



The Evolution of Digital Violence in the Indonesian Media Ecosystem: An Analysis of the Patterns and Characteristics of Digital Attacks 2021-2025

Evolusi Kekerasan Digital dalam Ekosistem Media di Indonesia: Pola dan Karakteristik Serangan Digital Tahun 2021-2025

Mufti Nurlatifah ^{1*}

¹ Department Ilmu Komunikasi, Universitas Gadjah Mada, Indonesia

OPEN ACCESS

ISSN 2541-2841 (online)

ISSN 2302-6790 (print)

Edited by:

Didik Hariyanto

*Correspondence:
mufti.latifah@ugm.ac.id

Citation:

Mufti Nurlatifah. (2026). Evolusi Kekerasan Digital dalam Ekosistem Media di Indonesia: Pola dan Karakteristik Serangan Digital Tahun 2021-2025. 14(2)

Doi:10.21070/kanal.v12i2.1947

Abstract

Media freedom in Indonesia faces increasing peril due to a paradigm shift from physical violence to systematic digital repression. This evolving phenomenon undermines the media's essential role in upholding democracy and ensuring public access to information. This study utilizes qualitative content analysis of 57 documented cases of digital attacks against journalists and media institutions from 2021 to 2025, sourced from the Alliance of Independent Journalists (AJI). To enhance the validity findings, a complementary desk study was conducted. The analytical framework is informed by AJI's categorization of digital violence, including malware, phishing, hacking, doxing, impersonation, online harassment, and gender-based violence. The results reveals a significant escalation in digital attack frequency, with hacking and Distributed Denial of Services (DDos) attacks emerging as the predominant methods. Notably, media websites constitute the primary targets, indicating a systematic effort to undermine the infrastructure of information dissemination. Alarming, 47,4% of attacks focused on local media, posing the risk of creating information deserts at the community level. Temporal patterns suggest that attacks correlate with politically sensitive events, exploiting vulnerabilities in media security. The findings underscore the need for enhanced digital security measures and comprehensive protective frameworks to preserve media freedom within Indonesia's digital landscape.

Keywords: digital attacks, media freedom, repression evolution, content analysis

Abstrak

Kebebasan bermedia di Indonesia mengalami tantangan serius seiring pergeseran pola represi dari kekerasan fisik menjadi kekerasan digital yang sistematis. Studi ini menganalisis pola serta karakteristik serangan digital terhadap jurnalis dan media pada periode 2021-2025 untuk memahami transformasi represi dalam ekosistem media digital. Penelitian dilakukan dengan metode analisis isi kualitatif terhadap 57

laporan yang dihimpun Aliansi Jurnalis Independen dan diperkuat dengan desk study guna menjamin keabsahan data. Kerangka analisis mengacu pada kategorisasi kekerasan digital AJI yang meliputi: malware, phishing, hacking, doxing, impersonating, pelecehan daring, dan kekerasan berbasis gender daring. Hasil studi ini menunjukkan peretasan dan Distributed Denial of Service (DDoS) menjadi mekanisme serangan yang paling banyak terjadi. Website berita menjadi target utama serangan digital, yang mengindikasikan strategi sistematis untuk melumpuhkan infrastruktur produksi dan distribusi informasi. Selain itu, studi ini juga menunjukkan bahwa serangan digital tidak hanya menyasar media nasional namun juga media lokal. Temuan ini menunjukkan keterkaitan antara intensitas serangan dengan momentum politik yang sensitif, sekaligus pemanfaatan kelemahan sistem media sebagai celah terjadinya serangan digital. Penguatan infrastruktur keamanan digital pada akhirnya menjadi kebutuhan mendesak untuk menjaga keberlangsungan kebebasan bermedia pada ekosistem digital.

Kata Kunci: serangan digital, kebebasan bermedia, evolusi represi, analisis isi

PENDAHULUAN

Kebebasan bermedia di Indonesia mengalami tantangan yang semakin kompleks dengan berkembangnya beragam media dan platform informasi pada lanskap digital. Kekerasan terhadap media dan jurnalis juga mengalami evolusi seiring dengan semakin beragamnya instrumen teknologi pada jurnalisisme. Belakangan, kekerasan digital menjadi salah satu mekanisme yang banyak ditemukan sebagai cara yang digunakan untuk mengganggu proses jurnalisisme, termasuk membungkam suara jurnalis dan media (Badran, 2017; Donovan & Boyd, 2021). Menurut laporan dari *World Press Freedom Index* yang dirilis oleh *Reporters Without Borders* (RSF), Indonesia pada periode tahun 2025 ini mengalami penurunan signifikan dengan skor 44,13 dari 100 poin (RSF, 2025). Posisi ini menempatkan Indonesia pada peringkat 127 dari 180 negara, dan posisi ini menjadi peringkat terendah Indonesia selama 15 tahun terakhir. Salah satu alasannya adalah jumlah kekerasan terhadap jurnalis dan media yang meningkat dalam satu tahun terakhir, termasuk kekerasan yang terjadi melalui serangan digital. Hal ini menunjukkan terjadinya deteriorasi sistematis terhadap kebebasan bermedia di Indonesia, yang tidak hanya mewujud pada kekerasan fisik, namun telah bertransformasi menjadi bentuk represi digital yang lebih sulit untuk diidentifikasi.

Kekhawatiran kemunduran kebebasan bermedia dengan meningkatnya serangan digital ini cukup beralasan karena data yang dihimpun oleh Aliansi Jurnalis Independen (AJI) menunjukkan kondisi tersebut (Wendratama, Suci, Suriyani, & Masduki, 2024). AJI mengungkap peningkatan yang cukup signifikan atas serangan digital, dari 5 kasus pada tahun 2021 menjadi 16 kasus pada tahun 2023. Laporan AJI juga menunjukkan keterkaitan kontekstual yang kuat antara serangan digital dengan momentum-momentum politis yang cukup sensitif. Misalnya, serangan digital terhadap Tempo.co dan Narasi pasca publikasi kasus Ferdy Sambo. Kemudian serangan digital terhadap Project Multatuli pada Maret 2022 pasca pengungkapan laporan investigasi mereka. Pola ini mengindikasikan adanya strategi sistematis untuk mengganggu kebebasan bermedia, terlebih yang dilakukan oleh jurnalis dan media yang bersuara lantang atas kasus pelanggaran hak asasi manusia, korupsi, dan kontroversi politik. Padahal dalam upaya memproduksi dan mendiseminasikan informasi sensitif, banyak media yang berusaha mencari ruang konstruksi yang memadai untuk bisa diterima masyarakat (Qorib, Kristie, & Hakim, 2-24).

Studi atas kekerasan digital yang dilakukan sebelumnya menunjukkan bahwa persoalan kekerasan digital ini bukan hanya sekedar gangguan sederhana. Dampak dari kekerasan digital terhadap ekosistem kebebasan bermedia bersifat mendalam dan multidimensional. Pertama, serangan digital mengganggu akses publik atas informasi yang layak, di mana informasi publik merupakan hak fundamental warga negara, sebagaimana diakui dalam *Universal Declaration of Human Rights* (Siatitsa, 2020; Reglitz, 2025). Indonesia juga mengakui hak tersebut melalui Undang-Undang Hak Asasi Manusia dan Undang-Undang Keterbukaan Informasi Publik. Gangguan atas akses informasi ini tidak hanya berdampak pada individu, namun juga mempengaruhi kualitas deliberasi publik karena ruang partisipasi publik di ranah digital dibatasi.

Kedua, kekerasan digital juga merusak fungsi akuntabilitas pemerintahan dengan mengganggu fungsi pers sebagai pilar keempat demokrasi untuk mengawasi kekuasaan, menginformasikan penyalahgunaan, dan menjaga kepentingan publik (Feldstein, 2021; Gohdes, 2024). Ketika jurnalis dan media menjadi target serangan digital fungsi pengawasan yang mereka jalankan tidak dapat berjalan secara optimal. Kondisi ini akan menghambat arus produksi dan distribusi informasi serta menimbulkan efek jera yang dapat membungkam independensi media. Mekanisme verifikasi informasi sebagai tugas media dapat tergerus ketika media tidak dapat beroperasi secara bebas akibat tekanan digital secara terus menerus. Akibatnya, transparansi pemerintahan melemah karena peluang terjadinya penyalahgunaan kekuasaan lebih besar tanpa pengawasan dari media (Allen, 2008; Lindstedt & Naurin, 2010; Tong, 2025). Jika kondisi ini dibiarkan, akan mendorong terjadinya *authoritarian turn* di ranah digital yang menghasilkan bentuk kontrol baru serta represi digital (Masduki, 2021). Kondisi tersebut menyebabkan *chilling effect* dan *self-censorship* di kalangan profesional media.

Ketiga, serangan digital berimplikasi langsung pada terkikisnya pluralisme media (Parcu, 2019; Jungherr, Rivero, & Gayo-Avello, 2020; Urkens, Harambam, & d'Haenens, 2024). Pada iklim demokratisasi media yang baik, pluralisme media merupakan prasyarat penting untuk menjamin keberagaman suara, representasi kepentingan, dan pertukaran gagasan di ruang publik (Raeijmaekers & Maesele, 2015; Valke, Sukosd, & Picard, 2015). Namun, praktik kekerasan digital melalui serangan siber secara perlahan dapat menciptakan konsentrasi kekuasaan, tidak hanya pada segelintir aktor namun juga penguasa sumber daya teknologi. Hal ini dapat menghilangkan keberagaman suara di dalam ruang publik, yang pada gilirannya dapat mengancam representasi dan keberagaman sudut pandang dalam masyarakat. Dengan demikian, serangan digital tidak hanya berdampak pada aspek teknis keamanan, namun juga memunculkan konsekuensi struktural pada pluralisme media. Jika hal ini berlanjut, ruang publik digital akan menjadi homogen, terpolarisasi, dan rentan dimonopoli oleh narasi dominan yang mengabaikan kepentingan kelompok-kelompok rentan.

Merujuk pada urgensi antisipatif atas serangan digital pada jurnalis dan media, kita perlu memahami dulu konseptualisasi dari serangan digital tersebut dalam studi ini. Terminologi “serangan digital” dalam ranah kekerasan terhadap jurnalis mengacu pada eksploitasi terhadap teknologi informasi dan komunikasi untuk melakukan intimidasi, destabilisasi, dan manipulasi kerja institusi media maupun jurnalis dengan maksud menghambat fungsi jurnalisisme untuk menguntungkan pihak-pihak tertentu. UNESCO dan Internasional Center for Journalists mendefinisikan fenomena ini sebagai *targetted harassment* yang dilakukan melalui teknologi terhadap orang, perempuan, atau pihak-pihak tertentu, yang mencakup ancaman fisik, invasi privasi, kebohongan yang merusak reputasi, seruan untuk menyakiti, dan penghinaan (Slavtcheva-Perkova, et al., 2023; Zviyita, 2024). Yang membedakan kekerasan digital dari bentuk kekerasan konvensional adalah karakteristiknya yang *insidious* dan *pervasive*, dapat dilakukan secara anonim, melampaui batas

geografis, memiliki dampak berkelanjutan dalam ruang digital, dan menciptakan jejak digital yang sulit dihapus (Dodds, Geboers, & Boukes, 2023; Slavtcheva-Perkova, et al., 2023).

Kekerasan digital ini termanifestasi dalam berbagai bentuk seperti perundungan siber, penyebaran konten tanpa konsensual, disinformasi dan misinformasi, pelanggaran privasi termasuk *doxing* dan *cyber-stalking*, serangan DDoS, pembungkaman ekspresi online, *surveillance*, *phishing*, sampai dengan penyitaan perangkat keras (Lewis, Zamith, & Coddington, 2020; Zviyita, 2024). Melalui elaborasi tersebut, kekerasan digital dapat dipahami sebagai serangkaian tindakan yang menggunakan teknologi digital, platform daring, maupun infrastruktur internet untuk mengintimidasi, membatasi, atau bahkan menghilangkan hak-hak individu maupun kelompok di lanskap digital. Bentuk kekerasan ini tidak hanya berkaitan dengan aspek teknis keamanan data, namun juga melibatkan aspek dimensi sosial, politik, dan psikologis terutama jurnalis dan media dalam konteks penelitian ini. Hal ini termasuk dampak lanjutan yang terjadi seperti melemahnya kebebasan berekspresi, terhambatnya akses atas informasi yang layak, dan iklim ketakutan yang tercipta karena pembatasan partisipasi publik. Merujuk pada konseptualisasi tersebut, kekerasan digital yang termanifestasi pada serangan digital pada jurnalis dan institusi media, bukan hanya fenomena insidental melainkan gejala struktural yang memiliki implikasi serius pada demokratisasi bermedia.

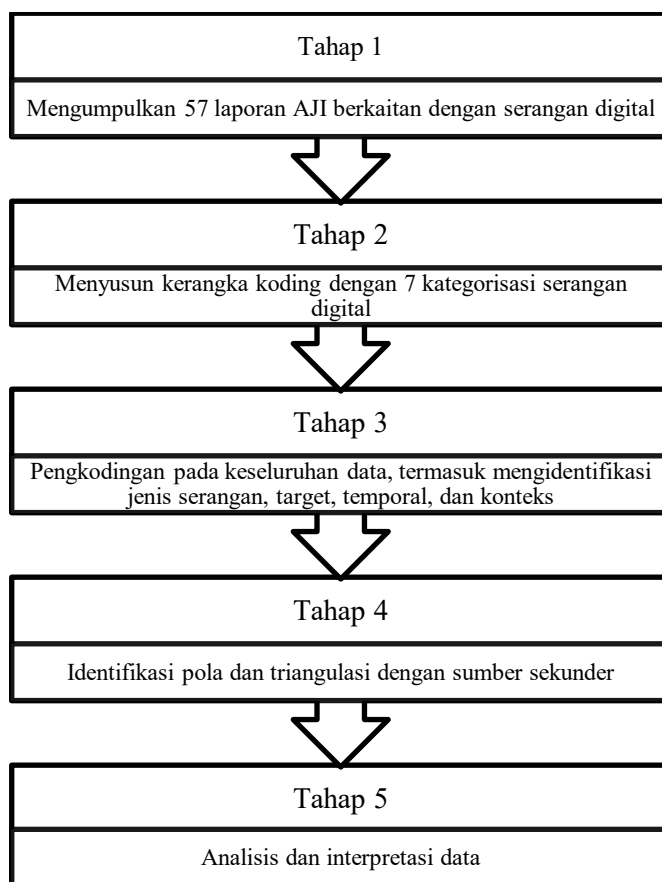
Berdasarkan urgensi pemahaman terhadap fenomena serangan digital yang dialami jurnalis Indonesia, studi ini menguraikan pertanyaan penelitian bagaimana karakteristik, pola, dan mekanisme serangan digital yang dialami oleh jurnalis dan institusi media di Indonesia selama kurun waktu 2021 sampai dengan 2025. Sejalan dengan pertanyaan penelitian tersebut, penelitian ini bertujuan untuk mengidentifikasi dan menganalisis karakteristik serangan digital terhadap jurnalis di Indonesia dengan menggunakan kerangka konseptual yang dikembangkan oleh Aliansi Jurnalis Independen (AJI) Indonesia. Selanjutnya, studi ini juga bermaksud memetakan pola temporal dan kontekstual serangan digital untuk mengungkapkan korelasi antara serangan dengan dinamika sosio-politik dan jenis liputan yang dilakukan oleh jurnalis. Dengan demikian aspek multidimensional serangan digital terhadap kebebasan bermedia dan praktik jurnalisisme di Indonesia dapat dielaborasi secara komprehensif.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan menggabungkan analisis isi dokumen dan *desk study* untuk menganalisis laporan serangan digital terhadap jurnalis yang dikumpulkan oleh Aliansi Jurnalis Independen selama kurun waktu 2021-2025. Analisis isi dokumen dipilih sebagai metode utama karena memungkinkan peneliti untuk mengekstraksi dan menganalisis informasi mendalam dari data sekunder yang telah tersedia, yaitu 57 laporan serangan digital pada laman lapor AJI Indonesia. Pendekatan ini sesuai dengan karakteristik data yang berupa dokumen laporan terstruktur yang memuat informasi yang dibutuhkan untuk memahami kronologi, jenis serangan, dan konsekuensi yang

ditimbulkannya (Altheide, 2011; Cheong, Lyons, Houghton, & Majumdar, 2023).

Kerangka analisis dalam studi ini mengadopsi kategorisasi kekerasan digital yang dikembangkan oleh Aliansi Jurnalis Independen (2022). AI mengkategorisasikan kekerasan digital ini ke dalam beberapa bentuk. Pertama, serangan malware (malicious software), termasuk virus, worm, trojan horse, dan spyware. Kedua, phishing melalui email, telepon, atau pesan teks yang bertujuan mendapatkan data-data sensitif. Ketiga, peretasan atau hacking untuk mengakses peralatan elektronik tanpa izin. Keempat, doxing dengan mempublikasikan informasi pribadi dengan tujuan mempermalukan atau menguak hal-hal personal. Kelima, *impersonating* atau membuat identitas palsu untuk mempersonifikasi seseorang. Keenam, pelecehan online atau *online harassment* dalam bentuk intimidasi dan pengancaman. Ketujuh, kekerasan berbasis gender online (KBGO). Kategorisasi ini akan menjadi kerangka koding utama dalam proses analisis data untuk mengidentifikasi pola dan karakteristik serangan digital yang dialami oleh jurnalis dan media di Indonesia. Secara lebih lanjut tahapan penelitian dalam studi ini adalah sebagai berikut:



Gambar 1. Tahapan Penelitian

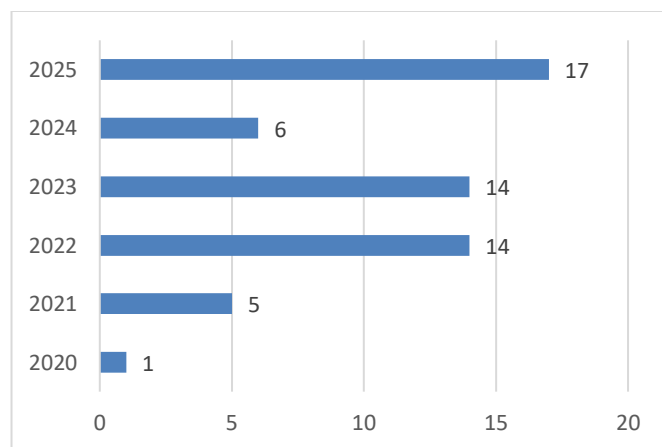
Sumber: Data Primer, 2026

Proses analisis data dilakukan dengan beberapa tahapan sistematis. Pertama, tahap preparasi data dengan melakukan inventarisasi dan digitalisasi seluruh dokumen laporan AJI, kemudian membuat prosedur pengkodean berdasarkan

kerangka kategorisasi AJI. Kedua, tahap pengkodean deduktif dengan mengklasifikasikan setiap laporan ke dalam tujuh kategorisasi serangan digital yang ditetapkan, sekaligus mencatat informasi kontekstual, seperti waktu kejadian, profil korban, jenis media, dan momentum politik yang terjadi. Ketiga, tahap pengkodean induktif untuk mengidentifikasi pola-pola yang muncul dalam data, termasuk sub-kategori dalam setiap jenis serangan dan faktor kontekstual atas terjadinya serangan tersebut. Keempat, tahap analisis temporal dan dampak, untuk memetakan tren dan dinamika serangan yang terjadi, termasuk peristiwa yang menyertainya sebagai konteks dan konsekuensi. Untuk menjamin kesahihan penelitian, triangulasi data dilakukan dengan membandingkan temuan dari laporan AJI dengan data sekunder lainnya yang didapatkan melalui *desk study*. Secara etis, penelitian ini memastikan anonimitas korban dengan tidak mengekspose detail data yang dapat membahayakan keselamatan jurnalis yang terlibat.

HASIL DAN PEMBAHASAN

Hasil dari penelitian ini menunjukkan bahwa dari 57 laporan yang dihimpun oleh Aliansi Jurnalis Independen dari tahun 2021 sampai dengan Agustus 2025, mengungkapkan pola sistematis kekerasan digital yang mengancam kebebasan bermedia di Indonesia. Merunut tren waktu dari tahun ke tahun, studi ini menemukan dinamika yang menarik atas serangan digital yang terjadi. Puncak serangan terjadi pada tahun 2025 dengan 17 kasus, diikuti periode 2022 dan 2023 yang masing-masing mencatat 14 kasus. Penurunan kasus secara drastis terjadi pada tahun 2024, namun kemudian diikuti lonjakan tajam pada tahun 2025. Fluktuasi ini mengindikasikan adanya korelasi antara dinamika sosio-politik nasional dan adopsi teknologi digital yang semakin masif. Hal ini ditandai dengan penurunan signifikan kasus pada tahun 2024 yang merupakan tahun politik di Indonesia, sehingga banyak pihak berusaha mengamankan diri dan berhubungan baik dengan media.

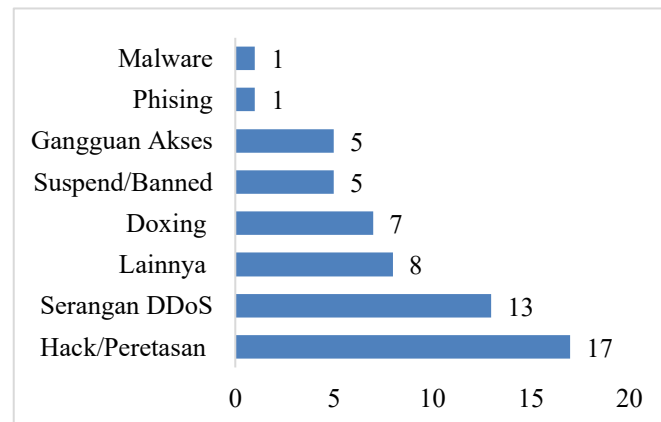


Gambar 2. Kasus Serangan Digital Berdasarkan Tahun
Sumber: Data Primer, 2026

a. Tren Kekerasan Digital

Merujuk pada kerangka kategorisasi Aliansi Jurnalis Independen (AJI), studi ini mengidentifikasi tren kekerasan

yang terjadi selama lima tahun dan menunjukkan bahwa hacking atau peretasan mendominasi serangan digital dengan 17 kasus (29,8%), diikuti oleh serangan DDoS dengan 13 kasus (22,8%). Mekanisme klasik namun cukup mengganggu operasionalisasi dari kinerja media dan institusi.



Gambar 3. Kategori Serangan Digital

Sumber: Diolah Peneliti

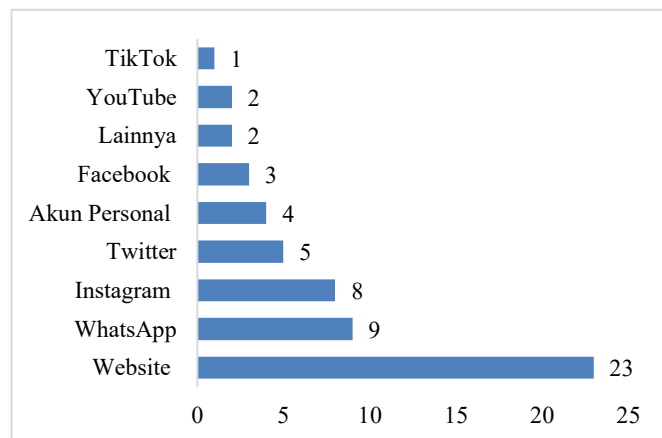
Temuan lain dalam studi ini juga mengidentifikasi doxing menempati posisi berikutnya dengan 7 kasus (12,3%). Serangan ini terjadi terutama kepada jurnalis dan pengelola media dengan cara menyebarkan informasi pribadi melalui platform digital. Sementara itu suspend/banned platform juga ditemukan sebanyak 5 kasus (8,8%) dan gangguan akses juga sebanyak 5 kasus (8,8%). Terjadinya pemblokiran dan penangguhan akun secara tidak langsung menunjukkan bahwa metode serangan digital juga dilakukan dengan mengandalkan kebijakan platform digital sebagai instrumen represi (Cobbe, 2021; Kokshagina, Reinecke, & Karamasios, 2023). Tekanan ini mengombinasikan tekanan algoritmik dan tekanan politik yang pada akhirnya membatasi ruang gerak jurnalis dan institusi media.

Hasil identifikasi tersebut mengonfirmasi bahwa serangan digital telah berevolusi dari gangguan teknis sederhana kepada media atau kepada jurnalis, menjadi strategi yang lebih sistematis dengan melumpuhkan infrastruktur digital media dan memberikan tekanan personal kepada jurnalis yang bekerja. Hal ini terjadi secara *multi-layered* dengan menghasilkan kerusakan yang berbeda-beda. Artinya, mekanisme serangan digital yang terjadi pada akhirnya akan berdampak langsung dan masif terhadap operasional media.

b. Target Serangan Digital

Menilik sasaran serangan digital yang terjadi, studi ini mengidentifikasi bahwa website media menjadi target utama serangan digital dengan 23 kasus (40,4%). Hal ini mencerminkan upaya sistematis untuk melumpuhkan sumber informasi utama bagi publik, mengingat website media dalam praktiknya menjadi rumah bagi institusi media dan jurnalis. Serangan terhadap website media akan menimbulkan efek berantai yang mengganggu operasional media. Kasus yang terjadi pada Tempo, Project Multatuli, dan Narasi memperlihatkan praktik penargetan selektif dengan mengeksploitasi titik rawan media. Berbeda dengan media sosial, website memiliki arsitektur informasi yang lebih terpusat sehingga gangguan digital yang terjadi dapat

menimbulkan efek berkelanjutan (Rosenfeld, Morville, & Arango, 2015; Ruzza, Tiozzo, Mantovani, D'Este, & Ravarotto, 2017). Tidak hanya akses produksi informasi yang dilakukan oleh media itu sendiri, namun juga aspek manajerial lainnya termasuk alur kerja redaksi, monetisasi konten, dan juga akses publik terhadap informasi.



Gambar 4. Target Platform Serangan Digital
Sumber: Data Primer, 2026

Selain website media, sasaran serangan digital ini juga ditujukan pada WhatsApp (9 kasus) dan Instagram (8 kasus). Keduanya adalah platform komunikasi dan distribusi konten yang bersifat strategis, baik bagi institusi media maupun jurnalis. Kasus peretasan yang dialami oleh Ketua Aliansi Jurnalis Independen dan Jurnalis Tempo menunjukkan adanya penargetan serangan yang mengganggu rantai operasional jurnalis. WhatsApp dalam kerja jurnalis tidak hanya berfungsi sebagai platform komunikasi namun juga menjadi tulang punggung operasional yang menghubungkan redaksi, sumber berita, dan jaringan distribusi konten dalam ekosistem komunikasi *real-time* (Dodds T., 2019; Kligler-Vilenchik & Tenenboim, 2020). Serangan terhadap akun WhatsApp dari jurnalis berpotensi mengganggu upaya perlindungan terhadap sumber informasi dan koordinasi editorial dalam produksi informasi.

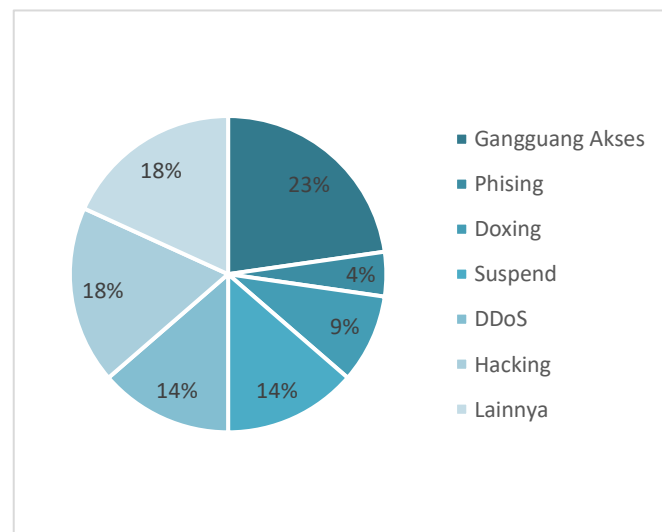
Dari perspektif institusi media, Tempo menjadi media yang paling sering menjadi target serangan digital dengan 6 kasus (10,5%), diikuti dengan Project Multatuli dengan 5 kasus (8,8%). Keduanya terhitung sebagai media nasional yang mengalami serangan digital lebih dari satu kali. Akan tetapi, dari sisi kuantitatif, media lokal atau media regional tercatat menempati persentase tertinggi mengalami serangan digital yaitu 27 kasus (47,4%), meskipun menyasar pada media yang berbeda-beda. Kondisi ini menunjukkan bahwa serangan digital yang terjadi pada media maupun jurnalis di Indonesia tidak selalu melibatkan media nasional yang berskala besar, namun juga bisa terjadi pada media lokal dan media *grassroots* yang memiliki peran penting dalam produksi dan diseminasi informasi di level yang lebih spesifik.

Menariknya, dari banyaknya media dan jurnalis yang mendapatkan serangan digital ini, tidak selalu serangan digital ini didasarkan oleh pemberitaan atas kasus-kasus sensitif yang menyasar pihak-pihak tertentu. Hanya 15 kasus saja yang

secara spesifik berhubungan dengan isu-isu sensitif di Indonesia. Serangan pada Pikiran Rakyat terjadi pasca mereka melakukan Live TikTok untuk menyiarkan demonstrasi yang sedang berlangsung. Hal yang sama juga dialami oleh Jaring.id dan Konde.co. Namun demikian, bukan berarti tidak ada liputan sensitif yang menjadi pemicu serangan digital pada media dan jurnalis. Pada konteks laporan investigasi, terdapat 5 serangan digital yang terjadi pasca penerbitan laporan-laporan sensitif seperti kekerasan seksual, korupsi, dan penyalahgunaan kekuasaan. Website Tempo.co pada 6 Agustus 2022 mengalami serangan DDoS pasca mereka mempublikasikan kasus Ferdy Sambo yang. Serangan serupa dialami oleh Project Multatuli pada 3 Agustus 2023, pasca penerbitan liputan gamifikasi ojek online.

c. Ruang Lingkup Media pada Serangan Digital

Secara lebih lanjut, studi ini juga mengidentifikasi bahwa media lokal juga tak luput dari serangan digital ini. Pada 11 November 2022, Floresa.co diserang setelah mempublikasikan laporan kolaboratif mereka bersama Project Multatuli dengan judul, “Saudara Kembar Komodo yang Menolak Dipinggirkan Korporasi Bisnis Pariwisata”. Kasus Floresa ini menunjukkan adanya *strategic targetting* dalam serangan digital, terutama pada laporan-laporan investigatif yang dianggap mengancam kepentingan bisnis dan proyek pembangunan daerah. Artinya, skala ancaman atas serangan digital ini tidak selalu berada pada aras isu nasional, namun juga pada isu-isu lokal di daerah. Floresa.co sendiri sudah tiga kali mengalami serangan digital ini selama periode 2021 sampai dengan 2025.



Gambar 5. Serangan Digital pada Jurnalis dan Media Lokal
Sumber: Data Primer, 2026

Dari laporan serangan digital yang dihimpun oleh Aliansi Jurnalis Independen, 23 kasus diantaranya (40,4%) adalah laporan yang menempatkan jurnalis dan media lokal sebagai pihak yang diserang. Temuan ini menunjukkan represi digital telah meluas pula ke ekosistem media daerah. Padahal media lokal dalam dinamika deliberatif di daerah acapkali menjadi sumber informasi kritis yang memiliki sudut pandang representatif terkait tata kelola pemerintahan

daerah, isu lingkungan, serta persoalan komunitas yang tidak tercakup dalam media nasional. Penyerangan terhadap media lokal menciptakan *information deserts* di tingkat komunitas dan dikhawatirkan akan menggerus akses informasi yang merupakan prasyarat bagi partisipasi demokratis oleh masyarakat (Lee & Butler, 2018; Torre, Ramos, Noronha, & Jeronimo, 2024).

Pergeseran Paradigma Kekerasan Media dan Terciptanya Digital Authoritarianism

a. Kekhawatiran Efek Jera dan Self-Censorship

Dominasi praktik *hacking*, serangan DDos, dan doxing menunjukkan bagaimana teknologi digital diinstrumentalisasi sebagai perangkat kontrol dalam kerangka yang kerap disebut sebagai otoritarianisme digital (Sinpeng, 2019; Dragu & Lupu, 2021; Roberts & Oosterom, 2024). Strategi ini membentuk relasi kuasa yang asimetris, di mana pihak dengan sumber daya teknologi yang lebih unggul mampu melumpuhkan media tanpa harus menggunakan kekerasan fisik secara langsung (Kalathil, 2020; Dragu & Lupu, 2021). Efek jera jurnalis atau media atas serangan tersebut, pada akhirnya bersifat antisipatif. Media cenderung melakukan penyensoran diri berdasarkan perkiraan adanya potensi serangan, bukan semata-mata sebagai respon terhadap ancaman yang eksplisit. Situasi ini menghasilkan mekanisme kuasa yang bersifat disipliner dan justru lebih ketat dibandingkan sensor tradisional, karena kontrol dijalankan melalui internalisasi oleh media itu sendiri. Dari sisi demokratisasi bermedia kondisi ini bukan sesuatu yang membahagiakan karena jurnalis dan media pada akhirnya harus waspada dan membatasi diri untuk tetap bisa bekerja secara profesional.

Selain itu, dominasi praktik serangan digital dengan *hacking*, DDos, dan doxing tadi juga menunjukkan terjadinya pergeseran paradigma dari kekerasan fisik menuju kekerasan digital sebagai mekanisme represi terhadap media di Indonesia. Pergeseran ini menunjukkan pula strategi adaptif para pelaku serangan digital yang memanfaatkan kerentanan infrastruktur digital serta keterbatasan kapasitas pertahanan media, sehingga melahirkan bentuk intimidasi yang lebih efektif dan bisa jadi lebih sulit dideteksi. Hal ini dibuktikan melalui analisis temporal dari data serangan digital pada penelitian ini. Analisis pola harian mengungkapkan bahwa Jumat menjadi hari dengan frekuensi serangan tertinggi yaitu 13 kasus (22,8%). Selain itu terdapat pula 10 kasus (17,5%) yang terjadi pada hari Rabu. Merujuk pada karakteristik ekosistem digital, hari Rabu adalah tengah pekan dan Jumat adalah periode menjelang akhir pekan. Pola ini menunjukkan strategi yang diperhitungkan dengan memanfaatkan momentum kelengahan kapasitas sistem media, baik dari sisi teknologi maupun manusia. Momentum tengah minggu dan akhir pekan merupakan periode kapasitas respon teknis cenderung mengalami penurunan (Loeschner, 2017; Kubo, et al., 2018).

Studi ini juga menemukan kegamangan serupa melalui temuan jenis platform sasaran pada serangan digital. Pola penargetan dalam serangan digital menunjukkan adanya prioritas yang hierarkis. Serangan terhadap website media dapat dimaknai sebagai serangan terhadap rumah institusional media dan jurnalis. Sementara serangan terhadap WhatsApp jurnalis dan media dapat dilihat sebagai mekanisme merusak

rantai komunikasi di dalam institusi media. Sedangkan serangan terhadap Instagram, Facebook, dan Twitter milik media maupun jurnalis mengindikasikan upaya perusakan antarmuka dari distribusi informasi. Kondisi tersebut menunjukkan pendekatan yang sistematis dengan mempertimbangkan karakteristik ekosistem digital dan pemanfaatannya oleh jurnalis maupun institusi media.

Berdasarkan elaborasi tersebut, serangan digital yang terjadi pada jurnalis dan media bisa jadi bukan sesuatu yang acak. Menilik dari upaya menciptakan efek jera dan *self-censorship* pada media, serangan digital dilakukan untuk menciptakan kerusakan operasional yang terprediksi, namun dengan tingkat kemungkinan terdeteksi yang minimal. Kondisi ini juga mengungkap kerentanan aspek digital yang selama ini mungkin tidak disadari oleh institusi media dan jurnalis, bahwa fragmentasi platform menciptakan banyak titik serangan yang tidak mudah dilindungi dalam waktu yang bersamaan.

b. Persoalan Akuntabilitas dan Erosi Pluralisme Media

Serangan digital sebagai disrupsi terhadap fungsi *fourth estate* tercermin dari penargetan strategis terhadap media yang bersuara kritis di tengah masyarakat. Serangan berulang terhadap Tempo, Narasi, Project Multatuli, dan Floresa.co saat media-media ini melaporkan terjadinya praktik penyalahgunaan kekuasaan, korupsi, dan kegagalan institusi dalam mengimplementasikan kebijakan, menandakan adanya kekhawatiran atas penyelenggaraan jurnalisme *watchdog* oleh media-media tersebut. Dominasi serangan peretasan pada infrastruktur media, seperti website dan platform media sosialnya, menandakan adanya upaya infiltrasi ke dalam sistem editorial yang akan mengganggu rantai produksi dan distribusi informasi (Aradau, Blanke, & Greenwat, 2019; Salvo, 2025).

Penargetan terhadap media lokal (38,6%) secara khusus menimbulkan kerusakan yang signifikan atas akuntabilitas media di tingkat akar rumput. Pasalnya, media-media daerah acapkali menjadi satu-satunya sumber informasi yang dirujuk untuk melihat dinamika sosial, ekonomi, dan politik di daerah (Ramadhan & Afala, 2024; Hidayat & Rusadi, 2025). Termasuk menjadi corong pelaporan atas rusaknya tata kelola dan kegagalan sistem yang berlangsung di tingkat lokal. Mereka juga memotret praktik-praktik di level lokal yang acapkali absen dari perspektif media nasional. Oleh karenanya gangguan terhadap media lokal ini bukan hanya menunjukkan makin luasnya ruang lingkup serangan digital, namun juga dikhawatirkan menciptakan kekosongan akuntabilitas di tingkat komunitas lokal yang penting bagi tata kelola demokrasi (Rianto, 2023).

Idealnya, pluralisme media yang kondusif termanifestasi melali representasi keragaman suara dan perspektif yang esensial bagi wacana di ruang publik lokal (Raeijmaekers & Maesele, 2015; Valke, Sukosd, & Picard, 2015). Penargetan serangan secara berulang pada Floresa.co menunjukkan adanya upaya strategis dalam mengganggu keberagaman ekosistem informasi yang bergantung pada *content sharing* lintas platform. Tidak ubahnya dengan media-media besar, kerentanan pada media lokal menjadi celah yang digunakan untuk melakukan penekanan dan pembungkaman secara terstruktur. Perspektif alternatif yang bersuara kritis seakan-

akan menjadi nada sumbang yang tidak bisa diterima begitu saja sehingga harus diganggu melalui serangan-serangan digital yang sulit dideteksi oleh media yang tidak dilengkapi dengan perlindungan digital yang memadai. Pola-pola semacam itu juga dijumpai pada media lokal lainnya seperti pada AcehKini.id dan SuaraPapua.com. Jika terus berlanjut, kondisi ini akan menyebabkan terjadinya monokultur informasi yang membatasi keberagaman perspektif dan melemahkan pluralisme media. Pasalnya, akumulasi serangan digital yang berulang dan terkoordinasi ini bisa mendorong perubahan struktural dalam ekosistem media di Indonesia. Hal inilah yang menciptakan otoritarianisme digital yang lebih halus dari sensor konvensional (Dragu & Lupu, 2021; Rianto, 2023). Gangguan teknis lebih ditakuti karena mereka berusaha mempertahankan eksistensinya dengan menjaga rumah mereka sebaik-baiknya, termasuk dengan menghindari bersuara yang berbeda dari media-media yang memberitakan informasi serupa namun baik-baik saja.

c. Kebutuhan Regulasi dan Kolaborasi Multi-Stakeholder

Sejumlah persoalan yang muncul dari analisis serangan di atas bermuara pada isu kerentanan infrastruktur digital yang menjadi persoalan pokok bagi institusi media dan jurnalis dalam menyelenggarakan pekerjaan profesionalnya. Oleh karena itu, perlindungan terhadap jurnalis dan media membutuhkan rekontekstualisasi terkait penguatan infrastruktur keamanan digital dan peningkatan ketahanan siber. Tanpa acuan kerangka keamanan digital yang komprehensif, baik institusi media maupun jurnalis akan tetap rentan terhadap beragam bentuk serangan digital yang mengganggu kerja media serta mengancam fondasi struktural kebebasan bermedia pada ekosistem digital (Miller & Vaccari, 2020; Henrichsen & Shelton, 2023). Pendekatan multi-stakeholder perlu dilakukan untuk memecahkan peliknya persoalan keamanan digital yang menempatkan media dan jurnalis dan posisi yang tidak cukup menguntungkan (Ciglic & Hering, 2021; Katrakazas & Papastergiou, 2024). Secara lebih lanjut, pemerintah perlu mengadopsi kerangka regulasi yang lebih relevan untuk mengambil tindakan yang lebih efektif dalam kacamata Indonesia. Kerangka regulasi ini tidak hanya berfokus pada keamanan siber, namun juga upaya yang lebih komprehensif dengan berfokus pada kebebasan bermedia dan mempertimbangkan karakteristik ekosistem digital, termasuk mekanisme penyelesaian sengketa terstruktur bagi media yang mengalami moderasi konten tidak adil dan serangan digital. Regulator pada konteks ini perlu memperluas perspektifnya dari sekedar , menangani keamanan jaringan menuju koordinasi proaktif dengan pemangku kepentingan, mengimplementasikan kolaborasi lintas sektor, tanggap terhadap insiden, dan bantuan teknis darurat jika terjadi serangan digital. Platform digital perlu menyediakan jalur khusus untuk menjamin keamanan digital bagi media dan jurnalis, sementara organisasi masyarakat sipil perlu membentuk kelompok kerja untuk mengkoordinasikan aspek-aspek strategis dalam kerja advokasi maupun keahlian teknis.

KESIMPULAN

Analisis mendalam terhadap 57 laporan serangan digital yang dihimpun oleh Aliansi Jurnalis Independen (AJI) pada periode 2021-2025 menunjukkan adanya pergeseran fundamental dari kekerasan fisik dan sporadis menuju represi digital yang sistematis dan terukur. Kondisi ini bisa diidentifikasi sebagai ancaman demokratisasi bermedia di Indonesia. Bentuk-bentuk serangan dominan seperti peretasan (29,8%), serangan Distributed Denial of Services (22,8%), dan doxing (12,3%), tidak lagi bisa dipandang sebagai sekedar gangguan teknis. Sebaliknya, serangan-serangan ini justru merepresentasikan strategi *weaponization* infrastruktur digital untuk melumpuhkan kerja jurnalis sekaligus menimbulkan efek jera bagi jurnalis dan institusi media. Apalagi menilik dari analisis temporal, serangan digital yang terjadi acapkali beriringan dengan terbitnya liputan sensitif atau isu-isu yang sebenarnya ingin dibungkam. Hal ini tentu menjadi penanda adanya upaya memberangus kebebasan bermedia dan menghambat pelaporan jurnalis yang akuntabel. Tingginya serangan terhadap website media bisa menjadi bukti penguat adanya dugaan tersebut. Apalagi website sebagai rumah bagi media menjadi penghubung mata rantai produksi dan distribusi informasi pada institusi media.

Temuan yang tak kalah mengkhawatirkan muncul dari jumlah serangan ke media lokal da daerah. Sebaran jumlah laporan serangan digital di daerah menunjukkan penguatan otoritarianisme digital dalam skala yang cukup luas, tidak hanya mengendalikan media arus utama, namun juga media lokal yang memegang kendali dalam arus informasi di daerah. Pola yang ada di daerah serupa dengan pola yang terjadi pada media nasional, di mana serangan terhadap media ataupun jurnalis terjadi pasca penerbitan informasi investigatif dan sensitif. Hal ini berpotensi menghasilkan *information deserts* dan mendorong terjadinya self-censorship secara antisipatif. Inilah yang dikatakan sebagai pergeseran paradigmatis dalam represi terhadap jurnalis dan media, di mana otoritarianisme digital yang bersifat *native*, adaptif, dan lebih sulit dideteksi terjadi secara terstruktur dengan memanfaatkan celah kelemahan media pada ekosistem digital. Situs ini menuntut adanya rekonseptualisasi mendasar terkait strategi perlindungan media dan jurnalis. Strategi yang tidak hanya sekesar reaktif terhadap serangan individual, namun lebih bisa mengantisipasi pola sistematis dengan mempertimbangkan infrastruktur ketahanan siber yang memadai guna menjaga keberlangsungan kebebasan bermedia pada ekosistem media digital.

REFERENSI

- Allen, D. (2008). The Trouble with Transparency: The Challenge of Doing Journalism Ethics in a Surveillance Society. *Journalism Studies*, 9(3), 323-340.
- Altheide, D. (2011). *Qualitative Media Analysis*. New York : Sage Publications.
- Aradau, C., Blanke, T., & Greenwat, G. (2019). Acts of Digital Parasitism: Hacking, Humanitarian Apps and Platformisation. *New Media & Society*, 21(11-12), 2548-2565.
- Badran, M. (2017). Violence Against Journalists: Suppressing Media Freedom. In M. Friedrichsen, & Y. Kamalipour, *Digital Transformation in Journalism and News Media* (pp. https://doi.org/10.1007/978-3-319-27786-8_31). Cham : Springer.
- Cheong, H., Lyons, A., Houghton, R., & Majumdar, A. (2023). Secondary Qualitative Research Methodology Using Online Data within the Context of Social Sciences. *International Journal of Qualitative Methods*, 22, 1-19.
- Ciglic, K., & Hering, J. (2021). A Multi-Stakeholder for Foundation for Peace in Cyberspace. *Journal of Cyber Policy*, 6(3), 360-374.
- Cobbe, J. (2021). Algorithmic Censorship by Social Platforms: Power and Resistance. *Philosophy & Technology*, 34, 739-766.
- Dodds, T. (2019). Reporting with WhatsApp: Mobile Chat Applications Impact on Journalistic Practices. *Digital Journalism*, 7(6), 725-745.
- Dodds, T., Geboers, M., & Boukes, M. (2023). "It Became No Man's Land": The Burden of Moderating Online Harassment in Newswork. *Journalism Practice* , <https://doi.org/10.1080/17512786.2024.2387664>.
- Donovan, J., & Boyd, D. (2021). Stop the Presses? Moving from Strategic Silence to Strategic Amplification in a Networked Media Ecosystem. *Americal Behavioral Scienciest*, 65(2), 333-350.
- Dragu, T., & Lupu, Y. (2021). Digital Authoritarianism and The Future of Human Rights. *International Organization*, 75(4), 991-1017.
- Feldstein, S. (2021). *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*. New York: Oxford University Press.
- Gohdes, A. (2024). *Repression in The Digital Age: Surveillance, Censorship, and the Dynamics of State Violence*. New York : Oxford University Press.
- Henrichsen, J., & Shelton, M. (2023). Expanding the Analytical Boundaries of Mob Censorship: How Technology and Infrastructure Enable Novel Threats to Journalists and Strategies for Mitigation. *Digital Journalism*, 11, 1848-1867.
- Hidayat, R., & Rusadi, U. (2025). Ekonomi Politik Media Platform Lokal: Relasi Kuasa antara Pemerintah Daerah dan Media Online di Jawa Timur. *Scriptura: Jurnal Ilmu Komunikasi*, 15(1), 50-63.
- Jungherr, A., Rivero, G., & Gayo-Avello, D. (2020). *Retooling Politics: How Digital Media are Shaping Democracy*. Cambridge, New York, Melbourne: Cambridge University Press.
- Kalathil, S. (2020). The Evolution of Authoritarian Digital Influence: Grappling with the New Normal. *PRISM*, 9(1), 32-51.
- Katrakazas, P., & Papastergiou, S. (2024). A Stakeholder Needs Analysis in Cybersecurity: A Systematic Approach to Enhancing Digital Infrastructure Resilience. *Businesses*, 225-240.
- Kligler-Vilenchik, N., & Tenenboim, O. (2020). Sustained Journalist-Audience Reciprocity in a Meso News-Space: The Case of a Journalistic WhatsApp Group. *New Media & Society*, 22(2), 264-282.
- Kokshagina, O., Reinecke, P., & Karamasios, S. (2023). To Regulate or Not to Regulate: Unravelling Institutional Tussles Around the Regulation of Algorithmic Control of Digital Platforms. *Journal of Information Technology*, 38(2), 160-179.
- Kubo, T., Izawa, S., Tsuchiya, M., Ikeda, H., Miki, K., & Takahashi, M. (2018). Day to day Variations in Daily Rest Periods Between Working Days and Recovery from Fatigue Among Information Technology Workers: One-Month Observational Study Using a Fatigue App. *Journal of Occupational Health*, 394-403.
- Lee, M., & Butler, B. (2018). How are Information Deserts Created? A Theory of Local Information Landscapes. *Journal of Association for Indormation and Technology*, 70(2), 101-116.
- Lewis, S., Zamith, R., & Coddington, M. (2020). Online Harassment and Its Implications for the Journalist-Audience Relationship. *Digital Journalism*, 8(8), 1047-1067.
- Lindstedt, C., & Naurin, D. (2010). Transparency is not Enough: Making Transparency Effective in Reducing Corruption. *International Political Review*, 31(3), 301-322.
- Loeschner, I. (2017). The Technology Mismatch Paradox of Mobile Email Access: When Changed Norms of Responsiveness Meet Technology Undersupply. *The Information Society*, 33(3), 133-146.
- Masduki. (2021). Media Control in the Digital Politics of Indonesia. *Media and Communication* , 52-61.
- Miller, M., & Vaccari, C. (2020). Digital Threats to Democracy: Comparative Lessons and Possible Remedies. *The International Journal of Press/Politics*, 25(3), 333-356.
- Parcu, P. (2019). New Digital Threats to Media Pluralism in the Information Age. *Competition and Regulation in Network Industries*, 21(2), 91-109.
- Ramadhan, M., & Afala, L. (2024). *Politik Media, Media Politik: Pers, Rezim, dan Kemunduran Demokrasi* . Malang: Universitas Brawijaya Press.
- Raeijmaekers, D., & Maesele, P. (2015). Media, Pluralism, and Democracy: What's in a Name? *Media, Culture, & Society*, 37(7), 1042-1059.
- Reglitz, M. (2025). Internet and Communications. In J. Qorib, F., Kristie, E., & Hakim, L. (2-24). Analysis of the Use of Constructive Journalism in the News "Police

- Shoot Police" in the Online Media Tirto.id. *Kanal: Jurnal Ilmu Komunikasi*, 13(1), 21-30.
- Rianto, P. (2023). Sourveillance dan Bentuk-bentuk Baru Pengawasan Warga Negara dalam Demokrasi Digital di Indonesia. *Interaksi*, 230-249.
- Roberts, T., & Oosterom, M. (2024). Digital Authoritarianism: a Systematic Literature Review. *Information Technology for Development*, 1-25.
- Rosenfeld, L., Morville, P., & Arango, J. (2015). *Information Architecture For the Web and Beyond*. Beijing, Boston, Farnham, Sebastopol, Tokyo: O'Reilly.
- RSF. (2025). *Reporter Without Borders*. Retrieved from Reporter Without Borders: Indonesia: <https://rsf.org/en/country/indonesia>
- Ruzza, M., Tiozzo, B., Mantovani, C., D'Este, F., & Ravarotto, L. (2017). Designing the Information Architecture of a Complex Website: A Strategy Based on News Content and Faceted Classification. *International Journal of Information Management*, 37, 166-176.
- Salvo, P. (2025). Hacking and Information Disorder: The Weaponization of Leaking. *Critical Studies in Media Communication*, 42(1), 83-88.
- Siatitsa, I. (2020). Freedom of Assembly Under Attack: General and Indiscriminate Surveillance and Interference with Internet Communications. *International Review of the Red Cross*, 102(913), 181-198.
- Sinpeng, A. (2019). Digital Media, Political Authoritarianism, and Internet Control in Southeast Asia. *Media, Culture, & Society*, 42(1), 25-49.
- Slavtcheva-Perkova, V., Ramaprasad, J., Springer, N., Hughes, S., Hanitzsch, T., Hamada, B., . . . Steindl, N. (2023). Conceptualizing Journalists' Safety Around the Globe. *Digital Journalism*, 11(7), 1211-1229.
- Tomalty, & K. Woods, *The Routledge Handbook of the Philosophy of Human Rights*. New York: Routledge.
- Torre, L., Ramos, G., Noronha, M., & Jeronimo, P. (2024). Sourcing Local Information in News Deserts. *Journalism and Media*, 1228-1243.
- Tong, J. (2025). Growing Government Secrecy: How and Why Information Access has Become Increasingly Restricted in the UK. *Journalism Practice*, 1-19.
- Urkens, J., Harambam, J., & d'Haenens, L. (2024). Threat or Menace to Media Pluralism? A Framework to Assess Alternative Conspiracy Media in Today's Information Landscape. *Journalism*, 1-18.
- Valke, P., Sukosd, M., & Picard, R. (2015). *Media Pluralism and Diversity: Concepts, Risks and Global Trends*. New York: Palgrave Macmillan.
- Wendratama, E., Suci, P., Suriyani, L., & Masduki. (2024). *Laporan Riset Keamanan Perusahaan Media di Indonesia*. Jakarta: Aliansi Jurnalis Independen.
- Zviyita, I. &. (2024). Same Threats, Different Platforms? Female Journalists Experiences of Online Gender-Based Violence in Selected Newsrooms in Namibia. *Journalism*, 25(4), 779-799.

Conflict of Interest Statement: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest. Copyright © Mufti Nurlatifah. This is an open-access article distributed under the terms of the Creative Commons Attribution

License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.