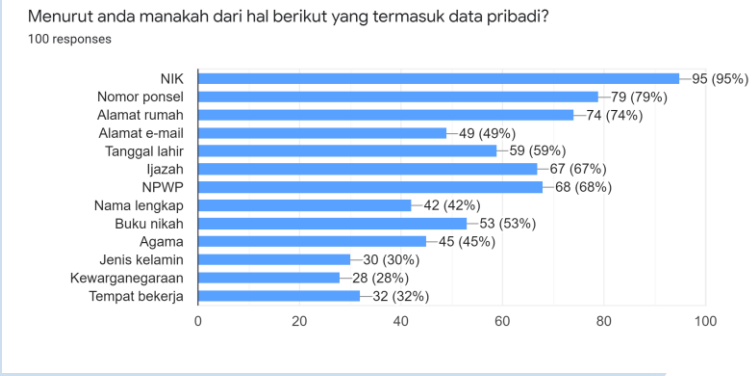
Variabel	Kategori	Frekuensi	Presentase
Usia	17-20 tahun	77	77%
	21-25 tahun	23	23%
Jenis Kelamin	Pria	44	44%
	Wanita	55	55%
	Memilih untuk tidak disebutkan	1	1%
Pekerjaan	Pelajar	5	5%
	Mahasiswa/i	51	51%
	Pekerja Kanatoran	23	23%
	Freelance	8	8%
	Wirausaha	6	6%
	Lainya	7	7%

Berdasarkan data di atas, kuesioner mayoritas diisi oleh responden pria dan wanita yang berusia 21-25 tahun (77%), dan berstatus mahasiswa/i (51%), responden yang lain memiliki profesi seperti pekerja kantoran (23%), *freelance*r (8%), wirausaha (6%), dan pekerjaan lainnya (7%).

Selanjutnya, penulis ingin mengetahui seberapa dalam pengetahuan responden terhadap data pribadi. Pada dasarnya, seluruh data yang disajikan dalam pertanyaan tersebut merupakan data pribadi, dengan pertanyaan tersebut penulis dapat melihat data apa saja yang dinilai responden sebagai data pribadi dan yang bukan, sehingga terlihat pula seberapa dalam pengetahuan responden terhadap data pribadi. Data tersebut kemudian dikelompokan menjadi dua, yaitu data pribadi umum dan data pribadi khusus.

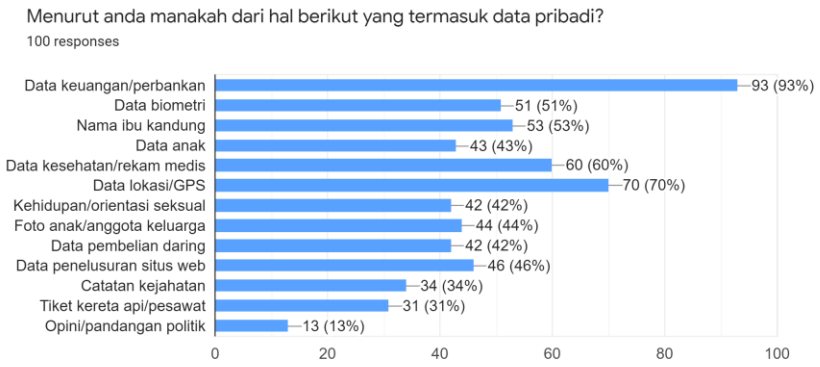
Pada data pribadi umum, mayoritas responden menilai bahwa Nomor Induk Khusus (NIK) merupakan data pribadi, dengan presentase (95%). Selanjutnya data yang dinilai oleh sebagian besar

responden sebagai data pribadi adalah yang berhubungan dengan kontak, seperti nomor ponsel (79%), alamat rumah (74%), dan nama lengkap (68%), sedangkan data yang paling sedikit dinilai oleh responden sebagai data pribadi adalah kewarganegaraan (28%) dan jenis kelamin (30%).



Gambar 3.1 Diagram Pengetahuan Responden terhadap Data Pribadi Umum.

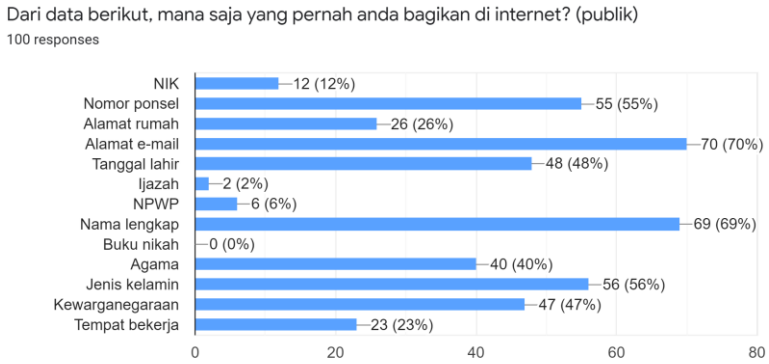
Sementara itu, pada pertanyaan mengenai data pribadi yang bersifat khusus, yang paling banyak diketahui oleh responden sebagai data pribadi adalah data keuangan/perbankan dengan presentase (93%), selanjutnya adalah data lokasi/GPS dengan presentase (70%), dan data kesehatan/rekam medis (60%), sedangkan yang mengetahui bahwa opini/pandangan politik merupakan data pribadi khusus, hanya diketahui oleh (13%) responden.



Gambar 3.2 Diagram Pengetahuan Responden terhadap Data Pribadi Khusus.

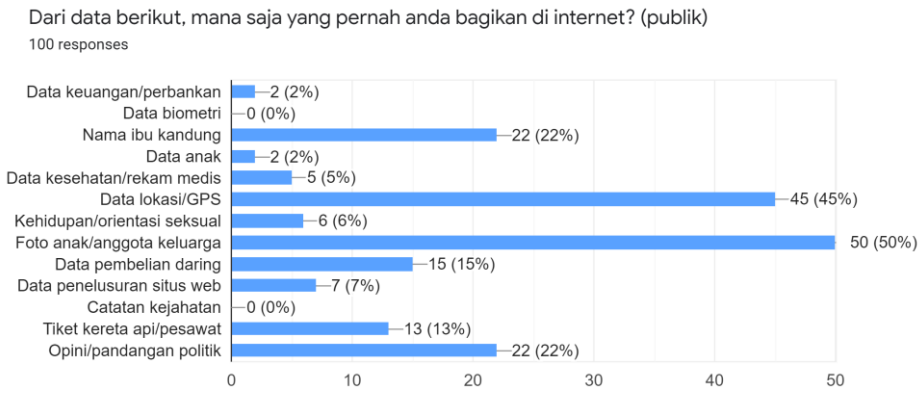
Para responden sebagian besar sudah mengetahui apa itu data pribadi, terutama NIK yang menyangkut data pribadi lainnya, serta data keuangan atau perbankan. hanya ada beberapa data pribadi saja yang masih belum banyak diketahui oleh responden sebagai data pribadi seperti kewarganegaraan, jenis kelamin, dan pandangan politik seseorang.

Setelah mengetahui pengetahuan responden terhadap data pribadi yang bersifat umum maupun khusus. Penulis ingin mengetahui data pribadi apa saja yang paling banyak dibagikan ke intenret oleh responden. Dari data yang didapatkan penulis, data pribadi umum yang paling banyak dibagikan adalah alamat e-mail (70%) dan nama lengkap (69%), disusul dengan jenis kelamin (56%) dan nomor ponsel (55%), dan dari total jumlah responden (100), tidak ada satupun yang pernah membagikan buku nikahnya di internet.



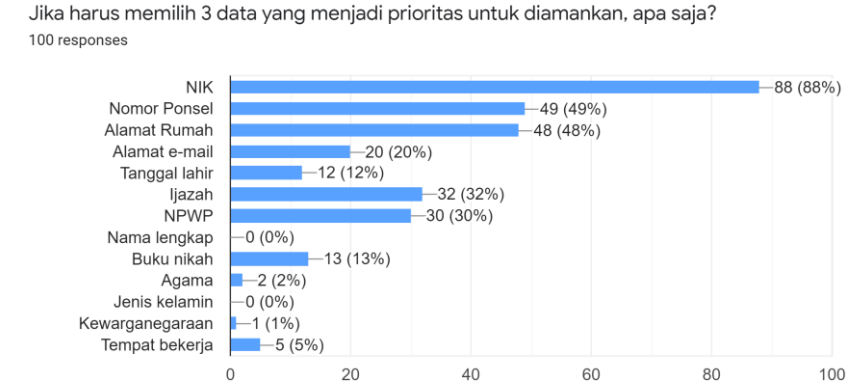
Gambar 3.3 Diagram Data Pribadi Umum yang pernah dibagikan

Selain membagikan data umum di internet, penulis juga mendapatkan responden membagikan data khusus mereka di internet. Foto anak/anggota keluarga merupakan data yang paling sering dibagikan, dengan presentase (50%) disusul dengan data lokasi/GPS (45%), kemudian nama ibu kandung dan opini/pandangan politik, dengan jumlah presentase yang sama, yaitu 22%. Sedangkan catatan kejahatan dan data biometri tidak pernah dibagikan oleh responden.



Gambar 3.4 Diagram Data Pribadi Khusus yang pernah dibagikan

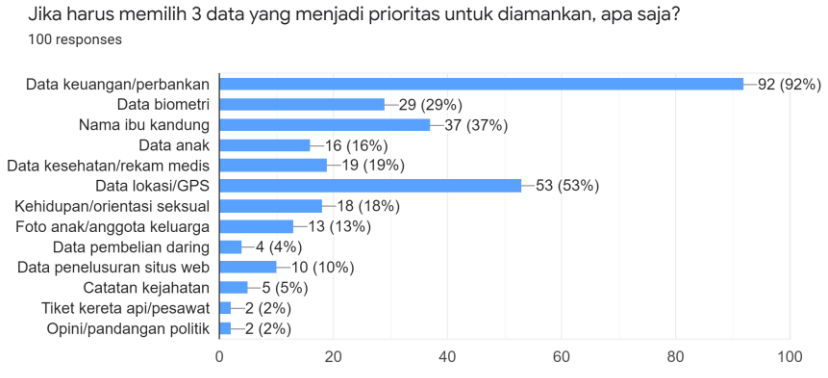
Pada bagian selanjutnya, penulis mencari tahu bagaimana prioritas responden untuk mengamankan data pribadi yang mereka miliki. Pada data pribadi yang bersifat umum, responden menjadikan NIK sebagai data dengan prioritas utama untuk diamankan (88%) kemudian disusul dengan nomor ponsel (49%) dan alamat rumah (48%). Sedangkan data seperti nama lengkap dan jenis kelamin, tidak menjadi prioritas satupun responden.



Gambar 3.5 Diagram Data Pribadi Umum yang menjadi prioritas untuk diamankan

Selanjutnya, mengenai data pribadi khusus yang menjadi prioritas utama untuk dilindungi, responden sangat mengutamakan data

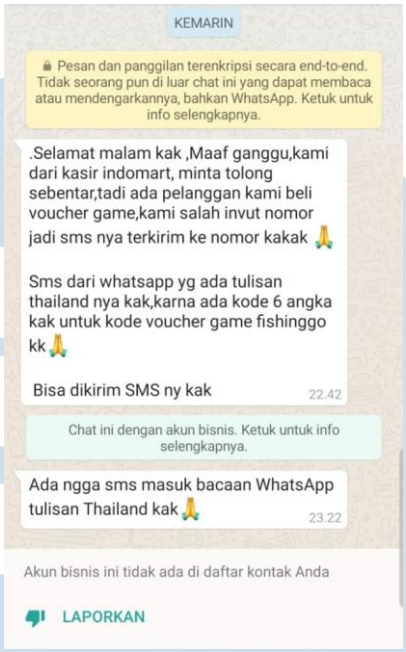
keuangan/perbankan (92%), lalu diikuti dengan data lokasi/GPS (53%) dan nama ibu kandung (37%). Sedangkan data pribadi khusus yang paling diabaikan mengenai keamanannya adalah opini/pandangan politik dan tiket kereta api/pesawat, yang masing-masing memiliki presentase sebesar (2%).



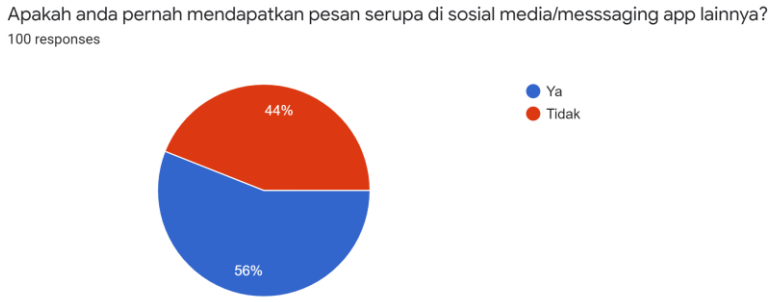
Gambar 3.6 Diagram Data Pribadi Khusus yang menjadi prioritas untuk diamankan

Pada sesi kuesioner selanjutnya, penulis ingin mengetahui bagaimana tingkat pengetahuan responden terhadap keamanan data pribadi yang mereka miliki. Penulis mengirimkan gambar berupa suatu pesan yang mengatasnamakan salah satu pegawai minimarket yang terkenal di Indonesia, didalamnya, sang pelaku penipuan meminta kode OTP atau kata sandi whatsapp sang korban.

Dari hasil kuesioner didapatkan bahwa mayoritas responden pernah menerima pesan serupa pada aplikasi kirim pesan maupun media sosial yang mereka miliki (56%), sisanya tidak pernah menerima pesan serupa (44%).

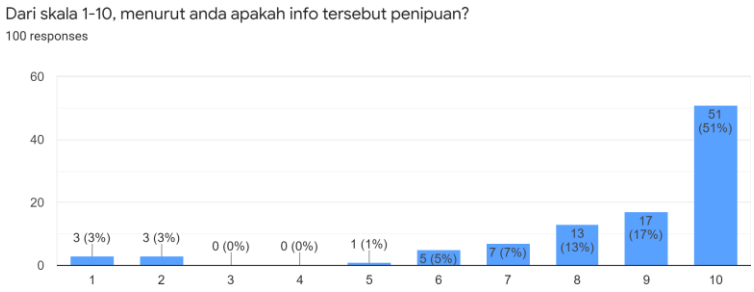


Gambar 3.7 Penipuan melalui *messaging app*,
Sumber: https://kumparan.com/kumparantech/waspada-penipuan-minta-kode-voucher-game-kasir-indomaret-tulisan-thailand-1v4ZvwlH0rE



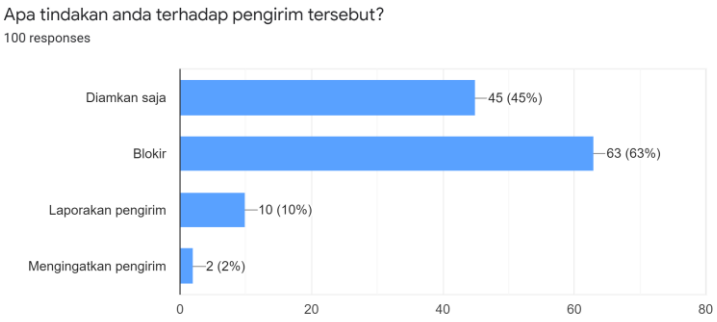
Gambar 3.8 Diagram Jumlah responden yang pernah menerima pesan serupa

Kemudian penulis menilai pendapat, serta mengukur tingkat keyakinan para responden apakah pesan tersebut merupakan penipuan atau modus pencurian data. Penuli memberikan opsi skala 1-10 (1 = sangat tidak yakin penipuan, dan 10 = sangat yakin penipuan). Ditemukan bahwa rata-rata responde menilai bahwa pesan tersebut merupakan penipuan atau modus pencurian data.



Gambar 3.9 Diagram tingkat keyakinan responden terhadap pesan mencurigakan

Selanjutnya, penulis ingin mengetahui bagaimana tindakan para responden bila mendapatkan pesan serupa, dan mayoritas masyarakat memilih untuk memblokir pelaku (63%), selain itu banyak juga dari responden yang mendiamkan pesan tersebut (45%), dan hanya dua (2%) responden yang memiliki kesadaran untuk melakukan tindakan lebih lanjut untuk mengingatkan pelaku penipuan tersebut. Responden juga dinilai kurang memiliki inisiatif untuk melaporkan pelaku, hanya sekitar (10%) responden saja yang memilih untuk melapor.



Gambar 3.10 Diagram tindakan responden terhadap pesan mencurigakan

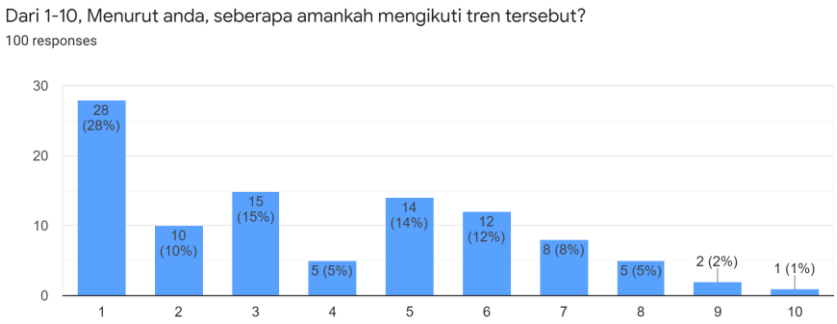
Selanjutnya, penulis juga membahas mengenai tren yang sempat meramaikan media sosial pada akhir tahun 2021 yang lalu, dimana tren tersebut berpotensi untuk dijadikan modus oleh pelaku pencurian data. Penulis memberikan penjelasan mengenai tren tersebut dan ingin mengetahui apakah responden pernah melihat tren serupa.

Dari hasil kuesioner ditemukan, sebagian besar responden pernah melihat tren tersebut pada media sosialnya (83%), dan hanya (17%) responden yang belum pernah melihat tren tersebut. Hal tersebut menandakan paparan tren tersebut terhadap responden atau target audiens sangatlah besar dan cukup popular.

Gambar 3.11 Tren "show your" pada instagram, menjadi modus baru pencurian data, Sumber: https://kabartegal.pikiran-rakyat.com/news/pr-933078650/viral-fitur-stiker-add-yours-di-instagram-berpotensi-bocorkan-data-hati-hati-penipuan

Gambar 3.12 Diagram Jumlah responden yang pernah melihat tren tersebut

Kemudian, penulis ingin mengetahui tingkat kepercayaan responden terhadap keamanan dalam mengikuti tren tersebut. Dari skala 1-10, sebagian besar responden menganggap tren tersebut tidak aman untuk diikuti dengan memilih skala satu, dengan presentase (28%). Hanya sebagian kecil responden yang meyakini tren tersebut sangat aman untuk diikuti, yaitu satu orang yang memilih skala sepuluh, dan dua orang yang memilih skala sembilan.

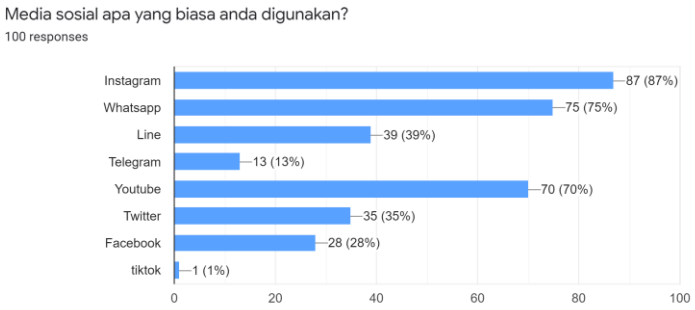


Gambar 3.13 Diagram tingkat keyakinan responden terhadap keamanan mengikuti tren "*show your*" pada instagram

Pada tahap selanjutnya, penulis ingin mengetahui media yang paling sering digunakan oleh responden dalam menemukan informasi terbaru. Hampir seluruh responden menemukan informasi-informasi baru melalui media sosial (91%), disusul dengan website (6%), dan (3%) lainnya melalui seminar dan televisi.

Gambar 3.14 Diagram media yang paling sering digunakan untuk menemukan informasi baru

Sosial media yang digunakan oleh responden cukup beragam, dan yang paling banyak digunakan adalah instagram dengan presentase (87%), disusul dengan whatsapp (75%), kemudian youtube (70%).



Gambar 3.15 Diagram Media Sosial yang Biasa Digunakan Responden

3.1.1.2 Kesimpulan Kuesioner

Berdasarkan uraian dari hasil kuesioner diatas, penulis mendapatkan kesimpulan, yaitu pertama, mengenai tingkat pengetahuan responden terhadap data pribadi, mayoritas responden sudah mengetahui tentang data pribadi, namun pengetahuan tersebut tudak didukung dengan tindakan yang tepat, meskipun masyarakat telah memprioritaskan beberapa data pribadi mereka untuk dilindungi, namun masyarakat masih kurang selektif dan sering membagikan data pribadi tersebut, seperti data lokasi/GPS dan nomor ponsel, serta data-data pribadi lainnya. Sehingga kemungkinan pencurian data pribadi masih cukup besar.

Untuk keamanan data pribadi, Dari pertanyaan-pertanyaan yang menyangkut hal tersebut, disimpulkan bahwa responden sering terpapar modus-modus pencurian data yang beragam bentuknya, mulai dari pesan melalui messaging apps maupun media sosial, juga melalui tren-tren yang sedang viral. Pada dasarnya responden sudah dapat melihat potensi pencurian data ketika menggunakan media sosial maupun internet secara umum, namun hal tersebut belum didukung tindakan responden, responden belum menghayati pengetahuan tersebut dan belum memiliki tingkat inisiatif yang besar

untuk bertindak lebih lanjut terhadap pihak-pihak yang mengancam keamanan data pribadi seseorang.

Mengenai pencarian informasi terbaru, responden cenderung menggunakan media sosial seperti instagram, whatsapp, dan youtube, dibandingkan media lainnya seperti televisi, radio, maupun media cetak seperti koran dan majalah. Media tersebut pula yang paling berpotensi mengalami kebocoran data, karena sifatnya yang terbuka dan dapat digunakan oleh siapa saja.

3.1.2 Metode Kualitatif

Menurut (Sugiyono, 2012). Metode kualitatif merupakan metode pengumpulan data untuk meneliti kondisi suatu objek alamiah, dimana peneliti menjadi instrumen dalam penelitian itu sendiri.

3.1.2.1 Wawancara

Esterberg dalam (Sugiyono, 2015), menjelaskan bahwa wawancara merupakan kegiatan dimana dua orang bertemu dan saling bertukar informasi dan ide dengan melakukan tanya jawab, dimana kegiatan tersebut dapat menghasilkan suatu kesimpulan mengenai topik tertentu. Wawancara yang dilakukan penulis dilakukan kepada 3 narasumber yang masing-masingnya merupakan ahli pada bidangnya. Berikut penjabaran hasil dari wawancara yang telah dilakukan penulis:

1) Wawancara kepada Ahli Media

Penulis mewawancarai Charles Tjung sebagai *Creative Director* di Rubicube Creative. Wawancara dilakukan untuk mengetahui bagaimana membuat sebuah *campaign* menjadi lebih efektif dan sesuai dengan audiens yang ditargetkan, serta media kampanye yang sesuai dengan target audiens. Wawancara tersebut dilakukan pada tanggal 10 April 2022 pukul 20.00 WIB, dan dilakukan secara daring, melalui situs Google Meet.

Gambar 3.16 Wawancara kepada Charles Tjung

Dari wawancara tersebut penulis mendapatkan beberapa jawaban yang dapat membantu penulis untuk merancang kampanye yang sedang dibuat. Charles berpendapat bahwa kampanye tidak lepas dari branding, dan kunci utama dari perancangan kampanye yang efektif adalah brand story dari kampanye tersebut, masyarakat biasanya ingin tahu alasan dibalik perancangan kampanye tersebut.

Dan dalam penyampaian cerita atau *brand story* tersebut, kita harus bisa menempaatkan posisi kita di tengah target audiens kita (*positioning*) dengan tepat. hal pertama yang harus dilakukan sebelum melakukan *positioning* adalah memiliki pengetahuan yang mendalam terhadap target market yang dituju.

Menurut Charles, target market kampanye sosial yang merupakan anak muda (Gen Z) dan hidup di perkotaan, biasanya merupakan orang-orang yang sudah melek digital, dan generasi ini (Gen Z), biasanya lebih *awake* secara sosial, dimana mereka cenderung lebih terlibat dalam *community* dan cenderung ingin ikut serta terjun langsung (*taking action*) bersama-sama dalam menghadapi suatu permasalahan sosial. Untuk itu penyampaian pesan kampanye kepada Gen Z dapat lebih dilakukan secara digital serta lebih melibatkan dirinya, bukan hanya sebagai *audiens*, namun juga sebagai bagian dari kampanye tersebut (*part of the campaign*). Kita

bisa mencapai hal itu dengan membuat kampanye lebih interaktif dan memberikan ruang kepada audiens untuk mengambil aksi.

Bila membicarakan penyampaian *brand story* kita sebagai perancang kampanye (brand/ lembaga) dan menentukan posisi kita diantara target audiens Gen Z, kita disarankan bukan lagi membicarakan seperti apa jati diri kita atau tidak lagi membicarakan tentang diri kita, namun membicarakan alasan kuat yang dapat diterima mengenai kenapa kampanye tersebut dilakukan, dan menunjukan bahwa kita memiliki kepedulian terhadap komunitas atau masyarakat melalui kampanye tersebut. Dalam kasus kampanye ini, kita dapat menempatkan diri kita sebagai pihak yang benar-benar khawatir dan peduli mengenai keamanan data pribadi masyarakat, dan kita harus menunjukannya dengan jelas.

Selain itu, Charles menjelaskan bahwa dalam penyampaian pesan kita juga harus memikirkan teknik komunikasinya, seperti bahasa yang digunakan, konten seperti apa, dsb. Teknik komunikasi harus disesuaikan dengan target audiensnya dan bertujuan agar pesan yang disampaikan mudah di cerna dan dimengerti oleh audiens. Dalam penyampaian pesan kepada Gen Z, kita tidak cukup hanya menyampaikan pesan secara *straight forward* atau blak-blakan, Gen Z cenderung tidak tertarik dengan cara penyampaian seperti itu.

Charles menambahkan, untuk mencari tahu teknik komunikasi apa yang efektif dalam menyampaikan informasi ke Gen Z, kita dapat melihat referensi dari *brand* dan konten apa yang sering dikonsumsi oleh generasi tersebut, serta siapa figur yang menjadi panutan dan diidolakan, bagaimana sifat, watak, bahasa dan cara berbicara orang tersebut. Sehingga dapat kita jadikan acuan untuk cara penyampaian informasi dan komunikasi dalam perancangan kampanye sosial kita. Salah satu contoh yang diberikan Charles adalah *brand* Gojek, dimana *brand* tersebut sangat dekat dengan generasi Z. Gojek selalu berusaha menempatkan dirinya dalam kehidupan sehari-hari target audiensnya,

gojek menyampaikan pesan secara persuasif dan membahas perannya dalam kehidupan sehari-hari masyarakat. Gojek juga sering menggunakan komedi receh dalam menyampaikan pesan, hal tersebut dikarenakan kalangan Gen Z menyukai dan sering mengonsumsi konten-konten receh.

Ketika ditanya mengenai media seperti apa yang efektif untuk berkampanye kepada Gen Z, Charles berpendapat media digital lah yang paling sesuai, karena Gen Z sangat aktif dalam penggunaan media tersebut, khususnya sosial media. Charles menjelaskan bahwa hal tersebut sudah terbukti dari beberapa survey yang telah dilakukan.

2) Wawancara kepada Ahli Hukum

Penulis juga mewawancarai Normand Edwin sebagai praktisi hukum dan advokat yang salah satunya menangani persoalan hukum teknologi, Edwin juga memiliki latar belakang reporter dan bekerja di bagian redaksi hukumonline.com. Wawancara dilakukan untuk mengetahui lebih dalam mengenai perlindungan data pribadi, dan bagaimana regulasinya di Indonesia. Sehingga dapat memperkuat urgensi dan menemukan materi untuk disampaikan ke masyarakat mengenai perlindungan data pribadi. Wawancara tersebut dilakukan pada tanggal 18 April 2022 pukul 16.00 WIB, dan dilakukan secara daring, melalui situs Google Meet.

Gambar 3.17 Wawancara kepada Normand Edwin

Ketika ditanya mengenai data pribadi, Edwin terlebih dahulu menjelaskan mengenai kepentingan untuk melindungi data pribadi. Edwin menjelaskan bahwa beberapa pakar hukum yang menyusun mengenai konsep data pribadi mengatakan bahwa data pribadi sangat berkaitan dengan hak asasi manusia, hak individu atau hak privasi, dan hak asasi manusia secara sosial disepakati harus dihormati dan dilindungi, untuk itu diperlukan suatu hukum untuk mengaturnya.

Namun Edwin menjelaskan adanya persoalan bila membicarakan apa itu data pribadi, karena tidak ada kesepakatan bersama di seluruh dunia yang membahas apa saja yang termasuk data pribadi, terkecuali di Eropa yang merupakan gabungan dari beberapa negara dan telah memiliki persetujuan mengenai apa itu data pribadi, pertsetujuan tersebut terdapat pada *General Data Protection Regulation* (GDPR). Dengan adanya persetujuan tersebut, mereka dapat lebih mudah membuat regulasi terhadap perlindungan data pribadi. Namun, di negara lain seperti, contohnya Amerika Serikat, mereka memiliki batasan definisi yang berbeda. Sehingga hal ini menjadi isu yang sering dibahas oleh para ahli hukum. Sehingga dapat dikatakan bahwa data pribadi memiliki keberagaman konsep di seluruh dunia, namun dalam penelitian dan riset yang dilakukan oleh Elsam, konsep data pribadi memiliki ciri dasar yang serupa di seluruh dunia, yaitu mengacu pada "segala informasi mengenai individu, untuk mengidentifikasi dirinya", namun batasannya tetap berbeda-beda di seluruh dunia. Definisi ini penting karena berhubungan dengan regulasi hukum.

Selanjutnya kenapa data pribadi dianggap penting untuk dilindungi, selain karena merupakan hak seseorang (kemanusiaan dan privasi) seperti yang sudah dijelaskan sebelumnya. Data pribadi juga penting dilindungi karena hal tersebut sangat berkaitan dengan keamanan seseorang. Hal tersebut dikarenakan data pribadi yang memang secara fungsi untuk mengidentifikasi seseorang, biasa

digunakan untuk mengakses fasilitas-fasilitas digital, yang seharusnya hanya pemilik data pribadinya saja yang bisa mengakses (fungsinya seperti kunci). Hal ini menjadi penting karena bila data tersebut diperoleh oleh orang lain, dapat digunakan untuk mengakses data kita yang tak seharusnya diakses orang lain. Pada akhirnya hal ini berkaitan erat dengan hak-hak dasar lainnya seperti hak harta benda, hak keselamatan jiwa, hak untuk untuk tidak diketahui mengenai kehidupan pribadnynya, dsb. Itulah mengapa perlindungan data pribadi sangat penting untuk diregulasi.

Perlindungan data pribadi di Indonesia sendiri sebenarnya sudah ada regulasinya, namun peraturan tersebut masih tersebar dan tidak satupun dari peraturan yang ada menggunakan definisi yang sama mengenai apa itu data pribadi. Regulasi peraturan tersebut paling tidak diatur dalam 32 Undang-undang yang memuat perlindungan data pribadi. Peraturan yang tersebar ini dirasa tidak cukup untuk melindungi data pribadi masyarakat Indonesia, hal ini tidak sejalan dengan perkembangan dunia teknologi dan digital yang semakin kompleks di Indonesia. Contohnya, dahulu e-mail tidak dianggap penting sebagai data pribadi, namun saat ini alamat e-mail telah digunakan untuk mengakses layanan-layanan digital lainnya, seperti registrasi akun media sosial, aplikasi, atau proram lainnya, dan bila alamat e-mail tersebut jatuh ditangan pihak yang tidak bertanggung jawab akan berbahaya dan disalahgunakan.

Selain dampak buruk yang dirasakan masyarakat, negara juga mengalami kerugian akibat terhambatnya bisnis dan kerjasama antar negara, karena negara yang sudah teregulasi dengan baik perlindungan data pribadinya, misalnya saja negara Eropa, mereka tidak ingin melakukan kerjasama maupun bisnis dengan Indonesia, karena khawatir atas keamanan data yang mereka miliki bila bekerja sama dengan Indonesia. Sehingga semua negara dituntut untuk memiliki perlindungan data pribadi yang kuat untuk menjalankan

kerjasama antar negara. Untuk itu peraturan tersebut sangat penting untuk diregulasi dalam suatu Undang-undang khusus, guna memperkuat perlindungan hukum data pribadi di Indonesia, dan bila terdapat permasalahan, jelas bagaimana cara menanganinya.

Edwin menjelaskan bahwa pembangunan atau perancang peraturan perundang-undangan didasari dari dua faktor, yaitu munculnya permasalahan secara nyata, dan faktor kedua adalah prediksi atau perhitungan mengenai permasalahan yang akan muncul di masa mendatang. Dua pendekatan tersebut berlaku dalam semua perancangan dan penegakan hukum dimana saja. Perancangan tersebut merupakan tanggung jawab masyarakat dan pemerintah melalui lembaga-lembaga tertentu. Dari pihak pemerintah, yang bertanggung jawab adalah pemerintah eksekutif dan pemerintah di parlemen. Lembaga yang paling dekat dengan isu tersebut adalah Kementerian Komunikasi dan Informasi, sebagai tangan panjang presiden, kementerian ini mengatur dan mengelola segala urusan perteknologian informasi dan komunikasi di Indonesia. Selanjutnya adalah DPR. Hukum kita dibuat di DPR bersama-sama dengan eksekutif yaitu kekuatan presiden beserta para pembantunya. Sedangkan peran masyarakat adalah untuk mendorong dan memberi penekanan kepada pemerintah mengenai isu-isu tersebut.

Mengenai permasalahan pencurian ataupun penyalahgunaan data pribadi, saat ini memang sudah ada rencana dari pemerintah, namun masih berupa Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP). RUU tersebut masih belum disahkan sampai saat ini, dan masih ditunda-tunda, padahal RUU PDP memiliki peran penting dalam meregulasi perlindungan data pribadi masyarakat, karena akan memudahkan proses dan penindakan pelanggaran terhadap data pribadi masyarakat.

Hambatan pengesahan ini disebabkan oleh kesadaran masyarakat dan pemerintah yang dinilai masih kurang, dan masih

mengesampingkan urgensi untuk pengaturan dan meregulasi perlindungan data pribadi, hal ini dapat dilihat dari politisi di parlemen yang masih belum semuanya satu frekuensi dalam perlindungan data pribadi, ini menyangkut permasalahan sosial. Selanjutnya faktor kesadaran masyarakat umumnya. Contohnya saja permasalahan kekerasan seksual yang RUUnya baru saja disahkan, pengesahan RUU ini berhasil dilakukan karena dukungan masyarakat mengenai kekerasan seksual sangatlah besar, masyarakat dinilai memiliki peran penting dan sangat besar untuk menekankan kebijakan-kebijakan pemerintah.

Namun sayangnya penekanan regulasi perlindungan data pribadi masih kurang, isu perlindungan data pribadi belum mendapatkan perhatian yang layak seperti perlindungan kekerasan seksual, padahal urgensinya juga cukup besar karena menyangkut hak asasi manusia dan keamanan masyarakat, dan kejahatan siber terhadap data pribadi dapat terjadi setiap saat dan kepada siapa saja di era yang serba digital, dimana masyarakat selalu berinteraksi dengan penggunaan teknologi digital, bahkan kekerasan seksual dapat terjadi secara digital.

Menurut Edwin ada perbedaan pola pikir masyarakat terhadap kedua isu tersebut, dan hal ini menyebabkan RUU kekerasan seksual berhasil dijalankan sedangkan perlindungan data pribadi masih terhambat. Menurut Edwin RUU kekerasan seksual dapat berhasil dijalankan karena isu tersebut dapat dirasakan secara langsung dan melukai rasa keadilan masyarakat, sedangkan kejahatan terhadap data pribadi tidak dirasakan langsung dampaknya oleh masyarakat, bahakan seringkali masyarakat tidak menyadari mereka sedang menjadi korban kejahatan siber.

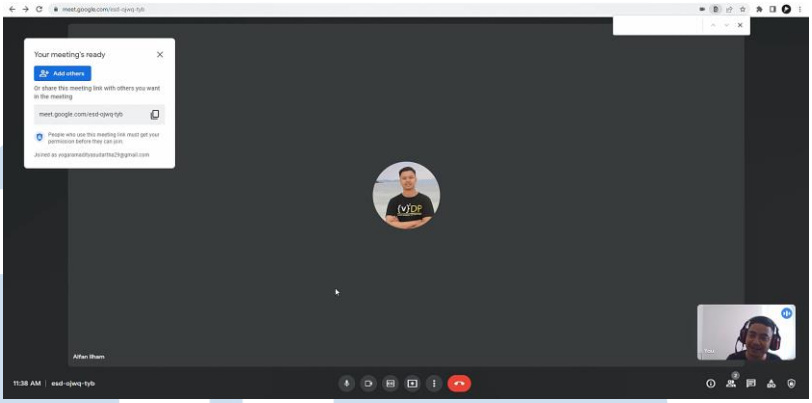
Itulah mengapa Edwin berpendapat bahwa peningkatan kesadaran masyarakat mengenai kejahatan siber dan perlindungan data pribadi itu penting, sehingga dapat mengingkatkan kepedulian

masyarakat terhadap data pribadi yang mereka miliki, dan agar masyarakat yang sudah lebih sadar, dapat terus menekankan pengesahan RUU PDP tersebut sebagaimana RUU kekerasan seksual saat ini.

Edwin menambahkan bahwa kampanye sosial memang penting untuk dilakukan untuk mengatasi permasalahan perlindungan data pribadi secara konkret, karena kampanye tersebut selain dapat menyadarkan masyarakat sehingga mendorong percepatan pengesahan RUU PDP, kampanye juga dapat mengubah *habit* atau prilaku masyarakat, karena bila RUU PDP sudah disahkan dan regulasi sudah berjalan dengan baik, bila tidak dibarengi dengan perubahan *habit* masyarakat, peraturan dan regulasi tersebut akan percuma. Masyarakat harus mengubah *habit* dan kebiasaan mereka untuk melindungi data pribadi yang mereka miliki masing-masing, karena Undang-undang hanya dapat membantu melindungi masyarakat secara hukum.

3) Wawancara kepada Ahli Keamanan Siber

Penulis juga mewawancarai Alfan Ilham sebagai ahli keamanan siber di suatu perusahaan yang tidak disebutkan namanya. Alfin berperan sebagai *red* team, dimana ia melakukan simulasi serangan siber dan mencoba menyerang keamanan perusahaan kliennya, tujuan dari hal tersebut adalah untuk menemukan celah dan kelemahan pada sistem klien untuk nantinya diperbaiki dan ditingkatkan lagi. Wawancara dilakukan untuk mengetahui bagaimana kejahatan siber dilakukan, bagaimana cara menghindarinya, dan mengetahui kondisi keamanan siber di Indonesia saat ini. Wawancara dilakukan pada tanggal 16 Mei 2022 pukul 11.30, melalui Google Meet.



Gambar 3.18 Wawancara kepada Alfan Ilham

Ketika ditanya bagaimana kondisi keamanan siber di Indonesia saat ini, Alfan berpendapat bahwa keamanan siber saat ini di Indonesia mulai disadari kepentingannya oleh para perusahaan-perusahaan besar, dan profesi keamanan siber seperti yang digeluti oleh Alfan saat ini sering dicari. Ketika ditanya mengenai kejahatan siber yang menyerang perseorangan atau pribadi, mengenai kenapa data pribadi rawan dicuri dan apa yang dilakukan oleh para pelaku terhadap data tersebut, Alfan menjelaskan bahwa pelaku kejahatan siber mengambil data pribadi untuk mendapatkan keuntungan, misalnya saja secara finansial, data yang diperoleh dapat digunakan untuk membobol rekening bank dan aplikasi finansial korban.

Menurut Alfin hal ini dapat terjadi karena kesadaran masyarakat Indonesia yang masih rendah terhadap keamanan siber ketika menggunakan internet. Alfin berpendapat bahwa masyarakat belum paham bahwa terkadang tindakan yang mereka lakukan dan dianggap tidak berbahaya, ternyata sangat berbahaya. Masyarakat tidak menyadari bahwa para pelaku kejahatan siber dapat mengumpulkan informasi korban melalui hal-hal yang tidak terduga sama seperti kasus masyarakat menyebarkan informasi pada instagramnya.

Menurut Alfin bentuk kejahatan siber yang paling sering muncul dan menargetkan data pribadi adalah *phising* dan *social engineering*. Alfin memberikan contoh *phising* yang sering terjadi adalah melalui e-mail, dimana seseorang mengirimkan tautan dan ketika dibuka akan mengarahkan ke website yang dibuat menyerupai website legal dan resmi, misalnya saja website pemerintah. Ketika korban memasukan data dirinya pada website tersebut, mereka sudah dicuri datanya. Selanjutnya ia menjelaskan mengenai *social engineering*, Alfan mencotohkan salah satu kasusnya seperti para pengguna aplikasi Shopee yang sering mendapatkan pesan bahwa pihak Shopee membutuhkan data seperti kata sandi para pelanggannya. Selain kedua modus tersebut para pelaku kejahatan juga biasanya pandai merancang suatu program penyusup yang biasa kita kenal sebagai virus, dimana virus tersebut dapat menyusup masuk ke sistem korban ketika korban secara tidak sengaja mengunduh virus tersebut dari internet. Selain membuat program virus, para pelaku kejahatan siber ini juga membuat program yang bisa membobol kata sandi seseorang, ini juga merupakan salah satu cara pelaku mendapatkan data pribadi korbanya.

Dari beberapa modus dan cara para pelaku kejahatan siber mendapatkan data pribadi korbannya, Alfan memberikan beberapa tips untuk menghindarinya. Pertama adalah mengenali perbedaan *phising* dan tautan yang memang berisikan website resmi, cara membedakannya biasanya bisa dilihat dari domainnya.

Untuk menghindari *Social Engineering* Alfin menjelaskan kita bisa mengaktifkan 2FA (*Two factor authentication*) atau otentifikasi dua kali, sehingga ketika kita memberikan kata sandi dan *username* kita kepada pelaku, mereka tidak bisa langsung masuk ke akun kita, karena perlu memasukan kode OTP yang merupakan bentuk dari 2FA, dan kode tersebut hanya bisa didapatkan oleh pemilik akunnya. Kode OTP juga sebaiknya tidak disebarkan kepada siapapun karena

perusahaan atau pihak resmi tidak akan pernah menannyakan Kode OTP maupun kata sandi pelanggannya. Selanjutnya untuk menghindari kata sandi di jebol menggunakan program yang dibuat oleh pelaku kejahatan siber, kita dapat memperkuat kata sandi yang akan sulit ditebak bahkan dengan program tersebut. Kata sandi yang kuat memiliki beragam variasi angka, huruf, dan huruf kapital. Alfan juga menyarankan jangan menggunakan kata sandi yang berhubungan erat dengan kita seperti tanggal jadian, nama hewan peliharaan, dsb. Kemudian kata sandi tersebut harus rutin diganti secara berkala, misalnya saja sebulan sekali. Dan tips terakhir untuk menghindari kejahatan siber yang menargetkan data pribadi adalah menggunakan antivirus, untuk mendeteksi dan menghapus virus yang berpotensi mencuri data pribadi kita.

3.1.2.2 Studi Literatur

Untuk memperkuat data mengenai perlindungan data pribadi di internet, penulis menggunakan metode studi literatur atau yang sering dikenal sebagai studi pustaka.

1) Data Pribadi

Menurut Permenkominfo Pasal 1, ayat (1) No.20 tahun 2016 tentang (Perlindungan Data Pribadi Dalam Sistem Elektronik, 2016). Data pribadi merupakan suatu data tertentu milik perseorangan yang selalu dijaga kebenarannya, disimpan, dirawat, dan dijaga kerahasiaannya. Sedangkan Kamus Besar Bahasa Indonesia (KBBI), mengertikan data pribadi sebagai data yang sesuai dengan ciri seseorang, misalnya nama, usia, pekerjaan, dsb.

Definisi lain juga datang dari Peraturan Perlindungan data di Inggris. Pasal 1, ayat (1) Data Protection Act Inggris tahun 1998, mengatakan bahwa data pribadi merupakan data yang

berhubunga dengan individu yang dapat diidentifikasi melalui data, atau informasi yang dimiliki oleh pemegang data.

Menurut RUU Perlindungan data pribadi, data pribadi dapat dibagi menjadi dua pengelompokan (Pasal 3, ayat (1-3) RUU Perlindungan Data Pribadi), yaitu Data bersifat umum dan spesifik:

a) Data pribadi bersifat umum

- Nama lengkap
- Jenis kelamin
- Kewarganegaraan
- Agama
- Kombinasi Data Pribadi untuk mengidentifikasi seorang individu

b) Data pribadi bersifat spesifik

- Informasi kesehatan
- Data biometrik
- Data Genetika
- Orientasi dan kehidupan seksual
- Pandangan politik
- Catatan pidana
- Data anak
- Data keuangan pribadi
- Data lainnya sesuai dengan peraturan UU

2) Hukum dan Regulasi Perlindungan Data Pribadi di Indonesia

Peraturan perlindungan atau regulasi terkait perlindungan data pribadi di Indonesia masih bersifat terpisah di dalam Undang-Undang, belum ada aturan khusus yang mengatur mengenai perlindungan data pribadi itu sendiri. Saat ini peraturan khusus tersebut masih berupa Rancangan Undang-undang Perlindungan

Data Pribadi (RUU PDP). Sehingga regulasi perlindungan data pribadi yang ada saat ini masih berbentuk Peraturan Kementrian Kominfo (Permenkominfo), Undang-undang Informasi dan Transaksi Elektronik (UU ITE).

Dalam peraturan kementrian. Permenkominfo Pasal 2, ayat (1) No.20 tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, Perlindungan data pribadi dalam sistem elektronik termasuk perlindungan terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilanm pengumuman, pengiriman, penyebarluasan, dan pemusnahan susatu data pribadi.

Dasar hukum perlindungan data pribadi di Indonesia saat ini, secara umum telah dibahas dalam Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang kini telah mengalami perubahan yang ditulis dalam Undang-Undang No.19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Di dalamnya dibahas mengenai tindakan yang melanggar UU terkait perlindungan data pribadi (Pasal 27-37).

Kepastian hukum pengguna internet mengenai perlindungan data pribadi yang mereka miliki terdapat pada Pasal 30 UU ITE. Perlindungan tersebut melindungi data pribadi bila terdapat pihak yang sengaja maupun tidak sengaja mengakses data milik orang lain untuk melakukan perbuataan yang melawan hukum.

3) Kejahatan Siber *(Cybercrime*)

Kejahatan siber atau sering disebut dengan *cybercrime*, adalah bentuk kejahatan yang dilakukan dengan mengunakan media internet. Setiap kegiatan ilegal dan melawan hukum, yang dilakukan secara *online* atau menggunakan koneksi internet biasanya disebut sebagai kejahatan siber. Ada pula definisi kejahatan siber menurut para ahli, yaitu sebagai berikut:

- **Parker**

  Parker mendefinisikan kejahatan siber sebagai tindakan kejahatan dan kejadian yang merugikan seseorang atau pihak tertentu, dan berkaitan dengan teknologi komputer

- **Wahid & Labib**

  Wahib dan Labib mendefinisikan kejahatan siber sebagai penyalahgunaan teknologi digital, dengan pemakaian jaringan dan teknologi komputer untuk melakukan tindakan kriminal.

- **Widodo**

  Widodo mendefinisikan kejahatan siber sebagai kegiatan seseorang atau kelompok yang menggunakan jaringan dan teknologi komputer sebagai media untuk melakukan kejahatan dan menargetkan komputer seseorang sebagai target sasarn.

  Dalam Undang-Undang No. 19 Tahun 2016 mengenai Informasi Transaksi Elektronik (UU ITE), dijelaskan bahwa kejahatan siber dikategorikan sebagai tindakan yang terlarang.

  a) Pelaku Kejahatan Siber

  Pelaku kejahatan siber adalah seseorang maupun kelompok yang memiliki kemampuan tinggi dalam ilmu teknologi digital dan komputer, mereka biasanya menguasai ilmu *programming* komputer dan dapat membuat *script* atau kode program yang bersifat merusak seperi *malware* dan virus, mereka mampu menganalisa bagaimana sistem komputer dan jaringan bekerja, dan menemukan celah pada sistem tersebut. Mereka menggunakan kemampuan tersebut untuk melakukan kejahatan dengan memanfaatkan kelemahan yang mereka temukan, kejahatan tersebut dapat berupa perusakan sistem atau pencurian data dari korbannya.

  Pelaku kejahatan siber juga biasanya mempunyai kemampuan *social engineering* atau dalam bahasa Indonesia disebut dengan rekayasa sosial, Dengan kemampuan

tersebut, pelaku dapat memanipulasi psikologi korban dan mengksploitasi kesalahan korban untuk mencuri data pribadi korban.

b) Jenis-jenis kejahatan siber

Ada banyak jenis dan bentuk dari kejahatan siber, berikut merupakan jenis kejahatan siber yang umum ditemukan dalam penggunaan internet sehari-hari:

(1) Akses Ilegal/ Tanpa izin

Akses tanpa izin, atau yang biasa disebut *unauthorized access* merupakan kejahatan digital dimana pelaku menyusup masuk kedalam sebuah sistem secara tidak sah dan tanpa izin dari pemilik sistem.

(2) Pencurian data & informasi

Pencurian data dan informasi dilakukan oleh pelaku untuk memperoleh keuntungan pribadi baik materil dan immateril. Pelaku melakukannya dengan berbagai cara, bisa dengan melakukan penipuan, mengakses sistem komputer korban tanpa sepengetahuannya, hingga menggunakan program ilegal yang disebarkan dan digunakan oleh korban.

(3) Penipuan

Penipuan merupakan kegiatan dimana pelaku mengelabui korban untuk mendapatkan keuntungan pribadi, hal ini masih berkaitan dengan kejahatan siber pencurian data. Pelaku biasanya menggunakan kemampuan rekayasa sosial atau *social engineering* terhadap korban. Rekayasa sosial sendiri merupakan teknik yang dapat mempengaruhi psikologi korban, agar korban dapat memberikan data, informasi atau hal-hal penting lainnya kepada pelaku.

(4) Konten Ilegal

Konten ilegal merupakan kejahatan dimana pelaku menyebarkan atau memasukan data dan informasi mengenai

hal-hal yang tidak baik, etis, dan mengganggu ketertiban publik ke internet. Beberapa contoh yang termasuk konten ilegal adalah pornografi, berita bohong atau *hoax*, fitnah, konten sadis, dan rahasia negara.

(5) Pemalsuan Data & Identitas

Kejahatan ini dilakukan dengan memasukan data palsu kedalam dokumen penting di internet. Biasanya dokumen ini disimpan oleh suatu institusi yang sudah menggunakan penyimpanan data menggunakan web.

(6) Perusakan Sistem

Perusakan sistem biasanya dilakukan oleh pelaku dengan menyebarkan program-program yang telah dirancang untuk merusak sistem komputer korban, program tersebut dapat berupa virus, trojan, worm, dsb. Ketika korban membuka program tersebut, program tersebut akan bekerja tanpa sepengetahuan pemilik sistem. Kerusakan yang ditimbulkan bisa berupa kerusakan kecil, memperlambat sistem komputer, hingga membuat sistem komputer tidak dapat digunakan samasekali.

(7) Teror Siber

Teror siber atau *cyber terrorism* adalah kejahatan dimana pelaku melakukan pengancaman pada suatu negara atau seseorang. Pelaku biasanya mengancam korbannya dengan ancaman yang cukup berat, dan bahkan dapat membahayaka nyawa korbannya.

(8) Pelanggaran Privasi

Pelanggaran privasi merupakan tindakan dimana pelaku mengakses suatu data yang bersifat pribadi dan rahasia, dan melanggar hak-hak pemilik data yaitu untuk tidak diketahui dan diganggu mengenai kehidupan pribadinya.

(9) Pelanggaran Hak Kekayaan Intelektual

Pelaku kejahatan ini biasanya melakukan tindakan yang melanggar hak kekayaan intelektual seseorang, seperti meniru tampilan suatu situs *website* milik seseorang secara ilegal.

(10) *Cyberbullying*

Cyberbullying adalah perundungan dan penindasan yang dilakukan melalui teknologi digital. Biasanya *cyberbullying* terjadi di sosial media, dalam *onlune games*, dan layanan *chatting* lainnya. Dalam penindasan ini biasanya ada perbedaan kuasa antara pembuli yang merasa kuat dan korban yang lebih lemah. Pembulian secara *online* biasanya dilakukan secara verbal dan berpengaruh kepada mental korban.

(11) Pencemaran Nama Baik

Pencemaran nama baik secara *online* dilakukan dengan menyebarkan informasi buruk mengenai seseorang, dan hal tersebut dapat merusak reputasi dam harga diri korbannya.

4) Buku Privasi Dan Perlindungan Data Pribadi oleh Kominfo dan Siber Kreasi

Penulis melakukan studi literatur guna menambahkan data dan informasi, studi dilakukan kepad Buku Privasi Dan Perlindungan Data Pribadi, hasil kolaborasi Kominfo dan Siber kreasi. Didalam buku ini dibahas mengenai pelanggaran privasi di Internet, melindungi data pribadi di internet, hingga pengaturan privasi di media sosial.

Gambar 3.19 Sampul Buku Privasi Dan Perlindungan Data Pribadi
Sumber: https://literasidigital.id/books/privasi-perlindungan-data-pribadi/ (2018)

c) Pelanggaran Privasi di Internet

Sering tidak disadari oleh kitam bahwa kita telah membagikan data pribadi kita ataupun teman kita di internet, khususnya di media sosial, hal tersebut merupakan salah satu pelanggaran privasi di internet. Tidak hanya itu, penyedia layanan seperti aplikasi media sosial itu sendiri dapat melakukan pelanggaran privasi penggunannya dengan memberikan data kita kepada pihak ketiga.

Contoh lain kasus pelanggaran privasi di internet adalah:

(1) Ketika menggunakan facebook, menandai teman pada suatu *post*, baik tulisan, tautan web, atau foto dan video, bila tanpa izin orang yang bersangkutan maka dapat dikategorikan sebagai pelanggaran privasi orang tersebut.

(2) Penyebaran foto pribadi dan keluarga seseorang di media sosial tanpa perizinan yang bersangkutan juga dikategorikan sebagai pelanggaran privasi.

(3) Penyediaan layanan transportasi online biasanya memberikan fitur untuk saling melihat nomor telepon mitra dan pelanggannya, hal tersebut seharusnya hanya digunakan ketika transaksi sedang berlangsung, namun ketika digunakan diluar proses tersebut, dapat menjadi pelanggaran hak privasi.

(4) Seringkali kita menemukan di *group* aplikasi seperti whasapp, seseorang memasukan orang lain kedalam group tersebut tanpa izin sebelumnya, sehingga nomor telepon orang tersebut dapat tersebar didalam group tanpa izin pemiliknya.

(5) Segala bentuk peretasan atau pencurian data pada media sosial yang sering terjadi

b) Melindungi Data Pribadi di Internet

Menurut buku ini, ada beberapa hal penting yang perlu diperhatikan dalam menjaga keamanan data pribadi yang dimiliki seseorang, yaitu:

(1) Gunakan kata sandi yang sulit untuk akun yang digunakan di internet, misalnya e-mail, media sosial, aplikasi, *marketplace*, dan sebagainya. Hindari pasword yang mudah ditebak dan berhubungan dengan data pribadi lainnya seperti alamat, tanggal lahir, nama orang tua, tempat bersekolah, dsb. Serta rutin mengganti kata sandi secara berkala (misalnya dua bulan sekali)

(2) Untuk memperkuat keamanan kata sandi, lebih baik jika kita juga menggunakan kata sandi yang berbeda pada setiap akun. Sehingga bila terdapat salah satu akun kita yang diretas, tidak akan membuat akun yang lain mudah diretas.

(3) Hal penting lainnya adalah jangan membagikan informasi, khususnya data pribadi di media sosial, karena data kita berpotensi dimanfaatkan oleh pihak yang tidak bertanggung jawab.

(4) Perhatikan alamat URL dari situs yang akan dikunjungi, termasuk ketika sedang berbelanja secara daring. Jangan sampai kita membuka URL palsu dan terjebak masuk kedalam situs yang dapat mencuri data pribadi kita.

(5) Ketika menerima tautan atau *link* suatu situs web, baik melalui e-mail, pesan singkat, dan lainnya, periksa kembali terlebih dahulu jika tautan tersebut merupakan tautan untuk website yang dituju, bukan situs web yang bermaksud melakukan *phising*.

(6) Jika ingin meng*install* suatu aplikasi baru pada perangkat atau gawai kita, perhatikan akses apa saja yang diminta oleh aplikasi tersebut. Jangan sampai lalai dan membiarkan aplikasi tersebut mengakses data pribadi kita yang tidak dibutuhkan dalam penggunaan aplikasi tersebut.

(7) Selalu berhati-hati ketika menggunakan Wi-Fi di publik atau tempat umum, hal ini dapat menjadi jalur masuk pencuri data ke perangkat kita. Ketika menggunakan Wi-Fi umum diusahakan untuk tidak membagikan data penting apalagi melakukan transaksi keuangan (memasukan kartu kredit, bertransaksi dengan menggunakan *e-banking*, dsb.)

(8) Langkah berikut tidak kalah penitng, butuh kesadaran diri untuk mengatur pengaturan privasi di setiap akun media sosial yang digunakan, batasi siapa yang dapat mengakses profil dan *posting*an kita.

(9) Dan yang terakhir selalu menjaga dan menghargai privasi orang, jangan membagikan data pribadi seseorang tanpa izin orang tersebut.

c) Mengatur Pengaturan Privasi di Media Sosial

(1) Facebook

Di Facebook, kita diberikan *tools* dalam pengaturan privasi untuk mengatur siapa saja yang dapat melihat postingan kita, siapa saja yang dapat mengirimkan pertemanan kepada kita, siapa saja yang dapat melihat profil kita, dsb. Kita juga dapat mengatur terkait siapa yang bisa mem*posting* pada linimasa

kita, mengatur bagaimana seseorang menandai kita (*tagging*), dan sebagainya.

(2) Instagram

Di Instagram, kita dapat mengatur pengaturan privasi kita seperti apakah *posting*an kita dapat dilihat publik atau hanya pengikut kita saja, selanjutnya kita dapat mengatur akun yang diblokir, hal ini berguna untuk memastikan akun-akun tertentu yang telah kita blokir agar tidak dapat melihat segala konten dari akun kita, dan tidak dapat mengirim pesan. Kemudian ada pengaturan starus aktivitas, dimana kita dapat mengatur bila ingin menunjukan atau tidaknya status aktif kita kepada pengguna lain, dan yang terakhir pengaturan komentar, dimana kita dapat mengatur siapa yang dapat memberikan komentar pada *posting*an kita.

(3) Youtube

Di Youtube, pengguna dapat mengubah setelan privasi video yang kita bagikan dan mengelola akses penayanganm sehingga kita dapat menentukan pada siapa video kita ingin ditampilkan, misalnya untuk publik, artinya video tersebut dapat dilihat dan dibagikan oleh siapa saja, kemudian tidak publik, artinya video kita hanya bisa dilihat dan dibagikan oleh siapa saja yang memiliki tautan dari video kita, dan yang terakhir adalah pengaturan pribadi, dimana video tersebut hanya dapat di lihat oleh pengguna yang dipilih.

5) Siberpedia Panduan Pintar Keamanan Siber oleh Azrina Darmayani

Dalam buku ini Azrina mengulas mengenai pentingnya keamanan di bidang siber, khususnya di Indonesia. Selain itu, buku ini membahas bagaimana cara mengamankan data tersebut, dengan menggunakan bahasa yang sederhana, sehingga mudah dimengerti oleh pembaca awam. Dengan

banyaknya masyarakat yang sadar melalui buku ini, diharapkan tumbuh budaya keamanan siber yang baik di Indonesia.

Gambar 3.20 Sampul Buku Siberpedia

Sumber: https://literasidigital.id/books/siberpedia-panduan-pintar-keamanan-siber-2/ (2018)

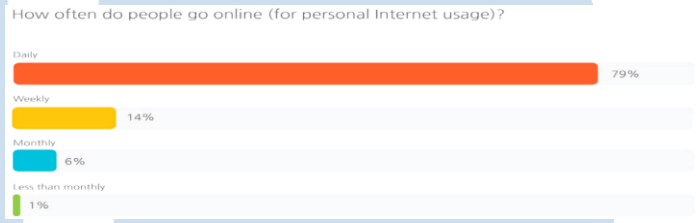
a) Asal Mula Pentingnya Keamanan Siber

Seiring perkembangan teknologi, muncul banyak kesempatan dan juga tantangan yang dihadapi oleh para penggunanya. Menggunakan internet masih sering dianggap sebagai kegiatan yang aman dan jauh dari resiku tindak kejahatan ketika kita belum pernah mengalami sendiri dan menjadi korban dari tindak kejahatan tersebut. Namun bila sudah berhadapan dengan masalah tersebut, kita dapat menyadari seberapa besar kekuatan sistem komputer saat ini. Oleh karenanya, dalam mengikuti perkembangan teknologi tersebut, diperlukan pemahaman bagaimana menggunakan sistem operasi tersebut dengan tepat, agar menciptakan dunia siber yang dapat kita kendalikan, bukan kita yang dikendalikan oleh teknologi tersebut.

(1) Internet dan gaya hidup baru di Indonesia

Perkembangan dunia teknologi dan komunikasi yang pesat di Indonesia, merupakan salah satu dampak besar yang disebabkan oleh globalisasi. Hal tersebut juga berpengaruh terhadap gaya hidup masyarakat Indonesia yang semakin

akrab dengan teknologi. Hal tersebut didukung oleh data dari (Google Consumer Barometer, 2015), di dalam survey tersebut dikatakan bahwa 79% pengguna internet di Indonesia menggunakan internet dalam frekuensi yang cukup tinggi, yaitu harian.



Gambar 3.21 Diagram Frekuensi Penggunaan Internet di Indonesia
Sumber: Google *Consumer Barometer* (2018)

Sudah tidak bisa dipungkiri lagi bahwa internet sudah menjadi bagian yang tak terpisahkan dalam kehidupan masyarakat Indonesia maupun dunia, hal tersebut mendorong peluang-peluang baru bagi para pegiat bisnis. Dengan pasar yang cukup luas dan besar, pelaku bisnis terus berinovasi, termasuk dengan memafaatkan tren yang berkembang di masyarakat, memahami kebutuhan dasar masyarakat, dan menggabungkan keduanya dalam suatu produk melalui internet. Berbagai perusahaan penyedia jasa makan dan minuman, transportasi, kebutuhan rumah tangga, dan pendidikan, lahir di Internet. Hal tersebut menciptakan sebuah gaya hidup baru bagi masyarakat Indonesia dan bergantung kepadanya.

Sadar atau tidak sdar, ketika pertama kali menggunakan berbagai aplikasi, terdapat proses sakral yang rutin dilakukan, seperti memasukan data pribadi kita di aplikasi tersebut untuk keperluan registrasi.

Sesederhana memasukan nama lengkap, alamat surel, tempat tanggal lahir, hingga yang lebih rumit seperti minat, hobi, alamat, latar belakang pekerjaan dan pendidikan, informasi mengenai keluarga, teman, dan kerabat, hingga momen-momen yang penting dalam kehidupan pribadi.

Selanjutnya juga kita sering melakukan ritual yang sedang popular saat ini, yaitu transaksi melalui internet yang mengintegrasikan rekening bank dengan menggunakan *fintech*. Kemunculan cara transaksi melalui internet seperti e-banking, e-trade, e-commerce, dsb, dinilai memberikan kemudahan bagi penggunannya sehingga transaksi menjadi lebih praktis. Namun dibalik dampak positif tersebut, terdapat juga dampak negatifnya, pernakah anda menyadari bahwa setiap kegiatan yang akrab dilakukan seperti yang disebutkan sebelumnya, hal tersebut dapat terekam secara abadi? Dan semua data dan informasi yang telah kita berikan atau bagikan di dunia digital tersebut dapat digunakan oleh pihak yang tidak bertanggung jawab?

Oleh karenanya sangat penting bagi kita untuk mengikuti kemajuan teknologi dengan kemampuan serta pengetahuan yang baik mengenai keamanan siber.

Menurut (WILDAN, 2014), setiap aktivitas yang kita lakukan saat menggunakan internet dapat memperkuat identitas diri pada dunia siber. Internet yang telah berkembang telah menghasilkan dunia baru yang biasa dikenal dengan *cyber space*. Dunia tersebut merupakan dunia komunikasi yang berbasis komputer dan menawarkan realitas baru yang berbentuk virtual atau tidak nyata. Menurut (ITU, 2017) *cyber space* memungkinkan terbentuknya komunikasi antara sesama pengguna jaringan komputer. Semakin tinggi intensitas penggunaan *cyber space*

oleh seseorang, semakin tinggi juga sinyal informasi terkait dirinya, sehingga gambaran sosok pengguna tersebut semakin jelas pada *cyber space*. Bayangkan seberapa banyak data dan informasi kita, yang dapat dikumpulkan seseorang untuk memahami identitas kita melalui berbagai macam layanan internet, sosial media, dan aplikasi yang kita gunakan.

Kemajuan, perkembangan internet, dan kecanduan masyarakat terhadapnya harus diterima dengan bijaksana. Karena hal tersebut dapat menjadi lahan dan peluang baru bagi pihak-pihak yang ingin memanfaatkan hal tersebut dengan maksud tidak baik, dapat dikatakan perkembangan dan kemajuan internet juga dibarengi oleh perkembangan dan kemajuan kejahatan siber.

(2) Peningkatan Kejahatan Siber

Seiring dengan kemajuan teknologi yang pesat, dan diikuti dengan perubahan serta kemunculan gaya hidup masyarakat yang baru, dimana gaya hidup tersebut serba digital, kebereadaan internet yang ada di genggaman tangan penggunannya, menjadikan segala kegiatan maupun aktivitas menjadi lebih praktis. Perubahan tersebut turut berdampak atas hilangnya batas ruang dan waktu dalam *cyber space*. Hal tersebut mendorong terciptanya peluang untuk pemanfaatan informasi yang tersebar dalamnya, yaitu untuk melakukan tindak kejahatan di dunia maya atau disebut juga dengan *cybercrime*.

Menurut (Wisnubroto, 1999), *cyber crime* atau dalam bahasa Indonesia disebut dengan kejahatan siber, merupakan perbuatan yang melawan hukum dan dilakukan dengan menggunakan teknologi komputer sebagai alat, baik untuk mendapatkan keuntungan maupun tidak, yang bersifat

merugikan orang lain. Secara ringkas *cybercrime* merupakan perbuatan melanggar hukum dengan menggunakan teknologi canggih seperti komputer.

Indonesia yang merupakan salah satu dengan jumlah penduduk terpadat di dunia dengan kemajuan teknologi internet yang pesat, tidak lepas dari fenomena *cybercrime*. Dalam laporan *Cybersecurity index* yang dikeluarkan oleh *The UN International Tele-communication Union* (2017), ditemukan bahwa Indonesia merupakan salah satu negara dengan keamanan siber yang rendah dan termasuk dalam 110 negara yang sering menjadi target sasaran pelaku *cybercrime*.

Tren *cybercrime* di Indonesia cenderung semakin meningkat setiap tahunnya, dengan tipe serangan yang bervariasi dan berbeda dari tahun-tahun sebelumnya. Menurut Suharnawi dan Danuri (2017), *cybercrime* dapat terjadi karena beberapa faktor, pertama yaitu adanya pelaku *cracker*, kesempatan beraksi, modus kejahatan, korban, reaksi sosial terhadap kejahatan tersebut, dan hukum yang mengaturnya. Kebanyakan dari pelaku *cybercrime* merupakan orang yang ahli atau lebih menguasai teknologi digital dan internet, dan menggunakan kemampuan tersebut untuk mengakses jaringan komputer milik orang lain secara ilegal.

Cybercrime seringkali dikaitkan dengan kehadiran seorang *hacker* dan *cracker*. *Hacker* sendiri merupakan seseorang yang mempercayai bahwa informasi merupakan hal yang berharga dan senang memprogram. *Hacker* cenderung ingin mendalami informasi-informasi tersebut lebih dalam lagi. Sedangkan *cracker* merupakan seseorang yang melakukan tindakan anarki dan pencurian saat mendapatkan akses terhadap suatu data. Hal tersebut melahirkan istilah baru

yaitu *whitehat* dan *blackhat*. *Whitehat* merupakan seorang *hacker* yang dinilai lugu, sedangkan *blackhat* adalah istilah yang digunakan untuk pelaku *cracker*. Namun orang lebih sering menyebut keduanya sebagai *hacker*, tanpa mengetahui perbedaan antara *whitehat* dan *blackhat*.

Menurut (Arifah, 2011), ada beragam jenis aktivitas *cybercrime*, mulai dari mencuri dan mengakses data kartu kredit seseorang, akun bank, informasi nasabah, melakukan pembelian menggunakan kartu kredit palsu atau milik orang lain (*carding*), hingga mengacak-acak sistem komputer dengan sengaja.

Dalam buku *Introduction to Cyber Security* oleh Jeetendra Pande, Aktivitas *cybercrime* tersebut dapat terjadi dikarenakan beberapa faktor, seperti uang, balas dendam, ingin diakui, anonimitas, dan spionase.

Menurut artikel (Gema, 2013), dalam artikelnya yang dimuat dengan judul "*Cybercrime*: Sebuah Fenomena di Dunia Maya", di dalamnya dijelaskan bahwa *cybercrime* dapat dikelompokan dalam beberapa kategori sendiri, antara lain:

- **Mengakses ke layanan dan sistem komputer tanpa izin**

  Merupakan kejahatan di mana seorang *cracker* mengakses suatu komputer secara tidak sah atau tanpa izin dan diketahui oleh pemilik sistem komputer tersebut. *Cracker* beraksi dengan mengambil alih sistem komputer atau mencuri data yang bersifat rahasia

- **Konten ilegal**

  Konten ilegal merupakan *cybercrime* yang terjadi ketika seseorang mengunggah data atau informasi yang tidak benar dan etis ke internet. Hal tersebut biasanya melanggar hukum dan dapat mengganggu ketertiban

umum, contoh yang sering ditemui adalah penyebaran hoaks dan fitnah, sehingga dapat merusak harga diri seseorang.

- **Pemalsuan data**

  Pemalsuan data adalah bentuk kejahatan di mana pelaku kejahatan mengunggah dokumen dengan data yang dipalsukan.

- **Spionase**

  Merupakan kejahatan dimana sang pelaku memata-matai seseorang menggunakan jaringan internet. Hal ini biasanya terjadi atas dasar persaingan bisnis.

- **Pemerasan dan sabotase**

  Merupakan kejahatan yang dilakukan dengan membuat kerusakan, penghancuran, dan gangguan terhadap data, program, dan sisetem jaringan. Bentuk kejahatan pemerasan dan sabotase yang paling banyak ditemui adalah penyusupan virus komputer. Virus tersebut dapat merusak atau menyabotase data dan program komputer korbannya.

- **Pelanggaran Kekayaan Intelektual**

  Pelaku kejahatan ini biasanya melakukan tindakan yang melanggar hak kekayaan intelektual seseorang, seperti meniru tampilan suatu situs *website* milik seseorang secara ilegal.

- **Pelanggaran privasi**

  Merupakan tindakan dimana pelaku mengakses suatu data yang bersifat pribadi dan rahasia seperti keterangan pribadi seseorang yang terdapat pada formulir *digital* yang tersimpan di jaringan komputer, dan apabila data tersebut diketahaui oleh orang lain, dapat merugikan pemilik data.

b) Memahami Keamanan Siber

Keamanan siber bagi beberapa orang mungkin masing terdengar asing, namun di tengah perkembangan teknologi informasi dan komunikasi, bijak dalam ruang siber merupakan tuntunan bagi penggunanya agar aman dan terhindar dari ancaman *cybercrime*. Untuk lebih memahami mengenai hal tersebut, berikut beberapa hal yang perlu diketahui terkain keamanan siber.

(1) Keamanan Siber di Era Digital

Menurut (*International Telecommunication Union,* 2018), kemanan siber merupakan suatu kumpulan alat, kebijakan, konsep, perlindungan, manajemen resiko, pedoman, tindakan, pelatihan, praktik, jaminan, dan teknologi untuk melindungi ruang siber, organisasim dan kepemilikan seorang pengguna internet. Secara singkat, keamanan siber merupakan aktivitas untuk mengamankan dan mencegah *cybercrime*.

Kebanyakan dari mereka yang paham mengenai pentingnya keamanan siber adalah yang berprofesi di bidang teknologi informasi dan komunikasi. Namun sebagian besar masyarakat umum masih memiliki pengetahun yang rendah mengenai pentingnya keamanan siber, dan beresiko tinggi untuk menjadi korban *cybercrime*.

Memiliki pengetahuan mengenai keamanan siber sangatlah penting untuk menghindari resiko kerugian dari *cybercrime*. Selain terhindar dari *cybercrime* yang besar dan terorganisasi, memahami keamanan siber juga dapat menghindari seseorang dari *cybercrime* bersakala kecil dan beresifat serangan individual. Hal tersebut juga memiliki urgensi yang besar mengingat perkembangan teknologi di era digital yang membuat masyarakat semakin dekat dengan

dunia siber, dimana hal tersebut dapat dimanfaatkan oleh pelaku kejahatan sebagai peluang mencuri data pribadi yang diperoleh melalui internet dan menyalahgunakannya. Oleh karena itu, kedekatan dengan dunia siber dan internet perlu dibarengi dengan pemahaman keamanan siber, setidaknya pada tingkat dasar, untuk menghindari hal-hal yang sudah disebutkan sebelumnya.

Untuk memahami lebih dalam mengenai keamanan siber, diperlukan pemahaman mengenai ruang lingkup keamanan siber dalam konteks yang dekat dengan keseharian masyarakat.

Pembahasan mengenai ruang lingkup keamanan siber terdiri dari beberapa hal yang ering ditemui pada keseharian masuarakat dan merupakan bagian dari keamanan siber seperti Perlindungan Data Pribadi, Privasi, dan Jejak Digital.

(2) Perlindungan Data Pribadi

Perlindungan data pribadi adalah perlindungan uang berfungsi untuk melindungi data pribadi bagi pengguna internet. Data pribadi yang dimaksud meliputi data pribadi umum dan spesifik. Data pribadi penting untuk idilidungi demi terhindar dari penyalahgunaan data yang bersifat rahasia.

Menurut (B.U, 2017), perlindungan data pribadi merupakan perlindungan terhadap data dan informasi mengenai kehidupan seseorang baik data yang yang dapat mengidentifikasi secara sendiri maupun gabungan dari informasi secara langsung dan tidak langsung.

Kesadaran masyarakat Indonesia yang rendah mengenai pentingnya melindungi data pribadi yang dimiliki dalam sosial media maupun pihak ketiga penyimpan data, membuat Indonesia menjadi salah satu negara dengan masyarakat yang

mudah di retas. Masyarakat tidak terlalu menghiraukan data pribadi yang digunakan di internet. Salah satunya ketikamengisi pendaftaran kartu kredit dan perbankan. Masyarakat sering tidak menghiraukan persetujuan yang diajukan oleh perusahaan dan cenderung tidak membaca persetujuan tersebut. Ketika data yang diberikan mengalami kebocoran, akan sulit untuk menutupi kebocoran data tersebut.

(Alamsyah, 2019), menjelaskan bahwa, untuk menghindari penyalahgunaan data, masyarakat disarankan untuk memastikan data pribadi yang telah diunggah ditarik dari sosial media atau meminta pihak ketiga untuk tidak menampilkan data tersebut ke publik, pastikan data yang disimpan oleh pihak ketiga seperti perusahaan, rumah sakit, maupun sekolah disimpan dengan aman. Sehingga bukan hanya sang pemilik data namun lembaga yang dipercaya juga wajib menjaga data pribadi kita.

Berikut beberapa hal yang harus diperhatikan ketika menggunakan layanan internet untuk menjaga data pribadi yang kita miliki:

- **Mengenkripsi data**

  Beberapa layanan situs web dan *browser* sudah menerapkan fitur enkripsi yang dapat memastikan pengiriman data aman dan terkode. Contoh dari fitur enkripsi yang sering ditemui adalah protokol *Secure HTTP* dan *SSL*. Kita perlu memastikan layanan yang kita gunakan telah menerapkan fitur ini. Kita dapat melihat fitur ini ketika membuka laman situs, dan biasanya saat menggunakan suatu *browser*, terdapat simbol gembok pada *searchbar* situs yang dikunjungi.

- **Penggunaan Jaringan WiFi**

Saat berada di tempat umum, kita harus berhati-hati dalam menggunakan jaringan wifit yang tersedia secara gratis. Jaringan tersebut dapat digunakan oleh seseorang untuk mencuri data. Cara yang paling sering dilakukan yaitu dengan membuat *access point* palsu, dan bila seseorang memasukan suatu akun menggunakan wifit tersebut, datanya akan diambil. Maka itu, kita harus berhati-hati dan selalu waspada ketika menggunakan wifi untuk mengakses internet di tempat umum atau publik.

- ***Phishing***

  Saat mengakses sebuah website, biasanya kita dapat menemukan *Hyperlink* liar bertebaran dalam website tersebut. Dalam beberapa kasus, *hyperlink* yang dibuka mengarahkan penggunannya ke laman login palsu, dan bertujuan untuk mencuri data dari pengunjung website. Hal ini biasa disebut dengan *Phising*.

- ***Password***

  Dalam merangkai suatu *password* atau kata sandi, ada beberapa hal yang perlu diperhatikan untuk menjadikan *password* kita lebih kuat, yaitu menghinadi penggunaan tanggal lahir, nama siapapun, gunakan kombinasi angka dan huruf, panjang password lebih dari 7 karakter, dan rutin mengganti password setiap 3 bulan sekali.

- **Mode *Incognito***

  Metode ini merupakan fitur yang sekarang sudah banyak ditemukan pada browser yang sudah modern. Fungsi dari fitur ini adalah untuk mematikan perekam dalam browser yang kita gunakan. Sehingga alamat situs yang kita kunjungi tidak akan terekam, juga data pribadi

seperti *username*, *password*, *cache* dan *cookies* dari situs yang dikunjungi.

(3) Privasi

Privasi adalah hak seseoran untuk mengatur, mengontrol, menghapus, dan mengubah informasi mengenai dirinya. Hal ini mencakup keputusan bagaimana, kapan dan untuk apa informasi tersebut disampaikan kepada pihak atau orang lain. Beberapa hal sering dilakukan untuk mendapatkan keuntungan tertentu, seperti mendaftar untuk mendapatkan hadiah undian, hal ini berbahaya dan cukup beresiko, karena data dan informasi yang kita berikan bisa saja dicuri dan disalahgunakan oleh pihak yang tidak bertanggung jawab.

Privasi merupakan hal yang penting sebagai senjata yang kuat, dengan *mindset* bahwa data pribadi yang kita berikan kepada orang lain merupakan hal yang berharga. Semakin dalam orang mengetahui informasi tentang diri kita, semakin, berkuasa pula orang tersebut atas diri kita. Maka dari itu, privasi dalam penggunaan internet sangatlah penting karena sangat lekat dengan kehidupan kita.

(4) Jejak Digital (Digital Footprint)

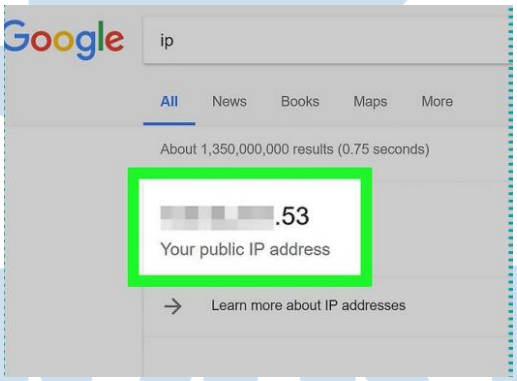
Sandi S. Varnado (2014) menjelaskan bahwa jejak digital adalah jejak dari data digital, seperti dokumen dan akun digital. Jejak digital dapat berupa data yang terdapat pada komputer *offline*, maupun yang terhubung dan disimpan secara *online*. Jejak digita juga dapat berupa data yang dibuat sendiri oleh pengguna dan dibuat oleh orang lain mengenai sang pengguna, berikut macam-macam jejak digital:

- Konten yang diciptakan oleh sang penggunanya sendiri seperti tulisan komentar, blog, serta profil dan foto yang diunggah oleh pengguna pada media sosial miliknya.

- Data atau catatan interaksi apa saja yang dilakukan seorang pengguna dalam mengakses sebuah website dan aplikasi. Aktivitas tersebut direkam oleh website dan aplikasi tersebut, beberapa hal yang direkam adalah halaman web apa yang dilihat, seberapa sering mengunjungi dan jangka waktu antar kunjungan, waktu yang dihabiskan oleh pengguna saat mengakses halaman website, klik, interaksi dengan form, gerakan mouse, keyboard, dan interaksi lainnya.
- Data seperti alamat ISP, IP, Lokasi, rekaman telepon, like, pertemanan, perilaku pengguna, dll.

Selain hal-hal tersebut, jejak digital dapat dibagi menjadi dua, yaitu pasif dan aktif.

- Pasif



Gambar 3. 22 Jejak Digital Pasif

Sumber: Buku Siberpedia: Panduan Pintar Keamanan Siber (2018)

Jejak digital pasif adalah jejak yang ditinggalkan oleh pengguna secara tidak sengaja, pengguna tidak dengan aktif meninggalkan jejak tersebut. Contoh dari jejak ini adalah alamat IP yang terdeteksi oleh server saat mengnjungi website, sehingga server mengetahui ISP yang digunakan dan lokasi saat kita mengakses website tersebut. Selain itu

jejak digital pasif juga dapat berupa riwayat pencarian ketika menggunakan situs pencarian.

- Aktif

Gambar 3.23 Jejak Digital Aktif

Sumber: Buku Siberpedia: Panduan Pintar Keamanan Siber (2018)

Jejak digital aktif adalah jejak yang dibuat secara aktif oleh sang pengguna, contohnya adalah status yang ditulis oleh pengguna pada jejaring sosial miliknya, juga email yang dikirim dan diterima.

Mengapa jejak digital dinilai penting?

Hal tersebut dikarenakan jejak digital dapat menjadi bom waktu yang tertanam oleh sang pengguna itu sendiri, dimana bom tersebut akan meledak bila jejak digital tersebut ditargetkan dan dicari oleh pihak tertentu. Hal tersebut menjadi lebih buruk bila pemilik jejak tersebut memiliki jejak digital yang dapat merugikan dirinya sendiri.

Jejak digital tersebut dapat menjadi boomerang yang menyerang kembali pemiliknya, seperti kalimat tidak etis yang diutarakan pada sosial media ketika membicarakan mengenai atasan di kantor. Kelly Moore dalam jurnalnya yang berjudul “The Influence of Personality on Facebook Usage, Wall Posting, and Regret” menjelaskan bahwa, sekitar 20% pengguna Facebook, tidak ingin atasan mereka

melihat unggahan apapun yang terdapat pada media sosial mereka.

Meski jejak digital memiliki resiko yang tinggi, pemilik jejak tersebut seringkali tidak sadar akan hal tersebut. Padahal setiap *likes*, komen, postingan, dan apapun yang kita lakukan pada perangkat digital akan terekam secara abadi atau selama-lamanya.

(5) Keamanan Siber di Internet

Keamanan siber bukanlah sebuah pilihan melainkan suatu kepastian. Dengan ketergantungan masyarakat digital terhadap internet, keamanan siber berfungsi sebagai pagar yang melindungi dari berbagai serangan *siber*. Sebab dengan adanya kemajuan teknologi, akan ada selalu pihak yang memanfaatkan hal tersebut. Macam dan bentuk *cybercrime* sudah dibahas sebelumnya, dan bila masyarakat tidak dibekali dengan pendidikan yang tepat mengenai cara mengamankan perangkat yang mereka gunakan, kemungkinan serangan *cybercrime* juga semakin tinggi. Selain melalui akses eksternal, ternyata ada beberapa cara pencurian data dapat terjadi akibat tindakan yang dilakukan kita sendiri, misalnya saja melalui *cookie*.

Cookie merupakan beberapa data yang tersimpan pada perangkat yang terhubung dengan internet. Saat kita mengakses berbagai informasi menggunakan internet, seperti website. *Cookie* merupakan hal yang lazim kita temui pada browser yang kita gunakan. *Cookie* digunakan untuk menyimpan data prilaku seseorang ketika mengakes sebuah website, sehingga website dapat menggunakan data yang kita berikan untuk mengelola informasi kita sesuai dengan data *cookie* tersebut.

Fungsi utama *cookie* adalah mengetahui mengenai pengguna website, sebagai contoh adalah ketika seseorang membuka Facebook. Pertama kali kita mengakses, website tersebut akan meminta alamat *E-mail* dan *password* kita, dan seterusnya kita tidak perlu memasukan data tersebut kembali, dan kita dapat langsung mengakses berada Facebook. Hal tersebut dapat terjadi karena *cookie* kita telah merekam identitas kita.

Cookie dapat menyimpan data seperti browser apa yang kita gunakan, pengaturan, lokasi, *interest* kita, dan masih banyak lagi. Informasi ini bertujuan untuk meningkatkan pengalaman pengguna dalam mengakses sebuah website. Secara umum, sebenarnya *cookie* tidaklah berbahaya. Namun bila dipegang oleh orang yang salah, akan menjadi berbahaya dan menjadi *boomerang* bagi penggunannya.

Memang kemungkinan tersebut kecil, dan jarang *cookie* dapat diretas oleh seorang *hacker*. Kemungkinan terburuk yang dapat terjadi adalah ketika seseorang mendapatkan akses dari *cookie* kita, dan dapat mengakses akun-akun kita.

Namun tidak perlu khawatir, karena keamanan *cookie* tergantung dari browser dan website yang kita gunakan, dan terdapat sebuah fitur keamanan enkripsi *cookie* pada saat ini. Hal yang bisa membahayakan dalam penggunaan *cookie* adalah ketika ada pihak yang menyalahgunakan fitur *cookie* tersebut, sehingga mengganggu privasi kita.

Kasus yang sering ditemui adalah "*Tracking cookie*", dimana *cookie* tersebut tidak meningkatkan pengalaman penggunanya, namun mengawasi dan melihat kegiatan apa yang kita lakukan pada suatu website. *Cookie* tersebut dapat mengakses informasi seperti riwayat browser yang kita

gunakan, dan menampilkan iklan bersifat spesifik dari data-data tersebut.

(6) Keamanan Siber di Bidang Finansial dan Perbankan

Pada era digital, banyak kegiatan sehari-hari yang sudah bisa dilakukan dengan lebih mudah dengan menggunakan teknologi digital, salah satunya dalam sektor finansial seperti perbankan.

Keamanan Siber Perbankan

Nasabah suatu bank dapat bertransaksi kapan saja dan dimana saja melalui *e-banking* (Internet), *SMS-banking* dan *mobile-banking* (telepon seluler). Dengan kemuadahan tersebut, terdapat pula resiko pengguna mengalami penyalahgunaan akun rekening yang mereka milik oleh penjahat siber. Untuk itu, ada beberapa hal tips bagi para nasabah untuk mengamankan data perbankan mereka pada era digital ini, yaitu sebagai berikut:

- **Penipuan melalui telepon**

  Modus ini dilakukan pelaku melalui komunikasi telepon, dan pelaku biasanya menyampaikan hal-hal yang melibatkan pengguna, seperti memenangkan suatu hadiah, atau keluarga pengguna sedang mengalami musibah. Setelah itu pelaku akan mengarahkan pengguna agar memberikan sejumlah uang dan memandu mengenai jumlah uang yang dibutuhkan untuk mengatasi hal-hal tersebut.

  Cara menghindari

  Untuk menghindari hal tersebut, hal yang pertama kita harus lakukan adalah memeriksa identitas penelepon, dan melakukan pengecekan mengenai informasi yang ia sampaikan.

Bila kita mendapatkan kabar kita telah memenangkan suatu hadiah tertentu, seperti undian dan semacamnya. pastikan pihak penyelenggara tidak meminta untuk diteransferkan dana apapun. Umumnya perusahaan yang menyelenggarakan undian tidak meminta untuk ditransfer dana oleh pemenangnya.

Sedangkan bila kita menerima telepon yang mengabarkan bahwa keluarga atau kerabat sedang mengalami musibah, diharapkan tidak panik dan langsung mengikuti instruksi dari penelepon. Tanyakan terlebih dahulu mengenai identitas penelepon dan lakukan pengecekan terhadap musibah yang dikatakan penelepon.

- **Penipuan melalui e-mail**

  Penipuan juga bisa terjadi melalui e-mail, pelaku penipuan biasanya mengaku sebagai pihak bank resmi, dan meminta kita untuk menuliskan nomor rekening beserta nomor PIN kartu debit/kredit yang kita miliki. Pada praktiknya, terkadang pelaku juga membuat suatu website alamat bank palsu untuk mengecoh nasabah, dalam website tersebut kita akan dimintakan hal serupa dengan alibi untuk pembaaruan data.

  Cara menghindari

  Bila mendapatkan e-mail mencurigakan, jangan membalas pesan tersebut dengan nomor rekening yang kita milliki ataupun PIN kartu kredit/ debit yang kita miliki, karena seharusnya bank resmi telah memiliki data tersebut dan tidak pernah meminta data tersebut kepada nasabah. Ketika kita mengakses website perbankan, perlu diperhatikan juga alamat website tersebut apakah sudah benar atau belum.

- **Penipuan penawaran investasi dengan bunga tinggi**

  Penipu biasanya mengatasnamakan dirinya sebagai perusahaan investasi dengan janji imbalan yang tinggi. Kita harus waspada karena beberapa penawaran serupa terbukti tidak dapat memenuhi imbal hasil yang dijanjikan.

  Cara Menghindari

  Bila mendapaatkan penawaran serupa, kita harus mempertimbangkannya secara kritis dan menggunakan logika. Apakah jumlah imbal bunga tersebut wajar? Dan lakukan pengecekan terhadap perusahaan yang menawarkan investasi tersebut, pastikan kredibilitas perusahaan tersebut terjamin dan sudah terlindungi secara hukum.

- **Penipuan menggunakan kartu kredit/ debit di Internet**

  Saat ini semakin banyak toko yang menawarkan produk atau jasa melalui internet dan panggilan telepon, transaksi yang ditawarkan juga menyediakan kemudahan pembayaran menggunakan kartu debit maupun kredit, dan kita biasanya akan diminta menyebutkan nomor kartu beserta masa berlaku dan 3 digit kode keamanan kartu kita, sehingga transaksi dapat dilakukan.

  Cara Menghindari

  Bila mendapaatkan penawaran seperti ini, kita harus memahami tentang produk atau jasa yang ditawarkan, serta memahami syarat dan ketentuan dari barang atau jasa tersebut. Selain itu, jangan pernah memberikan nomor kartu, masa berlaku, dan kode keamanan yang berada di belakang kartu debit atau kredit yang kita

miliki kepada siapapun, kecuali untuk hal yang kita telah pahami dan kita setujui.

- **Pemalsuan panggilan telepon call center bank**

  Modus ini merupakan salah satu yang paling sering terjadi, para pelaku biasanya membuat seolah mesin ATM bank yang kita gunakan rusak dan telah menelan kartu yang kita miliki, sehingga kita mengalami kepanikan dan menghubungi nomor call center palsu yang telah dipasang pelaku di mesin ATM. Ketika kita menelepon nomor tersebut, pelaku akan meminta PIN rekening kita dan menjanjikan akan mengganti kartu tersebut dengan yang baru. Pelaku yang berhasil mendapatkan PIN rekening, kemudian akan mencuri dana yang dimiliki korban.

  Cara Menghindari

  Pastikan kita mengingat nomor resmi call center bank yang kita gunakan. Jika menghubungi nomor call center resmi, biasanya kita akan dijawab oleh mesin penjawab otomatis terlebih dahulu, sebelum akhirnya kita diminta memilih layanan apa yang kita inginkan. Sebagai pengingat, pihak bank resmi tidak akan pernah meminta nomor PIN rekening nasabah.

Bila hal-hal tersebut terjadi, ataupun kita merasa ada hal yang mencurigakan ketika melakukan perbankan secara online, seperti diminta data sensitif ketika ingin bertransaksi, segera batalkan transaksi tersebut.

Keamanan Siber Fintech

Kemudahan bertransaksi pada era digital sangatlah membantu kehidupan masyarakat. Pada era ini, kita sering menjumpai transaksi non-tunai. Dengan transaksi ini, kita tidak perlu repot mendatangi mesin ATM untuk menarik sejumlah uang tunai.

Kita juga dipermudah dalam sisi pembayaran dengan munculnya sistem pembayaran *e-wallet* seperti Gopay dan OVO. Dengan aplikasi *e-wallet* tersebut, penggunanya dapat melakukan transaksi dengan lebih mudah, tanpa uang tunai dan hanya perlu mengisi ulang saldo *e-wallet* tersebut.

Meskipun begitu, dengan kemudahan yang ditawarkan, potensi tindak kejahatan tetap ada. Maka itu, ada beberapa hal yang perlu diperhatikan dalam melakukan transaksi dengan sistem pembayaran digital:

- Jangan memberikan kode PIN atau kode akses kepada orang lain.
- Jangan menyimpan atau mencatat kode akses di tempat yang diketahui orang banyak.
- Periksa secara detail mengenai transaksi yang akan dilakukan sebelum mengkonfirmasi transaksi.
- Ketika melakukan transaksi, selalu pastikan dan menunggu respon balik dari transaksi itu.
- Setelah melakukan transaksi, pastikan anda menerima konfirmasi berupa nontifikasi pada *e-mail* anda atau sms, dan pastikan pesan konfirmasi tersebut berada pada *inbox* bukan *spam*.
- Bila merasa PIN yang anda miliki diketahui seseorang, segera mengganti PIN tersebut.
- Jika anda kehilangan kartu SIM anda, baik dicuri maupun hilang, segera menelepon *call center* dari perusahaan kartu SIM anda.
- Selalu berhati-hati ketika menggunakan aplikasi online, pastikan aplikasi tersebut tidak berupa *spam* atau mengandung *malware* untuk mencuri data anda.

- Jangan lakukan transaksi di publik seperti tempat umum, warnet, wifi publik, karena berpotensi membahayakan data yang terdapat pada gadget kita.
- Jangan lupa untuk mengeluarkan akun setelah melakukan transaksi digital.
- Ketika mengganti *handphone*, pastikan data yang terdapat pada *handphone* lama kita telah dihapus, agar tidak digunakan oleh pihak yang tidak bertanggung jawab.

Keamanan Siber di Media Sosial

Media sosial telah menjadi suatu hal yang tidak lepas dari kehidupan masyarakat Indonesia. Namun kesadaran masyarakat untuk melindungi dan menjaga keamanan di sosial media masih rendah. Maka dari itu masih banyak celah yang berpotensi dimanfaatkan oleh pelaku *sybercrime* untuk mendapatkan keuntungan pribadi. Berikut ini merupakan beberapa hal yang kurang dijadikan perhatian khusus oleh para pengguna media sosial, khususnya di Indonesia. (Genmuda.com, 2016)

- **Menerima Pengikut dan Pertemanan dari Orang yang Tidak Dikenal**

  Ingin memiliki pengikut atau *followers* pada sosial media dan mencari pertemanan baru memang bukanlah hal yang salah. Namun perlu diingat juga bahwa hal tersebut sama saja kita membiarkan orang asing yang tidak dikenal untuk mengetahui informasi pribadi kita. Menurut survei yang dilakukan Kaspersky Lab, 31 persen pengguna media sosial meng*accept* pertemanan dari orang yang tidak mereka ketahui. Hal ini dapat meningkatkan resiko kejahatan siber masuk dalam kehidupan kita.

- **Sembarangan membuka tautan**

  Tautan seperti gambar dan video memang merupakan hal yang wajar dibagikan pada media sosial. Namun, kita tetap harus berhati-hati ketika membuka tautan dari orang asing dan tidak kita kenal, terutama yang terlihat mencurigakan. Dalam penelitian yang sama oleh Kaspersky Lab terungkap bahwa, 26 persen pengguna sosial media membuka tautan secara langsung tanpa pertimbangan terlebih dahulu.

- **Membagikan informasi dan data pribadia**

  Kaspersky Lab, dalam penelitianya juga menemukan bahwa sekitar 30 persen pengguna media sosial pernah membagikan informasi yang bukan hanya kepada kerabat, namun juga kepada semua orang yang *online* secara publik. Hal ini juga menjadi peluang bagi pelaku *cybercrime* untuk melakukan kejahatannya tanpa disadari penggunanya.

- **Mengabaikan pengaturan privasi**

  Walaupun data mengatakan bahwa sekitar 78 perseb dari para pengguna internet telah mengakses media sosial, namun survei juga menunjukan kesadaran pengguna yang rendah. Sekitar 9 persen pengguna tidak menyadari bila apa yang mereka unggah dapat dilihat oleh orang asing diluar pertemanan mereka. Hal ini menyebabkan resiko data dan informasi yang mereka miliki jatuh ke pihak yang tidak bertanggung jawab. Data ini dapat digunakan untuk mencuri identitas pengguna dan melakukan penipuan. Jika data seperti foto, status, dan informasi kita lainnya tidak ingin diketahui orang-orang yang tidak dikenal, pastikan kita telah mengatur pengaturan privasi pada media sosial tersebut. Agar

lebih memahami pengaturan tersebut, pengguna dapat membaca FAQ yang disediakan oleh media sosial yang mereka gunakan.

- **Menggunakan *Password* yang sama dan menggunakan fitur pengingat pada *Browwser***

  Menggunakan kata sandi yang sama pada berbagai media sosial yang digunakan memang dapat memudahkan kita untuk mengingat sandi tersebut. Pada beberapa *browser* juga terdapat fitur pengingat sandi. Dengan melakukan keduanya tentu akan mempermudah dan mempercepat pengguna untuk mengakses media sosial mereka. Namun ang perlu kita ingat bahwa *browser* yang kita gunakan dapat diretas oleh pihak yang tidak bertanggung jawab. Maka dari itu pembaharuan sandi secara rutin merupakan suatu hal yang penting, dan jangan menyimpan sandi tersebut pada *browser* yang kita gunakan.

Kejahatan yang ditemui di sosial media

Berikut ini merupakan beberapa jenis kejahatan yang biasa muncul di sosial media:

- **Penipuan dengan kedok jual beli**

  Selain terjadi di dunia nyata, penipuan seperti ini juga terjadi di ruang siber secara *online*, dan modus yang paling umum digunakan oleh pelaku adalah penawaran harga yang sangat murah, produk terbaru yang belum ada di pasar, nomor resi dan testimoni palsu.

  Untuk mengatasi hal tersebut yang bisa dilakukan oleh pengguna media sosial adalah teliti dalam memilih barang dan harganya, pastikan toko dapat dipercaya dan memiliki ulasan baik dan asli, gunakan mrketplace yang menggunakan rekening bersama dimana uang pembeli

tidak langsung dipegang oleh penjual, dan mencoba melakukan transaksi secara COD, sehingga barang dapat langsung dicek.

- **Membajak sosial media**

  Pembobolan dan pembajakan sosial media adalah *cybercrime* yang sudah sering terjadi. Pelaku biasanya merupakan orang yang memiliki ilmu dan keahlian pada bidan teknologi digital dan internet. Biasanya pelaku juga menargetkan orang terkenal seperti pejabat dan selebriti. Selain itu mereka juga biasa membajak akun pemerintah dan perusahaan. Tujuan mereka melakukan hal tersebut biasanya untuk meminta sejumlah tebusan ataupun melancarkan propaganda yang mereka inginkan pada sosial media tersebut.

  Untuk menghindari hal tersebut terjadi pada kita, ada beberapa hal yang dapat dilakukan, yaitu menggunakan keamanan ganda yang diverifikasi melalui *e-mail* dan SMS, perhatikan alamat url bahwa website tersebut resmi dan bukan merupakan *phising*, berhati-hati dan lebih teliti ketika ingin memasukan sandi, gunakan sandi yang berbeda-beda, dan mengganti sandi secara berkala.

- **Pemerkosaan dan penculikan**

  Pemerkosaan dan penculikan memang tidak terjadi langsung pada sosial media, namun hal tersebut dapat menjadi media dimana pelaku mendekati calon korban. Cara pelaku melakukannya cukup beragam, ssalah satunya menggunakan media sosial dan berkedok ingin berteman dengan calon korban. Kemudian pelaku membujuk korban dengan imbalan dan menawarkan segala macam hal agar korban tertarik padanya,

sehingga korban berkeinginan bertemu langsung dengan pelaku.

Untuk menghindari hal tersebut, masyarakat disarankan untuk lebih berhati-hati untuk berkenalan dengan orang yang tidak dikenal, kita harus menelusuri identitas orang tersebut dan mempertimbangkan apakah orang tersebut memiliki niatan buruk atau tidak sebelum memutuskan untuk bertemu secara langsung, dan bila perlu kita dapat mengajak teman kita ketika ingin bertemu dengan orang tersebut.

- **Prostitusi Online**

  Modus ini bervariasi dan pelaku melakukannya dengan beragam cara, misalnya saja pelaku akan menggoda calon korban dengan rayuan sehingga calon korban tertarik terhadap pelaku. Kejahatan siber ini merupakan salah satu kejahatan yang ramai dibincangkan dan menjadi salah satu kasus yang paling populer karena melibatkan sejumlah selebriti terkenal.

  Untuk mengatasi hal tersebut, masyarakat perlu dibekali dengan pendidikan seksual sejak dini, pemerintah juga perlu membangun suatu fasilitas agar masyarakat memiliki suatu kegiatan atau bakat yang dapat disalurkan, perlu juga adanya pendidikan mengenai konten pornografi dan untuk tidak menyebarkannya, hal tersebut tidak terlepas dari pentingnya sosialisasi mengenai internet sehat.

- ***Cyberbullying***

  Penindasan atau *bully* merupakan tindakan yang sering dilakukan pelaku secara tidak sadar maupun secara sadar, perilaku penindasan ini dapat mencakup penindasan secara fisik maupun verbal, dan hal ini dapat

mempengaruhi korban, mulai dari penurunan semangat belajar hingga hal-hal fatal lain yang tidak diinginkan. Seiring dengan perkembangan teknologi yang pesat, seseorang tidak perlu lagi melakukan tatap muka untuk melakukan komunikasi, hal ini berlaku juga untuk kasus *bullying*. Teknologi yang ada memungkinkan para pelaku *bullying* untuk terhubung langsung dengan korban, dan tindakannya sangat sulit untuk dilacak.

Beberapa hal yang dapat dilakukan untuk mengindari *cyberbullying* adalah untuk tidak bereaksi, ketika korban *bully* mengabaikan aksi penindas, maka mereka akan merasa tidak diperhatikan, selanjutnya adalah jangan membalas tindakan pelaku, dengan melakukan balas dendam dan mengintimidasi pelaku kembali akan membuat kita menjadi pelaku itu sendiri. Selanjutnya adalah memblokir pelaku, berprilaku sopan pada siapapun pada media sosial, dan tidak diam pada tindakan *bullying* yang terjadi.

3.1.2.3 Studi Referensi

Penulis melakukan studi referensi atau eksisting terhadap kampanye serupa yang pernah dilakukan sebelumnya. Studi ini bertujuan untuk memperoleh referensi gaya visual dan teknik penyampaian yang sesuai dalam perancangan kampanye tersebut.

1) **Better Cyber Safe Than Sorry**

Gambar 3.24 Logo *Better Cyber Safe Than Sorry*
Sumber: https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/bettercybersafethansorry

Better Cyber Safe Than Sorry adalah sebuah kampanye sosial yang dilakukan oleh CSA (*Cyber Security Agency of Singapore*). Kampanye tersebut merupakan kampanye nasional negara Singapura dengan tujuan meningkatkan kesadaran keamanan siber terhadap masyarakatnya dan meningkatkan praktis keamanan siber dalam kehidupan sehari-hari masyarakatnya. Kampanye tersebut telah berjalan dari Juli 2021 sampai Januari 2022, dan menggunakan beberapa gabungan media, seperti media luar rumah atau *out-of-hime*, media digital, dan *free to air media*.

Gambar 3.25 Poster kampanye *Better Cyber Safe Than Sorry*
Sumber: https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/bettercybersafethansorry

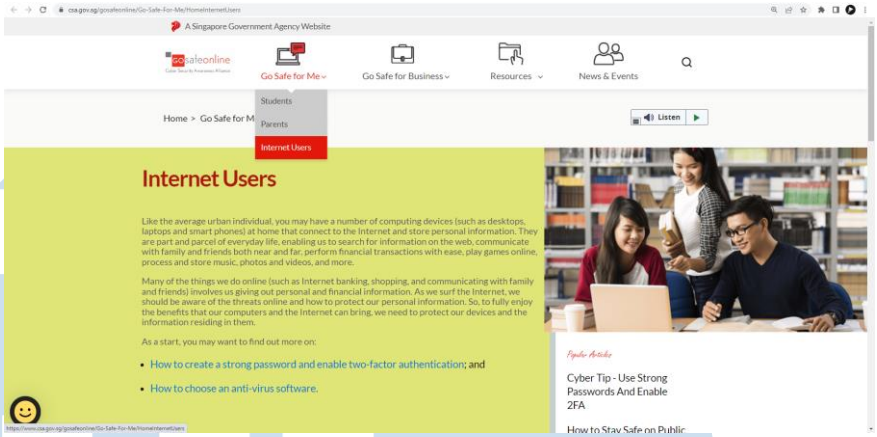
Kampanye tersebut berfokus untuk menggabungkan dan menggambarkan antara empat tips keamanan siber dan kehidupan sehari-hari. Empat tips tersebut adalah penggunaan kata sandi yang kuat dan otentifikasi, mengenali tanda-tanda *phising*, menggunakan perangkat lunak antivirus, dan memperbaharui perangkat lunak dengan tepat waktu.

Kampanye ini memanfaatkan berbagai macam media, khususnya media *online* dimana terget audiens mereka adalah para pengguna internet, beberapa poster dan konten yang mereka berikan diunggah di facebook, instagram, dan youtube pribadi CSA.

Kampanye tersebut berusaha meningkatkan kesadaran keamanan siber dengan mengingatkan audiens yang biasanya selalu waspada pada potensi kejahatan di dunia nyata, namun tidak waspada terhadap keamanan siber, audiens dibuat bertanya-tanya mengapa tidak melakukan hal yang sama terhadap aset digital yang mereka miliki. Audiens juga diingatkan bahwa potensi dan bahaya dari kejahatan siber tidaklah berbeda dengan kejahatan di dunia nyata. Secara tidak langsung kampanye tersebut mengedukasi dan mengingatkan hal tersebut melalui cerita yang mengkaitkan kejahatan dunia nyata dengan kejahatan siber.

Gambar 3.26 Poster kampanye *Better Cyber Safe Than Sorry*
Sumber: https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/bettercybersafethansorry

Selain menyadarkan audiens, kampanye ini juga memberikan beberapa tips utama untuk menghindari terjadinya kejahatan siber pada setiap postingannya, dan menyediakan informasi lebih lengkap dalam website CSA *Go safe online*. Audiens diarahkan kepada website tersebut melalui *barcode* maupun *link* yang terdapat pada beberapa postingan mereka, dan barcode maupun link tersbut akan mengarahkan audiens ke alamat web https://www.csa.gov.sg/gosafeonline/. Pada website tersebut audiens dapat memperoleh informasi lebih dalam mengenai perlindungan siber dan 4 tips keamanan siber, tips tersebut dikategorikan menjadi tiga, yaitu untuk pelajar, orang tua, dan pengguna internet (umum). Tips tersebut disesuaikan konten dan isinya bedasarkan kategori tersebut.



Gambar 3.27 Tips untuk penegguna internet pada website

Sumber: https://www.csa.gov.sg/gosafeonline/Go-Safe-For-Me/HomeInternetUsers

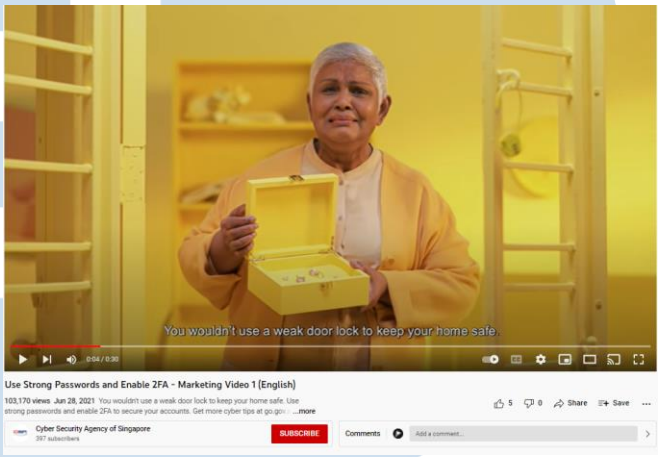
Selain tips untuk 3 kategori *user* tersebut, website juga memberikan informasi mengenai keamanan siber bisnis, menyediakan berita dan *events* terbaru mengenai keamanan siber, dan menyediakan aset-aset yang dapat diunduh, seperti *handbook* aman berinternet, tinjauan kasus-kasus kejahatan siber yang pernah terjadi, *handbook* interaktif, rekomendasi buku tentang keamanan siber, *password checker*, brosur kampanye, poster kampanye, dsb.

Gambar 3.28 Pilihan aset yang dapat diunduh pada website

Sumber:

https://www.csa.gov.sg/gosafeonline/Resources/bettercybersafethansorry

Selain itu, kampanye juga memberikan pesan dan tips tersebut dalam bentuk *video* yang diupload melalui youtube, dengan pesan yang serupa. Namun penjelasan dalam video lebih jelas dan menarik, karena dapat dijelaskan melalui visual dan audio. Video yang dibuat dan diunggah di youtube juga ditampilkan pada website kampanye tersebut.



Gambar 3.29 Video youtube kampanye *Better Cyber Safe Than Sorry*
Sumber: https://www.youtube.com/watch?v=OUHbUiiw1Q4

Gambar 3.30 Video youtube kampanye *Better Cyber Safe Than Sorry*
Sumber: https://www.youtube.com/watch?v=cKUeW7Laqis

Tabel 3.2 Data Demografis Responden

Strength	Weakness
• Gaya visual konsisten. • Branding kampanye sudah baik, dengan logo yang mudah dikenali. • Penyampaian pesan simpel dan mudah dimengerti. • Kampanye dilengkapi informasi lengkap dan konkret mengenai permasalahan tersebut. • Penyampaian pesan dibuat relate dengan permasalahan yang terlihat secara nyata.	• Media masih menggunakan media umum dan kurang interaktif. • Penyampaian pesan yang cukup straight forward, tanpa melibatkan audiens
Opportunity	Threat
• Kampanye serupa mengenai kesadaran keamanan siber belum banyak dilakukan. • Permasalahan siber sedang marak • Program kampanye ini didukung oleh pemerintah singapura.	• Penyampaian pesan kurang menarik bagi generasi muda yang menyukai pendekatan interaktif

3.2 Metodologi Perancangan

Dalam merancang kampanye, penulis akan menggunakan metode perancangan yang dirumuskan oleh Robin Landa dalam bukunya yang berjudul *Advertising by Design*. Terdapat 6 tahapan perancangan yang akan dilakukan penulis, yaitu melakukan *overview*, menentukan dan menerapkan strategi, menemukan ide, merancang desain, produksi, dan melakukan implementasi (Landa, 2010).

3.2.1. *Overview*

Pada tahap *overview*, penulis akan mengumpulkan data atau informasi mengenai topik terpilih, kemudian data atau informasi yang dicari oleh penilulis untuk perancangan ini adalah data mengenai prilaku masyarakat, terutama Gen Z dalam penggunaan internet dan penggunaan data pribadi yang mereka miliki, serta informasi mengenai kejahatan siber yang sering terjadi di Indonesia. Setelah mencari informasi dan data mengenai topik, penulis akan menganalisis data tersebut untuk menentukan strategi perancangan yang tepat.

3.2.2. *Strategy*

Pada tahapan *strategy*, penulis menentukan strategi yang akan digunakan untuk merancang kampanye. Penulis juga akan menentukan taktik pesan dari kampanye, membuat *creative brief* dan menentukan media yang akan digunakan.

3.2.3. *Idea*

Dalam tahapan *Idea*, penulis akan mencari kata kunci atau *keywords* dengan melakukan brainstorming dan *mind* mapping mengenai topik dengan mengelola data yang sudah dikumpulkan dan dikembangkan menjadi ide dan konsep perancangan. Setelah menemukan kata kunci tersebut, penulis akan membuat suatu *moodboard* yang sesuai dengan ide dan konsep tersebut, untuk dijadikan sebagai referensi perancangan desain.

3.2.4. *Design*

Pada tahap ini, penulis mulai merancang dan mengelola ide dan konsep yang telah ditentukan. Selain itu, pada tahap ini penulis akan melakukan sketsa kasar terhadap ide dan konsep yang telah dituangkan dalam bentuk visual. Pada tahap ini penulis juga akan membuat key visual dan mengevaluasi

desain yang telah dibuat untuk nantinya dilakukan revisi atau perbaikan sesuai kebutuhan.

3.2.5. *Production*

Setelah tahapan desain dilakukan, penulis akan melakukan tahapan produksi, dimana solusi desain yang telah dibuat akan dicetak dan diterapkan dalam bentuk nyata atau pada media-media yang telah ditentukan.

3.2.6. *Implementation*

Pada tahap akhir ini, desain kampanye yang telah dibuat akan diterapkan pada dunia nyata. Pada tahap ini juga, penulis menguji dan melakukan *review* terhadap desain kampanye yang telah dibuat.