Serangan Digital dan Perlindungan Jurnalis

R Manuhoro Setyowati

[1]*Universitas Semarang*
retnomanuhoro@usm.ac.id

ABSTRAK

Catatan akhir tahun 2023 dari Aliansi Jurnalis Independen menyatakan bahwa tren kekerasan terhadap jurnalis cenderung meningkat, terkhusus dalam serangan digital. Dampak serangan digital sangat mengganggu kerja jurnalis. Serangan digital juga menjadi salah satu indikasi adanya deligitimasi tugas pers sebagai pilar keempat demokrasi. Serangan digital tidak hanya menyasar ke media pewarta saja, namun juga pada personal jurnalisnya. Sementara itu perlindungan terhadap profesi ini juga mengalami posisi dilematis dengan kondisi yang belum tegak dan kuat serta menjamin keselamatannya dalam menjalankan tugas jurnalistiknya. Oleh karena itu, riset ini bertujuan mengungkapkan pengalaman para jurnalis terkait dengan serangan digital yang pernah dialaminya dan keterkaitannya dengan perlindungan profesi. Apa saja bentuk serangan digital, dan bagaimana cara mereka melindungi diri. Metode yang digunakan adalah kualitatif dengan pendekatan fenomenologi. Hasil temuan riset ini menunjukkan serangan yang pernah diterima adalah peretasan, doxing, D-Dos, dan Kekerasan Berbasis Gender Online (KBGO). Upaya perlindungan terhadap jurnalis dalam menghadapi serangan digital masih jauh dari optimal. Kelemahan ini disebabkan oleh belum adanya regulasi yang memadai, seperti yang terlihat pada Undang-Undang No. 40 Tahun 1999 tentang Pers yang belum secara rinci mengatur mengenai kekerasan berbasis digital. Perlindungan hukum yang masih terpaku pada Undang-Undang ITE juga belum cukup efektif dalam menanggapi kasus kekerasan terhadap jurnalis di ranah digital. Para informan dalam riset ini juga memaparkan kegelisahan sekaligus ketidakberdayaan mereka dalam perlindungan hukum terutama dalam kasus serangan digital.

Kata Kunci: Serangan Digital, Perlindungan Jurnalis, Keamanan Siber

ABSTRACT

The year-end report of the Independent Journalist Alliance in 2023 states that the trend of violence against journalists is on the rise, particularly in digital attacks. The impact of digital attacks significantly disrupts the work of journalists. Digital attacks also serve as an indication of the delegitimization of the press's role as the fourth pillar of democracy. Digital attacks not only target media outlets but also the personal lives of journalists. Meanwhile, protection for this profession faces a dilemma due to the current condition, which is not robust enough to ensure their safety in carrying out journalistic duties. Therefore, this research aims to reveal the experiences of journalists regarding digital attacks they have encountered and their connection to professional protection. The study explores the forms of digital attacks and the methods they employ for self-protection. The method used is qualitative with a phenomenological approach. The findings of this research indicate that the experienced attacks include hacking, doxing, DDoS, and Online Gender-Based Violence (OGBV). Efforts to protect journalists from digital attacks are far from optimal. This weakness is attributed to the lack of adequate regulations, particularly evident in Law No. 40 of 1999 on the Press, which does not comprehensively address digital violence. Legal protection relying on the Information and Electronic Transactions Law (ITE Law) is also deemed insufficient in responding to cases of violence against journalists in the digital realm. The informants in this study also express their anxiety and helplessness in legal protection, especially in cases of digital attacks.

Keywords: Digital Attacks, Journalist Protection, Cybersecurity

Pendahuluan

Menjelang Pemilu 2024, serangan digital terhadap jurnalis dikhawatirkan akan mengalami peningkatan. Kemungkinan besar jurnalis akan lebih banyak menerima bentuk intimidasi apalagi jika karya jurnalistiknya berseberangan dengan pandangan politik mayoritas. Kegiatan menakut-nakuti, mengancam secara langsung maupun tidak langsung ini seringkali juga muncul ketika jurnalis menayangkan berita yang mengemukakan pikiran kritis terhadap sebuah persoalan yang sedang mengemuka di publik. Contoh nyata yang terjadi belakangan ini adalah situs dan aplikasi Kompas.id yang diserang secara digital sehingga mengakibatkan berita Kompas sulit diakses dari kanal tersebut. Atas peristiwa ini, pihak Kompas resmi mengumumkan kekerasan digital ini melalui platform media sosial X mereka pada 15 Desember 2023 lalu. (Harian Kompas [@hariankompas], 2023)

Gambar 1. Pemberitahuan Harian Kompas melalui cuitan di media sosial X
Sumber : X @hariankompas, 15 Desember 2023

Laman Kompas.id diserang dengan cara “kebanjiran”, yakni masuknya traffic yang tidak wajar sehingga menyebabkan situs Kompas sama sekali tidak bisa diakses pada hari itu. Serangan digital tersebut muncul pasca dipublikasikannya hasil liputan investigasi mengenai judi online. Berdasarkan observasi dari peneliti, setidaknya terdapat 19 tulisan yang mengangkat tentang judi online dalam bentuk tulisan investigatif. (Media, t.t.) Kompas bahkan berani membuat judul berita yang sangat “lantang” dan menjadi headline

yaitu berita berjudul "WNI Kendalikan Judi Daring dari Kamboja". Penyerangan digital juga terjadi baru-baru ini pada media massa alternatif, yaitu Project Multatuli (PM). Situs PM pernah diserang pada saat PM memberitakan kasus pencabulan terhadap anak di bawah umur di kota Baubau, Sulawesi Tenggara. Sama persis dengan serangan yang diderita oleh Kompas, situs PM menjadi sulit diakses oleh publik.

Data dari Aliansi Jurnalis Independen (AJI) Indonesia mencatat sepanjang Januari 2023 hingga Desember 2023, telah terjadi 13 serangan digital yang dialami media massa dan jurnalis. Tak hanya menyasar media massa saja, penyerangan digital juga terjadi pada jurnalis secara langsung, sebagaimana yang dialami oleh Ketua Umum Aliansi Jurnalis Independen (AJI) Indonesia, Sasmito Madrim. Aplikasi *WhatsAppnya* diretas, dan secara tiba-tiba ia menerima notifikasi bahwa nomornya telah didaftarkan pada perangkat lain. Akibatnya, fatal. Nomor personalnya sama sekali tidak bisa menerima panggilan dan non aktif mendadak. Demikian juga dengan akun-akun media sosialnya, tiba-tiba telah berubah foto profil menjadi profil porno. Peretasan itu ternyata berkesinambungan, foto Sasmito digunakan untuk menyebarkan berita bohong/ hoax tentang berbagai issue yang mencolok, seperti dukungan pembubaran FPI dan dukungan agar pemerintah segera membangun Bendungan Bener di Purworejo Jawa Tengah. Realitas yang tidak hanya dialami oleh segelintir jurnalis ini membuat Aliansi Jurnalis Independen menyatakan bahwa ini adalah status darurat. (*Jurnalis Semakin Rentan Diserang di Ranah Digital – DW – 03.05.2022*, t.t.)

Tak dapat dipungkiri, aksi-aksi serangan digital yang dilakukan oleh berbagai oknum dengan motivasi utama mengacaukan dan merusak kepercayaan ini berdampak secara psikologis kepada jurnalis sebagai pekerja media dan juga berpotensi mempengaruhi kredibilitas media massa yang diserang. Jurnalis bisa saja terserang paranoid, ketakutan akut, dan kecemasan hingga dapat mempengaruhi kesehatan fisiknya. Serangan digital dapat mengancam privasi dan keamanan personal. Hal ini dapat menyebabkan rasa tidak aman, kekhawatiran dan dampak psikologis jangka panjang dan berujung pada ketidak percayaan pada teknologi (Poetri AL-Viany, 2023). Penyerangan digital tidak hanya terjadi di kota metropolitan saja. Serangan siber menyasar siapa saja dan dimana saja, termasuk jurnalis di Jawa Tengah, kususnya di Kota Semarang. Berangkat dari latar belakang tersebut, maka riset ini bertujuan untuk mengetahui pengalaman dari para jurnalis di Semarang yang pernah mendapatkan serangan digital, apa saja jenisnya dan bagaimana mereka dapat melindungi dirinya dalam melanjutkan tugas jurnalistiknya. Tinjauan literatur dalam riset ini adalah penelitian Cynthia Rahmawati dengan judul Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era

Revolusi Industri 4.0 pada tahun 2020. Risetnya mengulas mengenai tantangan keamanan siber dari sudut pandang keberlangsungan bisnis yang aman dan berkelanjutan. (Rahmawati, 2020). Selanjutnya riset dari Ido Prijana Hadi tahun 2017 tentang Tantangan Etika dan Regulasi Media Digital. Riset ini mengulas mengenai etika jurnalisme dan dinamikanya dalam dunia digital, namun belum membahas mengenai perkembangan digital attack atau serangan digital serta kompleksitas perlindungan bagi jurnalis di Indonesia.(Hadi, 2017) Berdasarkan dua riset terdahulu itulah, maka penulis merasa perlu melanjutkan riset tersebut dengan memperkaya dengan pengalaman keseharian jurnalis di era digital dan tantangannya dalam menghadapi serangan digital. Sebagaimana yang pernah dikemukakan oleh Marshall McLuhan penemu teori "desa global", masa kini adalah bentuk nyata dari perpanjangan dari panca indera kita. Dunia semakin mengecil dan semuanya tersambung melalui internet. Terjadi perubahan perubahan budaya, dan komunikasi manusia akan membentuk eksistensi kehidupannya. Selain menggunakan Undang-undang No 40 tahun 1999 tentang Pers, peneliti juga menggunakan konsep hak-hak digital dan perlindungan jurnalis.(Juniarto, 2021)

Metode Penelitian

Penelitian ini menggunakan metode kualitatif yang dijelaskan secara deskriptif dengan pendekatan fenomenologi. (Hasbiansyah, 2005)Pendekatan ini digunakan untuk meneliti pengalaman hidup manusia demi mendapatkan pemahaman tentang "kebenaran" esensial dari pengalaman hidup. Data diperoleh dan dikaji dengan cara yang mendalam (Sudarsyah, 2013) Paradigma yang digunakan adalah paradigma konstruktivis dimana paradigma ini memahami suatu realitas sosial tidak bisa digeneralisasikan begitu saja. Teknik analisis dan interpretasi data yang bersifat deskriptif kemudian disajikan dengan menggunakan bahasa yang khas serta bukan bertujuan untuk menggeneralisasi hasil. Tiap kasus dilihat sebagai sebagai sesuatu yang memiliki kekhasan tersendiri. Adapun yang menjadi subjek penelitian ini adalah para jurnalis media siber/ media online yang bekerja untuk berbagai media massa di Jawa Tengah. Subyek penelitian dipilih dengan menggunakan kriteria (1) Bekerja di media online selama lebih dari lima tahun, (2) jurnalis yang memiliki pengalaman khusus terkait dengan perlindungan profesi dan serangan digital, (3) jurnalis yang lingkup kerjanya meliputi seluruh wilayah Jawa Tengah. Kriteria pemilihan informan ini tidak melihat jenis kelamin, sehingga jurnalis perempuan dan jurnalis laki-laki tidak secara khusus dibedakan materi pertanyaannya. Para jurnalis ini kemudian menjadi sumber data primer dengan teknik pengumpulan data berupa wawancara mendalam dan observasi. Sebagai bagian dari tahap penelitian, data sekunder dilakukan penulis melalui pengumpulan dokumen publik seperti koran, makalah, laporan

kantor. Pengumpulan data juga menggunakan dokumentasi dokumen privat yaitu *e-mail* tentang berbagi pengalaman selama menjadi jurnalis media online. Semua data dari dokumentasi tersebut kemudia ditelaah secara intens sehingga dapat mendukung data primer.

Teknik analisis data diawali dengan mentranskrip hasil wawancara, reduksi data, analisis, interpretasi data dan triangulasi. Dari hasil analisis data yang kemudian dapat ditarik kesimpulan. Dalam riset ini penulis langsung membagi tema menjadi dua (2) bagian yakni pengalaman serangan digital secara personal dan institusional, perlindungan jurnalis dan hak di era digital.

Hasil dan Pembahasan

Peneliti mewancarai sepuluh (10) jurnalis yang sesuai dengan kriteria dimana para informan diwawancarai secara personal. Setiap informan menghasilkan data yang tidak sama, sesuai dengan pengalaman yang mereka dapatkan terkait dengan serangan digital dan perlindungan jurnalis. Dari wawancara dengan sepuluh informan, tema mengenai serangan digital secara personal dan institusional dapat digambarkan melalui diagram di bawah ini.

Gambar 2 Diagram presentase serangan digital terhadap jurnalis

Munculnya kategori terancam dalam diagram tersebut, didapatkan dari data transkrip wawancara informan yang menyatakan bahwa ia secara langsung memang belum pernah mengalami serangan digital, namun pengancaman untuk peretasan akun media sosialnya pernah didapatkan selama menjalankan tugas jurnalistiknya. Informan (1) seorang jurnalis perempuan yang bekerja untuk media online alternatif.

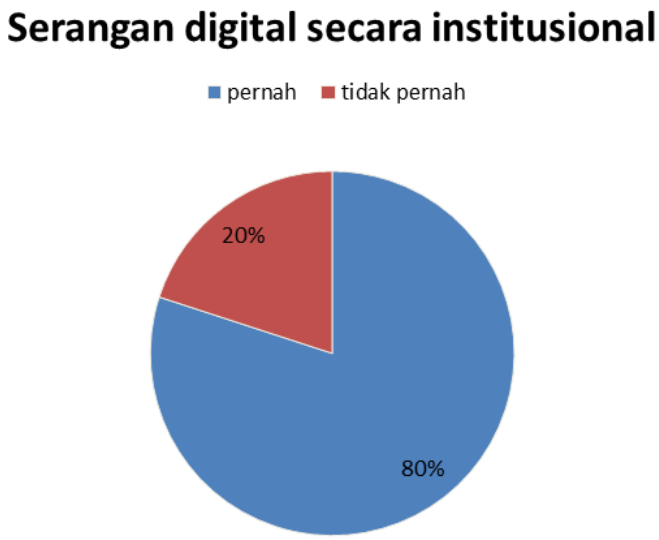
"Ya awalnya saya anggap itu sebagai candaan saja, tapi setiap kali narasumber itu merasa tidak nyaman dengan materi pertanyaan saya, ia mengulang pernyataannya bahwa suatu saat nanti ia akan meretas dan mengganti akun Instagram saya secara diam-diam."

Informan (5) seorang jurnalis yang bekerja untuk media online lokal menyatakan juga pernah terancam, meski akun media sosial dan gawainya masih dalam keadaan baik-baik saja. Informan tersebut menyatakan ia menerima ancaman secara verbal, sesaat ia bertemu dengan pejabat salah satu instansi yang membaca berita unggahannya tentang penataan kota.

"Mas, kalau tulisanmu nggak sesuai dengan kenyataan, hati-hati lo Mas, kamu selamat di darat tapi bisa jadi nggak selamat di medsos."

Ucapan verbal bernada mengancam masuk dalam kategori ancaman, karena meski belum terjadi, jurnalis tetap sempat diliputi rasa khawatir dan tidak nyaman dalam menjalankan tugasnya. Dua informan lainnya juga menyatakan hal serupa, dengan kisah dan kejadian yang beragam diman sebagian besar mendapatkan ancaman secara verbal secara langsung namun selalu berkaitan dengan keutuhan dan keselamatan akun media sosial jurnalis secara personal.

Data primer melalui wawancara langsung dengan informan secara personal dan mendalam juga mendapati kenyataan bahwa hampir semua informan menyatakan bahwa perusahaan media online tempatnya bekerja pernah menerima serangan digital dalam berbagai bentuk. Berikut adalah gambaran diagram serangan digital secara institusional.

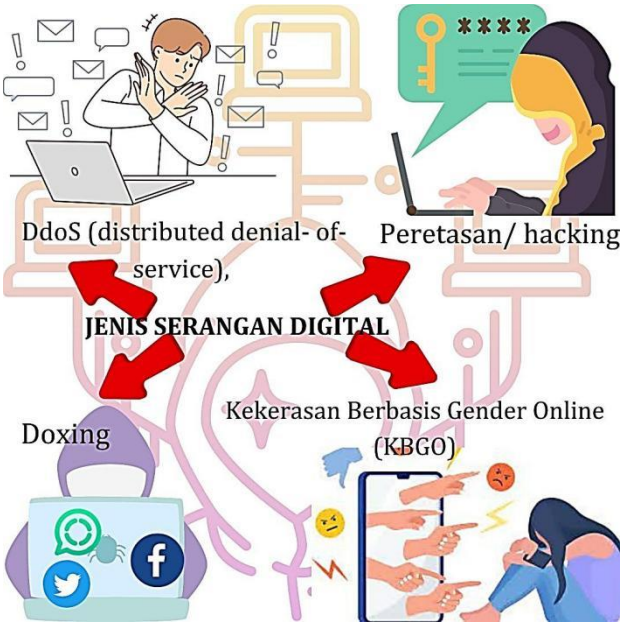


Gambar 3 Diagram presentase serangan digital kepada perusahaan media online

Jenis serangan digital yang pernah diterima jurnalis

Berpijak dari analisis data yang sudah ditempuh, maka peneliti mencatat pernyataan-pernyataan dari pengalaman nyata informan selama menjalankan tugas

jurnalistiknya. Peneliti juga menanyai apakah pernah menerima serangan siber selama menjalankan tugas sebagai jurnalis dijawab oleh informan dengan pengalaman yang bervariasi, namun sebagian besar menyatakan pernah menerima serangan dan ancaman siber. Berikut adalah visualisasi jenis serangan digital yang pernah diterima oleh jurnalis media online di Semarang.



Gambar 4 visualisasi serangan digital yang dialami oleh jurnalis di Semarang

Berdasarkan Panduan Keamanan Digital Bagi Jurnalis, yang diterbitkan oleh Aliansi Jurnalis Independen Indonesia tahun 2022, munculnya serangan digital pada prinsipnya selalu diawali dengan ancaman digital. Ancaman digital adalah tindakan kejahatan yang berupaya merusak data, mencuri data, atau mengganggu kehidupan di dunia maya secara umum. (Marsiela & Suriyani, 2022)Di era digital, jurnalis memiliki kerentanan ganda menerima ancaman digital, sebagai individual maupun karena risiko dari pekerjaan. Hal ini karena kerja-kerja jurnalis saat ini menggunakan berbagai perangkat teknologi yang terhubung dengan internet, baik dalam berkomunikasi, menggali data, serta mempublikasikan laporannya. Kekerasan digital bisa menjadi pintu atau bersamaan atas terjadinya bentuk-bentuk kekerasan fisik. Berikut ini adalah bentuk-bentuk ancaman digital yang bisa menyerang jurnalis(Marsiela & Suriyani, 2022). Empat (4) dari tujuh (7) ancaman digital tersebut telah menjadi serangan digital bagi jurnalis media online di Semarang.

1. Malware

Malicious software (malware) adalah istilah yang merujuk pada program atau file yang

dapat menimbulkan risiko bagi pengguna komputer atau ponsel. Varian-varian malware mencakup virus, worm, trojan horse, dan spyware. Jenis perangkat lunak berbahaya ini dapat melakukan berbagai fungsi, termasuk pencurian, enkripsi, atau penghapusan data, perubahan atau pengambilalihan fungsi komputasi inti, serta pemantauan aktivitas komputer atau ponsel pengguna tanpa izin mereka.

2. Phishing

Phishing merupakan bentuk kejahatan siber yang melibatkan pendekatan target melalui email, telepon, atau pesan teks oleh pelaku yang berpura-pura sebagai entitas resmi. Maksudnya adalah untuk mengelabui individu agar memberikan data sensitif seperti informasi pribadi, rincian kartu kredit, dan informasi perbankan, serta kata sandi. Data tersebut kemudian dapat digunakan untuk mengakses akun-akun krusial, berpotensi menyebabkan pencurian identitas dan kerugian finansial.

3. Peretasan

Hacking, atau peretasan, merujuk pada tindakan mengakses perangkat seperti laptop atau ponsel, akun, dan jaringan tanpa sepengetahuan pemiliknya. Motivasinya dapat bervariasi mulai dari mencari keuntungan finansial, merusak reputasi, hingga menyebabkan ketakutan. Peretasan ini seringkali terkait dengan tingkat keamanan digital yang kurang memadai pada perangkat atau akun individu.

Berikut kutipan salah satu informan nomor 6 yang menyatakan ia pernah mendapatkan ancaman ganda yaitu hilangnya channel YouTube milik kantor yang dibarengi dengan peretasan akun WhatsApp nya (WA).

> *"Waktu liputan isu lingkungan di pulau kecil yang ada di luar kota Semarang dapat WA dari orang tak dikenal. Tanya mau ngapain aja di sana, jangan macam-macam dan harus lapor aktivitas yang saya lakukan melalui WA nomor itu. Entah dia dapat nomor saya darimana, dan setelah itu WA saya menjadi non aktif mendadak."*

Tak seberapa lama dari matinya aplikasi chat itu, ia mendapat kabar bahwa channel YouTube milik kantor tiba-tiba lenyap, padahal channel YouTube itu sudah mempunyai banyak subcriber. Peretasan akun chat atau hacking juga menjelma menjadi serangan teror dalam bentuk spam pesan maupun panggilan bertubi-tubi di gawainya.

> *"Dulu pernah pas selesai menghadiri acara, mendadak puluhan brondongan message meluncur menuhi inbox, pesan yang nggak jelas semua. Semuanya nomor yang tidak saya kenal, bikin jengkel karena mengganggu kerjaan, hape jadi bunyi terus."*

4. Doxing

Doxing adalah tindakan mengumpulkan dan menyebarluaskan informasi pribadi seseorang secara daring dengan maksud merendahkan atau mengundang pelecehan terhadap individu tersebut. Data pribadi yang diungkapkan mencakup berbagai hal, mulai dari foto, nomor telepon, alamat rumah, nomor kartu kredit, hingga sejarah

dukungan politik. Penjahat doxing menggunakan informasi pribadi yang dapat diakses di internet untuk membalas dendam dengan menyebarkan narasi yang mengandung fitnah dan kebencian.

Tentang serangan digital jenis doxing, informan 8 menceritakan pengalamannya yang berujung pada rasa takut dan ketidaknyamanan karena informasi pribadinya disebar ke semua jejaring kerja dan lingkar pergaulannya.

> *"Ada laporan dari kawan kerja saya yang curiga dengan kiriman seseorang di wall Facebook yang beredar. Tulisan itu sangat mengerucut ke sosok saya karena alamat rumah, nama Bapak saya hingga pohon peneduh di sekitar rumah saya sama persisnya dengan narasi yang diunggah, tapi narasi yang dipajang itu memuat kebencian terhadap suatu ras tertentu."*

Akibat doxing itu, informan 8 merasa sangat terganggu karena komentar netizen yang langsung menyudutkannya dan menuduh sangat rasis.

> *"Saya mau lapor ke Polisi, tapi sudah males duluan karena malah di gas light. Akhirnya ya sudah, tidak bisa ngapa-ngapain selain membuat klarifikasi bahwa itu saya kena doxing"*

5. Impersonating

Pemalsuan akun, atau impersonating, terjadi ketika seseorang membuat profil palsu, situs web, atau email yang menggunakan nama atau identitas Anda, sehingga menyerupai akun asli Anda. Tujuan dari impersonating ini dapat bervariasi, mulai dari penciptaan kampanye yang merugikan, penyebaran informasi yang menyesatkan, rekayasa sosial, hingga pencurian identitas untuk menciptakan kegaduhan di media sosial, mengurangi tingkat kepercayaan, dan melibatkan pelanggaran data yang dapat berdampak pada reputasi, terutama bagi seorang jurnalis.

6. Pelecehan

Pelecehan daring (online harassment) adalah tindakan di dunia maya yang memiliki sifat mengintimidasi, mengancam, dan mencemarkan nama baik seseorang secara online. Bentuknya dapat berupa penyebaran pernyataan online yang merusak reputasi dengan cara memfitnah atau merendahkan, pembuatan serta penyebaran informasi palsu atau disinformasi untuk tujuan mencemarkan nama baik, penyampaian pernyataan cabul, pengiriman materi yang bersifat ofensif atau cabul, serta penyebaran pesan intim seksual (baik berupa foto atau video secara daring) tanpa izin seseorang.

7. Kekerasan Berbasis Gender Online

Jurnalis perempuan atau yang bergender minoritas (LGBT), rentan menjadi korban kekerasan berbasis gender online (KBGO). Kekerasan Berbasis Gender Online (KBGO) pernah dialami oleh informan 2. Ia mengungkapkan pengalaman pahitnya yang membuatnya sangat geram.

> *"Itu pelakunya justru dari kolega jurnalis, kenal lama. Ketika ngobrol di WA tiba-tiba kirim stiker porno gambar orang berhubungan intim. Kan bikin risih, ya akhirnya saya biarkan saja meski kayak terintimidasi."*

Bentuk-bentuk ancaman digital terhadap jurnalis tentunya semakin kompleks dan berkembang. Seperti Cyber Amok, Spam Calls, hingga Ddos Attack yang dulunya hanya menyasar pihak-pihak tertentu saja. Sama halnya dengan yang terjadi di kalangan jurnalis media online di Semarang, serangan digital ditujukan tidak hanya secara tunggal, namun bisa jadi menjadi sasaran ganda yakni secara institusional maupun personal sekaligus. Sementara itu untuk jenis serangan D-Dos yang terjadi, dialami oleh informan 10 dimana websitenya pernah mengalami kerusakan sementara dan tidak dapat diakses. Tidak tanggung-tanggung kejadian itu bahkan terulang berkali-kali karena para pengirim serangan berada di luar negeri, dan susah dilacak.

> *"Pernah beberapa kali kena website down sampai 3-4 hari. Ternyata dibajak dari dalam bahkan dari luar negeri. Kami tidak paham di IT bilang harus negosiasi ke mereka agar website bisa diambil alih. Walaupun bisa kembali lagi tapi bentuknya jadi berantakan, acak adul sehingga kami harus menata ulang kembali."*

Sama halnya dengan informan 10, informan yang lain mengaku YouTube milik perusahaan medianya juga diserang. Penggunaan kanal YouTube era kini menjadi semacam opsi wajib bagi media online untuk meresponi era konvergensi media.

> *"Youtube official sering diserang. Entah sekadar iseng dari random hacker yang tidak mudah dilacak karena penyerang mempunyai aplikasi mengkamuflase."*

Southeast Asia Freedom of Expression Network/SAFEnet) adalah salah satu organisasi regional yang fokus pada usaha memperjuangkan hak-hak digital di wilayah Asia Tenggara. SAFENet telah mengidentifikasikan jenis serangan digital yang digolongkan ke dalam dua kategori utama, yaitu serangan yang bersifat kasar seperti peretasan, penyadapan, dan serangan DDoS (Distributed Denial of Service). Serangan-serangan tersebut melibatkan pemanfaatan teknologi dan keahlian khusus. (Juniarto, 2021)

Selain itu, terdapat serangan yang bersifat lebih halus yang bertujuan untuk menciptakan intimidasi psikologis terhadap korban atau merusak kredibilitas mereka di mata publik. Serangan ini terjadi secara terbuka melalui media sosial, baik dengan menggunakan profil anonim maupun nyata oleh pelaku. Contoh serangan jenis ini mencakup penyebaran informasi pribadi tanpa izin (doxing), pembuatan akun palsu, serta serangan dengan cara memberikan komentar atau unggahan yang merugikan (trolling). Umumnya, serangan halus semacam ini dilakukan oleh tim yang berkoordinasi.

Serangan digital yang dialami oleh jurnalis di Semarang, jika dikelompokkan menurut kategorisasi yang disusun oleh Southeast Asia Freedom of Expressi on Network (SAFEnet) maka akan menjadi seperti tabel berikut ini.

Tabel 1. Dua kategori serangan digital yang dialami oleh jurnalis Semarang

Jenis serangan digital yang dialami jurnalis media online di Semarang		
Halus	Kasar	ceklist
	Peretasan	√
	DDoS (Distributed Denial of Service).	√
Doxing		√
Trolling/ sexting		KBGO√

Sumber : olah data peneliti

Berdasarkan data yang dirangkum oleh peneliti, menunjukkan bahwa jurnalis media online di Semarang setidaknya telah mengalami lebih dari separuh jumlah kategori serangan digital, yang dikuatkan dengan pengalaman-pengalaman dari informan tentang kejadian serangan siber selama melakukan tugas jurnalistiknya. Temuan lainnya dari data yang terkumpul adalah tidak semua jurnalis perempuan dalam wawancara mendalam ini mau melaporkan tindakan Kekerasan Berbasis Gender Online kepada atasannya, atau kepada perusahaan media massa tempatnya bekerja. Pelaku KBGO selain dari narasumber berita, juga berasal dari kolega lama. Menurut Aliansi Jurnalis Independen yang selama ini sangat peduli dengan ruang aman bagi jurnalis di era siber menyatakan bahwa fenomena tersebut sangat mengkhawatirkan. Walaupun jurnalis perempuan sering menjadi korban pelecehan daring, mereka seringkali menganggapnya sebagai sesuatu yang "umum" atau biasa. Padahal, salah satu tujuan utama dari pelaku Kekerasan Gender Berbasis Online (KGBO) adalah untuk mengekang kebebasan suara jurnalis. (Marsiela, 2022). Ini juga bertentangan dengan azas kebebasan pers. (Marsiela & Suriyani, 2022)

Perlindungan keamanan dari serangan digital bagi jurnalis

Pada bagian ini, informan memberikan pengalamannya yang terkait dengan belum adanya perlindungan dari perusahaan media. Perlindungan yang dimaksud, adalah bagaimana membekali para jurnalisnya dan bagaimana perusahaan media melindungi jurnalisnya jika serangan digital terjadi. Informan 5 menyatakan beberapa kasus peretasan akun personal dari jurnalis hanya menjadi sebuah cerita biasa tanpa solusi.

> *"Sejauh ini belum pernah dilakukan pembekalan secara khusus untuk keamanan dan perlindungan hak digital jurnalis. Kalo sudah kejadian ya paling berhenti di kantin alias jadi obrolan curhat dan sharing pengalaman saja buat nyari solusinya."*

Apabila pimpinan atau penanggung jawab redaksi mengetahui bahwa anak buahnya mengalami kasus peretasan, doxing ataupun serangan digital lainnya, juga belum ditemukan adanya garis tegas yang bersifat membantu bawahannya. Pembicaraan mengenai langkah pengamanan personal dari serangan siber juga minim.

> *"Seperti autopilot saja, dianggap kudu mudeng sendiri, kalo ada kejadian ya seolah tutup mata."*

Perlindungan dari pimpinan redaksi atau perusahaan media terhadap jurnalisnya bisa dikatakan masih sangat kurang karena tidak semua perusahaan media memberikan panduan keselamatan digital untuk mendukung peliputan yang aman. Informan 3 malah mempertanyakan kesungguhan negara dalam campur tangan penanganan kasus D-Dos yang menimpa website "Narasi News", "Konde" dan Project Multatuli. Ada semacam ketakutan sekaligus ketidakberdayaan jurnalis dalam menghadapi serangan digital ini.

> *" Lama-lama sikap skeptis saya menjadi galau tanpa arah karena ada rasa tidak aman ketika kirim berita dan cari berita karena semuanya kan pake teknologi."*

Jurnalis sadar bahwa pihak perusahaan media belum melindungi pekerja medianya. Meski demikian, kenyataan ini tidak juga membuat jurnalis memiliki kesadaran diri sendiri akan keamanan dan perlindungan digital

> *"Saya menyadari kadang-kadang saya abai dengan pengamanan dan perlindungan diri sendiri. Padahal tanpa disadari aktifitas harian kita terbuka banyak peluang kejahatan digital yang justru dimulai dari kita sendiri."*

Sejauh ini, perlindungan dari perusahaan media masih diberikan kepada perangkat kerja saja dalam hal ini media itu sendiri. Perusahaan media bahkan baru bergerak pasca terjadinya serangan digital.

> *"Kami ini masih media kecil. Backup website sudah sih, meski dulu pernah kehilangan konten dan apesnya bagian maintenance khusus IT juga tidak tahu jalan keluarnya. Pengalaman pahit akhirnya membuat kami sekarang lebih peduli dengan perlindungan pada website dan diberi proteksi tambahan."*

Akhirnya, upaya perlindungan terhadap jurnalis dalam menghadapi tantangan dan serangan siber masih mengalami penundaan. Kehati-hatian mereka belum dapat dijamin karena Undang-Undang No. 40 Tahun 1999 tentang Pers belum secara rinci mengatur mengenai kekerasan berbasis digital. (Dewan, 1999). Oleh karena itu, saatnya bagi pemerintah, Dewan Pers, dan pihak terkait untuk bersama-sama merumuskan regulasi yang tepat, sehingga ke depannya tidak ada lagi ancaman kekerasan digital terhadap profesi jurnalis di Indonesia. Hingga saat ini, satu-satunya acuan hukum terkait kekerasan digital adalah Undang-Undang ITE, namun pelaksanaannya masih terbatas dalam menangani kasus-kasus kekerasan terhadap jurnalis di ranah digital. Dari perspektif hukum, instrumen perlindungan terhadap pers masih terpaku pada Undang-Undang Nomor 40 Tahun 1999, sehingga belum sepenuhnya mencakup perlindungan terhadap pers dalam dunia digital. Hal ini mengakibatkan ketidaksesuaian dengan perkembangan media daring, komunitas, dan jurnalisme warga yang memanfaatkan teknologi digital. (Eni, 2022) Penelitian di Amerika menunjukkan bahwa ketika politisi mengadopsi sikap anti-media, jurnalis menjadi lebih rentan terhadap tindakan kekerasan (*Anti-Media Discourse*

and Violence Against Journalists: Evidence From Chávez's Venezuela - Kyong Mazzaro, 2023, t.t.). Dengan kata lain, pengalaman berbagai jurnalis terkait kekerasan dan serangan digital menjadi tantangan dalam menjalankan peran dan fungsi media atau pers di masyarakat, serta menghambat perkembangan demokrasi di Indonesia. Riset Indeks Keselamatan Jurnalis yang dilakukan oleh AJI Indonesia pada tahun 2022 mengungkapkan bahwa mayoritas responden menyatakan kurangnya dukungan keamanan dari tempat kerja, dengan beberapa indikator mencakup minimnya pelatihan keamanan dari perusahaan media dan kurangnya protokol keamanan yang khusus melibatkan jurnalis perempuan untuk melindungi mereka dari Kekerasan Berbasis Gender Online. (Muryanto & Tanjung, 2022). Perlindungan terhadap jurnalis perempuan saat ini masih banyak mengandalkan upaya perorangan untuk menghindari ancaman Kekerasan Berbasis Gender Online. Kelemahan perlindungan dari pemerintah terhadap profesi jurnalis juga disertai dengan masih tingginya impunitas terhadap pelaku kejahatan terhadap jurnalis.

Simpulan dan saran

Simpulan

Kesimpulan dari data yang telah disajikan menunjukkan bahwa jurnalis media online di Semarang menghadapi serangan digital yang bervariasi, termasuk peretasan, doxing, Dos, dan Kekerasan Berbasis Gender Online. Serangan tersebut tidak hanya ditujukan secara individu, melainkan seringkali menjadi sasaran ganda, baik secara institusional maupun personal. Analisis data menunjukkan bahwa lebih dari separuh jumlah kategori serangan digital telah dialami oleh jurnalis di wilayah tersebut. Selain itu, temuan menarik lainnya adalah bahwa tidak semua jurnalis perempuan mau melaporkan tindakan Kekerasan Berbasis Gender Online kepada atasan atau perusahaan tempat mereka bekerja. Pelaku kekerasan jenis ini tidak hanya berasal dari narasumber berita, tetapi juga dari kolega lama, menunjukkan kompleksitas dan beragamnya sumber ancaman. Terlepas dari seringnya jurnalis perempuan menjadi korban pelecehan daring, mereka cenderung menganggapnya sebagai sesuatu yang "umum" atau biasa. Hal ini menunjukkan tingkat kelangkaan kesadaran akan seriusnya dampak kekerasan digital terhadap profesi dan kesejahteraan jurnalis.

Upaya perlindungan terhadap jurnalis dalam menghadapi tantangan dan serangan siber masih jauh dari optimal. Kelemahan ini disebabkan oleh belum adanya regulasi yang memadai, seperti yang terlihat pada Undang-Undang No. 40 Tahun 1999 tentang Pers yang belum secara rinci mengatur mengenai kekerasan berbasis digital. Perlindungan hukum yang masih terpaku pada Undang-Undang ITE juga belum cukup efektif dalam menanggapi kasus kekerasan terhadap jurnalis di ranah digital. Selain itu, jurnalis rentan terhadap serangan digital karena

kurangnya penerapan protokol keamanan digital. Perlindungan keamanan digital dari perusahaan media juga masih lemah dan belum menjadi prioritas utama, terutama karena keterbatasan sumber daya. Oleh karena itu, perlu adanya kolaborasi antara pemerintah, Dewan Pers, dan pihak terkait untuk merumuskan regulasi yang tepat, meningkatkan kesadaran akan keamanan digital, dan menghadirkan perlindungan yang lebih kuat bagi jurnalis, sehingga mereka dapat menjalankan tugas mereka tanpa terancam oleh serangan digital.

Saran

Bagi jurnalis, saran penulis adalah menekankan pentingnya perlindungan data pribadi bagi jurnalis. Sealin itu, masih diperlukan literasi digital bagi perusahaan media dan jurnalis sebagai pekerja media. Idealnya jurnalis juga berupaya melakukan peningkatan kapasitasnya melalui training digital safety and security sehingga memperoleh pemahaman demi perlindungan dirinya sendiri. Bagi peneliti selanjutnya dapat mengembangkan riset ini secara kuantitatif atau metode gabungan dengan area cakupan yang lebih luas, agar didapatkan hasil secara lebih komprehensif.

Ucapan terimakasih

Terimakasih kepada jurnalis media online Semarang yang menjadi informan riset.

Daftar Rujukan

Anti-Media Discourse and Violence Against Journalists: Evidence From Chávez's Venezuela—Kyong Mazzaro, 2023. (t.t.). Diambil 31 Desember 2023, dari https://journals.sagepub.com/doi/abs/10.1177/19401612211047198

Dewan, P. (1999). *Undang- Undang Republik Indonesia Nomor 40 Tahun 1999 Tentang Pers*. Dewan Pers.

Eni, M. (2022). *Idealisme Jurnalis & Inovasi Model Bisnis Industri Media.* LP3M LSPR Publishing.

Hadi, I. P. (2017, Mei 15). *Tantangan Etika dan Regulasi Media Digital (REVISI)* [PeerReviewed]. Tantangan Etika dan Regulasi Media Digital (REVISI); Aspikom Korwil Jatim dan Buku Litera. https://repository.petra.ac.id/18518/-

Harian Kompas [@hariankompas]. (2023, Desember 15). *Saat ini, laman dan aplikasi http://Kompas.id sedang mengalami gangguan. Ini terjadi setelah kami memublikasikan seri liputan investigasi judi online. Kami sedang berupaya mengatasinya. Kami akan tetap menghadirkan jurnalisme mencerahkan. Https://t.co/zzfQrSgOfz* [Tweet]. Twitter. https://twitter.com/hariankompas/status/1735506231723450565

Hasbiansyah, O. (2005). *Pendekatan Fenomenologi: Pengantar Praktik Penelitian dalam Ilmu Sosial dan Komunikasi*.

Juniarto, D. (2021). *Laporan Situasi Hak- Hak Digital Indonesia 2020*. Southeast Asia Freedom of Expression Network (SAFEnet).

Jurnalis Semakin Rentan Diserang di Ranah Digital – DW – 03.05.2022. (t.t.). Diambil 31 Desember 2023, dari https://www.dw.com/id/jurnalis-rentan-diserang-di-ranah-digital/a-61659114

Marsiela, A., & Suriyani, L. D. (2022). *KEAMANAN DIGITAL UNTUK JURNALIS*.

Media, K. C. (t.t.). *Berita Harian Judi Online Terbaru Hari Ini*. KOMPAS.com. Diambil 31 Desember 2023, dari https://www.kompas.com/tag/judi-online

Muryanto, B., & Tanjung, E. (2022). *INDEKS KESELAMATAN JURNALIS 2022*. Aliansi Jurnalis Independen Indonesia (AJI INDONESIA).

Poetri AL-Viany, M. (2023). *Psikologi Siber: Konsep dan Strategi Penanganan Masalah Perilaku Manusia di Era Digital*. Get Press Indonesia.

Rahmawati, C. (2020). Tantangan Dan Ancaman Keamanan Siber Indonesia Di Era Revolusi Industri 4.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *2*, 299–306.

Sudarsyah. (2013). *Kerangka Analisis Data Fenomenologi (contoh analisis teks sebuah catatan harian)*.