

# PERSEPSI MASYARAKAT ATAS PELINDUNGAN DATA PRIBADI



SURVEI NASIONAL TAHUN 2021

**PERSEPSI MASYARAKAT  
ATAS PELINDUNGAN  
DATA PRIBADI**

SURVEI NASIONAL  
TAHUN 2021







**TIM PENYUSUN****Pengarah:**

Direktur Jenderal Aplikasi Informatika,  
Semuel Abrijani Pangerapan

**Penanggung Jawab:**

Sekretaris Direktorat Jenderal Aplikasi Informatika,  
Slamet Santoso

**Perencana Program:**

Poppy Yuniarti Ramdhanian  
Moh. Wildan

**Analisis:**

Hendri Sasmita Yuda  
Ulfah Diah Susanti  
Ajeng Risda Rahmadani

**Periset Kuantitatif:**

Aini Devi Agustian  
Amalia Afifah  
Laksamana Yuda Citra Handika  
Leski Rizkinaswara Yustafa  
Pratiwi Agustini

**Penulis:**

Risanti Delphia  
Maykada Harjono K.

**Editor:**

Adek Media Roza  
Stevanny Limuria  
Vivi Zabkie

**Desain Grafis:**

Muhamad Yana  
Wahyu Risyanto





# KATA PENGANTAR



Salam sejahtera bagi kita semua,

Puji syukur ke hadirat Tuhan YME atas rahmat dan hidayah-Nya, laporan *Persepsi Masyarakat atas Pelindungan Data Pribadi* sebagai hasil kerja sama antara Kementerian Komunikasi dan Informatika dengan Katadata Insight Center telah selesai disusun.

Di tengah pertumbuhan pengguna internet di Indonesia yang terus melonjak, kami berharap sajian dalam laporan ini mampu membangun kesadaran masyarakat akan pentingnya pemahaman tentang data pribadi ketika berinteraksi secara daring.

Penyusunan laporan dilakukan setelah melalui Survei Nasional terhadap 11.305 responden pada Juli 2021. Survei tersebut mengukur seberapa luas pemahaman masyarakat akan pentingnya data pribadi dan hak untuk melindunginya, serta mengetahui bagaimana penerapan pelindungan data pribadi yang berjalan selama ini.

Salah satu tujuan laporan ini adalah untuk menunjukkan tingkat pemahaman dan kepedulian masyarakat tentang data pribadi, penyalahgunaan, serta kesadaran akan hak untuk melindungi data pribadi mereka. Diharapkan pula, seluruh paparan dalam laporan ini dapat membantu pemerintah dalam mematangkan perumusan RUU Pelindungan Data Pribadi (PDP), dan menjadi acuan bagi pengembangan kebijakan PDP pada masa mendatang.

Akhir kata, kami mengucapkan terima kasih dan penghargaan kepada semua pihak yang telah memberikan andil terhadap terbitnya laporan ini. Semoga amal usaha kita direstui Tuhan Yang Maha Esa.



**Semuel Abrijani Pangerapan**  
Direktur Jenderal Aplikasi Informatika  
Kementerian Komunikasi dan Informatika





# DAFTAR ISI

TIM PENYUSUN	III
KATA PENGANTAR	V
DAFTAR GAMBAR	VIII
DAFTAR TABEL	VIII
DAFTAR GRAFIK	VIII
RINGKASAN EKSEKUTIF	X
BAB 1 PENDAHULUAN	3
1.1 Kerangka Penelitian	7
1.2 Pengumpulan Data	8
1.3 Pengolahan dan Analisis Data	9
1.4 Keterbatasan Penelitian	9
1.5 Profil Responden Survei	10
BAB 2 PENGGUNAAN MEDIA SOSIAL DI INDONESIA	15
2.1 Akses dan Durasi Penggunaan Media Sosial	16
2.2 Aktivitas di Media Sosial	17
2.3 Pengaturan Media Sosial	20
BAB 3 PENGETAHUAN TENTANG DATA PRIBADI	23
3.1 Tingkat Pengetahuan Data Pribadi	27
3.2 Prioritas Data Pribadi	30
3.3 Data Pribadi Dibagikan ke Publik	30
3.4 Pengetahuan Kebijakan Privasi	32
BAB 4 PENYALAHGUNAAN DATA PRIBADI	35
4.1 Lembaga atau Produk yang Rentan Kebocoran Data	36
4.2 Penyalahgunaan Data di Media Sosial	38
4.3 Lembaga Pengumpul Data Pribadi	39
BAB 5 PENGETAHUAN AKAN KEAMANAN DATA PRIBADI	41
5.1 Notifikasi Akses Aplikasi Komunikasi, Lokapasar ( <i>Marketplace</i> ) dan Transportasi Daring	42
5.2 Notifikasi Akses Aplikasi Perbankan, Kesehatan, dan Pinjaman <i>Online</i>	43
5.3 Notifikasi Pesan WhatsApp/SMS	46
BAB 6 RUU PELINDUNGAN DATA PRIBADI	51
6.1 Pengetahuan tentang RUU Pelindungan Data Pribadi	52
6.2 Sistem Pelindungan Data di Indonesia	56
BAB 7 PENUTUP	59
7.1 Kesimpulan	60
7.2 Temuan	60
7.3 Rekomendasi	62

# DAFTAR GAMBAR

Gambar 1.1	Jenis data pribadi	7
Gambar 1.2	Data pribadi sensitif	8

# DAFTAR TABEL

Tabel 1.1	Sebaran responden	10
-----------	-------------------	----

# DAFTAR GRAFIK

Grafik 1.1	Informasi yang dicantumkan di media sosial	4
Grafik 1.2	Profil responden berdasarkan usia	11
Grafik 1.3	Profil responden berdasarkan jenis kelamin	11
Grafik 1.4	Profil responden berdasarkan pendidikan terakhir	12
Grafik 1.5	Profil responden berdasarkan pekerjaan	12
Grafik 1.6	Profil responden berdasarkan SES	13
Grafik 2.1	Akses penggunaan media sosial	16
Grafik 2.2	Durasi penggunaan media sosial	16
Grafik 2.3	Akses media sosial berdasarkan usia	17
Grafik 2.4	Aktivitas media sosial	17
Grafik 2.5	Jumlah pertemanan di media sosial	18
Grafik 2.6	Memilih/menerima pertemanan di media sosial	18
Grafik 2.7	Pengaturan di Facebook	20
Grafik 2.8	Pengaturan di Instagram	21
Grafik 3.1	Pengetahuan tentang data pribadi	24
Grafik 3.2	Top 5 hal yang termasuk data pribadi berdasarkan usia	26
Grafik 3.3	Tingkat pengetahuan data pribadi berdasarkan demografi	28
Grafik 3.4	Tingkat pengetahuan data pribadi berdasarkan aplikasi	29
Grafik 3.5	Data pribadi yang pernah dibagikan ke publik	31
Grafik 3.6	Pengetahuan tentang kebijakan privasi	32
	• Grafik 3.6.1 Alasan tidak mengetahui kebijakan privasi	32

Grafik 4.1	Lembaga atau produk keuangan yang rentan kebocoran data	36
Grafik 4.2	Kebocoran data finansial/keuangan	37
	• Grafik 4.2.1 Akibat kebocoran data finansial	37
Grafik 4.3	Tingkat kesetujuan untuk menjual/membagi informasi data pribadi	38
Grafik 4.4	Tindakan ketika terjadi penyalahgunaan data di media sosial	38
Grafik 4.5	Lembaga pengumpul data pribadi	39
	• Grafik 4.5.1 Lembaga yang dipercaya memberikan perlindungan data pribadi	39
Grafik 5.1	Pemberian izin akses pada aplikasi komunikasi, lokapasar, dan transportasi daring	42
Grafik 5.2	Pemberian izin akses pada aplikasi keuangan/perbankan, kesehatan, dan pinjaman <i>online</i>	44
Grafik 5.3	Penginstalan aplikasi dengan memberikan izin akses	45
	• Grafik 5.3.1 Penginstalan aplikasi dengan memberikan izin akses berdasarkan kelompok usia	46
Grafik 5.4	Pengalaman dalam mendapatkan pesan SMS/WhatsApp	47
	• Grafik 5.4.1 Tingkat keyakinan terhadap pesan yang berupa penipuan	47
Grafik 5.5	Tindakan terhadap pengirim pesan berisi motif penipuan	48
Grafik 6.1	Pengetahuan tentang RUU Pelindungan Data Pribadi	52
Grafik 6.2	Pengetahuan tentang RUU Pelindungan Data Pribadi berdasarkan jenis kelamin, SES, dan pendidikan terakhir	53
Grafik 6.3	Pengetahuan tentang RUU Pelindungan Data Pribadi berdasarkan lokasi	54
Grafik 6.4	Pengetahuan tentang RUU Pelindungan Data Pribadi berdasarkan generasi	55
	• Grafik 6.4.1 Sumber informasi tentang RUU Pelindungan Data Pribadi berdasarkan generasi	55
Grafik 6.5	Penilaian terhadap sistem pelindungan data pribadi di Indonesia	56
Grafik 6.6	Pentingnya institusi mengatur penerapan UU Pelindungan Data Pribadi	57



# RINGKASAN EKSEKUTIF

**P**erkembangan teknologi informasi yang demikian pesat berdampak pada berbagai aktivitas masyarakat. Meningkatnya jumlah pengguna internet di Indonesia menjadi urgensi bagi keberadaan aturan perlindungan data pribadi di dunia digital. RUU Pelindungan Data Pribadi yang tengah digodok oleh pemerintah bersama DPR akan menjadi landasan hukum perlindungan data pribadi di Indonesia.

Kementerian Komunikasi dan Informatika bersama Katadata Insight Center menyusun *Laporan Persepsi Masyarakat atas Pelindungan Data Pribadi* guna menyajikan pemahaman masyarakat akan hak untuk melindungi data pribadi dan pengetahuan ihwal Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP). Laporan ini menganalisis data primer dari survei terhadap 11.305 responden di 34 provinsi pada 14 - 21 Juli 2021.

Melalui survei diketahui jika penyalahgunaan data pribadi terjadi di seluruh wilayah Indonesia. Responden yang melaporkan pernah mengalami kebocoran data pribadi berasal dari 34 provinsi di Indonesia, total berjumlah 3.246 orang. Kerugian yang mereka alami antara lain berkurangnya saldo di rekening bank dan *e-wallet*.

Survei ini menemukan mayoritas responden (94,1%) sebetulnya mengetahui tentang data pribadi. Nomor Induk Kependudukan (NIK) merupakan data pribadi umum yang paling banyak diketahui karena terintegrasi dengan berbagai urusan dokumen. Data pribadi khusus yang paling banyak diketahui adalah data keuangan/perbankan (68,7%) dan data biometri (60,8%). Mayoritas juga mengaku membaca, walau tidak sampai selesai, kebijakan privasi yang tersedia pada tiap aplikasi atau media sosial. Dengan alasan, narasi penjelasan terlalu panjang dan sulit dipahami isinya.

Pada sejumlah pertanyaan yang menguji kemampuan masyarakat dalam melindungi data pribadinya, riset ini menemukan masyarakat belum terlalu selektif dalam mengatur akses atas gawai dan aplikasi yang memungkinkan pencurian data.

Secara keseluruhan, responden umumnya tidak terlalu peduli dengan akses yang dibutuhkan oleh aplikasi agar dapat terinstal selama diperlukan. Akses dan pengaturan privasi pada media sosial pun masih belum banyak yang peduli. Sebanyak 55,5% pengguna Facebook dalam survei ini, misalnya, membuka profil secara publik. Sedangkan 25,5% pengguna Instagram sama sekali tidak mengubah pengaturan akun.

Pengguna pinjaman *online* yang tertangkap dalam survei pun masih ada yang memberikan akses untuk kontak pribadi dan sejumlah akses lain, di mana Otoritas Jasa Keuangan (OJK) telah memperingatkan akan rentan pencurian data. OJK menyebutkan jika data yang boleh diakses oleh perusahaan keuangan seperti *fintech* adalah *camera*, *microphone*, dan *location* (Camilan). Aplikasi yang mengakses data di luar Camilan patut diduga ilegal.

Masyarakat menilai sistem perlindungan data di Indonesia saat ini dianggap cukup baik namun belum memadai, dengan skor rata-rata 6,05 dari skala 10. Oleh sebab itu, Indonesia perlu meningkatkan sistem dan implementasi aturan perlindungan data pribadi.

Perbincangan di media mengenai kehadiran RUU Pelindungan Data Pribadi cukup mendapat perhatian masyarakat dengan hampir separuh responden (48,8%) mengetahui atau pernah membaca tentang RUU Pelindungan Data Pribadi. Mayoritas responden juga menganggap perlu ada lembaga yang mengatur dan mengawasi penerapan Undang-Undang Pelindungan Data Pribadi. Hal ini diperlukan agar masyarakat mengetahui apa yang harus dilakukan dan ke mana melapor ketika mengalami permasalahan terkait data pribadi.

Sosialisasi serta upaya edukasi mengenai perlindungan data pribadi dapat merujuk pada sejumlah temuan survei ini, seperti penekanan pada pentingnya pengaturan privasi data dan kontrol akses, baik saat mengunduh aplikasi maupun bermedia sosial. Menurut survei ini, komunikasi melalui media sosial dan media daring tampaknya masih menjadi sarana paling efektif dalam menjangkau publik karena banyak dijadikan rujukan informasi tentang perlindungan data pribadi.





# BAB 1

# PENDAHULUAN



Pada 2019, Asosiasi Pengguna Jasa Internet Indonesia (APJII) mencatat 196,71 juta orang di Indonesia telah mengakses internet. Angka tersebut mencakup 73,7% dari total 270 juta penduduk Indonesia. Jawa merupakan pulau dengan pengguna terbanyak, mencapai 55,7% populasi pengguna internet di Indonesia. Penggunaan teknologi membuat masyarakat lebih mudah dalam berbagai aktivitas, mulai dari berkomunikasi, transportasi hingga bertransaksi secara digital.

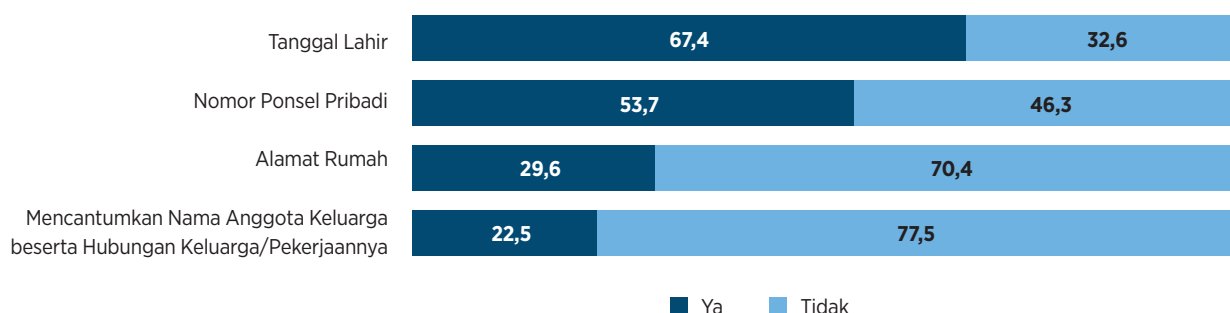
Pemanfaatan teknologi internet berimplikasi pada rentannya data pribadi pengguna. Setiap pengguna seharusnya dapat menentukan apakah datanya dapat digunakan dan disebarluaskan oleh pengelola media sosial atau aplikasi. Ia juga berhak menentukan persyaratan yang berlaku dalam satu komunitas terkait penggunaan data.

Data pribadi mengenai nama lengkap, *e-mail*, akun media sosial bahkan nomor rekening diperlukan oleh berbagai layanan aplikasi, salah satunya untuk memastikan keabsahan pengguna dan ketepatan pelayanan. Namun, tidak ada jaminan bahwa data pribadi tersebut terhindar dari penyalahgunaan. Nomor kontak, rekening bank, dan alamat rumah dapat digunakan oleh pihak yang berniat jahat, misalnya untuk melakukan penipuan melalui telepon genggam, meretas rekening bank, dan merampok rumah.

Riset Status Literasi Digital Indonesia 2020 oleh Katadata Insight Center (KIC), mengungkapkan bahwa pemahaman publik ihwal pentingnya kerahasiaan data pribadi belum tinggi. Sebanyak 67,4% pengguna internet di Indonesia membagikan tanggal lahirnya, dan 53,7% menuliskan nomor teleponnya di media sosial.

**Grafik 1.1 Informasi yang dicantumkan di media sosial (%)**

"Apakah di akun media sosial anda tercantum informasi berikut?" [SA]  
Basis: seluruh responden



SUMBER: KATADATA INSIGHT CENTER

Pelindungan privasi dan data pribadi merupakan faktor yang menentukan tingkat kepercayaan daring (*online trust*). Minimnya pelindungan menyebabkan data privasi tersebar ke pihak yang tidak bertanggung jawab, sehingga dapat merugikan secara finansial, bahkan mengancam keselamatan pemiliknya.

Indonesia memiliki sejumlah peraturan mengenai pelindungan data pribadi, tetapi tersebar di beberapa undang-undang. Oleh sebab itu, pemerintah dan Dewan Perwakilan Rakyat tengah menyiapkan Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP).

Survei Persepsi Publik atas Pelindungan Data Pribadi bertujuan memetakan persepsi masyarakat terhadap hak atas pelindungan data pribadi di 34 provinsi Indonesia. Pengumpulan data primer ini diharapkan dapat menggambarkan pemahaman masyarakat akan data pribadi, penyalahgunaannya, kesadaran akan hak untuk melindungi data pribadi dan Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP).

**Tujuan dan sasaran survei ini adalah untuk mengetahui:**

1. Status kesadaran masyarakat terhadap hak atas pelindungan data pribadi.
2. Tingkat pemahaman masyarakat akan data pribadi, penyalahgunaannya, dan kesadaran akan hak untuk melindungi data pribadi mereka.
3. Pengetahuan tentang RUU Pelindungan Data Pribadi dan data pribadi yang perlu dilindungi.
4. Perilaku dan kebiasaan (*habit*) publik di internet atas pelindungan data pribadi.
5. Persepsi publik atas pemahaman tentang kerahasiaan data pribadi.





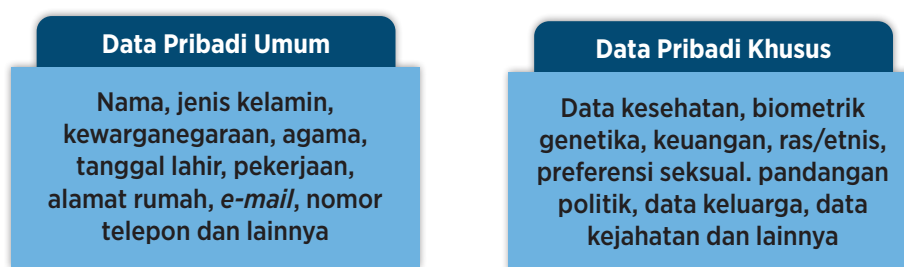
## METODOLOGI

### 1.1 Kerangka Penelitian

**P**okok kajian dalam penelitian ini adalah membahas dan menganalisis konsep perlindungan privasi atas data pribadi sebagai salah satu hak konstitusional warga negara serta pengaturan privasi data pribadi dalam bermedia sosial. Survei ini menguraikan konsep perlindungan privasi atas data pribadi dan perlindungan privasi data pribadi dalam perspektif persepsi masyarakat terkini, sejauh mana pengetahuan dan pemahaman data pribadi diukur melalui *self-assesment*. Responden juga diminta mengisi beberapa pertanyaan untuk meng-*cross check* keamanan data pribadi, pengalaman penyalahgunaan data pribadi, pengetahuan terhadap Rancangan Undang-Undang Pelindungan Data Pribadi (RUU PDP) serta berbagai kebiasaan dalam bermedia sosial.

Di Indonesia, RUU PDP mendefinisikan data pribadi sebagai setiap data tentang seseorang yang teridentifikasi dan atau dapat diidentifikasi secara tersendiri atau dikombinasikan dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik dan/atau non-elektronik (Monggilo, Kurnia & Banyumurti, 2020). Secara umum, terdapat dua jenis data pribadi yakni:

**Gambar 1.1 Jenis data pribadi**



SUMBER: MODUL AMAN BERMEDIA DIGITAL, HAL 58 – 59  
KOMINFO, JAPELIDI, SIBERKREASI

Selain itu, data pribadi sensitif berkaitan dengan kategori data tertentu yang didefinisikan sebagai data yang berkaitan dengan asal ras seseorang; pendapat politik atau agama atau kepercayaan lainnya; kesehatan fisik atau mental; kehidupan seksual; hukuman pidana atau dugaan dilakukannya suatu pelanggaran; keanggotaan serikat pekerja (Data Protection Act – UK, 1988).

Gambar 1.2 Data pribadi sensitif



SUMBER: DATA PROTECTION ACT - UK, 1988

## 1.2 Pengumpulan Data

Survei Persepsi Publik atas Pelindungan Data Pribadi dilakukan dengan survei *online/Computer Aided Web Interviewing (CAWI)*. Mereka yang mengisi adalah penduduk Indonesia pengguna internet berusia 17 tahun ke atas.

Walaupun dengan *non-probability sampling*, penyebaran responden pada tiap provinsi diupayakan mengikuti proporsi jumlah penduduk Indonesia yang dikeluarkan BPS berdasarkan sensus penduduk 2020.

Pertanyaan dalam kuesioner meliputi:

1. Penggunaan media sosial
2. Pengetahuan tentang data pribadi
3. Penyalahgunaan data pribadi
4. Pengetahuan keamanan data pribadi
5. RUU Pelindungan Data Pribadi

### 1.3 Pengolahan dan Analisis Data

Sebelum melakukan analisis data, dilakukan pengolahan data terlebih dahulu. Tahap pengolahan data dalam penelitian ini meliputi *editing*, *coding*, dan tabulasi.

#### 1. Editing

*Editing* atau pemeriksaan adalah pengecekan atau penelitian kembali data yang telah dikumpulkan untuk mengetahui dan menilai kesesuaian dan relevansi data yang dikumpulkan untuk bisa diproses lebih lanjut. Hal yang perlu diperhatikan dalam *editing* ini adalah kelengkapan pengisian jawaban, kesesuaian jawaban, dan relevansi jawaban.

#### 2. Coding

*Coding* atau pemberian kode adalah pengklasifikasian jawaban yang diberikan responden sesuai dengan macamnya. Dalam tahap *coding* biasanya dilakukan pemberian skor dan simbol pada jawaban responden agar nantinya bisa lebih mempermudah dalam pengolahan data.

#### 3. Tabulasi

Tabulasi merupakan langkah lanjutan setelah pemeriksaan dan pemberian kode. Dalam tahap ini data disusun dalam bentuk tabel agar lebih mempermudah dalam menganalisis data sesuai dengan tujuan penelitian. Tabel yang digunakan dalam penelitian ini adalah tabel frekuensi yang dinyatakan dalam persen.

Analisis data yang digunakan dalam penelitian ini adalah deskriptif kuantitatif. Analisis kuantitatif yang dimaksud di sini merupakan penyajian hasil pengolahan data dalam bentuk angka. Data yang sudah berupa tabel frekuensi kemudian dianalisis secara deskriptif yaitu dengan memaparkannya dalam bentuk naratif yang representatif dengan data hasil olahan agar lebih mudah dipahami.

Untuk memperkuat analisis data yang didapat, dilakukan *Focus Group Discussion (FGD)*. Narasumber yang terlibat perwakilan dari berbagai instansi pemerintah, swasta, LSM dan akademisi.

### 1.4 Keterbatasan Penelitian

Penyebaran kuesioner daring tidak 100% akurat, tetapi setidaknya dapat menggambarkan persepsi perlindungan data pribadi yang ada di masyarakat.

## 1.5 Profil Responden Survei

Survei Persepsi Publik atas Pelindungan Data Pribadi dilakukan di 34 provinsi kepada 11.305 responden.

**Tabel 1.1 Sebaran responden**

NO	PROVINSI	JUMLAH	%	DATA BPS
1	Aceh	148	1,3%	2,0%
2	Sumatera Utara	479	4,2%	5,5%
3	Sumatera Barat	166	1,5%	2,0%
4	Riau	210	1,9%	2,4%
5	Jambi	144	1,3%	1,3%
6	Sumatera Selatan	289	2,6%	3,1%
7	Bengkulu	71	0,6%	0,7%
8	Lampung	292	2,6%	3,3%
9	Kep. Bangka Belitung	38	0,3%	0,5%
10	Kep. Riau	89	0,8%	0,8%
11	DKI Jakarta	803	7,1%	3,9%
12	Jawa Barat	2.448	21,7%	17,9%
13	Jawa Tengah	1.495	13,2%	13,5%
14	DI Yogyakarta	305	2,7%	1,4%
15	Jawa Timur	1.650	14,6%	15,1%
16	Banten	543	4,8%	4,4%
	Wilayah Barat	9.170	81,1%	77,8%
NO	PROVINSI	JUMLAH	%	DATA BPS
17	Bali	202	1,8%	1,6%
18	Nusa Tenggara Barat	202	1,8%	2,0%
19	Nusa Tenggara Timur	160	1,4%	2,0%
20	Kalimantan Barat	183	1,6%	2,0%
21	Kalimantan Tengah	112	1,0%	1,0%
22	Kalimantan Selatan	205	1,8%	1,5%
23	Kalimantan Timur	211	1,9%	1,4%
24	Kalimantan Utara	34	0,3%	0,3%
25	Sulawesi Utara	102	0,9%	1,0%
26	Sulawesi Tengah	90	0,8%	1,1%

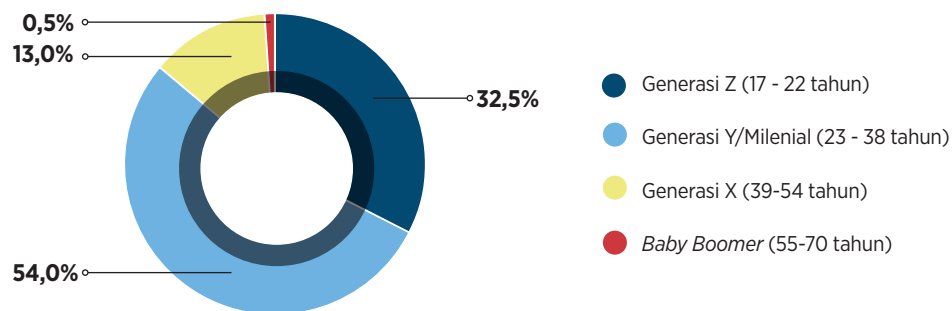


NO	PROVINSI	JUMLAH	%	DATA BPS
27	Sulawesi Selatan	286	2,5%	3,4%
28	Sulawesi Tenggara	72	0,6%	1,0%
29	Gorontalo	48	0,4%	0,4%
30	Sulawesi Barat	39	0,3%	0,5%
	Wilayah Tengah	1.946	17,2%	19,0%

NO	PROVINSI	JUMLAH	%	DATA BPS
31	Maluku	55	0,5%	0,7%
32	Maluku Utara	44	0,4%	0,5%
33	Papua Barat	37	0,3%	0,4%
34	Papua	53	0,5%	1,6%
	Wilayah Timur	189	1,7%	3,2%

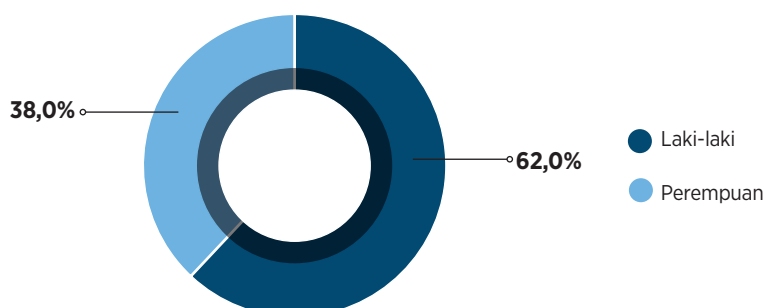
Responden survei berasal dari kelompok usia yang beragam. Sebagian besar (86,5%) berada di rentang 17 hingga 38 tahun, yang 54,0% di antaranya berasal dari generasi milenial dan 32,5% generasi Z.

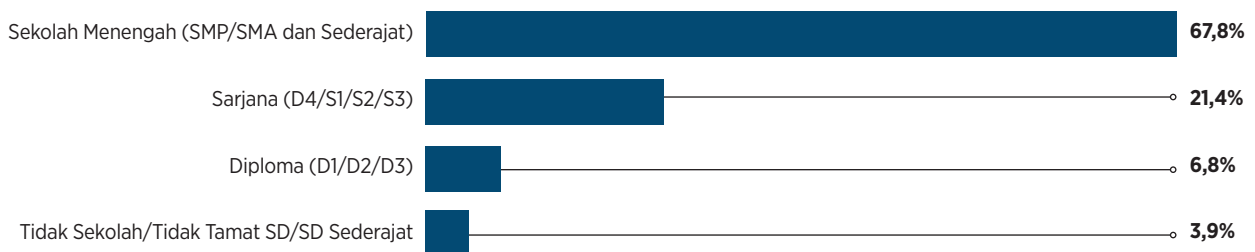
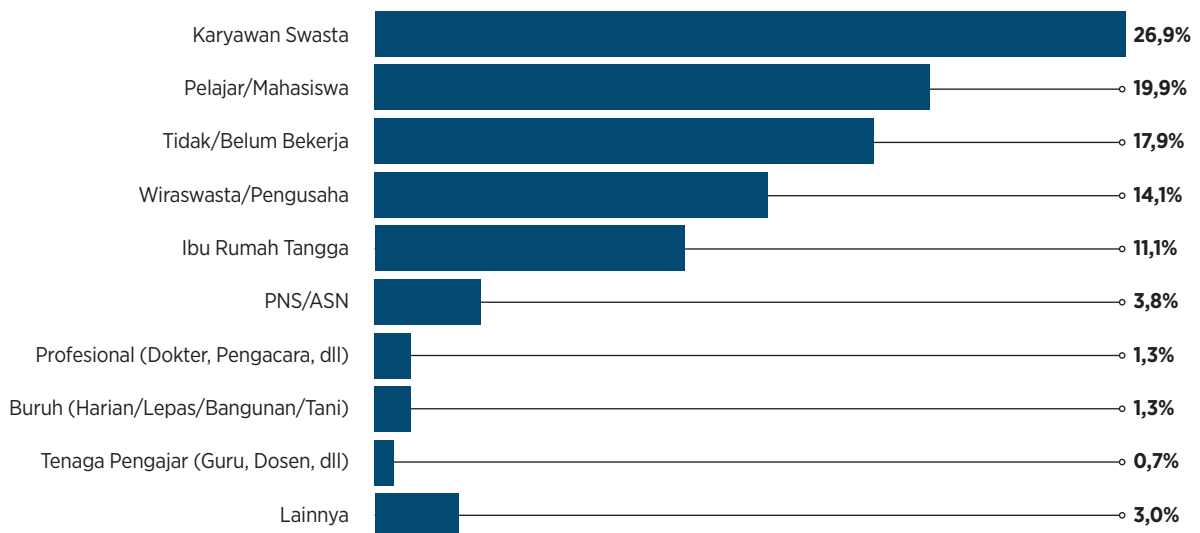
**Grafik 1.2 Profil responden berdasarkan usia**



Dari jenis kelamin, proporsi responden laki-laki lebih besar, seperti terlihat di grafik di bawah ini. SMA merupakan pendidikan terakhir yang ditempuh oleh 67,8% responden. Adapun 26,9% adalah karyawan swasta.

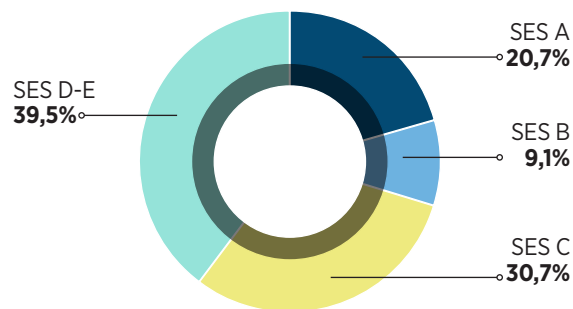
**Grafik 1.3 Profil responden berdasarkan jenis kelamin**



**Grafik 1.4 Profil responden berdasarkan pendidikan terakhir****Grafik 1.5 Profil responden berdasarkan pekerjaan**

SES (*Socioeconomic Status*) adalah klasifikasi yang memetakan seseorang atau keluarga berdasarkan kemampuan ekonomi dan status sosialnya. Pada umumnya SES dihitung berdasarkan pendapatan. Namun, di Indonesia, besar pengeluaran rutin bulanan menjadi tolak ukur yang lebih akurat. Hal ini disebabkan keengganan kebanyakan orang di Indonesia untuk menyebutkan penghasilan. Sebanyak 29,8% responden memiliki status ekonomi sosial AB atau berpengeluaran di atas Rp 4 juta per bulan, sedangkan 30,7% memiliki status ekonomi sosial C (di atas Rp 2 juta-4 juta).

**Grafik 1.6 Profil responden berdasarkan SES**







# **BAB 2**

# **PENGGUNAAN**

# **MEDIA SOSIAL**

# **DI INDONESIA**

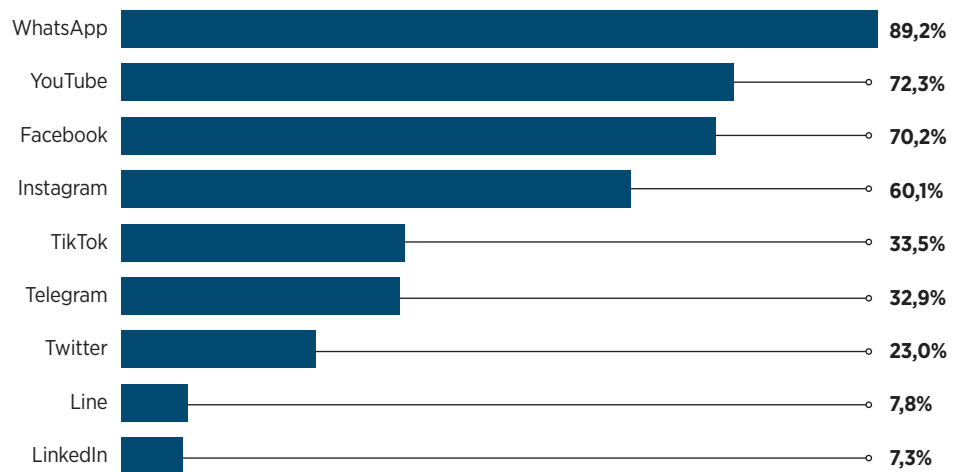


## 2.1 Akses dan Durasi Penggunaan Media Sosial

**A**plikasi media sosial yang digunakan di Indonesia cukup beragam. Berdasarkan survei, yang paling banyak digunakan dalam satu bulan terakhir adalah WhatsApp (89,2%), YouTube (72,3%), dan Facebook (70,2%).

**Grafik 2.1 Akses penggunaan media sosial**

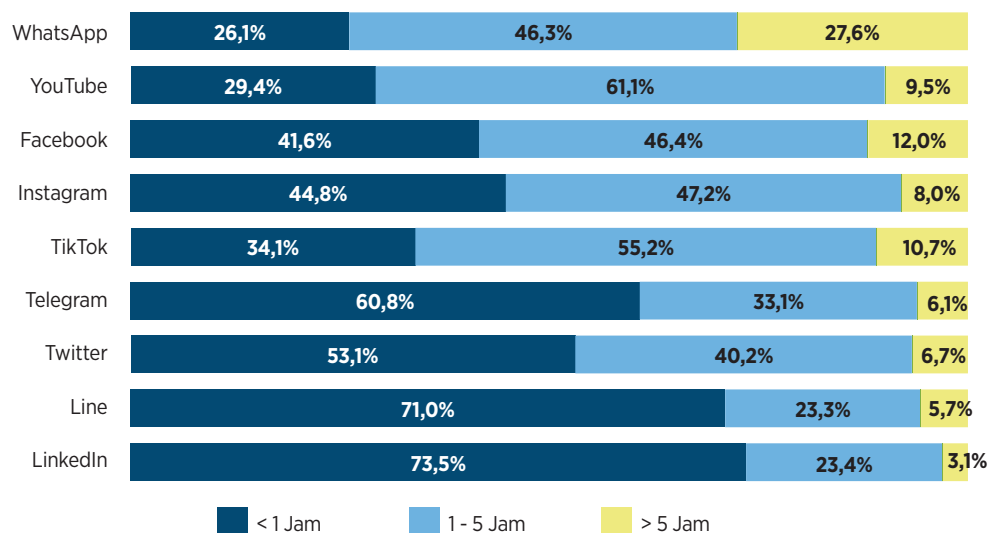
"Media sosial apa saja yang anda akses/gunakan dalam 1 bulan terakhir?" [MA]  
 Basis: seluruh responden



Sebanyak 89,2% pengguna WhatsApp menggunakan aplikasi tersebut lebih dari satu jam setiap hari, bahkan 27,6% responden menggunakannya lebih dari lima jam setiap hari. Selain itu, lebih dari 65% pengguna YouTube dan TikTok juga menggunakan aplikasi ini lebih dari satu jam setiap hari. Sementara itu, LinkedIn dan Line merupakan aplikasi yang digunakan kurang dari satu jam oleh sebagian besar penggunanya.

**Grafik 2.2 Durasi penggunaan media sosial**

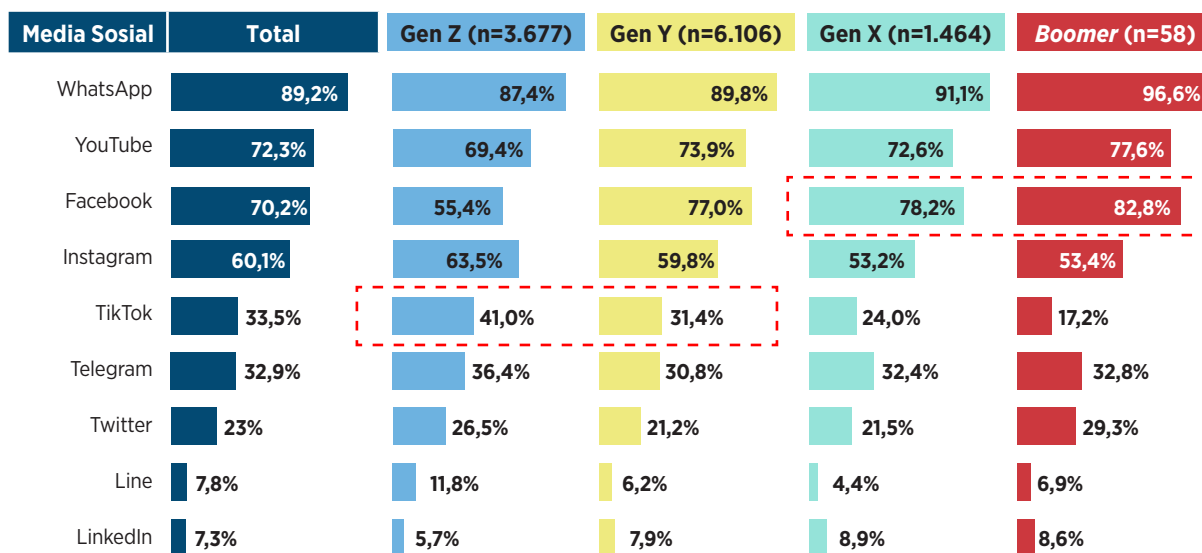
"Dalam sehari berapa lama anda membuka media sosial tersebut?" [SA]  
 Basis: seluruh responden



Jika melihat penggunaan media sosial berdasarkan usia, Facebook paling banyak digunakan oleh kelompok dewasa. Gen X dan *boomer* yang menggunakan Facebook berturut-turut sebesar 78,2% dan 82,8%. Sedangkan mayoritas pengguna TikTok berasal dari kelompok usia yang paling muda yaitu Gen Z (41,0%) dan Gen Y (31,4%).

**Grafik 2.3 Akses media sosial berdasarkan usia**

"Media sosial apa saja yang anda akses/gunakan dalam 1 bulan terakhir?" [MA]  
 Basis: seluruh responden

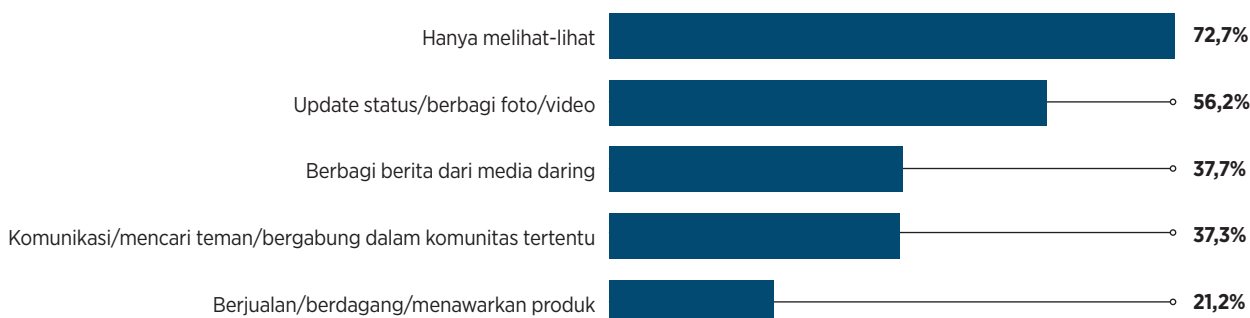


## 2.2 Aktivitas di Media Sosial

Aktivitas yang paling sering dilakukan responden ketika membuka media sosial adalah melihat-lihat saja (72,7%). Sementara itu, 56,2% melakukan berbagai aktivitas seperti update status dan atau berbagi foto dan video. Hanya 21,2% responden yang menggunakan media sosial untuk berjalan.

**Grafik 2.4 Aktivitas media sosial**

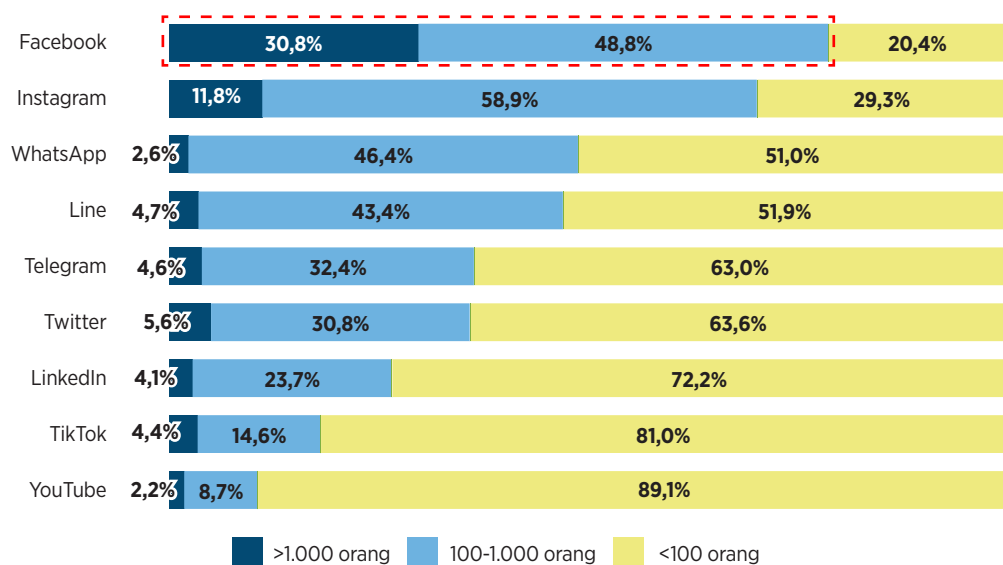
"Apa saja aktivitas yang anda lakukan di media sosial tersebut dalam 1 bulan terakhir?" [MA]  
 Basis: seluruh responden



Berdasarkan grafik di atas, 37,3% aktivitas media sosial digunakan untuk mencari teman. Facebook, Instagram, YouTube, TikTok, Twitter, dan LinkedIn memiliki jaringan pertemanan yang luas dan tidak terbatas. Semakin besar lingkaran pertemanan yang dibuat, maka semakin beragam orang yang terhubung dan mendapat informasi dari konten yang dibagikan. Sedangkan WhatsApp, Line, dan Telegram lebih selektif dalam menerima pertemanan. Hal tersebut disebabkan karena aplikasi ini harus dikaitkan dengan nomor ponsel terlebih dahulu.

**Grafik 2.5 Jumlah pertemanan di media sosial**

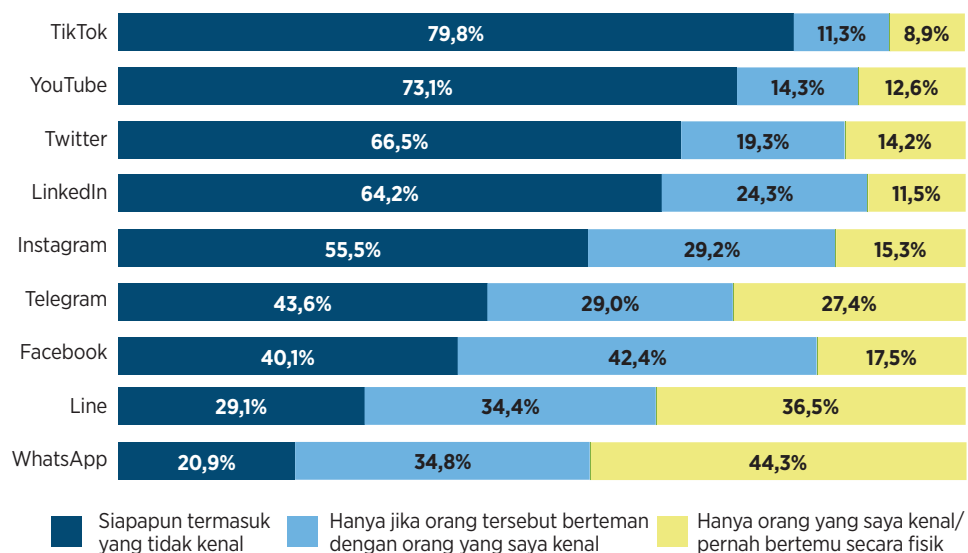
"Berapa banyak teman/followers/subscriber yang anda miliki di media sosial anda?" [SA]  
 Basis: seluruh responden



Dari cara menerima pertemanan di media sosial, TikTok dan YouTube merupakan media sosial yang paling bebas. Sebesar 79,8% dan 73,1% pengguna kedua media itu menerima pertemanan dari siapapun, termasuk yang tidak dikenal.

**Grafik 2.6 Memilih/menerima pertemanan di media sosial**

"Bagaimana anda memilih/menerima pertemanan di media sosial anda?" [SA]  
 Basis: seluruh responden



# Social Media



Twitter



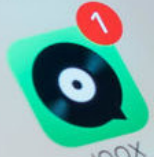
LinkedIn



WhatsApp



YouTube



JOOX



Google



Instagram



Facebook



LINE

## 2.3 Pengaturan Media Sosial

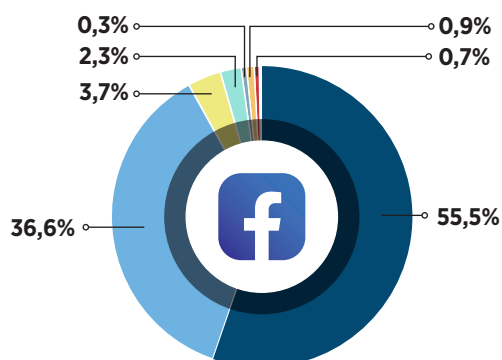
Ketika menggunakan media sosial, pengguna dapat melakukan pengaturan terhadap informasi yang diunggah di profil mereka. Hal ini menjadi penting karena terkait dengan privasi pengguna. Selain itu, profil media sosial biasanya terkait dengan data pribadi seperti *e-mail*, nomor telepon dan identitas lainnya.

Berdasarkan hasil survei, 55,5% pengguna Facebook membuka profilnya secara publik. Hanya 8% pengguna Facebook melakukan pengaturan ekstra sehingga tidak semua teman di Facebook mereka dapat melihat informasi yang dibagikan.

**Grafik 2.7 Pengaturan di Facebook**

**"Bagaimana pengaturan orang yang bisa melihat postingan Facebook yang sering anda gunakan?" [SA]**

Basis: responden pengakses Facebook dalam 1 bulan terakhir



- Publik (Semua orang di dalam atau luar Facebook)
- Teman (Teman anda di Facebook)
- Teman tertentu (Teman anda di Facebook kecuali yang tidak anda inginkan untuk melihat)
- Hanya saya (Tidak dibagikan untuk teman dan publik)
- Teman spesifik (Hanya tampilkan ke beberapa teman saja)
- Khusus (Teman yang sudah anda *list* berdasarkan komunitas/kelompok tertentu)
- Teman dekat

Sedangkan di Instagram, 35,7 % responden mengatur akun menjadi akun privat, 34,3% responden menghubungkan akunnya ke Facebook, dan 23,3% responden memblokir pengguna yang membuat tidak nyaman. Namun, masih ada 25,5% responden tidak melakukan perubahan pengaturan sama sekali.



**Grafik 2.8 Pengaturan di Instagram**

"Bagaimana pengaturan anda di Instagram?" [MA]  
 Basis: responden pengakses Instagram dalam 1 bulan terakhir



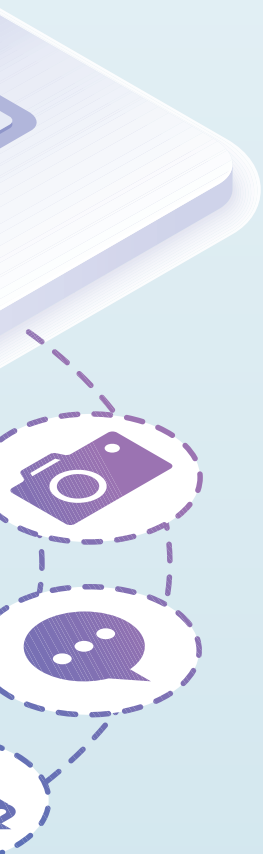
Semua akun media sosial memiliki pengaturan privasi yang dapat digunakan untuk mengatur dan menghubungkan akun media sosial satu dengan lainnya. Akun media sosial yang sudah dikunci dapat mencegah dari penyalahgunaan data pribadi yang tersimpan di media sosial.





# **BAB 3**

## **PENGETAHUAN TENTANG DATA PRIBADI**

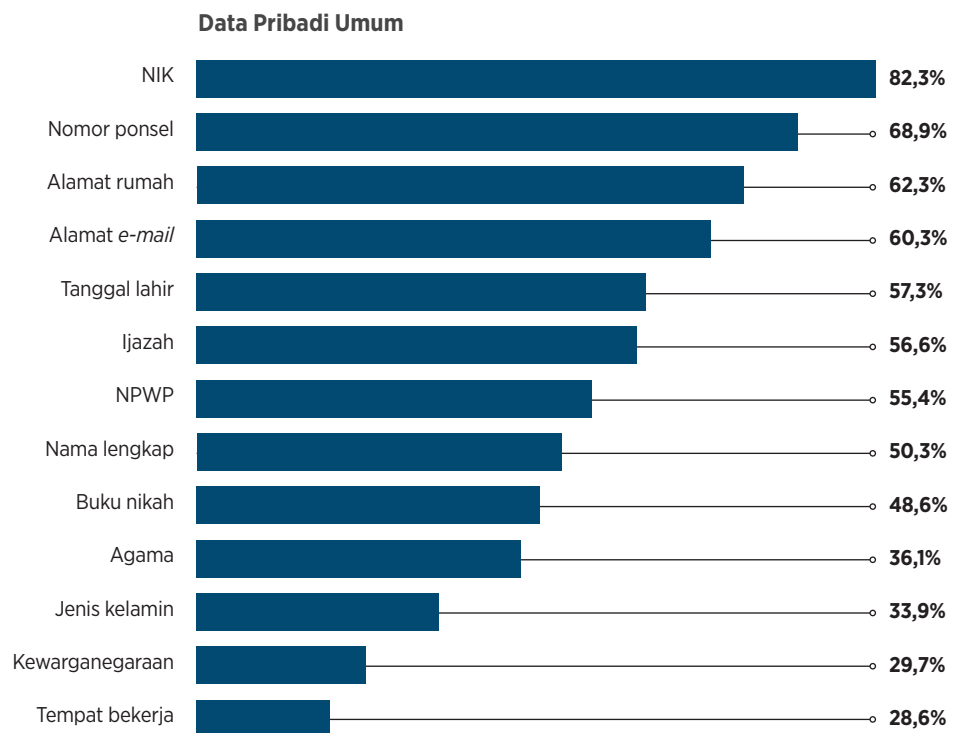


**K**etika menginstal aplikasi media sosial atau berhubungan dengan lembaga/ produk keuangan, masyarakat harus mengisi data-data pribadi yang dibutuhkan ketika pendaftaran. Berdasarkan hasil survei, mayoritas masyarakat sudah mengetahui apa yang dimaksud dengan data pribadi (94,1%).

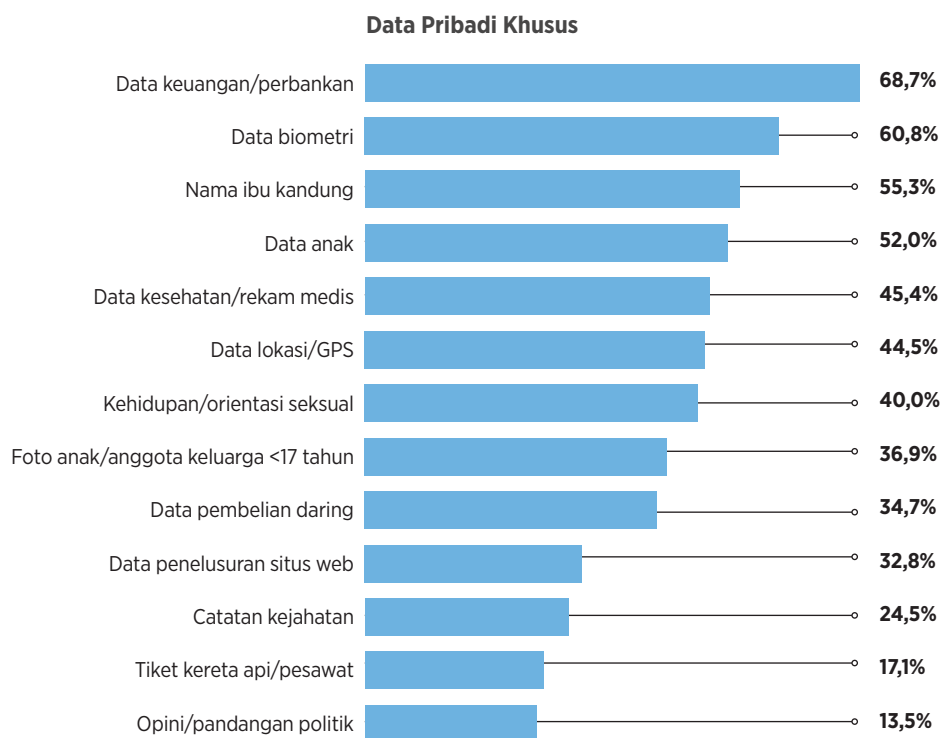
Saat melakukan analisa data, pengetahuan masyarakat terhadap data pribadi tersebut kemudian dikelompokkan menjadi dua, data pribadi umum dan data pribadi khusus. Pada data pribadi umum, sebagian besar responden menilai Nomor Induk Kependudukan (NIK) merupakan data pribadi karena terintegrasi dengan berbagai dokumen lainnya yang dibutuhkan setiap orang. Selanjutnya yang dianggap oleh sebagian besar responden sebagai data pribadi adalah yang berkaitan dengan kontak.

**Grafik 3.1 Pengetahuan tentang data pribadi**

**"Menurut anda manakah dari hal berikut yang termasuk data pribadi?" [MA]**  
Basis: responden yang mengetahui data pribadi



Sementara itu, data pribadi khusus yang paling banyak diketahui adalah data keuangan/perbankan (68,7%). Selain itu, hampir setengah responden juga tahu bahwa data kesehatan/rekam medis merupakan data pribadi khusus. Namun, hanya 13,5% yang mengetahui jika opini/pandangan politik termasuk data pribadi khusus.



Seiring matangnya usia, masyarakat semakin peduli terkait data pribadi yang dimiliki baik itu data pribadi umum maupun data pribadi khusus. Hal tersebut terlihat dari tingkat pengetahuan terhadap data pribadi berdasarkan kelompok umur. Generasi *boomer* memiliki tingkat pengetahuan paling tinggi terhadap data pribadi sebesar 96,6%. Sedangkan Gen Z merupakan kelompok dengan persentase terendah yaitu 91,1%.

Dari seluruh kelompok usia, hampir seluruhnya memiliki pengetahuan yang sama mengenai data yang termasuk data pribadi umum. NIK dan nomor ponsel menjadi data yang paling diketahui sebagai data pribadi umum. Namun, generasi *boomer* punya tingkat pengetahuan tertinggi terhadap NIK dibandingkan kelompok usia lainnya (91,1%).

Hal serupa juga terlihat pada pengetahuan terhadap data pribadi khusus. Semua kelompok usia sama-sama menjadikan data keuangan/perbankan sebagai data yang paling diketahui sebagai data pribadi khusus. Di sisi lain, Gen Z dan Gen Y menjadikan data biometri (sidik jari, tinggi badan, berat badan, dan lain-lain) sebagai data kedua paling banyak diketahui yang termasuk data pribadi khusus.



**Grafik 3.2 Top 5 hal yang termasuk data pribadi berdasarkan usia**

"Menurut anda manakah dari hal berikut yang termasuk data pribadi?" [MA]  
Basis: responden yang mengetahui data pribadi

DATA PRIBADI UMUM (TOP 5)	GEN Z (n=3.349)	DATA PRIBADI KHUSUS (TOP 5)	GEN Z (n=3.349)
NIK	77,2%	Data keuangan/perbankan	64,9%
Nomor ponsel	67,8%	Data biometri	61,7%
Alamat rumah	62,6%	Data anak	50,3%
Alamat <i>e-mail</i>	58,0%	Nama ibu kandung	47,2%
Tanggal lahir	54,1%	Data lokasi /GPS	45,9%

DATA PRIBADI UMUM (TOP 5)	GEN Y (n=5.837)	DATA PRIBADI KHUSUS (TOP 5)	GEN Y (n=5.837)
NIK	83,6%	Data keuangan/perbankan	69,5%
Nomor ponsel	68,8%	Data biometri	60,3%
Alamat rumah	61,6%	Nama ibu kandung	56,8%
Alamat <i>e-mail</i>	60,6%	Data anak	52,5%
Ijazah	58,3%	Data kesehatan/rekam medis	46,2%

DATA PRIBADI UMUM (TOP 5)	GEN X (n=1.396)	DATA PRIBADI KHUSUS (TOP 5)	GEN X (n=1.396)
NIK	86,9%	Data keuangan/perbankan	73,1%
Nomor ponsel	72,1%	Nama ibu kandung	67,9%
Alamat <i>e-mail</i>	64,6%	Data biometri	59,7%
Alamat rumah	64,0%	Data anak	53,8%
Tanggal lahir	63,9%	Data kesehatan/rekam medis	47,9%

DATA PRIBADI UMUM (TOP 5)	BOOMER (n=56)	DATA PRIBADI KHUSUS (TOP 5)	BOOMER (n=56)
NIK	91,1%	Data keuangan/perbankan	75,0%
Nomor ponsel	60,7%	Nama ibu kandung	76,8%
Alamat <i>e-mail</i>	53,6%	Data biometri	76,8%
Alamat rumah	67,9%	Data anak	51,8%
Tanggal lahir	67,9%	Data kesehatan/rekam medis	53,6%

Jika dipetakan berdasarkan tingkat pengetahuan, dari total 8.730 responden yang mengetahui NIK merupakan data pribadi, tertinggi berasal dari Jawa Barat dengan 1.894 (21,7%) responden mengetahui NIK merupakan data pribadi. Sedangkan Kalimantan Utara yang terendah dengan sejumlah 26 dari total 34 responden.

Hal yang sama juga terjadi pada tingkat pengetahuan data perbankan sebagai data pribadi dengan Kalimantan Utara juga menempati posisi terendah dengan 22 dari 34 total responden. Sedangkan Jawa Barat memiliki tingkat pengetahuan tertinggi dengan 1.520 dari total 2.448 responden.

### 3.1 Tingkat Pengetahuan Data Pribadi

Survei juga melakukan pengukuran pengetahuan data pribadi baik data pribadi umum maupun data pribadi khusus. Pengukuran tersebut dihitung dari jumlah jawaban responden dari masing-masing kategori data pribadi umum dan data pribadi khusus. Berdasarkan pengukuran, secara umum dapat terlihat tingkat pengetahuan data pribadi umum lebih tinggi daripada data pribadi khusus.

Tingkat pengetahuan data pribadi umum mencatatkan skor rata-rata 6,70, sedangkan skor rata-rata tingkat pengetahuan data pribadi khusus lebih rendah dengan angka 5,26.

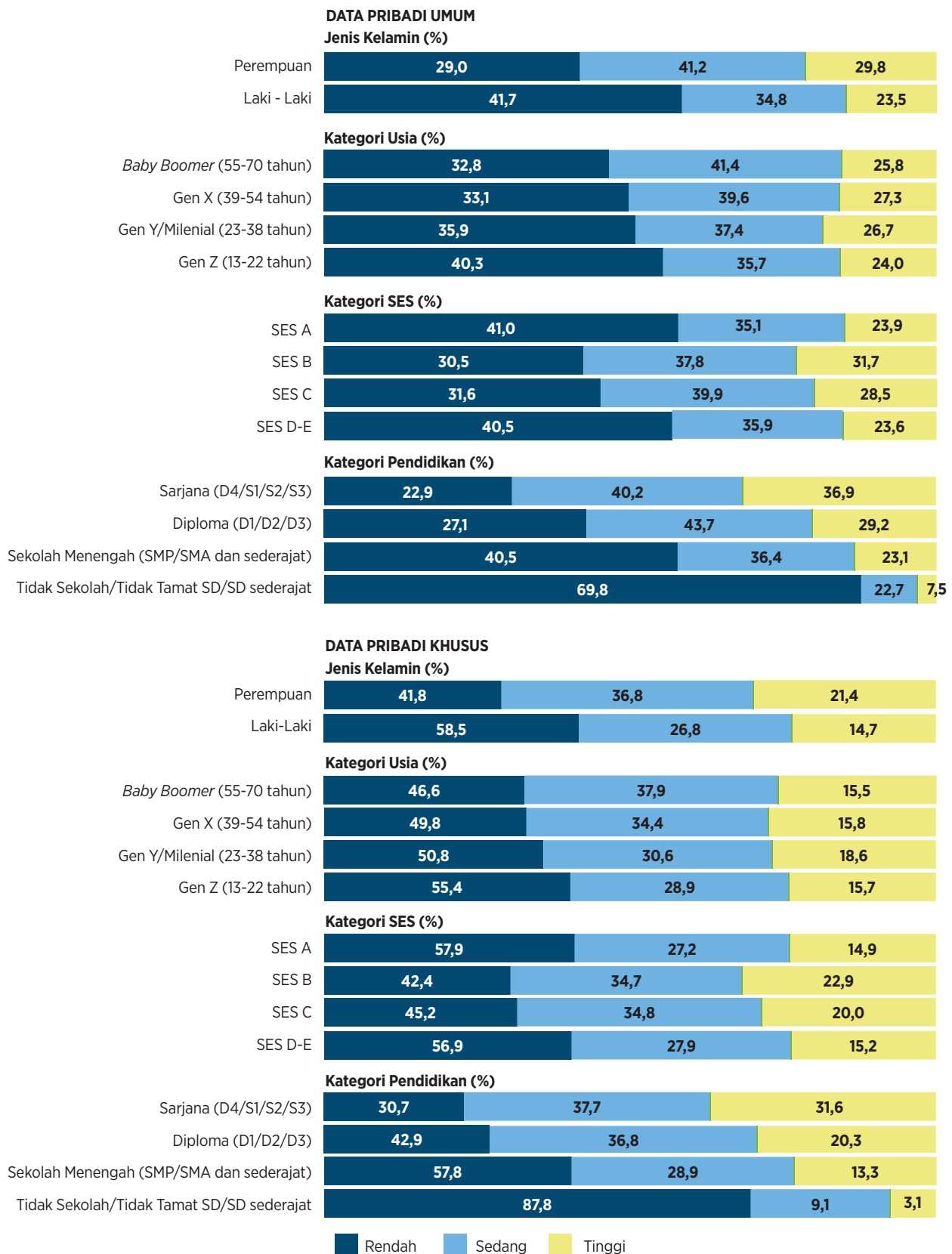
Berdasarkan demografi, perempuan memiliki tingkat pengetahuan terhadap data pribadi umum lebih tinggi (29,8%) dibandingkan laki-laki. Berdasarkan kelompok usia, Gen X memiliki tingkat pengetahuan yang tertinggi (27,3%) dibandingkan kelompok usia lainnya.

Berdasarkan kelompok pengeluaran (SES), responden yang memiliki tingkat pengetahuan paling tinggi terhadap data pribadi umum berasal dari kelompok SES B (31,7%). Sedangkan pada tingkat pendidikan, responden yang tidak sekolah/tidak tamat SD/SD sederajat merupakan kelompok yang memiliki tingkat pengetahuan yang paling rendah terhadap data pribadi umum (69,8%).

Terkait data pribadi khusus, laki-laki memiliki pengetahuan yang lebih rendah (58,5%). Lalu pada kelompok usia, Gen Z memiliki tingkat pengetahuan yang terendah (55,4%) dibandingkan kelompok usia lainnya.

Berdasarkan kelompok pengeluaran (SES), responden dengan pengetahuan yang paling rendah berasal dari kelompok SES A (57,9%), disusul kelompok SES D dan E dengan 56,9%. Sedangkan jika ditilik dari tingkat pendidikan, mayoritas responden yang tidak sekolah/tidak tamat SD/SD sederajat memiliki tingkat pengetahuan yang paling rendah terhadap data pribadi khusus (87,8%).

Grafik 3.3 Tingkat pengetahuan data pribadi berdasarkan demografi

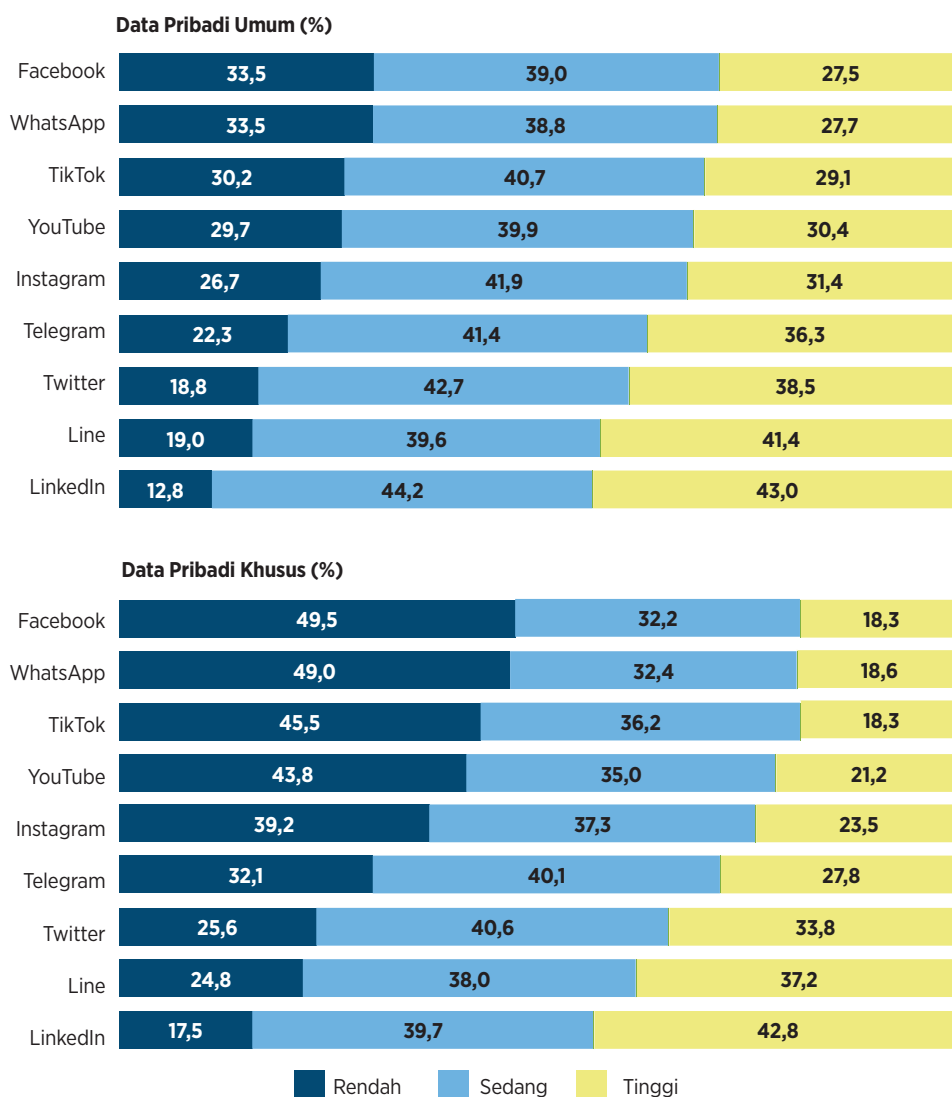


Jika dikelompokkan menurut provinsi, rata-rata provinsi di Indonesia memiliki tingkat pengetahuan sedang terhadap data pribadi umum yaitu 4.201 dari total responden 11.305 (37,2%). Namun, beberapa provinsi memiliki tingkat pengetahuan yang tinggi, seperti Kalimantan Timur (73 dari 211 responden), Nusa Tenggara Timur (62 dari 160), dan Sulawesi Utara (38 dari 102).

Pada data pribadi khusus, rata-rata provinsi memiliki pengetahuan yang rendah yaitu 5.899 dari total responden 11.305 (52,2%). Sulawesi Utara menjadi satu-satunya provinsi dengan tingkat pengetahuan sedang dengan 39 dari 102 responden.

Jika dibandingkan berdasarkan aplikasi yang digunakan, tingkat pengetahuan data pribadi baik umum maupun khusus yang paling rendah terdapat pada pengguna Facebook, WhatsApp dan TikTok. Sementara itu pengguna LinkedIn yang memiliki pengguna dengan pengetahuan data pribadi yang tinggi.

**Grafik 3.4 Tingkat pengetahuan data pribadi berdasarkan aplikasi**



### 3.2 Prioritas Data Pribadi

Jika diminta untuk mengurutkan 3 data pribadi yang menjadi prioritas untuk dijaga keamanannya, responden memilih Nomor Induk Kependudukan (NIK) sebagai prioritas pertama pada data pribadi umum. NIK dianggap sebagai data yang paling penting dan paling khawatir untuk disalahgunakan karena data NIK terintegrasi dengan banyak hal. Kemudian disusul nomor ponsel dan alamat rumah.

Pada data pribadi khusus, data keuangan/perbankan menjadi prioritas utama karena dapat merugikan responden secara finansial. Kemudian disusul data biometri dan nama ibu kandung.

Sebaliknya, data pribadi yang dianggap responden paling aman untuk dibagikan adalah agama, jenis kelamin, dan tanggal lahir. Padahal menurut Data Protection Act-UK (1988), agama merupakan salah satu data pribadi sensitif. Namun, sebagian besar masyarakat merasa tidak khawatir jika dibagikan ke publik.

### 3.3. Data Pribadi Dibagikan ke Publik

Data pribadi umum yang paling banyak pernah dibagikan responden ke publik yaitu nama lengkap, disusul jenis kelamin. Namun, responden justru paling menyesal karena pernah membagikan data NIK, karena data NIK dianggap cukup rawan untuk dibagikan. Di samping itu, banyak responden yang membagikan kontak pribadi ke publik dan mengalami penyesalan, seperti nomor ponsel dan alamat *e-mail*.

Agama memiliki tingkat penyesalan yang paling rendah. Hal tersebut sejalan dengan penemuan bahwa yang paling tidak mereka pedulikan untuk dijaga keamanan/privasinya.





**Grafik 3.5 Data pribadi yang pernah dibagikan ke publik**

DATA PRIBADI UMUM		n	Menyesali
Nama lengkap	58,3%	6.586	31,1%
Jenis kelamin	53,7%	6.070	11,2%
Nomor ponsel	48,2%	5.444	72,5%
Agama	45,1%	5.094	10,6%
Tanggal lahir	44,3%	5.007	30,4%
Alamat e-mail	38,2%	4.324	42,9%
Kewarganegaraan	31,6%	3.575	8,5%
Alamat rumah	30,0%	3.389	38,8%
Tempat bekerja	25,3%	2.863	26,4%
NIK	10,2%	1.153	60,8%
Ijazah	4,8%	541	22,6%
NPWP	2,9%	331	26,9%
Buku nikah	1,3%	147	27,2%

DATA PRIBADI KHUSUS		n	Menyesali
Data lokasi /GPS	16,4%	648	35,0%
Foto anak anggota keluarga <17 tahun	13,7%	693	44,6%
Opini/pandangan/pilihan politik	13,1%	475	32,1%
Nama ibu kandung	10,0%	316	27,9%
Data anak	6,8%	250	32,7%
Data pembelian daring	5,8%	223	34,3%
Data penelusuran situs web	4,2%	184	38,6%
Tiket kereta api/pesawat	3,8%	92	21,2%
Kehidupan/orientasi seksual	3,6%	130	31,7%
Data biometri	3,4%	129	33,2%
Data kesehatan/rekam medis	2,8%	80	25,6%
Data keuangan/perbankan	2,3%	116	44,1%
Catatan kejahatan	0,8%	42	46,2%

### 3.4 Pengetahuan Kebijakan Privasi

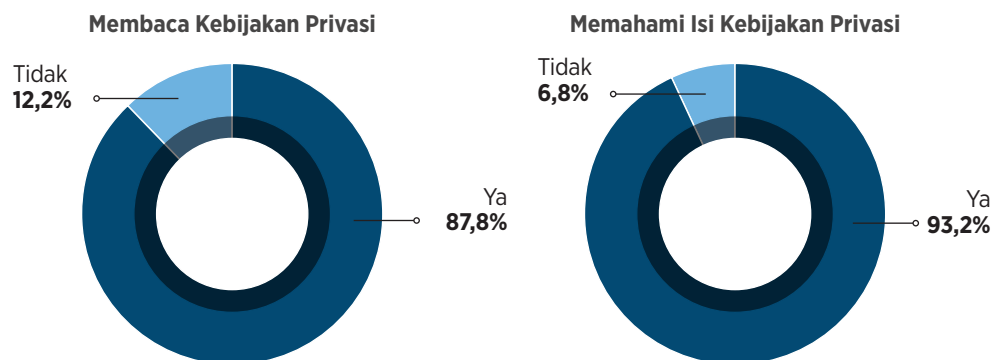
Pada saat menginstal aplikasi atau media sosial, responden akan dihadapkan dengan ketentuan kebijakan data privasi. Mayoritas masyarakat (87,8%) membaca dan mengetahui kebijakan privasi saat membuka atau menginstal aplikasi. Mayoritas masyarakat juga memahami isi kebijakan data privasi tersebut. Pada kelompok masyarakat yang tidak memahami kebijakan pribadi, kebijakan yang terlalu panjang menjadi alasan sehingga mereka mengalami kesulitan.

Di sisi lain, terdapat 12,2% masyarakat yang tidak membaca dan mengetahui kebijakan privasi. Alasan utamanya adalah kebijakan tersebut terlalu panjang. Selain itu, kalimat pada isi kebijakan privasi dinilai sulit dimengerti.

**Grafik 3.6 Pengetahuan tentang kebijakan privasi**

"Apakah anda mengetahui/membaca kebijakan privasi pada saat membuka/menginstal aplikasi/media sosial?" [SA]

Basis: seluruh responden



**Grafik 3.6.1 Alasan tidak mengetahui kebijakan privasi**

"Sebutkan alasan tidak membaca kebijakan privasi." [MA]

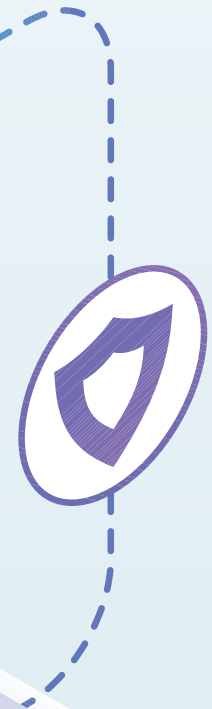
Basis: responden yang tidak mengetahui/membaca kebijakan privasi



Secara keseluruhan, jika ada perubahan ataupun pembaruan kebijakan privasi dari aplikasi yang sudah digunakan, kebanyakan dari responden akan tetap menggunakan aplikasi tersebut, namun tetap waspada sambil mencari aplikasi alternatif yang dapat melindungi data pribadi.







# **BAB 4**

## **PENYALAHGUNAAN DATA PRIBADI**

**K**asus penyalahgunaan data pribadi yang merugikan masyarakat marak terjadi di banyak wilayah di Indonesia belakangan ini. Berdasarkan survei, sebanyak 28,7% masyarakat memiliki pengalaman penyalahgunaan data pribadi.

Akibat penyalahgunaan data pribadi tersebut, kerugian atau dampak yang paling banyak dialami masyarakat adalah diteror atau dihubungi oleh pihak lain yang tidak dikehendaki. Selain itu, mereka yang mengalami penyalahgunaan data pribadi juga mengaku akun media sosial yang mereka miliki dibajak dan digunakan untuk penipuan.

Berdasarkan demografi, laki-laki memiliki pengalaman penyalahgunaan data pribadi yang lebih banyak (31,5%) dibandingkan perempuan (24,1%). Berdasarkan SES, kelompok SES B paling banyak mengalami penyalahgunaan data pribadi (32,2%). Sedangkan berdasarkan pendidikan terakhir, masyarakat berpendidikan sarjana menjadi yang paling banyak mengalami penyalahgunaan data pribadi (35%).

Jika dilihat dari sebarannya, terdapat kasus penyalahgunaan data pribadi di seluruh wilayah Indonesia. Semisal di provinsi Jawa Barat, 504 responden mengalami penyalahgunaan data pribadi dari total 2.448 responden.

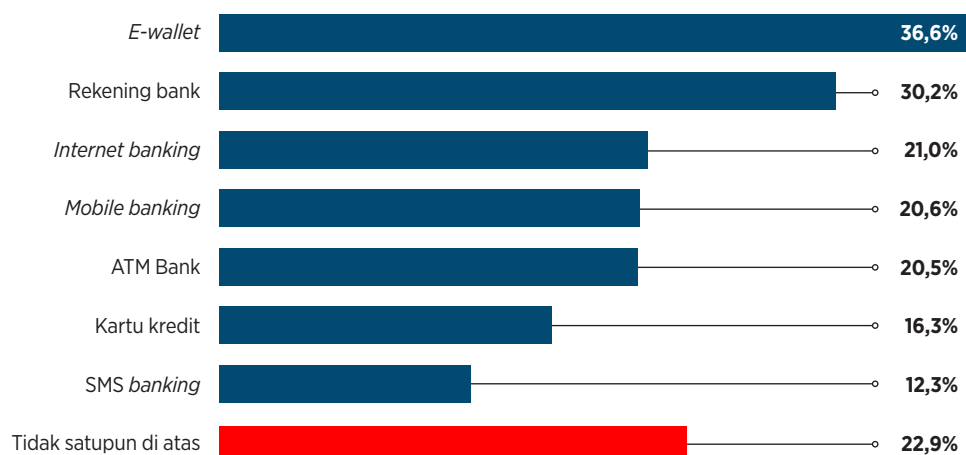
#### 4.1 Lembaga atau Produk yang Rentan Kebocoran Data

Dari sejumlah produk perbankan atau lembaga keuangan, responden menilai *e-wallet* dan rekening bank sebagai produk yang dianggap rentan mengalami kebocoran data. Di sisi lain, sebanyak 22,9% responden mempercayai bahwa produk perbankan dan lembaga keuangan memiliki perlindungan data yang memadai sehingga tidak mungkin mengalami kebocoran data.

**Grafik 4.1 Lembaga atau produk keuangan yang rentan kebocoran data**

"Dari produk perbankan/lembaga keuangan berikut ini, mana yang menurut anda rentan mengalami kebocoran data?" [MA]

Basis: seluruh responden



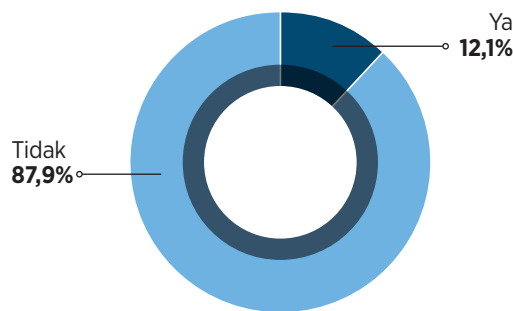


Sebanyak 12,1% responden pernah mengalami kebocoran data finansial. Akibat kebocoran data tersebut, hal yang paling banyak mereka alami adalah berkurangnya uang tabungan di rekening bank (44,1%), disusul berkurangnya saldo di *e-wallet* (32,2%). Kerugian lain yang dirasakan responden yaitu seperti melakukan transfer atau pembelian karena dihubungi oleh orang ataupun perusahaan tertentu.

Meskipun di tengah isu kebocoran data pribadi oleh lembaga keuangan, tingkat keyakinan responden terhadap perlindungan data pribadi saat menggunakan pembayaran digital cukup baik (*mean score* 6,84), walaupun belum cukup tinggi.

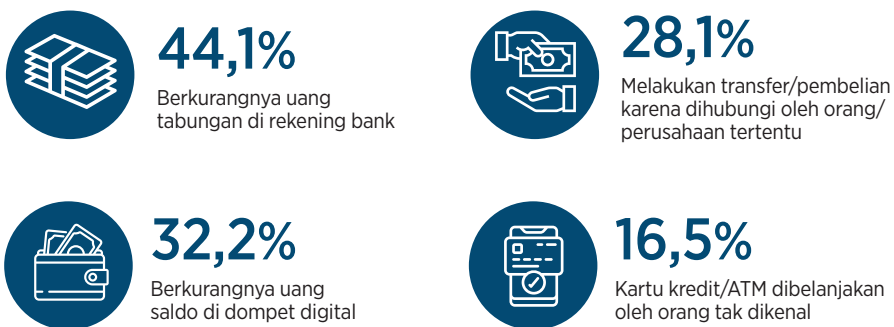
**Grafik 4.2 Kebocoran data finansial/keuangan**

"Apakah anda pernah mengalami kebocoran data finansial/keuangan?" [SA]  
Basis: seluruh responden



**Grafik 4.2.1 Akibat kebocoran data finansial**

"Apakah akibat dari kebocoran data finansial yang pernah anda alami?" [MA]  
Basis: responden yang pernah mengalami kebocoran data finansial

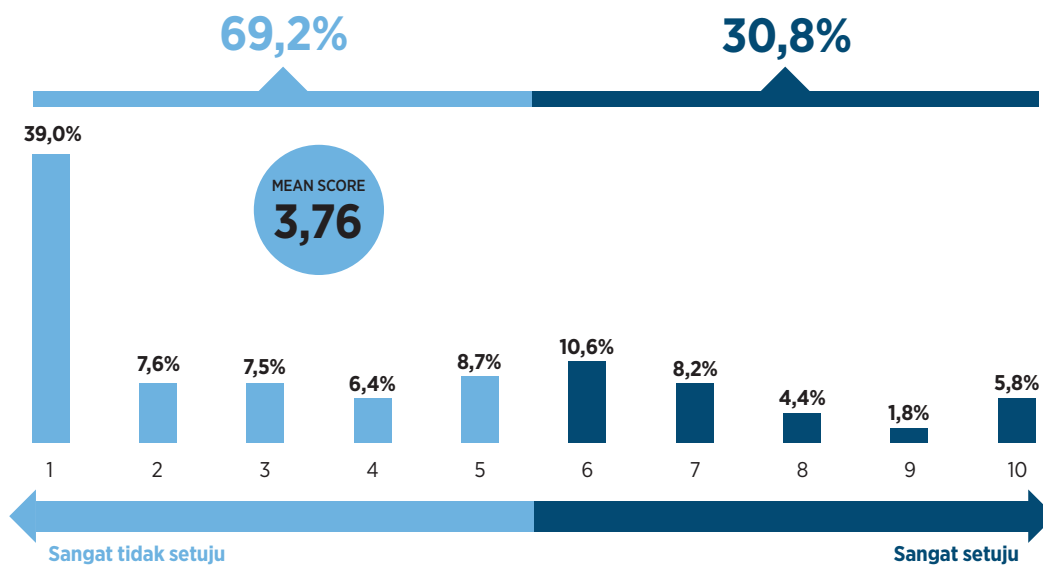


Maraknya kasus kebocoran dan penyalahgunaan data pribadi masyarakat oleh pihak yang tidak bertanggung jawab, membuat masyarakat tidak setuju dengan adanya aktivitas saling berbagi atau kegiatan menjual data pribadi masyarakat yang dilakukan antar lembaga.

Hasil survei menunjukkan mayoritas masyarakat merasa tidak setuju jika suatu platform atau penyedia layanan mempunyai hak untuk membagikan atau menjual informasi penggunaannya kepada instansi dan perusahaan lain. Hal tersebut terlihat dari *mean score* sebesar 3,76 dari rentang 1-10. Skor 1 berarti sangat tidak setuju, sedangkan 10 menunjukkan sangat setuju.

**Grafik 4.3 Tingkat kesetujuan untuk menjual/membagi informasi data pribadi**

"Bagaimana tingkat kesetujuan anda jika suatu platform/penyedia layanan mempunyai hak untuk membagikan/ menjual informasi penggunaanya ke instansi/perusahaan lain?" [SA]  
 Basis: seluruh responden



## 4.2 Penyalahgunaan Data di Media Sosial

Ketika data pribadi disalahgunakan di media sosial, mayoritas masyarakat akan langsung mengambil tindakan untuk melaporkan ke platform media sosial tersebut. Namun, beberapa responden memutuskan untuk tidak melapor atau tidak melakukan apapun.

Hal itu terjadi karena banyak dari responden yang tidak tahu harus melapor ke mana, atau sudah melapor namun tidak terjadi apa-apa. Bagi Gen Y dan Milenial (23-38 tahun), mengajukan tuntutan hukum ke pihak berwajib tidak menjadi pilihan yang populer.

**Grafik 4.4 Tindakan ketika terjadi penyalahgunaan data di media sosial**

"Apa yang anda lakukan ketika data pribadi anda telah disalahgunakan di media sosial?" [MA]  
 Basis: seluruh responden

	Total (%)	Gen Z (n=3.677) (%)	Gen Y (n=6.106) (%)	Gen X (n=1.464) (%)	Boomer (n=58) (%)
Melaporkan ke platform media sosial tersebut	83,4	80,9	84,8	84,4	79,3
Mengajukan tuntutan hukum ke pihak berwajib	38,5	38,0	6,6	36,7	39,7
Meminta kompensasi kepada perusahaan atas bocornya data pribadi	27,2	29,9	26,6	23,3	19,0
Tidak peduli/tidak melakukan apapun	5,1	5,9	4,5	5,3	5,2
Memblokir aktivitas akun/menutup akun	0,2	0,2	0,2	0,4	1,7

### 4.3 Lembaga Pengumpul Data Pribadi

Ketika berhubungan dengan suatu lembaga, ada kalanya masyarakat membagikan data pribadi kepada lembaga tersebut. Menurut hasil survei, responden menganggap bank dan lembaga keuangan merupakan instansi yang paling banyak mengumpulkan data pribadi. Meskipun begitu, responden merasa bank dan lembaga keuangan dapat dipercaya dan dianggap memberikan perlindungan data pribadi yang memadai.

Sebaliknya, responden menganggap kepolisian sebagai lembaga yang tidak banyak mengumpulkan data pribadi, namun dianggap memiliki perlindungan data yang memadai.

**Grafik 4.5 Lembaga pengumpul data pribadi**

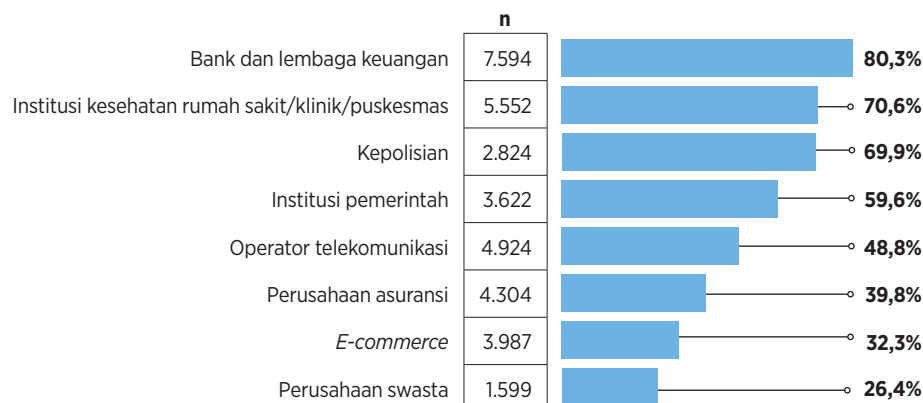
"Lembaga apa yang menurut anda banyak mengumpulkan data pribadi?" [MA]  
Basis: seluruh responden



**Grafik 4.5.1 Lembaga yang dipercaya memberikan perlindungan data pribadi**

"Di antara lembaga berikut, mana saja lembaga yang memberikan perlindungan data pribadi yang memadai?" [MA]

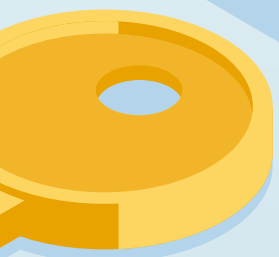
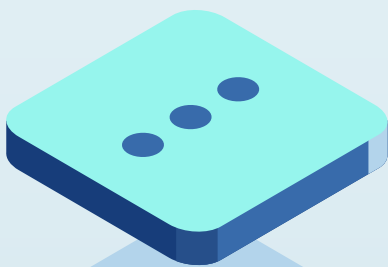
Basis: responden yang memilih tiap-tiap lembaga





# **BAB 5**

## **PENGETAHUAN AKAN KEAMANAN DATA PRIBADI**



**K**asus kebocoran dan pencurian data pribadi di Indonesia masih kerap kali terjadi. Salah satu penyebabnya bisa berasal dari aplikasi yang diinstal di gawai. Setiap kali kita menginstal aplikasi ke gawai, akan muncul notifikasi yang meminta akses pada informasi tertentu seperti kontak, kamera, audio, lokasi/GPS, *file*/media, dan sebagainya.

### 5.1 Notifikasi Akses Aplikasi Komunikasi, Lokapasar (*Marketplace*), dan Transportasi Daring

Survei tersebut menunjukkan bahwa saat menginstal aplikasi, responden paling banyak memberikan izin akses pada aplikasi komunikasi seperti WhatsApp, Facebook, Instagram, dan sebagainya. Selanjutnya, sekitar 40% responden juga memberikan akses pada aplikasi lokapasar (Tokopedia, Shopee, dan sebagainya) dan aplikasi transportasi daring (Gojek, Grab, dan sebagainya). Aplikasi-aplikasi tersebut sudah menjadi bagian esensial yang digunakan oleh masyarakat dalam kehidupan sehari-hari.

Pada saat menginstal aplikasi komunikasi, sekitar 90% responden memberikan izin akses pada foto, media, dan *file*, serta mengambil gambar dan merekam video. Di samping itu, sekitar 90% responden juga memberikan izin pada panggilan telepon, kontak, dan audio. Sementara, ada 80% responden yang memberikan akses pada bagian SMS, lokasi/GPS, dan kalender.

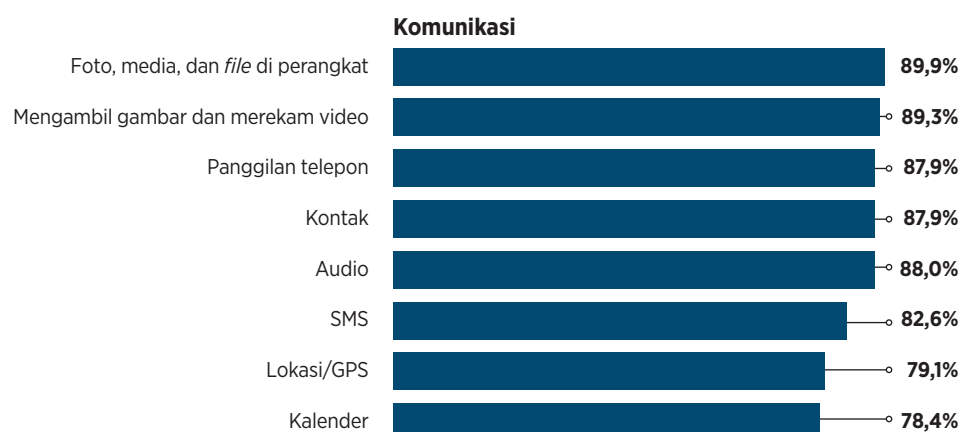
Saat menginstal aplikasi lokapasar, ketiga pengaturan terbanyak yang diberikan oleh responden pada izin akses terhadap lokasi atau GPS (51,5%), SMS (46,8%), serta foto, media, dan *file* di perangkat (45,8%). Lalu, untuk aplikasi transportasi daring, responden paling banyak memberikan akses pada lokasi (54,9%), panggilan telepon (43,8%), dan SMS (41,0%).

Dari pengaturan ini terlihat bahwa responden mengizinkan akses pada bagian-bagian yang sesuai dengan kebutuhan akan penggunaan tiap aplikasi. Sebagai contoh untuk aplikasi komunikasi, responden memberikan akses untuk mengirimkan berbagai *file*, gambar atau video ataupun kontak seseorang.

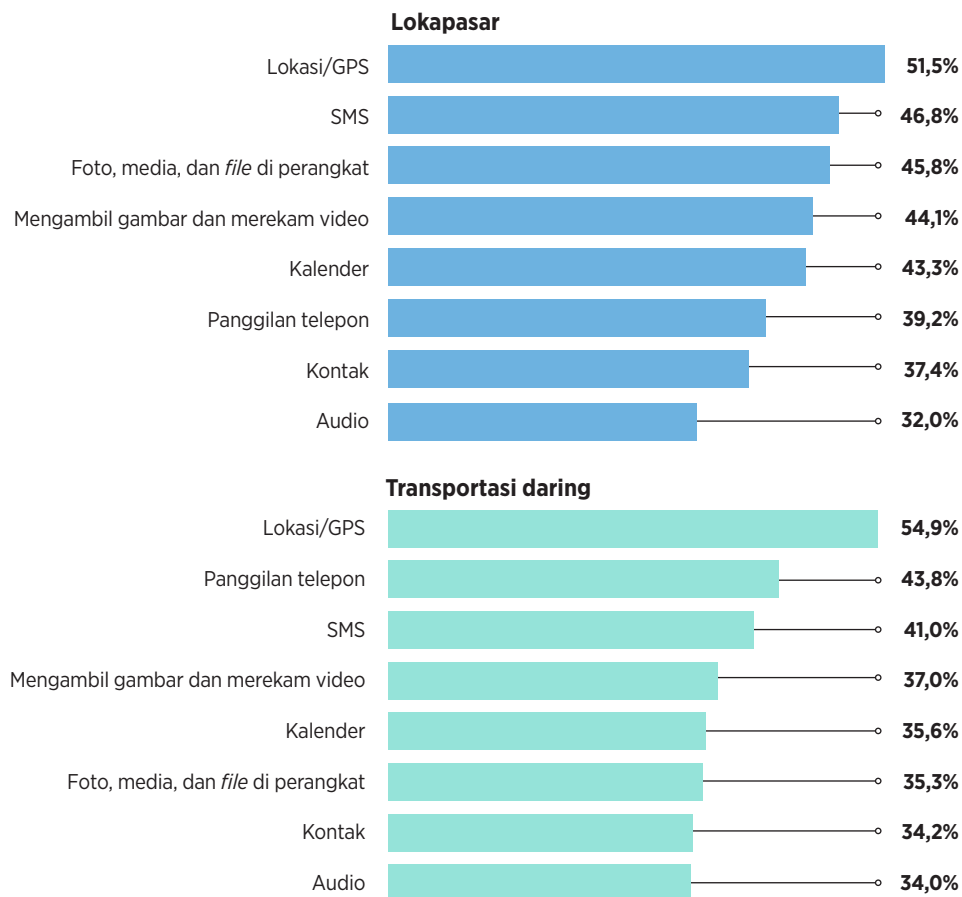
#### Grafik 5.1 Pemberian izin akses pada aplikasi

"Saat anda menginstal aplikasi muncul notifikasi di gawai anda seperti di bawah ini, aplikasi mana saja yang anda *allow*/izinkan?" [MA]

Basis: seluruh responden







## 5.2 Notifikasi Akses Aplikasi Perbankan, Kesehatan, dan Pinjaman *Online*

Ketika menginstal aplikasi keuangan dan perbankan, responden paling banyak memberikan izin akses pada SMS (43,0%), kalender (37,6%), dan foto, media di perangkat (35,1%). Demikian juga untuk aplikasi kesehatan, responden paling banyak mengizinkan akses pada bagian kalender, SMS, dan foto, media di perangkat.

Untuk aplikasi pinjaman *online*, ketiga pengaturan terbanyak yang diberikan oleh responden pada izin akses terhadap kalender (9,3%), SMS (8,6%), serta mengambil gambar dan video (8,6%). Selain itu, terdapat 8,4% responden mengizinkan akses pada lokasi, dan 8,1% lainnya pada panggilan telepon.

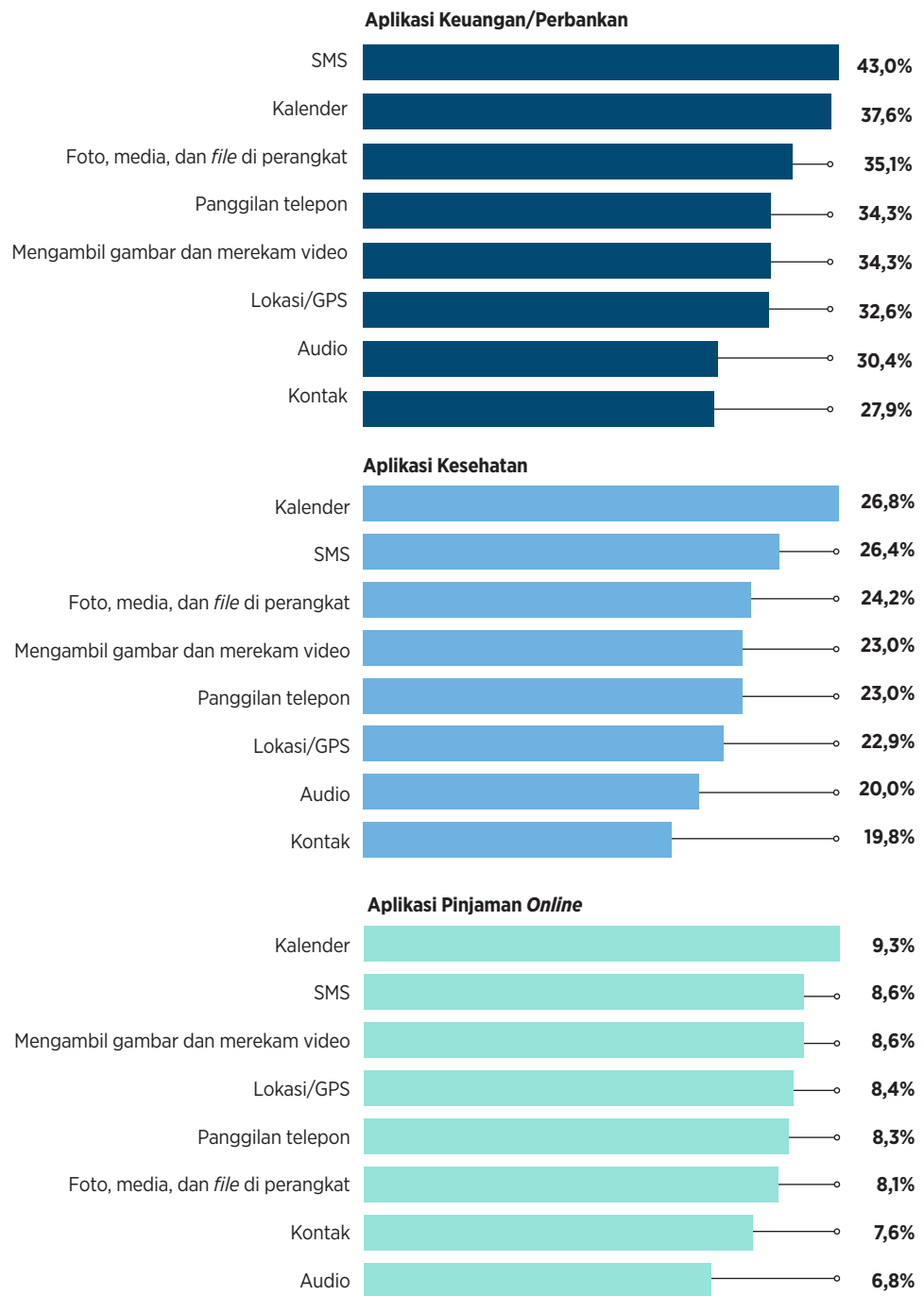
Otoritas Jasa Keuangan (OJK) sendiri membatasi akses data digital pribadi untuk pinjaman *online* (*fintech lending*). Lembaga tersebut mengatur pemberian akses oleh perusahaan pinjaman *online* hanya pada kamera, mikrofon, dan lokasi.

Dari survei terlihat bahwa sebagian responden tidak memperhatikan ketentuan tersebut, dengan memberikan izin di luar ketiga pengaturan tersebut seperti untuk SMS, kalender, dan foto, media ataupun *file* yang ada di perangkat. Hal tersebut tentunya menjadi ancaman bagi bocornya informasi berharga yang dimiliki oleh pengguna gawai.

**Grafik 5.2 Pemberian izin akses pada aplikasi keuangan/perbankan, kesehatan, dan pinjaman *online***

"Saat anda menginstal aplikasi muncul notifikasi di gawai anda seperti di bawah ini, aplikasi mana saja yang anda *allow/izinkan*?" [MA]

Basis: seluruh responden



Saat mendapatkan notifikasi izin akses ke banyak hal seperti identitas, kontak, lokasi, dan sebagainya, rata-rata responden memberikan akses dan tetap menginstal aplikasi tersebut (Grafik 5.3).

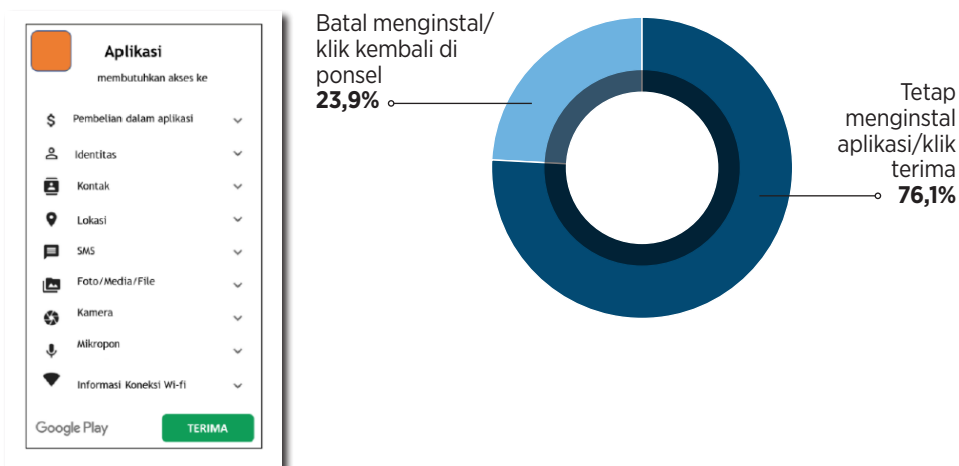
Berdasarkan hasil riset perusahaan keamanan siber Kaspersky, 14,8% pengguna perangkat seluler menjadi target *malware/adware* pada tahun 2019, dan aplikasi *default* pra-instal adalah salah satu yang berperan di dalamnya.

Dibandingkan antar beda generasi, generasi yang lebih tua cenderung lebih memilih untuk membatalkan menginstal aplikasi ketika muncul notifikasi untuk memberikan akses pada banyak data dan informasi. Hampir 50% responden dari generasi *boomer* membatalkan untuk menginstal aplikasi dan sekitar 40% responden dari generasi X juga melakukan hal yang sama.

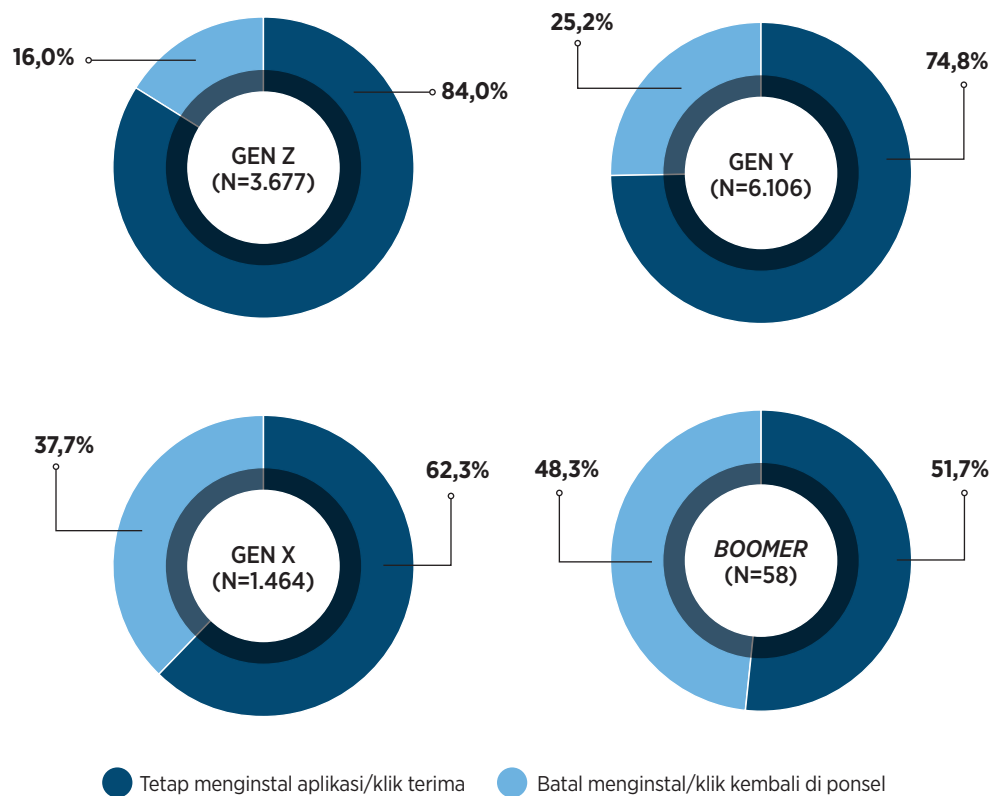
Sebaliknya, generasi yang lebih muda cenderung lebih pasrah pada pengaturan terhadap pemberian izin akses tersebut. Sekitar 75% responden dari generasi Y dan 85% responden dari generasi Z tetap menginstal aplikasi tersebut. Dari sini menandakan bahwa generasi lebih muda cenderung lebih rentan pada kemungkinan data diambil saat berinteraksi dengan suatu aplikasi.

**Grafik 5.3 Penginstalan aplikasi dengan memberikan izin akses**

"Saat anda menginstal aplikasi yang anda inginkan muncul notifikasi berikut ini, apakah anda tetap akan menginstal/klik terima?" [SA]  
Basis: seluruh responden



**Grafik 5.3.1** Peningstalan aplikasi dengan memberikan izin akses berdasarkan kelompok usia



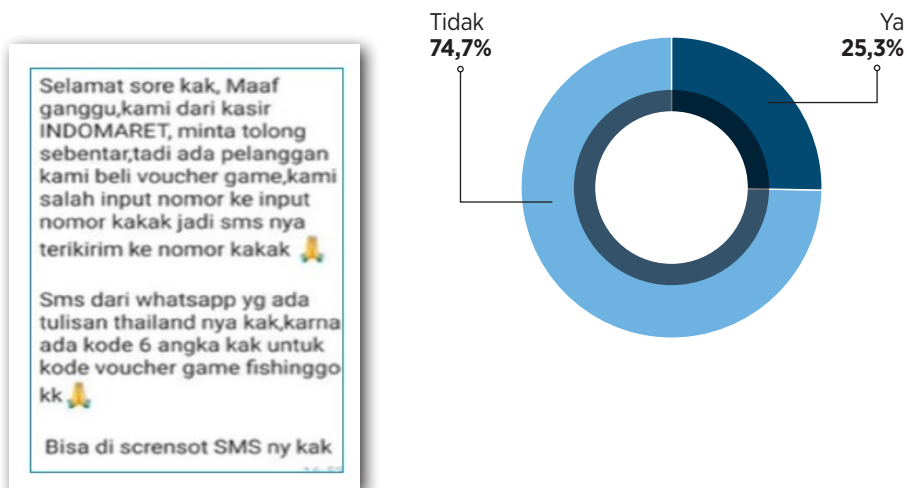
### 5.3 Notifikasi Pesan WhatsApp/SMS

Salah satu modus penipuan dunia maya lainnya adalah melalui pesan singkat yang dikirimkan melalui SMS dan WhatsApp dan meminta pengguna untuk mengklik suatu tautan yang tercantum atau mengirimkan kode atau informasi personal ke pengirim pesan tersebut. Dari hasil survei didapatkan bahwa mayoritas responden belum pernah mendapatkan pesan yang meminta penerima membagikan kode angka untuk suatu pembelian barang. Sementara itu, terdapat 25% responden pernah mendapatkan pesan SMS dan WhatsApp serupa (Grafik 5.4).

Survei tersebut kemudian menilai pendapat dan mengukur tingkat keyakinan responden apakah informasi tersebut berupa penipuan atau kejahatan pencurian data. Dari skala 1-10, rata-rata skor responden adalah 8,15, yang artinya rata-rata responden berpendapat bahwa pesan tersebut merupakan penipuan, sebuah pesan berisikan motif pencurian data pribadi.

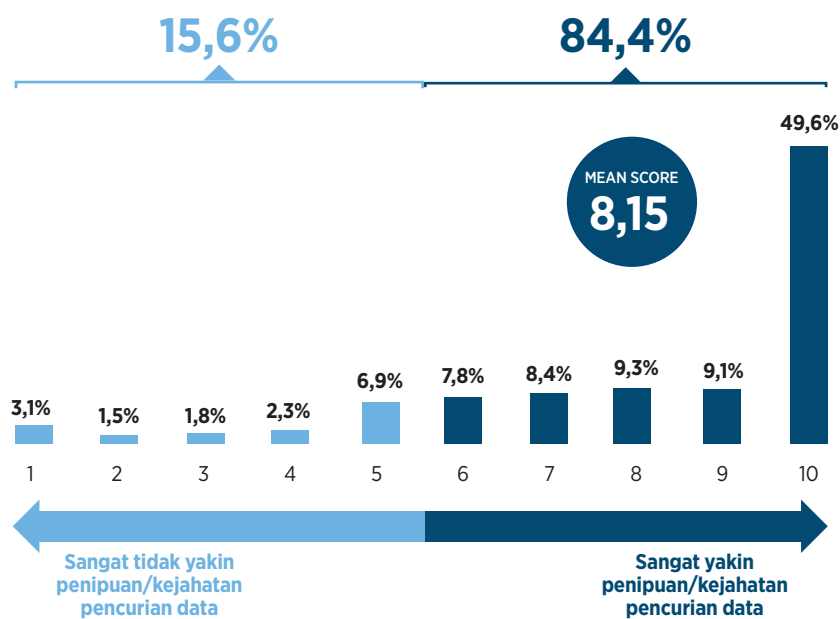
**Grafik 5.4 Pengalaman dalam mendapatkan pesan SMS/WhatsApp**

"Apakah anda pernah mendapatkan pesan WhatsApp/SMS seperti di berikut?" [SA]  
 Basis: seluruh responden



**Grafik 5.4.1 Tingkat keyakinan terhadap pesan yang berupa penipuan**

"Dari skala 1-10, menurut anda apakah info tersebut penipuan?" [SA]  
 Basis: seluruh responden

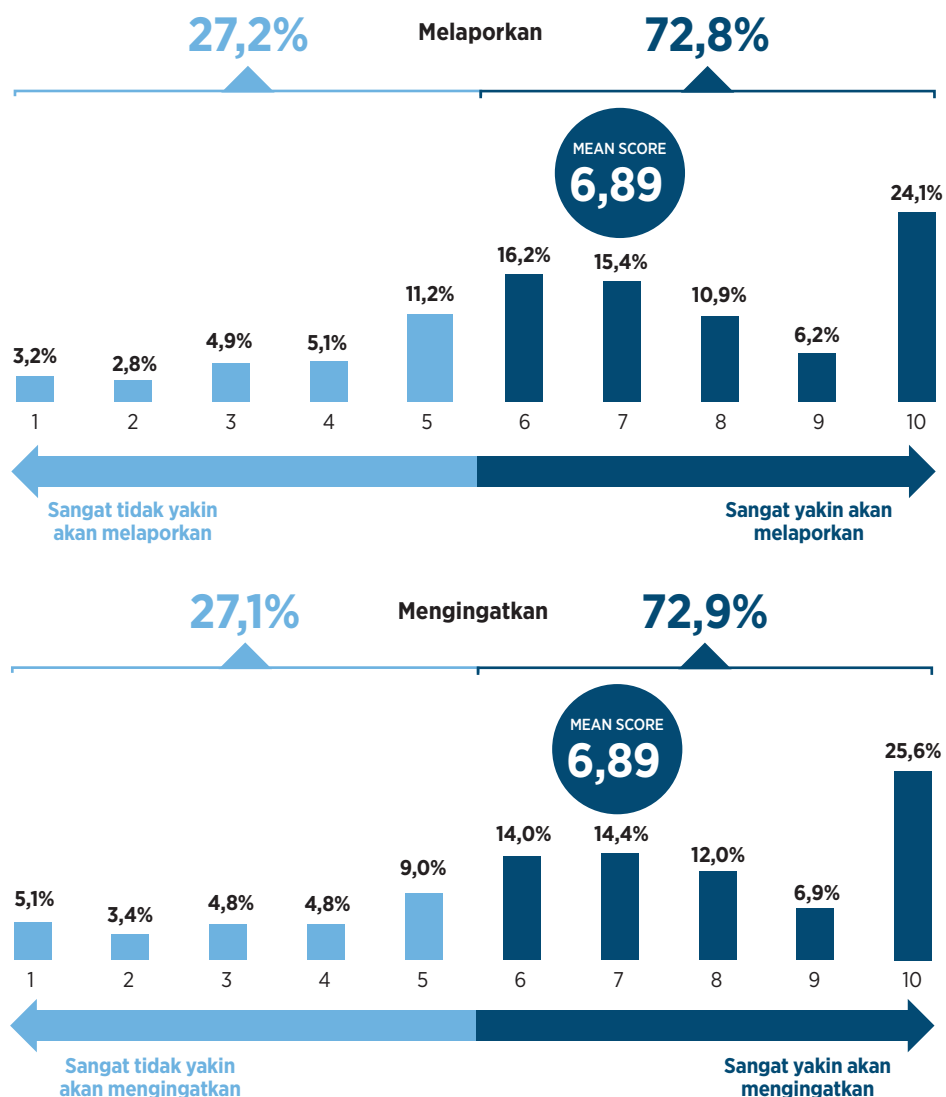


Selanjutnya, survei juga mengukur bagaimana respons terhadap orang yang mengirimkan pesan tersebut. Rata-rata responden yang menganggap bahwa pesan tersebut penipuan berkeinginan untuk melaporkan pengirim pesan tersebut. Dari skala 1-10, rata-rata skor tingkat keyakinan responden adalah 6,89, artinya responden relatif yakin untuk melaporkan suatu pesan yang mengandung motif penipuan/pencurian data pribadi.

Terhadap pesan yang sama, responden juga berkeinginan untuk mengingatkan orang yang telah mengirimkan suatu pesan yang berisikan motif penipuan atau pencurian data. Hal tersebut menunjukkan bahwa responden cukup menyadari pentingnya suatu tindakan lebih lanjut terhadap pihak-pihak yang mengirimkan informasi yang mengancam kebocoran data pribadi seseorang.

#### Grafik 5.5 Tindakan terhadap pengirim pesan berisi motif penipuan

"Dari skala 1-10, menurut anda, apakah anda akan melaporkan orang yang mengirimkan pesan tersebut?"[SA]  
 Basis: responden yang menganggap pesan tersebut penipuan







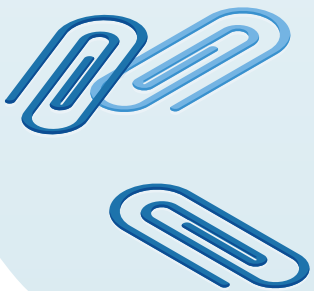
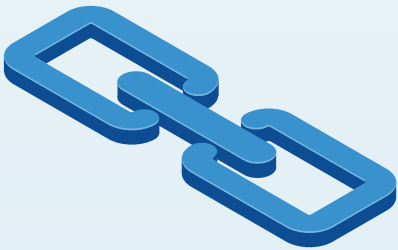


# BAB 6

## RUU

# PELINDUNGAN

# DATA PRIBADI



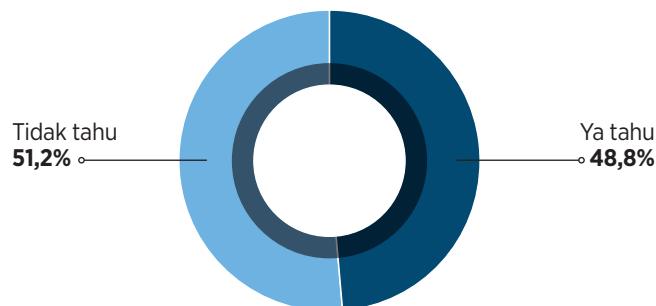
**K**eberadaan instrumen hukum memiliki andil besar dalam memberikan perlindungan bagi masyarakat, swasta maupun pemerintah dari tindak pencurian data pribadi ataupun bentuk kejahatan siber lainnya. Kementerian Komunikasi dan Informatika (Kemkominfo) telah menyusun Rancangan Undang-Undang (RUU) Pelindungan Data Pribadi untuk meningkatkan keamanan data pribadi seseorang. Saat ini, RUU sedang dalam tahap pembahasan di DPR RI.

### 6.1 Pengetahuan tentang RUU Pelindungan Data Pribadi

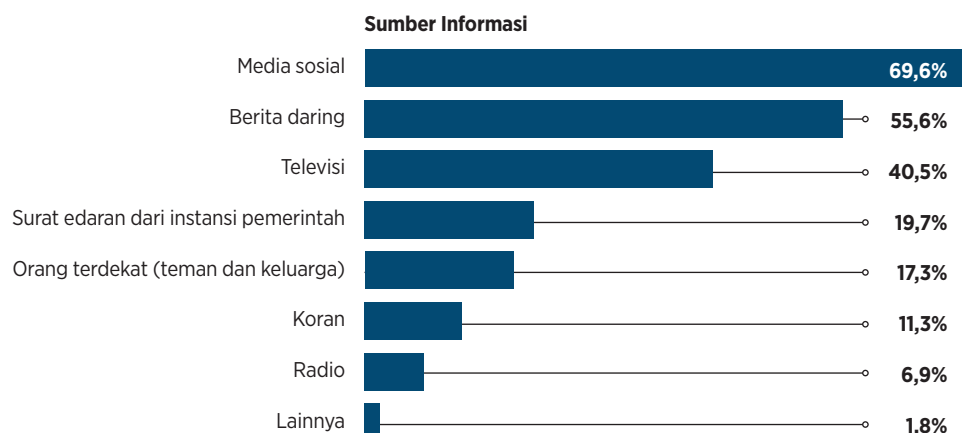
Survei menunjukkan bahwa hampir setengah responden mengetahui atau pernah membaca tentang RUU Pelindungan Data Pribadi. Kebanyakan dari responden mengetahuinya dari media sosial (69,6%), portal berita daring (55,6%), dan televisi (40,5%). Aturan tersebut nantinya perlu disebarluaskan secara efektif melalui media tersebut mengingat sekitar 50% responden belum mengetahui tentang keberadaan rancangan aturan tersebut.

**Grafik 6.1 Pengetahuan tentang RUU Pelindungan Data Pribadi**

"Apakah anda mengetahui/membaca tentang RUU Pelindungan Data Pribadi?" [SA]  
Basis: seluruh responden



"Dari mana anda mengetahui/membaca tentang RUU Pelindungan Data Pribadi?" [MA]  
Basis: responden yang mengetahui/membaca tentang RUU Pelindungan Data Pribadi

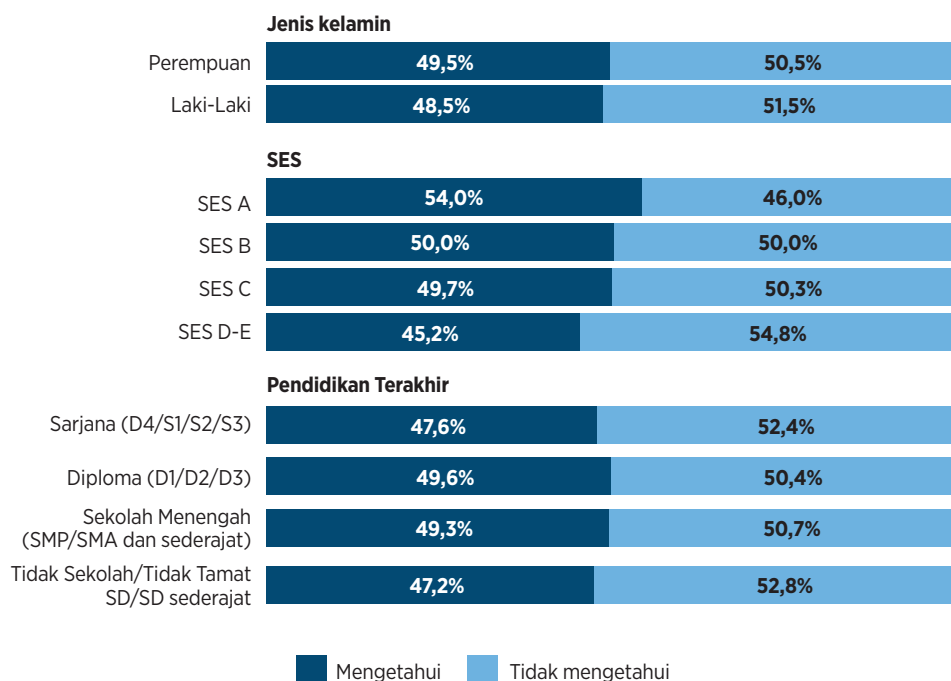


Terdapat setengah dari responden baik laki-laki maupun perempuan mengetahui atau pernah membaca tentang RUU Pelindungan Data Pribadi. Responden yang mengetahui tentang RUU Pelindungan Data Pribadi cenderung berasal dari kelas ekonomi yang lebih tinggi. Survei menunjukkan 54% responden SES A dan 50% responden SES B mengetahui tentang rancangan regulasi tersebut. Sementara ada lebih sedikit responden dari kelas ekonomi lebih rendah, sekitar 45% responden berasal dari kelas ekonomi D dan E yang mengetahui tentang RUU tersebut.

Dari latar belakang tingkat pendidikan, lebih banyak responden yang mengetahui atau pernah membaca tentang RUU Pelindungan Data Pribadi adalah lulusan sekolah menengah sederajat (49,3%) dan diploma (49,6%). Meskipun dengan level pendidikan lebih tinggi, jumlah responden dari tingkat pendidikan sarjana justru lebih sedikit (47,6%), ada kemungkinan ini berkaitan dengan jenis paparan informasi yang biasa didapatkan oleh responden.

**Grafik 6.2 Pengetahuan tentang RUU Pelindungan Data Pribadi berdasarkan jenis kelamin, SES, dan pendidikan terakhir**

"Apakah anda mengetahui/membaca tentang RUU pelindungan Data Pribadi?" [SA]  
Basis: seluruh responden



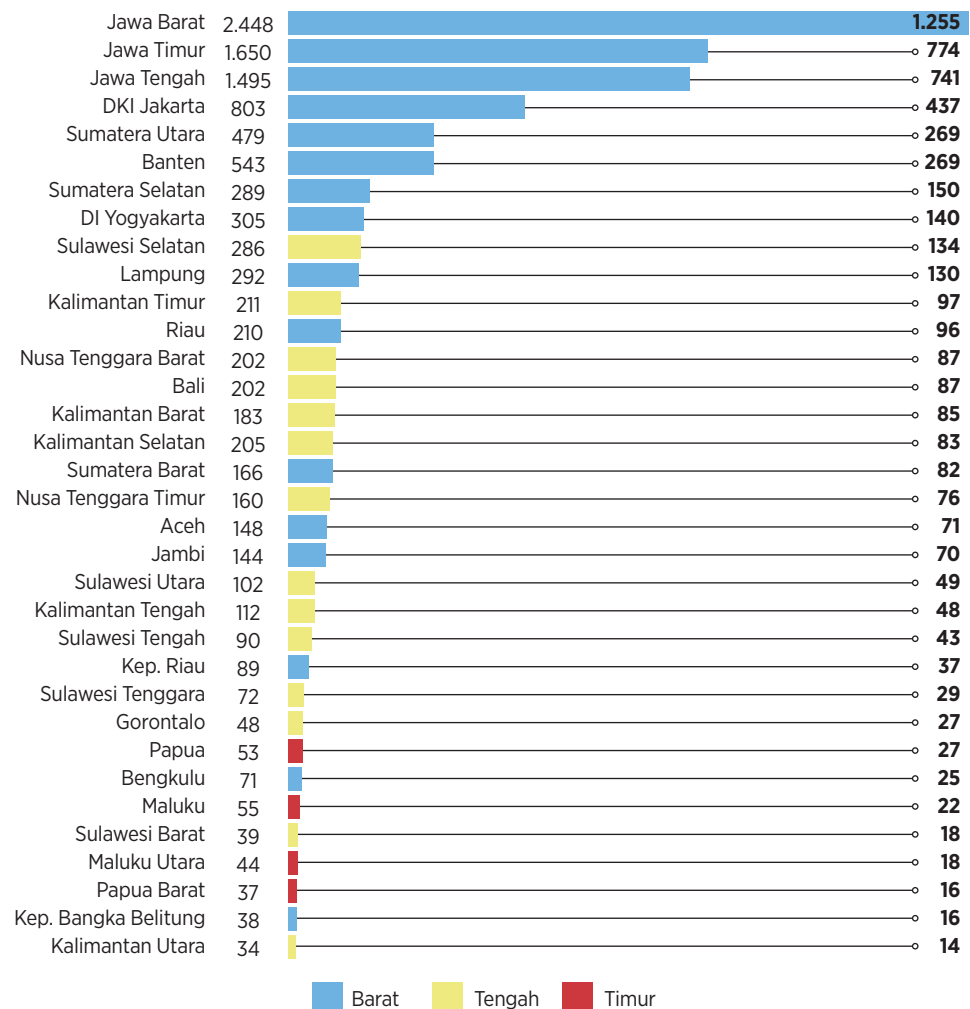
Survei juga mengidentifikasi banyaknya responden yang mengetahui atau membaca tentang RUU Pelindungan Data Pribadi berdasarkan lokasi. Secara keseluruhan, responden yang lebih banyak mengetahui tentang RUU Pelindungan Data Pribadi berada di wilayah Barat, lalu disusul responden di wilayah Tengah dan lebih sedikit di wilayah Timur.

Responden yang paling banyak mengetahui tentang RUU Pelindungan Data Pribadi berada di provinsi Jawa Barat, Jawa Timur, Jawa Tengah, DKI Jakarta, Sumatera Utara, dan Banten. Adapun jumlah responden yang paling sedikit mengetahui RUU tersebut berada di provinsi Sulawesi Barat, Maluku Utara, Papua Barat, Bangka Belitung, dan Kalimantan Utara (Grafik 6.3).

Berdasarkan penyebaran tersebut, dapat dikatakan bahwa informasi mengenai RUU Pelindungan Data Pribadi masih belum merata diketahui oleh responden baik dari wilayah Barat, Tengah maupun Timur.

**Grafik 6.3 Pengetahuan tentang RUU Pelindungan Data Pribadi berdasarkan lokasi**

"Apakah anda mengetahui/membaca tentang RUU Pelindungan Data Pribadi?" [SA]  
Basis: seluruh responden



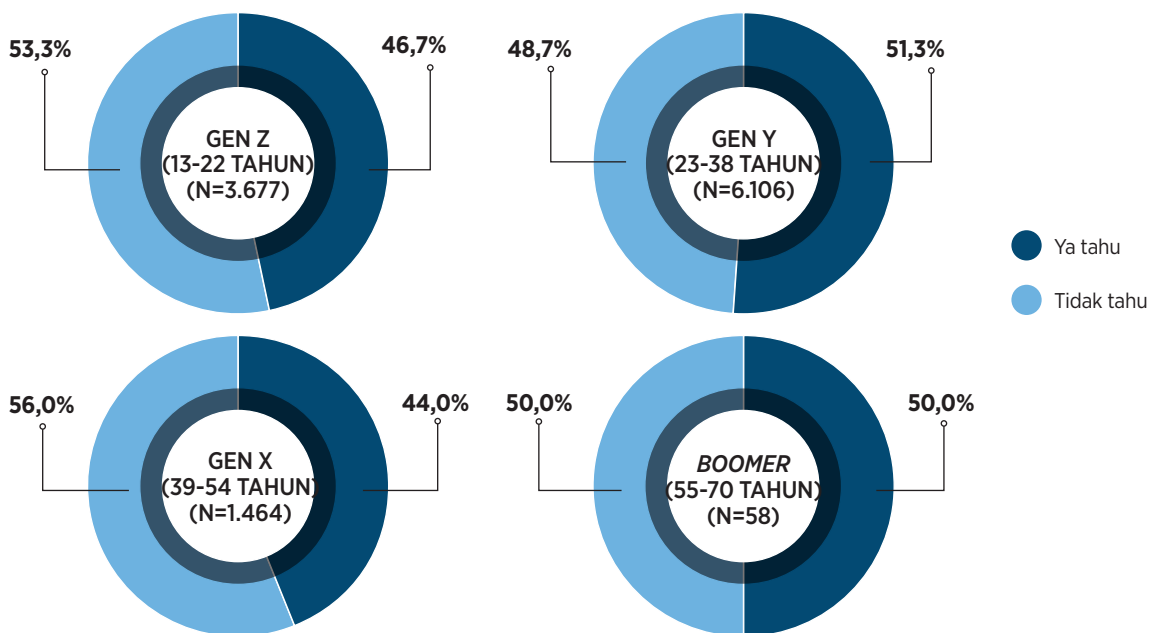


Generasi yang paling banyak mengetahui atau membaca tentang RUU Pelindungan adalah generasi Y (51,3%), lalu diikuti oleh generasi boomer (50,0%), generasi Z (46,7%), dan yang paling sedikit adalah generasi X (44,0%).

Kebanyakan responden dari tiap generasi mengetahui tentang rancangan aturan tersebut dari media sosial dan portal berita daring. Meski dengan tingginya akses terhadap media digital oleh generasi lebih muda (Gen Z), dari survei terlihat hal ini tidak menjadikan generasi tersebut paling banyak mengetahui RUU Pelindungan Data Pribadi dibandingkan dengan generasi lainnya.

**Grafik 6.4 Pengetahuan tentang RUU Pelindungan Data Pribadi berdasarkan generasi**

"Apakah anda mengetahui/membaca tentang RUU Pelindungan Data Pribadi?" [SA]  
Basis: seluruh responden



**Grafik 6.4.1 Sumber informasi tentang RUU Pelindungan Data Pribadi berdasarkan generasi**

"Dari mana anda mengetahui/membaca tentang RUU Pelindungan Data Pribadi?" [MA]  
Basis: responden yang mengetahui/membaca tentang RUU Pelindungan Data Pribadi

	Total	Gen Z (13-22 tahun) (n=3.677)	Gen Y (23-38 tahun) (n=6.106)	Gen X (39-54 tahun) (n=1.464)	Boomer (55-70 tahun) (n=58)
Media sosial	69,6%	68,7%	69,8%	70,5%	69,0%
Berita daring	55,6%	44,9%	58,6%	69,1%	65,5%
Televisi	40,5%	37,0%	41,8%	42,7%	51,7%
Surat edaran dan instansi pemerintah	19,7%	13,9%	21,7%	25,2%	24,1%
Orang terdekat (teman dan keluarga)	17,3%	15,4%	17,6%	21,1%	17,2%
Koran	11,3%	8,8%	11,5%	16,3%	27,6%
Radio	6,9%	6,2%	7,0%	9,0%	3,4%

## 6.2 Sistem Pelindungan Data di Indonesia

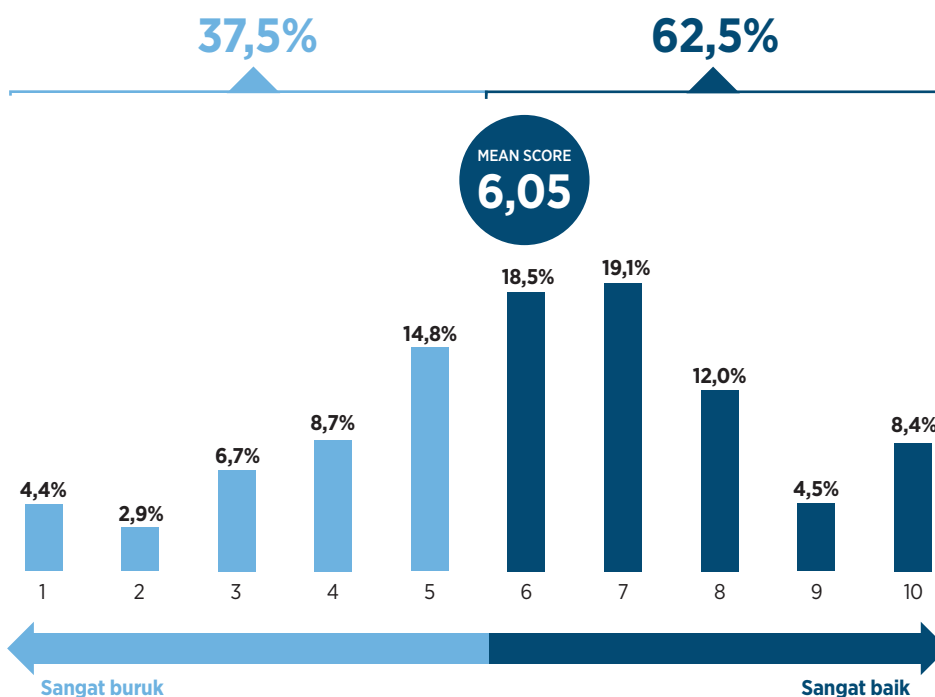
Di dalam Data Privacy Handbook (PwC, 2019) dijelaskan bahwa data pribadi penting untuk dilindungi karena berkaitan langsung dengan hak asasi manusia, diantaranya hak untuk mengakses, menghapus, membatasi, mengoleksi dan mentransfer data pribadi.

Menurut responden, sistem pelindungan data di Indonesia saat ini berada pada level cukup baik dengan skor rata-rata 6,05, dari skala 1-10. Terhadap penilaian tersebut, dapat dikatakan bahwa Indonesia masih perlu meningkatkan sistem dalam melindungi informasi dan data personal agar tidak rentan untuk diretas dan disalahgunakan.

Berdasarkan lokasi, responden dengan penilaian 3 tertinggi berasal dari provinsi Nusa Tenggara Timur (skor 6,8), Gorontalo (skor 6,3), dan Sumatera Selatan (skor 6,3). Sementara penilaian 3 terendah datang dari responden yang berada di provinsi Maluku Utara (skor 5,5), Kalimantan Utara (skor 5,5), dan Papua Barat (skor 5,3).

### Grafik 6.5 Penilaian terhadap sistem pelindungan data pribadi di Indonesia

"Dari skala 1-10 (1= Sangat buruk, 10= Sangat baik), bagaimana anda menilai sistem pelindungan data pribadi di Indonesia saat ini?" [SA]  
Basis: seluruh responden

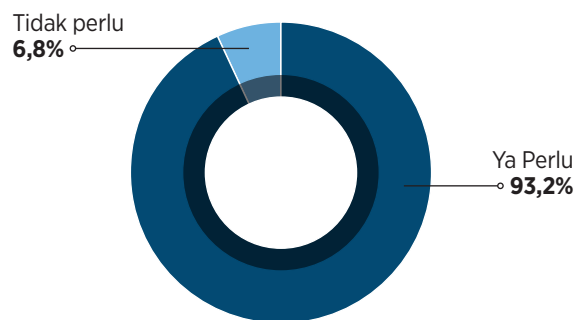


Bagi hampir keseluruhan responden, keberadaan institusi/lembaga merupakan hal penting dalam mengatur dan mengawasi penerapan Undang-Undang Pelindungan Data Pribadi. Ini menandakan bahwa bagi responden, independensi penting untuk memastikan lembaga menjalankan prinsip-prinsip pelindungan data pribadi secara efektif.

Dengan keberadaan lembaga tersebut, 80% responden berharap dapat mengadu/melaporkan kejadian yang berkaitan dengan data pribadi dan bisa ditindaklanjuti dengan lebih baik. Di samping itu, sekitar 60% responden berharap lembaga tersebut dapat berperan dalam memberikan edukasi tentang pelindungan data pribadi.

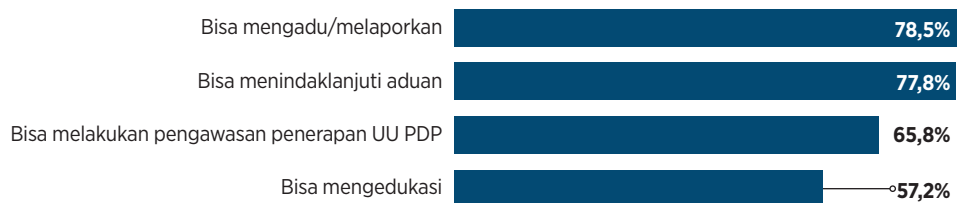
**Grafik 6.6 Pentingnya institusi mengatur penerapan UU Pelindungan Data Pribadi**

"Menurut anda apakah perlu adanya institusi/lembaga yang mengatur dan mengawasi penerapan Undang-Undang Pelindungan Data Pribadi?" [SA]  
Basis: seluruh responden



**Grafik 6.6.1 Harapan terhadap institusi**

"Apa harapan anda terhadap hadirnya lembaga tersebut?" [MA]  
Basis: Responden yang menganggap perlunya ada lembaga yang mengatur pelindungan data pribadi





# BAB 7

## PENUTUP



### 7.1 Kesimpulan

Berdasarkan uraian di atas, berikut sejumlah kesimpulan yang dapat diambil dari survei terhadap masyarakat mengenai perlindungan data pribadi.

1. Melalui survei ini diketahui masyarakat sadar bila perlindungan data pribadi penting tetapi belum cukup baik dalam mengambil tindakan atau langkah perlindungan atas data pribadinya. Hal ini tercermin dari pengetahuan mereka atas isu ini, salah satunya bahwa 87,8% masyarakat membaca dan mengetahui kebijakan privasi saat membuka dan menginstal aplikasi. Namun, masyarakat belum sepenuhnya selektif dalam mengatur akses atas gawai dan aplikasi yang memungkinkan pencurian data.
2. Tingkat pemahaman masyarakat akan data pribadi ditunjukkan dengan hampir seluruh masyarakat telah mengetahui tentang data pribadi. Skor pengetahuan data pribadi umum 6,70 dari skala 10, sementara skor untuk pengetahuan data pribadi khusus 5,26 dari skala 10. Survei juga menemukan bahwa penyalahgunaan data pribadi masih terjadi di seluruh wilayah Indonesia.
3. Masyarakat secara umum telah mengetahui tentang RUU Pelindungan Data Pribadi. Pengetahuan ini didapatkan masyarakat dari media sosial (69,6%), portal berita daring (55,6%), dan televisi (40,5%).
4. Kepedulian masyarakat terhadap perlindungan data pribadi masih tergolong kurang. Ini ditunjukkan dengan 55,5% pengguna Facebook dan 25,5% pengguna Instagram tidak melakukan pengaturan privat pada akun media sosial tersebut.
5. Persepsi publik atas pemahaman tentang kerahasiaan data pribadi dianggap cukup baik tetapi belum memadai. Hal tersebut terlihat dari penilaian terhadap sistem perlindungan data di Indonesia dengan skor rata-rata 6,05 dari skala 10. Oleh sebab itu, Indonesia perlu meningkatkan sistem dan implementasi aturan perlindungan data pribadi.

### 7.2 Temuan

Berikut sejumlah temuan yang dapat diambil dari survei terhadap masyarakat mengenai perlindungan data pribadi.

- WhatsApp merupakan media sosial yang paling banyak diakses saat ini (88,8%). Setiap kelompok usia memiliki preferensi penggunaan media sosial yang berbeda. Secara proporsi terlihat, Facebook banyak digunakan oleh kelompok usia dewasa, dan TikTok digunakan oleh kelompok usia yang lebih muda.

- Untuk media sosial berupa aplikasi perpesanan instan (*messenger*), responden lebih selektif dalam menambah teman. Hal tersebut juga disebabkan karena aplikasi perpesanan instan biasanya harus dikaitkan dengan nomor ponsel terlebih dahulu. TikTok dan YouTube adalah media sosial yang memiliki cara menambah teman paling bebas.
- Survei juga menemukan bila pertemanan (jejaring) terbanyak ada di Facebook. Namun pada media sosial ini pula setengah lebih pengguna tidak melakukan pengaturan khusus untuk orang yang bisa melihat postingan atau unggahan (55,5% pengguna Facebook mengatur aksesnya menjadi publik atau dapat dilihat orang di dalam dan di luar Facebook).
- TikTok, media sosial yang belakangan ini populer dan Twitter adalah medium paling terbuka. Lebih dari 70% pengguna dua media sosial ini tidak melakukan pengaturan khusus untuk orang yang bisa melihat unggahan mereka.
- Survei juga mengukur Pengetahuan Data Pribadi yang dihitung dari jumlah jawaban responden dari masing-masing kategori data pribadi umum dan data pribadi khusus. Secara umum dapat terlihat tingkat pengetahuan data pribadi umum lebih tinggi daripada data pribadi khusus.
- Mayoritas responden sudah mengetahui mengenai data pribadi (94,1%). Nomor Induk Kependudukan (NIK), merupakan data yang dianggap paling penting dan paling khawatir untuk disalahgunakan karena data NIK terintegrasi dengan banyak hal. Disusul data keuangan pribadi/perbankan dan juga data biometri.
- Tiga data pribadi yang dianggap paling aman untuk dibagikan adalah agama, jenis kelamin dan tanggal lahir. Padahal menurut Data Protection Act – UK, 1988, agama merupakan salah satu data pribadi sensitif. Namun, sebagian besar masyarakat merasa tidak khawatir jika dibagikan ke publik.
- Mayoritas responden (87,8%) membaca dan mengetahui kebijakan privasi saat membuka/menginstal aplikasi. Responden yang tidak memahami dan tidak mau membaca kebijakan pribadi kebanyakan beralasan kebijakan tersebut terlalu panjang, sehingga kesulitan memahami isinya.
- Secara umum responden menyadari bahwa memberikan akses data pribadi pada pihak ketiga dapat menjadi sesuatu yang berbahaya. Namun karena aplikasi tersebut dibutuhkan, responden biasanya memberikan akses terhadap data pribadinya.
- Hanya hampir dari setengah responden (48,8%) yang mengetahui atau membaca tentang RUU Pelindungan Data Pribadi, di mana mereka banyak mengetahuinya melalui media sosial dan portal berita daring. Kelompok



usia yang paling banyak mengetahui atau membaca RUU perlindungan pribadi adalah Gen Y (51,29%).

- Sistem perlindungan data di Indonesia dianggap cukup baik namun belum memadai (*mean score* 6,05/10), sehingga 93,2% responden menganggap perlu adanya institusi/lembaga yang mengatur dan mengawasi penerapan Undang-Undang Pelindungan Data Pribadi. Hal ini diperlukan ketika mengalami permasalahan terkait data pribadi, responden langsung mengetahui apa yang harus dilakukan dan ke mana mereka harus melapor atau mengajukan aduan.

### 7.3 Rekomendasi

Berdasarkan hasil riset tersebut, berikut beberapa hal yang dapat dilakukan untuk membangun kesadaran (*awareness*) upaya pelindungan data pribadi.

1. Terus meningkatkan kesadaran publik tentang pentingnya menjaga keamanan data pribadi melalui:
  - Pelatihan dengan tema, antara lain cara memahami kebijakan privasi aplikasi, menerapkan pengamanan berlapis pada aplikasi, selektif dalam menginstal aplikasi, dan cara menyikapi kebocoran data pribadi;
  - Sosialisasi mengenai instrumen yang terkait dengan pelindungan data pribadi. Pendekatan edukasi dapat diperluas dalam bentuk publikasi yang variatif (infografis, teks, dan video); dan
  - Diskusi publik di berbagai daerah dengan menghadirkan pembicara, antara lain dari Kemkominfo, kepolisian, dan pimpinan daerah setempat.
2. Pemilihan medium kampanye dapat menyesuaikan pada kecenderungan profil pengguna media. Jika melalui media sosial, generasi muda cenderung menggunakan media sosial yang lebih baru seperti TikTok & Instagram, sementara kelompok usia lebih dewasa lebih menggemari Facebook.
3. Fokuskan konten kampanye pada sejumlah temuan, seperti kerentanan Facebook yang cenderung terbuka atau tidak memiliki pengaturan privasi dibandingkan media sosial lain seperti Instagram. Sementara itu, jejaring pada media sosial Facebook cenderung lebih luas.
4. Mengkomunikasikan temuan survei sebagai strategi kampanye untuk memperingatkan kerentanan perilaku yang patut diduga rawan pencurian data.
5. Mengkaji dan melakukan antisipasi dengan temuan bahwa umumnya masyarakat menganggap agama bukan sebagai data pribadi yang prioritas untuk dibagikan, mengingat Indonesia yang sensitif pada gangguan intoleransi karena keberagamannya.

6. Bekerja sama dengan Otoritas Jasa Keuangan (OJK) dan lembaga lainnya untuk mengedukasi batasan akses aplikasi agar terhindar dari pencurian data. Langkah OJK mengenalkan Camilan (*camera, microphone, location*) dapat menjadi salah satu materi mengenalkan pentingnya batasan akses saat mengunduh aplikasi.
7. Sebagian besar masyarakat sudah mengetahui bahwa NIK dan data perbankan merupakan data pribadi dan penting untuk dilindungi. Oleh karena itu, RUU Pelindungan Data Pribadi perlu segera disahkan untuk menghindari berbagai modus penyalahgunaan data pribadi seperti penipuan berkedok pinjaman *online*.
8. Menggiatkan publikasi RUU Pelindungan Data Pribadi di media sosial dan portal berita daring. Hal ini karena masyarakat paling banyak mendapatkan informasi mengenai rancangan aturan itu melalui kedua media tersebut.
9. Seluruh provinsi Indonesia tak luput dari kasus kebocoran data pribadi. Sudah 3.246 orang di 34 provinsi mengaku pernah menjadi korban kebocoran data. Maluku Utara, Kepulauan Bangka Belitung, Kalimantan Utara, Sulawesi Barat, Papua Barat dan Maluku menjadi daerah yang perlu mendapatkan perhatian karena kasus terbanyak dilaporkan dari provinsi-provinsi tersebut. Namun, kampanye secara umum nasional tetap perlu dilakukan.



