



***BADAN SIBER
DAN SANDI
NEGARA***

PEMETAAN PERILAKU PENGGUNA RUANG SIBER

2024



DIREKTORAT OPERASI KEAMANAN DAN PENGENDALIAN INFORMASI

www.bssn.go.id



***BADAN SIBER
DAN SANDI
NEGARA***

PEMETAAN PERILAKU PENGGUNA RUANG SIBER

2024



DIREKTORAT OPERASI KEAMANAN DAN PENGENDALIAN INFORMASI

www.bssn.go.id

Pemetaan Perilaku Pengguna Ruang Siber di Indonesia

PENULIS

Indy Rahmadhona

Kirana Larasati Dewi

Lisa Saputri

Dzakwan Al Dzaky Bewasana

Erfandra Ramadhan Susanto

Siti Manayra Sabiya

Pemetaan Perilaku Pengguna Ruang Siber di Indonesia

Penulis

Indy Rahmadhona
Kirana Larasati Dewi
Lisa Saputri
Dzakwan Al Dzaky Bewasana
Erfandra Ramadhan Susanto
Siti Manayra Sabiya

Pengarah

Dominggus Pakel

Penanggung Jawab

Satryo Suryantoro

Koordinator

Eri Suprayitno

Periset

Dhea Septi Kurnia Dati
Muhammad Syihaab Al Faaruuq
Naufal Madega Pratama
Shalihati Mutiara Rejki

Desainer Grafik, Sampul, dan Tata Letak

Dzakwan Al Dzaky Bewasana
Erfandra Ramadhan Susanto
Fachrul Ali Nurfadilah
Siti Manayra Sabiya

Penerbit

**DIREKTORAT OPERASI KEAMANAN
DAN PENGENDALIAN INFORMASI
BADAN SIBER DAN SANDI NEGARA**

Jl. Harsono RM 70 Ragunan, Pasar
Minggu, Jakarta Selatan, 12550 Telp.
+62 21 780 5814 Fax. +62 21 7884 4104

UKURAN :

E-ISBN :

ISBN

CETAKAN PERTAMA : JANUARI 2025

Hak Penerbitan ©2025 Badan Siber dan Sandi Negara
Dilarang mengutip dan memperbanyak tanpa izin tertulis dari
penerbit, sebagian atau seluruhnya dalam bentuk apa pun, baik
cetak, *photoprint*, *microfilm*, dan sebagainya.



Kata Pengantar



SOCIAL CYBERSECURITY IS FOCUSED ON HUMANS SITUATED IN SOCIETY, AND HOW THE DIGITAL ENVIRONMENT CAN BE MANIPULATED TO ALTER BOTH THE COMMUNITY AND THE NARRATIVE



Ruang siber menciptakan sebuah kehidupan yang dimediasi secara mendasar oleh teknologi, sehingga berbagai fungsi kehidupan nyata kini diambil alih oleh substitusi teknologisnya, yang disebut kehidupan artifisial (*artificial life*). Berbagai aktivitas manusia seperti politik, sosial, ekonomi, kultural, spiritual bahkan seksual yang dapat dilakukan di dunia nyata kini dapat dilakukan dalam bentuk artifisialnya di dalam ruang siber. Pengaruh ruang siber terhadap kehidupan sosial terlihat pada tingkat individu, antar individu, dan komunitas. Interaksi sosial antar individu di ruang siber sangat dipengaruhi oleh perkembangan berbagai macam platform media sosial.

Keberadaan media sosial menciptakan ekosistem perilaku siber dan memberikan dampak positif dan negatif. Media sosial memberikan ruang yang luas untuk meningkatkan kreativitas dalam membangun presentasi diri seseorang. Namun media sosial juga dapat menjadi media untuk menyebarkan konten yang bertentangan dengan peraturan perundang-undangan. Terbukanya ruang media sosial dapat memberikan ancaman bagi masyarakat Indonesia. Secara tak sadar, pola pikir dan perilaku masyarakat dapat berubah dan terbentuk karena aktivitas interaksi di dalamnya. Gangguan informasi di bidang Ipoleksosbudhankam inilah jika dibiarkan dapat mengikis ketahanan digital masyarakat dan pada skala nasional dapat mengganggu ketahanan siber negara.

Negara dalam hal ini BSSN mengambil langkah konkret dengan melakukan pemantauan perilaku siber pengguna media sosial. Pemantauan dan analisis perilaku siber ini dapat menjadi *early warning* bagi pemerintah dan *stakeholder* terkait. Sehingga pemerintah dapat menentukan strategi yang tepat dalam meminimalisir penyebaran berbagai bentuk gangguan informasi di ruang siber.

Gangguan informasi yang tercipta akibat eksistensi media sosial saat ini beberapa diantaranya terkait dengan perilaku *cyberbullying*, pornografi, penyebaran paham radikalisme atau terorisme, kejahatan *online*, hoaks, dan transaksi narkoba. Gangguan informasi tersebut merupakan ancaman siber sosial yang nyata di dalam kehidupan sehari-hari. Ancaman ini justru lebih berbahaya dibandingkan ancaman siber secara teknis.

Buku “**Pemetaan Perilaku Pengguna Ruang Siber**” merupakan buku kedua pemetaan hasil prediksi perilaku masyarakat Indonesia (*cyber behaviour*) berdasarkan survei pada Generasi Z. Gen Z atau generasi dengan kelahiran diantara tahun 1997 sampai 2012 termasuk ke dalam pengguna media sosial terbanyak di Indonesia sehingga perlu dilakukan pemantauan perilaku siber dan cara mereka memitigasi berbagai macam gangguan informasi. Pemetaan perilaku siber bertujuan untuk mengukur sejauh mana ketahanan digital dan kesiapan Gen Z sebagai pemuda calon pemimpin bangsa di masa Indonesia Emas 2045.

Kami mengapresiasi seluruh *stakeholder* terkait serta Disdik dan Diskominfo di 34 provinsi yang telah mendukung proses kegiatan survei dari awal hingga akhir. Kami berharap kerja sama yang baik ini dapat diteruskan dan ditingkatkan agar memperoleh hasil yang semakin baik.

Akhir kata, semoga buku “**Pemetaan Perilaku Pengguna Ruang Siber**” ini dapat dimanfaatkan sebagai bentuk pertanggungjawaban bagi Badan Siber dan Sandi Negara secara khusus dan masyarakat secara umum. Selain itu, semoga buku ini dapat memberikan wawasan yang berharga bagi semua pihak untuk menjaga ruang siber Indonesia.

Bersama BSSN, Kita #JagaRuangSiber!



**SATRYO SURYANTORO,
S.Sos.**

Direktur Operasi Keamanan Dan
Pengendalian Informasi Badan Siber
dan Sandi Negara

Daftar Isi

i	◆◆	Kata Pengantar
iii	◆◆	Daftar Isi
iv	◆◆	Daftar Gambar
v	◆◆	Daftar Grafik
vi	◆◆	Pendahuluan
12	◆◆	Keamanan Siber Sosial
20	◆◆	Hasil & Pembahasan
50	◆◆	Penutup
57	◆◆	Referensi

Daftar Gambar

- 4 — **Gambar 1.1** SPRS 2023
- 5 — **Gambar 1.2** Bagan Metodologi
- 6 — **Gambar 1.3** Bagan Variabel Penelitian
- 8 — **Gambar 1.4** Ilustrasi Alasan Penetapan Responden
- 9 — **Gambar 1.5** Alur Pengambilan Data
- 10 — **Gambar 1.6** Alur Pengambilan Data
- 13 — **Gambar 2.1** Kelemahan dalam Keamanan Siber
- 15 — **Gambar 2.2** Perpres Nomor 47 Tahun 2023
- 15 — **Gambar 2.3** Urgensi Ancaman Ruang Siber
- 15 — **Gambar 2.4** Serangan Siber bisa Memecah Bangsa
- 17 — **Gambar 2.5** Kasus Cyberbullying
- 17 — **Gambar 2.6** Kasus Radikalisme dan Terorisme
- 18 — **Gambar 2.7** Kasus Narkotika
- 18 — **Gambar 2.8** Kasus Hoaks dan Ujaran Kebencian
- 19 — **Gambar 2.9** Kasus Penipuan dan Kejahatan *Online*
- 28 — **Gambar 3.1** Contoh Peringatan Keamanan yang Dianggap
Penting
- 28 — **Gambar 3.2** Contoh Peringatan Keamanan yang Dianggap
Kurang Penting
- 36 — **Gambar 3.3** Contoh Kasus Judi *Online*
- 40 — **Gambar 3.4** Chatbot Pemilu 2024

Daftar Grafik

- 21 — **Grafik 3.1** Karakteristik Responden Survei
- 22 — **Grafik 3.2** Durasi Penggunaan Media Sosial
- 22 — **Grafik 3.3** Durasi Penggunaan Media Sosial
- 23 — **Grafik 3.4** Jenis Perangkat yang Digunakan
- 24 — **Grafik 3.5** Jenis Media Sosial yang Digunakan
- 24 — **Grafik 3.6** Jenis *Platform* Pesan Instan yang Digunakan
- 25 — **Grafik 3.7** Alasan Penggunaan Internet
- 25 — **Grafik 3.8** Jenis Koneksi Internet
- 26 — **Grafik 3.9** Jenis Konten Media Daring atau Media Sosial
- 27 — **Grafik 3.10** Sikap Saat Menerima *Alert Warning*
- 29 — **Grafik 3.11** Kasus *Cyberbullying* di Media Sosial
- 29 — **Grafik 3.12** Tindakan Saat Mengalami/Melihat *Cyberbullying*
- 30 — **Grafik 3.13** Kasus Radikalisme/Terrorisme di Media Sosial
- 30 — **Grafik 3.14** Tindakan Saat Mengalami/Melihat
Radikalisme/Terrorisme
- 31 — **Grafik 3.15** Kasus Narkotika di Media Sosial
- 31 — **Grafik 3.16** Tindakan Saat Mengalami/Melihat
Informasi/Konten Narkotika
- 32 — **Grafik 3.17** Konten Hoax/Ujaran Kebencian di Media Sosial
- 32 — **Grafik 3.18** Tindakan Saat Menemukan Konten *Hoax*/Ujaran
Kebencian
- 33 — **Grafik 3.19** Konten Penipuan/Tindak Kejahatan *Online*
- 33 — **Grafik 3.20** Kasus Penipuan/Tindak Kejahatan Secara *Online*
yang Pernah Dialami/Dilihat

Daftar Grafik

- 34 — **Grafik 3.21** Konten Pornografi di Media Sosial
- 35 — **Grafik 3.22** Pembelian Barang *Online* yang Dilakukan
- 36 — **Grafik 3.23** Tawaran Mengikuti Judi *Online*
- 36 — **Grafik 3.24** Media yang Memberikan Tawaran Judi *Online*
- 37 — **Grafik 3.25** Penipuan Finansial *Online*
- 37 — **Grafik 3.26** Media yang Mengirimkan Pesan Tawaran *Financial Crime*
- 38 — **Grafik 3.27** Pengetahuan terhadap Dampak Algoritma *Filter Bubble*
- 38 — **Grafik 3.28** Tindakan Mengurangi *Filter Bubble*
- 39 — **Grafik 3.29** Pengetahuan terhadap Platform *Chatbot* Pemilu
- 41 — **Grafik 3.30** Pengetahuan Larangan di Internet Berdasarkan UU ITE
- 41 — **Grafik 3.31** Larangan di Internet berdasarkan UU ITE
- 42 — **Grafik 3.32** Peran Orang Tua/Keluarga dalam Mengingatnkan Siswa
- 42 — **Grafik 3.33** Peran Guru dalam Mengingatnkan Siswa
- 43 — **Grafik 3.34** Temuan Konten Negatif Pulau Sumatra (1)
- 44 — **Grafik 3.35** Temuan Konten Negatif Pulau Sumatra (2)
- 45 — **Grafik 3.36** Temuan Konten Negatif Pulau Jawa
- 46 — **Grafik 3.37** Temuan Konten Negatif Pulau Bali, NTT, dan NTB
- 47 — **Grafik 3.38** Temuan Konten Negatif Pulau Kalimantan
- 48 — **Grafik 3.39** Temuan Konten Negatif Pulau Sulawesi
- 49 — **Grafik 3.40** Temuan Konten Negatif Pulau Maluku dan Papua

BAB I

Pendahuluan



Fenomena Netizen Masa Kini

Keamanan siber secara umum tidak hanya mencakup keamanan lapisan fisik dan logis dari perangkat, tetapi juga keamanan siber sosial. Keamanan siber sosial merupakan ilmu yang mempelajari bagaimana **teknologi digital dapat mempengaruhi perilaku, budaya, hingga pandangan politik masyarakat.** Seiring dengan peningkatan ancaman teknis di ruang siber, ancaman siber sosial seperti **cyberbullying, tindak kejahatan online, penipuan (scam),** serta **penyebaran misinformasi dan disinformasi** (contoh: hoaks) pun semakin marak. Selain itu, ruang siber juga dimanfaatkan untuk melakukan praktik ilegal, seperti penyebaran **lowongan kerja palsu, transaksi barang terlarang** (obat terbatas, obat keras, psikotropika, dan narkoba), hingga **penyebaran konten berbahaya** seperti radikalisme dan pornografi.

Ruang Siber

Ruang Siber adalah lingkungan virtual yang terbentuk dari koneksi antar berbagai perangkat komputasi dalam sebuah jejaring digital raksasa yang terhubung ke seluruh dunia, sehingga memungkinkan terjadinya komunikasi dengan media internet.



Data dari APJII (Asosiasi Penyedia Jasa Internet Indonesia) tahun 2024 menyebutkan bahwa kontribusi pengguna internet di Indonesia mayoritas berasal dari Generasi Z (kelahiran 1997–2012). Peran kelompok Generasi Z ini menjadi krusial dalam mewujudkan cita-cita Indonesia Emas tahun 2045. Sementara itu, berdasarkan data Kementerian Komunikasi dan Digital tahun 2024, sebanyak **80% pelajar Indonesia** yang rutin mengakses media sosial memperlihatkan pola perilaku yang **mencerminkan budaya keamanan siber yang sangat perlu ditingkatkan**. Hal ini diperkuat oleh laporan UNESCO tahun 2024, yang mengungkapkan bahwa **1 dari 5 pelajar SMA terpapar konten negatif** atau **berbahaya** di internet setiap harinya, serta studi *American Academy of Pediatrics* tahun 2023, yang menunjukkan bahwa **60% remaja** yang menghabiskan **lebih dari 3 jam** per hari di media sosial mengalami **gangguan psikologis**.

Peningkatan budaya keamanan siber bertujuan menciptakan **lingkungan digital yang sehat dan aman**. Budaya keamanan siber menjadi penting bagi pelajar karena ruang siber menghadirkan ancaman nyata terhadap keamanan pribadi dan mental pelajar yang mencakup **77,75% populasi** usia muda di Indonesia (BPS, 2023). Data dari Badan Siber dan Sandi Negara (BSSN) pada kuartal ke-3 tahun 2024 mencatat peningkatan signifikan kasus peretasan akun media sosial dan penyebaran konten berbahaya yang **melibatkan anak muda** sebagai korban maupun pelaku.



Pemerintah Indonesia melalui Badan Siber dan Sandi Negara (BSSN) mendukung upaya **peningkatan budaya keamanan siber** dengan menjalankan tugas dan fungsi diantaranya melakukan edukasi keamanan siber. Hal ini bertujuan untuk memastikan masyarakat Indonesia secara luas memiliki **kesadaran lebih baik dalam memanfaatkan ruang siber** secara aman dan bertanggung jawab.

Kesadaran keamanan siber penting bagi pelajar untuk melindungi diri dari ancaman siber. Oleh karenanya, membangun budaya keamanan siber sejak dini pada generasi muda adalah langkah strategis untuk menciptakan ketahanan siber yang baik pada masyarakat. Pemetaan perilaku pengguna ruang siber di kalangan pelajar bertujuan mengidentifikasi pola penggunaan dan kesadaran pelajar terhadap keamanan siber, sehingga dapat menjadi dasar penyusunan strategi dan kebijakan yang tepat sasaran. Budaya keamanan siber yang diukur mencakup kapabilitas pengguna, lingkungan, serta motivasi dan informasi yang diperoleh dari ruang siber.

Melalui Peraturan Presiden (Perpres) Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Kriris Siber, diatur penguatan koordinasi dan kebijakan strategis dalam menghadapi ancaman siber nasional, sementara itu Peraturan BSSN Nomor 6 Tahun 2021 menetapkan standar minimum pengamanan siber di berbagai sektor, termasuk pendidikan.

Kedua regulasi ini menjadi landasan penting dalam membangun budaya keamanan siber yang menyeluruh di Indonesia.

Buku Pemetaan Perilaku Pengguna Ruang Siber dimaksudkan untuk memberikan gambaran komprehensif mengenai pola perilaku pengguna ruang siber di Indonesia, khususnya di tingkat pelajar SMA. Data yang didapat berguna untuk memetakan area serta daerah yang memerlukan intervensi khusus dalam peningkatan budaya keamanan siber, serta prediksi potensi ancaman siber sosial melalui analisis perilaku *cyber behaviour* dengan metode survei.

Survei dilakukan pada 34 provinsi di Indonesia dengan tujuan mendapatkan data acuan dalam pemetaan perilaku pengguna ruang siber. Instrumen survei meliputi karakteristik responden, penggunaan internet dan media sosial, peraturan perundang-undangan Informasi dan Transaksi Elektronik (ITE), dampak negatif media sosial serta peluang ancaman pada media sosial.

SPRS itu Apa?

SPRS atau **Survei Pemetaan Ruang Siber** adalah survei yang dilakukan untuk mengetahui pola perilaku pengguna ruang siber di Indonesia. Pemetaan pola perilaku pengguna ruang siber (*cyber behaviour*) diharapkan dapat mendukung upaya peningkatan budaya keamanan siber di Indonesia. Buku Pemetaan Perilaku Pengguna Ruang Siber (P3RS)

merupakan hasil dari SPRS yang telah disebarkan untuk memetakan perilaku masyarakat di ruang siber. Survei ini disebarkan kepada pelajar SMA di seluruh provinsi di Indonesia menggunakan metode *sampling*. Dalam buku ini, dijelaskan hasil survei mendalam, analisis yang terperinci, dan rekomendasi strategis yang dapat diimplementasikan untuk memitigasi risiko kejahatan siber sosial yang muncul.



Gambar 1.1 SPRS 2023



Metodologi

Metodologi pada pelaksanaan SPRS terdiri atas beberapa tahapan, dimulai dengan melakukan **persiapan** yang meliputi **persiapan administratif**, **penentuan variabel** dan **penyusunan kuesioner**. Setelah itu, pada tahap **pengumpulan data**, dilakukan penetapan responden dan lokasi serta penentuan target responden. Kemudian, data yang terkumpul diproses pada tahap **pengolahan data**. Selanjutnya, dilakukan analisis data untuk mendapatkan temuan yang relevan. Terakhir, dilakukan **penyusunan laporan** berdasarkan hasil analisis tersebut.



Gambar 1.2 Bagan metodologi

Persiapan

Persiapan survei

Tahap persiapan survei terdiri atas proses **penentuan variabel** dan **penyusunan kuesioner**.

Penentuan Variabel

Variabel yang digunakan dalam **Survei Pemetaan Perilaku Pengguna Ruang Siber (SP3RS)** ini adalah:



Gambar 1.3 Bagan Variabel Penelitian

Penyusunan Kuesioner

Pelaksanaan Survei Pemetaan Perilaku Pengguna Ruang Siber dibagi menjadi 3 (tiga) bagian sesuai dengan tujuan survei, yaitu :

BAGIAN I

Identitas responden, meliputi: wilayah survei, nama responden, kontak nomor handphone responden, usia responden, jenis kelamin responden, asal dan nama sekolah responden.

1

BAGIAN II

1. Penggunaan Internet dan Media Sosial, terkait penggunaan internet dan media sosial yang bertujuan untuk mengetahui kebiasaan responden dalam memanfaatkan internet dan media sosial.

2. Dampak Negatif Media Sosial, terkait media sosial yang biasa ditemui kasus dampak negatif media sosial, meliputi *cyberbullying*, radikalisme/terorisme, narkoba, hoaks/ujaran kebencian, penipuan/tindak kejahatan secara *online*, pornografi.

3. Peluang Ancaman, terkait peluang dan ancaman yang terjadi di media terhadap masyarakat.

4. Peraturan Perundang-Undangan, mengenai pemahaman mengenai salah satu dasar hukum terkait yaitu undang-undang ITE.

2

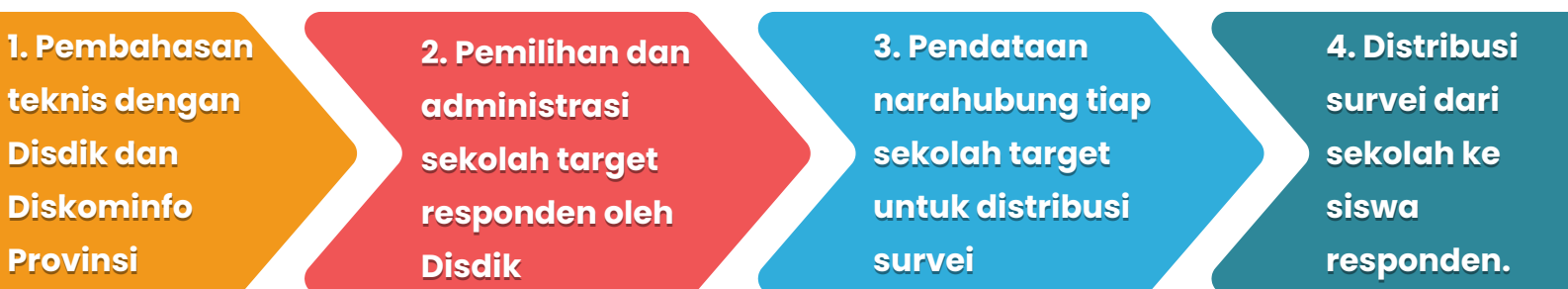
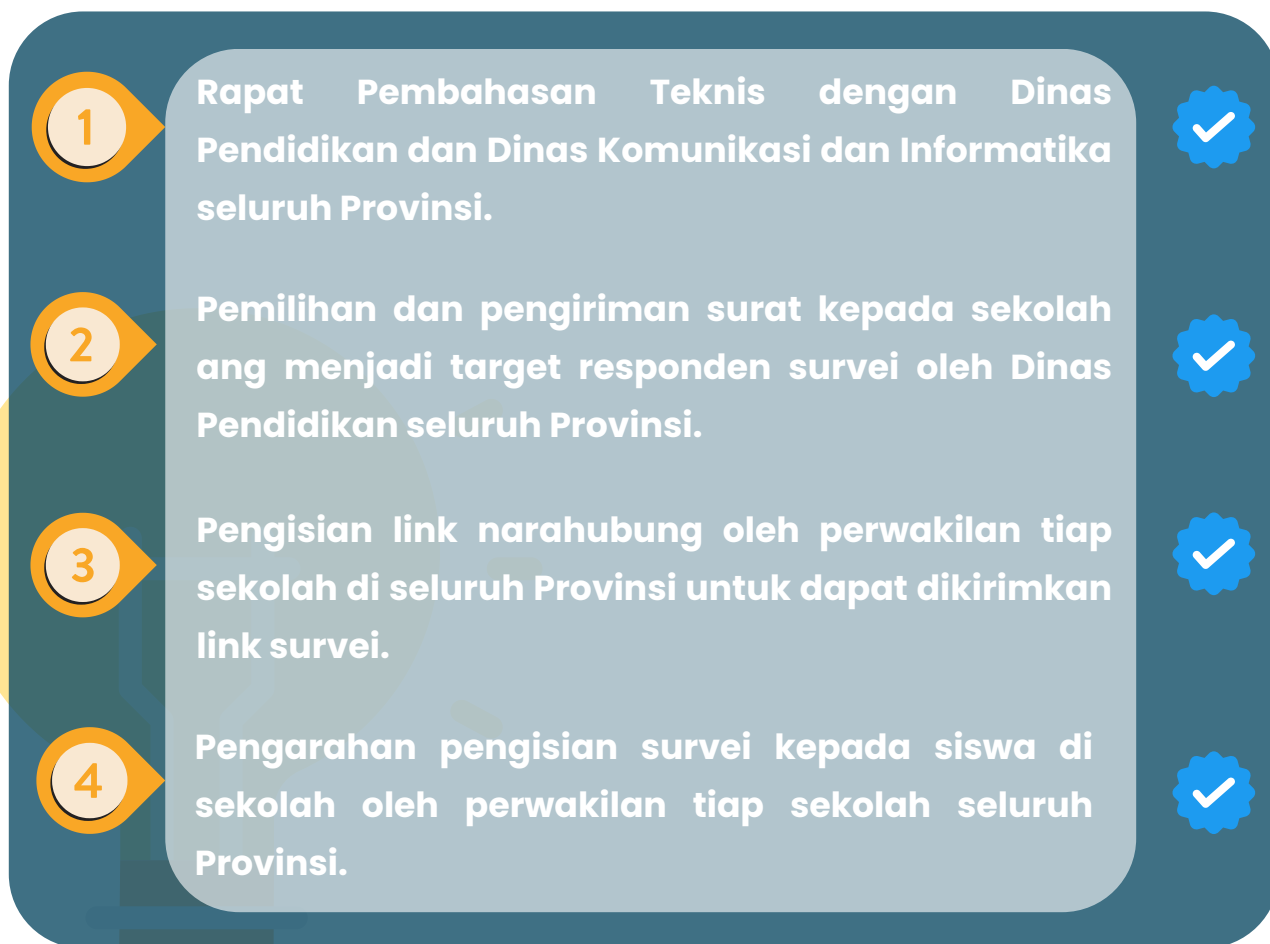
3

BAGIAN III

Saran, opini atau pendapat bebas dari responden

Persiapan administratif

Tahap persiapan administratif dititik beratkan pada proses koordinasi dengan stakeholder terkait, yang terdiri dari:



Gambar 1.6 Alur Pengambilan Data

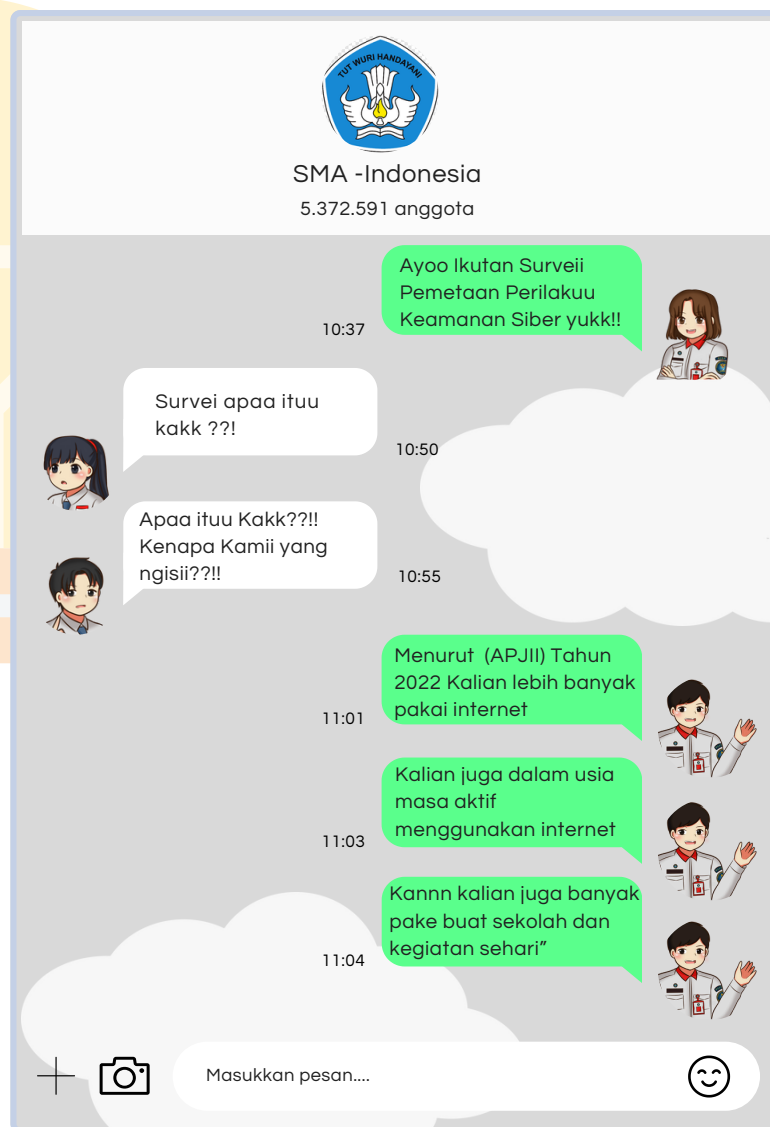
Pengumpulan Data

Pengumpulan data yang terdiri atas **penetapan responden** dan **lokasi**, **penentuan target responden**, dan **pengambilan data**.

Penetapan responden

Responden pada kegiatan Survei Pemetaan perilaku Pengguna Ruang Siber adalah **generasi Z**, diwakili oleh siswa-siswi **Sekolah Menengah Atas (SMA)** atau sederajat yang tersebar di **34 provinsi di Indonesia**.

Alasan pemilihan kelompok tersebut untuk menjadi responden survei yaitu sebagai berikut :



Gambar 1.4 Ilustrasi Alasan Penetapan Responden

Penetapan Target Responden

Penetapan target responden dilakukan menggunakan rumus slovin pada Survei Pemetaan Perilaku Pengguna Ruang Siber. Penentuan target responden untuk menentukan **sampel minimum** menggunakan **rumus** sebagai berikut:

$$N = \frac{n}{1 + Ne^2} = \frac{5.259.520}{1 + 5.259520(0,014)^2} = 5.100$$

Gambar 1.5 Perhitungan Jumlah Sampel Minimum

Populasi : 34 provinsi Indonesia

Tingkatan : 34 provinsi populasi – seluruh Kab/Kota – SMA – perkotaan dan pedesaan

Sampel : 2 SMA negeri dan 2 SMA swasta per Kab/Kota, masing-masing 1 di perkotaan dan 1 di pedesaan

Sampel Acak : 50 responden per sekolah

Pengolahan dan analisis data

Pengolahan dan **analisis data** hasil polling Survei Pemetaan Perilaku Pengguna Ruang Siber dilakukan setelah tahap **pengumpulan data**. Pada tahap ini, data survei yang didapatkan kemudian dikelompokkan dan dihitung jumlah responden yang memilih dalam bentuk **grafik**. Grafik tersebut diolah berdasarkan asal daerah provinsi responden untuk mendapatkan grafik pemetaan perilaku ruang siber masing-masing daerah. Selanjutnya, berdasarkan grafik-grafik tersebut kita dapat melakukan **analisis data** untuk mengambil kesimpulan pada survei pemetaan perilaku ruang siber di Indonesia



Penyusunan laporan

Setelah mendapatkan data dan hasil, selanjutnya dilakukan **penyusunan laporan**. Tahap ini dimulai dari penentuan informasi-informasi yang ingin disampaikan kepada pembaca secara jelas dan lugas. Kemudian dilanjutkan dengan Penyusunan buku ini juga merupakan salah satu upaya untuk menyampaikan mengenai informasi hasil survei yang telah dilakukan.



BAB II

Keamanan Siber Sosial





Gambar 2.1 Kelemahan dalam Keamanan Siber



Rantai terlemah dalam sebuah sistem keamanan adalah **manusia**

Semakin banyaknya informasi yang beredar di media sosial dapat menyebabkan fenomena "**banjir informasi**." Seorang penerima informasi bisa **kewalahan** dalam memproses informasi karena **banyaknya** informasi yang diterima. Akibatnya, kemampuan mereka dalam membuat keputusan akan **berkurang**. Oleh karena itu, manusia cenderung **mempercayai** apa yang mereka yakini benar.

Fenomena banjir informasi ini kemudian dimanfaatkan oleh **oknum/pihak yang tidak bertanggungjawab** untuk **mempengaruhi** dan **memanipulasi** individu di ruang siber melalui **konten-konten** yang dikemas menjadi konten disinformasi, misinformasi, malinformasi dan konten menyesatkan lainnya.



Keamanan Siber Sosial

Memangnya ada berapa jenis keamanan siber, *sih*?



Ada **dua**! Keamanan siber dibagi menjadi keamanan siber **teknis** dan **sosial**.

Keamanan siber **sosial** merupakan bidang keamanan siber yang berfokus untuk meminimalisir dampak negatif dari aktivitas penyerang dalam **memengaruhi** atau **memanipulasi** individu manusia, grup, ataupun komunitas sehingga dapat merubah perilaku mereka di bidang sosial, budaya dan politik.

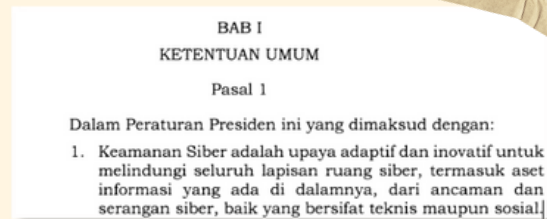
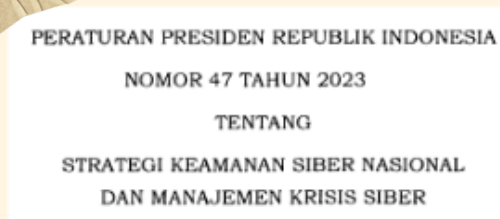


Keamanan siber **teknis** merupakan bidang keamanan siber yang berfokus untuk meminimalisir dampak negatif dari aktivitas yang dilakukan peretas untuk menyerang infrastruktur IT dan teknologi yang dapat menyebabkan **kerugian materiil**.



Kesimpulannya, keamanan siber sosial menempatkan **manusia** sebagai **target**, sedangkan keamanan siber teknis menempatkan **teknologi** sebagai **targetnya**.

Urgensi Keamanan Siber Sosial



Gambar 2.2 Perpres Nomor 47 Tahun 2023

Urgensi keamanan siber sosial telah memiliki **payung hukum** yang menjadi dasar pelaksanaan keamanan siber di Indonesia, yaitu Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.



Gambar 2.3 Urgensi Ancaman Ruang Siber

Pada acara BSSN Award di Cibubur, Bekasi (8/6/2023) Kepala BSSN, Bapak Hinisa Siburian mengatakan terdapat **2 sifat ancaman** pada ruang siber. Pertama bersifat **teknis**, menyerang sistem elektronik yang digunakan lembaga negara berbasis **elektronika**. Kedua, bersifat **sosial** yang menyerang **manusia**. Menurut beliau, ancaman kedua sangat berbahaya karena musuh mencari titik kelemahan yaitu persatuan. Untuk menangkal ancaman sosial, warga negara harus memperkuat persatuan Indonesia.

Deputi Bidang Operasi Badan Siber dan Sandi Negara (BSSN), Mayjen TNI Dominggus Pakel, dalam pertemuan dengan Korps Menwa Indonesia di Kantor BSSN, Ragunan, Pasar Minggu, Jakarta Selatan (17/10/2024), menyampaikan bahwa ancaman serangan siber kini **tidak** lagi **hanya** bersifat **teknis**, tetapi juga **sosial**, dan berpotensi besar dapat **memecah belah bangsa** melalui penyebaran hoaks, propaganda, dan manipulasi informasi. Menurut beliau, ancaman negara saat ini tidak hanya berfokus pada empat matra pertahanan (TNI dan Polri), tetapi juga pada dimensi kelima, yaitu ancaman siber di dunia maya.



Gambar 2.4 Serangan Siber bisa Memecah Bangsa

Pemanfaatan Media Sosial



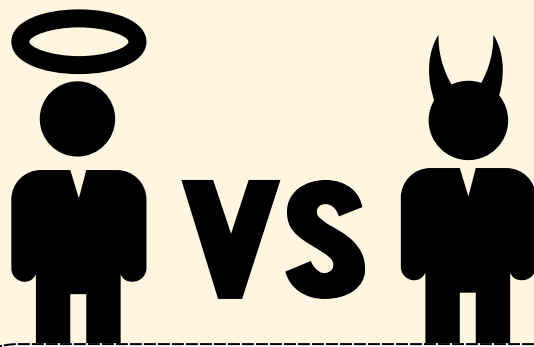
Media sosial memungkinkan masyarakat untuk **mengakses** dan **membagikan informasi** dengan cepat dan mudah.



Masyarakat dapat memanfaatkan media sosial untuk membangun **personal branding** dan sebagai sarana untuk mengaktualisasikan diri.



Masyarakat dapat memanfaatkan **e-commerce** untuk melakukan transaksi jual beli secara *online* dengan berbagai pilihan



Keberadaan media sosial bagaikan pisau bermata dua. Media sosial bisa berdampak **positif**, namun juga bisa berdampak **negatif**, tergantung bagaimana pengguna memanfaatkannya.

Dampak negatif dari media sosial di bidang Ipoleksosbudhankam bisa menjadi suatu **ancaman siber sosial** yang mengganggu kehidupan masyarakat. Pemantauan terhadap ancaman siber sosial ini yang menjadi fokus **BSSN** dalam **menjaga ruang siber** Indonesia.



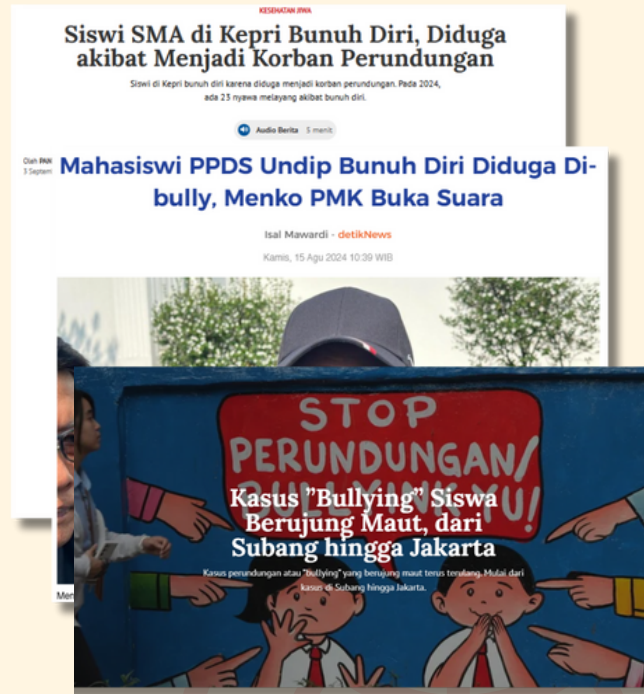
Dampak negatif media sosial

Cyberbullying (Perundungan Dunia Maya)

Cyberbullying adalah **perundungan** yang dilakukan melalui **teknologi digital**. Perundungan ini terjadi di media sosial, *platform chatting*, dan *game online*, yang dapat **merusak kesehatan mental korban** dan berdampak pada stres, depresi, atau bahkan keinginan untuk bunuh diri.

Radikalisme dan Terorisme

Radikalisme, yang menginginkan perubahan sistem sosial atau politik melalui kekerasan, telah diatur dalam UU Nomor 5 Tahun 2018 tentang Tindak Pidana Terorisme. Penyebaran ideologi radikal yang mendorong/mendukung tindakan **kekerasan** sering ditemukan melalui media sosial. Penggunaan media sosial sendiri sering dijadikan **medium** bagi kelompok ekst untuk **merekrut anggota** atau **menyebarkan propaganda**.



Gambar 2.5 Kasus Cyberbullying

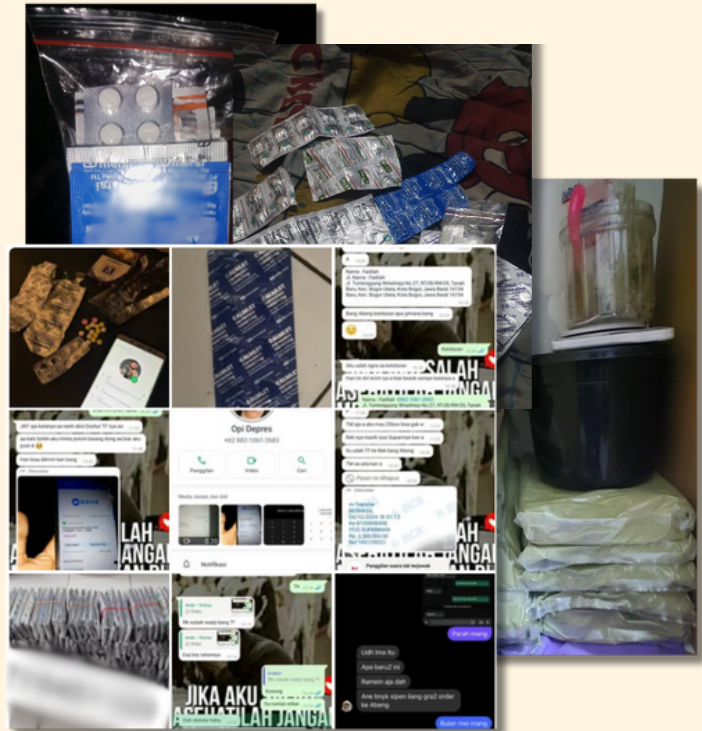


Gambar 2.6 Kasus Radikalisme dan Terorisme

Dampak negatif media sosial

Narkotika

Narkotika adalah zat adiktif yang jika disalahgunakan dapat merusak tubuh dan kehidupan seseorang, serta mengganggu tatanan sosial. Penyalahgunaan narkotika tidak hanya terjadi di dunia nyata, tetapi juga memanfaatkan **media sosial** untuk **promosi** dan **peredarannya**.



Gambar 2.7 Kasus Narkotika

Hoaks dan Ujaran Kebencian

Hoaks merupakan Berita palsu yang **sengaja** dibuat untuk menyesatkan pembaca. Hoaks sering **memanipulasi** fakta agar terlihat menarik dan mudah dipercaya.

Sedangkan **Ujaran Kebencian** merupakan Tindakan **menyebarkan kebencian** atau permusuhan terhadap individu atau kelompok tertentu berdasarkan SARA (suku, agama, ras, dan antar golongan).

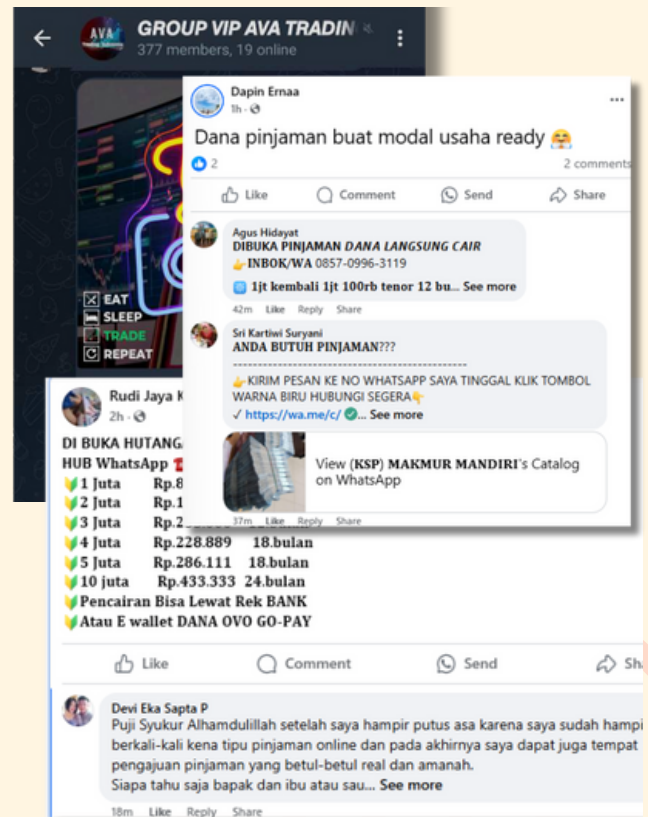


Gambar 2.8 Kasus Hoaks dan Ujaran Kebencian

Dampak negatif media sosial

Penipuan dan Kejahatan Online

Seiring dengan kemajuan teknologi, semakin banyak peluang bagi **berbagai jenis kejahatan online** seperti penipuan, pencurian data pribadi, atau hacking. Kejahatan ini sering memanfaatkan **internet** sebagai **media** atau **sarana** perantaranya.



Gambar 2.9 Kasus Penipuan dan Kejahatan Online



Pornografi

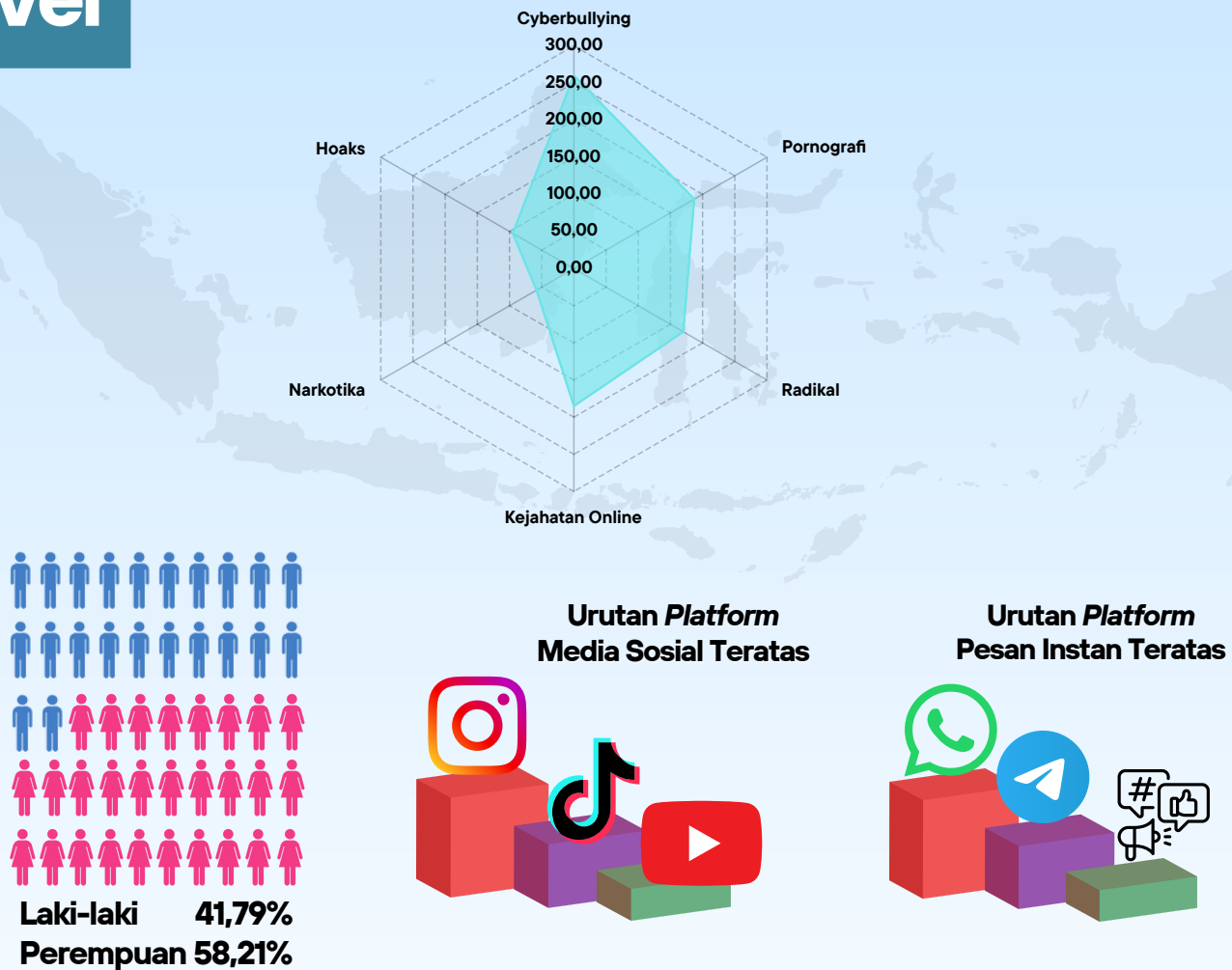
Internet dan media sosial telah menjadi saluran utama penyebaran pornografi. Kemudahan akses **tanpa pembatasan** atau **sensor** membuat konten pornografi mudah dijangkau, yang dapat berdampak buruk pada moral dan perkembangan mental, terutama bagi anak-anak dan remaja.

BAB III

Hasil & Pembahasan

The page features several decorative geometric elements. On the left side, there is a vertical stack of shapes: a dark teal triangle pointing left, followed by a light blue triangle pointing right, and then a cluster of six triangles (three dark teal and three light blue) arranged in a circular pattern. Additionally, there are light blue curved shapes at the top right and bottom left corners of the page.

Karakteristik Responden Survei

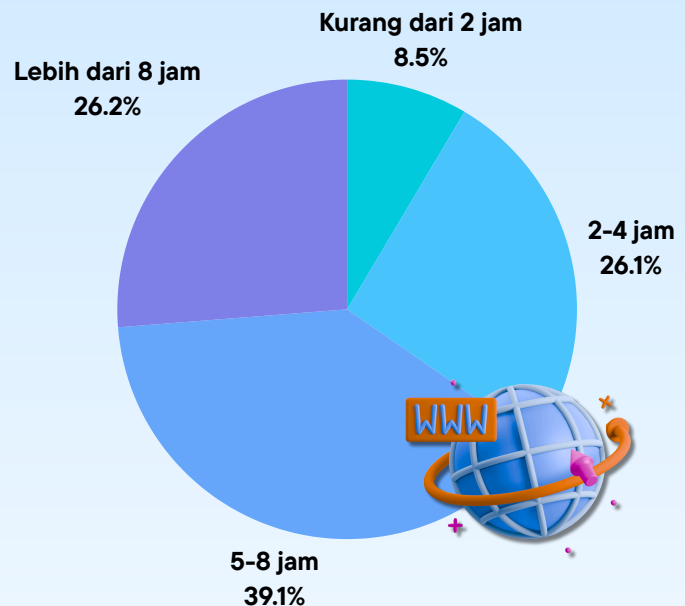


Grafik 3.1 Karakteristik Responden Survei

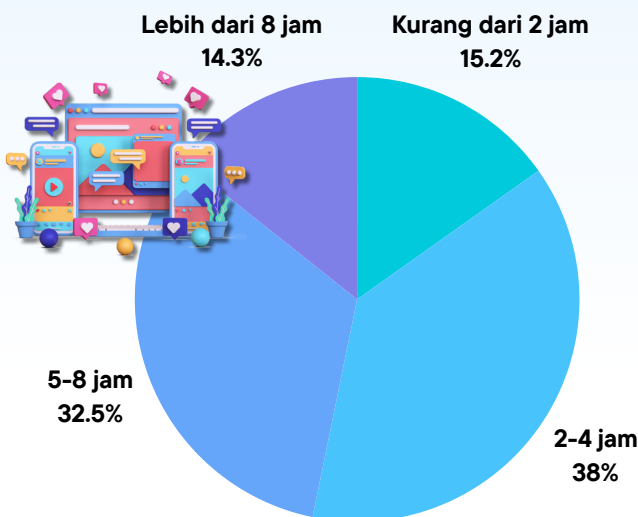
Karakteristik responden SPRS dapat dilihat pada grafik di 3.1. Responden utama SPRS merupakan **siswa SMA** dengan rata-rata umur **14-18 tahun** sebagai populasi yang merepresentasikan **Generasi Z** di seluruh Indonesia. Berdasarkan jenis kelamin, responden **perempuan** lebih besar **1,64%** dibandingkan responden laki-laki. Terdapat **3 (tiga) platform media sosial** yang paling banyak digunakan responden, yaitu **Instagram, TikTok dan YouTube**, sedangkan pada **platform pesan instan**, terdapat **3 (tiga) platform** yang paling banyak digunakan responden yaitu **WhatsApp, Telegram, dan platform pesan instan lainnya** (di luar opsi survei)

Durasi Penggunaan Internet dan Media Sosial per hari

Berdasarkan hasil survei, selama satu hari sebanyak 26,25% responden menggunakan internet paling lama adalah **5-8 jam**. Kemudian sebanyak 26,2% responden menggunakan internet lebih dari 8 jam, lalu sebanyak 26,1% responden menggunakan internet selama 2-4 jam, dan sebanyak 8,53% responden menggunakan internet kurang dari 2 jam dalam sehari.



Grafik 3.2 Durasi Penggunaan Internet



Grafik 3.3 Durasi Penggunaan Media Sosial

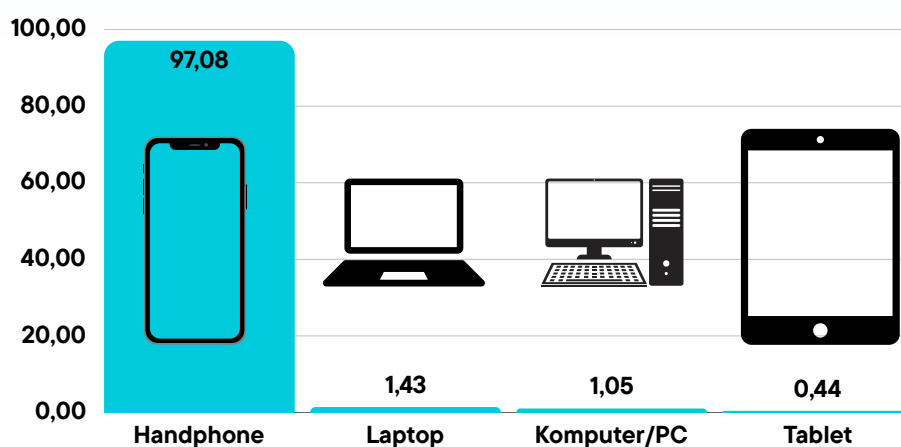
Selain itu, penggunaan media sosial memiliki nilai terbesar pada rentang waktu **2 hingga 4 jam** yaitu sebanyak 38,04% atau sebanyak 3.523 responden. Selanjutnya, diikuti oleh rentang penggunaan 5 hingga 8 jam sebesar 32,5%, penggunaan kurang dari 2 jam sebesar 15,2%, dan nilai terkecil yaitu penggunaan lebih dari 8 jam sebesar 14,3%.

Jenis Perangkat yang Digunakan untuk mengakses internet dan media sosial

Berdasarkan survei mengenai jenis perangkat yang digunakan responden untuk mengakses internet maupun media sosial, sebagian besar responden memilih menggunakan **handphone** dengan persentase sebesar 97,08% atau sebanyak 8.992 responden. Kemudian disusul dengan penggunaan laptop sebesar 1,43%, *personal computer* sebesar 1,05% dan yang paling sedikit yaitu tablet sebesar 0,44%.

Handphone lebih dominan digunakan oleh responden karena merupakan perangkat gadget **yang praktis** untuk dibawa kemanapun serta sudah dilengkapi **fitur-fitur** yang lengkap untuk membantu aktivitas sehari-hari.

Sedangkan tablet minim digunakan responden karena tablet lebih banyak digunakan oleh kalangan pebisnis, profesional, atau pekerja kreatif yang membutuhkan **spesifikasi tertentu**, sehingga pelajar **bukan merupakan target pasar utama**. Selain itu ukurannya yang **kurang praktis** dan adanya **aturan terkait larangan** penggunaan perangkat tertentu di sekolah juga dapat memengaruhi jumlah penggunaan tablet.

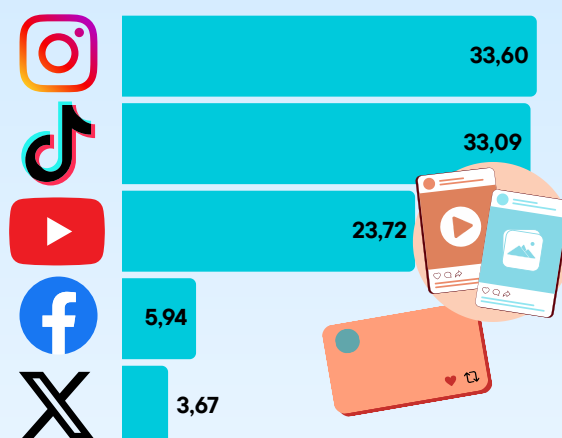


Grafik 3.4 Jenis Perangkat yang Digunakan

Tiga indikator selanjutnya, yaitu **Jenis Media Sosial yang Digunakan**, **Jenis Platform Pesan Instan yang digunakan**, dan **Alasan Penggunaan Internet** dapat dipilih lebih dari satu jawaban oleh masing-masing responden.

Jenis Media Sosial yang Digunakan

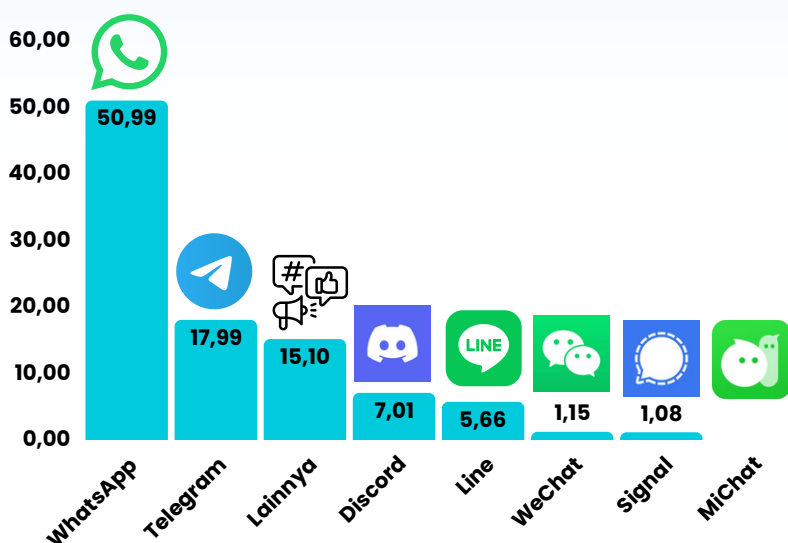
Instagram dan **TikTok** adalah media sosial yang paling sering digunakan dengan persentase responden yang menggunakan instagram sebesar 33,6% dan responden yang menggunakan TikTok sebesar 33,09%. Media sosial lain yang juga banyak digunakan adalah **YouTube** sebesar 23,72%, **Facebook** sebesar 5,94%, dan **X (Twitter)** sebesar 3,67%. Hasil tersebut menunjukkan **platform berbasis konten gambar** lebih digemari oleh pelajar dari pada **platform berbasis konten teks**.



Grafik 3.5 Jenis Media Sosial yang Digunakan

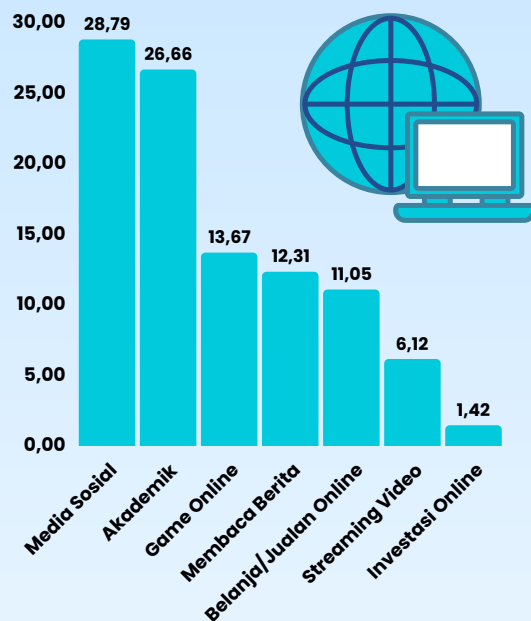
Jenis Platform Pesan Instan yang Digunakan

WhatsApp menjadi **platform pesan instan** yang paling sering digunakan pelajar dengan persentase sebesar 50,99% atau sejumlah 9.167 responden. Platform lainnya yaitu Telegram dengan persentase sebesar 17,99%, Discord sebesar 7,01%, Line sebesar 5,66%, WeChat sebesar 1,15%, Signal sebesar 1,08%, MiChat sebesar 1,03% dan platform pesan instan selain dari pilihan yang disediakan survei sebesar 15,10%.



Grafik 3.6 Jenis Platform Pesan Instan yang Digunakan

Alasan Penggunaan Internet



Grafik 3.7 Alasan Penggunaan Internet

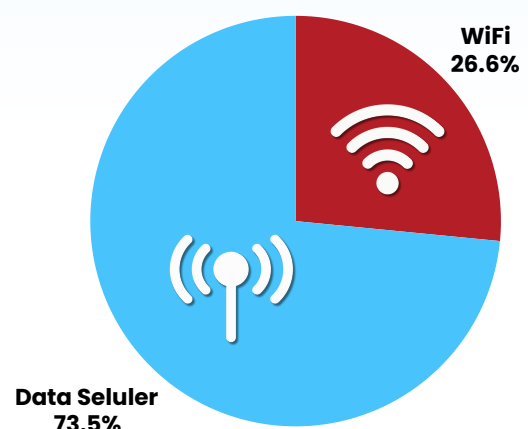
Diketahui bahwa responden lebih banyak menggunakan internet untuk membuka **media sosial** dengan persentase sebesar 28,79% atau sebanyak 7.619 responden, kemudian diikuti dengan mengerjakan kebutuhan sekolah/pembelajaran jarak jauh dengan presentase sebesar 26,66% atau sebanyak 7.056 responden. Alasan lainnya yaitu *game online* sebesar 13,7%, membaca berita sebesar 12,3%, transaksi *online* sebesar 11%, streaming video

sebesar 6,1%, dan trading/investasi *online* sebesar 1,4%. Hasil tersebut berkaitan dengan kategori responden sebagai **pelajar** dan termasuk Gen Z yang berada dalam **rentang umur pelajar**.

Jenis Koneksi Internet yang Sering Digunakan

Responden lebih sering menggunakan **paket data/kuota** dari operator seluler sebesar 73,45% atau sebanyak 6.803 responden, sedangkan WiFi hanya sebesar 26,55% atau sebanyak 2.459 responden.

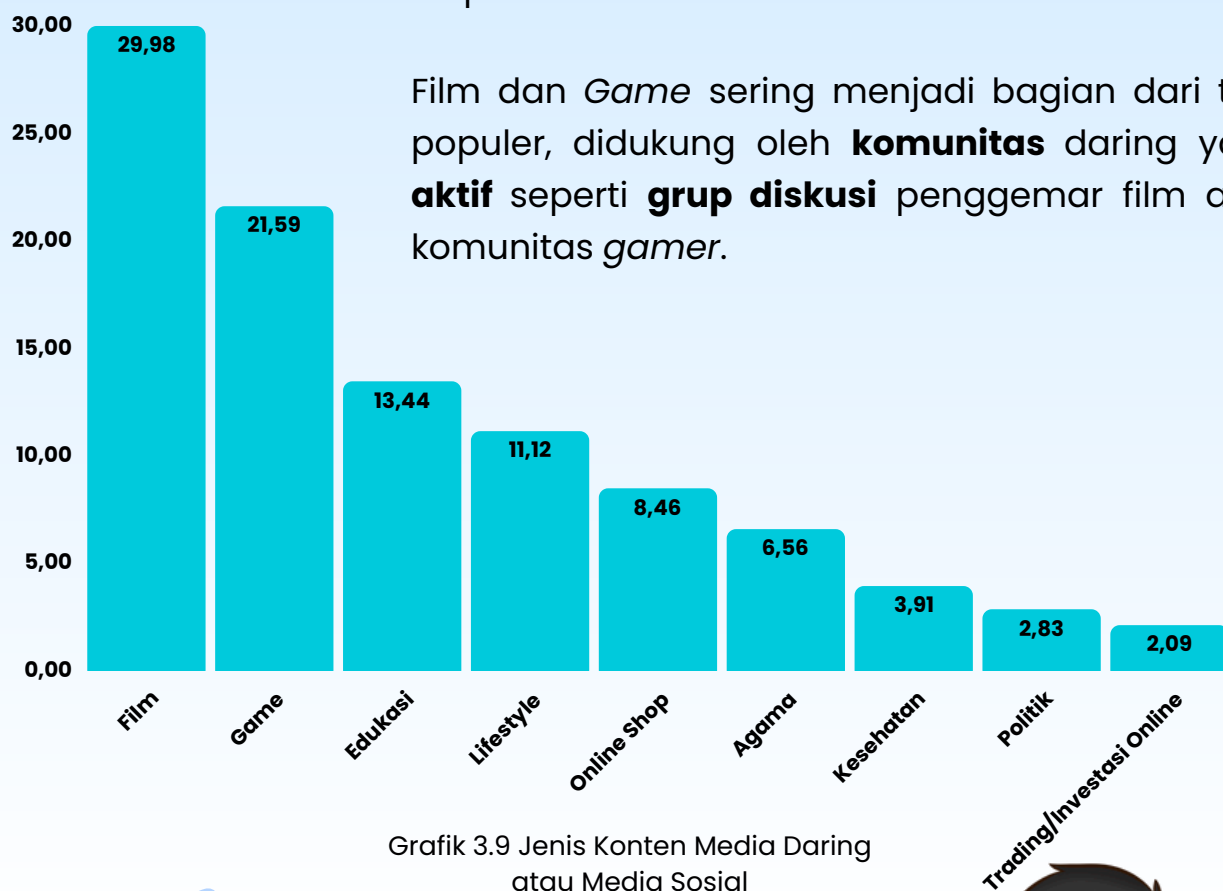
Hasil tersebut dikarenakan penggunaan paket data lebih **fleksibel** dan tidak semua tempat menyediakan **WiFi gratis** di ruang publik.



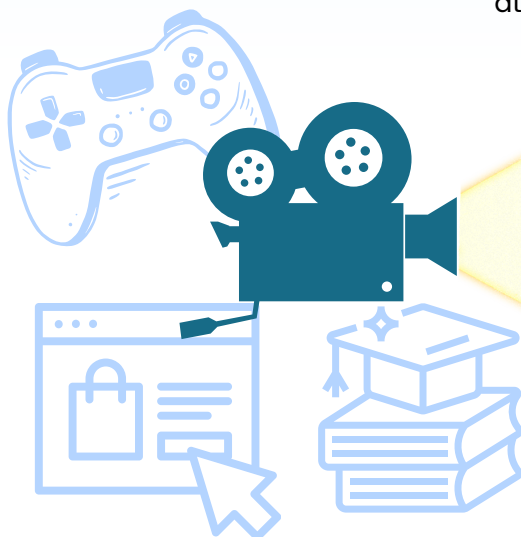
Grafik 3.8 Jenis Koneksi Internet

Jenis Konten Media Daring atau Media Sosial yang Paling Disukai

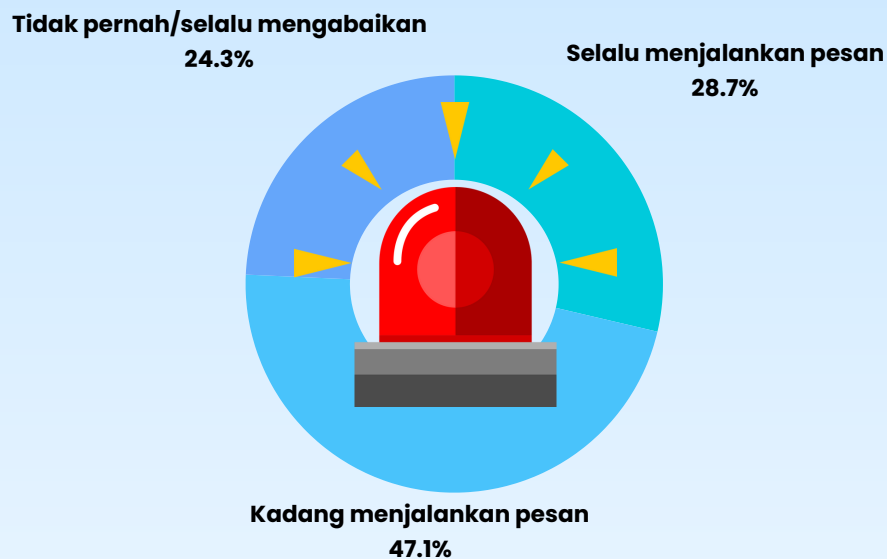
Konten media sosial yang banyak disukai oleh responden adalah **Film** dengan persentase sebesar 29,98% atau sebanyak 2.777 responden dan **Game** sebesar 21,59% atau sebanyak 2.000 responden.



Grafik 3.9 Jenis Konten Media Daring atau Media Sosial



Sikap saat menerima Notifikasi Alert Warning



Grafik 3.10 Sikap Saat Menerima Alert Warning

Menilik sikap responden saat menerima notifikasi alret warning, sebanyak 4.358 atau sebesar 47,05% responden **kadang-kadang** menjalankan pesan/notifikasi peringatan. Sebesar 28,67% atau 2.655 responden memilih untuk selalu menindaklanjuti notifikasi dan 24,28% atau sebanyak 2.249 responden lainnya tidak pernah menindaklanjuti notifikasi peringatan.

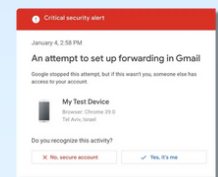
Hal ini dikarenakan notifikasi *Alert Warning* mungkin **terlalu sering** muncul, sehingga sebagian responden terbiasa **mengabaikannya**. Namun, saat notifikasi tampak **penting** dan **serius**, responden mungkin cenderung **menjalankan** pesan.



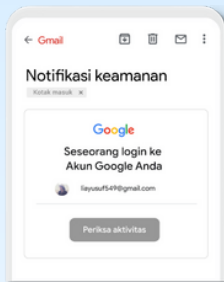


Alert Warning

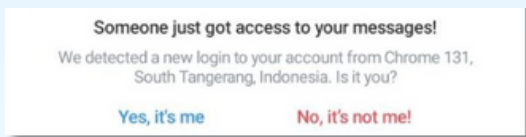
Peringatan Keamanan yang Dianggap Penting



Sumber : google.com



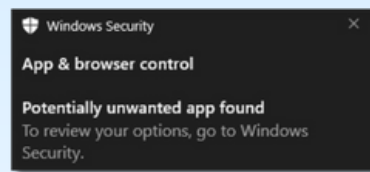
Sumber : google.com



Sumber : Dok. pribadi

Gambar 3.1 Contoh Peringatan Keamanan yang Dianggap Penting

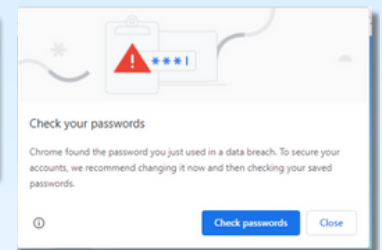
Peringatan Keamanan yang Dianggap Kurang Penting



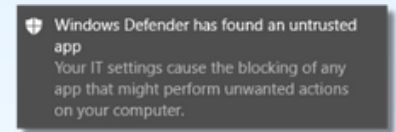
Sumber : microsoft.com



Sumber : reddit.com



Sumber : google.com



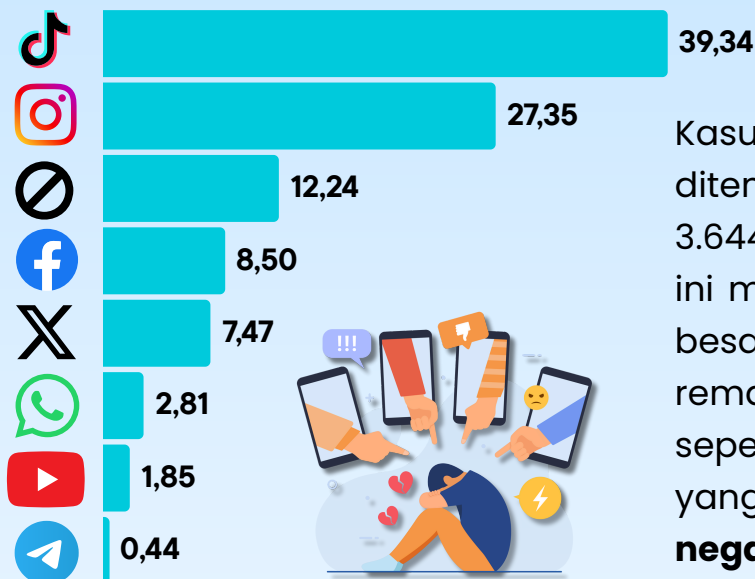
Sumber : ghacks.net

Gambar 3.2 Contoh Peringatan Keamanan yang Dianggap Kurang Penting

Peringatan yang umumnya dianggap **penting** mencakup perlindungan data pribadi, seperti keamanan media sosial dan transaksi *online*, risiko penipuan dalam pembelian *online*, serangan *phishing* untuk mencuri informasi sensitif, deteksi malware atau virus oleh perangkat lunak antivirus, serta notifikasi tentang aktivitas login mencurigakan dari lokasi atau perangkat tidak dikenali.

Di sisi lain, beberapa peringatan dianggap **kurang penting**, seperti penggunaan kata sandi lemah, pembaruan perangkat lunak yang sering ditunda, sertifikat keamanan situs web yang tidak valid, risiko penggunaan jaringan WiFi publik tanpa pengamanan, serta izin aplikasi pada perangkat *mobile* yang sering diabaikan.

Kasus Cyberbullying di Media Sosial



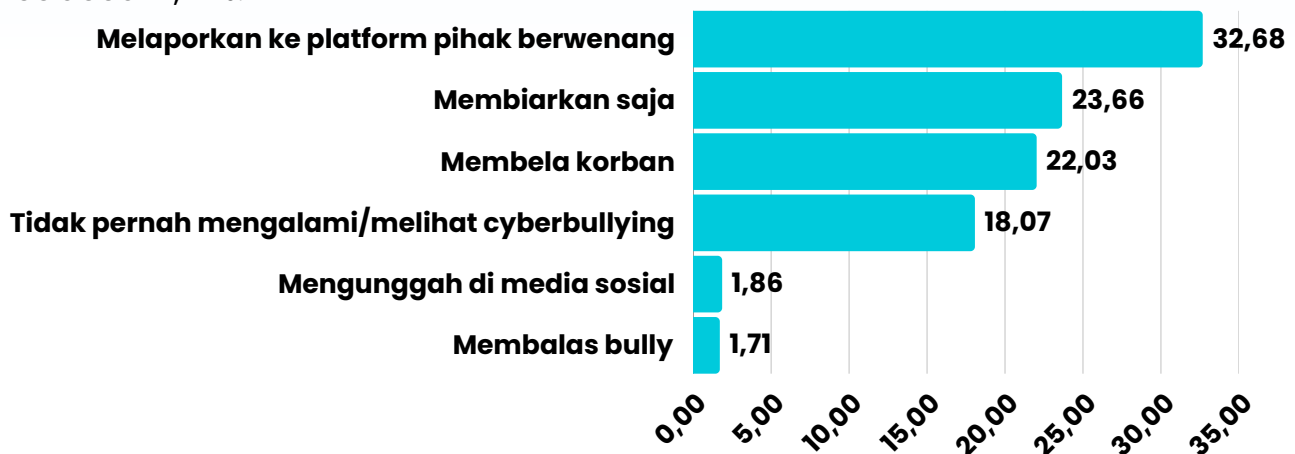
Grafik 3.11 Kasus Cyberbullying di Media Sosial

Kasus cyberbullying paling tinggi ditemukan di **TikTok** (39,34%) oleh 3.644 responden karena *platform* ini memiliki basis pengguna yang besar, terutama di kalangan remaja, dengan **fitur interaktif** seperti **komentar** dan **video duet** yang sering memicu interaksi **negatif**.

Tindakan Saat Mengalami/Melihat Cyberbullying di Media Sosial

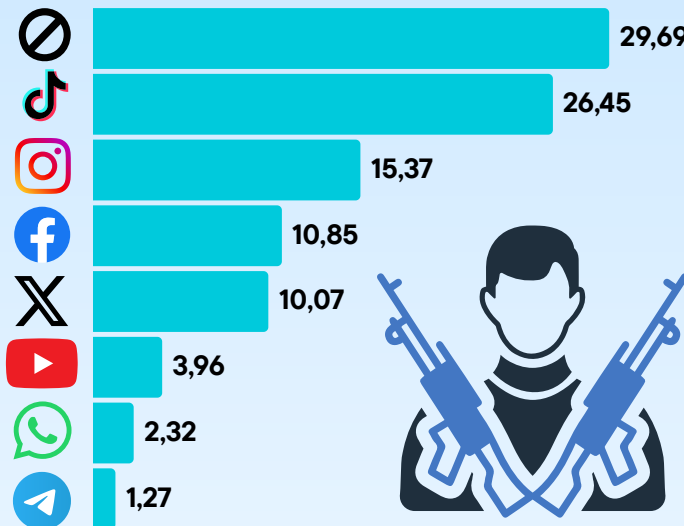


Sebesar 32,68% responden **melaporkan** cyberbullying ke pihak yang berwenang. Pilihan ini menjadi hasil yang dominan karena siswa cenderung mencari **dukungan** dari orang yang mereka **percayai**, seperti teman, guru, atau orang tua, untuk membantu mengatasi masalah ini. Sebagian kecil responden juga ada yang membalas *bully* sebesar 1,71%.



Grafik 3.12 Tindakan Saat Mengalami/Melihat Cyberbullying

Kasus Radikalisme/Terrorisme di Media Sosial

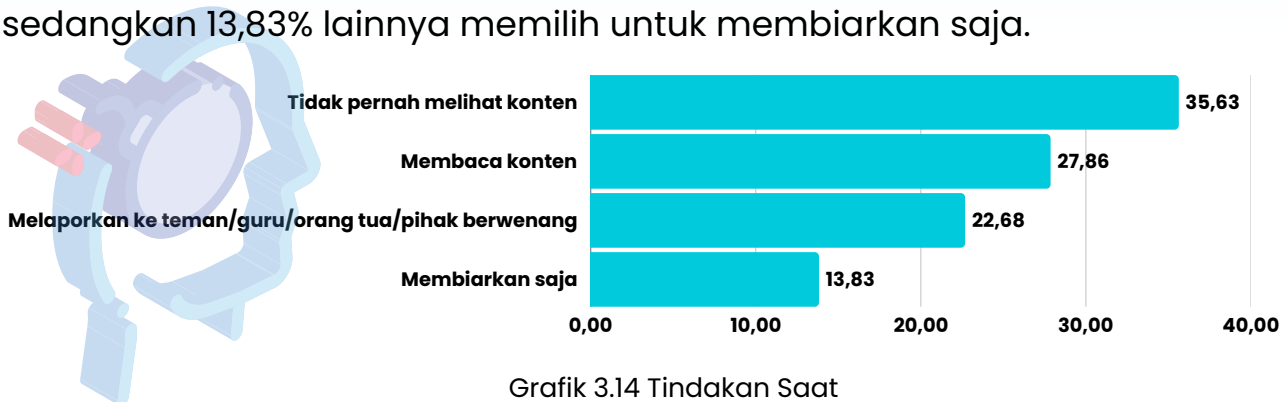


Platform yang paling sering dijumpai oleh responden terkait konten Radikalisme/Terrorisme yaitu **TikTok** sebesar 26,45%, Instagram sebesar 15,37%, Facebook sebesar 10,85%

Grafik 3.13 Kasus Radikalisme/Terrorisme di Media Sosial

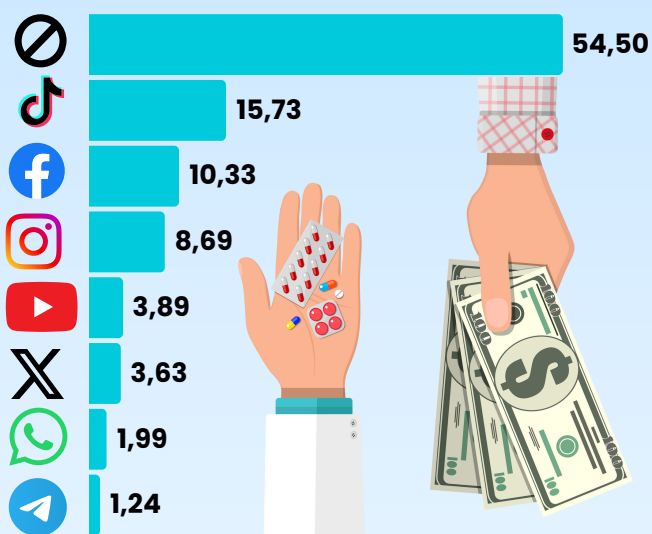
Tindakan Saat Mengalami/Melihat Perilaku Radikalisme/Terrorisme di Media Sosial

Sebesar 35,63% responden mengaku tidak pernah melihat konten radikalisme/terorisme di media sosial. Meski begitu, dari responden yang pernah melihat konten radikalisme/terorisme di media sosial, sebesar 27,86% memilih untuk membaca konten tersebut, sebesar 22,68% melaporkan ke teman, guru, orang tua atau pihak berwenang, sedangkan 13,83% lainnya memilih untuk membiarkan saja.



Grafik 3.14 Tindakan Saat Mengalami/Melihat Radikalisme/Terrorisme

Kasus Transaksi Narkotika di Media Sosial

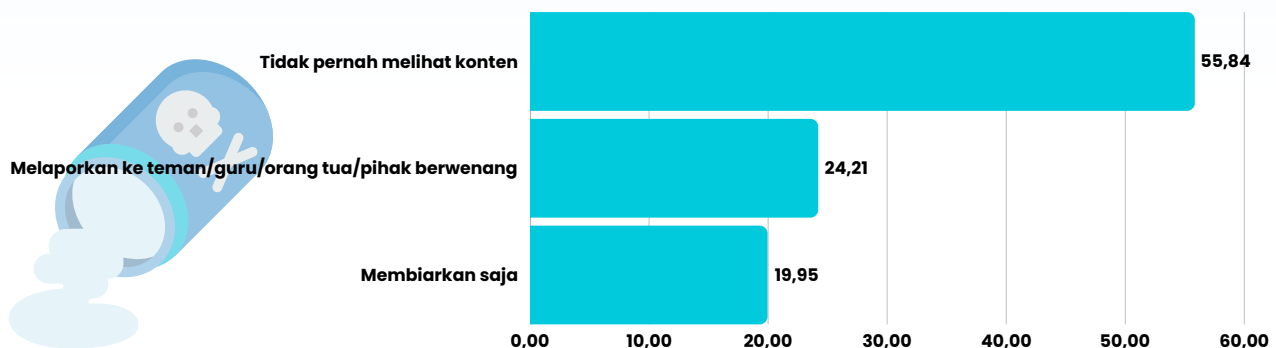


Kasus Narkotika paling banyak ditemui di 3 platform, yaitu **TikTok** dengan persentase responden yang menemui 15,73%, Facebook 10,33%, Instagram 8,69% dan paling sedikit di platform Telegram dengan persentase 1,24% responden.

Grafik 3.15 Kasus Narkotika di Media Sosial

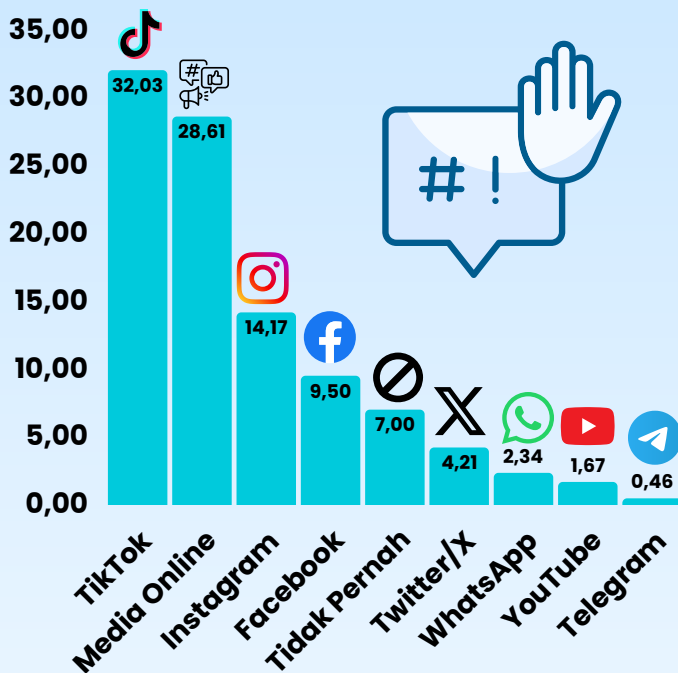
Tindakan Saat Menemukan Informasi/Konten Transaksi Narkotika di Media Sosial

Sebesar 55,84% responden mengaku tidak pernah melihat konten narkotika di media sosial. Meski begitu, dari responden yang pernah melihat konten narkotika di media sosial, sebesar 24,21% memilih untuk melaporkan ke teman, guru, orang tua atau pihak berwenang, sedangkan 19,95% lainnya memilih untuk membiarkan saja.



Grafik 3.16 Tindakan Saat Mengalami/Melihat Informasi/Konten Narkotika

Konten Hoax/Ujaran Kebencian di Media Sosial



Grafik 3.17 Konten Hoax/Ujaran Kebencian di Media Sosial

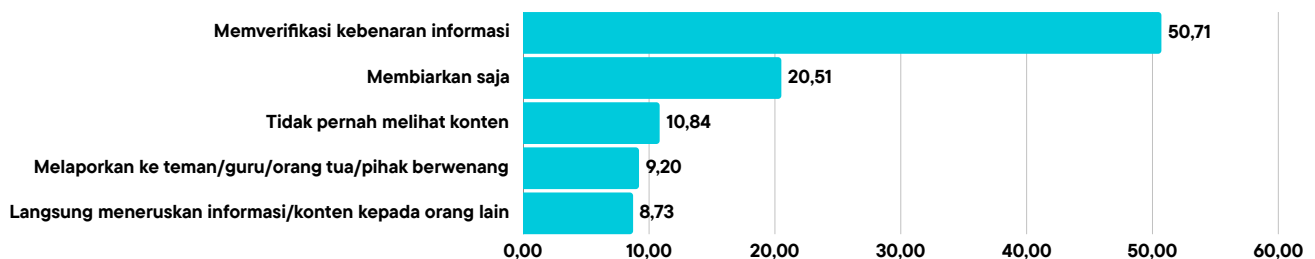
Kasus hoaks/ujaran kebencian di media sosial paling banyak ditemukan responden pada platform **TikTok** sebesar **32,03%** atau sebanyak 2.967 responden dan media *online* sebesar 28,61% atau sebanyak 2.650 responden.

Sebesar 7% atau sebanyak 648 dari responden tidak pernah menemukan hoaks/ujaran kebencian di media sosial.



Tindakan Saat Menemukan Informasi/Konten yang Terindikasi Menyebarkan Hoax/Ujaran Kebencian

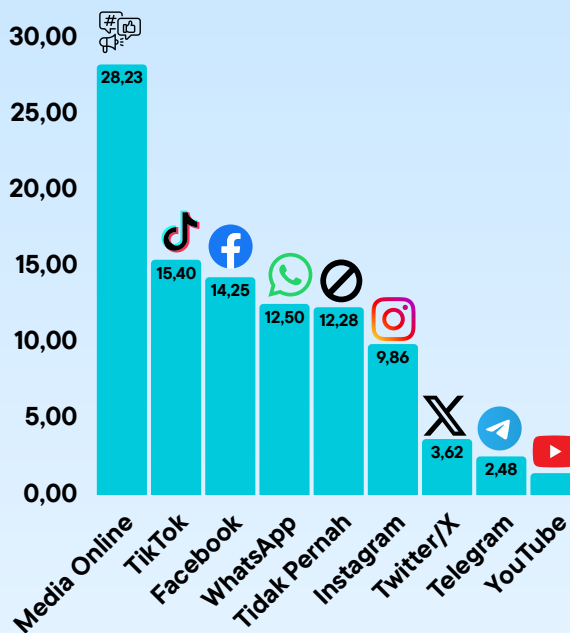
Sebesar **50,71%** responden mengaku memverifikasi kebenaran informasi ketika menemukan konten terindikasi **hoax/ujaran kebencian**, dan sebesar 9,20% responden mengaku melaporkan ke teman/guru/orang tua/pihak berwenang. Selain itu, sebesar 10,84% responden mengaku tidak pernah melihat konten dan 8,73% responden mengaku langsung meneruskan informasi/konten yang dilihat kepada orang lain.



Grafik 3.18 Tindakan Saat Menemukan Konten Hoax/Ujaran Kebencian



Konten Penipuan/Tindak Kejahatan Online



Grafik 3.19 Konten Penipuan/Tindak Kejahatan Online

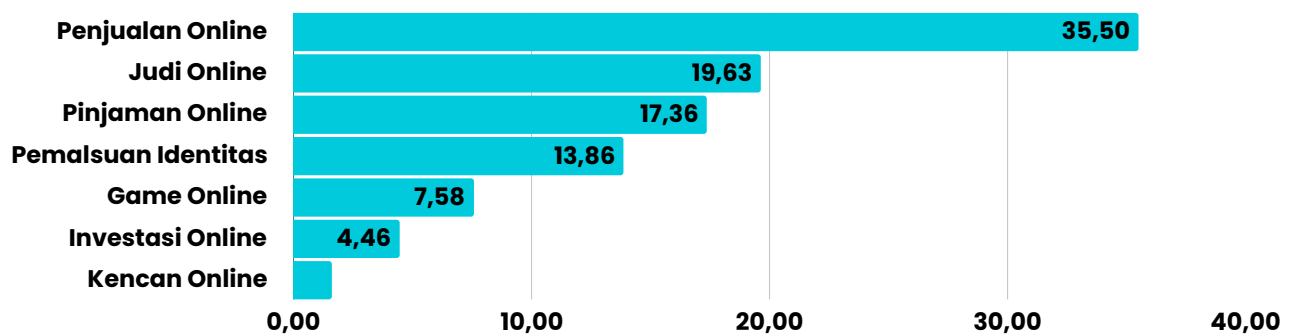
Kasus penipuan/tindak kejahatan *online* di media sosial paling banyak ditemukan responden pada *platform media online* sebesar 28,23% atau sebanyak 2.615 responden.

Sebesar 12,28% atau sebanyak 2.615 responden tidak pernah mengalami kasus penipuan atau tindak kejahatan *online* tersebut.

Kasus Penipuan/Tindak Kejahatan Secara Online yang Pernah Dialami/Dilihat



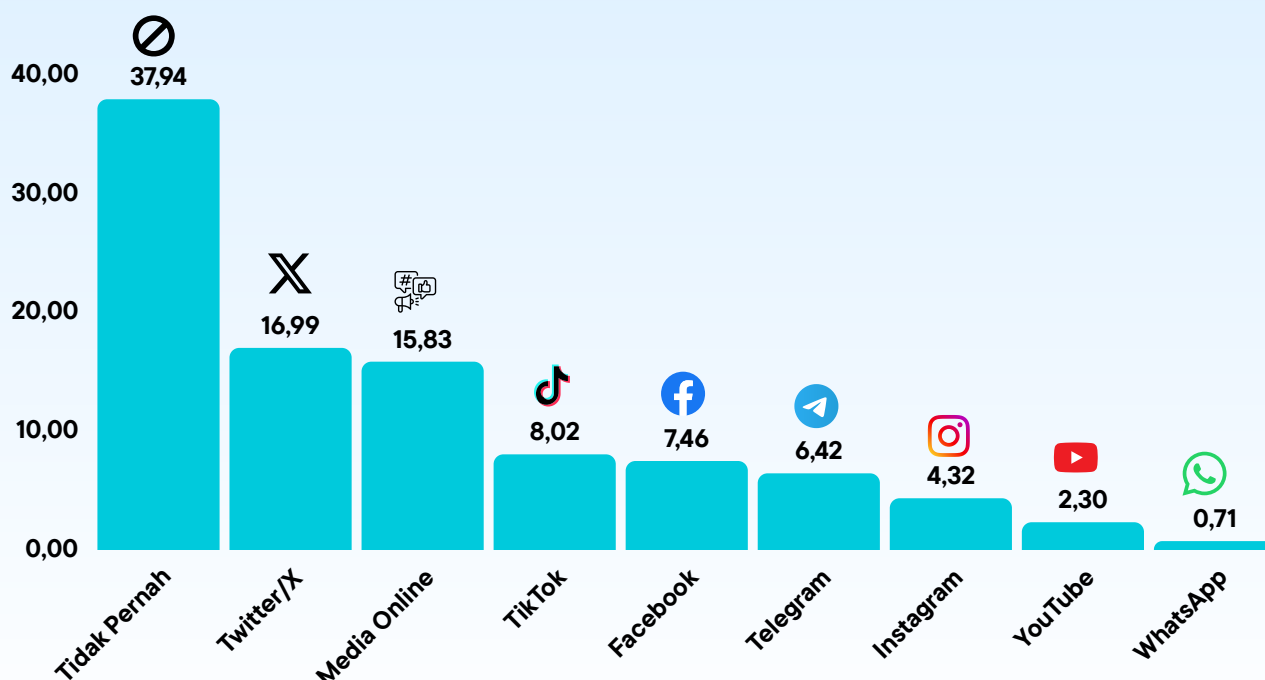
Kasus penipuan/tindak kejahatan secara *online* yang pernah dilihat/dialami oleh responden paling banyak yaitu pada transaksi **penjualan online** sebanyak 35,5% atau sejumlah 3.288 responden. Kasus lainnya ditemukan pada judi *online* sebanyak 19,63%, peminjaman *online* sebanyak 17,36%, pemalsuan identitas sebanyak 13,86%, *game online* sebanyak 7,58%, investasi *online* sebanyak 4,46%, dan paling sedikit yaitu kencan *online* 1,61%.



Grafik 3.20 Kasus Penipuan/Tindak Kejahatan Secara Online yang Pernah Dialami/Dilihat

Konten Pornografi di Media Sosial

Konten pornografi di media sosial paling banyak ditemukan oleh responden pada *platform X (Twitter)* sebesar 16,99% dan **media online** sebanyak 15,83%. Sebanyak 37,94% atau 3.514 dari responden tidak pernah menemukan **konten pornografi** di media sosial. Platform lainnya yang menjadi sumber konten yaitu **TikTok** sebesar 8,02%, **Facebook** sebesar 7,46%, **Telegram** sebesar 6,42%, **Instagram** sebesar 4,32%, **YouTube** sebesar 2,3% dan **WhatsApp** sebesar 0,71%.



Grafik 3.21 Konten Pornografi di Media Sosial



Pembelian barang *online* yang sering dilakukan

Peluang ancaman terhadap responden dapat diidentifikasi berdasarkan data hasil survei pembelian barang *online* yang sering dilakukan responden. Tiga persentase teratas yaitu produk **fashion** dan **kecantikan** sebesar 46,98% atau sebanyak 4.351 responden, kemudian untuk kebutuhan **pendidikan** sebesar 15,20% dan kebutuhan **games** sebesar 7,89% atau sebanyak 731 responden.

Sementara itu, sebesar 13,49% atau sebanyak 1.249 responden **tidak pernah** membeli barang secara *online*.

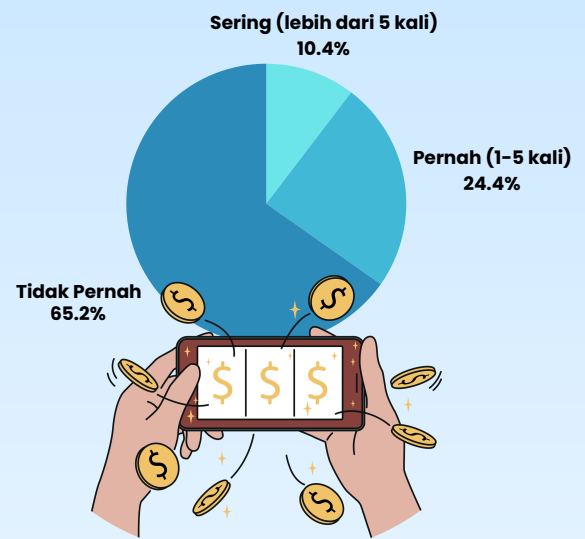


Grafik 3.22 Pembelian Barang *Online* yang Dilakukan

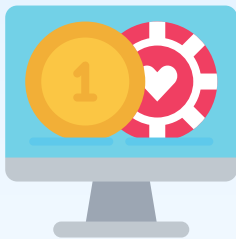


Tawaran mengikuti judi online

Peluang ancaman lain melalui media sosial dapat diidentifikasi berdasarkan jumlah konten terkait judi *online*. Sebagian besar responden menjawab **tidak pernah** mendapatkan tawaran judi *online*, yaitu sebesar 65,2% atau sebanyak 6.043 responden. Hampir seperempat responden **pernah ditawarkan** judi *online* dalam rentang **1 sampai 5 kali** sebesar 24,38% dan sisanya sebesar 10,38% atau sebanyak 961 responden mengaku **sering mendapat** tawaran tersebut.



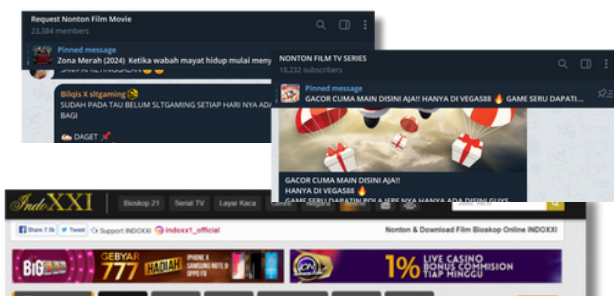
Grafik 3.23 Tawaran Mengikuti Judi Online



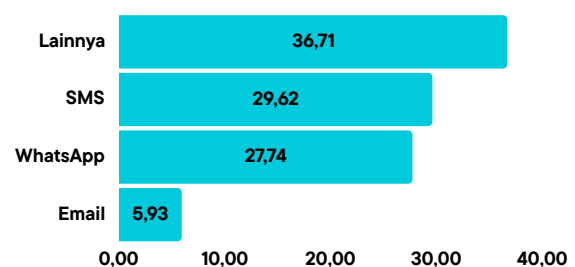
Media yang memberikan tawaran judi online

Media yang digunakan oknum untuk menawarkan judi *online* kepada responden diantaranya melalui **SMS** (29,62%), *platform* WhatsApp (27,74%), dan email (5,93%).

Selain itu, sebanyak 3.080 (36,71%) responden mengaku mendapatkan tawaran judi *online* melalui media lain. Media lain yang dimaksud antara lain laman web, *platform* media sosial (contoh: Telegram), dan penyedia layanan film gratis ilegal.



Gambar 3.3 Contoh Kasus Judi Online



Grafik 3.24 Media yang Memberikan Tawaran Judi Online

Financial Crime (Penipuan Finansial Online)



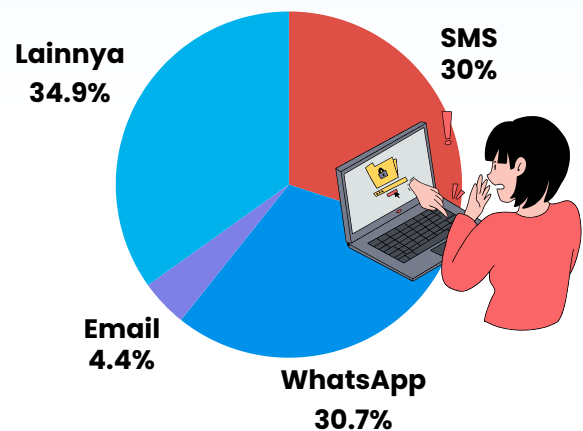
Grafik 3.25 Penipuan Finansial Online

Responden yang pernah menjadi korban dari tindak penipuan *online* (*financial crime*) yaitu sebesar 25,66% atau sebanyak 2.377 responden, kurang lebih hanya satu per empat bagian dari keseluruhan responden.

Responden yang **tidak pernah menjadi korban** tindak kejahatan *financial crime* sebesar 74,34% atau sebanyak 6.885 responden.

Media yang mengirimkan pesan tawaran Financial Crime

Pesan tawaran mengenai **financial crime** diterima oleh responden melalui *platform* pesan instan **WhatsApp** sebesar 30,72% atau sebanyak 2.480 responden, melalui **SMS** sebesar 29,99% dan email 4,43%. Responden paling banyak menjawab **media lainnya** selain pilihan yaitu WhatsApp, SMS maupun email dengan persentase sebesar 34,86% atau sebanyak 2.815 responden.



Grafik 3.26 Media yang Mengirimkan Pesan Tawaran Financial Crime

Pengetahuan Terhadap Dampak Algoritma Filter Bubble



Sumber : [Medium.com](https://www.medium.com)

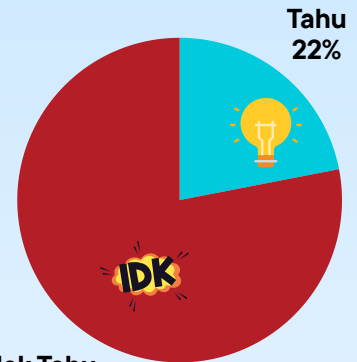


Filter Bubble memungkinkan user untuk **mendapatkan konten serupa sesuai dengan perilakunya** ketika menggunakan layanan internet. Algoritma tersebut diciptakan untuk **memudahkan pencarian** di media sosial dan membantu pengiklan **menyasar target** pasarnya.

Sumber : [Medium.com](https://www.medium.com)



Menilik pengetahuan responden terhadap algoritma *Filter Bubble* (gelembung virtual penyaring informasi) yang ada di media sosial, **mayoritas responden (78,05%) mengaku tidak mengetahui**, sedangkan 21,95% lainnya mengaku sudah mengetahui. Hal ini menunjukkan pengetahuan responden yang relatif masih rendah terkait dengan adanya algoritma *Filter Bubble* di media sosial.



Tidak Tahu
78.1%

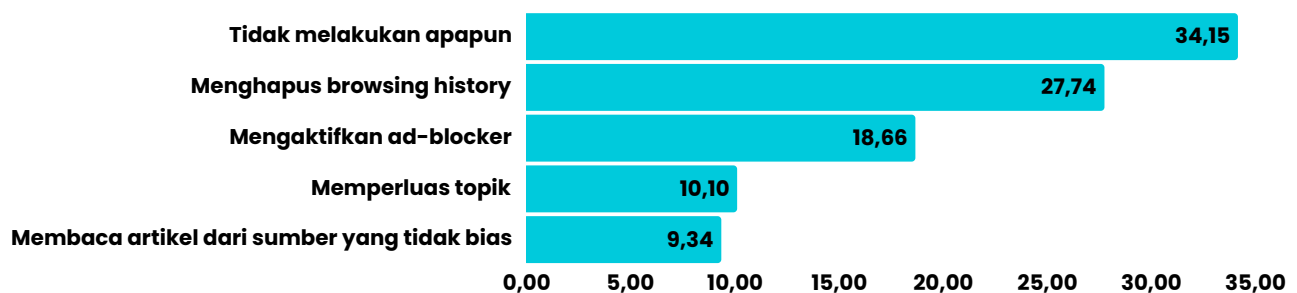
Grafik 3.27 Pengetahuan terhadap Dampak Algoritma Filter Bubble

Tindakan Untuk Mengurangi Dampak Dari Algoritma Filter Bubble

Menilik tindakan yang dilakukan responden untuk mengurangi dampak dari algoritma *Filter Bubble*, sebesar 34,15% atau sebanyak 3.890 responden mengaku tidak melakukan apapun sebagai tindak pencegahan. Sementara itu, sebesar 65,84% responden melakukan berbagai tindak pencegahan seperti menghapus *history browser* (27,74%), mengaktifkan *ad-blocker* (18,66%), memperluas topik yang dikonsumsi (10,10%), dan membaca artikel dari sumber yang tidak bias (9,34%).



Sumber : [nbcnews.com](https://www.nbcnews.com)



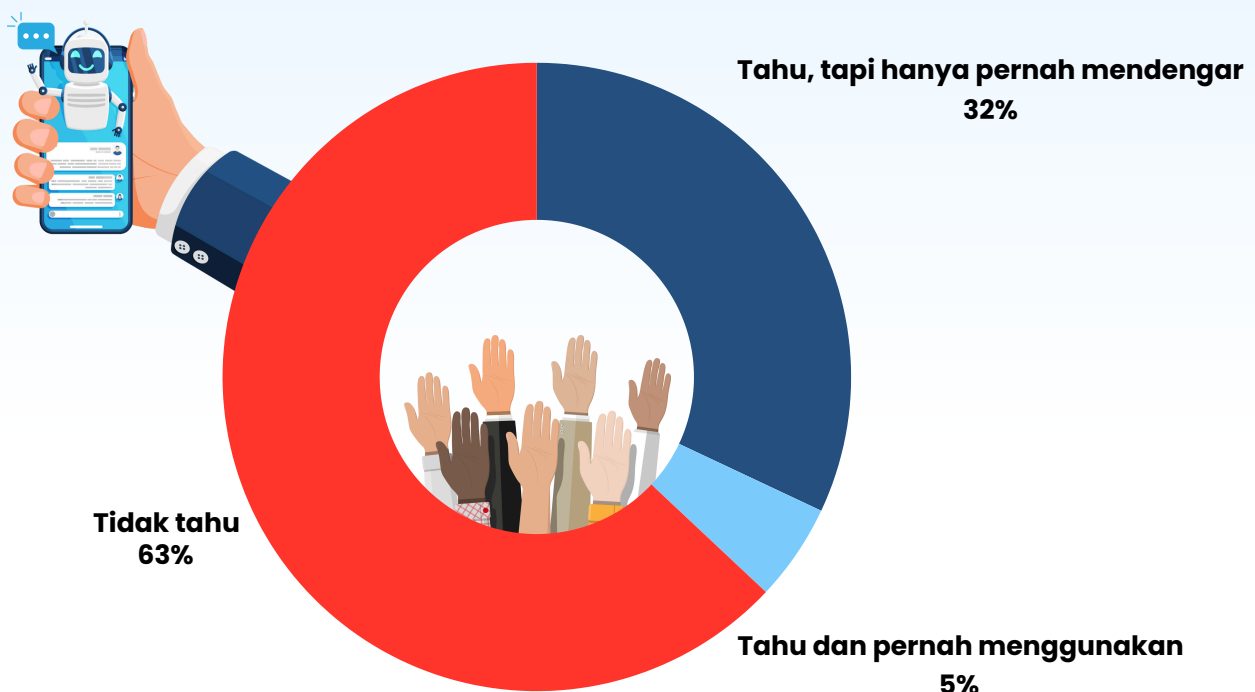
Grafik 3.28 Tindakan Mengurangi Filter Bubble

Pengetahuan Mengenai Platform Bot Pemilu

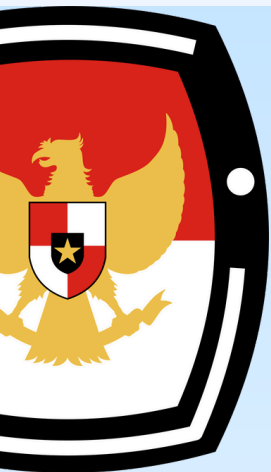


Menilik pengetahuan responden terhadap adanya Platform Bot Pemilu, **mayoritas responden (63%) mengaku tidak mengetahui**, sedangkan 32% lainnya mengaku tahu, tapi hanya pernah mendengar, dan 5% lainnya mengaku tahu dan pernah menggunakan. Adanya penggunaan Platform Bot Pemilu ini salah satunya adalah karena tahun

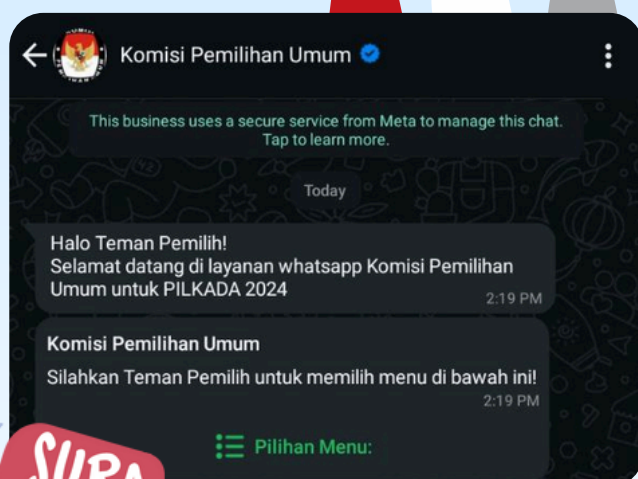
2024 merupakan tahun Pemilu, sehingga Platform Bot Pemilu digunakan sebagai media edukasi politik yang sehat bagi masyarakat. Namun, dari hasil survey menunjukkan bahwa tingkat pengetahuan responden terhadap keberadaan bot ini masih relatif rendah.



Grafik 3.29 Pengetahuan terhadap Platform Bot Pemilu



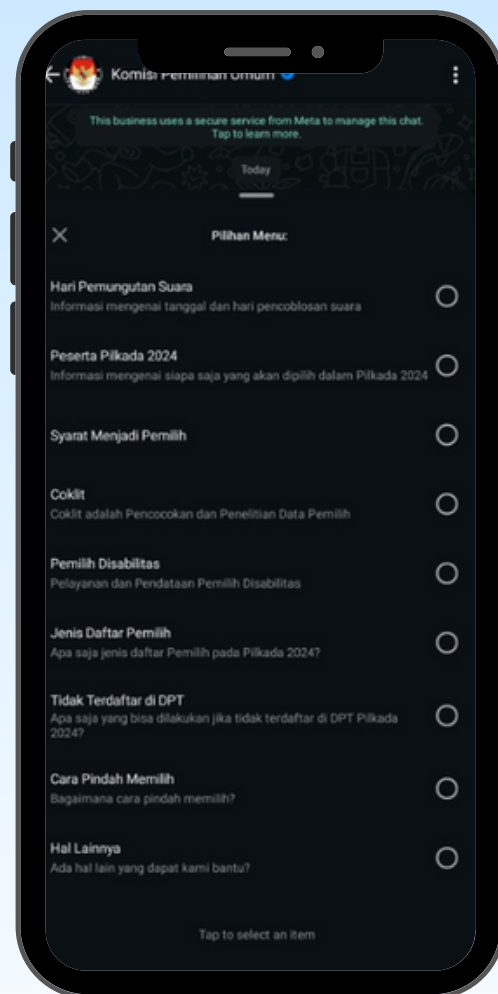
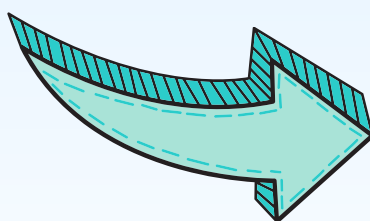
Chatbot Pemilu 2024



**SURA
SULU**

SUARA RAKYAT, SUARA PEMILU

Sumber : kpu.go.id



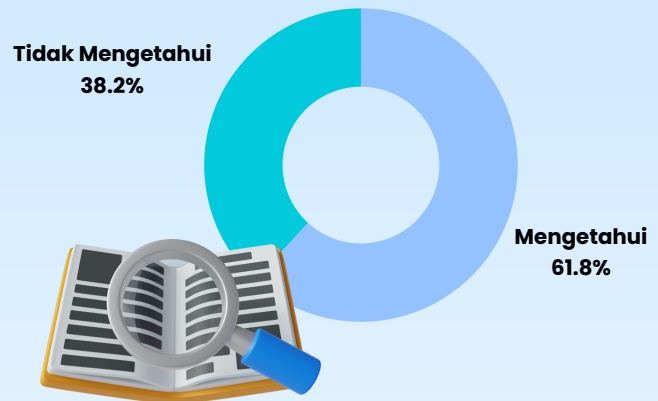
Gambar 3.4 Chatbot Pemilu 2024

Chatbot Pemilu 2024 adalah bot yang disediakan oleh Komisi Pemilihan Umum (KPU) sebagai bentuk layanan bagi masyarakat Indonesia yang ingin **mengetahui informasi seputar Pemilu 2024** serta dalam rangka memperluas informasi kepemiluan. Bot ini berbasis *platform* WhatsApp dan memiliki fitur berbagai **menu** bagi para pengguna.

Informasi yang disediakan *chatbot* ini meliputi **kampanye**, cara menggunakan **hak pilih**, cara **pindah** memilih, daftar calon tetap (**DPT**), **partai politik** pemilu pilihan Pemilu 2024, **cek** daftar pemilih, **jenis** daftar pemilih, **syarat** menjadi pemilih, hingga informasi.

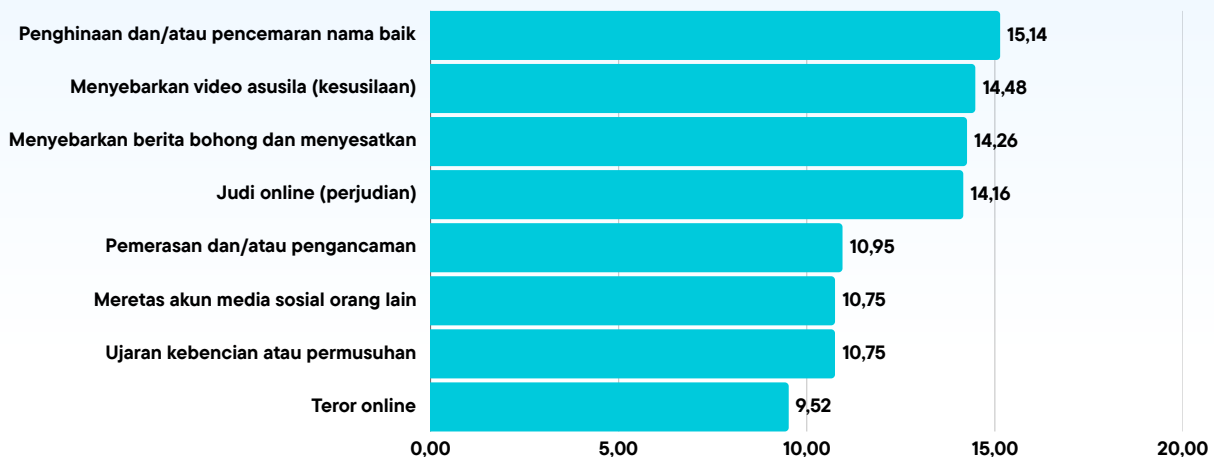
Pengetahuan Larangan Internet Berdasarkan UU ITE

Berdasarkan hasil survei, mayoritas responden (sebesar 61,81% atau sebanyak 5.725 responden mengaku **mengetahui hal-hal yang dilarang** dilakukan di **internet** berdasarkan undang-undang ITE, sementara sebesar 38,19% atau sebanyak 3.537 responden tidak mengetahui hal tersebut.



Grafik 3.30 Pengetahuan Larangan di Internet Berdasarkan UU ITE

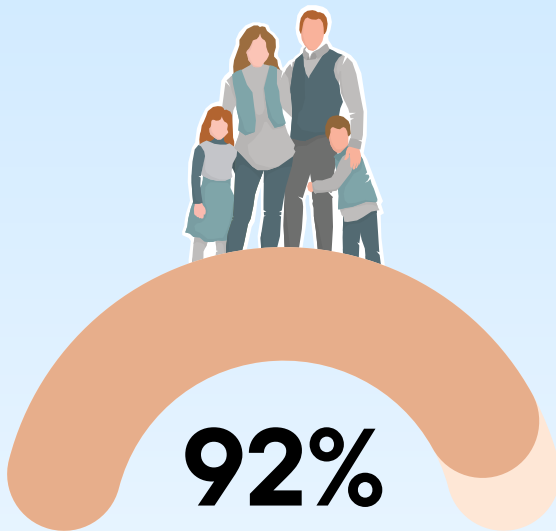
Hal-hal yang dilarang Internet Berdasarkan UU ITE



Grafik 3.31 Larangan di Internet berdasarkan UU ITE

Larangan berdasarkan UU ITE yang diketahui responden paling banyak yaitu **Penghinaan dan/atau pencemaran nama baik** (sebesar 15,14% atau sebanyak 6.036 responden), sedangkan paling rendah yaitu **Teror online** (sebesar 9,52% atau sebanyak 3.794 responden).

Peran orang tua/keluarga dalam mengingatkan siswa terhadap bahaya penggunaan internet

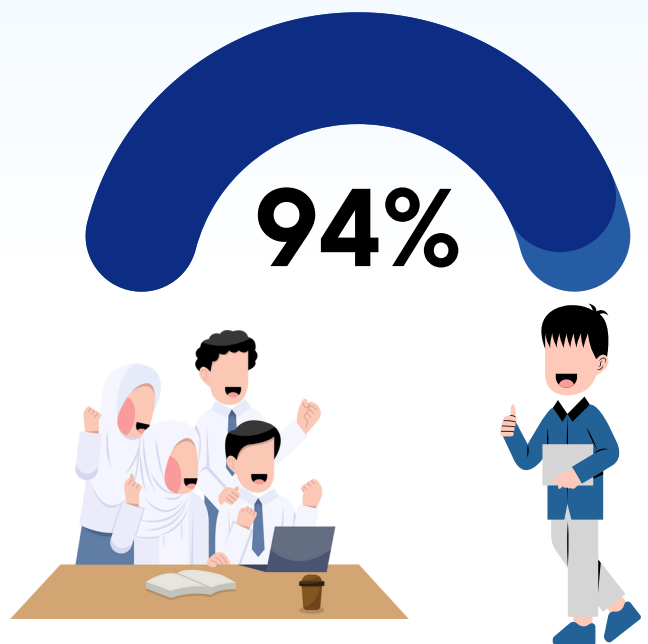


Grafik 3.32 Peran Orang Tua/Keluarga dalam Mengingatkan Siswa

Berdasarkan hasil survei, hampir seluruh responden menyatakan **setuju** bahwa **orang tua/keluarga berperan** dalam mengingatkan siswa terhadap bahaya penggunaan internet (sebanyak 92,36% atau 8.554 responden), sedangkan sebanyak 7,64% atau 708 responden mengaku orang tua/keluarga tidak berperan dalam mengingatkan bahaya penggunaan internet.

Peran guru dalam mengingatkan siswa terhadap bahaya penggunaan internet

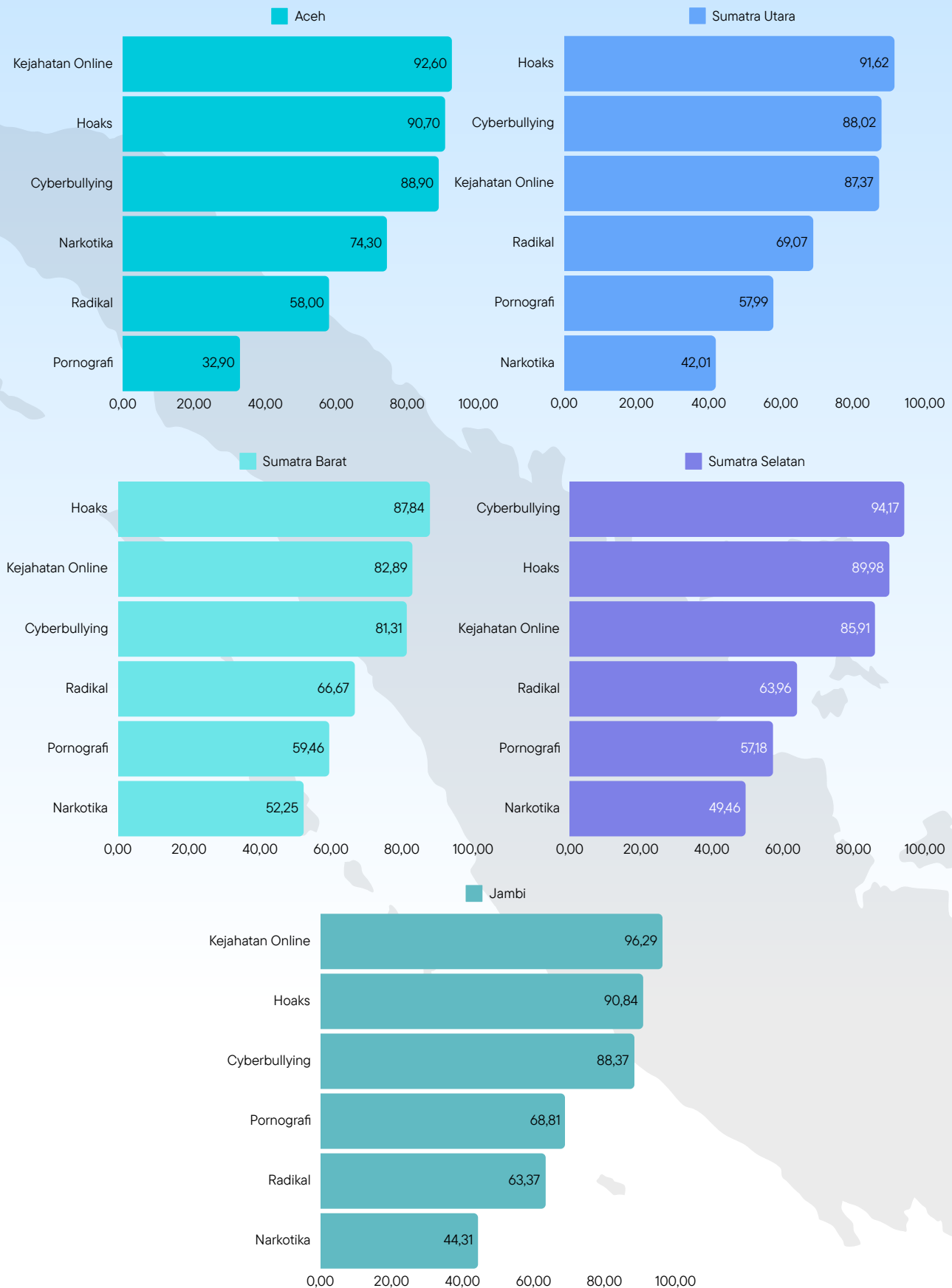
Berdasarkan hasil survei, hampir seluruh responden menyatakan **setuju** bahwa **guru berperan** dalam mengingatkan siswa terhadap bahaya penggunaan internet (sebanyak 94,46% atau 8.749 responden), sedangkan sebanyak 5,54% atau 513 responden mengaku orang tua/keluarga tidak berperan dalam mengingatkan bahaya penggunaan internet. Apabila dibandingkan dengan peran orang tua/keluarga, diketahui bahwa peran guru sedikit lebih besar dalam mengingatkan siswa terhadap bahaya penggunaan internet.



Grafik 3.33 Peran Guru dalam Mengingatkan Siswa

Temuan konten negatif per Provinsi

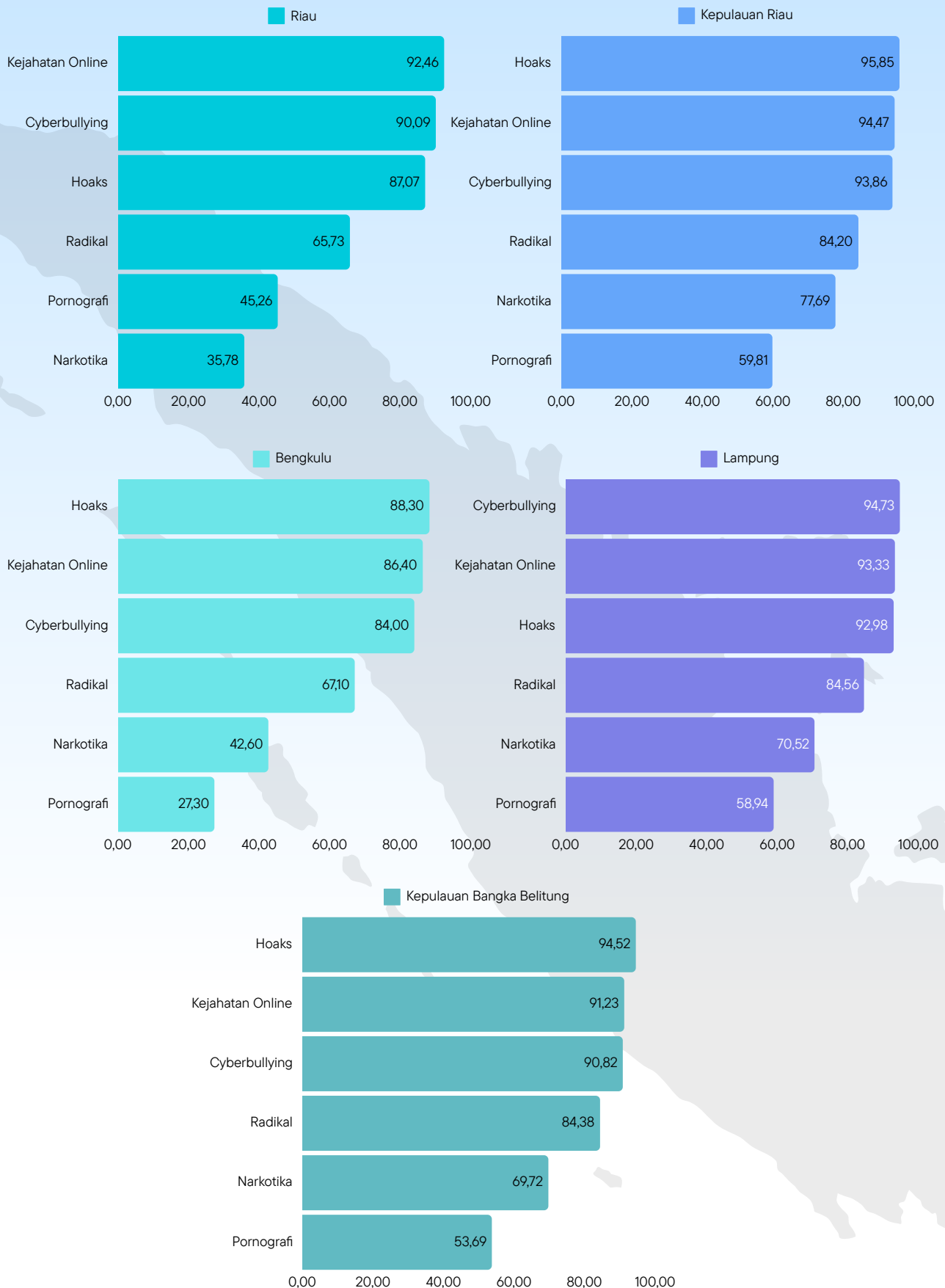
Pulau Sumatra (1)



Grafik 3.34 Temuan Konten Negatif Pulau Sumatra (1)

Temuan konten negatif per Provinsi

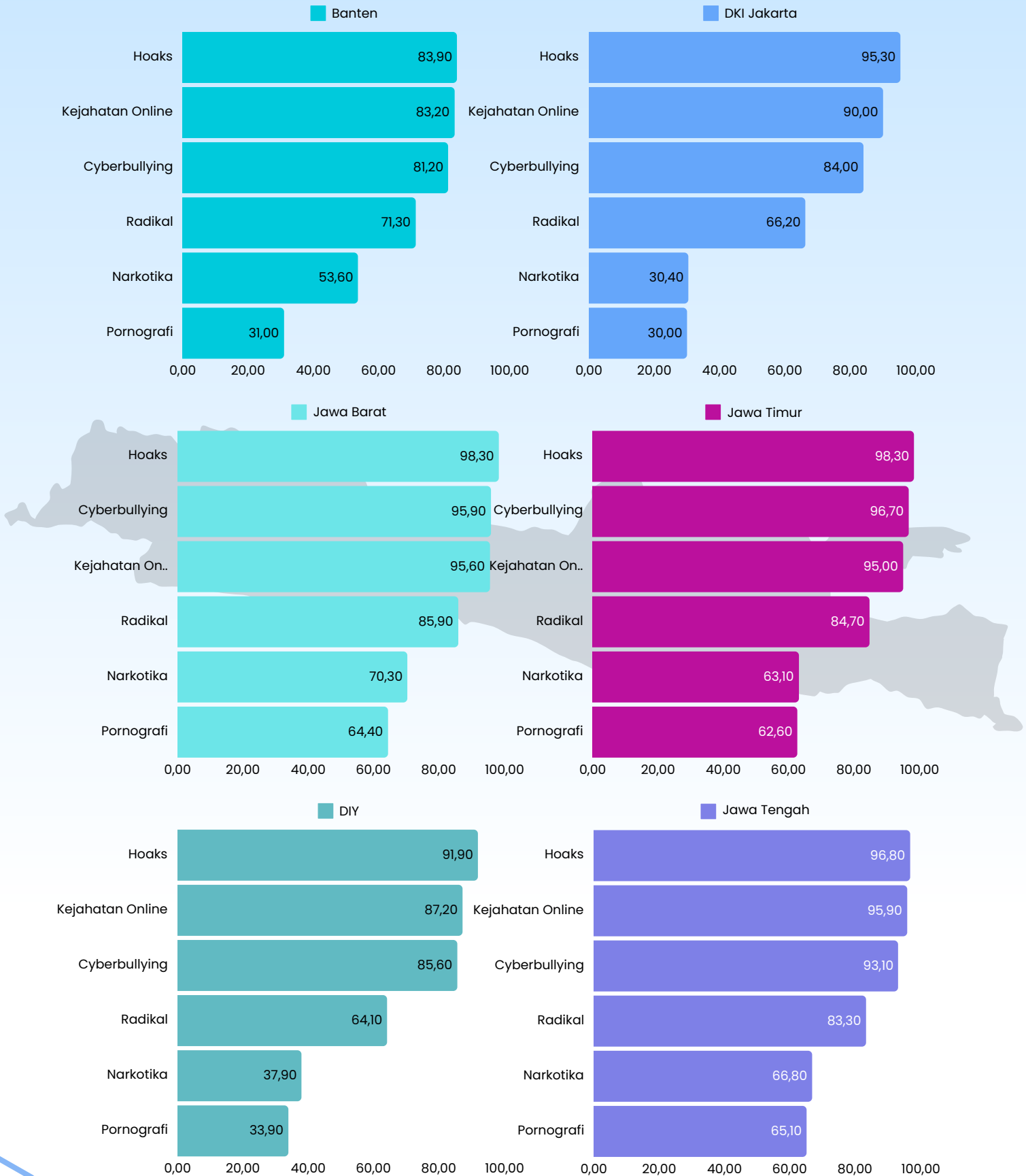
Pulau Sumatra (2)



Grafik 3.35 Temuan Konten Negatif Pulau Sumatra (2)

Temuan konten negatif per Provinsi

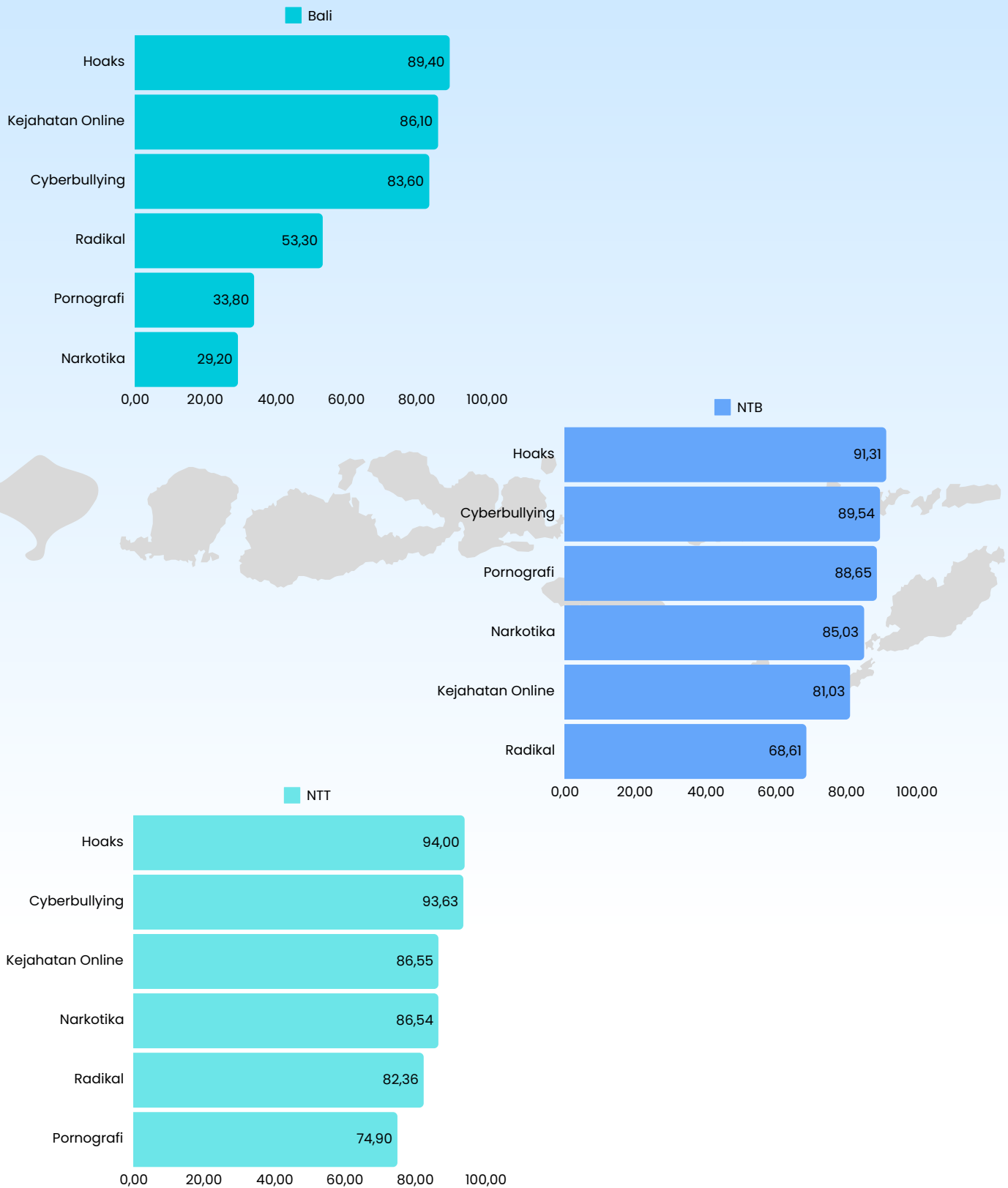
Pulau Jawa



Grafik 3.36 Temuan Konten Negatif Pulau Jawa

Temuan konten negatif per Provinsi

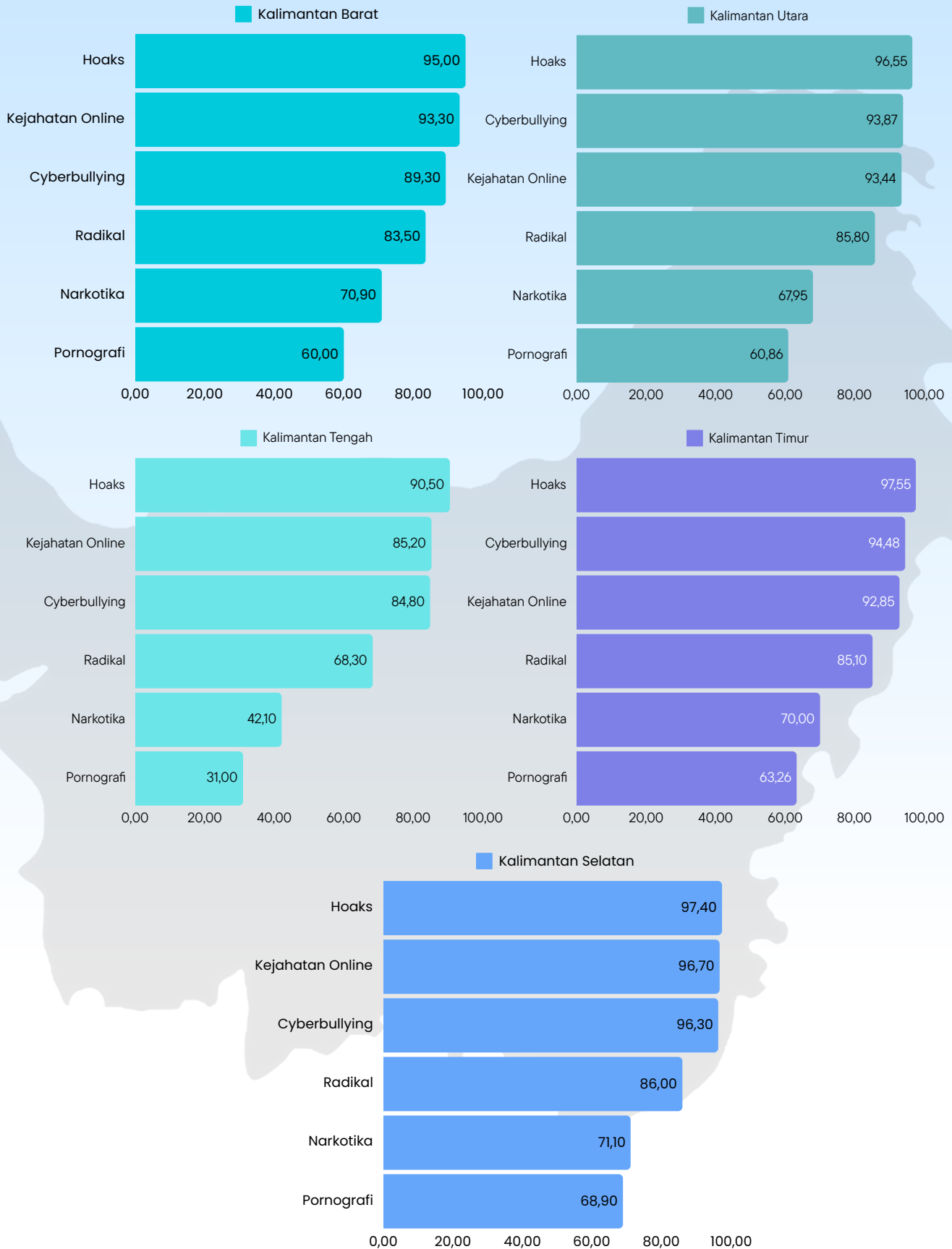
Pulau Bali NTT dan NTB



Grafik 3.37 Temuan Konten Negatif Pulau Bali, NTT, dan NTB

Temuan konten negatif per Provinsi

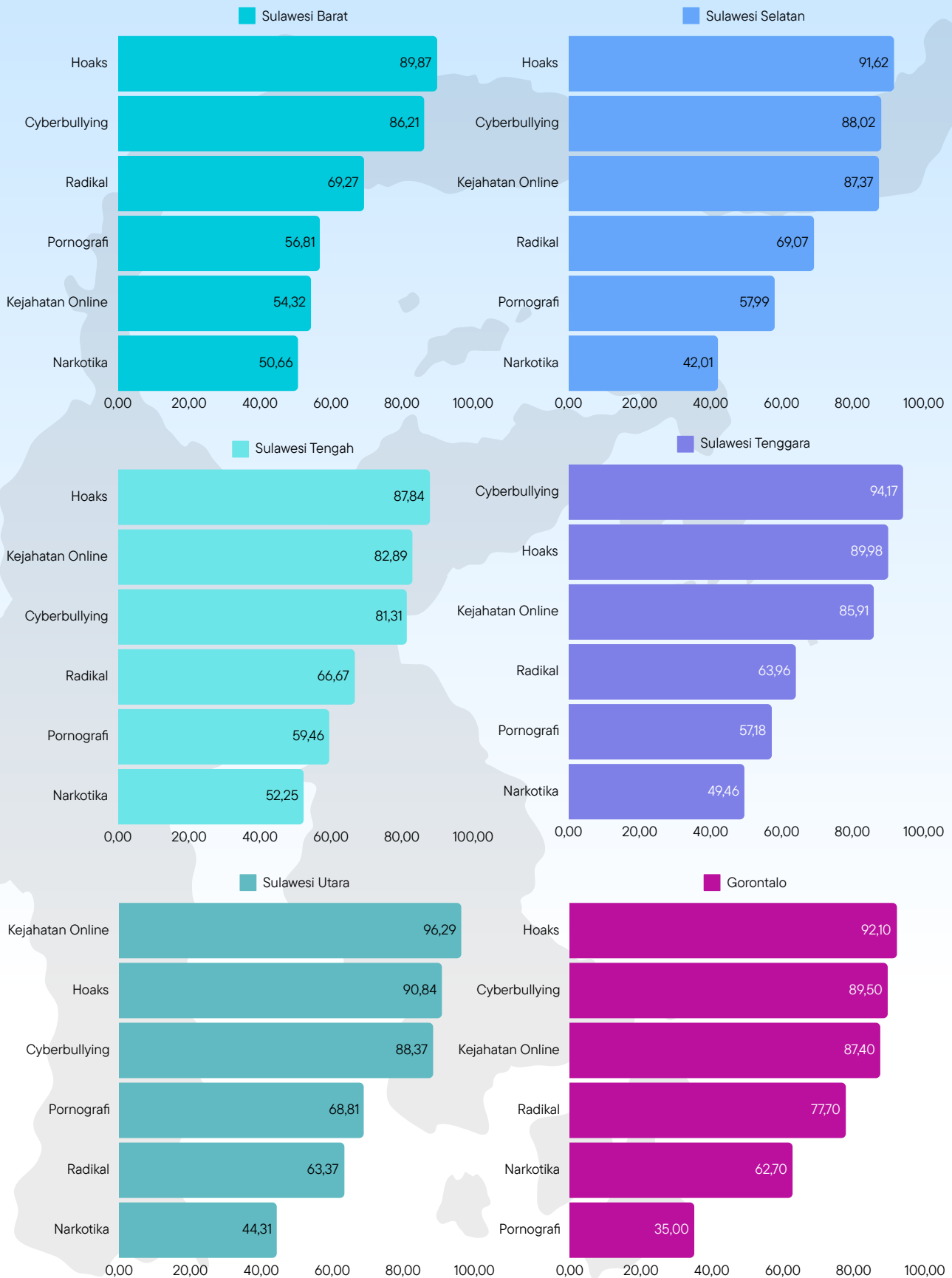
Pulau Kalimantan



Grafik 3.38 Temuan Konten Negatif Pulau Kalimantan

Temuan konten negatif per Provinsi

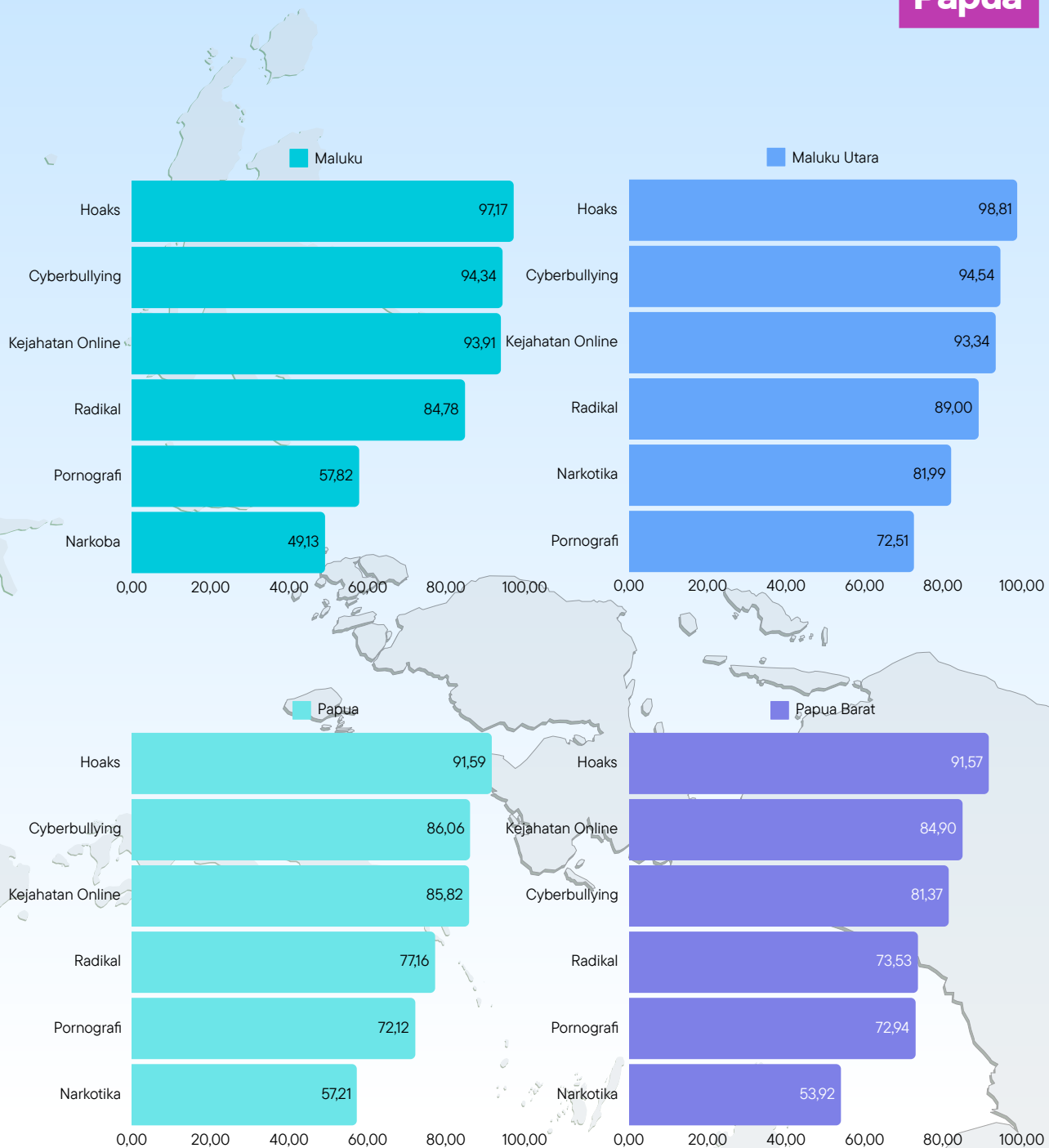
Pulau Sulawesi



Grafik 3.39 Temuan Konten Negatif Pulau Sulawesi

Temuan konten negatif per Provinsi

Pulau Maluku dan Papua



Grafik 3.40 Temuan Konten Negatif Pulau Maluku dan Papua

BAB IV

Penutup

A collection of decorative geometric shapes, primarily triangles, in various shades of green and dark green. Some are solid, while others are outlined. They are arranged in a cluster on the left side of the page, with some overlapping. The background is a solid dark green with a light green curved shape at the top right and bottom left.

Peringkat Provinsi berdasarkan Dampak Negatif Media Sosial

Cyberbullying



Grafik 4.1 Peringkat Provinsi berdasarkan Dampak Negatif Cyberbullying

Posisi 1: Jawa Timur (96.7%)
Posisi 2: Kalimantan Selatan (96.3%)
Posisi 3: Jawa Barat (95.9%)

Pornografi



Grafik 4.2 Peringkat Provinsi berdasarkan Dampak Negatif Pornografi

Posisi 1: Sumatera Selatan (93.72%)
Posisi 2: Nusa Tenggara Barat (88.65%)
Posisi 3: Nusa Tenggara Timur (74.90%)

Peringkat Provinsi berdasarkan Dampak Negatif Media Sosial

Radikalisme



Grafik 4.3 Peringkat Provinsi berdasarkan Dampak Negatif Radikalisme

Posisi 1: Maluku Utara (89%)
Posisi 2: Jawa Barat (85.9%)
Posisi 3: Kalimantan Utara (85.8%)

Kejahatan Online



Grafik 4.4 Peringkat Provinsi berdasarkan Dampak Negatif Kejahatan Online

Posisi 1: Kalimantan Selatan (96.7%)
Posisi 2: Sulawesi Utara (96.29%)
Posisi 3: Jawa Tengah (95.9%)

Peringkat Provinsi berdasarkan Dampak Negatif Media Sosial

Narkotika



Grafik 4.5 Peringkat Provinsi berdasarkan Dampak Negatif Narkotika

Posisi 1: Sumatra Selatan (96.86%)

Posisi 2: Sumatra Barat (95.27%)

Posisi 3: Sumatra Utara (90.22%)

Hoaks



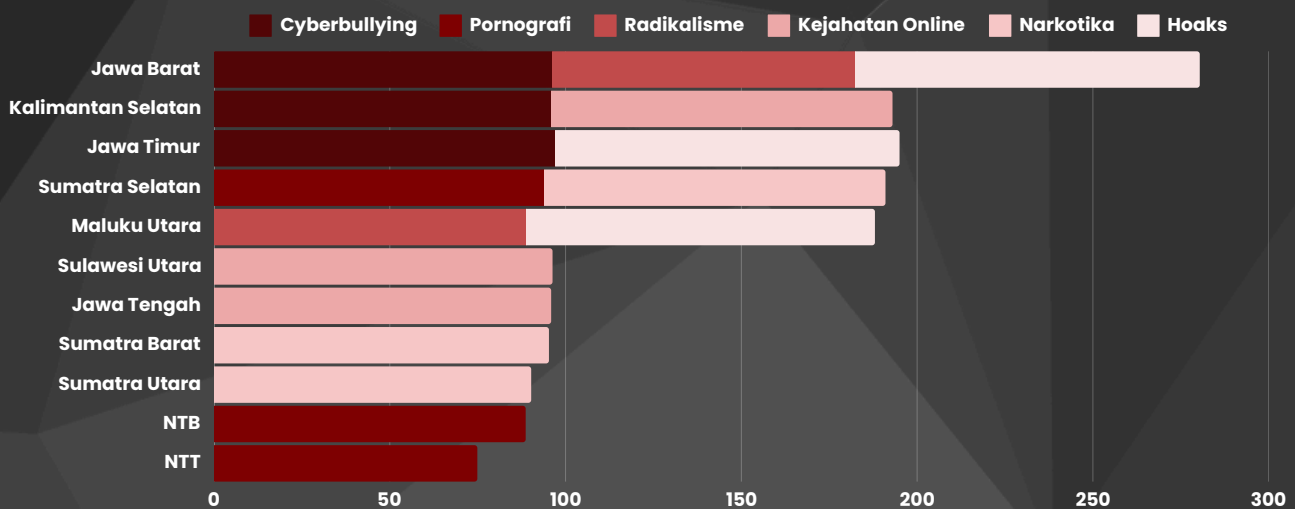
Grafik 4.6 Peringkat Provinsi berdasarkan Dampak Negatif Hoaks

Posisi 1: Maluku Utara (98.81%)

**Posisi 2: Jawa Barat (98.3%) dan
Jawa Timur (98.3%)**

Posisi 3: Kalimantan Selatan (97.4%)

Temuan konten negatif tertinggi di tahun 2024 berdasarkan indikator dan dampak media sosial yang telah ditentukan sesuai dengan urutan provinsi sebelumnya (halaman 43 s.d. 49) ditunjukkan pada grafik berikut.



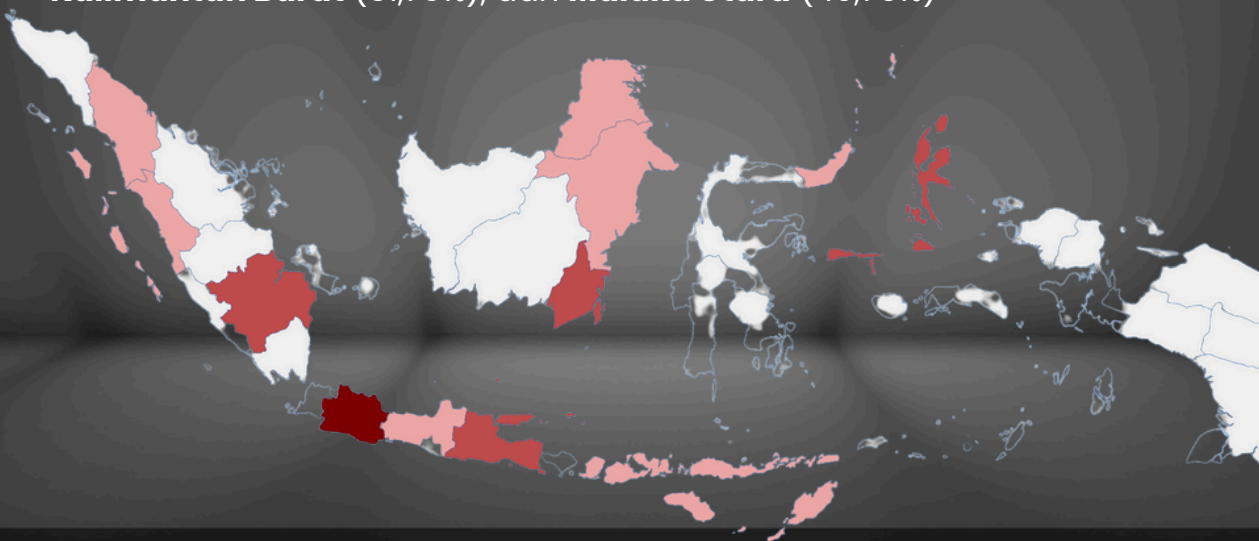
Grafik 4.7 Temuan Konten Negatif Tertinggi di Provinsi Indonesia

1. Penemuan informasi yang berkaitan dengan Cyberbullying: Jawa Timur (96,7%), Kalimantan Selatan (96,3%), dan Jawa Barat (95,9%)
2. Penemuan informasi yang berkaitan dengan Pornografi: Sumatra Selatan (93,72%), Nusa Tenggara Barat (88,65%), dan Nusa Tenggara Timur (74,90%)
3. Penemuan informasi yang berkaitan dengan Terorisme/Radikalisme: Maluku Utara (89%), Jawa Barat (85,9%), dan Kalimantan Utara (85,8%)
4. Penemuan informasi yang berkaitan dengan Kejahatan *Online*: Kalimantan Selatan (96,7%), Sulawesi Utara (96,29%), dan Jawa Tengah (95,9%)
5. Penemuan informasi yang berkaitan dengan Narkotika: Sumatra Selatan (96,86%), Sumatra Barat (95,27%), dan Sumatra Utara (90,22%)
6. Penemuan informasi yang berkaitan dengan Hoaks: Maluku Utara (98,81%), Jawa Barat dan Jawa Timur (98,3%), serta Kalimantan Selatan (97,4%)

Berdasarkan pemetaan perilaku pengguna ruang siber pada tahun 2023 dan 2024, responden secara umum melaporkan pernah menemui konten negatif di media sosial. Pada tahun 2023, ancaman siber sosial di Indonesia lebih didominasi oleh dampak media sosial berupa pornografi. Namun, pada tahun 2024, ancaman siber sosial di Indonesia lebih didominasi oleh dampak media sosial yang berkaitan dengan penyebaran hoaks

Kesimpulan

1. Durasi penggunaan internet terlama oleh responden (lebih dari 8 jam) paling tinggi di provinsi **Sulawesi Selatan** (44,33%), **Kalimantan Tiimur** (40%), dan **Jawa Barat** (39,26%)
2. Durasi penggunaan media sosial paling lama (lebih dari 8 jam) paling tinggi di **Sulawesi Selatan** (25,25%), **Gorontalo** (22,27%), dan **Kalimantan Timur** (20,4%)
3. Penggunaan koneksi internet yang masih bergantung pada paket data atau kuota operator seluler paling tinggi pada provinsi **Maluku** (53,91%), **Papua** (41,34%), dan **Gorontalo** (40,28%)
4. Responden di provinsi **Riau** (39,22%), **Papua Barat** (34,5%), dan **Sulawesi Tenggara** (30,63%) masih cenderung tidak melakukan tindak lanjut atau mengabaikan *alert warning* pada perangkat
5. Beberapa responden dari provinsi **Kalimantan Selatan** (2,32%), **Bali** (2,1%), dan **Daerah Istimewa Yogyakarta** (1,28%), **Jawa Tengah** (1,48%), **Kalimantan Tiimur** (1,63%), **Papua** (1,92%), **Sulawesi Barat** (1,32%), dan **Sumatra Utara** (1,38%) pernah melakukan *investasi/trading*
6. Tawaran terkait judi *online* sering didapati oleh responden yang berada di provinsi **Jambi** (18,03%), **Banten** (17,4%), dan **Papua Barat** (15,3%)
7. Responden pernah menjadi korban dari tindak kejahatan *financial crime* pada provinsi **Jawa Barat** (37,48%), **Sumatra Utara** (35,24%), dan **Papua** (34,61%)
8. Algoritma *Filter Bubble* paling tinggi diketahui pada provinsi **Jawa Timur** (32,23%), **Papua** (30,28%), dan **Sumatra Barat** (28,01%)
9. *Chatbot* pemilu paling tinggi belum diketahui pada provinsi **Gorontalo** (72,51%), **Bangka Belitung** (71%), dan **Kalimantan Utara** (70,1%)
10. Undang-undang terkait dengan hal-hal yang dilarang dilakukan di internet paling tinggi belum diketahui pada provinsi **Sumatra Selatan** (53,67%), **Kalimantan Barat** (51,70%), dan **Maluku Utara** (49,76%)



Gambar 4.1 Peta Provinsi dengan Dampak Negatif Media Sosial Tertinggi



Referensi

Amarullah, A.H, Runturambi, A. J. S., & Widiawan Bondan. 2021. Analisis Ancaman Kejahatan Siber Bagi Keamanan Nasional Pada Masa Pandemi COVID-19. Jurnal Kajian Stratejik Ketahanan Nasional, Vol.4 No.2.

Awaliyah, C., Dewi, D. A., & Furnamasari, Y. F. 2021. Media Sosial Mempengaruhi Integrasi Bangsa. ISSN: 2614-3097, Vol.5 No.3.

Doni, F. R. 2017. Perilaku Penggunaan Media Sosial Pada Kalangan Remaja. IJSE – Indonesian Journal on Software Engineering, Vol.3 No.2.

Drakel, W. J. 2018. Perilaku Mahasiswa Dalam Menggunakan Media Sosial di Universitas Sam Ratulangi Manado. Holistik, Vol.11 No.21A.

Dyson, E., Gilder, G., Keyworth, G., & Toffler, A. (1994). Cyberspace and the american dream: A magna carta for the knowledge age, future insight.

Indonesia. 2003. Undang-Undang Nomor 25 Tahun 2003 tentang Perubahan atas Undang Undang Nomor 15 Tahun 2002 tentang Tindak Pidana Pencucian Uang. Sekretariat Negara. Jakarta. Indonesia. 2008. Undang-Undang Nomor 44 tahun 2008 tentang Pornografi. Sekretariat Negara. Jakarta.

Indonesia. 2009. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik. Sekretariat Negara. Jakarta.

Indonesia. 2016. Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Sekretariat Negara. Jakarta.

Referensi

Indonesia. 2018. Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan atas Undang Undang Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang Undang Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang. Sekretariat Negara. Jakarta.

Indonesia. 2023. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana. Sekretariat Negara. Jakarta.

Peraturan Badan Siber dan Sandi Negara. 2023. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 Tentang Perubahan Atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 Tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara. Jakarta.

Peraturan Badan Siber dan Sandi Negara. 2018. Peraturan Badan Siber dan Sandi Negara Nomor 3 Tahun 2018 tentang Sistem Nilai Badan Siber dan Sandi Negara. Jakarta.

Peraturan Presiden. 2021. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. Sekretariat Negara. Jakarta.

Suryani, I., Liliyana, Handar, M., & Ekasuci, R. 2020. Pemanfaatan Media Sosial Sebagai Media Promosi Bagi Radio Mersi 93.9 FM. Journal Komunikasi, Vol.11 No.1.

Direktorat Operasi Keamanan dan Pengendalian Informasi
Badan Siber dan Sandi Negara



*"Ingatlah, Bahwa **Kechilafan** Satu Orang Sahaja Tjukup Sudah Menjebabkan
Keruntuhan Negara"*

– dr. Roebiono Kertopati (Bapak Persandian RI)

Peta Perilaku Pengguna Ruang Siber di Indonesia

2024

9000+ Survei

Sebuah survei pemetaan perilaku siber **netizen masa kini** di media sosial



AKTIVITAS MEDIA SOSIAL DI INDONESIA



**BADAN SIBER
DAN SANDI
NEGARA**