KECENDERUNGAN KEBEBASAN DIGITAL DALAM PEMERINTAHAN PRABOWO SUBIANTO-GIBRAN RAKABUMING RAKA

THE TRENDS OF DIGITAL FREEDOM UNDER THE PRABOWO SUBIANTO-GIBRAN RAKABUMING RAKA REGIME

Oleh:
Shinta Ressmy Cakra Ningrat
NPM. 170820220007

TESIS
Untuk memenuhi salah satu syarat ujian
guna memperoleh Magister Ilmu Politik
Program Studi Ilmu Politik

PROGRAM PASCASARJANA
FAKULTAS ILMU SOSIAL DAN ILU POLITIK
UNIVERSITAS PADJAJARAN
BANDUNG
2026

LEMBAR PENGESAHAN

KECENDERUNGAN KEBEBASAN DIGITAL DALAM PEMERINTAHAN PRABOWO SUBIANTO-GIBRAN RAKABUMING RAKA

THE TRENDS OF DIGITAL FREEDOM UNDER THE PRABOWO SUBIANTO-GIBRAN RAKABUMING RAKA REGIME

Oleh:
Shinta Ressmy Cakra Ningrat
NPM. 170820220007

USULAN PENELITIAN TESIS
Untuk memenuhi salah satu syarat ujian guna memperoleh Magister Ilmu Politik
Program Studi Ilmu Politik

Telah disetujui oleh Tim Pembimbing pada tanggal seperti tertera di bawah ini

Bandung Juli 2026

Menyetujui,

Tim Pembimbing

Ketua Pembimbing	Anggota Pembimbing
Prof. Dr. Caroline Paskarina, S.IP., M.Si	**Dra. Mudiyati Rahmatunisa, M.A., Ph.D**
NIP. 19770326 200604 2 001	**NIP. 19690509 199403 2 001**

Mengetahui,
Ketua Program Studi Pascasarjana Ilmu Politik

Ari Ganjar Herdiansah, S.Sos., M.Si., Ph.D
NIP. 19801225 201504 1001

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa:

1. Karya tulis saya, Tesis ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik magister baik di Universitas Padjadjaran maupun di perguruan tinggi lainnya.

2. Karya tulis ini murni gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan Tim Pembimbing.

3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

4. Pernyataan ini saya buat dengan sesungguhnya, dan apabila dikemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya tulis ini, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi ini.

Bandung, 31 Juli 2026
Yang Membuat Pernyataan,



Shinta Ressmy Cakra Ningrat
NPM. 170820220007

ABSTRAK

Penelitian ini menguji mengenai kebebasan digital di masa pemerintahan Prabowo Subianto dan Gibran Rakabuming Raka. Penelitian ini dilatarbelakangi oleh berbagai peristiwa pelanggaran hak digital, yaitu hak atas rasa aman di ruang digital, kebebasan berekspresi di ruang digital, dan pelanggaran rasa aman di ruang digital. Pelanggaran tersebut secara konsisten mengalami peningkatan sejak beberapa tahun terakhir. Hal ini juga dipengaruhi oleh legitimasi yang dilakukan oleh negara melalui berbagai instrumen. Penelitian ini menggunakan beberapa teori, untuk menganalisis pola dan tingkat keparahan pelanggaran dan kecenderungan kebebasan digital di masa pemerintahan Prabowo-Gibran. Adapun teori tersebut antara lain adalah Roberts (2013) untuk mengukur cakupan sasaran dan melihat siapa korban yang paling terdampak serta melihat bagaimana ketakutan, gesekan, dan banjir informasi mempengaruhi kebebasan digital, kemudian teori Balkin (2018) dan mengenai peran negara beserta dengan platform dan hubungannya dengan masyarakat sipil, teori Deiber (2015) untuk mengukur bagaimana diga generasi kontrol bekerja dan terakhir ialah teori Schauer (1978) untuk melihat dampak yang terjadi di masyarakat sipil. Penelitian ini menghasilkan kesimpulan adanya kecenderungan kebebasan digital pada masa pemerintahan Prabowo Subianto-Gibran Rakabuming Raka ialah ruang digital Indonesia pada periode ini menyempit dan bersifat regresif .

Kata Kunci: kebebasan digital, otoritarianisme digital, *chilling effect*, pelanggaran hak digital, represi digital

ABSTRACT

This research examines digital freedom during the administration of Prabowo Subianto and Gibran Rakabuming Raka. The study is motivated by various incidents of digital rights violations, specifically concerning the right to security in the digital space, freedom of expression in the digital sphere, and violations of a sense of safety in digital environments. These violations have consistently escalated in recent years, a trend further influenced by the state's legitimization through various instruments. This study employs several theories to analyze the patterns and severity of these violations, as well as the trajectory of digital freedom during the Prabowo-Gibran administration. These theoretical frameworks include Roberts (2013) to measure the scope of the targets, identify the most affected victims, and examine how fear, friction, and information flooding impact digital freedom; Balkin (2018) to analyze the role of the state and platforms in relation to civil society; Deibert (2015) to assess how the three generations of control operate; and Schauer (1978) to observe the subsequent impacts on civil society. The research concludes that the trajectory of digital freedom during the administration of Prabowo Subianto and Gibran Rakabuming Raka indicates a shrinking and regressive digital space in Indonesia.

Keywords: digital freedom, digital authoritarianism, chilling effect, digital rights violations, digital repression

KATA PENGANTAR

Puji dan syukur peneliti panjatkan atas berkat dan karunia Allah SWT, peneliti dapat menyelesaikan tugas akhir berupa tesis yang berjudul "Kecenderungan Kebebasan Digital di Masa Pemerintahan Prabowo Subianto-Gibran Rakabuming Raka" sebagai salah satu syarat untuk memperoleh gelar Magister pada Program Studi Ilmu Politik Universitas Padjadjaran. Penelitian ini menganalisis pola pelanggaran hak digital dan melihat arah kebebasan digital selama satu setengah tahun masa pemerintahan Prabowo Subianto dan Gibran Rakabuming Raka. Peneliti berharap riset ini dapat memberikan kontribusi pada perkembangan ilmu pengetahuan dan teknologi. Lebih jauh lagi, penelitian ini adalah bentuk dukungan kepada seluruh pihak yang tak henti dan tak kenal lelah melawan penindasan.

Peneliti menyadari bahwa penelitian ini jauh dari kata sempurna, banyak kekurangan dalam penelitian ini yang menjadi tanggung jawab penulis. Peneliti sangat menerima berbagai kritik dan saran sebagai bagian dari upaya dan proses perbaikan diri dan pengembangan kemampuan riset di masa yang akan datang. Pada prosesnya, peneliti mendapat banyak dukungan, bantuan, dan kepercayaan dari berbagai pihak. Ini menjadi salah satu proses panjang dan penting dalam hidup peneliti, untuk itu, peneliti mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Dr. Ari Ganjar Herdiansah, S.Sos., M.Si selaku Kepala Departemen Ilmu Politik Fakultas Ilmu Sosial dan Ilmu Politik dan Ketua Program Studi Pascasarjana Ilmu Politik di Universitas Padjadjaran;

2. Dr. Caroline Paskarina, S.IP., M.Si dan Dra Mudiyati Rahmatunisa, M.A., Ph.D selaku dosen pembimbing yang selama ini penuh kesabaran dan keyakinan membimbing saya dari awal perkuliahan hingga akhir perkuliahan, terutama untuk membimbing pengerjaan tesis ini;
3. Dr. Yusa Djuyandi, S.IP., M.Si dan Dr. Mas Dadang Enjat Munajat, S.Si., MTI, selaku dosen penguji yang memberikan kritik dan saran untuk penelitian ini;
4. Seluruh dosen dan tenaga kependidikan di Program Studi Pascasarjana Ilmu Politik di Fakultas Ilmu Sosial dan Ilmu Politik Universitas Padjadjaran yang telah memberikan pelayanan dan pengetahuan;
5. Bapak Suratno, Ibu Nurhayati PL, dan Kakak Wahyu CN, selaku orang tua dan kakak yang selama ini memberikan dukungan dan pengorbanan yang tiada putus tiada henti kepada peneliti sehingga dapat menyelesaikan studi ini dengan cukup baik. Terima kasih untuk segala cinta dan kasihnya;
6. Teman-teman seperjuangan di Program Pascasarjana Ilmu Politik Universitas Padjadjaran, yang telah menjadi teman belajar dan diskusi yang menyenangkan
7. Rekan-rekan di Southeast Asia Freedom and Expression Network (SAFEnet) yang telah memberikan ruang kepada peneliti untuk belajar banyak hal dan mencoba banyak hal baru. Terima kasih untuk kepercayaan pada peneliti dan dedikasinya pada kerja-kerja advokasi dan kampanye pelanggaran hak digital di Indonesia dan Asia Tenggara;

8. Rekan-rekan aktivis, teman disabilitas dan masyarakat adat, terima kasih sudah berjuang sehingga memberikan peneliti kekuatan, harapan, dan tekad yang teguh untuk bersama-sama melawan penindasan dan ketidakadilan;
9. Kepada Ardy Wibisana, sebagai pasangan peneliti, terima kasih untuk dukungan dan kasih sayang yang diberikan. Terima kasih sudah menjadi rekan diskusi dan rekan berdebat yang baik untuk peneliti semoga banyak waktu kita untuk menjelajah lebih jauh;
10. Kepada Iin Valentine, Elsa Tiurma Tobing, dan Amalia Fitri, rekan peneliti kala berkeluh kesah, terima kasih sudah menyediakan telinga untuk mendengar. Terima kasih juga sudah menemani peneliti di masa sulit dan baik.

DAFTAR ISI

TESIS ..... **i**

LEMBAR PENGESAHAN ..... **ii**

LEMBAR PERNYATAAN ..... **iii**

ABSTRAK ..... **iv**

ABSTRACT ..... **v**

KATA PENGANTAR ..... **vi**

DAFTAR ISI ..... **ix**

DAFTAR TABEL ..... **xi**

DAFTAR GAMBAR ..... **xii**

BAB I PENDAHULUAN **1**

1.1 Latar Belakang Riset 1

1.2 Rumusan Masalah 20

1.3 Tujuan Penelitian 21

1.4 Manfaat Penelitian 21

1.4.1 Manfaat Teoritis 21

1.4.2 Manfaat Praktis 22

BAB II TINJAUAN PUSTAKA **23**

2.1 Kebebasan Digital 23

2.2 Dimensi Kebebasan Digital 28

2.3 Otoritarianisme Digital 31

2.4 Kerangka Pemikiran 34

BAB III METODE PENELITIAN **37**

3.1 Pendekatan Riset 37

3.2 Penentuan Sumber Data 38

3.3 Teknik Pengumpulan Data 39

3.3.1 Studi dokumentasi dan literatur 40
3.4 Data Set 40
3.5 Teknik Analisis Data 42
3.5.1 Reduksi data 42
3.5.2 Penyajian data 42
3.5.3 Penarikan Kesimpulan 43
3.6 Teknik Validitas Data 43
3.7 Jadwal Penelitian 44
BAB IV PENGATURAN KEBEBASAN DIGITAL DI INDONESIA 45
4.1 Deskripsi Pengaturan Kebebasan Digital di Indonesia 45
4.2 Kecenderungan Kebebasan Digital dalam Masa Pemerintahan Prabowo Subianto-Gibran Rakabuming Raka 51
4.3 Analisis Dimensi Jumlah 53
4.4 Analisis Jenis Pelanggaran Hak Digital 67
4.5 Analisis Cakupan Sasaran Pelanggaran Hak Digital 80
4.6 Analisis Aktor Pelanggaran Hak Digital 95
4.7 Analisis Instrumen yang Digunakan untuk Pelanggaran Hak Digital 101
4.8 Analisis Dampak Keparahan Pelanggaran Hak Digital 108
BAB V KESIMPULAN DAN SARAN 117
5.1 Kesimpulan 117
5.2 Saran 119
DAFTAR PUSTAKA 121

DAFTAR TABEL

Tabel 3.1 Data Set 41

Tabel 3.2 Jadwal Penelitian..... 44

Tabel 4.1 Pelanggaran Hak Akses Internet di Indonesia 2025..... 67

Tabel 4.2 Pelanggaran Akses Internet di Indonesia tahun 2026 68

Tabel 4.3 Jenis Pelanggaran Kebebasan Berekspresi Berdasarkan Latar Belakang Kasus tahun 2025-2026..... 70

Tabel 4.4 Serangan Digital Berdasarkan Jenis pada 2025-2026 72

Tabel 4.5 Kasus KBGO di Indonesia 2025-2026..... 76

Tabel 4.6 Latar Belakang Korban Pelanggaran Kebebasan Berekspresi 2025-2026..... 84

Tabel 4.7 Latar Belakang Serangan Digital 2025-2026 87

Tabel 4.8 Kasus KBGO 2025-2026 92

Tabel 4.9 Operasionalisasi Otoritarianisme Digital di Indonesia 2024-2026 .. 108

DAFTAR GAMBAR

Gambar 4.1 Insiden per Kategori Q4 2024 54

Gambar 4.2 Gangguan Akses Internet per Jenis – Q4 2024 54

Gambar 4.3 Tren Insiden Per Kategori 2015 58

Gambar 4.4 Teguran X kepada pengguna atas permintaan Komdigi 62

Gambar 4.5 Tren Insiden Per Kategori 2026 63

Gambar 4.6 Bukti Pengancaman Terhadap Jurnalis 66

Gambar 4.7 Pemberitahuan di akun @cabinetcouture_idn..... 69

BAB I

PENDAHULUAN

1.1 Latar Belakang Riset

Demokrasi kontemporer mengalami transformasi struktural ketika ruang digital tidak lagi sekadar menjadi saluran tambahan, melainkan bergeser menjadi arena utama tempat ekspresi politik diartikulasikan, informasi diproduksi dan didistribusikan, serta relasi antara negara dan warga dinegosiasikan. Pergeseran ini berlangsung seiring perkembangan teknologi yang kian pesat dan meningkatnya penetrasi penggunaan internet di dunia, tak terkecuali di Indonesia.

Penggunaan internet kini tidak berhenti pada penyebaran dan penerimaan informasi secara satu arah, melainkan telah menjelma menjadi arena bagi warga untuk mengartikulasikan pilihan dan pandangan politiknya. Pada saat yang sama, pemerintah turut memanfaatkan ruang digital untuk berinteraksi dengan masyarakat, menyampaikan produk kebijakan, menjalankan kampanye politik, hingga menyaring aspirasi warga terhadap arah pembangunan negara dan pemerintahan. Namun, pergeseran ini bersifat konstitutif dan bermata dua: *platform* digital turut membentuk cara publik mendeliberasi, memobilisasi tuntutan, dan mengawasi kekuasaan, sekaligus membuka celah bagi bentuk-bentuk kontrol dan manipulasi baru seperti pengawasan negara, disinformasi terorganisir, hingga penyempitan ruang sipil melalui regulasi konten.

Diamond (2010) menyebut teknologi ini sebagai *liberation technology*, yaitu sarana yang memperluas kapasitas warga untuk mendokumentasikan

penyalahgunaan kekuasaan, menuntut akuntabilitas, dan memobilisasi gerakan sosial dengan kecepatan serta jangkauan yang tidak dimungkinkan era sebelumnya. Dalam kerangka (Balkin, 2003), perubahan ini menyentuh inti tujuan kebebasan berekspresi itu sendiri, yaitu teknologi digital memungkinkan warga biasa berpartisipasi secara setara dalam pembentukan makna dan wacana publik yang mengatur hidup mereka, suatu kondisi yang disebutnya *democratic culture.* Karena adanya perpindahan arena dari fisik ke digital, maka kebebasan digital tidak hanya dipahami sebagai kemajuan teknologi semata, melainkan bagian dari kualitas demokrasi kontemporer. Ketika akses informasi, ekspresi politik, dan pengorganisiran kolektif berlangsung secara digital, maka pembatasan terhadap ruang tersebut seperti pemblokiran akses informasi, kriminalisasi ekspresi, pengawasan tanpa akuntabilitas, dan manipulasi informasi dapat diklam sebagai bagian dari gejala penurunan kualitas partisipasi dan akuntabilitas yang menjadi salah satu indikator demokrasi (Feldstein, 2021). Dewan HAM PBB sudah mneyatakan bahwa hak-hak yang ada pada ruang fisik juga berlaku di ruang digital, termasuk segala bentuk perlindungannya (UN Human Rights Council, 2012). Lembaga pemeringkat atau yang melakukan penilaian terhadap demokrasi suatu negara kini menjadikan kebebasan di internet sebagai salah satu indikator tersendiri dalam menilai kondisi demokrasi suatu negara(Freedom House, 2025).

Konsep kebebasan digital yang ada saat ini dominan dibangun oleh pengalaman yang terjadi di *global north*, sehingga acuan dan standar yang digunakan juga mengikuti negara *global north*. Contohnya adalah *Freedom on The Net* yang mengeluarkan indeks kebebasan digital dengan acuan dari pembangunan

infrastruktur yang merata, negara hukum yang sudah progresif dan ideal, subjek hukum yang sudah pasti dan pemerintahan dari negara yang sudah berkapasitas untuk melangsungkan kebijakan terkait ruang digital. Akan tetapi, penilaian demokrasi di negara-negara *global south* tanpa adanya penyesuaian konsep dan indikator perlu dihindari karena secara mendasar karakteristik negara tersebut sangat berbeda(Harindranath & Gómez-Cruz, 2023). Penyesuaian harus dilakukan menimbang adanya keadilan secara epistemik, bahwa pengalaman digital warga di selatan dan utara berbeda dan tidak diwakili oleh kondisi objektif satu sama lain, termasuk pada probduksi pengetahuan dan metodologi yang digunakan (Gómez-Cruz et al., 2023)

Kajian kebebasan digital di *global south* perlu diadopsi dengan pendekatan dekolonial, kontekstual, dan partisipatif yang menempatkan posisi subjek lokal dan realitas sosial-budaya sebagai bagian dari unit analisis (Das, 2026; J. B. Y. Lim, 2025). Pada tataran Asia Tenggara, dapat dilihat bahwa dinamika kebebasan digital dibentuk oleh interaksi khas antara budaya lokal, represi negara dan budaya algoritmik *platform* yang tidak serupa dengan negara di *global north*, contohnya adalah aktivisme berbasis pembuatan *meme* dan solidaritas transnasional *Milk Tea Alliance* yang terjadi karena kesamaan kondisi dan kesamaan bentuk represi yang dilegitimasi negara, hingga adanya kontrol internet yang dilegitimasi melalui jalur politik dan hukum (Jalli, 2025; J. B. Y. Lim, 2025; Putra, 2024; Sinpeng, 2020; Yilmaz, 2023).

Konsekuensi dari perbedaaan situasi dan kondisi objektif tersebut adalah kebebasan digital di Indonesia tidak cukup dinilai dengan indikator yang dibuat

oleh *Freedom on the Net*, yang mana indeks tersebut dapat digunakan sebagai rujukan dasar namun untuk validitas penilaian harus mengacu paling tidak pada lima konteks utama, yakni, pertama karakter negara, kebijakan di Indonesia yang berpusat pada negara(Gumati, 2024). Kedua, adanya ketimpangan infrastruktur yang dipengaruhi oleh kondisi wilayah dan pembangunan sehingga berdampak pada tidak meratanya pembangunan, literasi, dan faktor sosio-demografis warga (Jaya et al., 2024; Rajagukguk et al., 2024). Ketiga, sistem hukum di Indonesia, yang menunjukkan bahwa regulasi digital di Indonesia masih terfragmentasi dan adanya UU ITE menunjukkan bahwa penegakan hukum masih lemah karena payung hukum ini masih multitafsir (Rahmazani, 2022; Utomo, 2025). Keempat, budaya *platform* yang ditunjukkan dengan algoritma TikTok dan Instagram memediasi visibilitas sekaligus risiko aktivisme, sehingga membentuk pola ekspresi yang khas (Jalli, 2025; M. Lim, 2023). Kelima, praktik masyarakat sipil yang menunjukkan adanya bentuk resiliensi kebebasan digital Indonesia justru banyak ditopang aliansi aktivis, media, dan organisasi masyarakat sipil yang membangun *connective resilience* di tengah represi (Masduki & Wendratama, 2025; Rahayu et al., 2024; Utami, 2026).

Indonesia memiliki karakter digital yang spesifik dan dipengaruhi oleh beberapa hal, pertama letak geografis luas dan berbentuk gugusan ribuan kepulauan sehingga pembangunan infrastrukturnya tidak merata. Kedua, adanya perbedaan ketimpangan konektivitas urban-rural yang konsisten sehingga penetrasi internet nasional yang mencapai 79,5 persen (APJII, 2024) menyembunyikan perbedaan tajam dalam kualitas dan keandalan akses antarwilayah (Jaya et al., 2024). Ketiga,

literasi digital yang tidak sama antara satu warga dengan warga lainnya, hal ini dipengaruhi oleh gender, usia, pendidikan, pendapatan, dan lokasi (Rajagukguk et al., 2024). Keempat, regulasi ruang digital yang masih terfragmentasi, tidak hanya pada tataran perundang-udangan, melainkan juga pada level lembaga yang lebih rendah, termasuk koordinasi antar lembaga tersebut yang masih belum rigid (Utomo, 2025). Kelima, ruang digitalnya disediakan dan didominasi oleh *platform* global, seperti aplikasi Whatsapp yang digunakan sebagai aplikasi perpesanan yang paling banyak digunakan, termasuk juga media sosial seperti Instagram dan TikTok, ini berindikasi pada kondisi yang mengharuskan pengguna untuk patuh pada keputusan dan peraturan yang sudah dibentuk oleh korporasi asing (Balkin, 2018; Gillespie, 2018). Keenam, negara masih mengandalkan cara-cara hukum pidana untuk menertibkan ruang digital, jarang untuk menggunakan instrument administratif dan perdata sehingga kemungkinan kriminalisasi sangat tinggi (SAFEnet, 2026). Terakhir, organisasi masyarakat sipil atau kolektif masyarakat sipil juga memiliki daya lenting kebebasan digital yang cukup kuat, dibuktikan dengan proses pemantauan, pendampingan korban, dan advokasi yang dilakukan (Masduki & Wendratama, 2025; Rahayu et al., 2024).

Ketimpangan akses menjadi persoalan yang paling dasar dan juga dominan, yang melahirkan kondisi koneksi yang tidak stabil, sehingga informasi yang diterima satu warga dengan yang lainnya tidak sama. Selain itu ini juga akan menentukan biaya akses yang relatif lebih tinggi di wilayah yang pembangunannya cenderung tertinggal (R. Handayani & Afrizal, 2018; Jaya et al., 2024). Konektivitas, kualitas, jaringan, perangkat, dan keterjangkauan yang akan

membentuk bagaimana warga bisa tersambung dan berpartisipasi di ruang digital, termasuk dalam aktivitas untuk menyampaikan pendapat dan berinteraksi secara sosio-politik dan kultural di ruang digital. Pada penelitian ini, penjelasan mengenai infrastruktur hanya akan menjelaskan konteks, bukan objek utama penelitian.

Akses internet dalam konteks kebebasan digital hanyalah bagian awal yang menentukan apakah hak digital bagi warga dapat diterapkan atau tidak. Akses internet merupakan bagian dari sumber daya yang dapat digunakan untuk menuju kebebasan digital, sementara itu bagian lainnya yang tidak kalah penting adalah literasi digital (Sen, 1999). Kajian kewargaan digital di Asia Tenggara menunjukkan partisipasi warga di ruang digital akan menjadi bermakna apabila di ruang digital dapat terjamin keamanan, kemampuan pengguna untuk menilai informasi yang diterima secara kritis dan menerapkan etika dalam berinteraksi (Hunawa et al., 2025; Yue et al., 2019). Literasi digital akan membantu pengguna untuk melindungi data pribadi, menilai ancaman, dan melakukan mekanisme banding kepada *platform*, seperti mekanisme keberatan pada kasus penghapusan konten, sementara mekanisme tersebut biasanya hanya bisa diakses oleh mereka yang paham dan mengetahui prosedurnya (Gillespie, 2018). Pada sisi yang lain, literasi digital juga dapat membantu pengguna untuk mengadvokasi apa yang dialami, misalnya dengan mendokumentasikan pelanggaran hak digital dan ini juga selaras bahwa literasi digital akan mengurangi risiko pengguna di ruang digital.

Dalam beberapa tahun terakhir, pemerintah Indonesia gencar menggunakan terminologi kedaulatan digital untuk melakukan justifikasi kontrol ruang digital, terutama untuk mengontrol *platform* dan aliran data secara digital (Komdigi,

2025). Bagi negara *global south*, kedaulatan digital merupakan bagian dari respons atas relasi pemerintahan atau negara dengan korporasi teknologi global yang juga berpengaruh pada infrastruktur, ekosistem data dan *platform* yang dikuasai oleh *platform* asing yang beroperasi lintas yurisdiksi sehinga kekhawatiran negara terkait dengan kehilangan kendali atas ruang hidup pengguna secara digital mejadi valid (Liu & Song, 2026).

Kebijakan mengenai Penyelenggara Sistem Elektronik (PSE) berupa kewenangan pemblokiran, permintaan data pengguna, pembatasan penggunan, serta perintah untuk penurunan konten dapat berubah menjadi *regulatory overreach* ketika hal tersebut tidak berjalan akuntabel dan tidak proporsional, mulai dari penerapan regulasi hingga pengawasan dan sistem hukuman (Gumati, 2024). Balkin (2018) menemukan bahwa ancaman pemblokiran akses dan konten bagi *platform* yang tidak mendaftar PSE menjadikan pengguna seperti sandera, terlebih bagi mereka yang bergantung pada aplikasi tersebut, hal itu juga menjadikan *platform* untuk bertindak menghapus konten pengguna secara berlebihan untuk menjaga rasa aman yang diinginkan oleh pemerintah atau biasa juga dikenal sebagai *collateral censorship*.

Permintaan data pengguna juga dinilai sebagai bagian dari pengawasan yang bersifat politis, seperti halnya penangguhan izin aplikasi TikTok di Indonesia yang berujung pada penyerahan data pengguna terkait dengan demonstrasi Agustus 2025 menunjukkan kontrol atas warga atau pengguna yang dibalut dalam konsep kedaulatan digital, alih-alih melindungi privasi warga atau pengguna (Freedom House, 2025).

Inilah kepentingan yang saling beradu satu sama lain, yaitu perlindungan kepentingan nasional yang diklaim harus dilakukan oleh negara termasuk melalui legitimasi hukum. Dalam hal otonomi *platform*, yakni ketika *platform* memiliki pedoman komunitas sendiri yang dapat dijadikan acuan untuk melakukan moderasi konten, tetapi ketika negara ikut campur dalam mengatur proses moderasi konten maka *platform* kehilangan otonominya dalam melakukan tugas dan fungsinya kepada pengguna (Gillespie, 2018).

Kebebasan digital tidak semata bergantung pada ada atau tidaknya larangan untuk berekspresi namun juga pada perlindungan data dan keamanan warga atau pengguna di ruang digital (SAFEnet, 2025b). Warga atau pengguna akan berpartisipasi penuh dan berinteraksi di ruang digital hanya apabila dapat dijamin rasa aman dan kebebasannya melalui hukum atau regulasi yang sah dari negara maupun *platform*. Glasius & Michaelsen (2018) menilai pelanggaran keamanan digital termasuk praktik illiberal yang mana berupa pelanggaran atas otonomi dan martabat individu yang kemudian bekerja beriringan dengan praktik otoriter dalam menyempitkan ruang sipil. Bukti empiris menunjukkan bahwa pengawasan saja, tanpa penindakan, sudah cukup menggentarkan perilaku yang sah (Penney, 2016) sementara itu rasa tidak aman adalah mekanisme *chilling effect* yang paling sunyi. Bentuk pelanggaran hak digital dapat berbeda-beda, mulai dari serangan yang menyasar individu seperti *doxing*, atau pengungkapan identitas dan data pribadi untuk mengintimidasi korban, peretasan perangkat dan akun. SAFEnet (2026) mencatat bahwa serangan ini menyasar kelompok berisiko tinggi seperti jurnalis, aktivis, dan pengkritik tepat setelah mereka menyampaikan kritik di ruang digital

sementara pelaku nyaris tidak pernah diusut tuntas melalui mekanisme hukum yang berlaku. Ini menjadi pola yang terus berulang selama beberapa tahun terakhir. Dibuktikan dengan adanya konsistensi korban yang didominasi aktivis, jurnalis, kelompok masyarakat sipil sebanyak 42,8% dari 326 korban pada 2022 dan pada Agustus 2024 di bulan Agustus bertepatan dengan momentum #peringatandarurat terdapat 40 insiden yang menyasar kelompok aktivis, jurnalis dan kelompok masyarakat sipil, sementara di 2025 terdapat 65 kasus dalam 12 hari berkenaan dengan momentum demonstrasi kenaikan tunjangan DPR (SAFEnet, 2023, 2025b, 2026).

Pelanggaran hak digital yang lebih luas dapat dilihat pada praktik yang terstruktur dan terorganisir, dilegitimasi oleh hukum, misalnya penggunaan patrol siber untuk melakukan pemantauan di ruang digital atau penggunaan *spyware* yang *invasive* tanpa akuntabilitas yang jelas (Amnesty International, 2024). Feldstein (2021) menyatakan bahwa represi digital sulit untuk dibuktikan karena warga atau pengguna akan menilai itu sebagai tindakan yang samar dan sulit untuk diatribusikan sementara negara dapat melakukan hal tersebut dengan kendali penuh. Kondisi tersebut diperparah karena Indonesia belum memiliki mekanisme perlindungan data pribadi yang kuat, misalnya melalui lembaga independen yang menjadi pengawas perlindungan data pribadi di Indonesia (CNN Indonesia, 2024). Risiko yang terjadi di ruang digital hampir sepenuhnya masih ditanggung oleh warga atau pengguna tanpa mereka mengetahui cara pemulihan yang efektif.

Gillespie (2018) menilai bahwa moderasi konten adalah komoditas inti *platform* yang dilakukan melalui rangkaian dan mekanisme yang tersembunyi dari

publik, *platform* dapat menentukan konten apa yang dapat dilihat oleh warga atau pengguna, ini biasa juga dikenal sebagai algoritma. *Platform* juga memiliki acuan yang disebut sebagai pedoman komunitas yang menjadi dasar *platform* untuk melakukan moderasi konten. Algoritma di satu sisi dapat memperluas jangkauan aktivisme digital yang dilakukan warga atau pengguna seperti adanya tren *meme* dan *spill the tea* yang biasanya dilakukan untuk membuat *viral* suatu isu yang biasanya tidak dijangkau oleh media konvensional (Jalli, 2025; M. Lim, 2023). Namun di sisi lain juga meningkatkan risiko keamanan warga atau pengguna yang melakukan aktivisme publik di ruang digital (Jalli, 2025). Pendengung juga berperan untuk memanipulasi informasi di ruang digital (*flooding*) sehingga isu berpotensi menjadi bias atau justru tertutup sepenuhnnya (Wijayanto et al., 2021). *Platform* dapat melakukan invisibilisasi konten secara senyap melalui penurunan peringkat atau *shadow banning*, bentuk sensor yang paling sulit dibuktikan justru karena tidak meninggalkan jejak penghapusan (Chaka, 2022; Gillespie, 2018). Hal-hal tersebut menjadikan aktivitas warga atau pengguna mengalami sensor yang nyata.

Kondisi umum ruang digital sebelum penetapan Prabowo Subianto dan Gibran Rakabuming Raka sebagai presiden dan wakil presiden sebenarnya sudah menunjukkan gejala praktik pengendalian ruang digital. Pada tataran hukum, terdapat UU ITE yang selama satu decade sudah digunakan sebagai insturmen utama kriminalisasi ekspresi di ruang digital, meskipun sudah dua kali mengalami revisi, pasal multitafsir tidak hilang secara keseluruhan, terutama pada pencemaran nama baik dan penyebaran berita bohong. SAFEnet (2025b) memantau terdapat

146 kasus pelanggaran kebebasan berekspresi dengan total 170 korban. Adapu sebaran pengguna pasal UU ITE adalah pemegang kekuasaan dan yang menjadi subjek kriminalisasi adalah kelompok berisiko tinggi seperti aktivis dan jurnalis, di antaranya adalah Fatia Maulidiyanti dan Haris Azhar yang dituntut secara pidana oleh Luhut Binsar Panjaitan setelah keduanya meriset soal keterlibatan Luhur dalam proyek di Papua (Freedom House, 2024).

Pada tataran teknis, negara telah melakukan pembatasan akses internet, contohnya adalah *internet shutdown* di Papua pada 2019. Ini dibuktikan dengan adanya putusan bahwa Joko Widodo terbukti bersalah dan melanggar hak digital warga Papua yang dibuktikan dengan putusan Pengadilan Tata Usaha Negara (Freedom House, 2024). Aparatus dan sistem pemblokiran konten rutin beroperasi sejak adanya Permenkominfo 5/2020 yang kemudian juga diperkuat mengenai keputusan bahwa seluruh *platform* yang beroperasi di Indonesia wajib mendaftar PSE, apabila tidak mandaftar maka akan dikenakan sanksi berupa pemblokiran, dibuktikan dengan pemblokiran serentak pada 2022 karena beberapa aplikasi terlambat mendaftar PSE (Gumati, 2024).

Pergantian kekuasaan tidak berarti secara otomatis mengubah kebebasan digital menjadi lebih baik. Masing-masing lembaga negara, perangkat hukum, teknis, dan sistem birokrasinya tidak berubah sedemikian rupa, melainkan cenderung bekerja mengikuti kebiasaan yang sudah berjalan sekian lama. Demikian dapat dilihat bahwa kebebasan digital bukan retorika sebuah pemerintahan, melainkan tindakan konkret yang berlangsung di bawah pemerintahan tersebut (Glasius & Michaelsen, 2018)

Perbandingan lintas negara juga menunjukkan bahwa represi digital lazim diwariskan dan bahkan menguat justru pada masa transisi kekuasaan, ketika pemerintahan baru menghadapi ujian legitimasi pertamanya (Feldstein, 2021). Berkenaan dengan kencenderungan kebebasan digital di masa pemerintahan Prabowo-Gibran, maka terdapat beberapa kemungkinan, yakni pertama, kontinuitas, intensitas pembatasan akan berjalan sebagaimana sebelumnya, hanya saja berganti pemain. Kedua, intensitas penggunaan instrumen represi yang sudah digunakan sebelumnya akan lebih sering, misalnya penggunaan pasal multitafsir yang lebih sering digunakan untuk melakukan kriminalisasi pada ekspresi warga atau pengguna. Ketiga, perubahan bentuk, sebelumnya represi dilakukan secara jelas misalnya dengan penjemputan paksa jurnalis yang melakukan pemberitaan terkait kasus tertentu akan berubah menjadi lebih halus, misalnya dengan tekanan kepada *platform* untuk menyesuaikan algoritma pengguna sesuai dengan yang diminta oleh pemerintah.

Pada tahun 2024-2026, pembatasan internet tidak ditemukan seperti halnya yang terjadi di Papua pada 2019 yang terjadi pemadaman internet secara total, melainkan terjadi pembatasan akses, pembatasan fitur, penangguhan akun, hingga moderasi konten yang berlebihan dan tidak proporsional terhadap beberapa situs, di antaranya adalah sebagaimana tercantum pada tabel berikut.

Tabel 1.1 Kasus Kunci Pembatasan Akses Internet 2025

Kasus	Jenis Pembatasan	Durasi	Aktor	Justifikasi
Pemblokiran archive.org (Mei 2025)	Pemblokiran situs	+/- 2 pekan	Komdigi	Konten perjudian dan pornografi
Penonaktifan fitur live TikTok (30 Agustus 2025)	Pembatasan fitur live	+/- 3 hari	TikTok	Konten perjudian dan scam
Penangguhan izin TikTok dan penyerahan data (September-Oktober 2025)	Tekanan perizinan dan penyerahan data	Izin akan dipulihkan setelah data diserahkan	Komdigi	Kepatuhan hukum dan investigasi pasca aksi
Penangguhan akun dan moderasi berlebihan (Agustus-September 2025)	Pembatasan akun dan penghapusan konten	Selama masa demonstrasi Agustus dan setelahnya	Platform (Instagram, X, TikTok) sebagian atas permintaan pemerintah	Pelanggaran pedoman komunitas

Sumber: (Freedom House, 2025; Kompas, 2025; SAFEnet, 2025b; Tempo, 2025a)

Sejalan dengan apa yang sudah disebutkan pada tabel sebelumnya, bahwa kriminalisasi terhadap ekspresi yang terjadi di unggahan media sosial juga meningkat. SAFEnet mencatat 351 kasus kriminalisasi ekspresi di sepanjang 2025. Temuan ini selaras dengan apa yang diungkapkan oleh King et al. (2013) yang menyatakan bahwa sensor utamanya akan menyasar kolektif yang melakukan aksi di ruang digital, dibuktikan dengan Khariq Anhar yang ditangkap di bandara setelah mengunggah kampanye aksi melalui akun Instagram dan dikenakan pasal 32 dan 35 UU ITE (SAFEnet, 2025b). Pasca demonstrasi, polisi siber melakukan operasi senyap, yakni perburuan di ruang digital terhadap para demonstran yang dilakukan

dengan permintaan data kepada platform dan penelusuran akun. Selain orang yang melakukan aksi di ruang digital, terror juga menyasar jurnalis Tempo yang menerima kiriman berupa kepala babi pada 19 Maret 2025 dan enam bangkai tikus tanpa kepala pada 22 Maret 2025. Terror tersebut juga dibersamai dengan *doxing* dan kampanye negatif berbasis rekayasa AI yang mana ini adalah bentuk intimidasi jurnalis yang dilakukan secara sistemik karena proses penyelesaian dan pemulihannya tidak berjalan baik (AJI, 2025). Band *punk* anonim Sukatani juga mendapat teror, penangkapan, dan pemaksaan penarikan lagu "Bayar, Bayar, Bayar" yang semula lagu tersebut ditujukan pada praktik korup yang dilakukan pihak kepolisian, tak hanya itu, mereka juga mendapat tekanan untuk mengungkap identitas dan meminta maaf secara publik (Tempo, 2025b). Namun demikian akhirnya lagu tersebut tetap menjadi simbol perlawanan pada momentum aksi demonstrasi Agustus 2025.

Langkah lain yang dilakukan oleh pemerintah adalah dengan melakukan penyensoran terhadap pemberitaan investigasi kasus Andrie Yunus, yang dikeluarkan oleh Magdalene.co. *Platform* melakukan pembatasan geolokasi sehingga konten tersebut tidak dapat dilihat di wilayah Republik Indonesia. Adapun pembatasan tersebut dilakukan atas dasar permintaan dari Komdigi sejak 3 April 2026 (BBC Indonesia, 2026). Padahal produk jurnalistik tersebut tidak dapat disensor begitu saja tanpa adanya mekanisme banding yang diajukan ke dewan pers.

Selama 25 Agustus-5 September 2025, SAFEnet mencatat adanya 65 kasus pelanggaran hak digital, sementara Tim Advokasi untuk Demokrasi (TAUD)

mencatat adanya 26 kasus gangguan akses dan 16 kasus moderasi konten yang berlebihan (*overmoderation*) (SAFEnet, 2025a; YLBHI, 2025). Konten yang mengalami moderasi konten secara berlebihan adalah konten yang berkaitan dengan aksi demonstrasi dan konten diturunkan dengan alasan memuat adegan kekerasan dan adanya upaya penghasutan (SAFEnet, 2025b). Sementara ini juga membuktikan bahwa bukti dan dokumentasi pelanggaran HAM hilang dari publik justru ketika publik membutuhkan hal tersebut. pengguna hanya menerima pemberitahuan general tanpa menyebut spesifik pedoman komunitas apa yang dilanggar atau pasal apa yang dilanggar dan tidak ada mekanisme banding dalam pemberitahuan tersebut. Ini memperkuat teori Gillespie (2018) bahwa *platform* menegasikan pengguna sebagai agen yang sebenarnya dapat dimintai pertanggungjawaban dari setiap tindakan yang dilakukan dan memperkuat mekanisme moderasi konten yang tidak proporsional dan akuntabel.

Komdigi juga melakukan pemanggilan terhadap TikTok dan META untuk membahas sistem algoritma yang banyak dilabeli banjir berita ujaran kebencian dan fitnah terhadap pemerintah, lalu beberapa hari kemudian terjadi *overmoderation* di Instagram, TikTok dan Youtube. Pihak pemerintah dan *platform* sama-sama menyangkal melakukan pengendalian informasi demonstrasi di ruang digital (Tempo, 2025a). Pemerintah juga memperketat pengaturan terhadap *platform* terutama melalui UU ITE pasal 40 yang menyatakan bahwa negara berwenang untuk mengatur pencegahan dan penanganan terhadap penyebaran informasi yang melanggar hukum. Pada 4 Maret 2026, Kantor Google dan META, yang menaungi Whatsapp, Facebook dan Instagram didatangi oleh Meutya Hafied dan jajaran

Komdigi (Wuragil, 2026). Adapun maksud dari sidak tersebut adalah untuk memastikan *platform* tersebut memenuhi kepatuhan terhadap regulasi nasional, yang sebelumnya dinilai sangat rendah yakni 28,47%.

Di sisi lain, intervensi yang dilakukan pemerintah di ruang digital tidak selamanya ditujukan untuk melakukan represi kepada pengguna. Terdapat regulasi yang bersifat protektif, seperti Peraturan Pemerintah Nomor 17 Tahun 2025 (PP Tunas) yang ditujukan untuk mengatur tata kelola sistem elektronik untuk perlindungan anak. Hal ini untuk menjawab permasalahan dan risiko yang dihadapi oleh 80 juta pengguna anak di ruang digital di Indonesia (Kompas, 2026a). PP Tunas dapat menjadi bukti bahwa bentuk perlindungan kepada warga dan pengguna anak di ruang digital memang dibutuhkan meskipun pada tahapan implementasinya belum menunjukkan adanya proporsi yang ideal dari tataran pemangku kebijakan hingga di tataran teknis.

SAFEnet (2026) yang menyatakan bahwa adanya lonjakan kasus dari tahun 2024 sebanyak 146 kasus ke tahun 2025 sebanyak 351 kasus tidak dengan sendirinya membuktikan bahwa kebebasan digital memburuk. Data pemantauan pelanggaran adalah data yang dilaporkan dan terpantau, bukan sensus atas seluruh pelanggaran yang terjadi, sehingga pergerakannya dipengaruhi faktor-faktor di sisi pengukuran itu sendiri. Terdapat beberapa faktor yang harus diperhitungkan seperti momen politik besar seperti demonstrasi Agustus 2025 mendorong lebih banyak korban melapor, sebagaimana tampak pada komposisi data SAFEnet atau faktor peningkatan kesadaran publik di mana warga yang semakin paham bahwa *doxing* atau peretasan adalah pelanggaran yang dapat dilaporkan akan lebih banyak

melapor. *Freedom on the Net* berguna sebagai pembanding makro karena metodologinya konsisten lintas negara dan lintas tahun, sehingga penurunan skor Indonesia dari 49 (2024) ke 48 (2025) dalam kategori *partly free* memberi konfirmasi independen bahwa arah pergerakan yang terekam data lokal juga terlihat dari luar (Freedom House, 2024, 2025). Namun sebagai indeks agregat nasional, ia secara struktural tidak menangkap hal yang justru krusial dalam kasus Indonesia, seperti kondisi hukum dan budaya hingga wilayah yang luas tidak disertai pembangunan yang merata.

Penelitian mengenai regulasi dan UU ITE, didominasi pendekatan hukum doktrinal. Studi-studi ini secara konsisten menunjukkan problem yang sama dari sudut yang berbeda yakni rumusan pasal yang multitafsir dan jangkauan kriminalisasi yang berlebihan (Astara, 2021), kebutuhan mempersempit frasa-frasa kunci Pasal 27 dari perspektif HAM (Astara, 2021), fragmentasi kerangka hukum digital dan arah reformasinya (Utomo, 2025), hingga posisi pemidanaan siber di persimpangan antara demokrasi digital dan otoritarianisme (E. P. Handayani et al., 2025). Kekuatan kelompok penelitian UU ITE ini adalah ketajaman analisis norma. Penelitian yang membahas represi dan otoritarianisme digital, datang terutama dari ilmu politik. Sinpeng (2020) memetakan kontrol internet di Asia Tenggara dan menempatkan Indonesia dalam pola regional sementara Yilmaz (2023) menelusuri legitimasi keagamaan atas otoritarianisme digital dengan Indonesia sebagai salah satu kasus. Lainnya seperti Wijayanto et al. (2026) membongkar infrastruktur operasi pendengung yang dibiayai negara, dan Margiansyah (2025) merumuskan digitalisasi otoritarianisme sebagai titik temu antara aktivisme sipil, represi digital,

dan erosi demokrasi. Kelompok penelitian ini dekat dengan pertanyaan penelitian yang dirumuskan peneliti, tetapi sebagian besar datanya berakhir sebelum peralihan kekuasaan 2024. Gumati (2024) menganalisis kebijakan pendaftaran *platform* sebagai dilema antara kedaulatan digital dan *regulatory overreach*, selain itu Tobing (2026) membandingkan inovasi kebijakan berbasis *platform* di Indonesia, Filipina, dan Thailand, kemudian Liu & Song (2026) menempatkan model kedaulatan digital Indonesia dalam peta kolonialisme digital *Global South*. Gugus keempat, kajian privasi dan keamanan, menyoroti lemahnya perlindungan data dan tata kelola keamanan siber, mulai dari analisis kesenjangan hukum perlindungan konsumen di era ekonomi digital berbasis AI (Poernomo et al., 2026), tantangan metodologis meneliti ketidakamanan siber di Global South dengan Indonesia sebagai kasus (Hadi et al., 2026), hingga dokumentasi non-akademik namun penting tentang ekosistem impor *spyware* (Amnesty International, 2024). Penelitian ini diposisikan untuk menganalisis kecenderungan kebebasan digital Indonesia 2024–2026 secara terintegrasi, yaitu dimulai dengan menghubungkan regulasi, praktik represi, perilaku *platform*, dan respons masyarakat sipil dalam satu kerangka berbasis kasus, sehingga kelompok penelitian yang sudah dibahas sebelumnya dalam paragraf ini dapat dipertemukan dalam satu analisis.

Pada penelitian ini, peneliti menyadari terdapat beberapa kesenjangan riset. Pertama, belum ada pengukuran terpadu berbasis data kasus SAFEnet untuk masa pemerintahan Prabowo-Gibran. Data pemantauan SAFEnet selama ini terbit sebagai laporan advokasi tahunan dan triwulanan (SAFEnet, 2025b, 2026). Kedua, studi-studi yang ada cenderung memisahkan empat ranah yang saling menentukan

yaitu kajian regulasi berhenti pada norma, kajian ekspresi pada kasus kriminalisasi, kajian keamanan pada insiden peretasan dan kebocoran, dan kajian *platform* pada kebijakan tata kelola. Ketiga, masih sedikit penelitian yang menghubungkan pola pelanggaran dengan struktur tata kelola digital Indonesia seperti halnya mengapa pelanggaran mengambil bentuk tertentu atau mengapa kriminalisasi lebih dominan daripada pemadaman internet, dan mengapa tekanan *platform* menggantikan sensor langsung lebih sering digunakan saat ini. Peneliti menawarkan kebaruan penelitian pada adaptasi kerangka kebebasan digital yang kontekstual untuk Indonesia yang sebelumnya lembaga lain menerapkan indeks internasional secara tanpa penyesuaian kontekstual, penelitian ini membangun kerangka yang mengintegrasikan standar universal (uji tiga tahap ICCPR) dengan karakter spesifik Indonesia seperti halnya ketimpangan pembangunan di daerah, fragmentasi regulasi, dominasi *platform* global, sentralitas hukum pidana, dan kekuatan masyarakat sipil. Ini juga akan sejalan dengan arah dekolonial dan kontekstual dalam kajian kebebasan digital *Global South* (Gómez-Cruz et al., 2023; Hadi et al., 2026). Penelitian ini juga menawarkan adanya analisis kecenderungan pada periode awal pemerintahan Prabowo-Gibran pada periode Oktober 2024-2026 yang mana hingga kini baru tersentuh laporan advokasi dan studi kasus dan penelitian ini menjadi salah satu upaya akademik yang menilai arah keseluruhan periode tersebut.

Penelitian ini tidak dimaksudkan menilai keseluruhan transformasi digital Indonesia, tidak mengukur kesenjangan infrastruktur maupun tingkat literasi digital secara langsung, dan tidak berpretensi menyimpulkan karakter rezim. Fokusnya diarahkan pada satu objek yang dirumuskan yakni pola pembatasan dan

pelanggaran hak digital serta arah perubahannya dalam dua tahun pertama pemerintahan baru dengan disesuaikan dengan konteks Indonesia. Penelitian ini memaknai kebebasan digital sebagai kondisi ketika warga dapat mengakses informasi, berekspresi dan berpartisipasi, menjaga privasi dan keamanan, serta memperoleh perlindungan hak dalam tata kelola *platform* dan regulasi negara. Kecenderungannya dianalisis melalui perubahan pola pelanggaran hak digital yang didokumentasikan SAFEnet pada masa pemerintahan Prabowo Subianto-Gibran Rakabuming Raka dengan memperhatikan jumlah, jenis, cakupan sasaran, aktor, instrumen, serta ditriangulasi dengan indeks internasional yang sudah dibuat oleh lembaga lain.

1.2 Rumusan Masalah

Berangkat dari latar belakang di atas, yakni ruang digital yang telah menjadi arena utama demokrasi Indonesia, warisan infrastruktur pengendalian yang lengkap saat peralihan kekuasaan, rangkaian kasus pembatasan dan pelanggaran hak digital sepanjang periode awal pemerintahan baru, serta kesenjangan kajian yang belum menilai arah keseluruhannya secara terpadu. Berkenaan dengan sikap negara dalam membatasi kebebasan sipil maka rumusan masalah dari penelitian ini adalah bagaimana kecenderungan kebebasan digital di masa pemerintahan Prabowo Subianto-Gibran Rakabuming Raka ditinjau dari pola pelanggaran hak digital?

1.3 Tujuan Penelitian

Penelitian ini bertujuan menganalisis kecenderungan kebebasan digital di Indonesia pada masa pemerintahan Prabowo Subianto-Gibran Rakabuming Raka. Secara lebih rinci, tujuan tersebut dicapai melalui analisis pada pola pelanggaran hak digital yang didokumentasikan SAFEnet berdasarkan jumlah, jenis, cakupan sasaran, aktor, instrumen.

1.4 Manfaat Penelitian

Secara umum, penelitian ini memiliki dua manfaat bagi perkembangan ilmu sosial humaniora, khususnya ilmu politik dalam kajian demokrasi dan Hak Asasi Manusia (hak digital).

1.4.1 Manfaat Teoritis

Penelitian ini berkontribusi pada pengembangan konsep kebebasan berekspresi di ruang digital sebagai konsep multidimensional. Penelitian ini menawarkan konseptualisasi yang mengintegrasikan empat dimensi sekaligus yakni akses terhadap informasi, ekspresi dan partisipasi, privasi dan keamanan, serta perlindungan hak dalam tata kelola platform dan regulasi negara. Dengan menguji konseptualisasi ini pada data kasus Indonesia, penelitian turut menjawab tuntutan literatur *Global South* akan kerangka kebebasan digital yang kontekstual dan mengakomodasi ketimpangan spasial, fragmentasi regulasi, dominasi platform global, dan peran masyarakat sipil di Indonesia.

1.4.2 Manfaat Praktis

Secara praktis, hasil penelitian diharapkan berguna bagi tiga pihak. Pertama, bagi organisasi masyarakat sipil, sebagai kerangka analisis yang memperkuat nilai akademik data pemantauan mereka. Kedua, bagi pembuat kebijakan, sebagai peta empiris titik-titik lemah tata kelola digital seperti halnya kejelasan aturan, proporsionalitas, transparansi, dan pengawasan independen yang perlu dibenahi. Terakhir, bagi publik, sebagai bahan untuk memahami arah perubahan ruang digital dalam konteks Indonesia.

BAB II

TINJAUAN PUSTAKA

2.1 Kebebasan Digital

Kebebasan digital merujuk pada seperangkat hak dan kondisi yang memungkinkan warga mengakses, memproduksi, dan menyebarkan informasi serta berekspresi secara bebas di ruang digital. Freedom House (2025), melalui laporan tahunan Freedom on the Net, mengoperasionalkan kebebasan digital ke dalam tiga dimensi utama: hambatan terhadap akses (*obstacles to access*), pembatasan terhadap konten (*limits on content*), dan pelanggaran terhadap hak-hak pengguna (*violations of user rights*), termasuk privasi dan perlindungan dari pengawasan. Kerangka ini menjadikan kebebasan digital bukan sekadar konsep normatif, melainkan indikator terukur yang dapat digunakan untuk menilai kualitas demokrasi suatu negara. Penting dicatat bahwa kebebasan digital mencakup dimensi yang saling terkait seperti kebebasan berekspresi daring, akses terhadap informasi, serta privasi data, sehingga pelanggaran pada satu dimensi kerap berimplikasi pada dimensi lainnya.

Konsep kebebasan digital yang beredar dalam literatur arus utama sebagian besar dibangun di atas pengalaman *global north* yang mana dasar filosofisnya berakar pada liberalisme barat, standar hukumnya dikembangkan dari yurisprudensi negara-negara demokrasi mapan, dan instrumen pengukurannya dirancang oleh lembaga-lembaga yang berbasis di utara. Dominasi ini tidak hanya bersifat kelembagaan tetapi juga epistemik, dapat

diartikan produksi pengetahuan dan metodologi kajian digital dikuasai aktor *global north*, sementara pengalaman digital di negara selatan diperlakukan sebagai kasus penerapan, bukan sumber teori (Marquez Bustos et al., 2025). Terhadap kondisi ini, literatur mutakhir mengajukan kritik yang kini dikenal sebagai *tropicalization of concepts*: praktik memindahkan konsep-konsep negara-negara barat ke realitas negara-negara selatan tanpa penyesuaian konteks, seolah konsep itu netral dan berlaku universal, padahal ia membawa asumsi-asumsi tersembunyi tentang negara, hukum, pasar, dan subjek yang tidak selalu ada di selatan (Gómez-Cruz et al., 2023). Konsekuensi kritik ini bagi kajian Indonesia bersifat langsung yaitu melalui indikator kebebasan digital tidak cukup dipinjam dari kerangka internasional, melainkan perlu dibangun atau setidaknya disesuaikan dari pengalaman masyarakat dan institusi Indonesia sendiri, mulai dari cara warga menggunakan dan kehilangan hak dan kebebasannya, dari cara aparat menegakkan aturan, dan dari cara lembaga-lembaga nasional bekerja.

Balkin (2018) mengemukakan konsep *free speech is a triangle*: regulasi ujaran di era digital tidak lagi bersifat dualistik antara negara dan penutur, melainkan berevolusi menjadi melibatkan negara, perusahaan *platform*, dan warga atau pengguna. Konsekuensinya, negara kini mempraktikkan apa yang disebut Balkin sebagai *new-school speech regulation*: alih-alih menindak pengguna satu per satu, negara menekan perantara seperti *platform* atau penyelenggara elektronik melalui kewajiban pendaftaran, ancaman pemblokiran, atau pencabutan izin, agar platform itulah yang menyensor

penggunanya sehingga melahirkan *collateral censorship* (Balkin, 2018). Konsep ini sangat relevan bagi Indonesia saat ini, seperti adanya kewajiban pendaftaran Penyelenggara Sistem Elektronik (PSE), pemblokiran layanan, hingga penangguhan izin operasi TikTok pada 2025 yang berujung pada penyerahan data pengguna terkait demonstrasi kepada pemerintah (Freedom House, 2025). Hal tersebut merupakan bentuk praktik empiris dari regulasi ujaran gaya baru tersebut.

Deibert, Palfrey, Rohozinski, dan Zittrain (2008), melalui proyek OpenNet Initiative, memetakan praktik penyaringan internet global dan mengategorikannya ke dalam empat tema: politik, sosial, konflik/keamanan, dan alat internet (*internet tools*). Kerangka ini menjadi rujukan standar untuk mengidentifikasi jenis konten yang paling sering disensor negara. King et al. (2013) memperdalam pemahaman ini melalui studi empiris di Tiongkok, dan menemukan bahwa sensor negara tidak terutama menyasar kritik terhadap pemerintah, melainkan konten yang berpotensi memicu aksi kolektif (*collective action*). Roberts (2018) menambahkan bahwa sensor modern kerap bekerja bukan melalui pelarangan total, melainkan melalui "gesekan" (*friction*) dan pengalihan perhatian (*flooding*) yang membuat informasi sulit diakses tanpa perlu memblokirnya secara terbuka sehingga menghasilkan *fear* atau ketakutan.

Perkembangan penting dalam literatur adalah pergeseran fokus dari negara ke *platform* sebagai aktor yang turut menentukan batas kebebasan digital. Gillespie (2018) menunjukkan bahwa moderasi konten bersifat konstitutif bagi cara kerja *platform*, di mana *platform* berperan sebagai penetap norma, penafsir

aturan, sekaligus penegak kebijakan atas ekspresi pengguna. Balkin (2018) menghubungkan kekuasaan privat ini dengan kekuasaan negara melalui konsep *new-school speech regulation* dan *collateral censorship*, yang berarti negara semakin menghindari menindak pengguna secara langsung, dan sebaliknya menekan perantara digital agar membatasi ekspresi pihak ketiga. Dengan demikian, kewajiban moderasi konten yang diatur negara berpotensi menjadi instrumen sensor tidak langsung yang mengancam kebebasan digital warga.

Sebagai jawaban atas kritik tersebut, kajian kebebasan digital *global south* bergerak ke pendekatan dekolonial dan kontekstual (Das, 2026; J. B. Y. Lim, 2025; Sabry et al., 2025). Pendekatan ini menuntut beberapa hal sekaligus. Pertama, keadilan epistemik, yakni kerangka konseptual harus merepresentasikan pengalaman digital kelompok subaltern yang selama ini tak terwakili dalam teori (Harindranath & Gómez-Cruz, 2023). Kedua, perhatian pada kelompok marjinal, seperti halnya pemrosesan datan dan algoritma menciptakan bentuk-bentuk marginalisasi dan eksklusi baru yang justru paling keras menimpa mereka yang sudah terpinggirkan (Chaka, 2022). Ketiga, agensi lokal, yauitu warga negara-negara selatan bukan korban pasif teknologi, melainkan aktor yang mengapropriasi, menyiasati, dan membentuk ulang teknologi menurut kebutuhannya (Nemmani & Rodriguez, 2023). Keempat, kepekaan pada perbedaan wilayah dan warga urban-rural, yang di Indonesia berarti kesenjangan akses dan literasi yang membentang antara Pulau Jawa dan Indonesia Timur (Jaya et al., 2024; Rajagukguk et al., 2024). Kelima, budaya politik setempat yang dapat dilihat dari praktik kewargaan digital di Asia

Tenggara berakar pada nilai kolektivisme dan solidaritas, bukan individualisme liberal yang diandaikan teori Utara (Yue et al., 2019), dan aktivismenya beradaptasi dengan budaya platform serta represi negara secara khas (M. Lim, 2023). Keenam, struktur regulasi nasional, berbicara mengenai kerangka hukum digital Indonesia yang terfragmentasi, bertumpu pada hukum pidana, dan minim pengawasan independen adalah konteks yang menentukan bagaimana kebebasan digital dibatasi dan diperjuangkan (Utomo, 2025).

Dalam konteks Indonesia, kebebasan digital menjadi arena yang semakin diperebutkan seiring meningkatnya penetrasi internet dan penguatan regulasi negara atas ruang digital. Peraturan Menteri Komunikasi dan Informatika No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat, misalnya, mewajibkan seluruh penyelenggara sistem elektronik untuk melakukan moderasi konten dan memastikan sistemnya tidak memuat informasi yang dilarang (Kominfo, 2020). Sejumlah organisasi masyarakat sipil menilai regulasi semacam ini memberi kewenangan yang luas kepada negara untuk mengendalikan konten, mengakses data pengguna, hingga memutus akses, sehingga berpotensi menyempitkan kebebasan sipil digital. Temuan ini sejalan dengan tren global yang dicatat Freedom House (2025), yakni menurunnya kebebasan internet secara berturut-turut, termasuk di negara-negara yang masih menyelenggarakan pemilu demokratis.

2.2 Dimensi Kebebasan Digital

Secara substantif, kebebasan digital didefinisikan dalam penelitian ini sebagai kondisi yang memungkinkan warga menggunakan ruang digital secara terbuka, aman, setara. Definisi ini sengaja dirumuskan sebagai kondisi, bukan sekadar ketiadaan larangan karena kebebasan digital tidak identik dengan absennya sensor, melainkan hadirnya prasyarat-prasyarat yang membuat warga benar-benar dapat mencari dan menyampaikan informasi, berpartisipasi dalam kehidupan publik, serta membentuk makna bersama di ruang digital (Balkin, 2004; UN Human Rights Council, 2012). Empat kunci utamanya yakni terbuka berarti akses terhadap informasi dan kanal ekspresi tidak dihalangi secara sewenang-wenang, aman berarti penggunaan ruang digital tidak menempatkan warga dalam risiko pengawasan, peretasan, atau persekusi, setara berarti kondisi itu dinikmati warga lintas wilayah, kelas, dan gender, bukan hanya oleh yang terkoneksi baik dan literat (Chaka, 2022).

Tingginya penetrasi internet yaitu 221,5 juta pengguna atau 79,5 persen penduduk Indonesia (APJII, 2024) dan besarnya ekonomi digital tidak otomatis menunjukkan tingginya kebebasan digital. Digitalisasi mengukur seberapa jauh kehidupan berpindah ke ruang digital seperti kebebasan digital mengukur kualitas kehidupan di ruang itu. Keduanya bahkan dapat bergerak berlawanan antara digitalisasi yang masif justru memperluas permukaan kontrol yang tersedia bagi negara, sehingga digitalisasi dapat berlangsung bersama atau menjadi kendaraan bagi negara untuk melakukan pengawasan, kriminalisasi, dan pembatasan (Feldstein, 2021; Margiansyah, 2025). Pengalaman Asia Tenggara menegaskan paradoks ini, bahwa kawasan dengan adopsi digital tercepat di dunia sekaligus

menjadi kawasan tempat otoritarianisme digital berkembang paling subur (Sinpeng, 2020; Tan & Denver, 2025). Karena itu, indikator adopsi seperti penetrasi, jumlah pengguna, nilai ekonomi tidak dipakai dalam penelitian ini sebagai ukuran kebebasan.

Dimensi pertama kebebasan digital bersifat struktural yaitu meliputi infrastruktur, perangkat, konektivitas, dan literasi. Literatur pengukuran menempatkan unsur-unsur ini sebagai fondasi setiap kerangka penilaian yang menjadikan infrastruktur dimensi pertamanya (Abdurrahman, 2025) dan kerangka yang mengintegrasikan infrastruktur dengan sumber daya manusia dan tata kelola (Eshtaev et al., 2026). Dalam bahasa pendekatan kapabilitas, dimensi struktural adalah kondisi yang memungkinkan (*enabling conditions*) sehingga ia tidak dengan sendirinya merupakan kebebasan, tetapi tanpa dirinya kebebasan formal tidak dapat dikonversi menjadi kemampuan nyata (Sen, 1999). Sesuai batasan yang telah ditetapkan, dimensi ini tidak diukur sebagai hasil utama penelitian namun digunakan sebagai lensa pembacaan untuk menjelaskan perbedaan lokasi kasus dan perbedaan kerentanan warga, mengingat ketimpangan konektivitas dan literasi antara urban-rural serta Indonesia Barat dan Indonesia Timur membuat pelanggaran yang sama berdampak tidak sama (Jaya et al., 2024; Rajagukguk et al., 2024).

Dimensi kedua adalah dimensi hak, inti normatif kebebasan digital. Beberapa hak utama dicakup penelitian ini. Akses terhadap informasi yang diartikan sebagai hak mencari dan menerima informasi melalui media apa pun (UN Human Rights Committee, 2011). Hak bebas berekspresi, yang diartikan sebagai hak menyampaikan pendapat tanpa ancaman kriminalisasi yang sewenang-wenang,

yang di Indonesia paling sering dilanggar melalui pasal-pasal UU ITE (Astara, 2021; SAFEnet, 2026). Hak untuk bebas berekspresi juga diartikan sebagai hak turut serta dalam kehidupan publik digital, termasuk mengorganisasi dan bermobilisasi, yang oleh temuan empiris justru menjadi sasaran utama sensor (King et al., 2013) Hak rasa aman yang merupakan bentuk dari perlindungan data pribadi dan ruang batin dari pengumpulan serta pengawasan yang tidak sah (Glasius & Michaelsen, 2018). Selain itu hak rasa aman juga diartikan bebas dari peretasan, doksing, dan serangan digital yang menjadikan ekspresi berisiko (SAFEnet, 2025b). Hak untuk setara yaitu hak atas proses yang jujur dalam relasi dengan platform yang tidak ditangguhkan sewenang-wenang, tidak dimoderasi tanpa alasan, dan tidak diserahkan datanya tanpa dasar (Gillespie, 2018; Hunawa et al., 2025).

Dimensi ketiga adalah tata kelola yang menentukan apakah dimensi hak dijamin atau dilanggar secara terlembaga. Ia mencakup beberapa unsur, di antaranya adalah hukum, yang mengatur kejelasan dan proporsionalitas aturan yang mengatur ruang digital, yang di Indonesia masih terfragmentasi dan bertumpu pada pemidanaan (E. P. Handayani et al., 2025; Utomo, 2025). Kedua, institusi, yang ditunjukkan dengan keberadaan dan independensi lembaga pelindung hak, termasuk pengawas data pribadi yang hingga kini belum terbentuk. Ketiga, transparansi yang diartikan sebagai keterbukaan atas tindakan pembatasan seperti pemblokiran dan permintaan penghapusan konten. Keempat, akuntabilitas yang memungkinkan meminta pertanggungjawaban negara atas tindakan digitalnya (Pribadi et al., 2024).

Melalui ketiga dimensi itu, dirumuskan definisi operasional yang dipakai sepanjang penelitian mengenai kebebasan digital adalah kondisi perlindungan hak warga dalam mengakses informasi, berekspresi dan berpartisipasi, menjaga privasi dan keamanan, serta memperoleh perlakuan yang transparan dan dapat dipertanggungjawabkan dari negara dan platform. Definisi ini menerjemahkan definisi substantif ke dalam empat komponen yang dapat diamati pada data kasus yaitu setiap kasus pelanggaran hak digital dapat diklasifikasi menurut komponen mana yang dilanggar (akses, kebebasan ekspresi, rasa aman), oleh aktor mana, dengan instrumen apa, dan sejauh apa sehingga kecenderungan kebebasan digital dapat dibaca sebagai pergeseran pola pelanggaran antarkomponen dari waktu ke waktu. Dengan konstruksi ini, definisi operasional sekaligus menjadi jembatan antara kerangka konseptual dan teknik analisis data yang diuraikan pada bab metode.

2.3 Otoritarianisme Digital

Feldstein (2021) mengonseptualisasikan *digital repression* sebagai penggunaan teknologi informasi oleh negara untuk membatasi ruang sipil, yang beroperasi melalui lima teknik utama, yaitu pengawasan (*surveillance*), penyensoran dan pemblokiran konten, manipulasi informasi dan disinformasi terorganisasi, pemutusan atau pembatasan akses internet, serta persekusi yang menyasar pengguna internet, seperti halnya kriminalisasi hingga intimidasi.

Temuan penting Feldstein adalah bahwa represi digital tidak eksklusif milik rezim otoriter penuh, melainkan banyak berkembang di negara demokrasi elektoral

dan rezim hibrida, karena teknik-tekniknya lebih murah, lebih halus, dan lebih mudah disangkal dibandingkan dengan represi fisik (Feldstein, 2021). Tipologi ini digunakan dalam penelitian ini untuk mengklasifikasi praktik negara di Indonesia, mulai dari patroli siber, pemblokiran, operasi pendengung (*buzzer*), hingga kriminalisasi ekspresi. Teori ini juga digunakan untuk menilai apakah kecenderungan yang terjadi mengarah pada apa yang oleh masyarakat sipil disebut sebagai otoritarianisme digital.

Glasius (2018) mengusulkan pergeseran unit analisis dari tipe rezim ke praktik, sehingga yang diamati bukan semata apakah suatu negara otoriter, melainkan apakah terdapat praktik otoriter (*authoritarian practices*), yaitu pola tindakan yang menyabotase akuntabilitas yang dilakukan melalui kerahasiaan, disinformasi, dan pelumpuhan suara warga, serta praktik iliberal (*illiberal practices*), yaitu pelanggaran terhadap otonomi dan martabat individu, misalnya lewat pengawasan yang tidak sah. Praktik otoriter digital dapat diidentifikasi dan diukur di negara demokrasi sekalipun, tanpa harus terlebih dahulu menyimpulkan bahwa negara tersebut telah berubah menjadi otoriter.

Adanya pola represi di ranah daring dinilai dapat menimbulkan *chilling effect* pada warga atau pengguna. Schauer (1978) *chilling effect* terjadi ketika individu menahan diri dari melakukan ekspresi yang sesungguhnya sah dan dilindungi hukum, karena takut terkena sanksi atau beban proses hukum. Sumber utamanya bukan sanksi itu sendiri, melainkan ketidakpastian: rumusan hukum yang kabur (*vague*) dan terlalu luas (*overbroad*) membuat warga tidak dapat memprediksi di mana batas legalitas berada, sehingga mereka memilih menjauh

jauh-jauh dari batas tersebut. Fenomena ini disebut Schauer sebagai *overdeterrence*, yakni penjeraan yang melampaui perilaku yang memang hendak dilarang (Schauer, 1978). Lebih jauh dari itu, yang hilang bukan hanya ekspresi satu orang yang dihukum, melainkan ekspresi banyak orang yang tidak pernah diucapkan. *Chilling effect* merupakan mekanisme mikro yang menghubungkan tindakan represif negara dengan penyempitan ruang sipil (*shrinking civic space*) pada tingkat makro. Ini meliputi regulasi yang ambigu, penegakan yang selektif, dan pengawasan yang meluas mengubah kalkulasi risiko individu, mendorong swasensor (*self-censorship*), dan pada akhirnya memiskinkan diskursus publik yang menjadi prasyarat akuntabilitas demokratis.

Kondisi yang oleh Schauer (1978) diidentifikasi sebagai pemicu utama *chilling effect,* yakni rumusan hukum yang kabur (*vague*) dan terlalu luas (*overbroad*), menggambarkan problem "pasal karet" dalam rezim UU ITE. Meskipun telah direvisi dua kali, ketentuan seperti pasal pencemaran nama baik (Pasal 27A) tetap menjadi instrumen pelaporan yang paling sering digunakan terhadap ekspresi kritis. SAFEnet mencatat 146 kasus pelanggaran kebebasan berekspresi digital sepanjang 2024 (SAFEnet, 2025b), yang melonjak menjadi 351 kasus pada 2025 seiring intensifikasi patroli siber oleh kepolisian (SAFEnet, 2026). Freedom House (2025) mencatat skor kebebasan internet Indonesia turun menjadi 48 dari 100 (kategori *partly free*), dengan swasensor di kalangan jurnalis dan pengguna sebagai salah satu indikator yang terus memburuk, serta penindakan terhadap ekspresi daring pasca-demonstrasi Agustus–September 2025.

2.4 Kerangka Pemikiran

Penelitian ini berangkat dari serangkaian fenomena empirik dalam dua tahun terakhir seperti halnya penerapan UU ITE dan patroli siber sebagai alat untuk melakukan kriminalisasi ekspresi warga, pemblokiran layanan digital, tekanan regulatif terhadap platform hingga penangguhan izin dan penyerahan data pengguna, serta operasi pendengung yang dibiayai negara (Freedom House, 2025; SAFEnet, 2026).

Konsep kebebasan digital dalam penelitian ini dibangun dari pertemuan dua dimensi. Dimensi pertama adalah standar universal yaitu prinsip bahwa hak yang dimiliki warga secara luring harus dilindungi sama ketika daring (UN Human Rights Committee, 2011; UN Human Rights Council, 2012). Dimensi kedua adalah kritik *global south* yaitu penolakan atas pemindahan konsep barat tanpa penyesuaian konteks (*tropicalization of concepts*) dan tuntutan membangun indikator dari pengalaman masyarakat serta institusi Indonesia (Gómez-Cruz et al., 2023; Harindranath & Gómez-Cruz, 2023). Pertemuan keduanya menghasilkan konseptualisasi kebebasan digital sebagai konsep multidimensional yaitu kondisi yang memungkinkan warga menggunakan ruang digital secara terbuka, aman, setara dengan penegasan bahwa digitalisasi tidak identik dengan kebebasan digital, sebab adopsi teknologi yang tinggi dapat berjalan seiring pengawasan, kriminalisasi, dan pembatasan (Feldstein, 2021; Sinpeng, 2020). Kebebasan digital adalah kondisi perlindungan hak warga dalam mengakses informasi, berekspresi dan berpartisipasi, menjaga

privasi dan keamanan, serta memperoleh perlakuan yang transparan dan dapat dipertanggungjawabkan dari negara dan platform.

Definisi ini menjadi jembatan ke arah data yang digunakan, setiap kasus pelanggaran hak digital yang didokumentasikan SAFEnet pada periode 2024 sampai 2026 diklasifikasi menurut komponen definisi yang dilanggar, lalu dianalisis polanya dengan tetap melakukan triangulasi terhadap indeks *Freedom on the Net*, perkembangan regulasi (Freedom House, 2024, 2025; SAFEnet, 2025b, 2026).

Definisi operasional yang telah dirumuskan, yaitu perlindungan hak warga dalam mengakses informasi, berekspresi dan berpartisipasi, menjaga privasi dan keamanan, serta memperoleh perlakuan transparan dan akuntabel dari negara dan platform kemudian akan diterjemahkan ke dalam analisis melalui enam dimensi pengukuran. Keempat dimensi ini diterapkan pada setiap kasus pelanggaran hak digital yang terdokumentasi, sehingga kecenderungan kebebasan digital dibaca bukan dari satu angka, melainkan dari pergeseran pola pada enam dimensi secara bersamaan.

Pertama, dimensi jumlah, yakni frekuensi kasus per satuan waktu. Dimensi ini memberi gambaran paling dasar tentang intensitas lonjakan kasus dari waktu ke waktu. Kedua, dimensi jenis pelanggaran yang akan menghubungkan setiap kasus dan melihat apa yang dilanggar misalnya pada pelanggaran akses informasi apa yang dilakukan pemerintah dan apa yang dilakukan untuk membatasi akses informasi tersebut. Ketiga, dimensi sasaran yaitu akan digunakan untuk melihat siapa korban, apakah secara spesifik

menyerang kelompok rentan dan berisiko tinggi atau kemungkinan lainnya. Keempat, dimensi aktor, yaitu untuk melihat siapa yang melakukan, apakah aparatus negara atau dilakukan oleh *platform* atau instrumen lainnya. Kelima, dimensi instrumen yang akan digunakan untuk melihat, apakah ada pola legitimasi yang dilakukan negara melalui peraturan atau melalui instrumen teknis seperti pembatasan fitur dan sebagainya. Keenam, dimensi keparahan yang akan digunakan untuk melihat begaimana dampak yang diterima oleh korban dan adakah dampak lain yang meluas seperti *chilling effect*. Keenam dimensi tersebut digunakan untuk menganalisis dan membuat kesimpulan serta digunakan untuk membaca pola dan perubahan sehingga relevan dan dapat menjawab rumusan masalah.

BAB III

METODE PENELITIAN

3.1 Pendekatan Riset

Penyensoran oleh negara menjadi fenomena yang berdampak pada demokrasi, khususnya kebebasan berekspresi dan kondisi masyarakat sipil. Penelitian ini akan menggunakan metode studi kasus. Yin (2009) menyatakan bahwa studi kasus adalah bentuk penelitian yang membahas, mengidentifikasi dan menyelidiki fenomena kontemporer dalam keseharian secara kontekstual. Studi kasus memiliki beberapa karakteristik menurut Creswell (1998), antara lain adalah: (1) mengidentifikasi kasus atau fenomena khusus untuk keperluan suatu studi, (ii) penelitian yang dilakukan akan terikat pada waktu dan lokus khusus dan spesifik, (iii) menggunakan berbagai sumber untuk mendapat sumber informasi dalam proses pengumpulan data agar dapat tergambar secara rinci dan mendalam terkait dengan respon akan suatu fenomena, dan (iv) penelitian akan fokus pada menjabarkan konteks dalam sebuah kasus.

Studi kasus menjadi metode yang tepat dalam penelitian ini didasari pada beberapa pertimbangan, seperti (i) kasus yang diteliti spesifik dan khusus, yakni penyensoran informasi oleh negara di masa satu tahun pertama pemerintahan Prabowo Subianto-Gibran Rakabuming, (ii) analisis empiris terkait metode yang dilakukan oleh negara untuk melakukan praktik otoritarianisme digital, yakni penyensoran atas informasi di internet di Indonesia, (iii) membuktikan alasan mengapa negara melakukan praktik penyensoran di internet.

Secara umum, proses penelitian ini terbagi menjadi beberapa tahap, pertama adalah memilih topik penelitian, merumuskan dan menentukan pertanyaan penelitian, menyusun desain penelitian, mengumpulkan dan menganalisis data temuan, terakhir adalah menyusun laporan penelitian (Neuman, 1997).

Peneliti memilih mengenakan metode penelitian kualitatif karena sesuai dengan kebutuhan penelitian, yakni untuk menjawab pertanyaan penelitian yang membutuhkan perangkat penelitian metodologis yang sudah sesuai dan disediakan oleh metode kualitatif. Penelitian ini akan berisi analisis data secara induktif. Peneliti akan membangun pola dan kategori tertentu untuk mengolah data agar lebih konstruktif dan terstruktur serta menyusun intepretasi atas data yang didapat dan dipahami oleh peneliti. Demikian dilakukan untuk menciptakan penelitian yang bisa menggambarkan fenomena iiliberal demokrasi, berupa penyensoran informasi di internet oleh negara supaya mudah dipahami secara holistik dan tersturktur (Margaret, 2014).

3.2 Penentuan Sumber Data

Penentuan sumber data dalam penelitian ini akan menggunakan teknik studi pustaka. Peneliti menggunakan data pelanggaran hak digital yang disediakan oleh Southeast Asia Freedom and Expression Network (SAFEnet). Data yang dimiliki SAFEnet bersifat terbuka sehingga bisa diolah dan dimanfaatkan dengan bebas. SAFEnet mengelola kanal pengaduan pelanggaran hak digital dan melakukan pemantauan media selama beberapa tahun terakhir. Data tersebut dapat diakses secara publik melalui website.

SAFEnet dipilih karena memiliki data dengan karakteristik spesifik, pertimbangan lainnya adalah SAFEnet merupakan lembaga yang memiliki spesifikasi keahlian untuk melakukan pendataan, pendokumentasian dan mampu menganalisis pelanggaran hak digital di Indonesia. Peneliti kemudian memilih laporan Freedom of House sebagai sumber data sekunder untuk memvalidasi temuan dan data yang diperoleh dari SAFEnet. Pemilihan sumber data sekunder tersebut berkenaan dengan kerja-kerja dan penelitian yang dilakukan oleh Freedom of House. Adapun kerja-kerja yang di maksud adalah, melakukan pemantauan, penerimaan data aduan advokasi, kampanye dan penelitian yang berkaitan dengan otoritarianisme digital, sensor informasi di internet oleh negara, dan kebebasan berekspresi di ranah digital. Adapun SAFEnet juga merupakan bagian dari jaringan Freedom of House dan rutin membantu untuk memberikan data pelanggaran hak digital dalam konteks Indonesia.

3.3 Teknik Pengumpulan Data

Pengumpulan data dilakukan dengan memanfaatkan data yang diperoleh dan dikumpulkan oleh SAFEnet. Data mentah dan data tertampil tersebut kemudian diolah kembali sehingga bisa ditampilkan dengan cara yang lebih mudah diakses dan mudah dipahami. Adapun tujuan dari teknik tersebut adalah untuk membantu memberi pemahaman secara holistik terkait dengan fenomena penyensoran informasi di internet yang merupakan bagian dari illiberal demokrasi.

3.3.1 Studi dokumentasi dan literatur

Studi literatur dilakukan untuk memperkuat dan memvalidasi data temuan yang diperoleh dari literatur utama. Pada penelitian ini, peneliti akan mengumpulkan literatur yang berkenaan dengan otoritarianisme digital, penyensoran informasi berlebihan oleh negara, moderasi konten dan kebijakan yang terkait dengan *state censorship*, dan aktivisme digital. Adapun literatur yang digunakan tidak terbatas dengan apa yang terjadi di Indonesia, melainkan juga yang terjadi di wilayah lain untuk memperkuat analisis dan data yang dibutuhkan.

3.4 Data Set

Data set adalah kumpulan data yang dibutuhkan dan akan digunakan sebagai acuan penelitian secara keseluruhan. Adapun data set penelitian ini adalah sebagai berikut:

Tabel 3.1 Data Set

Variabel Utama	Dimensi	Parameter	Sumber Data	Teknik Pengumpulan Data	Instrumen
Menilai kecenderungan kebebasan digital	**Jumlah (SAFEnet)**	- frekuensi kasus dari waktu ke waktu - Membaca pergerakan antar waktu melalui momentum yang terjadi	Laporan triwulan dan tahunan SAFEnet	Studi dokumentasi	Panduan analisis dokumen
	Jenis Pelanggaran (Fleidstein, 2021)	- kalsifikasi kasus terhadap empat domain hak digital, yaitu akses informasi, kebebasan berekspresi, keamanan digital, dan kesetaraan di ruang digital	Laporan triwulan dan tahunan SAFEnet, Laporan Freedom of House	Analisis data sekunder (Freedom of House)	Panduan analisis dokumen
	Sasaran (Robert, 2013)	- Siapa korban dan yang terdampak?	Laporan triwulan dan tahunan SAFEnet	Studi dokumentasi	Panduan analisis dokumen
	Aktor (Balkin, 2018; Fleidstein, 2021)	- Siapa pelakunya - Proporsi yang dilakukan negara, platform atau instrumen lain yang dinilai sebagai aktor	Laporan SAFEnet, meda massa	Studi dokumentasi	Panduan analisis dokumen
	Intrumen (Deibert, 2015; Robert, 2016)	- Alat yang digunakan sebagai instrument legitimasi - Analisis pemetaan tiga generasi kontrol Deibert	Laporan triwulan dan tahunan SAFEnet	Analisis data sekunder	Panduan analisis dokumen
	Keparahan (Schauer, 1978)	- Gradasi keparahan dan dampak pada korban dan kelompok terdampak lainnya	Laporan triwulan dan tahunan SAFEnet	Studi dokumentasi	Panduan analisis dokumen

3.5 Teknik Analisis Data

Analisis data yang digunakan dalam penelitian ini adalah analisis model interaktif. Miles dan Huberman (2014) mengemukakan tiga komponen dalam bentuk teknik analisis data, yakni reduksi data, penyajian data, dan penarikan kesimpulan. Adapun ketiga komponen tersebut apabila diaplikasikan dengan penelitian ini adalah sebagai berikut:

3.5.1 Reduksi data

Reduksi data adalah proses pemilihan, penyederhadaan dan transofrmasi data mentah dari proses pengumpulan data untuk menjadi analisis data yang utuh dan terstruktur. Pada tahapan reduksi data, hal pertama yang dilakukan adalah mengarahkan penelitian pada informasi yang paling substantif dan relevan sehingga pada penataan data bisa dilakukan dengan terstruktur dan logis. Proses reduksi data juga meliputi pemilihan data yang tidak perlu dimasukkan dan tidak relevan sehingga batasan penelitian akan lebih jelas dan menghasilkan penelitian yang terfokus pada topik tertentu.

3.5.2 Penyajian data

Proses ini bertujuan untuk mengorganisir dan menyajikan temuan penelitian secara terstruktur dan sistematis agar bisa dengan mudah dipahami, diinterpretasikan oleh pembaca dan peneliti lain. Pada proses ini, peneliti akan menjelaskan temuan penelitian dan mencari data pendukung sehingga tidak menjadi klaim sepihak dari peneliti. Peneliti akan

mengaitkannya dengan latar belakang dan menyajikannya secara logis dalam bentuk naratif deskriptif dan analitik.

3.5.3 Penarikan Kesimpulan

Proses ini akan berkenaan dengan interpretasi temuan yang dilakukan oleh peneliti dan dibuat menjadi lebih ringkas dan disajikan untuk menjawab pertanyaan penelitian. Penarikan Kesimpulan harus terlebih dahulu melewati proses verifikasi latar belakang, data awal, temuan penelitian dan hasil akhir dari reduksi data. Kesimpulan harus menjelaskan mengapa dan bagaimana sebuah fenomena yang diteliti dapat terjadi. Dengan demikian penelitian ini harus menjelaskan bagaimana kecenderungan kebebasan digital di Indonesia pada masa pemerintahan Prabowo Subianto-Gibran Rakabuming. Kesimpulan ini juga akan menjawab pertanyaan penelitian secara ringkas dan komprehensif.

3.6 Teknik Validitas Data

Proses ini bertujuan untuk memastikan hasil temuan dan data yang disajikan sudah sesuai dengan kebutuhan penelitian. Selain itu, proses ini juga akan membuktikan akurasi data dan relevansi data dengan konteks topik yang sudah dipilih sebelumnya. Penelitian ini mengacu pada konteks kecenderungan kebebasan digital selama masa pemerintahan Prabowo Subianto-Gibran Rakabuming. Relevansi datanya dapat diartikan bahwa data yang diambil harus relevan dengan kebutuhan topik tersebut dan sesuai dengan periode tersebut.

Proses ini juga akan menggunakan teknik triangulasi sumber, yaitu proses memvalidasi data yang sudah didapat dari sumber utama dan dari sumber sekunder, dengan tujuan memperkuat temuan dari sumber utama. Misalnya memperkuat data temuan dari SAFEnet dengan studi literatur melalui laporan atau riset ilmiah yang dilakukan oleh lembaga kredibel. Ini bertujuan untuk melihat konsistensi data, apakah sudah sesuai atau harus dipilah kembali. Proses ini juga akan berisi penyelarasan antara teori dan konsep penelitan yang digunakan dengan data yang didapat. Setelah teknik validitas data selesai dilakukan, maka kredibilitas data dan temuan penelitian bisa dibuktikan dalam proses penarikan kesimpulan.

3.7 Jadwal Penelitian

Tabel 3.2 Jadwal Penelitian

No	Kegiatan	Lokasi	Periode
1	Memilih dan menentukan topik kajian dengan mengkaji paradigma dan fenomena empiris	Jakarta	Mei 2025
2	Menetapkan objek penelitian	Jakarta	Mei 2025
3	Memutuskan konsep dan teori yang digunakan	Jakarta	Mei-Juni 2026
4	Menentukan teknik pengumpulan data	Jakarta	Mei 2026
5	Menentukan sumber data primer penelitian	Jakarta	Juni 2026

BAB IV

PENGATURAN KEBEBASAN DIGITAL DI INDONESIA

Bab ini akan menjelaskan menyajikan deskripsi tentang bagaimana kebebasan digital diatur di Indonesia, termasuk mengenai kerangka kebijakannya, infrastruktur fisik dan teknisnya, arsitektur kelembagaannya, serta mekanisme sehari-hari yang dipakai negara mengelola ruang digital. Tujuannya untuk memperjelas posisi politik, tata kelola, dan tempat kasus-kasus pelanggaran hak digital yang dianalisis pada bab berikutnya. Pola pelanggaran hanya dapat dipahami bila struktur kewenangan, aturan, dan aktor yang melatarinya dipetakan terlebih dahulu.

4.1 Deskripsi Pengaturan Kebebasan Digital di Indonesia

Pada tingkat konstitusi, kebebasan digital berpijak pada Pasal 28E ayat (3) UUD NKRI 1945 (kebebasan berserikat, berkumpul, dan berpendapat) dan Pasal 28F (hak berkomunikasi dan memperoleh informasi melalui saluran apa pun), dengan pintu pembatasan melalui undang-undang pada Pasal 28J ayat (2) yang menjelaskan bahwa hak dan kewajiban warga negara sudah ditetapkan di perundang-undangan. Regulasi ruang digital tersusun berlapis namun tidak terkodifikasi dalam satu periode pemerintahan, ada UU No. 11 Tahun 2008 tentang Informasi dan Transkasi Elektronik (ITE) yang sudah dua kali direvisi melalui UU No. 19 Tahun 2016 dan UU No. 1 Tahun 2024. UU ITE kemudian menjadi instrumen pidana utama atas ekspresi daring lalu selanjutnya juga ada

UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur ranah privasi ditambah UU No. 1 Tahun 2023 tentang KUHP, yang berlaku sejak Januari 2026, menambahkan pasal penghinaan presiden dan lembaga negara dengan jangkauan eksplisit ke media elektronik. Sementara itu juga terdapat PP No. 71 Tahun 2019 dan Permenkominfo No. 5 Tahun 2020 yang mengatur tata kelola administratif Penyelenggara Sistem Elektronik (PSE) beserta dengan kewajiban pendaftaran, pemutusan akses, dan penghapusan konten, dan yang terbaru terdapat PP No. 17 Tahun 2025 (PP Tunas) yang berfokus untuk menambahkan lapisan pelindungan anak di ruang digital (Gumati, 2024; Utomo, 2025).

Sebagai penyeimbang, terdapat pula regulasi yang bercorak menjamin seperti halnya UU No. 40 Tahun 1999 tentang Pers yang digunakan untuk melindungi kerja jurnalistik, termasuk produk jurnalisme di ruang digital, melalui mekanisme Dewan Pers. Selain itu juga terdapat UU No. 14 Tahun 2008 tentang Keterbukaan Informasi Publik menjamin hak warga atas informasi badan publik melalui Komisi Informasi. Namun masih didapati celah, mulai dari arsiteksur pelaksanaan hingga implementasi dari pelaksanaan peraturan-peraturan tersebut. Pertama, aturan tersebar di banyak undang-undang dan peraturan pelaksana dengan definisi yang tidak selalu konsisten dan koordinasi antarlembaga yang lemah (Utomo, 2025). Kedua, dominasi pendekatan pidana yang masih dilakukan, instrumen yang paling sering dipakai terhadap ekspresi warga adalah pemidanaan, bukan mekanisme perdata, administratif, atau ko-regulasi (E. P. Handayani et al., 2025). Ketiga, terkait dengan kewenangan yang

terlalu luas, termasuk kewenangan menentukan konten yang dilarang, memblokir, dan menjatuhkan sanksi administratif terkonsentrasi di pemerintah tanpa keharusan uji pengadilan terlebih dahulu (Gumati, 2024).

Secara fisik, konektivitas internet di Indonesia ditopang proyek-proyek negara berskala besar seperti halnya jaringan serat optik Palapa Ring yang menyambungkan wilayah barat, tengah, dan timur, lalu ada juga satelit multifungsi SATRIA-1 yang diluncurkan pada 2023 untuk melayani titik-titik layanan publik di daerah tertinggal, serta pembangunan menara BTS 4G oleh Badan Aksesibilitas Telekomunikasi dan Informasi (BAKTI) di wilayah terdepan, terluar, dan tertinggal. Infrastruktur ini memperluas akses secara nyata, tetapi juga memperlihatkan kerentanan tata kelolanya, misalnya proyek BTS 4G BAKTI menjadi perkara korupsi besar yang merugikan negara sekitar Rp8 triliun dan berujung vonis 15 tahun penjara bagi Menteri Komunikasi dan Informatika Johnny G. Plate pada November 2023 (Kompas, 2023). Peristiwa ini menunjukkan lemahnya kredibilitas kementerian pengelola ruang digital saat menjelang pergantian pemerintahan. Kerentanan serupa tampak pada infrastruktur data, seperti kasus lumpuhnya Pusat Data Nasional Sementara (PDNS) oleh serangan *ransomware* pada 2024, kasus ini mengekspos lemahnya keamanan sistem yang menopang ratusan layanan publik (BSSN, 2024).

Di samping infrastruktur konektivitas, negara juga memiliki infrastruktur pengendalian seperti sistem penyaringan TrustPositif yang menjadi basis data pemblokiran situs dan konten, perangkat pemantauan media sosial di kementerian dan kepolisian, serta kanal aduan konten yang menjadi pintu

masuk permintaan penghapusan. Keberadaan dua jenis infrastruktur ini yang menyambungkan dan yang membatasi dalam satu tangan kelembagaan yang sama merupakan ciri penting posisi politik kelembagaan Indonesia, yaitu lembaga yang bertugas memperluas akses adalah juga lembaga yang berwenang memutusnya.

Aktor negara pengelola ruang digital berpusat pada Kementerian Komunikasi dan Digital (Komdigi) yang merupakan hasil dari transformasi Kominfo pada awal pemerintahan Prabowo-Gibran. Komdigi memegang kewenangan paling luas, seperti pengendalian registrasi PSE, pemblokiran dan pemutusan akses, permintaan penghapusan konten, pengelolaan aduan, hingga penegakan sementara UU PDP selama badan pengawas belum terbentuk yang sementara perannya dijalankan oleh Direktorat Jenderal Pengawasan Ruang Digital (Kompas, 2026b). Di sampingnya berdiri Badan Siber dan Sandi Negara (BSSN) untuk keamanan siber, lalu ada Direktorat Tindak Pidana Siber (Dittipidsiber) Polri yang menjalankan penegakan hukum pidana, patroli siber, dan pendekatan "polisi virtual" yang menegur unggahan warga sejak 2021, kemudian ada kejaksaan dan pengadilan sebagai hilir pemidanaan, serta lembaga-lembaga penjamin seperti Dewan Pers, Komisi Informasi, Komnas HAM, dan Komnas Perempuan yang menangani dimensi kebebasan pers, keterbukaan informasi, dan hak asasi (SAFEnet, 2026).

Celah kelembagaan paling mencolok adalah absennya lembaga pengawas pelindungan data pribadi. Hampir empat tahun sejak UU PDP disahkan dan hingga pertengahan 2026, Badan PDP belum berdiri, saat ini rancangan

peraturan presiden pembentukannya masih berproses di tingkat harmonisasi dan penetapan, sementara keterlambatan ini telah digugat ke Mahkamah Konstitusi oleh masyarakat sipil (CNBC Indonesia, 2026; Hukumonline, 2026; Kompas, 2026b). Pengawasan sementara oleh Komdigi menimbulkan persoalan struktural seperti kementerian yang menjadi pengendali data sekaligus regulator ruang digital merangkap pengawas pelindungan data. Hal ini menunjukkan ketiadaan independensi yang justru menjadi alasan lembaga itu disyaratkan undang-undang. Dalam peta kelembagaan ini, fungsi pengawasan independen atas kewenangan digital eksekutif praktis hanya dijalankan oleh Mahkamah Konstitusi melalui pengujian norma sebagaimana ditunjukkan Putusan No. 105/PUU-XXII/2024 dan oleh masyarakat sipil melalui pemantauan.

Dalam praktik harian, pengelolaan ruang digital berjalan melalui lima mekanisme utama. Pertama, melalui pendaftaran PSE yang menjadikan status legal platform bergantung pada kepatuhan administratif kepada pemerintah. Kedua, sistem aduan konten dan perintah penghapusan dengan tenggat singkat, yang menekan platform untuk menghapus lebih dahulu dan memeriksa kemudian. Ketiga, pemblokiran situs dan layanan melalui TrustPositif, dari situs perjudian hingga layanan arsip global seperti Archive.org (Freedom House, 2025). Keempat, penindakan pidana melalui patroli siber dan laporan warga, yang menjadi mesin utama kriminalisasi ekspresi (SAFEnet, 2026). Kelima, pemanggilan dan negosiasi informal dengan platform yang dinilai sebagai mekanisme paling tidak transparan karena bekerja melalui daya tawar

perizinan sebagaimana tampak dalam kasus penangguhan izin TikTok pada 2025 (Freedom House, 2025; Gillespie, 2018) Kelima mekanisme ini menunjukkan bahwa pengelolaan ruang digital Indonesia lebih banyak berlangsung di ranah administratif dan informal daripada di ruang sidang yang terbuka.

Posisi politik ini dilengkapi dua kelompok aktor non-negara. Di satu sisi, platform global seperti Meta, Google/YouTube, TikTok, X yang menguasai arsitektur ekspresi warga Indonesia dan menjadi titik tumpu tekanan negara sekaligus pemegang kekuasaan moderasi privat (Gillespie, 2018). Di sisi lain, jejaring masyarakat sipil yang menjalankan fungsi pengawasan informal seperti SAFEnet yang memantau dan mendokumentasikan pelanggaran hak digital, Lembaga Studi dan Advokasi Masyarakat (ELSAM) mengadvokasi pelindungan data, Institute Criminal Justice and Reform (ICJR) mengawal reformasi hukum pidana, Aliansi Jurnalis Independen (AJI) dan Lembaga Bantuan Hukum (LBH) Pers melindungi kerja jurnalistik, sementara koalisi advokasi seperti Tim Advokasi untuk Demokratisasi Ruang Digital Indonesia (TAKDIR) membawa persoalan struktural ke Mahkamah Konstitusi (Masduki & Wendratama, 2025; Rahayu et al., 2024; SAFEnet, 2026). Ketiadaan pengawas negara yang independen membuat peran jejaring ini melampaui advokasi biasa dan merekalah yang secara *de facto* menjalankan fungsi akuntabilitas dalam tata kelola digital Indonesia.

Dari deskripsi di atas, posisi politik pengelolaan kebebasan digital Indonesia dapat dirangkum dalam empat ciri. Pertama, konsentrasi kewenangan pada

eksekutif, yang mana kewenangan menentukan, membatasi, dan menghukum terkumpul di kementerian dan kepolisian, dengan uji yudisial hanya sebagai koreksi belakangan. Kedua, ketimpangan antara kapasitas membatasi dan kapasitas melindungi yaitu infrastruktur dan kelembagaan pengendalian (pemblokiran, patroli, tekanan platform) telah matang dan beroperasi penuh, sementara kelembagaan pelindung (badan PDP, mekanisme pemulihan korban) belum berdiri atau lemah. Ketiga, informalitas, di mana sebagian besar keputusan yang menentukan nasib ekspresi warga seperti penghapusan, penangguhan, negosiasi dengan platform terjadi di ruang administratif dan informal yang tidak transparan. Keempat, akuntabilitas yang bertumpu pada aktor non-negara, fungsi pengawasan efektif dijalankan masyarakat sipil dan sesekali Mahkamah Konstitusi, bukan oleh desain kelembagaan negara itu sendiri.

4.2 Kecenderungan Kebebasan Digital dalam Masa Pemerintahan Prabowo Subianto-Gibran Rakabuming Raka

Bab sebelumnya telah membangun tiga hal yang menjadi bekal analisis pada ini. Pertama, mengenai kerangka konseptual kebebasan digital yang dipahami sebagai konsep multidimensi, seperti halnya kondisi ideal ruang digital yang terbuka, aman, setara yang kemudian dianalisis ke dalam empat domain hak digital, yaitu hak akses, hak bebas berekspresi, hak aman dan hak kesetaraan di ruang digital. Empat domain terebut yang akan memisahkan pelanggaran apa saja yang terjadi di ruang digital. Kedua, posisi politik, di mana

sejauh ini Indonesia masih mengandalkan kewenangan eksekutif sebagai struktur utama yang mengatur ruang digital di Indonesia, terlebih konsentrasi penggunaan pidana sebagai salah satu penyelesaian yang paling sering digunakan untuk menyelesaikan pelanggaran di ranah daring. Ketiga, mengenai kondisi objektif seperti halnya infrasturktur pengendali yang sudah ada lalu dilanjutkan di masa pemerintahan Prabowo-Gibran, contohnya adalah polisi siber sebagai aparatur yang melakukan kriminalisasi ekspresi, pasal multitafsir, jaring operasi informasi, dan model kerja sama dengan platform.

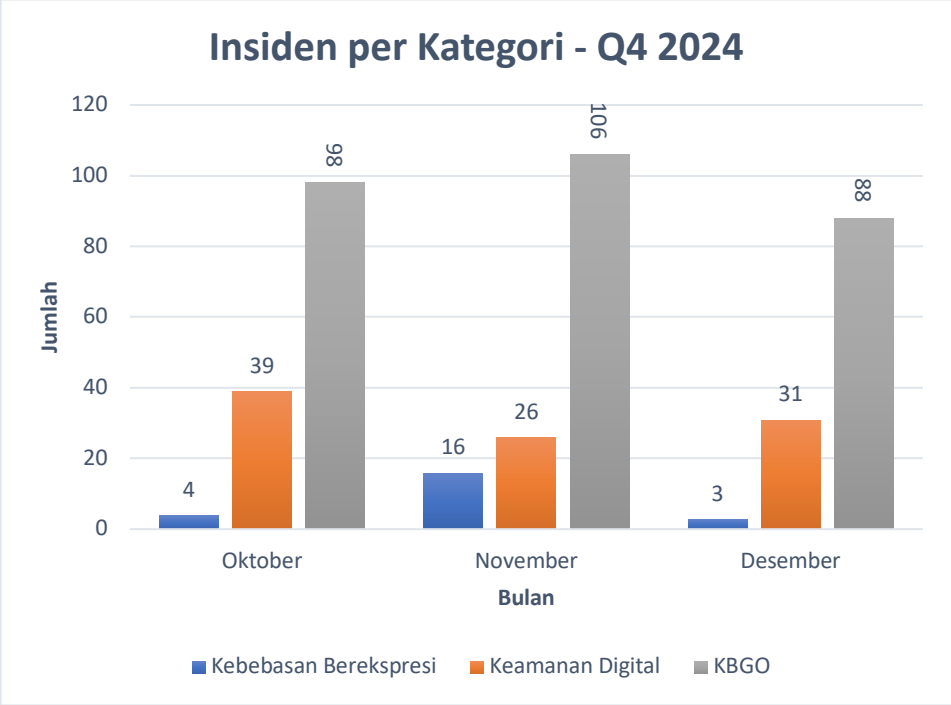
Analisis pada bab ini akan disusun berdasarkan dimensi pengukuran yang sudah ditetapkan pada bab sebelumnya, yakni, pertama akan memeriksa dimensi jumlah yang digunakan untuk membaca pergerakan frekuensi kasus yang terjadi antar periode. Kedua, dimensi analisis jenis pelanggaran yang ada pada domain akses, kebebasan berekspresi, keamanan digital, dan kesetaraan di ruang digital. Ketiga, menelurusi cakupan sasaran untuk melihat siapa korban dan kelompok paling terdampak pada pelanggaran hak digital tersebut. Keempat, memetakan aktor yang melakukan pelanggaran hak digital, kelima, melihat instumen apa yang digunakan untuk melakukan pelanggaran hak digital. Terakhir, menilai bagaimana dampak itu berlangsung pada perilaku warga atau pengguna.

Pada 20 Oktober 2024, Prabowo Subianto-Gibran Rakabuming Raka dilantik sebagai presiden dan wakil presiden sehingga melanjutkan sistem dan instrumen pengendalian ruang digital yangs sudah ada sebelumnya. Instrumen itu antara lain ialah penggunaan pasal hukum pidana untuk menindak ekspresi

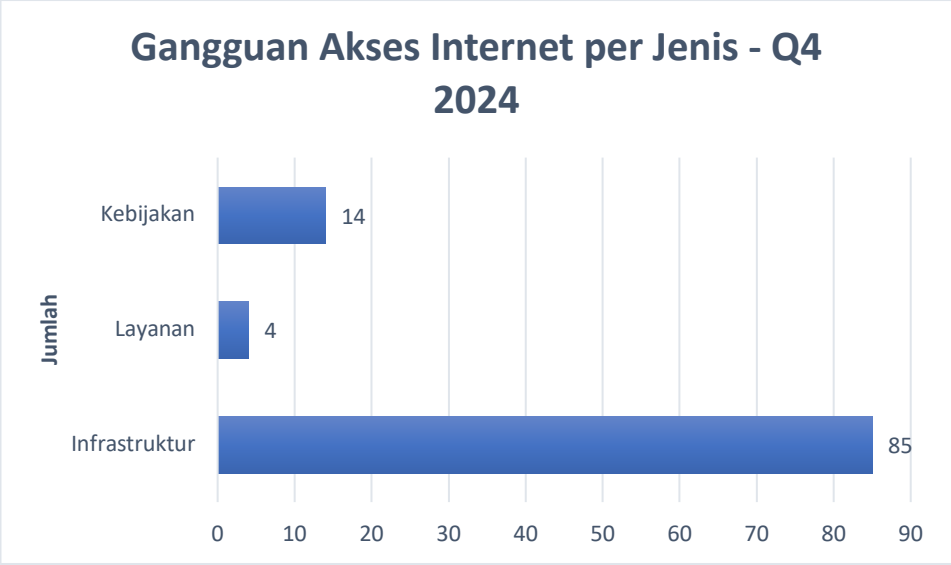
di ruang digital, alat penyaring konten, aparatus yang menindak warga sipil di ruang digital, hingga operasi informasi. Analisis dilakukan dengan menempatkan pelanggaran hak digital sebagai unit analisis. Setiap kasus yang terdokumentasi dinilai sebagai satuan data yang berisi informasi bentuk pelanggaran, pihak yang menjadi sasaran (korban), aktor yang terlibat, instumen yang digunakan, hingga dampak yang ditimbulkan, baik kepada korban maupun kelompok yang lebih luas. Analisis ini dilakukan karena anka keseluruhan tidak semata dapat membaca pola dan dan kecenderungan kebebasan berekspresi sehingga analisis yang digunakan harus lebih kompleks. Pola kekerasan, pelanggaran dan penggunaan kekuasaan dapat direkonstruksi melalui pembacaan sistematis kasus-kasus yang ada.

4.3 Analisis Dimensi Jumlah

Dimensi jumlah ialah lapisan analisis paling awal dan paling dasar yang memberikan gambaran awal mengenai intensitas tekanan terhadap kebebasan digital dan menjadi titik awal untuk membaca data secara keseluruhan mengenai kebebasan digital di Indonesia. Jumlah akan dibaca secara temporal, berurutan dari waktu ke waktu supaya pola perubahannya lebih jelas, terutama apabila terjadi momentum tertentu yang mengindikasikan adanya eskalasi kasus karena momentum tersebut. Kemudian pembuktian eskalasi tersebut akan dilakukan pada analisis dimensi selanjutnya.



Gambar 4.1 Insiden per Kategori Q4 2024
Sumber: diolah peneliti (2026)



Gambar 4.2 Gangguan Akses Internet per Jenis – Q4 2024
Sumber: diolah peneliti (2026)

Pada tiga bulan pertama pemerintahan Prabowo-Gibran, dapat dilihat bahwa pelanggaran kebebasan digital masih didominasi oleh domain

pelanggaran rasa aman dan setara di ruang digital. Dibuktikan dengan tingginya kasus Kekerasan Berbasis Gender Online (KBGO). Kasus KBGO biasanya akan beririsan dengan kasus serangan digital, yang membedakan ialah KBGO secara spesifik menyerang orientasi seksual, gender, atau ketubuhan seseorang. Ini menjadi ciri dan pola yang khas dari KBGO sehingga dibedakan dari domain serangan digital. Kemudian, yang membedakan selanjutnya apabila dibandingkan dengan kekerasan seksual di ranah fisik ialah biasanya KBGO disertai dengan penyebaran konten yang selanjutnya menjadi jejak digital yang sulit untuk dihapus. Pola KBGO juga dapat dilihat tidak terbatas pada kondisi tertentu seperti wilayah atau waktu tertentu.

Sejak tiga bulan pertama pelantikan Prabowo-Gibran, belum ditemukan KBGO yang didasari motif politik, namun demikian terdapat satu kasus penyalahgunaan teknologi kecerdasan buatan atau *Artifisial Intelligence* (AI) dengan korbannya ialah anak dan proses hukum tidak berjalan hingga saat ini. Korban bersama pendampingnya sempat mengalami penolakan dari Polres Jakarta Selatan saat pertama kali melaporkan kasusnya. Laporan kasus tersebut diterima pihak kepolisian setelah pendampingnya memviralkan kasus tersebut di media sosial, sementara pelaku melaporkan pendamping korban dengan pasal pencemaran nama baik UU ITE. Ini menunjukkan bahwa instrumen hukum pidana berupa pasal multitafsir masih digunakan untuk merepresi korban kekerasan seksual.

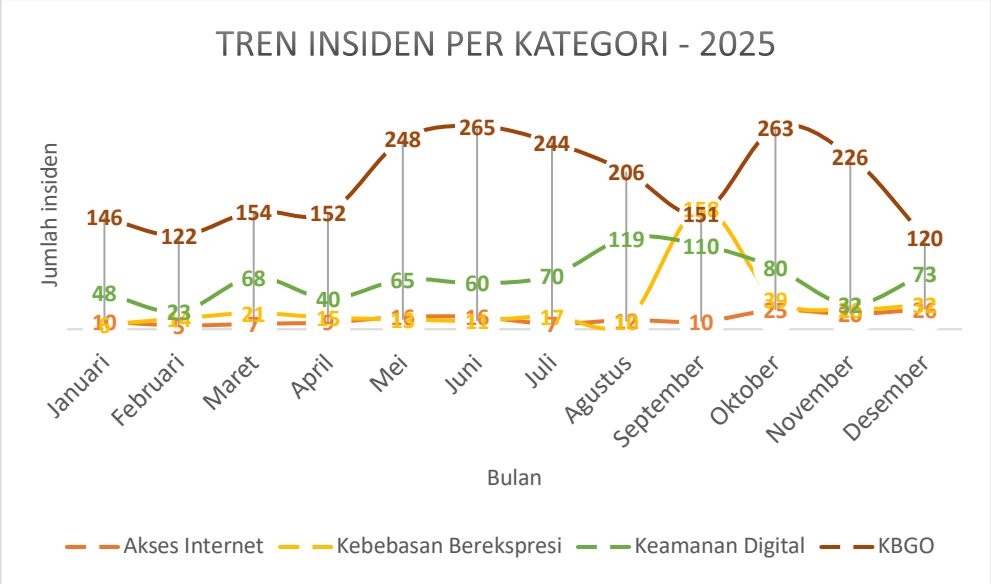
Selanjutnya, pada domain serangan digital sudah ditemukan motif politik di tiga bulan pertama pelantikan Prabowo-Gibran, secara keseluruhan terdapat

kenaikan kasus serangan digital apabila dibandingkan dengan tahun sebelumnya. Terdapat kasus penangguhan akun kepada beberapa pengguna akun X yang aktif bersuara mengenai isu #KawalMK yang mana isu tersebut merupakan isu politik. #KawalMK muncul setelah ada indikasi kecurangan dalam pencalonan Gibran sebagai wakil presiden, yang menjadi perhatian adalah bahkan isu ini masih diperbincangkan setelah Gibran resmi dilantik sebagai wakil presiden. Pengguna X yang mengalami penangguhan akun mendapat pemberitahuan melalui surel berupa link unggahan yang dianggap melanggar hukum yang berlaku di Indonesia, namun demikian tidak dijelaskan secara jelas pasal apa yang dilanggar.

Domain selanjutnya ialah kebebasan berekspresi. Pada masa peralihan pemerintahan di tiga bulan pertama, tidak ditemukan kasus yang terindikasi bagian dari kasus bermuatan politik, meskipun pada awal tahun 2024 hingga pertengahan tahun banyak kasus kriminalisasi yang bermotif politik karena berkenaan dengan momentum Pemilihan Umum (Pemilu). Pada tiga bulan pertama pemerintahan Prabowo-Gibran, ditemukan beberapa rancangan peratuhan yang berpotensi digunakan untuk melakukan represi kepada masyarakat sipil di ruang digital, di antaranya adalah Rancangan Perubahan Ketiga atas UU Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia (RUU POLRI), pada rancangan tersebut Polri memiliki kewenangan untuk membatasi dan memperlambat akses internet tanpa putusan pengadilan atau proses hukum yang jelas. Tanpa pengawasan yang akuntabel dan mekanisme yang efektif, peraturan ini berpotensi risiko peyalahgunaan

kekuasaan dan mempersempit ruang demokrasi terutama di ruang digital. Kedua, terdapat Rancangan Perubahan Kedua atas UU Nomor 34 Tahun 2004 tentang Tentara Nasional Indonesia (RUU TNI). Peraturan tersebut memungkinkan adanya perluasan wewenang prajurit aktif untuk mendapat jabatan sipil termasuk jabatan kementerian atau lembaga negara lainnya.

Domain terakhir ialah akses internet, terdapat beberapa perlanggaran akses internet yang terindikasi karena motif politik. Salah satunya ialah dua media yang berbasis di Papua, yaitu Laolao Papua dan The Papua Journal mengalami gangguan akses berupa sensor dan blokir. The Papua Journal mengalami penurunan konten yang memuat pemberitaan mengenai Pater Izak Bame yang saat itu terpilih menjadi Wakil Uskup Keuskupan Manokwari-Sorong. Sementara Laolao Papua mengalami pembatasan penyebaran konten di *Facebook*. Tak hanya itu, terdapat juga pembatasan akses terhadap informasi dan konten dukungan kepada Palestina di *Instagram*, sejumlah *template* yang digunakan untuk menyuarakan isu Palestina dibatasi dan dihapus oleh pihak *Instagram* tanpa pemberitahuan yang jelas. Indonesia Corruption Watch (ICW) juga mengalami pembatasan pada akun *Shopee* dan *Tokopedia* yang selama ini digunakan untuk menjual produk, adapun produk yang dilarang untuk dijual adalah *merchandise* kaos dengan desain “Korban Mulyono”.



Gambar 4.3 Tren Insiden Per Kategori 2015
Sumber: SAFEnet (2026)

Sepanjang 2025 tercatat 163 kasus gangguan akses internet, kategori dengan volume terkecil, hanya 4,5% dari total insiden tahun itu. Terdapat indikasi kenaikan pada paruh pertama tahun yang hanya hanya 63 kasus, sementara paruh kedua mencapai 100 kasus (SAFEnet, 2026). Angka terendah terjadi pada Februari (5) dan sempat naik ke 16 pada Mei dan Juni, lalu turun lagi ke 7 di Juli. Pada triwulan pertama tahun 2025, kategori kebijakan didominasi oleh rencana peraturan yang berpotensi mempersempit gerak masyarakat sipil di ruang digital, seperti inisiasi pembentukan PP Tunas, pembaruan sistem moderasi konten (SAMAN), sementara dari sisi infrastruktur, SAFEnet mencatat permasalahan yang dominan ialah melemahnya jaringan Telkomsel di wilayah Terpencil, Tertinggal, dan Terluar (3T) di Pulau Sumatera. Hal ini dikeluhkan masyarakat karena cukup berdampak pada hambatan mengakses

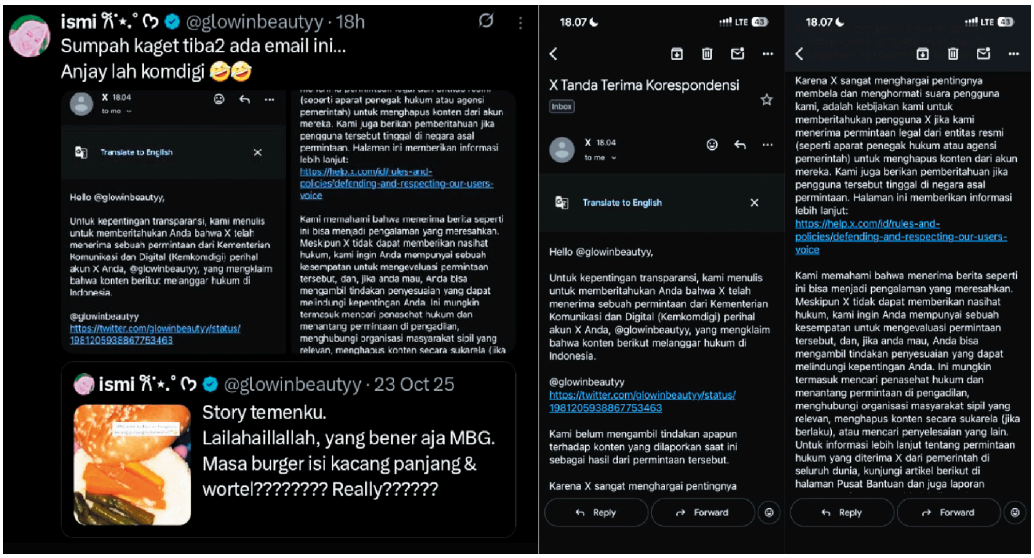
informasi dan layanan publik. Sementara itu pada triwulan kedua tahun 2025, dampak dari kewajiban sektor privat untuk mendaftar PSE berdasar pada Permenkominfo Nomor 5 Tahun 2020 masih cukup terasa. Terdapat insiden pemblokiran situs archive.org, e-Bay karena tidak mendaftar PSE. Selain itu, terdapat regulasi yang mulai dijalankan yaitu migrasi pendaftaran dari kartu sim fisik ke e-sim. Kasus lainnya adalah penyensoran Pulau Gag di aplikasi Google Earth yang disinyalir dilakukan oleh platform atas permintaan dari Komdigi karena berkaitan dengan aktivitas industri ekstraktif pertambangan yang sedang berjalan.

Lonjakan sesungguhnya baru muncul di kuartal terakhir yaitu Oktober 25, November 20, dan Desember 26, selama tiga bulan mencapai 71 kasus atau 44% dari seluruh kasus setahun. Desember menjadi bulan tertinggi, dan tren yang belum melandai di akhir tahun mengindikasikan tekanan pada akses internet justru mengeras menjelang tutup tahun. Lonjakan ini dipengaruhi oleh adanya bencana banjir di Sumatera dan pemulihannya yang begitu lambat. Di sisi lain, apabila ditinjau dari aspek kebijakan, permasalahan kewajiban pendaftaran PSE masih mendominasi, selain itu juga terdapat momen di mana pemerintah meminta data pengguna kepada platform seperti yang terjadi pada META dan TikTok pasca aksi demonstrasi Agustus 2025. Hal ini selaras dengan meningkatnya kriminalisasi ekspresi di ranah daring yang terjadi, dan berimbas pada mudahnya pihak kepolisian mendaptkan data pribadi pengguna hingga titik geolokasi secara spesifik.

Kategori kebebasan berekspresi mencatat 362 kasus, atau 10% dari total. Januari sebagai titik terendah (6) dan Maret sebagai puncak periode itu (21). Namun September memutus pola tersebut sepenuhnya dengan 158 kasus, yang mana angka tersebut hampir delapan kali lipat rata-rata bulan-bulan sebelumnya, dan menyumbang 44% dari total kasus setahun. Setelah puncak itu angkanya turun tajam tetapi tidak kembali ke level semula, Oktober 39 kasus, November 26 kasus, Desember 32 kasus, masih di atas rata-rata delapan bulan pertama (sekitar 13 kasus). Lonjakan September berkaitan dengan banyaknya kriminalisasi ekspresi yang dilakukan oleh pihak kepolisian. Sebanyak 157 korban kriminalisasi pada 2025 mengalami perburuan secara fisik dan digital oleh kepolisian, termasuk adanya penyitaan barang bukti perangkat digital tanpa surat keputusan dan penahanan tanpa pendampingan hukum yang ideal. Pasal yang paling banyak digunakan pihak kepolisian untuk melakukan penangkapan dna penahanan adalah Pasal 28 (2) UU ITE *juncto* Pasal 45A (2) UU ITE tentang ujaran kebencian yang menjerat 77 dari total korban. Banyak pula korban di antaranya yang dijerat menggunakan pasal penghasutan karena mengunggah respons dan informasi demonstrasi di media sosial, seperti yang dialami oleh Laras Faizati (pegawai swasta), Adetya Pramandera (Walhi Jawa Tengah), Fathul Munif (Aksi Kamisan Semarang). TikTok menjadi salah satu platform yang paling banyak dilaporkan selain X dan Instagram, yakni sebanyak 39 kasus, ini salah satu yang mendasari permintaan data pribadi pengguna oleh pihak kepolisian.

Domain selanjutnya adalah serangan digital, yang mana pada 2025 tercatat terdapat 788 kasus, keamanan digital menjadi kategori terbesar kedua (21,8% dari total). Lonjakan terjadi di bulan Maret sebanyak 68 kasus, hal ini berkenaan dengan momentum penolakan warga terhadap revisi UU TNI yang banyak dilakukan secara daring. Tiga demonstran di Surabaya seketika tidak dapat mengakses akun Whatsappnya karena diambil alih sesaat setelah melakukan aksi secara langsung. Terdapat juga ancaman dan tekanan untuk menurunkan unggahan yang dianggap menyebarkan kebencian terhadap pemerintah, adapun akun tersebut antara lain adalah @barengwarga, @BudiBukanIntel, @karimakayyim, @Imparsial. Keempat akun tersebut mendapat ancaman dan tekanan di waktu yang berdekatan dan pada hari yang sama. Lonjakan kasus kembali terjadi pada Agustus sebanyak 199 kasus dan September 110 kasus. Pada bulan keduanya dipengaruhi oleh aksi penolakan kenaikan tunjangan DPR RI yang salah satu dampaknya adalah kematian Affan Kurniawan karena dilindas kendaraan milik BRIMOB. Banyak warga yang melakukan kritik secara daring dan menyampaikan kekecewaan terhadap respons pemerintah disaat krisis justru mendapat intimidasi dan serangan digital. Di sejumlah daerah terdapat pelanggaran hak digital berupa pengambilalihan aset data digital tanpa adanya surat pemberitahuan yang sah sebanyak 15 kasus, penyitaan perangkat secara paksa sebanyak 15 kasus, pengancaman 6 kasus, doxing 5 kasus, dan seluruhnya berkaitan dengan momentum aksi Agustus 2025. Selain momentum aksi demonstrasi Agustus 2025, kritik terhadap Makan Bergizi Gratis (MBG) juga menjadi pemicu melonjaknya serangan digital di

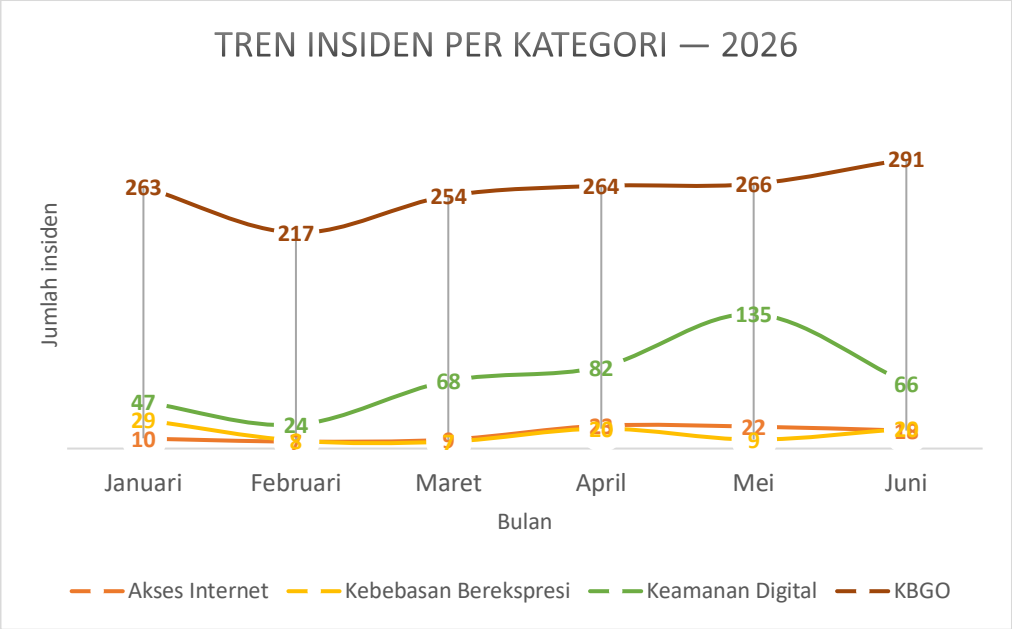
Oktober dan November 2025. Beberapa pengguna mendapat teguran oleh X via surel atas permintaan Komdigi yang menyampaikan bahwa unggahan MBG telah melanggar hukum yang berlaku di Indonesia, namun tidak disertakan pasal yang sudah dilanggar oleh pengguna tersebut.



Gambar 4.4 Teguran X kepada pengguna atas permintaan Komdigi
Sumber: Peneliti, 2026

Selanjutnya, ialah domain KBGO. KBGO mendominasi keseluruhan data dengan 2.297 kasus. Pada 2025, sudah ditemukan KBGO yang didasari oleh motif politik. Pada momentum penolakan revisi UU TNI, korban perempuan mendapatkan *flaming* atau teror malalui pesan dan kolom komentar terkait dengan identitas gender dan ketubuhannya. Adapun pelaku disinyalir berasal dari bagian satuan militer. Ancaman tidak hanya terjadi secara daring, namun ada indikasi tereskalasi secara fisik karena terdapat ancaman akan mendatangi korban. Melalui kasus ini dapat dilihat bahwa KBGO tidak hanya menjadi bagian dari serangan digital, melainkan bagian dari cara negara untuk menekan warga negara yang mengkritik kebijakan yang tengah dijalankan oleh

pemerintah. Secara spesifik, ini menunjukkan adanya penggunaan relasi kuasa pada warga sipil. Kasus lainnya adalah *doxing* yang dilakukan pendengung kepada salah satu warga sipil yang melakukan kritik terhadap sikap pemerintah pasca aksi demonstrasi Agustus 2025.



Gambar 4.5 Tren Insiden Per Kategori 2026

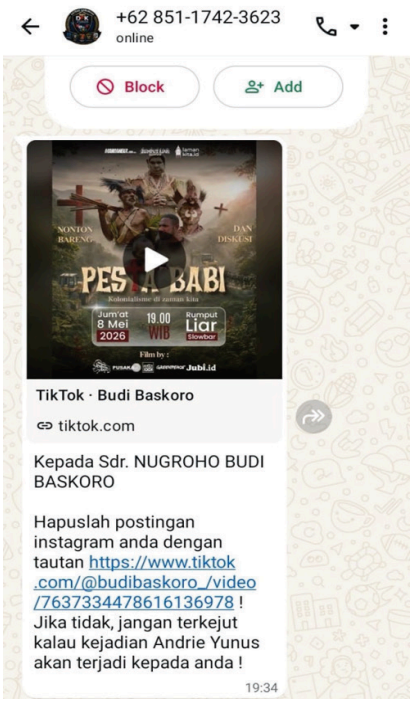
Selama Januari–Juni 2026 tercatat 89 kasus gangguan akses internet. Kuartal pertama masih di dominasi oleh kasus yang berkenaan dengan bencana alam di Sumatera. Pemulihan belum efektif dilakukan oleh pemerintah. Pada Februari 2026, laman Wikimedia tidak dapat diakses pengguna dan kontributor, SAFEnet menemukan bahwa domain tersebut sudah diblokir oleh Komdigi melalui mekanisme *trust positif*. Komdigi kemudian mengarahkan Wikimedia mendaftar PSE agar situsnya dapat diakses kembali. Pada kuartal yang sama Komdigi melalui X juga kembali mengirimkan peringatan pada akun Soe Tjen Marching (@SoeTjenMarching) seorang akademisi dan aktivis.

Akun tersebut bukanlah yang pertama kali menerima peringatan, Adapun peringatan tersebut disinyalir berkenaan dengan aktivitas kritiknya terhadap kebijakan pemerintah, namun Komdigi melalui X tidak menyebutkan pasal yang dilanggar. Sementara itu di kuartal kedua 2026, pelanggaran hak akses yang berkenaan dengan aspek kebijakan masih di dominasi oleh Komdigi yang mengultimatum 25 *platform* untuk segera mendaftar PSE. Komdigi bersama dengan DPR RI juga membahas kebijakan untuk meregulasi ulang kepemilikan media sosial dengan satu akun hanya bisa diregistrasi dengan satu nomor kartu sim. Tentu kebijakan ini adalah bentuk kontrol pemerintah atas warga dan pengguna media sosial, pemerintah dengan mudah mendapatkan data pribadi pengguna dan mengetahui siapa pemilik akun.

Domain selanjutnya adalah kebebasan berekspresi. Pada kuartal pertama kasus tertinggi ada di bulan Januari sebanyak 29 kasus. Salah satu kasus bermotif politik yang paling menonjol adalah kriminalisasi terhadap jurnalis Nusa Tenggara Barat (NTB) bernama Badai yang mengungkap jaringan peradaran narkotika di NTB. Ia justru diadukan oleh seorang pejabat publik dengan pasal pencemaran nama baik. Kasus ini menjadi salah satu batu uji terhadap perlindungan jurnalis sebagai salah satu kategori dari kelompok berisiko tinggi serta bagaimana perlindungan terhadap produk jurnalistik. Pada triwulan kedua, kasus dengan latar belakang politik yang paling mengemuka salah satunya adalah kriminalisasi kepada Tiyo, mantan ketua BEM UGM yang sebelumnya mengkritik kebijakan MBG. Kritik tersebut dilatarbelakangi oleh meninggalnya seorang anak di Nusa Tenggara Timur yang mengakhiri

hidupnya karena tidak mampu membeli alat tulis. Setelah melakukan kritik terhadap kebijakan MBG, dirinya dilaporkan ke pihak kepolisian oleh salah satu pengacara publik karena dianggap menghasut publik untuk menekan pemerintah menghentikan program MBG dan dianggap menghina nama baik presiden dan wakil presiden. Laporan ini merujuk pada pasak 263 (1) KUHP Nasional.

Domain selanjutnya adalah serangan digital, terdapat 422 kasus dalam enam bulan, keamanan digital menjadi kategori terbesar kedua (19,5% dari total). Pada triwulan pertama, ditemukan kasus dengan latar belakang politik. Terdapat kasus yang menimpa seorang konten kreator yang mengkritik kebijakan Komdigi yang menggunakan Google Drive untuk menghimpun data rekrutmen calon pegawai dan dibuat dalam akses publik. Setelah berkomentar mengenai hal tersebut, korban mengalami serangan digital berupa serangan *bot* pada aplikasi *start up* miliknya yaitu ordal.id. Sementara itu pada triwulan kedua juga ditemui kasus berlatar belakang politik, pertama ialah 9 kasus yang berkaitan dengan film Pesta Babi, kritik terhadap TNI, MBG, dan Sufmi Dasco. Jurnalis media Mongabay Indonesia, Nugroho Budi Baskoro, mendapat pesan ancaman dan tekanan sesaat setelah mengunggah informasi *nobar* film Pesta Babi. Kedua, tercatat 60 kasus kebocoran data, 45 di antaranya ialah kebocoran data situs pemerintah.



Gambar 4.6 Bukti Pengancaman Terhadap Jurnalis

Domain terakhir ialah KBGO, selama 2026 terdapat 1.555 kasus. Motif politik ditemukan pada kasus pengalihan isu terhadap kelompok ragam gender. DPR RI sedang dalam masa proses penyusunan RUU Penyiaran dengan dalih bahwa perlu pembatasan konten dan tayangan yang berhubungan dengan LGBT karena dinilai merusak generasi muda dan merugikan anak-anak. Padahal, apabila dilihat lebih jauh, RUU Penyiaran justru akan membatasi tayangan seperti halnya jurnalisme investigatif dan mengancam independensi media melalui beberapa pasal yang sudah dirumuskan dalam RUU Penyiaran tersebut. Pada triwulan kedua, motif politik juga dialami oleh 37 lembaga, komunitas, atau organisasi yang bergerak di isu pemberdayaan perempuan dan kelompok ragam gender mengalami *doxing* dan *framing* oleh pendengung. *Doxing* dan

framing tersebut menyatakan bahwa organisasi tersebut berafiliasi dan didanai oleh lembaga asing dan menormalisasi LGBT di Indonesia.

4.4 Analisis Jenis Pelanggaran Hak Digital

Apabila dimensi jumlah menunjukkan seberapa besar tekanan yang terjadi, dimensi jenis menunjukkan pada bagian mana tekanan itu bekerja. Analisis pada dimensi ini mengklasifikasikan setiap kasus menurut komponen hak yang dilanggar, mengikuti definisi operasional yang telah ditetapkan, yaitu

1. Pelanggaran terhadap akses informasi

   SAFEnet membagi jenis pelanggaran akses terhadap informasi ke dalam tiga aspek, yaitu pertama, infratruktur yang mencakup jaringan teknologi internet yang bermasalah atau tidak berfungsi, termasuk apabila terdapat *blank spot* dan ini menjadi tanggung jawab pemerintah dan jasa penyedia layanan internet. Kedua, layanan, ini mencakup aksesibilitas pengguna dalam mengakses layanan internet dan digital, termasuk biaya yang harus dikeluarkan, aksesibilitas terhadap pengguna disabilitas, layanan yang diskriminatif maupun yang bias kelas. Ketiga, kebijakan yang masuk dalam permasalahan regulasi, isu aturan, hingga keputusan politik.

Tabel 4.1 Pelanggaran Hak Akses Internet di Indonesia 2025

Kategori	Q1	Q2	Q3	Q4	Total
Infrastruktur	12	25	17	27	81
Kebijakan	9	13	11	4	37
Layanan	1	3	1	2	7
TOTAL	**22**	**41**	**29**	**33**	**125**

Sumber: SAFEnet, 2026

Melalui tabel di atas dapat dilihat bahwa pelanggaran hak akses internet yang mendominasi ialah permasalahan terkait infrastruktur dan kebijakan. Infrastruktur banyak berkaitan dengan pembangunan yang tidak merata, terutama di wilayah 3T. Sementara itu kebijakan berhubungan dengan permasalahan peraturan pemerintah yang berpotensi mempersempit ruang demokrasi di ruang digital. Salah satu kebijakan yang disoroti dalam tataran masyarakat adalah kebijakan pemerintah menertibkan internet komunitas. Internet komunitas lahir dari keinginan dan inisiatif warga untuk dapat mengakses internet sesuai dengan kemampuan yang dimiliki warga setempat. Pemerintah berinisiasai mengatur penggunaan internet karena dianggap illegal dan tidak mengikuti aturan yang berlaku, semnetara itu di sisi lain tindakan pemerintah justru mengabaikan kedaulatan warga dalam mengakses internet.

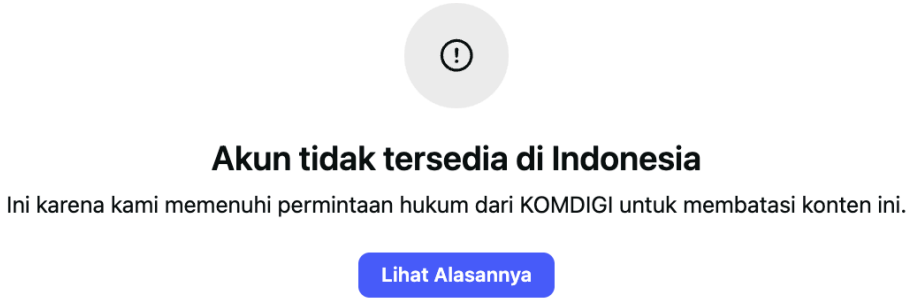
Tabel 4.2 Pelanggaran Akses Internet di Indonesia tahun 2026

Kategori	TW I (Jan–Mar)	TW II (Apr–Jun)	Total
Infrastruktur	6	15	21
Kebijakan	19	44	63
Layanan	1	4	5
TOTAL	**26**	**63**	**89**

Sumber: SAFEnet 2026

Selama semester pertama tahun 2026, pelanggaran akses internet didominasi oleh pelanggaran kebijakan dan infrastruktur. Kebijakan berkaitan dengan proses penurunan akun dan unggahan warga yang banyak terjadi di platform X, terdapat pula penangguhan akun dan kebijakan *georestriction* di akun Instagram yang diinisiasi oleh Komdigi, misalnya

yang terjadi pada akun @cabinetcourture_idn, akun tersebut mengungkap barang mewah yang digunakan oleh pejabat di Indonesia.



Gambar 4.7 Pemberitahuan di akun @cabinetcouture_idn

Sumber: Instagram

Selain hal tersebut, SAFEnet juga melakukan pendokumentasian terkait dengan pengiriman "surat cinta" atau peringatan kepada pengguna yang diinisiasi oleh Komdigi melalui *platform*. Adapun pada triwulan kedua terdapat 17 kasus pengiriman peringatan kepada 15 pengguna. Adapun konten yang ditindak bukanlah misinformasi atau berita bohong, melainkan kritik masyarakat sipil di ruang digital terhadap kebijakan pemerintah.

2. Pelanggaran kebebasan berekspresi

   SAFEnet membagi jenis pelanggaran kebebasan berekspresi berdasarkan latar belakang terjadinya kasus, terdapat beberapa latar belakang yang menjadi kategori utama yaitu politik, ekonomi, korupsi/kolusi/nepotisme, agraria atau lingkungan, faktor identitas sosial, dan beberapa kategori lainnya.

Tabel 4.3 Jenis Pelanggaran Kebebasan Berekspresi Berdasarkan Latar Belakang Kasus tahun 2025-2026

Isu	2025	2026 (1)	2026 (2)
Politik	215	13	9
Personal	44	6	9
Korupsi/Kolusi/Nepotisme	18	4	7
Ekonomi	17	8	9
Agraria/Lingkungan	14	-	1
Faktor Identitas Sosial	9	3	3
Kekerasan Seksual	6	-	4
Kemanusiaan/Krisis	5	-	-
Olahraga	4	-	-
Kesehatan	3	-	-
Ketenagakerjaan	3	-	-
Pendidikan	3	3	-
Kebijakan	2	-	-
Pelayanan Publik	2	-	-
Kebijakan publik	1	1	2
Kekerasan	1	-	2
Kekerasan Aparat	1	-	-
Penodaan Agama	1	6	1
Perlindungan Konsumen	1	-	-
TOTAL	**350**	**45**	**47**

Sumber: SAFEnet (2026)

Permasalahan di tahun 2025 didominasi oleh latar belakang politik, hal ini disebabkan oleh banyaknya kriminalisasi yang dialami oleh warga saat momentum demonstrasi Agustus dan September 2025. Polri menjadi terlapor terbanyak dalam lingkup kasus dengan latar belakang politik, yaitu sebanyak 17 kasus. Pasal yang paling sering digunakan adalah Pasal 28 ayat (2) UU ITE tentang ujaran kebencian terhadap individu atau kelompok. Ini digunakan ketika ada yang melakukan kritik terhadap institusi Polri. Lebih lanjut, aparat kepolisian siber melaporkan teridentifikasinya sekitar 592

akun media sosial yang diduga menyebarluaskan konten provokatif serta berpotensi menghasut masyarakat untuk melakukan tindakan yang bertentangan dengan hukum dalam konteks penyelenggaraan aksi demonstrasi. Ratusan akun tersebut telah dikenai tindakan pemblokiran melalui koordinasi dengan Komdigi. Kebijakan pemblokiran semacam ini menimbulkan persoalan normatif tersendiri, sebab pembatasan akses terhadap ruang ekspresi digital berpotensi mereduksi jaminan kebebasan berekspresi yang dilindungi konstitusi di Indonesia.

Rangkaian kasus yang dilatarbelakangi oleh politik memperlihatkan bahwa pembatasan kebebasan berekspresi di Indonesia tidak dapat dibaca sebagai insiden yang berdiri sendiri, melainkan sebagai pola yang bekerja secara sistematis melalui instrumentalisasi hukum pidana. Terdapat korelasi yang konsisten antara derajat kedekatan suatu ekspresi dengan kepentingan kekuasaan dan probabilitas ekspresi tersebut diproses secara hukum. Kritik yang menyasar kebijakan unggulan pemerintah, mempersoalkan validitas klaim capaian negara, maupun mengungkap dugaan keterlibatan pejabat dalam kejahatan terorganisasi, cenderung memicu respons pemidanaan.

Pada tataran praktik, terjadi pergeseran aktor represi dari negara secara langsung menuju pelibatan aktor non-negara yang berafiliasi dengan kekuasaan, seperti halnya pada kasus pelaporan Tiyo, mantan ketua BEM UGM. Pelaporan yang diajukan oleh organisasi pendukung pemerintah maupun individu yang mengklaim mewakili kepentingan publik memungkinkan negara mempertahankan jarak formal dari tindakan

represif, sekaligus memperoleh legitimasi seolah-olah proses hukum lahir dari inisiatif masyarakat. Fenomena ini dapat dipahami sebagai bentuk pengalihdayaan represi (*outsourcing of repression*) yang mengaburkan pertanggungjawaban negara atas penyempitan ruang sipil.

3. Serangan Digital

Serangan digital menempati posisi khusus dalam analisis jenis pelanggaran karena karakteristiknya yang berbeda dari bentuk pembatasan lainnya. Berbeda dengan kriminalisasi yang berlangsung melalui prosedur hukum formal dan dapat diidentifikasi pelakunya, atau pemblokiran yang dilakukan secara terbuka oleh otoritas berwenang, serangan digital umumnya berlangsung tanpa atribusi yang jelas seperti halnya pelakunya anonim, prosesnya tidak terdokumentasi secara resmi, dan pertanggungjawabannya hampir tidak pernah diperoleh melalui mekanisme hukum yang tersedia. Karakteristik inilah yang menjadikannya, dalam kerangka Feldstein (2021), sebagai teknik yang secara khusus menarik bagi aktor negara maupun aktor yang bekerja searah dengan kepentingannya, sebab efek penggentarannya tinggi sementara risiko politiknya rendah.

Tabel 4.4 Serangan Digital Berdasarkan Jenis pada 2025-2026

Jenis Serangan	2025	2026 (1)	2026 (2)
Pengancaman	209	36	73
Peretasan	166	7	60
Doxing	118	28	45
Akun Ditangguhkan	85	-	-
Lainnya	59	7	12
Pemerasan	48	9	6
Impersonasi	43	16	17

Jenis Serangan	2025	2026 (1)	2026 (2)
Akun tak bisa diakses	41	0	7
Phishing	33	8	11
Data Bocor	27	7	60
Penyitaan	21	-	-
Penyedotan Data	18	-	-
Trolling	14	7	4
Deface	8	-	-
Panggilan Massal	6	0	7
DDoS	6	1	4
Ransomware	5	1	0
TOTAL	**907**		

Sumber: SAFEnet (2025)

Rangkaian kasus selama 2025 memperlihatkan karakteristik yang membedakan serangan digital bermotif politik dari gangguan keamanan siber pada umumnya. Serangan siber konvensional umumnya bermotif ekonomi, menyasar korban secara acak atau berdasarkan kerentanan teknis, dan berhenti setelah tujuan finansialnya tercapai. Pola yang terekam dalam data justru menunjukkan sebaliknya pada tiga aspek.

Pertama, pemilihan sasaran bersifat selektif dan berkorelasi dengan tindakan politik korban. Serangan tidak diawali oleh kerentanan teknis, melainkan oleh unggahan kritik yang memperoleh perhatian publik. Urutan peristiwa. menunjukkan bahwa yang menjadi pemicu adalah tindakan berekspresi itu sendiri, bukan atribut teknis maupun ekonomis korban. Kedua, tujuan serangan adalah penghentian ekspresi, bukan perolehan keuntungan. Hal ini paling terang pada kasus 22 Mei 2025, ketika pesan dari nomor tidak dikenal secara eksplisit memerintahkan penghapusan unggahan

kritik. Tuntutan yang disampaikan bukan tebusan melainkan pencabutan pernyataan, sehingga sifat serangan bergeser dari kejahatan siber menjadi tindakan pembungkaman. Ketiga, perpindahan serangan dari ruang publik ke ruang privat menunjukkan strategi yang terarah. Migrasi dari X sebagai kanal ekspresi, ke Instagram sebagai medium serangan berbasis identitas, hingga WhatsApp sebagai saluran intimidasi langsung, memperlihatkan bahwa pelaku memahami fungsi berbeda tiap platform dan memanfaatkannya secara tepat. Perluasan sasaran hingga menjangkau keluarga korban memiliki logika politik yang spesifik seperti halnya pelaku mengubah biaya berekspresi dari risiko personal menjadi risiko relasional, sehingga penggentaran bekerja bahkan pada warga yang bersedia menanggung risiko bagi dirinya sendiri.

Memasuki tahun 2026, tiga kasus kebocoran data yang terdokumentasi memiliki karakteristik yang secara fundamental berbeda dari serangan digital yang dianalisis sebelumnya. Pada dugaan kebocoran data kepegawaian Kementerian Energi dan Sumber Daya Mineral (SAFEnet, 2026), kelemahan sistem rekrutmen Komdigi yang mengekspos berkas melalui Google Drive, serta dugaan kebocoran 76.217 data administrasi kependudukan pada laman Dinas Kependudukan dan Pencatatan Sipil Surabaya yang memuat nomor kartu keluarga, nomor induk kependudukan, nama, alamat, dan status, korban tidak dipilih berdasarkan sikap politiknya. Warga yang datanya terekspos tidak mengalami kerugian karena mereka mengkritik, melainkan karena mereka berurusan dengan

negara. Dengan demikian, kategori pelanggaran ini tidak dapat dianalisis menggunakan kerangka penargetan politik sebagaimana diterapkan pada kasus doksing dan intimidasi. Namun ini sangat mencerminkan bahwa meskipun sudah ada UU Perlindungan Data Pribadi, tidak menjamin keamanan data warga yang disimpan oleh pemerintah, demikian dengan pertanggungjawaban pemerintah atas risiko kebocoran data. Pada serangan digital bermotif politik, negara berada pada posisi aktor yang diduga menyerang atau membiarkan serangan, namun pada kebocoran data instansi, negara berada pada posisi pengendali data yang gagal menjalankan kewajiban perlindungannya. Kegagalan ini bersifat struktural, dan menunjukkan bahwa tata kelola internet dan perlindungan data masih harus banyak melalui tahap evaluasi dan perbaikan.

4. Kekerasan Berbasis Gender Online (KBGO)

Kekerasan berbasis gender online (KBGO) menempati kedudukan yang khas dalam analisis jenis pelanggaran karena karakter aktor dan mekanisme kerjanya yang berbeda dari kategori-kategori sebelumnya. Pada kriminalisasi ekspresi, pelaku pelanggaran adalah negara melalui aparat penegak hukumnya; pada pembatasan akses, pelakunya adalah otoritas administratif dan platform, sedangkan pada KBGO, pelaku sebagian besar merupakan aktor horizontal yang bertindak tanpa atau dengan mandat kekuasaan formal.

Penelitian ini menempatkan KBGO sebagai bagian dari analisis berdasarkan dua pertimbangan. Pertimbangan pertama bersifat konseptual.

Definisi operasional yang digunakan memaknai kebebasan digital sebagai kondisi penggunaan ruang digital yang terbuka, aman, setara, dan terlindungi; KBGO menyerang tiga di antaranya secara langsung dengan menjadikan ruang digital tidak aman, tidak setara, dan tidak terlindungi bagi kelompok tertentu. Sekalipun pelakunya horizontal, KBGO tidak sepenuhnya terpisah dari struktur kekuasaan. Sejumlah bentuk KBGO, terutama doksing dan penyebaran materi intim tanpa persetujuan muncul sebagai instrumen dalam serangan terhadap jurnalis dan aktivis perempuan, sehingga berfungsi sebagai teknik pembungkaman yang bekerja melalui kerentanan gender. Selain itu, lemahnya penegakan hukum dan ketiadaan mekanisme pemulihan yang efektif menempatkan negara pada posisi pembiaran, sebagaimana halnya pada kasus kebocoran data. Dengan demikian, KBGO dianalisis pada dua lapis sekaligus, yaitu sebagai pelanggaran privasi dan keamanan yang dialami korban, dan sebagai indikator kegagalan perlindungan yang bersifat struktural.

Tabel 4.5 Kasus KBGO di Indonesia 2025-2026

Jenis KBGO	2025	2026 (1)	2026 (2)
Ancaman penyebaran konten intim	1150	237	318
Pemerasan seksual (sextortion)	592	54	241
NCII	280	74	141
Sextortion dan ancaman penyebaran konten intim	274	131	0
Sextortion dan NCII	199	20	0
Penyebaran konten intim tanpa izin	158	12	34
Cyber harassment	119	20	25
Doxing berbasis gender	78	15	24

Jenis KBGO	2025	2026 (1)	2026 (2)
Perekaman tanpa izin (creepshot)	76	13	5
Penyebaran konten intim buatan tanpa izin (AI)	66	12	0
Peniruan akun berbasis gender	46	0	11
Penyerangan daring (flaming)	54	0	6
Lainnya	116	395	93
TOTAL		**983**	**898**

Sumber: SAFEnet (2026)

Kasus yang terjadi pada masa aksi penolakan RUU TNI Maret 2025 memperlihatkan bahwa KBGO tidak selalu dapat dibaca sebagai kekerasan interpersonal yang kebetulan berlangsung di ruang digital. Rangkaian peristiwanya menunjukkan struktur yang berbeda, yaitu keadaan di mana korban tidak diserang karena identitas gendernya semata, melainkan karena menyampaikan pernyataan politik dan gender kemudian menjadi saluran yang dipakai untuk menyerangnya. Keterkaitan temporal dengan siklus mobilisasi politik. Kemunculan kasus KBGO pada periode aksi penolakan RUU TNI dan gerakan Bubarkan DPR menunjukkan bahwa serangan mengikuti irama konflik politik, bukan irama kehidupan personal korban. Pola ini sejalan dengan temuan bahwa mekanisme kontrol terutama diaktifkan ketika ekspresi berpotensi memperoleh resonansi kolektif (King, Pan, & Roberts, 2013), dan menempatkan KBGO pada periode tersebut sebagai bagian dari respons terhadap gelombang kritik, bukan sebagai insiden yang berdiri sendiri.

Rangkaian peristiwa yang berlangsung sejak awal 2026 memperlihatkan mekanisme yang berbeda dari kasus-kasus KBGO yang telah dianalisis sebelumnya. Apabila pada kasus terdahulu serangan bergerak dari bawah, dilakukan aktor horizontal terhadap individu yang menyampaikan kritik, namun yang terjadi pada 2026 rangkaian ini bergerak dari atas, narasi yang dilontarkan aktor politik dan kemudian dikukuhkan instrumen kebijakan negara diikuti oleh serangan terhadap warga di tingkat masyarakat. Analisis atas rangkaian ini karenanya diarahkan pada empat lapis mekanisme yang saling terhubung.

Pembahasan RUU Penyiaran menempatkan pembatasan konten yang berkaitan dengan kelompok minoritas seksual sebagai salah satu justifikasi publiknya. Namun sebagaimana ditunjukkan penolakan berbagai pihak, draf yang sama juga memuat ketentuan yang membatasi jurnalisme investigatif dan berpotensi menggerus independensi media. Konfigurasi ini mengindikasikan pola instrumentalisasi, seperti halnya isu moral yang memiliki daya resonansi publik ditempatkan di permukaan pembahasan, sementara ketentuan yang berdampak pada kebebasan pers memperoleh perlindungan dari sorotan. Kelompok minoritas seksual dalam kerangka ini menempati posisi ganda yang merugikan, yaitu menjadi sasaran pembatasan sekaligus menjadi sarana legitimasi bagi pembatasan terhadap pihak lain. Dari sudut kebebasan digital, mekanisme ini penting dicatat karena memperlihatkan bahwa pembatasan ekspresi tidak selalu diajukan dengan

alasan keamanan negara, melainkan dapat diajukan dengan alasan perlindungan moral yang secara politis lebih sulit ditolak.

Pernyataan Amin Rais yang merupakan seorang tokoh politik yang mengaitkan identitas seksual seorang pejabat negara melalui *platform* video direspons dengan penghapusan konten oleh otoritas, tanpa disertai klarifikasi atas substansi pernyataannya. Respons semacam ini menghasilkan dua akibat yang saling memperkuat. Pertama, penghapusan tanpa koreksi hanya menghilangkan jejak pernyataan tanpa membantah premisnya, sehingga secara implisit membiarkan pandangan bahwa identitas tersebut merupakan sesuatu yang layak dijadikan bahan tuduhan. Pencatatan tujuh kasus KBGO yang menyasar kelompok minoritas seksual setelah beredarnya narasi tersebut menunjukkan adanya jalur yang menghubungkan wacana di tingkat elite dengan tindakan di tingkat masyarakat. Bentuk yang menonjol adalah *online outing*, yakni pengungkapan identitas sensitif seseorang tanpa persetujuannya, yang mana hal tersebut merupakan suatu tindakan yang secara teknis bagian dari pelanggaran privasi, tetapi dampaknya melampaui ranah digital. Hal ini tampak pada kasus seorang mahasiswa yang rekaman pribadinya diambil secara diam-diam dan disebarkan di media sosial, yang berujung pada dikeluarkannya korban dari perguruan tinggi dan pada tersudutnya keluarga korban di hadapan opini publik. Kasus ini memperlihatkan karakteristik yang membedakan pelanggaran privasi terhadap kelompok minoritas dari pelanggaran privasi pada umumnya, yaitu informasi yang tersebar tidak

hanya merugikan reputasi, tetapi mengaktifkan sanksi sosial dan institusional yang sudah tersedia dalam masyarakat, sehingga pelaku cukup membuka informasi dan membiarkan struktur sosial menjatuhkan hukumannya.

4.5 Analisis Cakupan Sasaran Pelanggaran Hak Digital

Dimensi cakupan sasaran mengalihkan fokus analisis dari pertanyaan mengenai apa yang dilanggar menuju pertanyaan mengenai siapa yang dilanggar haknya. Pergeseran fokus ini memiliki nilai analitis tersendiri karena distribusi korban menyimpan informasi mengenai logika kerja pembatasan yang tidak dapat diperoleh dari dimensi jumlah maupun jenis. Sebaran sasaran yang terkonsentrasi pada kelompok tertentu menunjukkan bahwa pembatasan bekerja secara selektif menurut posisi politik atau sosial korban dan sebaliknya, sebaran yang meluas menunjukkan bahwa batas ekspresi yang dianggap aman sedang bergeser dan menjangkau kelompok yang sebelumnya berada di luar jangkauan penindakan.

1. Akses Internet

   Pelanggaran pada komponen hak akses memiliki struktur korban yang secara fundamental berbeda dari pelanggaran pada komponen ekspresi maupun privasi. Pada kriminalisasi unggahan, doksing, atau intimidasi, korban dapat diidentifikasi secara individual, mengetahui dirinya menjadi korban, dan setidaknya secara teoretis memiliki pihak yang dapat dituntut pertanggungjawabannya. Pada pemblokiran dan gangguan akses, ketiga hal

tersebut umumnya tidak terpenuhi. Korban bersifat menyebar dan tidak berwajah, sebagian besar tidak menyadari bahwa haknya sedang dibatasi, dan tidak memiliki kedudukan hukum yang jelas untuk mengajukan keberatan. Karakteristik inilah yang menjadikan pelanggaran hak akses sebagai kategori yang paling jarang terdokumentasi sebagai kasus individual, sekalipun jumlah warga yang terdampak justru paling besar. Berdasarkan narasi kebijakan yang terdokumentasi sepanjang periode, sasaran korban pada kategori ini dapat dipilah ke dalam empat tipe.

Pemblokiran suatu layanan berdampak seragam pada seluruh penggunanya tanpa memandang perilaku masing-masing. Pada pemblokiran mesin pencari DuckDuckGo, misalnya, seluruh pengguna kehilangan akses karena sebagian kecil hasil pencarian dinilai memuat konten terlarang dan karena penyelenggara tidak memenuhi kewajiban pendaftaran sebagai penyelenggara sistem elektronik lingkup privat. Dalam kerangka analisis penelitian ini, konfigurasi tersebut merupakan persoalan proporsionalitas, yaitu sanksi dijatuhkan kepada pihak yang tidak melakukan pelanggaran, sebagai konsekuensi tidak langsung dari sengketa antara negara dan penyelenggara layanan. Kelompok terdampak lainnya ialah pengguna yang justru berupaya melindungi privasinya. Pemblokiran mesin pencari yang mengedepankan perlindungan privasi memiliki implikasi yang melampaui hilangnya satu layanan, sebab yang tersaring adalah warga yang secara sadar memilih alat dengan perlindungan data lebih baik. Konsekuensinya bersifat berlapis apabila dibaca bersama temuan

pada bagian sebelumnya mengenai kebocoran data instansi pemerintah dan lemahnya penegakan pelindungan data. Warga menghadapi kondisi ketika negara belum mampu menjamin keamanan data yang dikelolanya, sementara pada saat yang sama akses terhadap sarana perlindungan mandiri dipersempit. Dari sudut dimensi hak, peristiwa ini merupakan pelanggaran yang bekerja pada dua komponen sekaligus, yakni akses dan privasi.

Korban lainnya ialah entitas kelembagaan dan pelaku ekonomi. Pemblokiran yang menimpa situs organisasi seperti Kamar Dagang dan Industri serta layanan seperti Vimeo memperlihatkan bahwa korban tidak terbatas pada individu. Pada kasus-kasus ini, persoalan utama bukan terletak pada tindakan pemblokirannya semata, melainkan pada mekanisme pemulihannya, yaiut proses penyanggahan berlangsung berlarut-larut, sebagian situs tetap terblokir dalam jangka panjang, dan penjelasan yang tersedia hanya berupa halaman pengalihan yang menyatakan adanya pelanggaran UU ITE tanpa merinci ketentuan yang dilanggar maupun konten yang dipermasalahkan. Ketiadaan spesifikasi tersebut menghasilkan situasi yang secara praktis meniadakan hak membela diri, sebab pihak terdampak tidak dapat menyusun keberatan atas tuduhan yang tidak diuraikan.

2. Kebebasan Bereskpresi

Berbeda dengan pelanggaran hak akses yang korbannya menyebar dan tidak terdiferensiasi, pelanggaran terhadap kebebasan berekspresi memiliki struktur sasaran yang terindividualisasi dan selektif. Setiap kasus

kriminalisasi unggahan, pemanggilan, atau penindakan atas konten kritis menunjuk pada orang tertentu yang dipilih berdasarkan apa yang dinyatakannya. Sifat selektif inilah yang menjadikan dimensi cakupan sasaran pada kategori ini bernilai analitis tinggi, apabila pemblokiran menunjukkan konten apa yang dianggap tidak boleh beredar, maka penindakan ekspresi menunjukkan siapa yang dianggap tidak boleh bersuara. Distribusi korban dengan demikian menyimpan informasi mengenai batas toleransi kekuasaan terhadap kritik, dan pergeserannya menunjukkan ke arah mana batas tersebut bergerak.

Analisis pada bagian ini mengelompokkan korban menurut posisinya dalam ruang publik digital, dengan pembedaan antara aktor yang secara struktural berhadapan dengan kekuasaan dan warga yang tidak memiliki afiliasi organisasional. Kelompok pertama meliputi jurnalis dan institusi media, aktivis serta organisasi masyarakat sipil, pembela hak asasi manusia dan lembaga bantuan hukum, serta akademisi. Kelompok kedua meliputi warga umum, mahasiswa, pekerja seni dan budaya, serta kreator konten yang tidak berhimpun dalam kerja advokasi. Pembedaan ini penting karena keduanya memiliki kapasitas bertahan yang berbeda, yaitu kelompok pertama memiliki akses pada pendampingan hukum, jaringan solidaritas, dan perhatian publik, sedangkan kelompok kedua umumnya menghadapi proses hukum tanpa dukungan tersebut. Konsekuensinya, penindakan dengan tingkat keparahan yang sama menghasilkan dampak yang berbeda menurut kategori korbannya.

Tabel 4.6 Latar Belakang Korban Pelanggaran Kebebasan Berekspresi 2025-2026

Latar Belakang Korban	2025	2026 (1)	2026 (2)
Warga	187	14	20
Akun Media Sosial	41	0	2
Pesoroh	21	2	5
Aktivis	19	2	2
Tidak Diketahui	11	1	4
Pelajar/Mahasiswa	9	2	0
Pejabat Publik	8	0	3
Pengacara	8	3	0
Lainnya	7	7	4
Jurnalis/Pekerja Media	7	2	0
Pengusaha/Wiraswasta	7	4	1
Politikus	6	1	0
Buruh	5	1	1
Akademisi	4	0	2
Pegawai Swasta	4	0	1
TOTAL	**344**	**32**	**41**

Sumber: SAFEnet (2026)

Data yang tersedia memperlihatkan bahwa penangkapan merupakan respons yang dominan terhadap ekspresi kritis pada periode ini: sebanyak 157 orang atau 46 persen dari keseluruhan korban pelanggaran kebebasan berekspresi daring mengalami penangkapan oleh kepolisian. Proporsi tersebut memiliki dua implikasi analitis. Pertama, penanganan ekspresi daring pada periode penelitian tidak berhenti pada teguran, pemanggilan, atau permintaan penghapusan konten, melainkan langsung memasuki ranah pemidanaan dengan tindakan yang membatasi kebebasan fisik korban. Kedua, keterlibatan kepolisian dari berbagai wilayah menunjukkan bahwa penindakan tidak terpusat pada satu institusi di tingkat nasional, melainkan

tersebar dan dijalankan secara mandiri oleh satuan-satuan di daerah, sehingga cakupan geografis korban meluas melampaui pusat-pusat aktivisme yang selama ini menjadi konsentrasi penindakan.

Penetapan tersangka terhadap admin akun yang berkaitan dengan seruan aksi menunjukkan bahwa yang menjadi sasaran bukan semata isi pernyataan, melainkan fungsi pengorganisasian yang melekat pada pengelolaan akun tersebut. Pembedaan ini penting karena menempatkan penindakan pada ranah yang berbeda, yakni yang ditindak bukan pendapat yang dinyatakan, melainkan kapasitas menghimpun orang. Kelompok lain yang menjadi sorotan adalah warga dan mahasiswa tanpa afiliasi advokasi. Penetapan tersangka terhadap seorang warga dan dua mahasiswa di Bandung berdasarkan Pasal 28 ayat (2) UU ITE menunjukkan pergeseran yang lebih signifikan daripada kenaikan angka. Ekspresi yang dipermasalahkan disampaikan melalui *Instagram story* dan berisi kekecewaan serta kemarahan atas tindakan represif aparat terhadap massa aksi. kategori korban meluas kepada warga yang tidak memiliki jaringan pendampingan hukum maupun perhatian publik, sehingga menanggung proses hukum dengan kapasitas bertahan yang jauh lebih rendah dibanding kelompok lainnya seperti aktivis atau jurnalis. Kelompok selanjutnya ialah korban yang dijaring melalui penelusuran proaktif. Penangkapan yang berlangsung selama dan setelah gelombang demonstrasi Agustus-September dilakukan melalui patroli siber, yakni pemantauan intensif terhadap media sosial dan platform digital untuk menelusuri unggahan,

komentar, dan konten yang dinilai berkaitan dengan seruan aksi, kritik terhadap aparat, atau penyebaran informasi mengenai demonstrasi. Mekanisme ini mengubah struktur risiko secara fundamental. Pada penindakan berbasis aduan, korban ditentukan oleh adanya pihak yang merasa dirugikan dan melapor, sehingga risiko terkonsentrasi pada ekspresi yang menyinggung pihak tertentu. Pada penindakan berbasis penelusuran proaktif, korban ditentukan oleh apa yang ditemukan aparat dalam pemantauannya, sehingga risiko terdistribusi kepada seluruh pengguna yang unggahannya memenuhi kriteria pencarian.

Pada 2026, terdapat kelompok korban yang berperan sebagai penyebar ulang konten sebagai kategori korban baru. Dua kasus yang terdokumentasi, J, yang mengunggah ulang konten kritik terhadap satuan Brimob melalui akun TikTok dan dijatuhi pidana lima bulan enam hari, serta Wawan Hermawan yang mengunggah ulang konten dengan penambahan teks dan diproses hingga tahap pengadilan. Kedua kasus tersebut memperlihatkan pergeseran yang secara analitis paling mendasar dalam bab ini. Pada kedua kasus tersebut, korban bukanlah pembuat konten melainkan penyebarnya. Pergeseran dari pembuat ke penyebar konten memiliki beberapa konsekuensi. Pertama, ambang pertanggungjawaban pidana menurun sampai pada tindakan digital yang paling lazim dilakukan warga, yakni membagikan ulang konten orang lain, padahal itu merupakan suatu tindakan yang secara sosial tidak dipersepsikan sebagai pernyataan pendapat, sehingga risikonya tidak diantisipasi. Kedua, dan paling penting

bagi kerangka *chilling effect*, penindakan terhadap penyebar ulang menyampaikan pesan yang jauh lebih luas jangkauannya daripada penindakan terhadap pembuat konten. Ini dapat diartikan apabila menyebar saja sudah mendapatkan risiko pidana, maka pembuat konten kemungkinan akan mendapat risiko yang lebih parah.

3. Serangan Digital

Dimensi cakupan sasaran memiliki bobot analitis yang paling besar pada kategori serangan digital, dan alasannya terletak pada keterbatasan yang melekat pada kategori ini. Pada pelanggaran kebebasan berekspresi, pelaku dapat diidentifikasi karena penindakan berlangsung melalui prosedur resmi yang menyebutkan institusi dan dasar hukumnya. Pada pelanggaran hak akses, pelaku juga dapat diidentifikasi karena kewenangan pemblokiran melekat pada otoritas tertentu. Pada serangan digital, sebaliknya, pelaku hampir selalu anonim dan proses hukum yang dapat mengungkapkan identitasnya nyaris tidak pernah berjalan hingga tuntas.

Tabel 4.7 Latar Belakang Serangan Digital 2025-2026

Latar Belakang Korban	2025	2026 (1)	2026 (2)
Pelajar/Mahasiswa	209	37	45
Warga Umum	170	34	61
Pegawai Swasta	143	31	47
Staf OMS/Aktivis	90	8	12
OMS	54	3	10
Pekerja Kreatif	53	12	7
Pegawai Pemerintah	28	0	7
Organisasi Mahasiswa	24	0	0
Lembaga Publik	24	3	49
Pengusaha/Wiraswasta	22	3	7

Latar Belakang Korban	2025	2026 (1)	2026 (2)
Akademisi	22	5	5
Jurnalis/Pekerja Media	19	3	9
Media	13	0	10
Perusahaan Swasta	12	3	5
Seniman	10	0	0
Pesohor	7	0	0
Pengacara	4	0	0
Ormas	3	0	0
Lainnya	0	6	0
TOTAL	**907**	**148**	**339**

Sumber: SAFEnet (2026)

Pada 2025, kelompok pelajar dan mahasiswa menempati proporsi terbesar sebesar 23,04 persen, disusul warga umum sebesar 18,74 persen, dan pegawai swasta sebesar 15,77 persen. Ketiga kelompok tersebut secara kumulatif mencakup lebih dari separuh keseluruhan korban, dan yang menjadikan temuan ini signifikan adalah karakteristik yang mereka miliki bersama. Ketiganya merupakan warga tanpa afiliasi advokasi, tanpa perlindungan profesi, dan tanpa akses langsung pada jaringan pendampingan hukum. Pergeseran komposisi ini merupakan indikasi perluasan dalam pengertian yang paling ketat sebagaimana dirumuskan dalam kerangka lintasan. Perluasan tidak ditunjukkan oleh bertambahnya jumlah korban pada kelompok yang sudah lama menjadi sasaran, melainkan oleh berpindahnya konsentrasi sasaran kepada kelompok yang sebelumnya berada di luar jangkauan. Dua penafsiran dapat diajukan atas pergeseran tersebut, dan keduanya menuju kesimpulan yang sejalan. Penafsiran pertama bersifat substantif, yaitu gelombang mobilisasi Agustus-September

menempatkan pelajar, mahasiswa, dan warga umum sebagai pelaku utama ekspresi politik daring, sehingga serangan mengikuti perpindahan pusat kritik dari aktor terorganisasi ke warga biasa. Penafsiran kedua bersifat komparatif, aktor terorganisasi telah mengembangkan literasi keamanan digital yang lebih baik selama bertahun-tahun menghadapi serangan, sehingga serangan bergeser ke sasaran yang perlindungannya lebih rendah. Kerentanan tersebut memiliki bentuk yang spesifik pada masing-masing kelompok, dan narasi kasus yang terdokumentasi memperlihatkan bahwa pelaku serangan justru memanfaatkan bentuk kerentanan tersebut secara terarah. Pada kasus seorang pegawai swasta yang aktif menyampaikan kritik kebijakan melalui media sosial, tangkapan layar unggahannya dikirimkan kepada perusahaan tempatnya bekerja hingga ia dipanggil oleh bagian sumber daya manusia. Mekanisme ini perlu dicermati karena memperkenalkan pola penindakan yang berbeda dari seluruh kategori yang telah dianalisis sebelumnya. Pertama, pelaku tidak memerlukan kewenangan negara, kemampuan teknis peretasan, maupun sumber daya khusus; yang dibutuhkan hanya tangkapan layar dan pengetahuan mengenai tempat kerja korban. Kedua, sanksi yang bekerja bukan sanksi hukum melainkan sanksi ekonomi, sehingga seluruh perangkat perlindungan yang melekat pada proses pidana seperti halnya asas praduga tak bersalah, hak atas pembelaan, dan hak mengajukan keberatan menjadi tidak berlaku sama sekali. Signifikansi kasus tersebut bertambah karena akibatnya dinyatakan

secara langsung oleh korban, yakni memilih mundur dari menyuarakan kritik karena kekhawatiran atas posisi pekerjaannya.

Pada tahun 2026, konsentrasi kembali kepada kelompok berisiko tinggi. Pergerakan bolak-balik ini memberikan koreksi penting terhadap penafsiran atas temuan sebelumnya: perluasan sasaran yang teridentifikasi pada 2025 tidak bersifat permanen dalam arti menggantikan kelompok sasaran lama. Satu catatan penafsiran perlu dikemukakan atas turunnya proporsi pelajar dan mahasiswa secara tajam. Penurunan tersebut memiliki dua kemungkinan penjelasan yang tidak dapat dibedakan hanya dengan data insiden. Kemungkinan pertama, serangan terhadap kelompok tersebut memang berkurang seiring meredanya mobilisasi. Kemungkinan kedua, penurunan angka mencerminkan berkurangnya aktivitas kritis kelompok tersebut di ruang digital, yang berarti angka yang menurun justru merupakan indikasi bekerjanya *chilling effect*, bukan indikasi membaiknya keamanan.

Kasus jurnalis di wilayah 3T. Peristiwa yang dialami seorang jurnalis NadiPapua pada 17 Februari 2026 memberikan gambaran mengenai bentuk tekanan yang menyertai rekonsentrasi tersebut. Yang bersangkutan menerima pesan WhatsApp dari Kepala Kepolisian Resor Nabire berkenaan dengan laporan investigasi mengenai pertambangan emas ilegal, yang berisi permintaan agar salah seorang wartawannya mempertanggungjawabkan pernyataannya dan memberikan keterangan resmi di kantor kepolisian;

sebelumnya, ia telah dihubungi nomor tidak dikenal yang mengatasnamakan kepolisian dengan pesan serupa.

4. Kekerasan Berbasis Gender Online

Analisis cakupan sasaran pada kategori kekerasan berbasis gender online menghadapi persoalan konseptual yang tidak muncul pada tiga kategori sebelumnya. Pada pelanggaran hak akses, kebebasan berekspresi, dan serangan digital, korban dikelompokkan menurut posisinya dalam ruang publik seperti jurnalis, aktivis, mahasiswa, pegawai swasta, warga umum, yakni kategori yang menunjukkan peran dan aktivitas seseorang. Pada KBGO, faktor yang menentukan seseorang menjadi sasaran bukanlah perannya melainkan atribut identitasnya, gender, orientasi seksual, dan usia. Konsekuensinya, kerangka pengelompokan yang digunakan pada bagian-bagian sebelumnya tidak dapat diterapkan secara langsung, dan analisis perlu dilakukan pada dua lapis sekaligus, yakni lapis identitas yang menjadikan seseorang rentan dan lapis peran yang menjadikannya menjadi sasaran.

Persinggungan antara kedua lapis tersebut merupakan inti persoalan pada kategori ini. Sejumlah korban berada semata pada lapis identitas. Mereka tidak menyampaikan kritik, tidak terlibat dalam aktivitas politik, dan menjadi sasaran hanya karena atribut identitasnya. Sejumlah korban lain berada pada kedua lapis sekaligus, yaitu mereka yang menyampaikan kritik atau menjalankan peran publik tertentu, dan serangan yang

diterimanya bekerja melalui kerentanan identitasnya. Pembedaan ini penting bagi penelitian, sebab keduanya menuntut penilaian yang berbeda. Pada kelompok pertama, kerugian yang terjadi merupakan pelanggaran hak digital yang bersumber dari relasi sosial dan kegagalan perlindungan negara. Pada kelompok kedua, KBGO berfungsi sebagai instrumen pembungkaman politik yang memanfaatkan gender dan seksualitas sebagai salurannya, sehingga peristiwanya termasuk dalam lingkup penyempitan kebebasan digital dalam pengertian yang paling langsung. Analisis pada bagian ini karenanya diarahkan untuk memilah keduanya, dengan memperhatikan keterkaitan antara serangan dan aktivitas publik korban sebelum serangan terjadi.

Tabel 4.8 Kasus KBGO 2025-2026

Gender Korban	2025	2026 (1)	2026 (2)
Perempuan	1531	476	559
Laki-Laki	778	236	246
Tidak Diketahui	50	16	14
Nonbiner	23	6	2
TOTAL	**2382**	**734**	**821**

Sumber: SAFEnet (2026)

Analisis atas sasaran korban KBGO pada periode 2024–2025 memperlihatkan pergeseran yang tidak terletak pada bertambahnya jumlah, melainkan pada berubahnya aktor pelaku dan instrumen yang digunakan. . Sepanjang 2024, kerentanan kelompok minoritas di ruang digital meningkat secara khusus pada situasi politik pemilihan umum dan periode sesudahnya, sebagaimana ditemukan dalam diskusi terpumpun yang melibatkan organisasi masyarakat sipil di berbagai daerah. Tiga kasus yang

terdokumentasi memperlihatkan mekanisme yang bekerja. Pertama, pengungkapan masa lalu seorang calon kepala daerah di Cilacap yang kemudian dijadikan bahan kampanye politik di media sosial dengan narasi yang berkaitan dengan identitas seksual. Kedua, temuan LAPPAN Maluku mengenai kampanye hitam melalui TikTok terhadap calon kepala daerah dan calon anggota legislatif di Maluku Utara, yang menyerang seorang calon legislatif perempuan dengan narasi buruk berdasarkan statusnya sebagai janda, dan berkembang hingga menimbulkan provokasi serta konflik bernuansa suku.

Pelaku merupakan aktor non-negara, yang diindikasikan merupakan pesaing politik, akun terkoordinasi, dan khalayak, sementara negara tidak berkedudukan sebagai pelaku maupun sebagai pelindung. Sasaran yang dipilih adalah perempuan dan kelompok minoritas seksual yang sedang menempati atau memasuki posisi publik. Lalu, yang diserang bukan pendapat yang mereka nyatakan, melainkan kelayakan mereka untuk menduduki posisi tersebut, dengan menggunakan kategori moral-sosial yang telah tersedia dalam masyarakat, seperti status perkawinan dan orientasi seksual.

Setelah peralihan pemerintahan, konfigurasi tersebut berubah pada dua unsurnya yang paling menentukan. Pelaku bergeser dari aktor non-negara kepada negara, dan instrumen bergeser dari kampanye pendiskreditan kepada penuntutan pidana melalui UU ITE. Kasus Rifa menunjukkan bagaimana ketentuan pidana diterapkan terhadap seorang

perempuan yang mengunggah rekaman peristiwa kerusuhan dan menyampaikan kritik terhadap kebijakan pemerintah pada masa aksi Agustus-September 2025. Yang bersangkutan dituntut berdasarkan Pasal 45A UU ITE dengan kualifikasi penyebaran berita bohong, dan jaksa menuntut pidana satu tahun penjara dengan penilaian bahwa unggahan tersebut bersifat ofensif. Kasus MFK menunjukkan bentuk yang berbeda. MFK dituntut berdasarkan Pasal 27 ayat (1) UU ITE berkenaan dengan kedudukannya sebagai administrator sebuah grup di Facebook yang menghimpun kelompok gay. Hal yang menjadi pusat perhatian ialah yang menjadi dasar penuntutan bukanlah suatu pernyataan yang disampaikan korban, melainkan fungsi yang dijalankannya, yakni menghimpun dan mengelola perkumpulan. Pola ini serupa dengan penindakan terhadap pengelola akun mobilisasi yang telah dianalisis pada bagian sebelumnya, dan menegaskan bahwa yang menjadi sasaran adalah kapasitas mengorganisasi, bukan isi ekspresi. Tahap pertama, pada 2024, identitas digunakan sebagai senjata dalam kompetisi elektoral oleh aktor non-negara, dengan negara berada pada posisi absen. Tahap kedua, pada 2025, kerentanan identitas menjadi landasan bagi penuntutan pidana oleh negara, sehingga negara berpindah dari posisi menjadi pelaku.

Tahun 2026 tidak lebih baik dibandingkan dengan tahun sebelumnya. Rencana pengesahan Rancangan Undang-Undang Penyiaran pada awal 2026 memuat ketentuan yang berpotensi membatasi konten tertentu, dengan ekspresi komunitas LGBT disebut secara khusus dalam

pernyataan anggota Komisi I DPR sebagai bagian dari batasan yang dinilai perlu ditegakkan secara tegas dan konsisten pada media konvensional maupun digital, dengan alasan perlindungan anak. Namun sebagaimana ditunjukkan penolakan dari berbagai pihak, draf yang sama juga memuat ketentuan yang membatasi jurnalisme investigatif dan berpotensi menggerus independensi media. Terdapat indikasi peran institusi sebagai penguat serangan. Sebagaimana telah dikemukakan pada bagian sebelumnya, pelaku pelanggaran privasi terhadap kelompok minoritas tidak perlu menjatuhkan sanksi sendiri; cukup mengungkapkan informasi, dan struktur sosial akan menjalankan penghukumannya.

4.6 Analisis Aktor Pelanggaran Hak Digital

Dimensi aktor memeriksa siapa yang melakukan atau diduga melakukan pelanggaran, dan dengan demikian mengoperasionalkan secara empiris teori segitiga tata kelola ekspresi digital yang menempatkan negara, platform, dan warga sebagai tiga simpul yang saling berelasi (Balkin, 2018). Nilai analitis dimensi ini terletak pada kemampuannya mengukur satu hal yang tidak terbaca pada dimensi lain, yakni sejauh mana pembatasan berlangsung dalam bentuk yang dapat digugat. Tindakan yang dilakukan aktor yang teridentifikasi melalui prosedur resmi dapat diuji melalui mekanisme hukum. Tindakan yang dilakukan aktor anonim atau disalurkan melalui perantara tidak menyediakan pihak yang dapat dimintai pertanggungjawaban. Sebagaimana dikemukakan Feldstein (2021), pergeseran ke arah bentuk kedua merupakan ciri khas represi

digital, justru karena kemampuan menyangkal yang dimilikinya. Analisis berikut memisahkan pembacaan menurut empat kategori pelanggaran, mengingat masing-masing memiliki konfigurasi aktor yang berbeda secara mendasar.

1. Akses Internet

   Kategori ini memiliki konfigurasi aktor yang paling sederhana sekaligus paling terpusat. Pelaku pembatasan adalah Kementerian Komunikasi dan Digital sebagai pemegang kewenangan pemutusan akses, yang bertindak melalui perangkat penyaringan konten. Tidak terdapat ambiguitas mengenai siapa yang melakukan pemblokiran, sebab kewenangan tersebut melekat secara eksklusif pada institusi tertentu berdasarkan peraturan perundang-undangan. Namun kejelasan identitas aktor ini tidak berbanding lurus dengan tersedianya pertanggungjawaban. Aktor kedua pada kategori ini adalah penyelenggara sistem elektronik, yang berkedudukan sebagai pihak yang tunduk pada rezim pendaftaran sekaligus sebagai pihak yang ketidakpatuhannya berakibat pada terputusnya akses pengguna. Pada kasus pemblokiran mesin pencari yang tidak terdaftar sebagai penyelenggara lingkup privat, relasi antara negara dan penyelenggara menghasilkan kerugian bagi pihak ketiga yang tidak terlibat dalam sengketa tersebut, yakni pengguna. Ini menjadi salah satu bentuk sensor kolateral sebagaimana dirumuskan Balkin (2018).

   Terakhir, perlu ditegaskan kembali bahwa gangguan akses yang bersumber dari kejadian luar biasa, seperti pemutusan serat optik di

Ponorogo dan perbaikan sistem komunikasi kabel laut yang berdampak pada sejumlah kabupaten di Papua dan Maluku, tidak memiliki aktor pelaku dalam pengertian dimensi ini dan karenanya tidak dimasukkan dalam penghitungan. Peristiwa tersebut tetap dianalisis, tetapi sebagai konteks infrastruktural, bukan sebagai tindakan.

2. Kebebasan Berekspresi

Berbeda dengan kategori sebelumnya yang aktornya tunggal dan terpusat, kategori ini melibatkan keseluruhan rantai sistem peradilan pidana, dengan masing-masing mata rantai memiliki peran yang berbeda. Kepolisian merupakan aktor yang paling dominan. Sebanyak 157 orang atau 46 persen korban mengalami penangkapan, dan penindakan dilakukan oleh satuan kepolisian di berbagai wilayah. Dua karakteristik perlu dicatat. Karakteristik pertama adalah desentralisasi, di mana penindakan tidak dijalankan oleh satu unit di tingkat pusat melainkan oleh banyak satuan yang bertindak secara mandiri, sehingga penerapan ketentuan yang sama dapat berbeda antarwilayah dan pengendalian atas keseragaman penafsiran menjadi lemah. Karakteristik kedua adalah pergeseran dari penindakan reaktif ke penindakan proaktif melalui patroli siber. Pada model reaktif, kepolisian bertindak setelah menerima laporan, sehingga cakupan penindakan dibatasi oleh keberadaan pelapor. Pada model proaktif, kepolisian menelusuri sendiri unggahan, komentar, dan konten yang dinilai berkaitan dengan seruan aksi, kritik terhadap aparat, atau penyebaran informasi mengenai demonstrasi. Perubahan ini mengubah kedudukan

kepolisian dari penegak hukum yang merespons pengaduan menjadi pemantau ruang publik digital secara terus-menerus.

Kejaksaan berperan sebagai penentu kualifikasi perbuatan, dan pada kasus Rifa penuntutan dilakukan berdasarkan ketentuan mengenai berita bohong dengan alasan bahwa unggahan bersifat ofensif. Ketidaksesuaian antara unsur ketentuan dan dasar penilaian menunjukkan bahwa penyaringan pada tahap penuntutan tidak berfungsi mengoreksi kelemahan pada tahap penyidikan, melainkan memperluasnya. Aktor ketiga adalah pembentuk undang-undang. Melalui pemeliharaan ketentuan yang rumusannya multitafsir, sebagaimana frasa "menimbulkan rasa kebencian atau permusuhan" pada Pasal 28 ayat (2) UU ITE yang tidak disertai parameter, serta melalui rencana pembentukan norma baru yang membatasi konten dan jurnalisme investigatif, pembentuk undang-undang berperan menyediakan landasan bagi keleluasaan penafsiran yang dimanfaatkan mata rantai lainnya.

Pengadilan berkedudukan sebagai mata rantai terakhir yang seharusnya menjadi penyaring paling ketat. Namun pada kasus J, seorang penyandang disabilitas intelektual yang mengunggah ulang konten kritik dan dijatuhi pidana lima bulan enam hari, pengadilan tidak mempertimbangkan kapasitas terdakwa dalam memahami konsekuensi perbuatannya.

3. Keamanan Digital

Kategori ini memiliki konfigurasi aktor yang paling kompleks, dan kompleksitas tersebut merupakan temuan tersendiri. Berbeda dengan dua

kategori sebelumnya, identitas pelaku pada sebagian besar kasus tidak dapat ditetapkan, sehingga analisis diarahkan pada pemetaan tingkat identifikasi pelaku. Pertama adalah pelaku yang sepenuhnya anonim, meliputi peretasan, pengambilalihan akun, dan doksing yang tidak dapat ditelusuri sumbernya. Kedua, adalah pelaku anonim yang mengatasnamakan otoritas, sebagaimana pada kasus jurnalis di Nabire yang lebih dahulu dihubungi nomor tidak dikenal yang mengaku sebagai kepolisian sebelum menerima pesan dari pejabat yang teridentifikasi. Ketiga, adalah pejabat yang teridentifikasi namun bertindak melalui saluran informal, sebagaimana pada penggunaan aplikasi pesan pribadi oleh Kepala Kepolisian Resor untuk meminta pertanggungjawaban atas produk jurnalistik, serta pada panggilan telepon aparat kepada orang tua korban yang memuat ancaman penangkapan dan pernyataan mengenai penyadapan. Keempat adalah dugaan keterlibatan institusi negara secara langsung.

Keberadaan aktor kedua dan ketiga menunjukkan adanya wilayah abu-abu yang menghubungkan serangan anonim dengan tindakan institusional, sehingga korban tidak dapat menentukan apakah tekanan yang dialaminya merupakan tindakan resmi, penyalahgunaan wewenang, atau intimidasi pihak lain yang meminjam kewibawaan institusi. Ketidakpastian ini bukan efek samping melainkan berfungsi sebagai bagian dari mekanisme penebar efek ketakutan, sebab ancaman yang tidak diketahui sumbernya sulit untuk dilawan melalui prosedur apa pun. Kelima, aktor pada kategori ini adalah jejaring akun terkoordinasi yang menjalankan operasi informasi.

Sebagaimana terdokumentasi pada kasus Andrie Yunus dan pada serangan terhadap KontraS, Celios, ICW, serta Kurawal Foundation, dan framing terhadap LGBT jejaring ini menyebarkan konten fabrikasi yang diproduksi dengan kecerdasan buatan disertai narasi yang menggambarkan organisasi masyarakat sipil sebagai penerima dana asing yang mengganggu stabilitas negara, dan menunjukkan penanda koordinasi berupa keseragaman tagar serta kesamaan narasi yang berlangsung serentak di TikTok, Threads, X, dan Instagram.

4. Kekerasan Berbasis Gender Online

Kategori ini memperlihatkan perpindahan aktor yang paling tegas di antara seluruh kategori, dan perpindahan tersebut berlangsung seiring peralihan pemerintahan. Pada 2024, aktor pelaku hampir seluruhnya berasal dari luar negara. Kompetitor politik memanfaatkan pengungkapan identitas dan status personal sebagai bahan kampanye, sebagaimana pada kasus calon kepala daerah di Cilacap dan kampanye hitam melalui TikTok terhadap calon kepala daerah serta calon anggota legislatif di Maluku Utara yang menyerang seorang calon perempuan berdasarkan statusnya sebagai janda. Khalayak anonim menjalankan pelecehan di ruang publik digital. Pada konfigurasi ini negara tidak berkedudukan sebagai pelaku, tetapi juga tidak berkedudukan sebagai pelindung, ketiadaan penanganan atas peristiwa-peristiwa tersebut menempatkan negara pada posisi pembiaran.

Pada 2025, aktor bergeser kepada negara melalui aparat penegak hukum. Penuntutan terhadap Rifa berdasarkan Pasal 45A UU ITE dan

terhadap MFK berdasarkan Pasal 27 ayat (1) UU ITE atas kedudukannya sebagai administrator perkumpulan daring kelompok gay memperlihatkan bahwa kerentanan yang sebelumnya dimanfaatkan aktor non-negara kini memperoleh saluran kelembagaan. Terhambatnya penasihat hukum dalam mendampingi MFK menambahkan satu lapis lagi, yakni bahwa aktor negara tidak hanya berperan pada tahap penindakan melainkan juga pada tahap yang seharusnya menjamin perlindungan prosedural.

4.7 Analisis Instrumen yang Digunakan untuk Pelanggaran Hak Digital

Dimensi instrumen memeriksa alat yang digunakan untuk melakukan pembatasan, dan memiliki dua fungsi analitis dalam penelitian ini. Fungsi pertama adalah untuk mengklasifikasi, yakni memetakan instrumen yang teridentifikasi ke dalam tiga generasi kontrol informasi (Deibert, 2015) sehingga tingkat kecanggihannya dapat dinilai. Fungsi kedua bersifat menentukan apakah komposisi instrumen bergeser ke bentuk yang lebih tersamar dan lebih sulit diatribusikan. Suatu pergeseran yang dalam kerangka lintasan penelitian ini merupakan indikator perubahan bentuk, dan yang secara khusus tidak terbaca melalui dimensi jumlah maupun jenis. Analisis berikut dipisahkan menurut empat kategori pelanggaran karena masing-masing memiliki perbendaharaan instrumen yang berbeda.

1. Akses Internet

   Instrumen pada kategori ini bekerja pada tingkat infrastruktur, bukan pada tingkat konten individual, dan karenanya menghasilkan dampak

massal dengan satu tindakan tunggal. Terdapat tiga jenis instrumen yang dapat teridentifikasi melalui data yang tersedia. Pertama, instrumen teknis penyaringan yang terdiri atas perangkat pengais konten negatif. Alat ini dioperasikan Komdigi merupakan instrumen utama pemblokiran, bekerja secara otomatis dengan mendeteksi konten yang dinilai terlarang dan memutus akses terhadapnya. Karakteristik penting instrumen ini adalah ketiadaan penilaian kasus per kasus, sebagaimana ditunjukkan terblokirnya domain Google akibat pendeteksian subdomain yang memuat konten perjudian. Otomasi menghasilkan tiga akibat sekaligus, yaitu skala penindakan meningkat tanpa penambahan sumber daya, kesalahan menjadi konsekuensi struktural yang dapat diperkirakan, dan tanggung jawab dapat dialihkan kepada sistem melalui kualifikasi kesalahan teknis. Dalam kerangka Deibert (2015), instrumen ini merupakan kontrol generasi pertama, yakni penyaringan dan pemblokiran yang bersifat langsung.

Kedua, instrumen administratif, yaitu melalui kewajiban pendaftaran PSE beserta ancaman sanksi pemutusan akses berfungsi sebagai instrumen tekanan terhadap platform, sebagaimana tampak pada pemblokiran mesin pencari yang tidak terdaftar sebagai penyelenggara lingkup privat. Pada tingkat yang lebih tinggi, penangguhan izin operasi merupakan instrumen dengan daya tekan terbesar, sebagaimana ditunjukkan pada kasus yang berakhir dengan penyerahan data pengguna terkait demonstrasi. Instrumen administratif berbeda secara mendasar dari instrumen pidana karena tidak mensyaratkan pembuktian di pengadilan,

tidak memberikan hak pembelaan yang setara, dan dapat dijatuhkan secara sepihak. Dalam kerangka Deibert, instrumen ini merupakan kontrol generasi kedua yang bekerja melalui selubung legalitas.

Ketiga ialah instrumen pembatasan fitur, yang dilakukan oleh platform, dan bisa jadi atas perintah dari pihak pemerintahan. Tindakan ini merupakan instrumen yang secara analitis berada di antara pemblokiran dan moderasi. Instrumen ini lebih halus daripada pemblokiran total karena layanan tetap dapat diakses, tetapi lebih efektif dalam konteks tertentu karena menyasar fungsi yang paling penting pada momen kritis, yakni kemampuan warga menyiarkan peristiwa secara langsung. Sifatnya yang dapat dinyatakan sebagai keputusan sukarela platform menjadikannya instrumen dengan tingkat penyangkalan tertinggi pada kategori ini.

2. Kebebasan Berekspresi

Instrumen pada kategori ini bersifat yuridis, dan temuan utamanya terletak bukan pada beratnya sanksi melainkan pada keleluasaan memilih dasar hukum. Instrument pidana yang digunakan misalnya menggunakan pasal 28 ayat (2) UU ITE dengan frasa "menimbulkan rasa kebencian atau permusuhan" yang tidak disertai parameter merupakan instrumen yang paling sering digunakan terhadap aktivis dan pengelola akun media sosial berkaitan dengan aksi demonstrasi. Rumusan yang multitafsir menjadikan penentuan terpenuhinya unsur bergantung pada penafsiran pelaksana, sehingga ketentuan yang sama dapat diterapkan pada tindakan yang sangat beragam. Kondisi inilah yang oleh Schauer (1978) diidentifikasi sebagai

sumber utama *chilling effect* yaitu warga tidak dapat memperkirakan batas legalitas, sehingga menjauh jauh-jauh dari batas tersebut. Instrumen hukum dengan perluasan norma baru juga ditemukan, misalnya dengan berlakunya KUHP baru pada Januari 2026 dengan ketentuan mengenai penghinaan presiden dan lembaga negara yang menjangkau media elektronik menambah perbendaharaan instrumen yang tersedia. Berbeda dengan ketentuan UU ITE yang mensyaratkan adanya pihak yang merasa dirugikan, ketentuan mengenai penghinaan lembaga menempatkan institusi negara sebagai objek yang dilindungi.

Terakhir, instrumen teknis penunjang. Patroli siber berfungsi sebagai instrumen deteksi yang mendahului penindakan, sedangkan permintaan data pengguna kepada platform berfungsi sebagai instrumen identifikasi. Keduanya tidak bersifat menghukum, tetapi menentukan siapa yang dapat dijangkau oleh instrumen pidana. Dalam kerangka Feldstein (2021), kombinasi antara pengawasan dan persekusi inilah yang menjadikan penindakan berskala besar dapat dijalankan.

3. Serangan Digital

Kategori ini memiliki perbendaharaan instrumen yang lebih beragam, dan yang membedakannya dari dua kategori sebelumnya adalah bahwa instrumen-instrumen tersebut tidak memerlukan kewenangan negara untuk digunakan. Pertama, instrumen teknis. Peretasan perangkat dan akun serta pengambilalihan akun merupakan bentuk yang tercatat dominan, dengan peretasan mencapai 18,30 persen dari keseluruhan bentuk serangan.

Instrumen ini menyerang kendali korban atas identitas digitalnya, dan dampaknya berlapis karena akun yang diambil alih dapat digunakan untuk merugikan korban lebih lanjut. Kedua, instrument non teknis yang terjadi pada kasus seperti *doxing*, karena bersumber pada informasi terbuka. Karakteristik instrumen ini adalah kesederhanaan teknisnya di mana pelaku tidak memerlukan kemampuan khusus, cukup memiliki akses pada data pribadi korban yang ketersediaannya biasanya bersumber dari kebocoran data pada sistem instansi pemerintah. Dengan demikian terdapat keterkaitan struktural antara kegagalan perlindungan data oleh negara dan ketersediaan bahan baku bagi instrumen serangan ini.

Instrumen non teknis juga didapati pada kasus yang berbasis serangan sosial dan psikologis korban. Pengancaman merupakan bentuk yang paling dominan dengan 23,04 persen, dan bekerja tanpa memerlukan tindakan teknis sama sekali. Instrumen ini mencakup ancaman penangkapan yang disampaikan melalui telepon kepada keluarga korban, pernyataan bahwa komunikasi korban telah disadap, hingga ancaman untuk mendatangi kediaman korban. Penney (2016) menjelaskan bahwa pengetahuan mengenai adanya pengawasan sudah cukup untuk memberi efek takut pada korban. Instrumen ini karenanya merupakan yang paling efisien dalam kategori ini, biayanya murah dan mudah dilakukan, tidak meninggalkan jejak teknis, dan dampaknya setara dengan tindakan yang sesungguhnya dilakukan.

Terakhir ialah instrumen non formal. Penggunaan aplikasi pesan pribadi oleh pejabat untuk menyampaikan permintaan pertanggungjawaban, sebagaimana pada kasus jurnalis di Nabire, merupakan instrumen yang memanfaatkan kewibawaan institusi tanpa menggunakan prosedurnya. Instrumen ini menghasilkan tekanan setara dengan panggilan resmi, tetapi tidak menghasilkan dokumen yang dapat diuji, tidak tunduk pada tenggat prosedural, dan tidak dapat dipersoalkan melalui mekanisme keberatan.

4. Kekerasan Berbasis Gender Online

Instrumen pada kategori ini memiliki kekhasan yang membedakannya dari seluruh kategori lain yang mana sebagian besar bekerja dengan memanfaatkan norma sosial yang telah tersedia dalam masyarakat, sehingga daya rusaknya tidak bersumber dari instrumen itu sendiri melainkan dari respons lingkungan sosial terhadapnya. Pertama, instrumen legal formal. Pada 2025, instrumen bergeser kepada ketentuan pidana, dengan Pasal 45A dan Pasal 27 ayat (1) UU ITE digunakan terhadap korban yang berasal dari kelompok rentan. Pada kasus MFK, yang dijadikan dasar bukan pernyataan melainkan kedudukan sebagai administrator perkumpulan daring, sehingga instrumen pidana digunakan untuk membatasi pelaksanaan hak berkumpul dan berserikat. Terhambatnya penasihat hukum dalam mendampingi yang bersangkutan merupakan instrumen tambahan yang bekerja pada tahap prosedural, dan dalam kerangka Roberts (2018) merupakan bentuk *friction* atau hambatan yang

tidak melarang tetapi mempersulit hingga pelaksanaan hak menjadi tidak efektif.

Contoh lainnya dari penggunaan instrument legal formal ialah tindakan perguruan tinggi mengeluarkan mahasiswa yang menjadi korban perekaman diam-diam tanpa didahului prosedur penanganan kasus merupakan instrumen yang dijalankan aktor non-negara namun berdampak paling merusak bagi korban.

Kedua, normatif. Kampanye hitam yang menyerang calon anggota legislatif perempuan berdasarkan statusnya sebagai janda di Maluku Utara memperlihatkan instrumen yang bekerja dengan mengaktifkan kategori moral-sosial untuk mendiskualifikasi seseorang dari kelayakan menduduki posisi publik. Instrumen ini tidak membantah kapasitas atau gagasan korban, melainkan memindahkan penilaian dari ranah kompetensi ke ranah kepantasan. Pada 2026, instrumen bergeser lagi ke tingkat pembentukan norma, melalui penetapan kelompok minoritas dalam kerangka ancaman pada instrumen kebijakan pertahanan serta melalui pembahasan rancangan undang-undang yang memuat pembatasan konten. Berbeda dengan instrumen sebelumnya yang bekerja per kasus, instrumen normatif menghasilkan pembatasan yang berlaku umum dan tidak memerlukan peristiwa pemicu.

Tabel 4.9 Operasionalisasi Otoritarianisme Digital di Indonesia 2024-2026

Generasi kontrol (Deibert, 2015)	Teknik (Feldstein, 2021)	Manifestasi di Indonesia 2024–2026
Generasi I: pemblokiran & penyaringan	Penyensoran; gangguan akses	Pemblokiran situs dan layanan (misal: archive.org, Mei 2025); pembatasan konten demonstrasi
Generasi II: kontrol legal-regulatif	Persekusi pengguna; tekanan pada platform	Kriminalisasi via UU ITE: 146 kasus (2024) menjadi 351 kasus (2025); patroli siber; kewajiban PSE; penangguhan izin platform
Generasi III: kontrol ofensif & tersamar	Pengawasan; manipulasi informasi	Permintaan data pengguna kepada platform pasca-demonstrasi 2025; operasi pendengung yang dibiayai negara

4.8 Analisis Dampak Keparahan Pelanggaran Hak Digital

Dimensi keparahan merupakan dimensi terakhir dan sekaligus yang paling menentukan dalam kerangka penelitian ini, karena pada dimensi inilah pelanggaran diterjemahkan menjadi kerugian yang benar-benar dialami warga. Sebagaimana ditetapkan pada bab metode, keparahan tidak diukur semata dari berat sanksi formal, melainkan melalui tiga ukuran yang saling melengkapi. Ukuran pertama adalah bobot langsung yang ditanggung korban, tersusun bergradasi dari penghapusan konten, penangguhan akun, pemanggilan dan intimidasi, proses pidana, penahanan dan pemidanaan, hingga ancaman terhadap keselamatan fisik. Ukuran kedua adalah keterpulihan, yakni sejauh mana kerugian dapat dikembalikan pada keadaan semula. Ukuran ketiga adalah

jangkauan penggentaran, yakni seberapa luas dampak suatu peristiwa menjangkau warga lain yang tidak menjadi korban langsung. Ukuran ketiga inilah yang menghubungkan dimensi keparahan dengan konsep chilling effect, dan yang menjadikan penilaian keparahan tidak dapat dilakukan dengan menjumlahkan kerugian individual semata (Schauer, 1978).

1. Akses Internet

    Bentuk dan bobot kerugian serta keparahan pada kategori ini tidak berbentuk sanksi terhadap individu, melainkan terhalangnya pemenuhan hak pada tingkat populasi. Data memperlihatkan paradoks yang mendasar yaitu angka penetrasi internet nasional sebesar 80,66 persen menutupi kenyataan bahwa sekitar 50 juta jiwa penduduk masih terisolasi secara digital. Ketimpangan berlanjut pada mutu layanan, sebagaimana ditunjukkan pengukuran kecepatan di Jawa yang jauh lebih unggul dibandingkan Sulawesi dan kawasan Ibu Kota Nusantara. Perbedaan mutu ini menghasilkan apa yang dapat disebut diskriminasi geografis, yaitu ketika warga di wilayah tertentu memperoleh hak yang secara hukum sama tetapi secara nyata tidak setara, dan ketidaksetaraan tersebut bersifat melanggengkan karena keterbatasan akses mempersempit peluang ekonomi dan pendidikan yang justru diperlukan untuk keluar dari keterbatasan itu.

    Kerugian pada kategori ini bersifat tidak dapat dipulihkan dalam pengertian tertentu. Sulitnya mengakses informasi mengenai pemilihan umum dan berlarutnya proses rekapitulasi akibat kondisi infrastruktur yang belum merata merupakan kerugian yang melekat pada momen politik

tertentu, yakni ketika momen tersebut berlalu, kerugiannya tidak dapat dikembalikan. Warga yang tidak memperoleh informasi kepemiluan pada waktunya tidak dapat memilih ulang dengan informasi yang lebih baik. Dalam kerangka Balkin (2004), kerugian semacam ini menyentuh langsung *democratic culture*, sebab yang hilang bukan satu layanan melainkan kesempatan berpartisipasi dalam pembentukan keputusan kolektif.

Pada ranah kebijakan, instrumen sensor melalui aturan penyelenggara sistem elektronik digunakan secara eksesif untuk memblokir akses dan menekan platform global, termasuk melalui pengenaan denda administratif bagi yang tidak patuh. Pada ranah layanan, digitalisasi yang bersifat intrusif justru menciptakan sekat birokrasi baru yang meminggirkan kelompok rentan, penyandang disabilitas, dan warga miskin. Ini menjadi suatu temuan yang penting karena menunjukkan bahwa digitalisasi layanan publik dapat memperbesar eksklusi apabila dirancang tanpa memperhitungkan keragaman kemampuan penggunanya. Hal yang paling menunjukkan orientasi kebijakan adalah dipersulitnya inisiatif mandiri warga berupa internet komunitas bahkan ketika warga berupaya mengatasi sendiri kesenjangan yang tidak diatasi negara, upaya tersebut justru menghadapi hambatan. Dalam kerangka Sen (1999), tindakan ini menghilangkan kapabilitas warga untuk mengubah sumber daya menjadi kebebasan nyata, dan mengindikasikan bahwa prioritas kebijakan terletak pada kontrol sentralistik alih-alih pemenuhan hak secara inklusif.

2. Kebebasan Berekspresi

Pada kategori ini, keparahan mencapai titik tertinggi dalam gradasi yang ditetapkan penelitian, yakni perampasan kemerdekaan dan kedaulatan individu. Sebanyak 157 orang atau 46 persen korban mengalami penangkapan, dan sejumlah kasus berlanjut hingga penjatuhan pidana, sebagaimana pada perkara J yang divonis lima bulan enam hari dan tuntutan satu tahun terhadap Rifa. Dalam gradasi keparahan, penahanan dan pemidanaan menempati posisi tertinggi bukan hanya karena beratnya sanksi, melainkan karena sifatnya yang tidak dapat dipulihkan seperti halnya waktu yang dihabiskan dalam tahanan, kehilangan pekerjaan atau pendidikan, dan stigma yang melekat setelahnya tidak dapat dikembalikan meskipun putusan kemudian dibatalkan.

Temuan yang paling penting pada kategori ini adalah bahwa kerugian tidak menunggu adanya putusan pengadilan. Sebagaimana ditunjukkan pola penggunaan UU ITE sebagai bagian dari instrumen hukum yang paling sering digunakan. Motif dasar pelaporan bukanlah memperoleh putusan melainkan mengintimidasi, membungkam, serta menguras sumber daya finansial dan psikologis korban. Ketidakseimbangan posisi tawar antara pelapor dan pihak terlapor menyebabkan proses hukum berlangsung berlarut-larut. Konsekuensinya, somasi dan surat pemeriksaan sudah cukup menyebabkan korban takut menyampaikan ekspresinya kembali, tanpa perlu perkara mencapai tahap pengadilan. Temuan ini merupakan konfirmasi empiris yang kuat atas proposisi Schauer (1978) bahwa kerugian *chilling effect* bersumber dari beban proses, bukan dari sanksi akhir, dan

dalam kerangka Roberts (2018), pola ini merupakan bentuk *friction* yang paling murni, yakni hambatan yang tidak melarang tetapi mempersulit hingga pelaksanaan hak menjadi tidak berkelanjutan.

Selain penindakan terhadap individu, pembungkaman berlangsung melalui kontrol teknis pada platform. TikTok tercatat sebagai media yang paling banyak menjadi dasar pelaporan dengan 39 kasus, dan pada masa aksi demonstrasi aparat bahkan melarang penggunaan fitur siaran langsung. Pemblokiran terhadap 592 akun media sosial yang dituduh provokatif oleh polisi siber dan Komdigi memperlihatkan tingkat keparahan yang berbeda jenisnya, apabila penangkapan menghilangkan kemerdekaan dan kedaulatan individu satu orang, pemblokiran ratusan akun menghilangkan kanal komunikasi sejumlah besar warga sekaligus, sebagian besar tanpa proses pengujian dan tanpa mekanisme keberatan yang efektif. Sebaran wilayah kriminalisasi yang meluas, misalnya Jawa Barat mencatat 130 kasus dan DKI Jakarta 103 kasus menunjukkan bahwa keparahan tidak terkonsentrasi pada satu titik melainkan tersebar mengikuti pusat-pusat aktivitas politik digital.

Kombinasi antara penangkapan berskala besar, beban proses yang melelahkan, dan pemblokiran akun secara massal menghasilkan penggentaran yang jangkauannya jauh melampaui jumlah korban. Sebagaimana dikemukakan Schauer (1978), yang hilang bukan hanya ekspresi yang dihukum, melainkan ekspresi yang tidak pernah diucapkan atau dilakukan. Pada konteks ini, kerugian tersebut menyentuh secara

khusus tiga fungsi demokratis yang menjadi kriteria penelusuran aparat, yakni menyerukan aksi, mengkritik aparat, dan menyebarkan informasi mengenai demonstrasi. Bagi warga tanpa afiliasi advokasi, yang sebagaimana ditunjukkan pada dimensi cakupan sasaran kini menempati porsi terbesar korban, keparahannya lebih berat lagi karena mereka menanggung beban proses tanpa pendampingan hukum, tanpa jaringan solidaritas, dan tanpa perhatian publik yang dapat berfungsi sebagai perlindungan.

3. Serangan Digital

Keparahan pada kategori ini mencapai bentuknya yang paling ekstrem melalui perlintasan batas antara gangguan digital dan kekerasan fisik. Pada kasus serangan digital biasanya korban akan memikirkan dua kemungkinan. Kemungkinan pertama adalah eskalasi bertahap, yang menghasilkan kondisi ketidakpastian berkelanjutan, korban tidak mengetahui apakah rangkaian telah berakhir atau akan berlanjut pada bentuk yang lebih berat. Kemungkinan kedua adalah penargetan kediaman, yang meniadakan pemisahan antara ruang publik tempat korban berekspresi dan ruang privat tempat korban seharusnya aman.

Berbeda dengan kriminalisasi yang keparahannya dapat dinyatakan dalam lama pidana, keparahan pada kategori ini bersifat kumulatif dan sebagian besar tidak terukur. Kerugian yang ditanggung mencakup gangguan psikologis berkelanjutan, kehilangan rasa aman di kediaman sendiri, terganggunya kehidupan keluarga, dan pada sejumlah kasus

kehilangan pekerjaan. Tidak satu pun dari kerugian tersebut memiliki mekanisme pemulihan, sebab tidak terdapat pelaku yang teridentifikasi untuk dimintai pertanggungjawaban dan hampir tidak ada kasus yang diusut hingga tuntas.

Fenomena yang dikenali sebagai pola lama dengan wajah baru menegaskan bahwa kritik diposisikan sebagai gangguan terhadap stabilitas yang harus ditumpas dengan segala cara. Dampaknya terhadap perilaku warga bersifat langsung dan dapat diamati, seperti halnya warga memilih diam demi keselamatan fisik dirinya dan keluarganya. Pergeseran dasar pertimbangan inilah yang menjadikan keparahan pada kategori ini melampaui kategori lain. Pada kriminalisasi, warga menimbang risiko hukum yang setidaknya memiliki prosedur, batas, dan kemungkinan pembelaan. Pada serangan digital yang berlanjut menjadi teror fisik, warga menimbang risiko keselamatan yang tidak memiliki prosedur, tidak memiliki batas yang diketahui, dan tidak menyediakan pembelaan apa pun. Sebagaimana ditunjukkan Penney (2016), pengetahuan mengenai adanya pengawasan saja sudah cukup mengubah perilaku lalu pengetahuan mengenai adanya kemungkinan kekerasan fisik menghasilkan perubahan perilaku yang jauh lebih besar. Dalam kerangka Glasius dan Michaelsen (2018), rangkaian semacam ini memenuhi kriteria praktik otoriter sekaligus praktik iliberal, sebab menyabotase akuntabilitas dengan membungkam kritik sekaligus melanggar otonomi dan martabat individu melalui teror yang menembus ruang privat.

4. Kekerasan Berbasis Gender Online

Keparahan pada kategori ini memiliki karakteristik yang tidak dimiliki kategori lain, yakni kerugian yang bersifat menetap dan menjangkau seluruh aspek kehidupan korban. Materi yang telah tersebar tidak dapat ditarik kembali secara tuntas, sehingga korban menanggung kemungkinan viktimisasi berulang tanpa batas waktu. Sanksi sosial yang menyertainya bersifat mencabut kedudukan sosial korban, bukan sekadar membatasi tindakannya. Berbeda dengan pidana yang memiliki masa berakhir, kerugian jenis ini hampir tidak pernah selesai.

Temuan yang paling menentukan pada kategori ini adalah bahwa sebagian keparahan justru bersumber dari respons negara, bukan dari tindakan pelaku. Korban kekerasan digital pada kasus KBGO harus menanggung akibat dari lemahnya sistem hukum yang tidak memberikan perlindungan, bahkan menghadapi sistem yang tidak berpihak dan mengandung risiko dikriminalisasi, sementara pelaku kerap bebas tanpa hukuman yang setimpal. Kondisi ini terjadi karena aparat penegak hukum tidak memiliki perspektif mengenai hak digital dan prinsip keberpihakan pada korban. Implementasi Undang-Undang Tindak Pidana Kekerasan Seksual berjalan lamban karena kepolisian memprioritaskan penanganan perjudian daring, sedangkan regulasi baru seperti PP Tunas dan pembaruan

hukum acara pidana menuai kritik karena berpotensi melanggar privasi dan memperluas kewenangan penyadapan.

Dampak ketakutan pada kategori ini bekerja pada tingkat yang lebih mendasar daripada kategori lain. Pada kategori sebelumnya, yang ketakutannya apabila melakukan tindakan menyampaikan pendapat namun pada kategori ini, ketakutan mencakup pula tindakan melaporkan kekerasan yang dialami. Konsekuensinya bagi kualitas demokrasi bersifat struktural yaitu apabila perempuan dan kelompok minoritas bersuara terkait dengan suatu isu, maka mereka juga harus menanggung Risiko yang sama atau bahkan lebih parah karena kerentanannya. Sebagaimana dikemukakan Chaka (2022), proses semacam ini menghasilkan marginalisasi yang berlapis, ketika kelompok yang telah rentan secara sosial mengalami eksklusi tambahan melalui mekanisme digital.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kerangka penelitian merumuskan lima kemungkinan lintasan, dengan kemungkinan bahwa lebih dari satu lintasan berlangsung serentak pada dimensi yang berbeda. Penilaian atas keenam dimensi menghasilkan kesimpulan berikut. Pertama, instrumen, aktor, sasaran, dan bentuk pelanggaran berjalan sebagaimana periode sebelumnya dengan intensitas yang relatif tetap. Data menunjukkan sebaliknya pada sekurang-kurangnya tiga bentuk, yaitu komposisi sasaran berubah secara signifikan, perbendaharaan instrumen bertambah dengan bentuk yang sebelumnya tidak ada, dan konfigurasi aktor bergeser. Pernyataan masyarakat sipil mengenai berlanjutnya pola represi dari pemerintahan sebelumnya.

Kedua, Penurunan pembatasan tidak terkonfirmasi, meskipun sudah ada Putusan Mahkamah Konstitusi Nomor 105/PUU-XXII/2024 mempersempit ruang kriminalisasi dengan menegaskan bahwa pengaduan pencemaran nama baik hanya dapat diajukan orang perseorangan, Undang-Undang Pelindungan Data Pribadi telah berlaku penuh, dan sejumlah regulasi bercorak protektif dibentuk. Namun terdapat tiga alasan menyebabkan keadaan tersebut tidak mengubah arah keseluruhan. Pertama, perbaikan bersifat normatif sementara kerusakan berlangsung pada tingkat penegakan, sehingga keduanya tidak bekerja secara beriringan. Kedua, perbaikan pada satu aspek diimbangi

kerusakan pada aspek lain, sebagaimana berlakunya pasal penghinaan presiden dan lembaga negara dalam KUHP baru yang justru berlawanan arah dengan putusan tersebut. Ketiga, dan paling menentukan, instrumen protektif tidak disertai kelembagaan pelaksananya sehingga perlindungan yang dijanjikan tidak memiliki kepastian.

Kenaikan terkonfirmasi pada dimensi jumlah, instrumen, dan keparahan. Kenaikan jumlah kasus lebih dari dua kali lipat antara 2024 dan 2025, bertambahnya perbendaharaan instrumen tanpa berkurangnya instrumen lama, serta meningkatnya bobot kerugian hingga mencapai perampasan kemerdekaan dan ancaman keselamatan fisik menunjukkan bahwa tekanan terhadap kebebasan digital meningkat secara nyata. Sesuai dengan teori, kenaikan jumlah tidak dibaca berdiri sendiri. Kesimpulan kenaikan intensitas ditarik karena kenaikan tersebut disertai penguatan pada dua dimensi lain.

Data cakupan sasaran menunjukkan bahwa pembatasan menjangkau kategori korban yang sebelumnya berada di luar jangkauan seperti halnya warga yang sekadar menyebarkan ulang konten, penyandang disabilitas yang kapasitasnya tidak dipertimbangkan, mahasiswa yang menyampaikan kemarahan melalui medium terbatas, pekerja seni, pegawai swasta, hingga keluarga korban yang tidak menyampaikan kritik apa pun. Pada dimensi jenis, aktor, dan instrumen, data secara konsisten menunjukkan pergeseran ke bentuk-bentuk yang lebih tersamar dan lebih sulit diatribusikan: dari pemadaman akses yang kasat mata ke pembatasan fitur yang dinyatakan sukarela; dari penindakan langsung ke tekanan melalui platform, pemberi kerja, dan institusi pendidikan;

dari penghapusan konten ke pembanjiran wacana melalui operasi informasi berbasis kecerdasan buatan; dan dari kesalahan kebijakan ke kesalahan yang dikualifikasikan sebagai persoalan teknis. Pergeseran ini merupakan inti dari jawaban atas rumusan masalah, sebab ia menunjukkan bahwa pembatasan tidak hanya bertambah banyak, melainkan bertambah sulit dikenali, dilawan, dan dipertanggungjawabkan.

Kecenderungan kebebasan digital pada masa pemerintahan Prabowo Subianto-Gibran Rakabuming Raka ialah ruang digital Indonesia pada periode ini menyempit, dan penyempitannya berlangsung dalam bentuk yang semakin sukar diperiksa. Penyempitannya berlangsung melalui kombinasi intensifikasi, perluasan, dan perubahan bentuk secara serentak. Warisan infrastruktur pengendalian yang diterima pemerintahan baru pada Oktober 2024 tidak sekadar dilanjutkan, melainkan diperluas cakupannya, ditambah perbendaharaan instrumennya, dan diubah cara kerjanya menjadi lebih tersamar. Penyempitan tersebut bersifat regresif dalam distribusinya. Beban terberat tidak ditanggung oleh aktor yang paling berhadapan dengan kekuasaan, melainkan oleh warga atau pengguna.

5.2 Saran

5.2.1 Saran Praktis

1. Bagi pembentuk undang-undang, perbaikan peraturan yang sudah ada sangat diperlukan. Pengharmonisan antara putusan Mahkamah Konstitusi yang mempersempit kriminalisasi dan norma baru yang

memperluasnya juga diperlukan agar kerangka hukum tidak mengandung arah yang saling berlawanan.

2. Bagi aparat penegak hukum, temuan mengenai kegagalan penyaringan pada setiap mata rantai sistem peradilan pidana menunjukkan bahwa reformasi penegakan hukum dibutuhkan untuk menciptakan ruang digital yang aman, bebas dan setara.

5.2.2 Saran Akademis

1. Penelitian lanjutan disarankan menerapkan kerangka enam dimensi yang sama pada periode berikutnya agar perbandingan antarperiode dapat dilakukan dengan satuan yang setara.
2. Penelitian lapangan dengan pendekatan etnografi digital di Indonesia bagian timur dan wilayah rural disarankan untuk menguji sejauh mana angka yang tercatat merupakan batas bawah dari kejadian sesungguhnya, sekaligus untuk menangkap bentuk-bentuk pelanggaran yang mungkin tidak dikenali sebagai pelanggaran oleh korbannya sendiri.
3. Kolaborasi antara akademisi dan organisasi pemantau untuk menyusun taksonomi pelanggaran hak digital yang stabil dan terdokumentasi metodologinya disarankan sebagai upaya jangka panjang, karena ketersediaan data yang dapat diperbandingkan merupakan prasyarat bagi kajian mengenai kecenderungan yang lebih presisi.

DAFTAR PUSTAKA

Abdurrahman, A. (2025). Extending the IBCDE framework to explore barriers and drivers in Indonesia's digital economy. *Journal of Digital Economy*, *4*, 123–143. https://doi.org/10.1016/j.jdec.2025.08.003

AJI. (2025). *Teror kepala babi ke jurnalis Tempo serangan berbahaya terhadap kemerdekaan pers*. Https://Aji.or.Id/Informasi/Teror-Kepala-Babi-Ke-Jurnalis-Tempo-Serangan-Berbahaya-Terhadap-Kemerdekaan-Pers. https://aji.or.id/informasi/teror-kepala-babi-ke-jurnalis-tempo-serangan-berbahaya-terhadap-kemerdekaan-pers

Amnesty International. (2024). *A web of surveillance: Unravelling a murky network of spyware exports to Indonesia*. https://www.amnesty.org/en/latest/news/2024/05/indonesia-a-murky-web-of-spyware-exports/

APJII. (2024). *APJII: Jumlah pengguna internet Indonesia tembus 221 juta orang*. Https://Apjii.or.Id/Berita/d/Apjii-Jumlah-Pengguna-Internet-Indonesia-Tembus-221-Juta-Orang. https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Astara, W. W. (2021). The urgency of restricting the making accessibility phrase in Article 27 of the Electronic Information and Transactions Law from the human rights perspective in Indonesia. *Review of International Geographical Education Online*.

Balkin, J. M. (2003). *Digital Speech and Democratic Culture: a Theory of Freedom of Expression for the Information Society*. https://doi.org/10.2139/ssrn.470842

Balkin, J. M. (2018). Free speech is a triangle. *Columbia Law Review*, *118*(7).

BSSN. (2024). *BSSN identifikasi Pusat Data Nasional Sementara diserang ransomware*. Https://Www.Bssn.Go.Id/Bssn-Identifikasi-Pusat-Data-Nasional-Sementara-Diserang-Ransomware/. https://www.bssn.go.id/bssn-identifikasi-pusat-data-nasional-sementara-diserang-ransomware/

Chaka, C. (2022). Digital marginalization, data marginalization, and algorithmic exclusions: A critical southern decolonial approach to datafication, algorithms, and digital citizenship from the Souths. *Journal of E-Learning and Knowledge Society*, *18*(3).

CNBC Indonesia. (2026, February 4). *Telat 2 tahun, Komdigi janji badan penjaga data warga RI berdiri 2026*. Https://Www.Cnbcindonesia.Com/Tech/20260204144446-37-708158/Telat-2-Tahun-Komdigi-Janji-Badan-Penjaga-Data-Warga-Ri-Berdiri-2026.

https://www.cnbcindonesia.com/tech/20260204144446-37-708158/telat-2-tahun-komdigi-janji-badan-penjaga-data-warga-ri-berdiri-2026

Das, A. (2026). Introduction: digital activism in the Global South. *Journal of Multicultural Discourses*, 1–16. https://doi.org/10.1080/17447143.2026.2681003

Diamond, L. (2010). Liberation Technology. *Journal of Democracy*, *21*(3), 69–83. https://doi.org/10.1353/jod.0.0190

Eshtaev, A., Karimov, M., Bekimbetova, G., Abdulov, D., Ikromov, A., & Sobirov, Y. (2026). Analyzing the digitalization level of countries using the DIGILOG economy framework. *Digital Policy, Regulation and Governance*, 1–18. https://doi.org/10.1108/DPRG-12-2025-0449

Feldstein, S. (2021). *The Rise of Digital Repression*. Oxford University PressNew York. https://doi.org/10.1093/oso/9780190057497.001.0001

Freedom House. (2024). *Freedom on the net 2024: Indonesia*. https://freedomhouse.org/country/indonesia/freedom-net/2024

Freedom House. (2025). *Freedom on the net 2025: Indonesia*. https://freedomhouse.org/country/indonesia/freedom-net/2025

Gillespie, T. (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media*. Yake University Press.

Glasius, M., & Michaelsen, M. (2018). Illiberal and authoritarian practices in the digital sphere . *International Journal of Communication*, *12*.

Gómez-Cruz, E., Horst, H., Siles, I., & Soriano, C. (2023). Beyond the tropicalization of concepts: theorizing digital realities with and from the Global South (introduction to a special issue). *Communication, Culture & Critique*, *16*(4), 217–220. https://doi.org/10.1093/ccc/tcad037

Gumati, M. R. (2024). Digital Sovereignty or Regulatory Overreach? The Case of Indonesia's Platform Registration Policy. *Competition and Regulation in Network Industries*, *25*(4), 131–146. https://doi.org/10.1177/17835917251392903

Hadi, I. S., Chang, L. Y.-C., & Davies, S. G. (2026). The Snapshot of Society: Challenges of Studying Cyber Insecurity in the Global South? *Asian Journal of Criminology*, *21*(1), 25. https://doi.org/10.1007/s11417-026-09494-4

Handayani, E. P., Arifin, Z., & Fernando, Z. J. (2025). Criminal Penalties in Cyberspace: Between the Development of Digital Democracy and Authoritarianism. *IJCLS (Indonesian Journal of Criminal Law Studies)*, *10*(1). https://doi.org/10.15294/ijcls.v10i1.19652

Handayani, R., & Afrizal, G. (2018). Thin Clients as Memoryless Computer for Reducing Digital Divide in East Indonesia. *2018 12th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, 1–5. https://doi.org/10.1109/TSSA.2018.8708828

Harindranath, R., & Gómez-Cruz, E. (2023). Beyond concepts as tokens: heuristic value and epistemic politics in the study of digital subalterns. *Communication, Culture & Critique*, *16*(4), 228–234. https://doi.org/10.1093/ccc/tcad025

Hukumonline. (2026). *Lembaga pelindungan data pribadi tak kunjung dibentuk, UU PDP digugat ke MK*. Https://Www.Hukumonline.Com/Berita/a/Lembaga-Pelindungan-Data-Pribadi-Tak-Kunjung-Dibentuk--Uu-Pdp-Digugat-Ke-Mk-Lt69fd48eb0ba0d/. https://www.hukumonline.com/berita/a/lembaga-pelindungan-data-pribadi-tak-kunjung-dibentuk--uu-pdp-digugat-ke-mk-lt69fd48eb0ba0d/

Hunawa, R., Amu, R. W., Ibrahim, Z. S., & Amri, S. R. (2025). *Empowering Citizens* (pp. 339–366). https://doi.org/10.4018/979-8-3373-5781-2.ch013

Jalli, N. (2025). Viral Justice: TikTok Activism, Misinformation, and the Fight for Social Change in Southeast Asia. *Social Media + Society*, *11*(1). https://doi.org/10.1177/20563051251318122

Jaya, I. G. N. M., Pahlevi, S. M., Susenna, A., Agustina, L., Kusumasari, D., Sukma, Y. A. A., Hernikawati, D., Rahmi, A. A., Pravitasari, A. A., & Kristiani, F. (2024). Framework for Monitoring the Spatiotemporal Distribution and Clustering of the Digital Society Index of Indonesia. *Sustainability*, *16*(24), 11258. https://doi.org/10.3390/su162411258

Johnny G Plate divonis 15 tahun penjara di kasus BTS 4G Kominfo. (2023). *Kompas*. Https://Nasional.Kompas.Com/Read/2023/11/08/15432841/Johnny-g-Plate-Divonis-15-Tahun-Penjara-Di-Kasus-Bts-4g-Kominfo. https://nasional.kompas.com/read/2023/11/08/15432841/johnny-g-plate-divonis-15-tahun-penjara-di-kasus-bts-4g-kominfo

KING, G., PAN, J., & ROBERTS, M. E. (2013). How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review*, *107*(2), 326–343. https://doi.org/10.1017/S0003055413000014

Kominfo. (2020). *Peraturan Menteri Komunikasi dan Informatika No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik*. Jdih.Kominfo.Go.Id. https://jdih.kominfo.go.id/produk_hukum/view/id/759/t/peraturan+menteri+komunikasi+dan+informatika+nomor+5+tahun+2020

Kompas. (2025, September 3). *Mengapa TikTok matikan fitur Live di tengah demo berkecamuk?* Https://Nasional.Kompas.Com/Read/2025/09/03/07343861/Mengapa-Tiktok-Matikan-Fitur-Live-Di-Tengah-Demo-Berkecamuk. https://nasional.kompas.com/read/2025/09/03/07343861/mengapa-tiktok-matikan-fitur-live-di-tengah-demo-berkecamuk

Kompas. (2026a, March 19). *PP Tunas resmi berlaku, regulasi untuk melindungi anak di ruang digital*. Https://Nasional.Kompas.Com/Read/2026/03/19/21511411/Pp-Tunas-Resmi-Berlaku-Regulasi-Untuk-Melindungi-Anak-Di-Ruang-Digital.

Kompas. (2026b, July 26). *Komdigi ungkap perpres pembentukan Badan Perlindungan Data Pribadi sedang disusun*. Https://Nasional.Kompas.Com/Read/2026/07/27/15423511/Komdigi-Ungkap-Perpres-Pembentukan-Badan-Perlindungan-Data-Pribadi-Sedang.

Lim, J. B. Y. (2025). *Digital Media Interventions in Southeast Asia A Decolonial Perspective*. Springer Nature Switzerland.

Lim, M. (2023). "Everything Everywhere All At Once": Social Media, Marketing/Algorithmic Culture, and Activism in Southeast Asia. *Georgetown Journal of International Affairs*, *24*(2), 181–190. https://doi.org/10.1353/gia.2023.a913644

Liu, Y., & Song, W. (2026). Navigating digital colonialism: Sovereignty models and development paths in the Global South. *Social Sciences & Humanities Open*, *13*, 102546. https://doi.org/10.1016/j.ssaho.2026.102546

Margiansyah, D. (2025). Digitalizing Authoritarianism in Indonesia: Exploring the Intersection of Civic Activism, Digital Repression, and Democratic Erosion. In *Indonesian Perspectives on Democracy* (pp. 183–209). Springer Nature Singapore. https://doi.org/10.1007/978-981-96-3137-7_11

Marquez Bustos, N., Gregorio Chaviano, O., & Cuellar Cuellar, J. E. (2025). Research in Digital Methods: Global Production, Key Actors, and Field Tensions from a Bibliometric Perspective. *Signo y Pensamiento*, *44*. https://doi.org/10.11144/Javeriana.syp44.rdmg

Masduki, & Wendratama, E. (2025). Digital Activism for Press Freedom Advocacy in Post-Authoritarian Indonesia. *Journalism and Media*, *6*(3), 101. https://doi.org/10.3390/journalmedia6030101

Nemmani, S., & Rodriguez, C. (2023). Between incursions and appropriations: digital technologies and pluriversal modernities in the Global South. *Communication, Culture & Critique*, *16*(4), 258–265. https://doi.org/10.1093/ccc/tcad028

Penney, J. W. (2016). Chilling effects: Online surveillance and Wikipedia use. *Berkeley Technology Law Journal*, *31*(1).

Poernomo, S. L., Husen, L. O., Sivakumar, S., Aulia, N. A., & Muzakkir, Abd. K. (2026). Reformulating Indonesia's Consumer Protection Law in the AI-Driven Digital Economy: A Gap Analysis and Regulatory Roadmap. *Khazanah Hukum*, *8*(1), 118–132. https://doi.org/10.15575/kh.v8i1.51594

Pribadi, U., Iqbal, M., Ibrahim, M. A., Juhari, & Ahdarrijal, Y. (2024). Nexus of public organization, transparency, and accountability in Indonesia's digital governance. *Journal of Public Affairs*, *24*(3). https://doi.org/10.1002/pa.2940

Putra, B. A. (2024). Digital activism in Southeast Asia: the #MilkTeaAlliance and prospects for social resistance. *Frontiers in Sociology*, *9*. https://doi.org/10.3389/fsoc.2024.1478630

Rahayu, R., Roisah, K., Wardana, K. A., & Erlangga, V. L. S. (2024). Human Rights Defenders in Indonesia's Digital Age: Navigating Limited Spaces in the Quest for Digital Democracy. *Sriwijaya Law Review*, 358–375. https://doi.org/10.28946/slrev.Vol8.Iss2.3860.pp358-375

Rahmazani. (2022). PROBLEMATIKA HUKUM PENERAPAN UNDANG-UNDANG INFORMASI DAN TRANSAKSI ELEKTRONIK (UU ITE) DI INDONESIA. *Mimbar Hukum*, *34*(1), 161–185. https://doi.org/10.22146/mh.v34i1.3078

Rajagukguk, W., Adolf, B. H., & Medyawanti, P. (2024). Demographic and Socioeconomic Determinants Affecting Uses of the Internet in Indonesia. *Population and Economics*, *8*(2), 82–96. https://doi.org/10.3897/popecon.8.e108914

Roberts, M. E. (2018). *Censored*. Princeton University Press. https://doi.org/10.2307/j.ctvc77b21

Sabry, T., Mano, W., & Medrado, A. (2025). *Decolonising Approaches to Users and Audiences in the Global South*. Routledge. https://doi.org/10.4324/9781003452669

SAFEnet. (2023). *SAFEnet: Pemenuhan hak-hak digital di Indonesia kian memburuk* . https://safenet.or.id/id/2023/03/safenet-pemenuhan-hak-hak-digital-di-indonesia-kian-memburuk/

SAFEnet. (2025a). *Laporan Pemantauan Hak-hak Digital di Indonesia April-Juni 2025*.

SAFEnet. (2025b). *Laporan situasi hak-hak digital Indonesia 2024: Tergencet estafet represi di internet*. https://safenet.or.id/id/2025/02/laporan-situasi-hak-hak-digital-indonesia-2024/

SAFEnet. (2026). *Laporan situasi hak-hak digital Indonesia 2025: Orba datang lagi, represi tak pernah pergi*. https://safenet.or.id/id/2026/02/safenet-ungkap-mutasi-otoritarianisme-digital-di-indonesia/

Schauer, F. (1978). Fear, risk and the First Amendment: Unraveling the "chilling effect." *Boston University Law Review*.

Sen, A. (1999). *Development as freedom*. Oxford University Press.

Sinpeng, A. (2020). Digital media, political authoritarianism, and Internet controls in Southeast Asia. *Media, Culture & Society*, *42*(1), 25–39. https://doi.org/10.1177/0163443719884052

Tan, N., & Denyer, R. L. (2025). Digital Authoritarianism. In *Routledge handbook of autocratization in Southeast Asia* (1st ed., Vol. 1). Routledge.

Tempo. (2025a). *Menteri Komdigi: TikTok secara sukarela menutup fitur Live*. Https://Www.Tempo.Co/Politik/Menteri-Komdigi-Tiktok-Secara-Sukarela-Menutup-Fitur-Live-2065214. https://www.tempo.co/politik/menteri-komdigi-tiktok-secara-sukarela-menutup-fitur-live-2065214

Tempo. (2025b, February). *Minta maaf ke Kapolri, band Sukatani tarik lagu Bayar Bayar Bayar dari semua platform*. Https://Www.Tempo.Co/Hukum/Minta-Maaf-Ke-Kapolri-Band-Sukatani-Tarik-Lagu-Bayar-Bayar-Bayar-Dari-Semua-Platform-1209747. https://www.tempo.co/hukum/minta-maaf-ke-kapolri-band-sukatani-tarik-lagu-bayar-bayar-bayar-dari-semua-platform-1209747

Tobing, D. H. (2026). Taking Digitalisation's Bull by the Horns: Case Studies on Policy Innovation and Platforms-Driven Growth from Indonesia, the Philippines, and Thailand. In *Policy Innovations from the Global South* (pp. 55–73). https://doi.org/10.1007/978-3-032-11061-9_4

Utami, P. (2026). Towards the connective resilience framework: social network analysis of Indonesia gelap digital activism. *Communication Research and Practice*, 1–18. https://doi.org/10.1080/22041451.2026.2676496

Utomo, S. (2025). The Digital Age and Human Rights Protection in Indonesia: Legal Framework, Challenges, and Reform Directions. *Yustisia Jurnal Hukum*, *14*(2), 225. https://doi.org/10.20961/yustisia.v14i2.85404

Wijayanto, Berenschot, W., Sastramidjaja, Y., & Ruijgrok, K. (2026). The Infrastructure of Domestic Influence Operations: Cyber Troops and Public Opinion Manipulation Through Social Media in Indonesia. *The International Journal of Press/Politics*, *31*(3), 551–569. https://doi.org/10.1177/19401612241297832

Wijayanto, Setiyono, B., Martini, R., & Elsitra, G. N. (2021). Digital Authoritarianism in Southeast Asia: A Systematic Literature Review. *Proceedings of the 6th International Conference on Social and Political Enquiries, ICISPE 2021*.

Yilmaz, I. (2023). *Digital Authoritarianism and its Religious Legitimization* (I. Yilmaz, Ed.). Springer Nature Singapore. https://doi.org/10.1007/978-981-99-3600-7

YLBHI. (2025). *Dokumentasi kasus berbasis hotline Tim Advokasi untuk Demokrasi (TAUD) dalam aksi massa Agustus–September 2025*. https://ylbhi.or.id/informasi/siaran-pers/dokumentasi-kasus-berbasis-hotline-tim-advokasi-untuk-demokrasi-taud-dalam-aksi-massa-agustus-september-2025/

Yue, A., Nekmat, E., & Beta, A. R. (2019). Digital Literacy Through Digital Citizenship: Online Civic Participation and Public Opinion Evaluation of Youth Minorities in Southeast Asia. *Media and Communication*, *7*(2), 100–114. https://doi.org/10.17645/mac.v7i2.1899

Peraturan Perundang-undangan dan Putusan

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 40 Tahun 1999 tentang Pers.

Undang-Undang Nomor 12 Tahun 2005 tentang Pengesahan International Covenant on Civil and Political Rights.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 61 Tahun 2024 tentang Perubahan atas Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Peraturan Pemerintah Nomor 17 Tahun 2025 tentang Tata Kelola Penyelenggaraan Sistem Elektronik dalam Pelindungan Anak.

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.

Putusan Mahkamah Konstitusi Nomor 105/PUU-XXII/2024.