ALIANSI JURNALIS INDEPENDEN
Alliance of Independent Journalist

IMS
GOOD JOURNALISM | BETTER SOCIETIES

Funded by
the European Union

LAPORAN RISET KEAMANAN DIGITAL PEMBUAT KONTEN DI INDONESIA

Laporan Riset
Keamanan Digital Pembuat Konten di Indonesia

Penulis:
Engelbertus Wendratama
Putri Laksmi Nurul Suci
Adib Muttaqin Asfar
Masduki

Penata Isi dan Perancang Sampul:
Krisna Sahwono

Agustus 2024

Aliansi Jurnalis Independen (AJI) Indonesia
Jalan Kembang Raya No. 6, Kwitang, Senen
Jakarta Pusat 10420

Telp 021-3151214, Fax 3151261
Email: sekretariat@ajindonesia.or.id
Web: www.aji.or.id

Didukung oleh:

IMS
GOOD JOURNALISM | BETTER SOCIETIES

Funded by
the European Union

Daftar Isi

Kata Pengantar

Pembuat Konten dan Ancaman Digital

Di era digital yang berkembang pesat, pembuat konten digital telah menjadi elemen esensial dalam ekosistem media modern. Mereka tidak hanya memberikan informasi dan hiburan, tetapi juga berpotensi besar dalam mendukung jurnalisme berkualitas dengan mengisi celah-celah yang sering terabaikan oleh media arus utama.

Dengan kedekatan emosional mereka dengan audiens, pembuat konten digital memiliki kemampuan untuk melawan penyebaran informasi palsu dan hoaks, serta menyediakan konten yang berbasis pada fakta dan sumber terpercaya.

Namun, meningkatnya kompleksitas teknologi dan ancaman serangan digital menjadikan pembuat konten digital sebagai sasaran utama kejahatan siber. Data SAFEnet menunjukkan bahwa insiden keamanan digital meningkat dari tahun ke tahun, menciptakan tantangan signifikan bagi integritas, keamanan, dan privasi para pembuat konten.

Dengan fenomena di atas, Aliansi Jurnalis Independen (AJI) dan para ahli media yang tergabung dalam PR2Media melakukan riset terkait situasi dan keamanan pembuat konten digital.

Penelitian ini diharapkan mampu memahami sistem keamanan digital di platform media sosial yang digunakan oleh pembuat konten digital, serta mengidentifikasi potensi bahaya, kerentanan, dan risiko yang mereka hadapi.

AJI dan PR2Media melibatkan tiga jenis responden untuk penelitian ini.

Responden pertama adalah pembuat konten digital yang fokus pada isu kelompok minoritas serta mewakili representasi daerah barat, tengah, dan timur Indonesia, sedangkan responden kedua adalah pembuat konten yang fokus pada produk yang terkait dengan kepentingan-kepentingan publik (kesehatan, isu sosial, lingkungan, dll) melalui platform digital.

Sementara responden ketiga adalah para jurnalis warga dan pers mahasiswa.

Ketiga responden itu punya kesamaan yaitu jenis produk yang dihasilkan berbau jurnalisme.

Dengan melibatkan 312 responden dari berbagai wilayah di Indonesia, penelitian ini mengukur indeks keamanan digital melalui empat aspek utama: persepsi terhadap keamanan digital, pengalaman menerima serangan digital, dampak serangan digital, dan praktik penanganan serangan digital.

Hasil penelitian menunjukkan bahwa meskipun indeks keamanan digital pembuat konten relatif baik, dengan nilai 2,41 dari maksimal 4, masih terdapat kekhawatiran signifikan, terutama terkait dengan pengalaman dan dampak serangan digital.

Jenis serangan digital yang sering dialami para pembuat konten ini juga nyaris sama, yaitu "diawasi/*stalked*", "*phishing*", "*bullying*, ancaman, dan intimidasi yang bukan berbasis gender", dan "peretasan/pengambilalihan akun media sosial".

Temuan lain yang tak kalah mencengangkannya adalah pembuat konten yang memproduksi konten kepentingan publik lebih rentan mengalami serangan digital, dibandingkan dengan yang tidak memproduksi konten kepentingan publik.

Melalui temuan-temuan ini, AJI mendorong peningkatan pengetahuan dan kecakapan pembuat konten digital serta mendorong transparansi dan akuntabilitas dari platform media sosial dan regulasi pemerintah yang mendukung keamanan digital.

Buku ini adalah salah satu persembahan AJI untuk dunia digital yang semakin "*crowded*" dengan kondisi kemajuan teknologi yang semakin cepat dan juga kejahatan dunia digital yang kreatif.

AJI mengucapkan terima kasih juga disampaikan untuk para enumerator yang sudah bekerja keras mengumpulkan informasi dari seluruh Indonesia. Kemudian rasa terima kasih tak terhingga juga disampaikan pada lembaga PR2Media yang sudah menterjemahkan data dan informasi dari enumerator untuk dianalisis.

AJI berharap buku ini menjadi panduan bagi semua pihak yang terlibat dalam ekosistem media digital.

Terima kasih

Nany Afrida
Ketua Umum AJI

Ringkasan Eksekutif

Penelitian ini mengidentifikasi dan mengukur indeks keamanan digital pembuat konten melalui empat aspek, yaitu persepsi tentang keamanan digital, pengalaman menerima serangan digital, dampak serangan digital, dan praktik menangani serangan digital. Berdasarkan penghitungan terhadap empat aspek tersebut, indeks keamanan digital pembuat konten yang menjadi responden riset ini cukup baik, yaitu memiliki nilai 2,41 dari nilai maksimal 4.

Aspek yang mencatat nilai paling tinggi adalah pengalaman menerima serangan digital, dengan nilai 3,33 dari maksimal 4. Nilai yang baik ini disebabkan seluruh responden (312 responden) rata-rata "sangat jarang" hingga "tidak pernah" mengalami 12 jenis serangan digital yang ditanyakan. Meski demikian, dari 312 responden, 63,5% di antara mereka menyatakan pernah mengalami setidaknya satu jenis serangan digital selama lima tahun terakhir. Ada empat jenis serangan digital yang perlu mendapat perhatian khusus karena keempatnya paling sering dialami pembuat konten, yaitu "diawasi/*stalked*", "*phishing*", "*bullying*, ancaman, dan intimidasi yang bukan berbasis gender", dan "peretasan/pengambilalihan akun media sosial".

Kemudian, bagi pembuat konten yang mengalami serangan digital, dampaknya sangat merugikan mereka. Hal ini ditunjukkan oleh nilai pada aspek dampak serangan digital yang nilainya paling rendah dibanding aspek lainnya (1,14 dari maksimal 4) dan berada di wilayah skala "tidak baik". Serangan digital sangat merugikan para pembuat konten, yaitu terancamnya keamanan (fisik maupun emosional) dan privasi serta menyebabkan hilangnya akses terhadap sumber pendapatan.

Sementara itu, terdapat dua aspek yang berada di antara penilaian "cukup baik" dan "baik", yaitu persepsi terhadap keamanan digital (nilai 2,50 dari maksimal 4) dan praktik menangani serangan digital (nilai 2,67 dari maksimal 4). Hal ini menunjukkan, berdasarkan penilaian mandiri para responden, mereka menilai keamanan digital mereka dan kemampuan mereka menangani serangan digital sudah relatif baik. Akan tetapi, seperti ditunjukkan dalam diskusi kelompok terarah, mereka tetap membutuhkan pembaruan pengetahuan dan kecakapan secara berkala mengingat perkembangan teknologi digital yang sangat dinamis,

terutama terkait dukungan atau fasilitas dari platform media sosial dan organisasi yang bergerak di bidang keamanan digital.

Riset ini juga menghubungkan pengalaman serangan digital dengan produksi konten berkepentingan publik. Riset ini mengartikan konten yang berkepentingan publik (*public interest content*) sebagai "konten (informasi, ide, opini, dan data) yang berhubungan dengan kepentingan masyarakat, yang ditujukan untuk membantu warga dalam membuat opini atau keputusan berbasis informasi, sehingga warga bisa terlibat dalam perdebatan atau persoalan di masyarakat". Temuannya, terdapat 66,8% pembuat konten yang memproduksi konten terkait kepentingan publik yang pernah mengalami serangan digital. Sementara itu, "hanya" 48,2% pembuat konten yang tidak memproduksi konten terkait kepentingan publik yang pernah mengalami serangan digital. Ini menunjukkan, pembuat konten yang memproduksi konten kepentingan publik lebih rentan mengalami serangan digital, dibandingkan dengan yang tidak memproduksi konten kepentingan publik.

Karena itu, riset ini menggarisbawahi pentingnya langkah pengamanan digital bagi para pembuat konten—terutama konten berkepentingan publik—yang mencakup peningkatan pengetahuan dan kecakapan untuk pencegahan dan penanganan berbagai serangan digital.

Selanjutnya, 30,5% responden yang pernah melaporkan serangan digital kepada platform media sosial menyatakan "tidak puas" dan "sangat tidak puas" terhadap tanggapan platform dalam menangani aduan mereka. Karena itu, dalam diskusi kelompok terarah, para pembuat konten mengharapkan platform media sosial lebih transparan terkait tindak lanjut aduan dari mereka (misalnya, selama ini permintaan pemulihan akun hanya dilayani oleh mesin dan sangat lamban) dan terkait laporan yang dilakukan oleh pihak lain terhadap akun mereka. Dua hal itu sangat penting untuk melindungi kebebasan berekspresi sekaligus menghindari pembuat konten dari laporan palsu atau tidak akurat.

Transparansi tersebut sangat penting mengingat peran strategis platform media sosial: konten diunggah di platform media sosial, yang aturan mainnya dibuat dan ditegakkan oleh platform media sosial. Untuk itu, perlu adanya regulasi dari pemerintah (sebagai turunan Undang-Undang Informasi dan Transaksi Elektronik yang direvisi pada akhir 2023) yang bisa lebih mendorong transparansi dan akuntabilitas platform media sosial terkait pengaturan konten (*content moderation*).

BAB 1
Pendahuluan

A. Latar Belakang

Interaksi secara daring meningkat secara signifikan akibat mudahnya aksesibilitas terhadap platform media sosial. Terbukti bahwa pada 2024, terdapat 139 juta pengguna media sosial di Indonesia–yang setara dengan 49,9% dari total penduduk di Indonesia (Kemp, 2024). Seiring popularitas platform media sosial, semakin terbuka pula peluang ekonomi yang ia bawa bagi penggunanya. Sebagai contoh, pembuat konten di Instagram dan YouTube bisa mendapatkan bayaran dengan adanya penempatan iklan, penjualan *merchandise*, dan langganan, yang masih ditambah dengan adanya lokapasar di Instagram dan TikTok (YouTube, 2024; Instagram, 2024; TikTok, 2024). Perputaran ekonomi pada platform media sosial dapat disebut dengan ekonomi kreator (Peres et al., 2024). Maka tak heran jika eksistensi pembuat konten pun menjadi entitas vital dalam ekosistem media digital modern. Mereka berkontribusi menyediakan informasi dan hiburan melalui pembuatan konten yang menarik untuk berinteraksi dengan pengikut–cara ini juga meningkatkan popularitas para pembuat konten (Cai et al., 2024).

Sayangnya, interaksi daring turut disertai dengan potensi penerimaan ancaman atau serangan digital terhadap pembuat konten. Jenis ancaman dan serangan digital pun juga beragam–mulai dari tindak kekerasan berbasis gender *online*

(KBGO) (Kusuma & Arum, 2019; Wendratama et al., 2021), hingga yang mengancam keamanan data dan informasi pribadi pengguna (Almaki et al., 2021). Probabilitas ini lebih besar dialami oleh para pembuat konten yang memproduksi konten kritis, terkhusus bagi mereka yang membawa isu kepentingan publik. Berdasarkan penelitian Masduki (2022) tentang aktivitas penyampaian opini kritis secara daring, serangan digital merupakan bagian dari upaya digital untuk menindak dan menghambat kebebasan digital di Indonesia. Serangan yang dilakukan oleh pasukan siber bayaran, misalnya, semakin mengikis ruang-ruang demokratis di ranah digital (Masduki, 2022).

Salah satu kasus dialami oleh aktivis dan peneliti kebijakan publik, Ravio Patra, pada tahun 2020. Serangan digital dialami Ravio di akun Twitter miliknya (@raviopatr), akibat mengkritik Staf Khusus Presiden Billy Mambrasar yang diduga kuat terlibat konflik kepentingan dalam berbagai proyek pemerintah di Papua, serta menuliskan esai kritik terhadap penanganan pandemi COVID-19 di media Tirto.id. Uniknya, setelah serangkaian serangan digital menimpa Ravio, ia ditangkap oleh polisi akibat dituding menyiarkan pesan mengajak onar (Ibrahim, 2021). Jenis serangan digital yang diterima Ravio pun beragam, seperti hilangnya akses terhadap akun digital miliknya dan teror telepon dari banyak nomor tak dikenal. Pada akhirnya, Ravio melaporkan kasus ini kepada SAFEnet, lalu ia melakukan berbagai prosedur keamanan standar (SAFEnet, 2020).

Ancaman dan serangan digital dapat marak berlangsung akibat dipicu oleh momen tertentu. Menurut Takimai et al. (2024), kasus ancaman dan serangan digital melalui platform digital semakin banyak bermunculan seiring kian dekatnya penyelenggaraan Pemilu 2024. Maka tak heran, Pemilu 2024 menimbulkan indikasi adanya penyerangan terhadap hak-hak digital. Melalui laporannya, SAFEnet mencontohkan fenomena adanya Pasukan Siber 08 yang dibentuk oleh pendukung capres Prabowo Subianto (Takimai et al., 2024). Pasukan ini tidak hanya menjadi mesin pencari informasi untuk mendukung Prabowo, tetapi juga mengidentifikasi mereka yang dianggap melakukan kampanye negatif terhadap Prabowo Subianto melalui platform digital. Fenomena ini laksana menunjukkan bahwa bentuk represi yang difasilitasi oleh teknologi akan lebih mudah untuk membungkam banyak pihak yang dianggap memiliki opini berseberangan.

Kasus pelecehan juga dialami oleh seorang *host* Kinderflix, salah satu kanal YouTube yang memiliki perhatian terhadap edukasi anak. Seiring meningkatnya popularitas kanal YouTube Kinderflix, akun ini tidak hanya ditonton oleh anak-anak, tetapi juga orang dewasa. Alih-alih menikmati edukasi yang diberikan, orang-orang dewasa tersebut justru memberikan komentar-komentar bersifat seksual dengan nada melecehkan, yang ditujukan kepada *host* Kinderflix (Nuri, 2023).

Oleh karena itu, dengan berbagai contoh serangan digital yang menimpa pembuat konten, riset ini ditujukan untuk memetakan pengalaman serangan digital yang dialami para pembuat konten di Indonesia. Riset ini turut dilengkapi dengan langkah mitigasi yang mereka lakukan untuk mengatasi serangan digital dan harapan terkait keamanan digital mereka.

B. Tinjauan Pustaka

Serangan digital semakin tak terpisahkan dari kebebasan digital yang dialami oleh pengguna media sosial. Berdasarkan data triwulan SAFEnet terkait insiden keamanan digital di Indonesia, terdapat 72 kasus serangan digital sejak Juli hingga September 2023–yang menimpa individu dari berbagai latar belakang (SAFEnet, 2023). Tentunya, fenomena ini turut menyerang pembuat konten sebagai pelaku kreatif yang cukup akrab dengan platform media sosial. Pembuat konten merupakan seseorang atau sekelompok orang yang secara aktif berbagi konten mengenai informasi tertentu secara digital, yang ditujukan untuk menghibur dan memengaruhi orang lain (Bucci, 2023; Kemp, 2023). Saat ini, maraknya profesi sebagai pembuat konten mampu melahirkan ekonomi kreator yang disebabkan oleh kebangkitan media sosial, meluasnya ketersediaan internet berkecepatan tinggi, dan kemudahan dari platform yang memungkinkan pembuat konten untuk menjangkau audiens global (IDN Research Institute, 2024). Maka dari itu, besarnya potensi pengaruh pembuat konten terhadap arus informasi di ruang digital bisa memicu orang lain untuk melakukan serangan digital kepada mereka.

Serangan digital yang dialami oleh pembuat konten bisa berbagai macam. Bentuk ancaman digital juga dapat mengarah kepada komentar yang bersifat seksual ataupun merendahkan. Persoalan ini turut berkelindan dengan beragam jenis kekerasan berbasis gender *online* (KBGO), seperti pendekatan untuk memperdaya (*cyber grooming*), pelecehan daring (*cyber harassment*), ancaman distribusi foto atau video pribadi (*malicious distribution*), pencemaran nama baik (*online defamation*) (Kusuma & Arum, 2019). Di sisi lain, serangan digital kerap mengancam keamanan data dan informasi pribadi, serta privasi mereka sebagai pengguna. Tak heran bila serangan digital lekat dengan tindak pencurian atau peniruan identitas, peretasan, *phishing,* hingga serangan *malware* (Almaki et al., 2021).

Riset lain terkait serangan digital terhadap individu pernah dilakukan oleh PR2Media, yang memetakan berbagai serangan digital terhadap jurnalis perempuan di Indonesia. Penelitian ini memerinci jenis kekerasan digital menjadi delapan jenis (Wendratama et al., 2021), yaitu (1) Penyadapan/pemantauan percakapan telepon dan/atau konten digital; (2) Ancaman kekerasan fisik hingga pembunuhan;

(3) Informasi pribadi terkait kehidupan domestik maupun profesional pernah diunggah orang lain tanpa izin; (4) Penghinaan terkait suku/agama/ras/gender; (5) Penyebaran disinformasi/fitnah; (6) Komentar mengganggu/melecehkan bersifat seksual; (7) Komentar mengganggu/melecehkan bersifat non-seksual; (8) Komentar *body shaming* secara daring. Temuannya, jenis kekerasan digital yang paling sering dialami oleh 1.256 jurnalis perempuan yang menjadi responden adalah komentar mengganggu/melecehkan bersifat non-seksual.

Selanjutnya, berdasarkan penelitian Thomas et al. (2022) terhadap 135 pembuat konten di Amerika Serikat, 70% pembuat konten pernah mengalami intimidasi, trolling (komentar kontroversial), pelecehan seksual, dan serangan identitas. Penelitian ini juga mencatat, banyak pembuat konten yang cenderung mengabaikan serangan dan pembenci (hater) mereka, karena dianggap sebagai kejadian biasa (36%). Sebagai respons mereka terhadap serangan digital, sebagian pembuat konten memilih menyembunyikan atau menutupi persoalan pribadi untuk menghindari serangan digital (22%), memilih untuk meninggalkan platform media sosial sementara waktu (*deactive*) (44%), dan memilih untuk menutup akun media sosial untuk menghindari serangan lebih lanjut (19%) (Thomas et al., 2022).

Selain itu, terdapat penelitian dari Samermit et al. (2023) yang memetakan berbagai risiko yang didapatkan oleh pembuat konten selama melakukan pekerjaannya. Bagi sebagian pembuat konten, berbagai risiko ini dapat diperburuk oleh identitas dan karakteristik personal yang cenderung terpinggirkan. Hasil penelitian menunjukkan, hanya sebagian pembuat konten yang menyadari risiko yang mungkin akan mereka hadapi saat memulai karir mereka. Oleh karena itu, penelitian tersebut menekankan pentingnya edukasi untuk membantu meningkatkan kompetensi keamanan digital mereka (Samermit et al., 2023).

Mengadaptasi penelitian Thomas et al. (2022), Samermit et al. (2023), dan Wendratama et al., (2021), peneliti menentukan aspek dan indikator untuk mengidentifikasi keamanan digital para pembuat konten di Indonesia, yang diuraikan dalam gambar berikut.

Gambar 1. Aspek dan indikator keamanan digital pembuat konten

No.	Aspek	Indikator
1	Persepsi terhadap Keamanan Digital	Kebebasan dalam membuat dan mengunggah konten
		Kebebasan dalam berinteraksi dengan audiens atau *followers*
		Aturan komunitas (*community guidelines*) dan moderasi konten oleh platform media sosial sudah sesuai dengan harapan
		Kondisi keamanan digital akunnya sudah sesuai dengan harapan
2	Pengalaman Menerima Serangan Digital	Jenis serangan digital: a. Penyebaran rumor/fitnah b. *Doxing* (penyebaran informasi pribadi korban dengan tujuan mengancam dan mengganggu) c. Intersepsi/penyadapan (pelaku menyimpan dan membaca komunikasi/ lalu lintas internet korban) d. Peniruan identitas (pembuatan akun palsu atas nama korban) e. Peretasan/pengambilalihan akun media sosial f. *Social engineering* (taktik manipulasi psikologis supaya korban memberikan akses terhadap akun, perangkat, atau data pribadi) g. *Phishing* (tindakan pencurian informasi dengan mengarahkan korban untuk masuk ke halaman/situs palsu) h. Perampasan perangkat digital (perampasan dan "penggeledahan" isi perangkat digital, yaitu kamera, telepon seluler, dan komputer) i. Serangan digital berbasis gender (misalnya pelecehan secara verbal melalui teks dan audio visual, hingga ancaman kekerasan fisik terkait gender korban) j. *Bullying,* ancaman, dan intimidasi yang bukan berbasis gender (mencakup ancaman tindak kekerasan, ancaman pembunuhan, hingga intimidasi terkait konten)

No.	Aspek	Indikator
		k. Diawasi/*stalked* l. Korban laporan palsu (seseorang melaporkan ke platform bahwa Anda mengunggah konten berbahaya/ilegal, padahal Anda tidak melakukan itu)
		Pemicu terjadinya serangan digital: a. Atribut pribadi (usia, gender, ras, orientasi seksual) b. Keyakinan pribadi (agama, pandangan politik) c. Jenis konten yang diunggah d. Adanya relasi tertentu dengan pihak lain (figur publik atau individu yang diberitakan media)
		Pelaku serangan digital (anonim, pengikut, pembuat konten lainnya, kepentingan bisnis atau politik tertentu)
3	Dampak Serangan Digital	Merugikan keamanan dan privasi diri sendiri
		Merugikan keamanan dan privasi orang terdekat
		Kehilangan akses terhadap sumber pendapatan berbasis iklan atau sumber pendapatan lainnya
4	Praktik Menangani Serangan Digital	Mengetahui atau memiliki panduan
		Memiliki keluarga, teman dekat, atau manajer yang mendukung

Berdasarkan indikator-indikator di atas, tim peneliti menyusun pertanyaan kuesioner dan panduan diskusi kelompok terarah untuk ditanyakan kepada para responden, yang merupakan pembuat konten aktif di berbagai platform media sosial.

Kemudian, penelitian ini juga ditujukan untuk mengetahui produksi konten terkait kepentingan publik yang dihasilkan oleh pembuat konten. Berdasarkan referensi yang ada (European Court of Human Rights, 2017; McGonagle, et al., 2023), penelitian ini mengartikan konten berkepentingan publik (*public interest content*) sebagai "konten (informasi, ide, opini, dan data) yang berhubungan dengan

kepentingan masyarakat, yang ditujukan untuk membantu warga dalam membuat opini atau keputusan berbasis informasi, sehingga warga bisa terlibat dalam perdebatan atau persoalan di masyarakat". Konten mengenai kepentingan publik bisa berhubungan dengan isu kesejahteraan masyarakat, sosial, lingkungan, atau isu lain yang menjadi persoalan di tengah masyarakat. Konten berkepentingan publik perlu mendapat perhatian karena data menunjukkan, mereka rentan mengalami serangan akibat konten yang mereka produksi (Muhajir, 2020; Amnesty International, 2020; Basyari, 2023). Karena itu, penelitian ini juga mengidentifikasi hubungan antara produksi konten berkepentingan publik dan keamanan digital pembuatnya.

C. Tujuan Penelitian

1. Mengidentifikasi situasi keamanan digital yang dialami oleh pembuat konten di platform media sosial.
2. Mengidentifikasi mitigasi risiko untuk memperkuat keamanan digital pembuat konten di platform media sosial.

D. Metodologi

a. Survei
   Survei dilakukan untuk mengetahui pengalaman responden terkait keamanan digital dalam memproduksi konten di platform media sosial. Sampelnya berjumlah 312 responden dari 38 provinsi di Indonesia, dengan mempertimbangkan *margin of error* ±5,5% dan level kepercayaan 95%. Sampel diambil melalui metode *snowball sampling* yang merepresentasikan 38 provinsi di Indonesia.

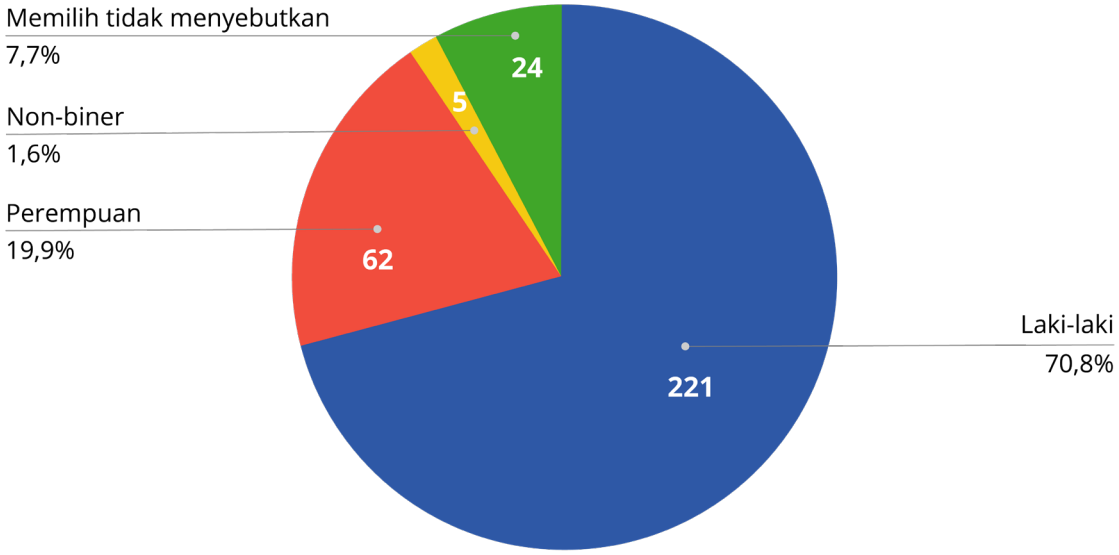
b. Diskusi kelompok terarah
   Untuk mendapatkan kedalaman dari data survei dan mengetahui lebih banyak pengalaman responden survei, peneliti melakukan diskusi kelompok terarah (FGD) secara luring dengan 16 peserta yang dipilih dari responden survei, yang mewakili keberagaman gender, pengalaman terkait serangan digital, jenis konten, dan asal provinsi.

Sebelum pengumpulan data dilakukan, rancangan riset ini sudah melalui kaji etik (*ethical clearance*) yang dilakukan oleh Pusat Pengembangan Etika Universitas Katolik Indonesia Atma Jaya dan dinyatakan "laik etik" untuk dilaksanakan.

E. Profil Responden

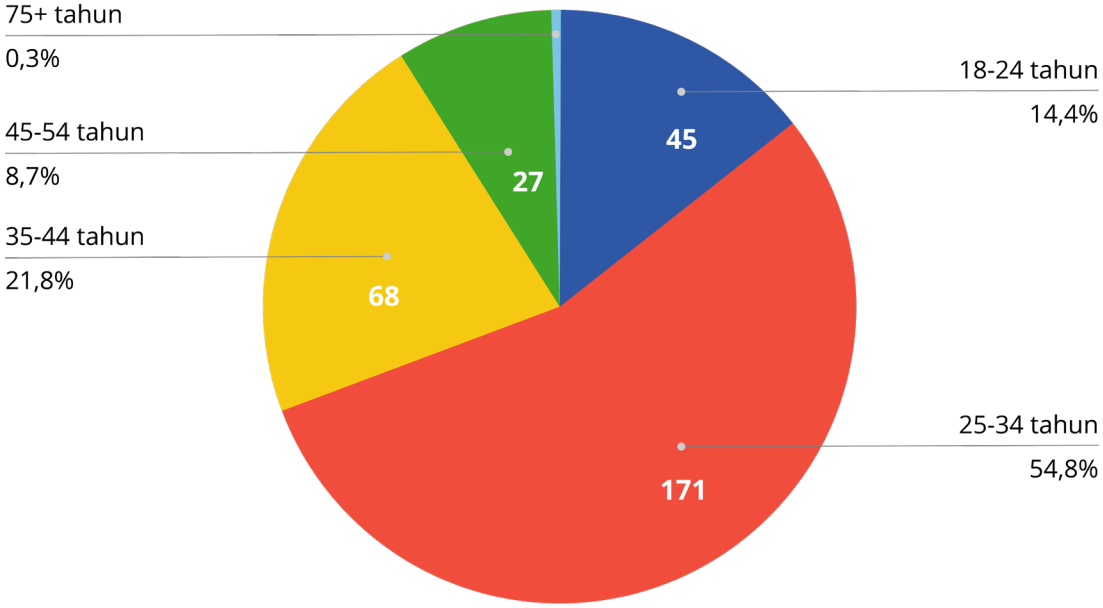
a. Gender

Gambar 2. Gender responden



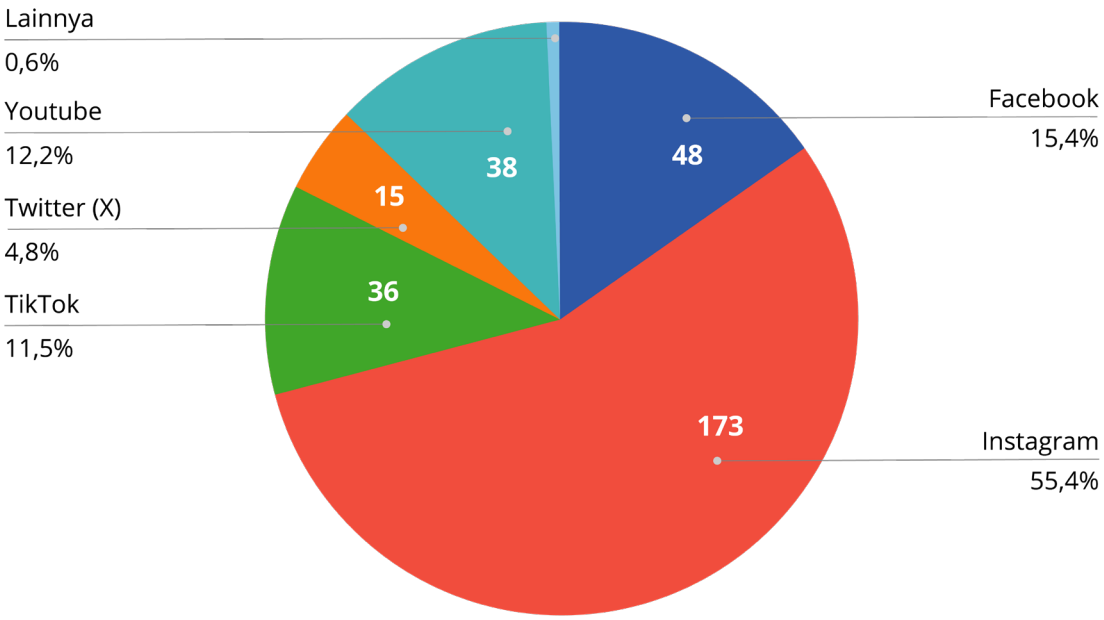
b. Usia

Gambar 3. Usia responden



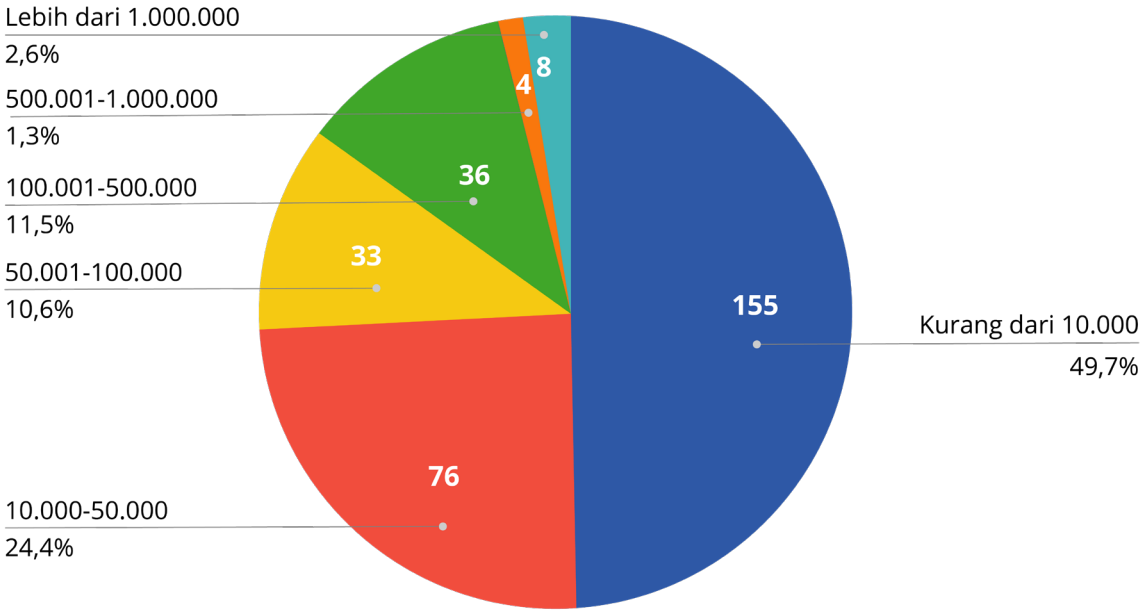
c. Platform media sosial dengan jumlah pengikut terbanyak

Gambar 4. Platform media milik responden dengan jumlah pengikut terbanyak



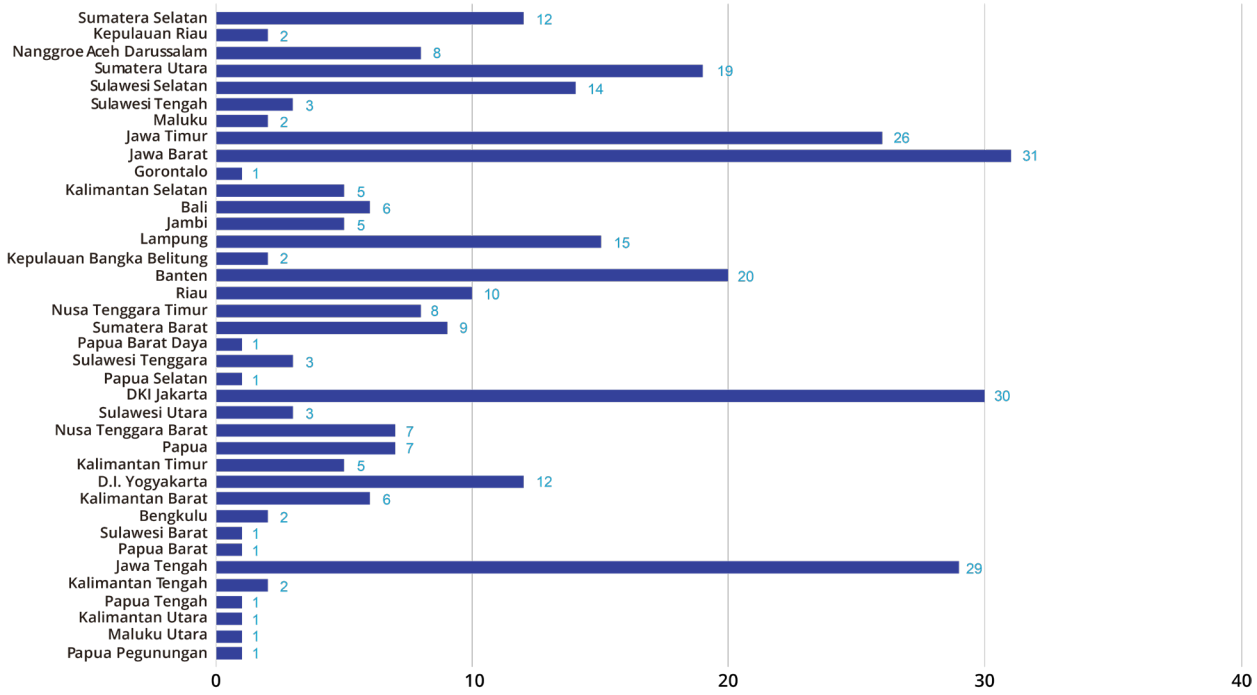
d. Jumlah pengikut (jumlah pada akun media sosial dengan pengikut terbanyak)

Gambar 5. Jumlah pengikut pada akun media sosial responden



e. Provinsi tempat tinggal

Gambar 6. Provinsi tempat tinggal responden



BAB 2
Temuan Survei

A. Persepsi terhadap Keamanan Digital

Bagian ini mengukur aspek persepsi pembuat konten terhadap keamanan di platform media sosial. Responden diminta memberikan pendapat terhadap pernyataan terkait pengalaman dan pengetahuan mereka sebagai pembuat konten. Untuk tiap pernyataan, mereka diminta memilih satu dari lima opsi jawaban, dari "Sangat tidak setuju" (memiliki nilai 0) hingga "Sangat setuju" (memiliki nilai 4). Semakin tinggi nilai (mendekati 4) maka semakin baik, semakin rendah nilai (mendekati 0) maka semakin buruk penilaian responden terhadap lingkungan digitalnya.

Empat pernyataan yang diajukan adalah:
1. Anda merasa bebas membuat dan mengunggah konten sesuai dengan keinginan/minat Anda tanpa takut mengalami serangan digital.
2. Kebijakan aturan komunitas (*community guidelines*) dan moderasi konten oleh platform media sosial sudah sesuai dengan harapan Anda.
3. Anda merasa bebas untuk berinteraksi dengan pengikut (*followers*) tanpa khawatir memperbesar risiko terjadinya serangan digital.
4. Kondisi keamanan digital akun Anda baik dan sudah sesuai dengan apa yang Anda harapkan.

Hasil olah data menunjukkan nilai jawaban para responden terhadap empat indikator tersebut, ditampilkan dalam gambar di bawah ini.

Gambar 7. Nilai persepsi terhadap keamanan digital

No.	Indikator	Nilai rata-rata responden	Skala
1	Pembuat konten merasa bebas membuat dan mengunggah konten sesuai dengan keinginan/ minatnya tanpa takut mengalami serangan digital.	2,47	0–4
2	Kebijakan aturan komunitas (*community guidelines*) dan moderasi konten oleh platform media sosial sudah sesuai dengan harapan pembuat konten.	2,41	0–4
3	Pembuat konten merasa bebas untuk berinteraksi dengan pengikut (*followers*) tanpa khawatir memperbesar risiko terjadinya serangan digital.	2,47	0–4
4	Kondisi keamanan digital akun pembuat konten baik dan sudah sesuai dengan apa yang ia harapkan.	2,63	0–4
	Total	2,50	0–4

Keterangan:
0: Sangat tidak baik, 1: Tidak baik, 2: Cukup baik, 3: Baik, 4: Sangat baik

Berdasarkan temuan di atas, persepsi para pembuat konten terhadap keamanan digital mereka bernilai 2,50, yaitu di antara “cukup baik” dan “baik”. Indikator yang memiliki nilai paling rendah dalam aspek ini adalah “Kebijakan aturan komunitas (*community guidelines*) dan moderasi konten oleh platform media sosial sudah sesuai dengan harapan pembuat konten” (nilai 2,41). Catatan mengenai ketidakpuasan para pembuat konten terhadap aturan komunitas dan pengaturan konten (*content moderation*) oleh platform diuraikan dalam temuan diskusi kelompok terarah di bab selanjutnya.

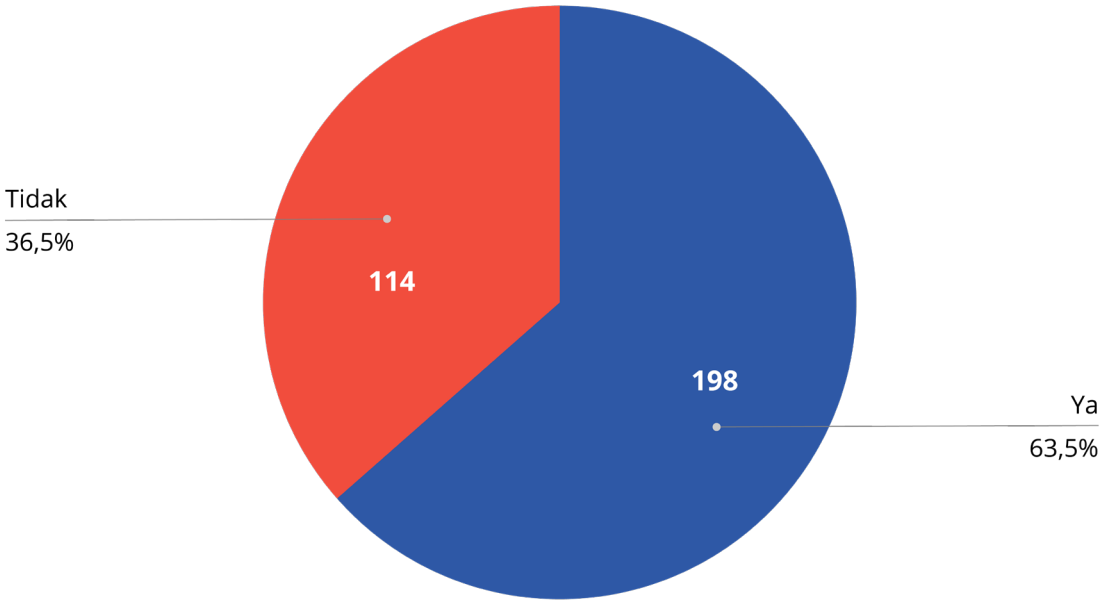
B. Pengalaman Menerima Serangan Digital

1. Apakah Anda pernah mengalami serangan digital dalam lima tahun terakhir ini?

Serangan digital ini mencakup:

a. Penyebaran rumor/fitnah
b. *Doxing* (penyebaran informasi pribadi korban dengan tujuan mengancam dan mengganggu)
c. Intersepsi/penyadapan (pelaku menyimpan dan membaca komunikasi/lalu lintas internet korban)
d. Peniruan identitas (pembuatan akun palsu atas nama korban)
e. Peretasan/pengambilalihan akun media sosial
f. *Social engineering* (taktik manipulasi psikologis supaya korban memberikan akses terhadap akun, perangkat, atau data pribadi)
g. *Phishing* (tindakan pencurian informasi dengan mengarahkan korban untuk masuk ke halaman/situs palsu)
h. Perampasan perangkat digital (perampasan dan "penggeledahan" isi perangkat digital, yaitu kamera, telepon seluler, dan komputer)
i. Serangan digital berbasis gender (misalnya pelecehan secara verbal melalui teks dan audio visual, hingga ancaman kekerasan fisik terkait gender korban)
j. *Bullying*, ancaman, dan intimidasi yang bukan berbasis gender (mencakup ancaman tindak kekerasan, ancaman pembunuhan, hingga intimidasi terkait konten)
k. Diawasi/*stalked*
l. Korban laporan palsu (seseorang melaporkan ke platform bahwa Anda mengunggah konten berbahaya/ilegal, padahal Anda tidak melakukan itu)

Gambar 8. Pembuat konten yang pernah dan tidak pernah mengalami serangan digital dalam lima tahun terakhir (N=312)



2. Apakah Anda pernah mendapatkan serangan digital di bawah ini?

Pada bagian ini, responden yang memilih jawaban "Ya" (198 responden) pada pertanyaan sebelumnya akan diminta mengidentifikasi lebih lanjut jenis serangan digital yang pernah menimpa mereka. Terdapat lima opsi jawaban pada bagian ini, yaitu "Tidak pernah" (memiliki nilai 4) hingga "Selalu" (memiliki nilai 0) untuk setiap jenis serangan digital, dan responden hanya dapat memilih satu opsi jawaban. Kemudian, seluruh responden yang menyatakan tidak pernah mengalami serangan (114 responden) dihitung menjawab "Tidak pernah" untuk semua jenis serangan.

Gambar 9. Jenis serangan digital yang pernah dialami pembuat konten (N=312)

Jenis serangan digital		Nilai rata-rata responden	Skala
a	Penyebaran rumor/fitnah	3,38	0–4
b	Doxing (penyebaran informasi pribadi korban dengan tujuan mengancam dan mengganggu)	3,47	0–4
c	Intersepsi/penyadapan (pelaku menyimpan dan membaca komunikasi/lalu lintas internet korban)	3,57	0–4
d	Peniruan identitas (pembuatan akun palsu atas nama korban)	3,36	0–4
e	Peretasan/pengambilalihan akun media sosial	3,24	0–4
f	Social engineering (taktik manipulasi psikologis supaya korban memberikan akses terhadap akun, perangkat, atau data pribadi)	3,31	0–4
g	Phishing (tindakan pencurian informasi dengan mengarahkan korban untuk masuk ke halaman/ situs palsu)	2,97	0–4
h	Perampasan perangkat digital (perampasan dan “penggeledahan” isi perangkat digital, yaitu kamera, telepon seluler, dan komputer)	3,69	0–4
i	Serangan digital berbasis gender (misalnya pelecehan secara verbal melalui teks dan audio visual, hingga ancaman kekerasan fisik terkait gender korban)	3,43	0–4

Jenis serangan digital		Nilai rata-rata responden	Skala
j	Bullying, ancaman, dan intimidasi yang bukan berbasis gender (mencakup ancaman tindak kekerasan, ancaman pembunuhan, hingga intimidasi terkait konten)	3,23	0–4
k	Diawasi/stalked	2,91	0–4
l	Korban laporan palsu (seseorang melaporkan ke platform bahwa Anda mengunggah konten berbahaya/ilegal, padahal Anda tidak melakukan itu)	3,40	0–4
	Total	3,33	0–4

Keterangan:
0: Selalu, 1: Sering, 2: Kadang, 3: Sangat jarang, 4: Tidak pernah

Berdasarkan olah data tersebut, nilai rata-rata para responden adalah 3,33 atau berada di antara "tidak pernah" dan "sangat jarang" mengalami 12 serangan digital tersebut. Meski demikian, ada empat jenis serangan yang memiliki nilai paling rendah (paling sering dialami), yaitu "diawasi/*stalked*" (2,91), "*phishing*" (2,97), "*bullying*, ancaman, dan intimidasi yang bukan berbasis gender" (3,23), dan "peretasan/pengambilalihan akun media sosial" (3,24). Terkait empat jenis serangan itu dan jenis serangan lainnya, para pembuat konten perlu memiliki langkah-langkah mitigasi sehingga ketika serangan tersebut muncul, mereka sudah siap menghadapinya.

3. Apa faktor pemicu terjadinya ancaman atau serangan digital tersebut?

Untuk pertanyaan ini, responden dapat memilih lebih dari satu pilihan jawaban. Jawaban responden tampak dalam gambar di bawah ini.

Gambar 10. Faktor pemicu terjadinya serangan digital terhadap pembuat konten
(N=198)

No.	Faktor pemicu	Frekuensi	Persentase
1	Atribut pribadi (usia, gender, ras, orientasi seksual)	44	12,4%
2	Keyakinan pribadi (agama, pandangan politik)	75	21,1%
3	Jenis konten yang diunggah	138	38,9%
4	Adanya relasi tertentu dengan pihak lain (figur publik atau individu yang diberitakan media)	76	21,4%
5	Lainnya	22	6,2%
	Total	355	100%

Berdasarkan data yang dihimpun, menurut para responden, faktor terbanyak yang menjadi pemicu terjadinya serangan digital adalah jenis konten yang diunggah (38,9%), diikuti oleh relasi tertentu dengan pihak lain (figur publik atau individu yang diberitakan media) (21,4%), dan keyakinan pribadi (21,1%).

Sementara itu, atribut pribadi (usia, gender, ras, dan orientasi seksual) tidak menjadi faktor kuat dalam memicu serangan digital (12,4%). Temuan ini menarik karena, jika kita melihat riset Thomas et al. (2022) terhadap 135 pembuat konten di Amerika Serikat, para pembuat konten di Amerika Serikat paling mengkhawatirkan atribut pribadi dan keyakinan pribadi sebagai faktor yang memicu serangan digital. Penjelasan terhadap perbedaan ini berada di luar cakupan riset ini, tapi hal ini menarik untuk diulas lebih lanjut dalam riset berikutnya, misalnya dengan mempertimbangkan konteks sosial politiknya.

4. Siapa pelaku serangan digital tersebut?

Di sini responden dapat memilih lebih dari satu jawaban, dengan jawaban mereka ditampilkan gambar di bawah ini.

Gambar 11. Pelaku serangan digital terhadap pembuat konten (N=198)

No.	Pelaku serangan	Frekuensi	Persentase
1	Orang tidak dikenal/anonim	195	50,7%
2	Seseorang yang sebelumnya pernah melakukannya	13	3,4%
3	Penggemar atau pengikut (*follower*)	52	13,5%
4	Pembuat konten lainnya	27	7%
5	Kepentingan bisnis tertentu	30	7,8%
6	Kepentingan politik tertentu	63	16,4%
7	Lainnya	5	1,3%
	Total	385	100%

Berdasarkan jawaban para responden, ditemukan bahwa 43,9% pelaku serangan digital terhadap pembuat konten adalah orang yang tidak dikenal atau anonim. Kemudian diikuti dengan pihak terkait kepentingan politik tertentu (16,4%) dan penggemar atau pengikut (*follower*) (13,5%). Kepentingan politik tertentu, yang dipilih oleh sebagian besar responden setelah pelaku anonim, akan diulas dalam temuan diskusi kelompok terarah.

C. Dampak Serangan Digital

Di bagian ini, responden diminta memberikan pendapat terhadap tiga pernyataan terkait pengalaman mereka setelah menerima serangan digital. Untuk setiap pernyataan, responden diminta memilih satu dari lima opsi jawaban, dari "Sangat setuju" (memiliki nilai 0) hingga "Sangat tidak setuju" (memiliki nilai 4). Semakin rendah nilai (mendekati 0), penilaian pun akan semakin baik. Sedangkan, semakin tinggi nilai (mendekati 4), penilaian pun akan semakin buruk.

Tiga pernyataan yang diajukan adalah:

1. Serangan digital yang pernah terjadi sangat merugikan keamanan (fisik maupun emosional) dan privasi Anda.
2. Serangan digital yang terjadi mengancam keamanan (fisik maupun emosional) dan privasi yang dimiliki oleh orang terdekat Anda, misalnya: keluarga dan teman.
3. Serangan digital yang terjadi menyebabkan Anda kehilangan akses terhadap sumber pendapatan berbasis iklan atau sumber pendapatan lainnya.

Hasil olah data jawaban para responden terhadap tiga indikator tersebut ditampilkan gambar berikut ini.

Gambar 12. Dampak serangan digital
(N=198)

No.	Faktor pemicu	Nilai rata-rata responden	Skala
1	Serangan digital yang pernah terjadi sangat merugikan keamanan (fisik maupun emosional) dan privasi pembuat konten.	0,62	0–4
2	Serangan digital yang terjadi mengancam keamanan dan privasi yang dimiliki oleh orang terdekat (misalnya: keluarga dan teman pembuat konten).	1,18	0–4
3	Serangan digital yang terjadi menyebabkan pembuat konten kehilangan akses terhadap sumber pendapatan berbasis iklan atau sumber pendapatan lainnya.	1,62	0–4
	Total	1,14	0–4

Keterangan:
0: Sangat setuju, 1: Setuju, 2: Cukup setuju, 3: Tidak setuju, 4: Sangat tidak setuju

Berdasarkan olah data tersebut, secara umum jawaban responden berada di antara jawaban “Sangat setuju” dan “Cukup setuju”. Indikator yang memiliki nilai paling rendah adalah indikator pertama, yaitu serangan digital sangat merugikan keamanan dan privasi pembuat konten (nilai 0,62). Dampak-dampak ini diulas

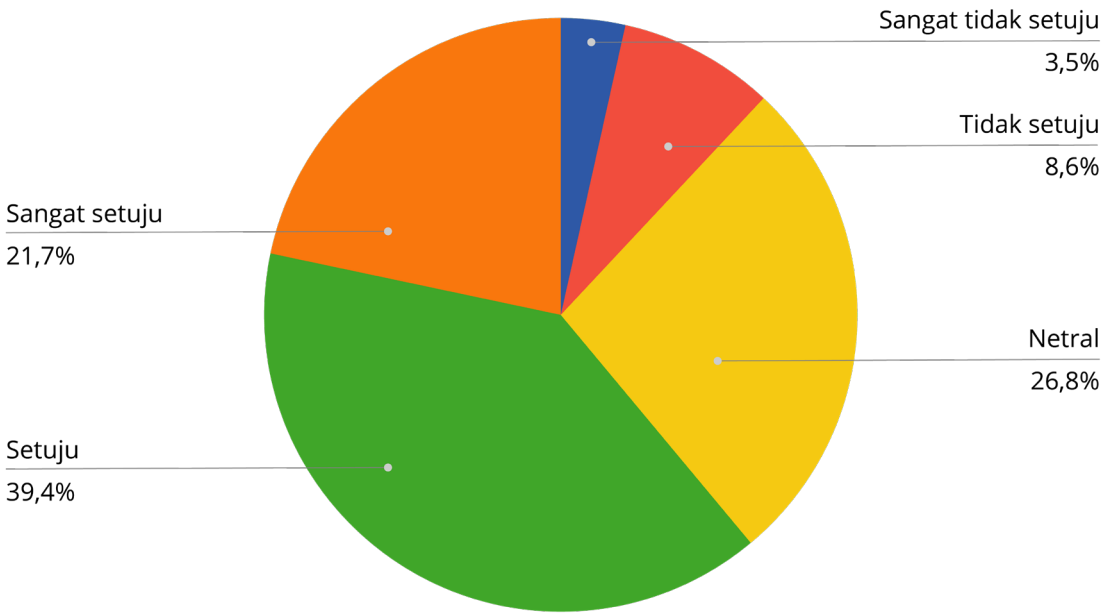
dalam laporan diskusi kelompok terarah.

D. Praktik Menangani Serangan Digital

1. Ketika serangan digital terjadi, Anda memiliki pengetahuan dan kecakapan yang memadai untuk menanganinya.

Pada pertanyaan ini, responden diminta memilih satu dari lima opsi jawaban, yaitu dari "Sangat tidak setuju" (memiliki nilai 0) hingga "Sangat setuju" (memiliki nilai 4) sesuai kondisi responden saat itu.

Gambar 13. Pengetahuan dan kecakapan pembuat konten dalam menangani serangan digital
(N=198)



Berdasarkan keseluruhan jawaban responden, ditemukan nilai rata-rata jawaban sebesar 2,67 (dengan skala 0–4). Dalam skala penilaian riset ini, nilai 2,67 berada di antara "Cukup setuju" (nilai 2) dan "Setuju" (nilai 3), yang berarti secara umum pembuat konten merasa memiliki pengetahuan dan kecakapan yang cukup memadai untuk menangani serangan digital.

2. Ketika terjadi serangan digital, kepada siapa Anda meminta bantuan?

Pada bagian ini, responden dapat memilih lebih dari satu jawaban. Melalui data yang dikumpulkan, persentase tertinggi (28,5%) menunjukkan bahwa pembuat konten cenderung meminta bantuan kepada platform media sosial yang menjadi medium tempat terjadinya serangan digital. Selanjutnya, diikuti dengan meminta bantuan kepada teman atau keluarga (27,1%) dan pengikut (*follower*) (11,5%). Pada pilihan "Lainnya", beberapa responden menuliskan contoh jaringan atau lembaga yang bergerak di bidang keamanan digital, seperti SAFEnet (Southeast Asia Freedom of Expression Network, https://safenet.or.id/) dan TRACE (Tim Reaksi Cepat, https://lapor.trace.mu/), yang menyediakan layanan bantuan untuk mengadukan atau melaporkan kasus yang melanggar hak-hak digital yang dialami oleh diri sendiri atau orang lain.

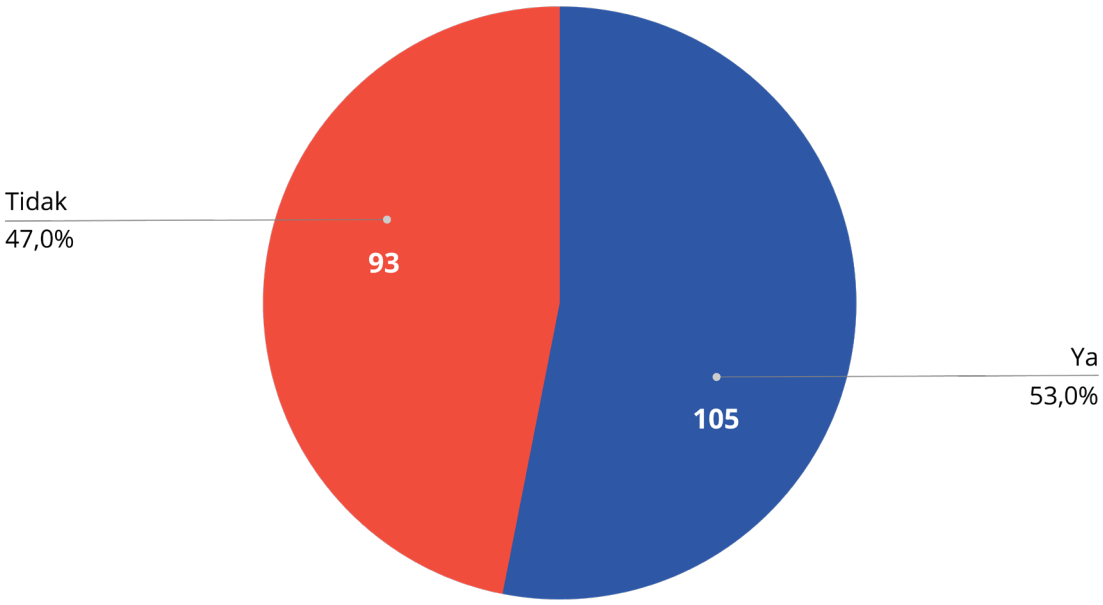
Gambar 14. Pihak yang dimintai bantuan oleh pembuat konten ketika mengalami serangan digital
(N=198)

No.	Pihak yang dimintai bantuan	Frekuensi	Persentase Responden
1	Teman atau keluarga	92	27,1%
2	Pengikut (*follower*)	39	11,5%
3	Manajer atau asisten	22	6,5%
4	Platform media sosial yang menjadi medium terjadinya serangan digital	97	28,5%
5	Penegak hukum	38	11,2%
6	Tidak ada	32	9,4%
7	Lainnya	20	5,9%
	Total	340	100%

3. Apakah Anda pernah melaporkan serangan digital yang Anda alami kepada pihak platform media sosial (layanan aduan platform)?

Pertanyaan ini meminta 198 responden untuk mengonfirmasi lebih lanjut terkait pernah atau tidaknya melaporkan kejadian serangan digital kepada pihak platform media sosial. Ditemukan 105 responden (53%) pernah memanfaatkan layanan aduan platform, dan 93 responden (47%) lainnya tidak pernah melakukan.

Gambar 15. Pembuat konten yang pernah dan tidak pernah melaporkan serang digital ke platform media sosial (N=198)



4. Mengapa Anda tidak melaporkan serangan tersebut kepada platform media sosial?

Pada bagian ini, 93 responden yang memilih opsi "Tidak" pada pertanyaan sebelumnya, diminta untuk menjawab pertanyaan ini dan boleh memilih lebih dari satu opsi jawaban. Temuan menunjukkan, alasan tertinggi yang memicu pembuat konten tidak melaporkan kasusnya kepada platform media sosial adalah cara atau prosedur melapor yang susah (28,1%), diikuti dengan pelaporan yang menghabiskan banyak waktu (23,5%) dan tindakan platform yang tidak sesuai harapan (17,6%).

Opsi jawaban “Lainnya” mempersilakan responden untuk menuliskan alasan lain yang belum termasuk ke dalam opsi jawaban yang disediakan. Hasilnya, beberapa responden menuliskan bahwa pelaporan dirasa belum diperlukan karena masih bisa ditangani secara mandiri. Selain itu, terdapat pula kekhawatiran bila pelaporan kepada platform media sosial harus mengeluarkan sejumlah biaya tertentu.

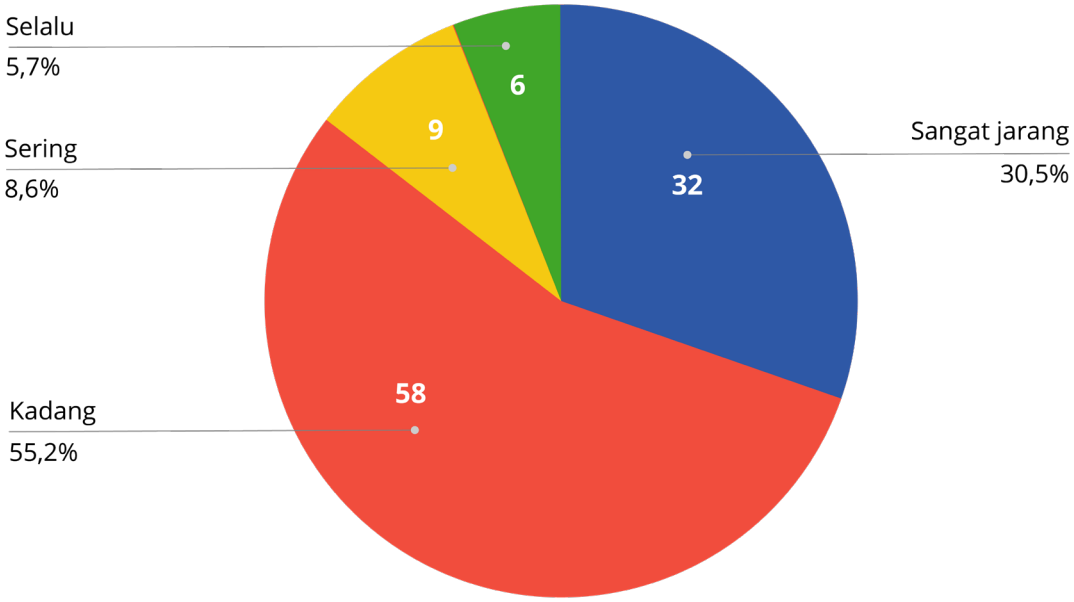
Gambar 16. Alasan pembuat konten tidak melaporkan serangan digital kepada platform media sosial (N=93)

No.	Alasan tidak melaporkan serangan digital kepada platform media sosial	Frekuensi	Persentase
1	Cara/prosedur melapor yang susah	43	28,1%
2	Pelaporan menghabiskan banyak waktu	36	23,5%
3	Pengalaman sebelumnya bahwa tindakan yang dilakukan platform tidak sesuai harapan	27	17,6%
4	Minimnya transparansi dan akuntabilitas platform dalam menanggapi dan menindaklanjuti aduan	30	19,6%
5	Lainnya	17	11,1%
	Total	153	100%

5. Seberapa sering Anda melaporkan serangan yang Anda alami tersebut kepada pihak platform (layanan aduan platform)?

Pertanyaan ini ditujukan bagi 105 responden yang menyatakan pernah melaporkan serangan digital kepada platform media sosial. Temuan menunjukkan, sebesar 55,2% responden menjawab “Kadang” melaporkan ke pihak platform media sosial, diikuti dengan “Sangat jarang” (30,5%) dan “Sering” (8,6%).

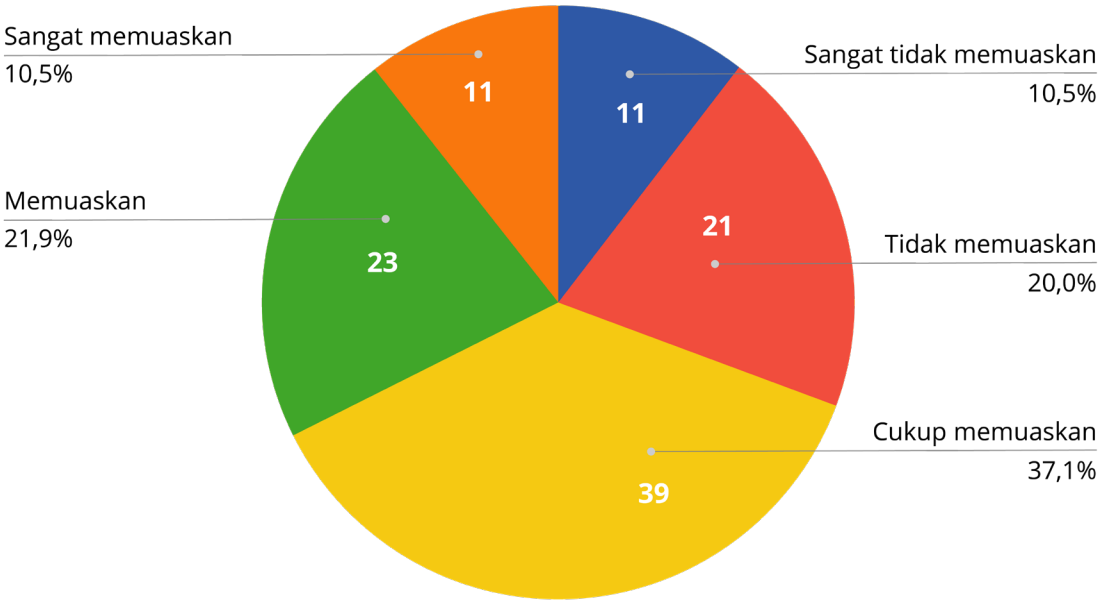
Gambar 17. Frekuensi melaporkan serangan digital kepada platform media sosial (N=105)



6. Bagaimana tindakan platform dalam menanggapi aduan Anda?

Bagian ini masih ditujukan kepada 105 responden yang pernah melaporkan serangan digital kepada platform media sosial. Terdapat lima opsi jawaban, mulai dari “Sangat tidak memuaskan” (memiliki nilai 0) hingga “Sangat memuaskan” (memiliki nilai 4). Para pembuat konten diminta untuk memilih satu dari lima opsi jawaban, yang didasari oleh pengalaman masing-masing.

Gambar 18. Tindakan platform dalam menanggapi aduan pembuat konten
(N=105)



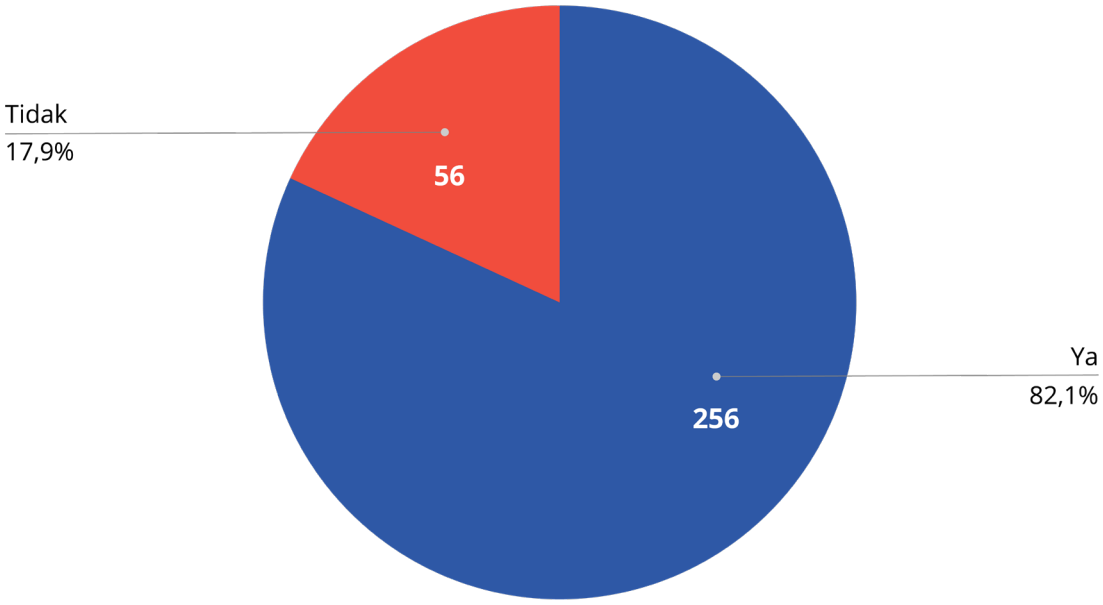
Temuan survei menunjukkan, nilai rata-rata jawaban responden berada pada skor 2,02 (dengan skala 0–4). Nilai tersebut menandakan, jawaban pembuat konten berada pada nilai "Cukup memuaskan" (nilai 2), yang berarti mereka cukup puas dengan tanggapan platform dalam menangani aduan. Meski demikian, terdapat 30,5% responden yang menyatakan bahwa tanggapan platform "Tidak memuaskan" dan "Sangat tidak memuaskan". Hal ini senada dengan temuan pada bagian pertama di kuesioner tentang persepsi terhadap keamanan digital, yaitu masih cukup banyak responden yang belum puas dengan aturan komunitas dan moderasi konten oleh platform media sosial.

E. Konten terkait Kepentingan Publik

1. Apakah Anda membuat konten yang terkait kepentingan publik?

Penelitian ini mendefinisikan konten terkait kepentingan publik sebagai "konten yang berhubungan dengan kepentingan masyarakat, isu sosial, atau persoalan di tengah masyarakat". Jenis konten ini diharapkan mampu membantu warga untuk dapat terlibat dalam perdebatan atau persoalan di masyarakat. Hasil menunjukkan terdapat 256 responden (82,1%) yang memproduksi konten terkait kepentingan publik.

Gambar 19. Jumlah pembuat konten yang menyajikan konten terkait kepentingan publik (N=312)



Pada bagian ini, peneliti juga melakukan tabulasi silang untuk membandingkan pengalaman menerima serangan digital antara pembuat konten yang memproduksi konten terkait kepentingan publik dan pembuat konten yang tidak memproduksi konten terkait kepentingan publik.

Gambar 20. Perbandingan pengalaman antara pembuat konten yang memproduksi dan tidak memproduksi konten kepentingan publik

No.	Kategori responden	Jumlah responden	Jumlah responden yang mengalami serangan digital	Jumlah responden yang tidak mengalami serangan digital	Persentase responden yang mengalami serangan digital dibandingkan yang tidak mengalami untuk tiap kategori
1	Pembuat konten yang memproduksi konten terkait kepentingan publik	256	171	85	66,8%
2	Pembuat konten yang tidak memproduksi konten terkait kepentingan publik	56	27	29	48,2%
	Total	312	198	114	-

Hasil temuan menunjukkan, terdapat 66,8% pembuat konten yang memproduksi konten terkait kepentingan publik yang mengalami serangan digital. Sementara itu, terdapat 48,2% pembuat konten yang tidak memproduksi konten terkait kepentingan publik yang mengalami serangan digital. Hal ini menunjukkan, pembuat konten yang memproduksi konten kepentingan publik lebih rentan mengalami serangan digital, dibandingkan dengan yang tidak memproduksi konten kepentingan publik.

2. Jenis/isu persoalan terkait kepentingan publik yang kerap dibahas oleh pembuat konten

Pertanyaan ini ditujukan bagi 256 responden yang memproduksi konten terkait kepentingan publik. Di sini, para pembuat konten dapat memilih lebih dari satu opsi jawaban, serta dapat menuliskan jawaban lainnya di luar opsi jawaban yang diberikan. Hasilnya, isu lingkungan menjadi isu tertinggi yang diproduksi

oleh pembuat konten (15,8%). Diikuti dengan isu politik (12,2%) dan hukum (11,3%). Sementara itu, pada opsi "Lainnya" ditemukan beragam isu lain, seperti perempuan, hak asasi manusia (HAM), perencanaan atau pembangunan wilayah, sejarah, olahraga, serta budaya dan kesenian.

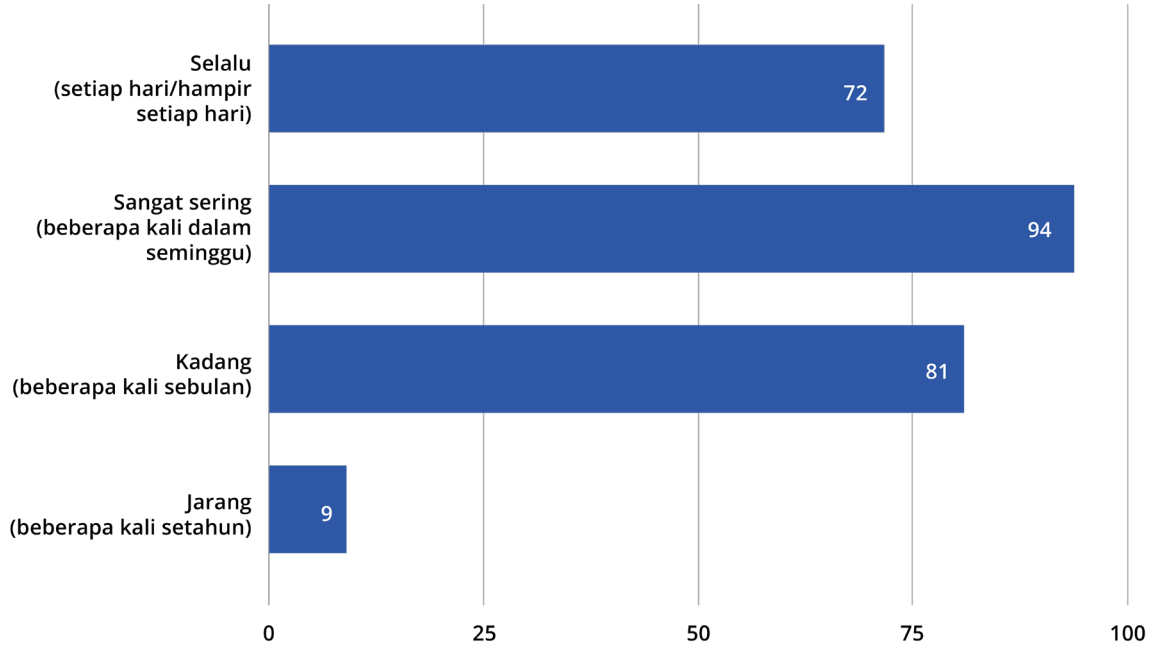
Gambar 21. Jenis/isu persoalan terkait kepentingan publik yang diproduksi oleh pembuat konten (N=256)

No.	Jenis isu/persoalan	Frekuensi	Persentase
1	Lingkungan	175	15,8%
2	Kesehatan	83	7,5%
3	Politik	135	12,2%
4	Hukum	125	11,3%
5	Minoritas gender	56	5,1%
6	Masyarakat adat	100	9%
7	Minoritas agama/ kepercayaan	65	5,9%
8	Disabilitas	43	3,9%
9	Teknologi	54	4,9%
10	Ekonomi	95	8,6%
11	Pendidikan	123	11,1%
12	Lainnya	52	4,7%
	Total	1106	100%

3. Frekuensi pembuat konten memproduksi konten terkait kepentingan publik

Bagian ini masih terpusat kepada 256 responden yang memproduksi konten terkait kepentingan publik. Peneliti hendak mengetahui frekuensi waktu pembuatan konten kepentingan publik yang dilakukan oleh pembuat konten. Berdasarkan data yang dikumpulkan, terdapat 94 pembuat konten yang mengaku "Sangat sering" memproduksi konten terkait kepentingan publik. Pada penelitian ini, "Sangat sering" memiliki arti produksi konten yang dilakukan beberapa kali dalam seminggu. Kemudian, diikuti dengan 81 responden menjawab "Kadang" (beberapa kali dalam sebulan), serta 72 responden yang menjawab "Selalu" (setiap hari atau hampir setiap hari).

Gambar 22. Frekuensi pembuat konten memproduksi konten terkait kepentingan publik
(N=256)



F. Indeks keamanan digital pembuat konten

Penelitian ini merancang pengukuran keamanan digital pembuat konten melalui empat aspek, yaitu persepsi tentang keamanan digital, pengalaman menerima serangan digital, dampak serangan digital, dan praktik menangani serangan

digital. Berdasarkan hasil penghitungan empat aspek tersebut, berikut gambar yang menunjukkan indeks keamanan digital pembuat konten yang menjadi responden survei.

Gambar 23. Indeks keamanan digital pembuat konten

No.	Aspek	Jumlah Indikator	Nilai rata-rata responden	Skala
1	Persepsi tentang keamanan digital	4	2,50	0–4
2	Pengalaman menerima serangan digital	12	3,33	0–4
3	Dampak serangan digital	3	1,14	0–4
4	Praktik menangani serangan digital	1	2,67	0–4
	Total	20	2,41	0–4

Keterangan:

0: Sangat tidak baik, 1: Tidak baik, 2: Cukup baik, 3: Baik, 4: Sangat baik

Berdasarkan hasil olah data, aspek yang memiliki nilai paling tinggi adalah pengalaman menerima serangan digital (nilai 3,33), yang menandakan secara umum jawaban para responden berada di antara "Tidak pernah" dan "Sangat jarang" mengalami 12 jenis serangan digital. Nilai yang baik ini disebabkan rata-rata responden "sangat jarang" hingga "tidak pernah" mengalami 12 jenis serangan digital yang ditanyakan. Meski demikian, ada empat jenis serangan digital yang perlu mendapat perhatian khusus karena keempatnya paling sering dialami pembuat konten, yaitu "diawasi/*stalked*", "*phishing*", "*bullying*, ancaman, dan intimidasi yang bukan berbasis gender", dan "peretasan/pengambilalihan akun media sosial".

Selain itu, bagi pembuat konten yang mengalami serangan digital, dampaknya sangat merugikan mereka. Hal ini ditunjukkan oleh nilai aspek yang paling rendah (nilai 1,14), yaitu aspek dampak serangan digital yang berada di wilayah skala "tidak baik". Serangan digital sangat merugikan para pembuat konten, seperti

terancamnya keamanan (fisik maupun emosional) dan privasi serta menyebabkan hilangnya akses terhadap sumber pendapatan.

Sementara itu, terdapat dua aspek yang berada di antara penilaian “cukup baik” dan “baik”, yaitu persepsi terhadap keamanan digital (nilai 2,50 dari maksimal 4) dan praktik menangani serangan digital (nilai 2,67 dari maksimal 4). Hal ini menunjukkan, berdasarkan penilaian mandiri para responden, mereka menilai keamanan digital mereka dan kemampuan mereka menangani serangan digital sudah relatif baik. Namun, mereka tetap membutuhkan adanya pembaruan pengetahuan dan kecakapan secara terus-menerus mengingat perkembangan teknologi digital yang sangat dinamis, terutama terkait dukungan dan fasilitas yang diberikan oleh platform media sosial, sebagai ruang yang mereka gunakan untuk berekspresi. Aspek ini juga diulas dalam laporan diskusi kelompok terarah di bab selanjutnya.

BAB 3
Temuan Diskusi Kelompok Terarah

Waktu: 29 Juli 2024
Tempat: Jakarta (luring)
Peserta: 16 pembuat konten yang dipilih dari responden survei

Para pembuat konten melihat serangan digital sebagai bentuk ancaman terhadap kebebasan berekspresi di media sosial. Serangan digital kerap tidak berdiri sendiri, tetapi juga diiringi dengan ancaman atau serangan pada ranah fisik. Dampaknya sangat merugikan mereka, mulai dari tekanan psikologis hingga ancaman terputusnya pendapatan ekonomi.

Salah satu pengalaman serangan digital disampaikan oleh Fauziah Azzahra Ngabalin, pembuat konten asal Ambon, Maluku.

"Sebenarnya kalau bicara soal keamanan atau serangan digital, [saya] agak trauma. Karena hampir semua jenis serangan digital pernah saya rasakan," kata Fauziah Azzahra Ngabalin, yang juga bekerja sebagai jurnalis untuk *Zona Maluku*.

Dalam diskusi, dia mengungkapkan sejumlah serangan dan latar belakangnya. Trauma Fauziah adalah muara dari serangkaian serangan digital yang beriringan dengan ancaman fisik yang dia terima.

Salah satu serangan terhadapnya adalah *doxing* atau pengungkapan identitas pribadi di media digital. Yang paling traumatis bukan *doxing* terhadap dirinya, melainkan pengungkapan identitas puluhan korban kekerasan seksual yang dia dampingi.

Pada 2022, Fauziah mendampingi korban kasus kekerasan seksual yang dilakukan oleh dosen, pegawai kampus, dan mahasiswa di salah satu perguruan tinggi di Ambon. Ada 32 orang korban dalam kasus itu[1] dan tiga jurnalis kampus dibekukan status mahasiswa mereka karena mengungkap kasus itu. Saat itu, pihak kampus dan kepolisian meminta data korban kepada tim pendamping korban, tetapi ditolak oleh Fauziah dan teman-temannya sebagai pendamping. Namun setelah itu, data korban justru tersebar luas.

"Salahnya aku itu, aku tidak mengamankan laptop, dan data 32 korban itu tersebar di kampus. Aku tahu itu kesalahan aku, karena ketika dicek oleh SAFENet ternyata ada *malware* di laptopku," kata Fauziah, yang kemudian didampingi oleh SAFENet.

Selain itu, berbagai informasi pribadinya seperti data kuliah dan pengalaman kerja tersebar di media sosial. Dia mengaku muncul ratusan rumor buruk tentang dirinya dalam sehari. Ia menyatakan, hal itu terkait dengan aktivitasnya sebagai pembuat konten dan pendamping korban kekerasan seksual.

Latar Belakang Serangan

Seperti Fauziah, sejumlah pembuat konten mengungkapkan berbagai serangan digital muncul setelah aksi, advokasi, atau kampanye mengungkap kasus dan isu-isu sensitif, khususnya yang melibatkan pejabat publik.

Peserta diskusi lainnya, yang merupakan pengelola akun Aksi Kamisan Bandung, mengungkapkan hampir setiap unggahan di media sosial terkait aksi mereka diserang oleh akun-akun pendengung (*buzzer*). Serangan berupa pernyataan negatif di kolom komentar itu muncul saat akun Instagram Aksi Kamisan Bandung mengunggah konten yang membahas isu Papua atau diskriminasi gender. Sebagian konten tersebut dilaporkan oleh pengguna ke penyelenggara platform digital. Yang lebih buruk, muncul berbagai percobaan peretasan akun setiap kali mereka mengunggah konten berisi ajakan aksi demonstrasi.

[1] Kasus ini banyak diberitakan media pada 2022, yang pertama kali diungkap oleh Lembaga Pers Mahasiswa (LPM) Lintas dalam liputan "IAIN Ambon Rawan Pelecehan". LPM Lintas kemudian dibekukan rektor dan dilaporkan ke polisi oleh pengurus kampus. Dewan Pers menyatakan, LPM Lintas semestinya tidak dibekukan dan justru perlu diberi apresiasi (BBC Indonesia, 2022).

"*Upload* poster yang mengajak publik ikut aksi di lapangan, seringkali setelah post naik, akun sulit diakses. Bahkan banyak yang mencoba untuk akses masuk dan meretas hampir di setiap postingan. Lalu *hate speech* di kolom komentar dengan narasi-narasi negatif misalkan membahas soal Papua yang selalu dikaitkan dengan kelompok tertentu," katanya.

Kasus Aksi Kamisan Bandung menunjukkan serangan digital kerap kali tidak berdiri sendiri. Ketika sebuah konten diunggah di Instagram, ratusan *direct message* (DM) langsung masuk. Tak lama kemudian, sejumlah akun mengancam akan mencari atau mengungkapkan siapa adminnya. Ancaman itu tidak main-main karena salah seorang admin Aksi Kamisan Bandung sempat didatangi polisi.

"Teman kami sempat ditangkap pada 2019 karena postingan yang mengarah ke pemerintahan. Didatangi dan dibawa ke Polres pasca aksi terkait dengan postingan. Tidak sampai diproses, dia ditangkap dan setelah beberapa hari kemudian dikeluarkan," ujar peserta tersebut.

Teror melalui media digital juga nyaris menjadi keseharian bagi pengelola akun *@Borneo_Melawan*, Wira Surya Wibawa. Menurutnya, serangan yang muncul tak lepas dari isu-isu terkait proyek Ibu Kota Negara (IKN) Nusantara seperti deforestasi, penggusuran lahan, terpinggirkannya masyarakat adat, dan masalah turunannya yang diangkat dalam berbagai konten.

"Beberapa waktu terakhir ini ada *update* dari teman-teman pembuat konten, mereka diserang [saat mengunggah konten] isu IKN, masyarakat adat, dan agraria," kata Wira.

Serangan digital itu terjadi beriringan dengan teror fisik. Salah satunya terjadi saat para aktivis dan pembuat konten meliput aksi demonstrasi menggunakan kamera ponsel masing-masing. Saat ponsel digunakan untuk mengunggah konten dan berkoordinasi, masalah bermunculan.

"Ketika ingin menelpon untuk koordinasi kejadian dalam aksi tersebut itu, handphone saya berbunyi '*ting ting ting*' dan menyala terus. Ketika diangkat, itu nyala terus seakan-akan merekam. Kata SAFENet ada peretasan dan perekaman pembicaraan," ujarnya.

Peretasan perangkat juga dialami oleh rekan-rekannya saat para aktivis lembaga bantuan hukum (LBH) setempat dan Wahana Lingkungan Hidup (Walhi) meliput aksi beberapa waktu lalu. Jenis serangan ini cukup sulit disadari karena tanda-

tandanya tersamarkan oleh buruknya sinyal selular di Kalimantan.

Serangan lain juga muncul saat rekan Wira kehilangan ponsel beberapa waktu lalu, yang menurutnya bermotif ekonomi. Setelah berhasil mendapatkan kartu SIM pengganti dengan nomor yang sama, mendadak banyak orang tidak dikenal yang menghubungi. Bahkan ada beberapa orang yang mengaku dari platform finansial atau pinjol yang tidak dikenal.

Awalnya, dia mendapatkan pesan melalui WhatsApp dari seseorang yang mengklaim diri perwakilan penyelenggara platform Instagram. Pesan itu menginformasikan tahapan verifikasi akun untuk mendapatkan status "centang biru". Saat itu akunnya memang sedang mendaftar untuk mendapatkan status terverifikasi.

"Setelah *login*, akun diambil alih. [Pelaku] meminta ditransfer [sejumlah uang] untuk tebus akun," kata dia.

Sementara itu, dari Papua, Bernardus Boki Koten, pengelola akun media sosial SKPKC Fransiskan Papua, menjelaskan isu politik di Papua menjadi latar belakang serangan digital yang dia dan staf SKPKC Fransiskan Papua hadapi. Menurutnya, serangan-serangan tersebut terkait kontennya yang berisi *counter narrative* tentang Papua.

"[Konten tentang] Papua bercerita menurut orang Papua. Akhirnya berdampak pada serangan digital, bahkan fisik juga ada. Pada 2018, ini bukan terkait dengan konten, ada intimidasi. Kali terakhir itu kejadian kedua, tahun 2019," kata Bernardus.

Menurutnya, serangan terjadi setelah muncul rencana diskusi tentang masalah Papua yang disebabkan oleh orang-orang luar Papua. Sebelum diskusi, kepolisian menyampaikan keberatan dengan diskusi itu.

Bernardus juga mengisahkan pernah mengalami peretasan akun WhatsApp yang kemudian ditangani oleh SAFENet. Serangan berikutnya muncul saat Bernardus diundang sebagai narasumber dalam sebuah diskusi. Setelah itu, dia mendapatkan panggilan dari nomor-nomor tak dikenal dan semuanya merupakan nomor luar negeri seperti dari Amerika Serikat dan Australia. Dia merasa diawasi baik secara fisik maupun dalam jaringan.

"Tetapi saya tidak angkat [panggilan telepon itu]. [Secara] fisik ya [mendapatkan] intimidasi secara pribadi karena berkaitan dengan publikasi [buku] saya," katanya.

Isu sensitif dan kritik terhadap negara bukan menjadi satu-satunya latar belakang serangan. Firmansyah Sundana dari Lingkar Studi Filsafat Discourse mengungkapkan lembaganya mengalami serangan digital berupa *phising* dan peretasan akun setelah menggelar Festival Filsafat. Serangan tersebut diduga bermotif ekonomi.

"Pada September 2021 ada kolaborasi untuk Festival Filsafat, lalu akun Lingkar Studi Filsafat Discourse diretas, diambil alih, [kontennya] diganti, mereka mengambil alih akun Instagram kami karena alasan ekonomi," kata Sunanda.

Respons terhadap Serangan

Para pembuat konten menyadari mereka membutuhkan prosedur operasional standar (SOP) penanganan serangan digital. Masalahnya, banyak pembuat konten yang tidak memiliki SOP atau setidaknya merujuk SOP yang dimiliki lembaga lain.

Miftahul Huda dari LBH Yogyakarta mencontohkan respons lembaganya terhadap serangan digital yang muncul saat mendampingi masyarakat Desa Wadas, Kecamatan Bener, Kabupaten Purworejo, Jawa Tengah pada 2021–2022. Saat itu akun Instagram LBH Yogyakarta sempat hilang dan akun WhatsApp direktur lembaga itu diambil alih orang tidak dikenal.

Karena belum memiliki SOP keamanan digital, langkah pertama yang dilakukan LBH Yogyakarta adalah melaporkan serangan tersebut kepada SAFENet dan beberapa organisasi yang fokus pada keamanan digital. Dari komunikasi dengan lembaga-lembaga tersebut, mereka melakukan asesmen terhadap akun Instagram dan WhatsApp yang menjadi sasaran serangan.

"[Hasil] identifikasinya, [serangan terjadi] karena [kami] menangani dua kasus yang ramai [dibahas publik], yaitu Wadas dan PHK [pemutusan hubungan kerja] dosen UP [Universitas Proklamasi] 45," kata Miftahul.

Pasca serangan tersebut, LBH Yogyakarta mulai menyusun SOP keamanan digital dan SOP keamanan holistik. Namun, Miftahul menyadari pihaknya masih lemah dalam memperbarui jenis dan pola-pola serangan digital. Untuk menutupi kelemahan itu, penguatan jaringan dengan organisasi masyarakat sipil yang fokus dalam isu keamanan digital menjadi krusial.

Melaporkan kasus ke jaringan masyarakat sipil seperti SAFENet dinilai jauh lebih efektif daripada melapor langsung ke penyelenggara platform media sosial. Malik Diazin, pengelola media sosial Wahana Lingkungan Hidup (Walhi) Nasional, menggambarkan efektivitas pelaporan ke jaringan masyarakat sipil seperti SAFENet saat terjadi serangan digital.

"Beberapa kali juga melapor ke SAFENet dan efektif. Kami enggak melapor ke platform meskipun [mediumnya] disediakan. SAFENet sangat berkontribusi dan semoga bisa terus mengawal kita karena sangat bermanfaat," kata Malik.

Bantuan itu bukan hanya penting untuk merespons serangan, tapi juga untuk pencegahan. Walhi berupaya mengeliminasi 20%–30% akun *bot* di platform X. Melalui bantuan SAFENet, mereka meminta X menghapus akun-akun yang tidak aktif atau diidentifikasi sebagai bot dari daftar pengikut.

Pengalaman menghadapi serangan dan kerja sama dengan SAFENet mendorong Walhi memiliki SOP keamanan digital. SOP dinilai sangat penting karena wilayah kerja advokasi lembaga tersebut berisiko tinggi.

"[Salah satu poin dalam SOP adalah] sangat meminimalisasi memposting kegiatan-kegiatan organisasi yang berkaitan kondisi krisis di akun media sosial pribadi," ujarnya.

Pengelola akun Instagram *@aksikamisanbdg* menyebut upaya peretasan sudah "menjadi makanan sehari-hari". Karena itu, yang paling penting menurutnya adalah memperkuat mitigasi serangan digital.

"Sebelumnya memang cukup sering berdiskusi dengan teman-teman AJI Bandung, mengobrol tentang mitigasi serangan digital. Walaupun memang sulit, tetapi kita upayakan, seperti ganti *password* setiap bulan dan langkah lain yang sebenarnya ribet tetapi harus dilakukan," kata pengelola akun tersebut.

Pengelola akun Instagram Dago Melawan mencontohkan percobaan peretasan yang terjadi pada 29 Juli 2024 atau menjelang sidang perdana perkara pidana kasus Dago Elos di Bandung. Begitu mendapatkan notifikasi upaya *login* dari perangkat lain, langkah pertama yang dilakukan adalah meminta konfirmasi kepada orang-orang yang menjadi sesama admin akun apakah memang ada yang hendak *login*. Jika upaya itu terindikasi sebagai percobaan peretasan, admin langsung mengganti *password*.

"Saya juga enggak tahu siapa aktor utamanya. Tetapi biasanya sangat terkait dengan apa yang dilakukan besok atau beberapa hari kemudian. [Misalnya] di Bandung akan ada apa besok, atau apakah akan ada aksi," kata dia.

Tantangan Pengaturan Konten oleh Platform

Banyak pembuat konten yang mengalami serangan digital mengatakan, pelaporan ke penyelenggara platform media sosial tidak efektif. Selain lambannya respons penyelenggara platform, pembuat konten juga menilai aturan yang dibuat platform kerap merugikan mereka.

"*Community guidelines* [aturan komunitas] dan layanan aduan itu tidak efektif, lama, dan ribet. Kami jadi malas karena dikejar dengan waktu. Kalau [serangan] tidak segera ditangani, bisa lebih dalam lagi dampaknya," kata Malik dari Walhi Nasional.

Syarifah Ainun Jamilah, pembuat konten yang juga pegiat Cadar Garis Lucu, mengatakan pengaturan konten oleh platform yang belum berpihak pada korban serangan digital. Antara 2019–2020, dia diwawancarai oleh seorang pembuat konten lain. Dalam artikel hasil wawancara tersebut, Ainun dicitrakan seolah-olah pernyataannya mewakili komunitas muslim secara umum. Hal itu memicu komentar-komentar berisi ujaran kebencian dan ancaman pembunuhan kepada dirinya, khususnya dari akun-akun *bot*.

Banyaknya serangan berupa ujaran kebencian itu mendorong Ainun melapor ke penyelenggara platform agar akun-akun *bots* itu tidak menyerang kontennya. Meski demikian, akun *bot* tetap bisa memberikan reaksi terhadap konten Instagram *story*-nya.

"Instagram pernah membatalkan laporan [saya] karena dianggap tidak sesuai. Padahal jelas akun *bot* itu ada 10 dan hampir tiap hari komentar," ujarnya.

Pada saat yang sama, dia merasa Instagram membatasinya karena dianggap melanggar aturan komunitas. Itu ditandai dengan sulitnya mendapatkan *followers* atau *viewers* (penonton). Misalnya saat kontennya diunggah, *followers*-nya bertambah lima akun, tetapi hanya terbaca dua akun dan tiba-tiba jumlah *followers*-nya turun drastis.

Riza Pratiko, pengelola akun Instagram *@pontianakinformasi*, menunjukkan bagaimana penegakan aturan komunitas membuat kontennya gagal menyebar luas.

Beberapa waktu lalu, unggahannya diidentifikasi oleh platform mengandung unsur terorisme karena mengabarkan rencana kedatangan Bahar bin Smith.

“Ternyata Habib Bahar Smith dan Habib Rizieq itu tidak boleh kita tulis secara frontal di *caption* maupun *font* postingan Instagram. Waktu itu kami cuma *up* ya, kebetulan ada permintaan dari *brand* makanan *ngucapin* selamat datang Habib Bahar di Pontianak. *Udah* itu aja enggak ada *embel-embel* apa pun. Waktu itu [hanya] Instagram *story*, enggak ada tambahan *caption* apa-apa,” kisahnya.

Konten tersebut tetap gagal diunggah meski dicoba hingga tiga kali. Masalah itu disusul dengan pemberlakuan *shadowban* sehingga akun tersebut tidak bisa digunakan untuk siaran *live* Instagram.

“Akun kami sudah [punya] ratusan ribu *followers* dan *shadowban* itu sangat amat kejam. Kami jadi seperti punya 200 *followers* saja dan buat dapetin 10 likes aja sangat susah,” kata dia.

Para peserta berharap, platform media sosial bisa lebih transparan terkait tindak lanjut aduan dari mereka dan aduan yang dilakukan oleh pihak lain terhadap akun mereka. Dua hal itu bagi mereka sangat penting untuk melindungi kebebasan berekspresi sekaligus menghindari pembuat konten dari korban laporan palsu atau tidak akurat.

BAB 4
Penutup Melindungi Pembuat Konten Kepublikan

Platform media sosial telah menjadi ekosistem sendiri yang mengandalkan algoritma tidak bebas nilai dan melibatkan faktor manusia maupun non-manusia, serta mengikuti logika pasar terbuka yang dibentuk oleh pengguna, pengendali, dan pemilik infrastruktur platform. Di dalamnya, ada tiga faktor, yaitu perilaku pengguna konten (kultural), dinamika teknologi (spasial), dan aktor di balik teknologi (struktural) yang saling berkelindan. Dalam relasi kuasa yang tidak seimbang itu, pengguna media sosial (yang mencakup pembuat konten) memiliki wajah ganda–bisa menjadi target maupun pelaku serangan digital.

Riset ini memberikan gambaran data bahwa pembuat konten Indonesia memiliki pengalaman yang nyaris serupa dengan profesi jurnalis di dunia digital. Karena peran kepublikan, mereka berisiko menjadi korban. Dalam banyak hal, pembuat konten lebih dominan (jumlah, kuantitas kerja, perilaku kerja, pendapatan ekonomi) ketimbang jurnalis profesional di media daring. Tugas keduanya tampak beririsan pada konten yang mengulas isu berkepentingan publik.

Problem struktural muncul pada kategori profesi pembuat konten, yang tidak dikenal dalam Undang-Undang Pers No. 40/1999. Dengan kata lain, mereka bukan dianggap jurnalis meski konten yang dibuat bercorak berita aktual atau liputan mendalam isu publik. Profesi pembuat konten masuk ranah kerja media digital secara umum, yang dalam batas tertentu terkait Undang-Undang Informasi dan Transaksi Elektronik. Mereka berisiko dianggap mencemarkan nama baik

dan masuk penjara tanpa pembelaan berarti. Ini bentuk lain atau lanjutan dari serangan digital.

Riset ini menemukan sejumlah bentuk serangan digital yang nyaris sama dialami kedua profesi tersebut, yaitu *surveillance, phishing, bullying*, dan intimidasi berbasis digital. Dari 312 pembuat konten yang menjadi responden survei, 63,5% di antara mereka pernah mengalami setidaknya satu dari 12 serangan digital yang ditanyakan. Temuan riset menegaskan, kerja produksi konten yang berkelindan dengan kepentingan publik lebih berisiko mengalami represi digital ketimbang konten non-kepentingan publik. Maknanya, selalu ada upaya menekan kerja advokasi digital lewat konten oleh pihak pihak yang kepentingan ekonomi-politiknya terganggu, dengan memakai ruang digital.

Dengan melihat dampak serangan digital sebagaimana diuraikan dalam temuan survei dan diskusi kelompok terarah, pengaruh serangan digital ini sangat serius. Kebebasan berekspresi, yang dijamin oleh konstitusi Indonesia, terancam oleh para "perusuh" digital. Dalam konteks ini, terjadi pelanggaran hak asasi terhadap warga negara yang berkarya di ruang digital.

Karena itu, profesi pembuat konten butuh dukungan dari negara, platform media sosial, dan pihak-pihak yang peduli terhadap kebebasan berekspresi. Peran platform media sosial di sini sangat strategis karena konten diunggah di platform media sosial, yang aturan mainnya dibuat dan ditegakkan oleh platform media sosial. Jika kita berkaca pada regulasi di Uni Eropa (Digital Services Act), mereka memberikan beragam kewajiban kepada penyelenggara media sosial supaya menegakkan "aturan main" yang lebih aman dan transparan, sementara Undang-Undang Informasi dan Transaksi Elektronik yang baru saja direvisi untuk kedua kalinya belum sampai ke sana—publik menunggu Peraturan Pemerintah sebagai turunan Undang-Undang Informasi dan Transaksi Elektronik hasil revisi tahun 2023 tersebut.

Riset ini membantu agar jika perumusan kebijakan untuk melindungi pembuat konten atau pengguna media sosial dibuat, nantinya regulasi berada dalam perspektif hak asasi, moderasi konten yang lebih baik oleh platform, dan penguatan kesadaran sosial oleh pembuat konten itu sendiri, dengan prioritas perlindungan pada pembuat konten berperspektif publik.

Daftar Pustaka

Almaki, S., Alghamdi, R., Sami, G., & Alhakami, W. (2021). Social media security and attacks. *IJCSNS International Journal of Computer Science and Network Security, 21*(1), 174–183. https://doi.org/10.22937/IJCSNS.2021.21.1.22

Amnesty International. (2020, June 17). End wave of digital attacks on students, journalists, activists. *Amnesty.id.* https://www.amnesty.id/kabar-terbaru/pernyataan-sikap/end-wave-of-digital-attacks-on-students-journalists-activists/06/2020/

Basyari, I. (2023, June 18). Serangan di ruang digital jadi ancaman serius di Pemilu 2024. *Kompas.id.* https://www.kompas.id/baca/polhuk/2023/06/14/serangan-di-ruang-digital-jadi-ancaman-serius-di-pemilu-2024

BBC Indonesia (2022, July 19). Dugaan pelecehan seksual di IAIN Ambon. BBC Indonesia. https://www.bbc.com/indonesia/majalah-62202322

Bucci, A. (2023). *Followed: The content creator's guide to being seen, facing judgment, and building an authentic personal brand*. BenBella Books, Inc.

Cai, Y., Wu, Y., & Xue, W. (2024). Social media retailing in the creator economy. Omega, 124. https://doi.org/10.1016/j.omega.2023.103014

European Court of Human Rights. (2017). *Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*. Strasbourg, France. https://hudoc.echr.coe.int/#{%22itemid%22:[%22001-175121%22]}

Halim, D., Meiliana, D. (2020, June 16). Bintang Emon Diserang setelah Kritik Kasus Novel, Safenet: Pelaku Bisa Dipidanakan. Kompas.com.https://nasional.kompas.com/read/2020/06/16/14584691/bintang-emon-diserang-setelah-kritik-kasus-novel-safenet-pelaku-bisa

IDN Research Institute. (2024). Indonesia Gen Z report 2024: *Understanding and uncovering the behavior, challenges, and opportunities*. IDN Research Institute.

Ibrahim, R. (2021, March 4). Kronologi peretasan WhatsApp & penangkapan Ravio Patra. *Asumsi.co*. https://asumsi.co/post/59013/kronologi-peretasan-whatsapp-penangkapan-ravio-patra/

Instagram. (2024). Create content and monetize your passion. *Creators.instagram.com*. https://creators.instagram.com/earn-cash-making-what-you-love?locale=en_US

Kemp, S. (2024). Digital 2024: Indonesia. *Datareportal.com*. https://datareportal.com/reports/digital-2024-indonesia

Kemp, A. (2023, October 13). What is a content creator? The what, why and how of the creator economy. *State of Digital Publishing*. https://www.stateofdigitalpublishing.com/content-strategy/what-is-a-content-creator/

Kusuma, E., & Arum, N. S. (2019). Memahami dan menyikapi kekerasan berbasis gender online: Sebuah panduan. SAFEnet. https://safenet.or.id/wp-content/uploads/2019/11/Panduan-KBGO-v2.pdf

Masduki. (2022). Cyber-troops, digital attacks, and media freedom in Indonesia. *Asian Journal of Communication*, 32(3), 218–233. https://doi.org/10.1080/01292986.2022.2062609

McGonale, T., Bosch, L., Buijis, D., Huang, M., Nazarski, M., Fathaigh, R., Poort, J., & Ulasiuk, I. (2023). *Public interest content in audiovisual platforms: Access and findability*. European Audiovisual Observatory. https://rm.coe.int/iris-special-2023-01en-public-interest-content/1680ad084d

Muhajir, A. (2020, October 26). The rise of political digital attacks. *The Jakarta Post.* https://www.thejakartapost.com/paper/2020/10/25/the-rise-of-political-digital-attacks.html/

Nuri, E. (2023, November 6). Host Kinderflix dapat komentar pelecehan seksual meskipun membuat konten edukasi. *Narasi.tv*. https://narasi.tv/read/narasi-daily/host-kinderflix-dapat-komentar-pelecehan-seksual-meskipun-membuat-konten-edukasi#google_vignette

Peres, R., Schreier, M., Schweidel, D., & Sorescu, A. (2024). The creator economy: An introduction and a call for scholarly research. *International Journal of Research in Marketing*. https://doi.org/10.1016/j.ijresmar.2024.07.005

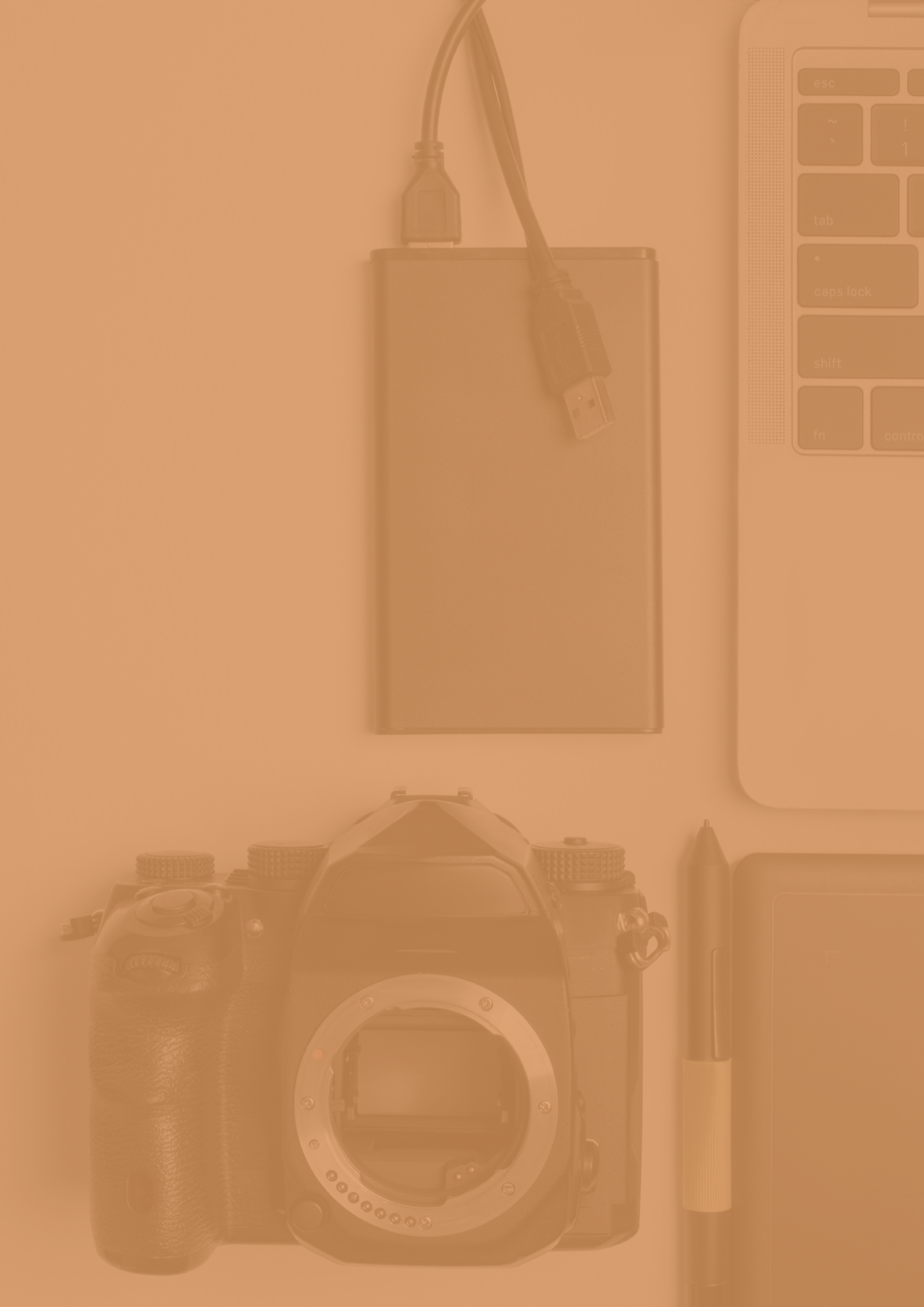
Southeast Asia Freedom of Expression Network (SAFEnet). (2020, April 23). [Rilis pers] Segera lepaskan Ravio Patra: Hentikan kriminalisasi, ungkap pelaku peretasan!. *Safenet.or.id.* https://safenet.or.id/id/2020/04/rilis-pers-segera-lepaskan-ravio-patra-hentikan-kriminalisasi-ungkap-pelaku-peretasan/

Southeast Asia Freedom of Expression Network (SAFEnet). (2023). *Laporan triwulan III: Pemantauan hak -hak digital di Indonesia.* SAFEnet. https://safenet.or.id/id/2023/11/laporan-pemantauan-hak-hak-digital-triwulan-iii-2023/

Takimai, A., Saputri, N., Arum, N. S., Ressmy, S., Ardhia, T., Sagena, U., & Arioka, W. (2024). *Laporan situasi hak-hak digital Indonesia 2023: Sudah roboh tertimpa pemilu pula.* Southeast Asia Freedom of Expression Network (SAFEnet).

Thomas, K., Kelley, P. G., Consolvo, S., Samermit, P., & Bursztein, E. (2022). "It's common and a part of being a content creator": Understanding how creators experience and cope with hate and harassment online [Paper presentation]. CHI '22: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems. https://doi.org/10.1145/3491102.3501879

Tim Reaksi Cepat (TRACE). (2024). Layanan. Trace.mu. https://trace.mu/layanan/
YouTube. (2024). *Monetisasi untuk Kreator. Youtube.com*. https://www.youtube.com/howyoutubeworks/product-features/monetization/#overview


esc
tab
caps lock
shift
fn