Tantangan Kerja Jurnalis Dalam Keamanan Siber

R Manuhoro Setyowati [1] Citra Safira [2] , Sinta Pramucitra [3]

[1]*Universitas Semarang*

retnomanuhoro@usm.ac.id, citrasafira@usm.ac.id, sinta@usm.ac.id

ABSTRAK

Selain sebagai pilar keempat demokrasi, jurnalis idealnya juga membangun kesadaran masyarakat mengenai keamanan siber. Apalagi kerja jurnalistik saat ini juga berada dalam ranah online. Hal ini penting dilakukan, karena beberapa kasus yang terkait dengan keamanan siber akhirnya mengganggu kerja jurnalis, seperti serangan DDoS yang menyerang infrastruktur jaringan menggunakan teknologi digital. Jurnalis semakin menghadapi tantangan yang kompleks karena belum semuanya memahami pentingnya keamanan siber saat menjalankan tugasnya. Penelitian ini mengeksplorasi tantangan jurnalis dalam kerja jurnalistik mereka, juga mencatat pengalaman nyata bagaimana antisipasi dan strategi yang dilakukan. Metode yang digunakan adalah kualitatif dengan pendekatan Interpretative Phenomenological Analysis (IPA). Temuan riset ini menyatakan tantangan terbesar justru muncul dari dalam diri jurnalis sendiri yang tidak semuanya sudah melek keamanan siber karena merasa belum perlu pengamanan padahal potensi serangan baik secara institusi maupun personal dapat terjadi kapan saja. Terlebih lagi, dari pihak perusahaan media juga tidak melakukan upaya preventif, dan bertindak jika sudah terjadi serangan siber. Dua hal ini menjadi tantangan yang harus dihadapi dan diharapkan dapat berubah demi keamanan siber di lingkungan kerja dan mendukung kerja jurnalistik yang aman.

Kata Kunci: Serangan Digital, Tantangan Jurnalis, Keamanan Siber

ABSTRACT

Apart from being the fourth pillar of democracy, journalists should ideally also build public awareness about cyber security. Moreover, journalistic work is currently also in the online realm. This is important to do, because some cases related to cybersecurity end up disrupting the work of journalists, such as DDoS attacks that attack network infrastructure using digital technology. Journalists are increasingly facing complex challenges because not all of them understand the importance of cybersecurity when carrying out their duties. This research explores the challenges journalists face in their journalistic work, as well as recording real-life experiences of anticipation and strategies. The method used is qualitative with an Interpretative Phenomenological Analysis (IPA) approach. The findings of this research state that the biggest challenge arises from journalists themselves, not all of whom are cybersecurity literate because they feel they do not need security even though potential attacks both institutionally and personally can occur at any time. Moreover, media companies also do not make preventive efforts, and act if a cyber attack has occurred. These two things are challenges that must be faced and are expected to change for the sake of cyber security in the work environment and support safe journalistic work.

Keywords: D*igital Attacks, Journalist Challenges, Cybersecurity*

Pendahulan

Serangan digital menjadi tren selama tahun 2022 yaitu berupa peretasan yang dialami oleh jurnalis dan DDoS yang ditargetkan ke situs organisasi media. Dalam catatan serangan siber, peretasan pernah dialami oleh 37 awak redaksi media Narasi sejak 24-29 September 2022 (Sinaga, 2022). Peretasan dan percobaan peretasan terhadap awak media Narasi mencakup beragam platform seperti akun Facebook, Instagram, Telegram dan Whatsapp. Awak redaksi yang menjadi target berasal dari berbagai level, dari pemimpin redaksi, manajer, bagian keuangan, produser hingga reporter. Selain awak redaksi Narasi, terdapat insiden peretasan lainnya yang dialami oleh jurnalis CNN Indonesia, Jaring.id, Ketua AJI Indonesia, serta akun YouTube Suara Kita dan akun Facebook Nuusdo.

Peretasan juga terjadi pada media alternatif seperti Konde.Co dan Magdelene.Co yang mengalami kelumpuhan situs akibat serangan digital. Dua nama media online tersebut adalah media yang menyuarakan hak-hak perempuan dan kelompok marjinal atau minoritas. Magdalene.co mendapat serangan DdoS (distributed denial- of-service), yaitu serangan dengan cara membanjiri lalu lintas jaringan internet pada server, sistem, dan jaringan yang membuat situs tak bisa diakses. Sementara serangan digital di Konde.co terjadi pada Senin, 24 Oktober 2022, setelah menuliskan berita tentang perkosaan yang terjadi di Kementerian Koperasi dan Usaha Kecil Menengah (UKM). (Adinda, 2021)Situs Konde.co tidak bisa diakses setelah mendapat serangan DDoS dan baru normal sepenuhnya pada 26 Oktober 2022. Selama dua hari itu pula, redaksi terhambat untuk mempublikasikan artikel lainnya dan mengeluarkan ongkos lebih untuk membayar konsultan IT, memasang perangkat tambahan dan mengganti plug-in yang rusak. Kerugian utama menimpa publik karena sulit mengakses informasi, terutama terkait cerita jalan terjal penyintas kekerasan seksual mencari keadilan.

Serangan siber ini tidak hanya terjadi pada hari-hari biasa, namun berpotensi semakin meningkat saat momentum politik atau menjelang Pemilu 2024, serangan siber terhadap jurnalis dikhawatirkan akan mengalami peningkatan. Serangan digital menjadi ancaman baru terhadap independensi pers dan keselamatan diri wartawan. Kisah wartawan Detik, Isal Mawardi, yang menjadi sasaran kemarahan pendukung pemerintah karena berita yang ditulisnya juga menjadi salah satu deretan korban penyerangan siber. Data pribadi Isal disebar luas di media sosial dengan tujuan menjatuhkan reputasi (doxing). (*Persekusi Doxing Sebagai Pola Baru Viktimisasi Terhadap Jurnalis Di Indonesia | Sari | Deviance Jurnal Kriminologi*, n.d.)

Southeast Asia Freedom of Expression Network, sebuah organisasi regional yang berfokus pada upaya memerjuangkan hak-hak digital di kawasan Asia Tenggara menyatakan bahwa dalam tiga tahun terakhir, ada tujuh wartawan yang mengalami doxing (Laporan Tahunan SAFEnet, 2019). Setiap tahun jurnalis menerima berbagai jenis serangan dengan pelaku baik dari aktor negara maupun aktor non negara Namun mekanisme perlindungan yang disediakan oleh institusi negara untuk melindungi jurnalis yang menjadi korban kekerasan seperti tersedianya bantuan kedaruratan, safety fund, atau pun pendampingan hukum belum nampak terlihat jelas. Mekanisme perlindungan masih menjadi inisiatif organisasi masyarakat sipil seperti AJI, LBH Pers, maupun Komite Keselamatan Jurnalis. Dewan Pers memang telah memiliki mekanisme perlindungan jurnalis dari kriminalisasi, ditandai dengan MoU dengan Kepala Polri dan tahun ini telah ditindaklanjuti dengan perjanjian kerja sama (PKS) tentang perlindungan kemerdekaan pers.1 Namun MoU tersebut selama ini masih minim sosialisasi dan tidak dilatihkan kepada jajaran kepolisian di tingkat bawah. Selain itu,

belum ada mekanisme sebagai respon cepat dan perlindungan menyeluruh jika terdapat jurnalis yang tetap dipidana karena karya jurnalistiknya, seperti tidak ada hotline yang mudah diakses oleh korban kriminalisasi, tidak ada bantuan dana litigasi, tidak ada pengacara yang disediakan oleh Dewan Pers, serta bagaimana advokasi litigasi yang diberikan Dewan Pers agar kasus pemidanaan dihentikan oleh Polri. Di sisi lain, organisasi media juga dianggap belum memberikan perlindungan secara holistik terhadap jurnalisnya.

Tantangan para jurnalis dalam menjaga diri dari serangan siber dan mempertahankan independensinya menjadi penuh beban karena seiring waktu, aktivitas daring kian tak terpisahkan dari kerja wartawan. Oleh karena itu, penelitian ini berupaya mendeskripsikan tantangan jurnalis dalam keamanan digital, karena dinilai penting dan mendesak sebagai upaya mengurangi risiko (mitigasi). Melihat latar belakang masalah tersebut, maka peneliti menilai penelitian mengenai tantangan jurnalis untuk menerapkan keselamatan digital penting untuk dilakukan. Adapun tujuan riset ini adalah untuk mengetahui pengalaman tantangan jurnalis terkait dengan keamanan siber dalam menjalankan tugasnya, juga untuk mengetahui strategi keamanan personal yang dilakukan jurnalis untuk mengantisipasi adanya serangan digital.

Penelitian terdahulu yang menjadi tinjauan literatur dalam riset ini pernah dilakukan oleh Basudiwa Supraba Sangga Buana pada tahun 2021 dengan judul "Kekerasan Terhadap Pers Melalui Serangan Siber : Studi Kasus Pada Media Online Tempo.co". (Buana & Rijal, 2021)Riset ini bertujuan untuk mengetahui motif dan alasan serta bentuk penyerangan digital yang terjadi di Tempo.co. Riset terdahulu lainnya adalah "Tinjauan Viktimologis Terhadap Jurnalis yang Menjadi Korban Penyebaran Data Pribadi (Doxing) melalui media siber yang ditulis oleh Nurul Insi Syahruddin pada 2022. (Syahruddin, 2022) Riset ini mengupas tinjauan jurnalis korban doxing dalam perspektif hukum. Kedua riset tersebut memberi perspektif bagi penulis untuk mengembangkan riset yang lebih komprehensif dengan topik yang lebih spesifik yakni mengenai tantangan keamanan siber bagi jurnalis.

Peneliti juga menggunakan tinjauan pustaka teori pers dunia. Adapun teori-teori pers di dunia dikategorikan dalam teori pers otoriter, teori pers bebas (liberal), teori pers bertanggungjawab sosial dan teori pers komunis Soviet. Keempat teori pers tersebut mengasumsikan bahwa pers selalu mengambil bentuk dan struktur sosial politik dimana pers tersebut beroperasi Undang-Undang Pers juga digunakan sebagai alat analisis dalam membedah tantangan jurnalis dalam keamanan siber. Undang-undang No 40 tahun 1999 tentang Pers memberikan sanksi kepada mereka yang menghalang-halangi kerja wartawan. (Amri et al., 2021) Pasal 18 mengenai ketentuan pidana UU Pers ini secara tegas menyatakan, setiap orang yang secara melawan hukum dengan sengaja melakukan tindakan yang berakibat menghambat atau menghalangi pelaksanaan ketentuan Pasal 4 ayat (2) dan ayat (3) dipidana dengan pidana penjara paling lama dua tahun atau denda paling banyak lima ratus juta rupiah (Dewan Pers, 2020). Sebagai landasan utama, penelitian ini mengacu pada teori determinisme, yang dikemukan oleh Marshall McLuhan dalam bukunya The Guttenberg Galaxy: The Making of Typographic Man. Dikutip dari buku Ajar Komunikasi Massa (Dr. Drs. Ido Prijana Hadi, M.Si Megawati et al., 2021)menyatakan, prinsip mendasar teori determinisme adalah bahwa perubahan dalam berbagai bentuk komunikasi akan berdampak pada bagaimana manusia menjalani kehidupannya di masa depan. Dalam teori tersebut, McLuhan juga menyatakan, bahwa media adalah pesan. Fungsi dan emosi manusia dapat diperkuat dan diperluas melalui penggunaan media. Setiap bentuk media baru yang ditemukan dianggap sangat memperluas beberapa kapasitas manusia. Media bertugas sebagai perpanjangan dari indera kita, sementara kehidupan di era elektronik membuat

dunia seakan semakin mengecil. Inilah yang disebut sebagai desa global (global village). Sebagai manusia sosial, sebenarnya aktivitas interaksi sosial tidak bisa dihindari, namun karena adanya desa global telah membentuk manusia menjadi individualis. Oleh karena itu, efek media massa tidak dilihat dari isinya melainkan dari bentuknya. Teori determinisme ini berasumsi bahwa media komunikasi membentuk perilaku manusia, dan setiap media memiliki karakteristik berbeda dan mempunyai keunikannya sendiri.

Metode Penelitian

Penelitian ini menggunakan metode kualitatif yang dijelaskan secara deskriptif dengan pendekatan fenomenologi interpretatif atau Interpretative Phenomenological Analysis (IPA). Pendekatan yang dikemukakan oleh Jonathan Smith pada 1996 ini, merupakan sebuah pendekatan di mana data diperoleh dan dikaji dengan cara yang mendalam (Sudarsyah, 2013). Sedangkan paradigma yang digunakan adalah paradigma konstruktivis. Paradigma konstruktivis memahami bahwa suatu realitas sosial tidak bisa digeneralisasikan. Kata kunci penelitian kualitatif ini terletak pada teknik analisis dan interpretasi data yang bersifat deskriptif yang disajikan dengan menggunakan bahasa yang khas serta bukan bertujuan untuk menggeneralisasi hasil. Penelitian ini menggunakan data primer berupa wawancara dan observasi. Wawancara merupakan teknik dalam pengumpulan data untuk mendapatkan informasi dari sumber data langsung melalui percakapan atau tanya jawab (Sugiyono, 2017). Sedangkan menurut Creswell wawancara tentu saja memerlukan pertanyaan-pertanyaan yang secara umum tidak tersruktur (unstructured), dan bersifat terbuka (open-ended) yang dirancang untuk memunculkan pandangan dan opini dari para partisipan. Observasi juga diperlukan upaya untuk pengumpulan data yang dilakukan ketika peneliti langsung turun ke lapangan untuk mengamati perilaku dan aktivitas individu-individu dilokasi penelitian (Creswell, 2016)

Adapun yang menjadi subjek penelitian ini adalah delapan (8) informan yakni para jurnalis yang bekerja di berbagai platform media massa dari dalam dan luar kota Semarang. Para informan diwawancarai secara personal melalui sebuah Forum Discussion Group (FGD). Tema FGD sudah langsung mengerucut yakni "tantangan kerja jurnalis dalam keamanan siber". Melalui sesi "sharing bout your digital siber journey", FGD sekaligus menjadi sebuah teknik untuk mendapatkan data, disamping juga teknik wawancara mendalam. Wawancara mendalam dilakukan secara personal dilakukan melalui telepon langsung maupun melalui kesempatan tatap muka, juga email, Setiap informan menghasilkan data yang berbeda-beda sesuai dengan pengalaman yang mereka dapatkan terkait dengan tantangan keamanan siber. Adapun kriteria subyek penelitian adalah :

Jurnalis yang sudah bekerja lebih dari lima (5) tahun.

Jurnalis yang wilayah kerjanya meliputi seluruh Jawa Tengah

Jurnalis dari berbagi platform media massa.

Jurnalis yang memiliki pengalaman khusus terkait dengan keamanan siber.

Sedangkan data sekunder didapatkan melalui dokumentasi. Penulis mengumpulkan dokumen-dokumen kualitatif yang bisa berupa dokumen publik (seperti koran, makalah, laporan kantor) ataupun dokumen privat (seperti buku harian, diary, surat, e-mail). Studi dokumentasi dalam penelitian ini mengumpulkan dokumen dan data-data yang diperlukan lalu ditelaah secara intens sehingga dapat mendukung data primer.

Teknik analisis data menggunakan bantuan tool Nvivo untuk melakukan coding data yang berupa hasil wawancara dengan 8 informan yang memenuhi kriteria. Meski demikian, proses awal koding mutlak dilakukan oleh peneliti terlebih dahulu sehingga ini bukan menjadi bagian secara

teknis yang dikerjakan oleh Nvivo. Sesuai dengan desainnya, penelitian ini menggunakan metode kualitatif yang dijelaskan secara deskriptif dengan pendekatan fenomenologi interpretatif atau Interpretative Phenomenological Analysis (IPA). Tahap-tahap Interpretative Phenomenological Analysis yang dilaksanakan sebagai berikut: 1) Reading and re-reading; 2) Initial noting; 3) Developing Emergent themes; 4) Searching for connections across emergent themes; 5) Moving the next cases; and 6) Looking for patterns across cases. Berikut adalah salah satu contoh transkrip wawancara dengan informan yang sebelumnya dikoding secara manual oleh peneliti untuk selanjutnya diolah dengan bantuan tool Nvivo agar dapat menjadi data primer.

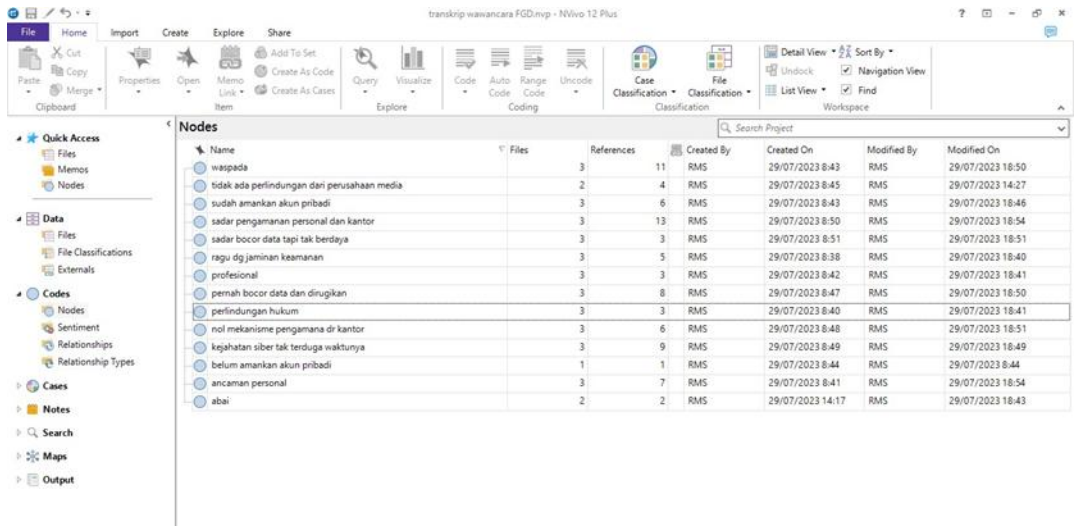
Tabel 1. Contoh transkrip wawancara yang telah dilakukan

Peneliti / Informan	Transkrip wawancara
Peneliti	***Apakah Anda pernah mengalami serangan digital selama menjalankan tugas sebagai seorang jurnalis?***
informan 1	Saya secara langsung memang belum pernah kena serangan digital, namun akhirnya muncul pertanyaannya sebenarnya kita ini aman nggak sih? Mau kirim berita kan semua pake perangkat teknologi, nah teknologi itu sendiri aman tidak sih? Contoh seperti kasus "narasi " yang dulu pernah terjadi, orangnya kan 11 orang, ke hack semua. Perangkatnya nggak aman, aplikasinya nggak aman, sudah tau nggak aman, terus tindak lanjutnya seperti apa? tapi sampai sekarang kan nggak pernah ketahuan siapa yang meng ngehack. Narasi. Atau ketika dulu aktivis kebijakan publik berbicara, ya bener diajukan, diberitakan juga sih..tapi kan kita tau kan nggak ada tindak lanjutannya. Dilacak kek..atau diurus lebih lanjut gitu lah..nggak ada kan.. Artinya kan nggak ada jaminan keselamatan. Kasus lainnya sebenarnya juga ada, seperti pembajakan situs, kan jarang yang
	dilacak..artinya ini juga nggak ada jaminan keamanan
peneliti	***secara personal di tingkat lokal pengalaman sebagai jurnalis ketika berinteraksi atau menggunakan perangkat digital ?***
Informan 1	kalo sama temen-temen sebenarnya biasa, yang menjadi ancaman tu ketika kita wawancara narasumber via whatssapp "mbok ojo diberitakan" atau " kok kamu bisa ngomong gitu?" ya walopun secara Undang Undang Pers kita sudah ada jaminan, cuman kan kita mikirin kemanan juga. Kita memberitakan salah, tidak memberitakan ya salah karena kita ini kan wartwan, kerjanya memberitakan. jadi ya memang harus ati-ati
Peneliti	***Untuk aktifitas pribadi , aktifitas dengan platfom digital kan ada akun*** ***banyak nih, ada email, ada medsos..lalu bagaimana perlakuan Anda terhadap akun-akun itu untuk aktifitas pribadi?***
Informan 1	Untuk aktifitas pribadi yang dilakukan adalah melakukan 2 langkah pengamanan. Untuk whatss app selain pake sidik jari juga setiap aktivasi kan ada otorisasi juga. Dari whatssApp sendiri kan juga menyarankan sebenarnya. Menghindari ada upaya peretasan. Kalo email nggak sekedar password aja, tapi juga terkoneksi dari mana, misalnya kalo kita pake komputer di tempat publik apalagi nih semuanya harus hati-hati.

Sumber : olah data peneliti

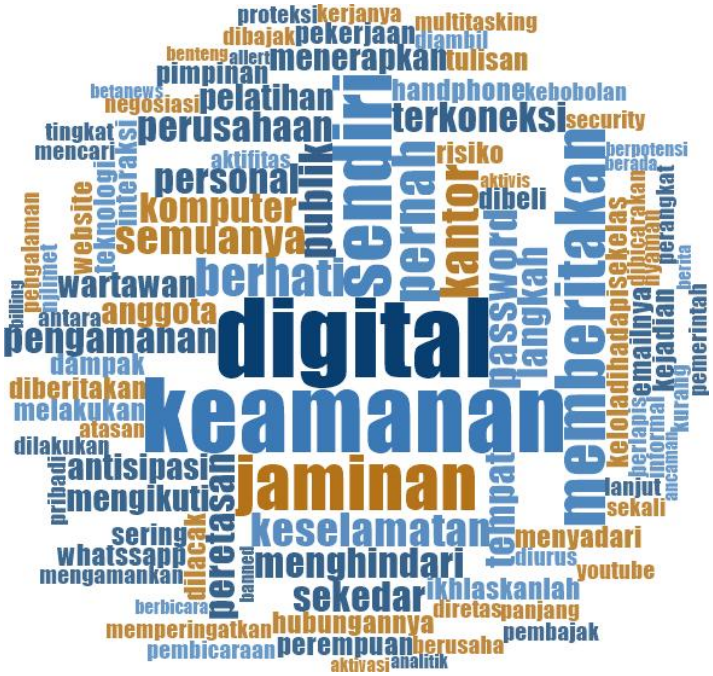
Hasil dan Pembahasan

Koding diperlukan untuk mengolah data, yang sebelumnya diawali oleh sebuah berpikir analitis oleh peneliti. Proses memberi kode pada kata, frasa, kalimat, atau paragraph yang mewakili kode tersebut disebut dengan koding. Kode berupa konsep atau istilah. First cycle coding berangkat dari data lapangan, dengan kode- kode yang merepresentasikan kondisi apa adanya. Setelah itu dilakukan second cycle coding yaitu kode yang lahir dari proses generalisasi kondisi lapangan. Dua tahapan tersebut bergerak dinamis sehingga bisa memaksimalkan hasil. Di Nvivo, ruang untuk koding diberi nama sebagai nodes. Nodes digunakan untuk mengklasifikasikan data-data dalam penelitian ini. Berikut adalah salah satu contoh proses nodes dengan tool Nvivo yang menggunakan data wawancara informan. File terkait penelitian ini yang sudah diimport kemudian dibaca untuk menemukan kalimat-kalimat yang ingin dianalisis. File yang digunakan untuk pemrosesan data di Nvivo ini ada 3 file yaitu 1 file wawancara informan secara personal, 1 file wawancara tertulis, dan 1 file transkrip wawancara informan melalui Focus Group Discussion (FGD).



Gambar 1 Lembar Kerja Codes pada NVivo (proses kerja koding)

Penggunaan Nvivo juga dapat memvisualisasi kata. (Rianto Rahadi, 2021). Kata-kata yang ukurannya paling besar adalah kata yang paling sering muncul sebagaimana yang tercatat dalam word frequency. Semakin ke pinggir, semakin sedikit disebut. Word cloud ini selanjutnya menjadi panduan atau pemahaman terhadap data yang sudah ada, bukan hasil final dari analisis.



Gambar 2 : Visualisasi data dalam Word Cloud

Melalui bantuan Nvivo, langkah analisis data dengan menggunakan Interpretative Phenomenological Analysis (IPA) dapat sekaligus mengerjakan tahap ke empat (4) yakni searching for connection a cross emergent themes atau tahap berikutnya yang mengaitkan tema-tema yang muncul juga pengerjaan tahap ke lima (5) yakni moving the next cases. Urutan yang digunakan awalnya adalah urutan kronologis kemunculan tema. Kemudian tahap berikutnya adalah mengurutkan dengan lebih bersifat analitis atau teoretis, dengan tujuan menemukan hubungan antar tema yang muncul hingga di tahap akhir dari analisis adalah mencari pola-pola yang muncul antar kasus/informan. Dari koding melalui nodes yang ada di NVivo, maka dapat dimunculkan tema-tema besar atau isi pesan yang merupakan intisari wawancara dari informan. Tema-tema pesan yang muncul adalah :

1. Ancaman personal dalam kerja jurnalistik
2. Jaminan keamanan jurnalis dari perusahaan media
3. Kesadaran terhadap keamanan data digital personal dan perusahaan

Langkah terakhir tahapan sesuai IPA adalah pola pemaknaan antar kasus (looking for patterns across cases) dan mendapatkan tema yang umum. Berikut adalah tema antar kasus yang berhasil disusun berdasarkan lima langkah analisis yang sudah dilakukan.

Tabel 2 : tema master antar kasus.

NO	TEMA
1	Ancaman personal dalam kerja jurnalistik • Ancaman kerja baik langsung maupun secara digital • Rasa tidak aman setelah melakukan peliputan sensitif • Peretasan akun pribadi media sosial jurnalis
2	Jaminan keamanan digital dari perusahaan media masing-masing informan. • Belum adanya perlindungan dari perusahaan media terkait dengan keamanan jurnalis pasca liputan • Perusahaan media tidak mau ikut menanggung risiko jurnalisnya • Ketidakjelasan penanganan dan tindak lanjut dari kasus yang pernah ada
3	Kesadaran terhadap keamanan data digital personal dan perusahaan. • Pernyataan informan tentang upaya yang dilakukan jurnalis setelah peretasan akun pribadi. • Antisipasi kejahatan siber.

Sumber : olah data peneliti

Ancaman personal dalam kerja jurnalistik

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 kutipan salah satu informan yang menyatakan ia pernah mendapatkan ancaman yang berujung kerugian secara personal, karena seseorang membajak akun WhatsApp nya (WA).

> *"WA saya pernah di hack –sepertinya ada kaitanya dengan liputan ya yang berkaitan dengan kilas balik kasus G.30 S PKI. Pada waktu itu secara tiba-tiba WA saya ada pending waktu lama, mau keluar juga susah WA masuk maupun keluar sama saja tidak bisa. Akhirnya saya ganti nomor dan saya delet nomor saya. Itu pengalaman saya ya."*

Akibat peristiwa itu, informan dirugikan karena kontak narasumber dan seluruh riwayat chat di aplikasi WhatsApp yang berkaitan dengan pekerjaannya terpaksa harus hilang, karena ia mengganti bahkan menghapus nomor. Dampak ancaman siber di akun pribadinya membuat informan memutuskan untuk tidak kembali menginstal WhatsApp dan menggunakan aplikasi chat lain yaitu Signal.

Risiko profesi sebagai jurnalis yang mengalami ancaman selama melakukan tugas jurnalistiknya juga terjadi secara langsung, bahkan jurnalis terkadang juga mengalami ancaman ganda. Diserang secara siber, dan diteror mentalnya secara langsung. Hal ini juga diungkapkan oleh informan yang

menceritakan kasus kawan baiknya yang mendapatkan teror pasca menulis soal kritik kepada penguasa.

> *"Ada juga pengalaman dari kawan saya yang dihack FB nya, Teman saya itu seorang blogger yang lebih sering mengkritik ke pemerintah. Message inbox di FB nya itu juga bisa pending lama sekali. Bahkan akhirnya ketahuan bahwa pesan yang masuk ke inboxnya baru masuk setahun berikutnya. Teman saya itu juga pernah ditelpon oleh nomor tidak dikenal dan ia tidak tahu darimana dari nomor tersebut. Di ujung telepon itu suara seorang perempuan menanyai teman saya itu dan menunjukkan bawa ia tahu persis aktifitas dari teman saya itu. Misalnya suara perempuan itu mengatakan " oh Bapak rumahnya di sini kan?" Jadi seperti ngancam, telpon tapi ia bisa dengan detil menyatakan rumah teman saya itu mulai dari RT RW berapa, hingga nomor rumahnya."*

Pengalaman informan lainnya yang bekerja di media online juga menunjukkan bahwa ancaman terjadi pasca liputan tidak hanya dialami oleh dirinya saja. Hal itu seolah-olah sudah jamak dan lumrah terjadi jika ada narasumber yang memberi peringatan awal terhadap hasil liputannya.

> *"Kalo sama temen-temen sebenarnya biasa, yang menjadi ancaman tu ketika kita wawancara, narasumber kirim pesan via WhatssApp "mbok ojo diberitakan" atau " kok kamu bisa ngomong gitu? Ya walaupun secara Undang Undang Pers kita sudah ada jaminan, cuman kan kita mikirin kemanan juga. Kita memberitakan salah, tidak memberitakan ya salah karena kita ini kan wartawan, kerjanya memberitakan. jadi ya memang harus ati-ati."*

Pesan bernada ancaman, kadangkala tidak muncul dalam bentuk kalimat yang menekan dan meneror, tapi bisa juga menggunakan kalimat yang dirasa tetap lunak namun tetap memberikan tekanan agar jurnalis tidak sembrono dalam menulis dan memberitakan. Teror atau ancaman juga muncul dalam bentuk panggilan pesan di Whatss App dan panggilan telpon ke nomor pribadi jurnalis yang juga digunakan sebagai alat kerja.

> *"Kalo soal keamanan diri setelah ada liputan atau mungkin advokasi ya ada sedikit cerita sih, yaitu pas selesai Musyawarah Daerah atau Musda. Ada sekitar 50 an nomor tidak dikenal masuk ke anggota , ke WA dan telpon. Ya tidak dikenal aja, mungkin semacam teror atau bagaimana kurang tau, yang jelas juga membuat semacam perasaan tidak nyaman"*

Tidak dapat dipungkiri, menjalankan tugas jurnalistik secara profesional di era new media ini mempunyai tantangan yang semakin kompleks. Sebagaimana yang sudah dijabarkan dalam pengalaman jurnalis menghadapi ancaman setelah liputan lapangan, maka hal tersebut sebenarnya tidak sejalan dengan Undang-undang Nomor 40 Tahun 1999 tentang Pers. Pasal 4 UU Pers No 40 Tahun 1999 ayat 2 yang menyatakan, "terhadap pers nasional tidak dikenakan penyensoran, pemberedelan atau pelarangan penyiaran". Ini jelas, pers bebas dari tindakan pencegahan, pelarangan, dan atau penekanan, sehingga hak masyarakat untuk memperoleh informasi terjamin. Penyensoran, pemberedelan atau pelarangan penyiaran tidak berlaku pada media cetak dan media elektronik. Siaran yang bukan merupakan bagian dari pelaksanaan kegiatan jurnalistik diatur lebih lanjut dalam ketentuan undang-undang. (Dewan, 1999)Pasal tersebut memberikan peluang bagi pers dan setiap warga untuk menggunakan kesempatan menyalurkan informasi dan gagasan serta pendapat seluas-luasnya. Namun dalam kenyataannya, dalam proses peliputan atau tahap awal pengumpulan data lapangan saja, seorang jurnalis harus sudah berhadapan dengan ancaman yang bervariasi. Sehingga praktis, bagi jurnalis di era siber saat ini ancaman terhadap kebebasan pers, selain datang dari sistem kekuasaan yang otoriter, juga bisa dari masyarakat. Masih ada kelompok di masyarakat yang merasa

kepentingannya terganggu oleh kebebasan pers. Mereka mencoba melakukan hal-hal yang mengancam kebebasan pers.

Jaminan Keamanan Jurnalis Dari Perusahaan Media

Pada bagian ini, informan yang datang dari berbagai platform media massa memberikan pengalamannya yang terkait dengan belum adanya perlindungan dari perusahaan media. Perlindungan yang dimaksud, rata-rata berbicara mengenai dampak pasca liputan oleh jurnalis. Beberapa kasus peretasan akun yang harus diderita oleh jurnalis, akhirnya hanya menjadi sebuah obrolan biasa di ruang redaksi. Berikut adalah pernyataan salah seorang informan (informan 2) yang bekerja di media online dan cetak.

> *"Kalo dibicarakan secara resmi sih enggak. Pembicaraan mengenai keamanan itu secara informal saja. Paling sesama temen-temen hanya ngobrolin itu aja, kalo secara formal maksudnya secara rapat redaksi sih enggak. Saya sendiri secara pribadi dalam menghadapi kasus saya lebih percaya ngobrol tatap muka dengan redpel saya, redpel itu kan sudah senior- senior, mereka lebih berpengalaman. Tapi kadang-kadang juga ngobrol sama temen-temen kota juga, yang lebih muda juga".*

Pimpinan dan penanggung jawab redaksi yang mengetahui adanya peristiwa tersebut, juga jarang membahas mengenai langkah pengamanan personal dari serangan siber dan tidak juga memberikan sebuah Standart Operational Procedur (SOP) agar jurnalisnya memperoleh jaminan ketenangan dan keamanan pada saat bertugas.

> *"Soal jaminan keamanan dari perusahaan media ya boleh dibilang belum ada, paling sharing- sharing aja."*

Sementara itu pengalaman dengan tema jaminan keamanan yang diberikan oleh perusahaan media juga berkembang pada persoalan tanggungjawab pengambilan keputusan sehubungan dengan hirarki di ruang redaksi. Salah seorang informan menyatakan bahwa pernah terjadi kasus pembobolan akun bank pada salah seorang kawan kerjanya dan mengakibatkan tagihan yang bukan seharusnya wajib dibayar oleh yang bersangkutan karena yang bersangkutan memang tidak berbelanja sejumlah tagihan yang melonjak hingga di luar kemampuan bayarnya di market place. Rekan kerja dari informan ini mendadak mendapatkan tagihan sebesar Rp.18 juta rupiah. Padahal ia hanya membeli sebuah barang dengan nilai yang tidak sebesar itu hingga belasan juta rupiah. Rekan kerja dari informan itu kemudian meminta bantuan kepada para pimpinan untuk memecahkan masalah, namun akhirnya juga tidak bisa mendapatkanya.

> *"Akhirnya ke kantor, rapat sama kantor, dan lapor atasan dan atasan angkat tangan alias tidak memberikan perlindungan atau jaminan. Padahal orangnya yang kena masalah itu –maaf— bukan kalangan yang punya uang banyak, bukan orang berada. Mungkin pimpinan melihatnya bahwa apa yang dibeli oleh kawan saya itu tidak ada hubungannya dengan pekerjaan kantor sehingga kantor merasa tidak perlu membantu."*

Dari dalam redaksi sendiri, tanggung jawab dan perlindungan dari pimpinan redaksi atau perusahaan media terhadap jurnalis yang terkenan peretasan atau kekerasan siber pada beberapa kasus yang pernah terjadi masih kurang bahkan cenderung tidak ada. Sementara itu, untuk aspek perlindungan hukum dari pemerintah atau negara juga dinilai oleh informan sebagai langkah yang masih malu-malu bahkan nyaris tidak tampak tindak lanjutnya. Salah seorang informan (informan 1) mempertanyakan mengenai tindak lanjut dari kasus serangan siber yang menimpa website "Narasi News".

> *"Akhirnya muncul pertanyaannya sebenarnya kita ini aman nggak sih? Mau kirim berita kan semuapake perangkat teknologi, nah teknologi itu sendiri aman tidak sih? Contoh seperti kasus "NARASI " yang dulu pernah terjadi, orangnya kan 11 orang, ke hack semua.Perangkatnya nggak aman, aplikasinya nggak aman, sudah tau nggak aman, terus tindak lanjutnyaseperti apa? tapi sampai sekarang kan nggak pernah ketahuan siapa yang meng ngehack. Narasi. Atau ketika dulu aktivis kebijakan publik berbicara, ya bener diajukan, diberitakan juga sih..tapi kan kita tau kan nggak ada tindak lanjutannya. Dilacak kek..atau diurus lebih lanjut gitu lah..nggak ada kan.. Artinya kan nggak ada jaminan keselamatan. Kasus lainnya sebenarnya juga ada, seperti pembajakan situs, kan jarang yang dilacak..artinya ini juga nggak ada jaminan keamanan."*

Kesadaran Terhadap Keamanan Data Digital Personal dan Perusahaan

Dari wawancara dengan para informan, didapatkan kenyataan bahwa tidak semua jurnalis sudah melakukan upaya pencegahan terhadap serangan / kekerasan siber. Dari 8 jurnalis yang diwawancarai, hanya tiga (3) jurnalis yang sudah melakukan pengamanan ganda untuk akun personalnya. Minimal pengamanan untuk mencegah kebocoran atau peretasan WhatssApp sebagai aplikasi komunikasi yang menunjang pekerjaan. Berikut pernyataan dari informan 2 yang melakukan pengamanan akunnya setelah terjadi ancaman dan teror.

> *"Saya sendiri secara pribadi kadang-kadang belum mengamankan akun-akun pribadi saya. Saya menyadari saya sering abai dengan hal ini. Kadang-kadang males, ribet karena selaku perempuan kita ini kan multitasking, jadi kayak nggak sempat, abai lah. Kadang-kadang kalo ke toko atau beli apa gitu terus dimintain nomor telpon ya asal kasih aja. Kalo sekarang ya jadi mikir lagi ya"*

Lain halnya dengan informan 1 yang sudah melakukan upaya pengamanan akun personalnya demi menunjang keselamatan personal.

> *"Untuk aktifitas pribadi yang dilakukan adalah melakukan 2 langkah pengamanan. Untuk WhatsApp selain pake sidik jari juga setiap aktivasi kan ada otorisasi juga. Dari whatssApp sendiri kan juga menyarankan sebenarnya. Menghindari ada upaya peretasan. Kalo email nggak sekedar password aja, tapi juga terkoneksi dari mana, misalnya kalo kita pake komputer di tempat publik apalagi nih semuanya harus hati-hati".*

Informan 2 yang sempat mengalami peretasan akun WhatsApp, menyatakan kini ia menjadi lebih berhati-hati dalam melakukan antisipasi pengamanan identitas diri di aplikasi mobile dan media sosial yang ada di perangkat digitalnya.

> *"Kalo untuk email saya mengamankan via password yang njlimet, nama anak saya misalnya yang panjang dan saya rasa itu cukup buat keamanan email saya"*

Dari sisi perusahaan media, langkah antisipasi adanya serangan siber dilakukan justru setelah terjadi serangan. Hal ini disebabkan karena rata-rata kejadian itu dikategorikan sebagai kejadian tak terduga meskipun sebenarnya mereka telah melakukan sejumlah langkah pengamanan sebagai salah satu strategi antisipasi. Berikut strategi pengamanan yang dilakukan oleh perusahaan media , sebagaimana yang dipaparkan oleh informan 4.

> *"Kejadian ini tidak hanya sekali tapi sampai 2 – 3 kali, makanya untuk proteksi sendiri, kami menerapkan beberapa model. Ada pengamanan 3 langkah yang dobel-dobel dan itu pun belum pasti bisa menjamin keamanan web kami juga, karena pencuri itu selalu lebih maju untuk mencari celah. Nah itu aja sekelas web kita sendiri, wong sekelas web nya pemerintah aja bisa bobol kok. Makanya kita harus antisipasi dan kelola sendiri dengan hati-hati walaupun ya kadang terjadi lagi."*

Strategi pengamanan website atau keamanan digital dilakukan juga oleh perusahaan media dalam berbagai skala, mengingat dampak yang dirasakan sangat merugikan bisnis dan prestasi. Hilangnya akun otomatis berakibat hilangnya follower atau audience dari media tersebut. Oleh karena itu, pengamanan siber dilakukan oleh perusahaan dengan berbagai cara dan berlapis-lapis untuk mengantisipasi adanya serangan atau peretasan.

> *"Media kami masih kecil. Belum powerfull banget. Untuk keamanan website ada 3 penerapan. Salah satunya melalui otentifikasi dua langkah. Sedangkan akses data analitik hanya diberikan ke beberapa orang, kemudian back up data penting apapun itu harus diback up baik dari wartawan karena kita nggak pernah tau, ngrecord di hp hapenya hank ntar repot. Website juga di back up. Pernah juga sih ada beberapa konten hilang, entah di hack atau tidak, karena IT pun juga nggak tau. Dari kejadian itu, di kantor kami selalu diadakan back up untuk segala hal, termasuk billing nya website nya juga diback up. Berita- berita dibackup karena kalo hilang nggak balik lagi. Website diberi proteksi tambahan." (informan 8)*

Era jurnalisme digital menjadi bukti dari Teori determinisme Mc Luhan. Era ini menjadi kepanjangan tangan dari kepentingan manusia yang membutuhkan kecepatan. Oleh karena itu, adanya kasus serangan digital yang mempengaruhi keamanan siber tiap perusahaan media massa, sekaligus menjadi sebuah "pisau bermata dua" . Di satu sisi, media online, internet dan kecepatan informasi saat ini membantu kebutuhan manusia, namun di sisi lain apabila terjadi peretasan atau serangan digital maka terbuka kemungkinan juga berpengaruh pada citra atau cerminan dari kredibilitas sebuah perusahaan media massa. Bagaimanapun media merupakan faktor utama untuk memengaruhi hal lainnya, karena setiap media memiliki karakteristik berbeda dan unik. Dari berbagai pendapat para informan, strategi keamanan digital jurnalis, menjadi hal penting yang idealnya mendapatkan perhatian besar. Informan 7 memberikan pernyataan apabila perusahaan media tempatnya bekerja mau memberikan pelatihan, maka sebagai pekerja ia juga mendapatkan haknya untuk dilindungi dan mendapatkan pengetahuan. Informan tujuh (7) juga menyatakan bahwa kantornya belum pernah memberikan pelatihan keselamatan siber bagi pekerjanya.

> *"Tentang jaminan keselamatan digital dari perusahaan media saya, belum ada, terkhusus digital security belum ada."*

Informan dua (2) juga menyatakan keinginannya untuk melindungi dirinya sendiri melalui kesempatan peningkatan keilmuan mengenai keamanan siber.

> *"Secara personal saya merasa harus update pengetahuan mengenai keamanan digital dengan cara ikut workshop"*

Simpulan dan Saran

Simpulan

Pengalaman yang diceritakan para informan kepada peneliti menunjukkan keterhubungan dan mengerucut menjadi sebuah temuan sekaligus menjawab pertanyaan penelitian. Ancaman personal yang dialami jurnalis sehubungan dengan tugas jurnalistiknya, terjadi karena jurnalis juga belum mengamankan akun di berbagai aplikasinya. Tidak semua jurnalis yang menjadi informan sudah melakukan pengamanan karena sebelumnya merasa belum perlu. Dari delapan (8) informan yang diwanwancarai secara mendalam, baru 3 orang saja yang sudah melakukan pengamanan akun personal yang digunakan sebagai penunjang kerja jurnalistiknya. Artinya, tantangan ini bahkan muncul dari dalam profesi jurnalis sendiri, yang menunjukkan bahwa merak belum semuanya melek akan keamanan siber. Ancaman kekerasan atau teror bahkan peretasan akun milik jurnalis secara personal menjadi cerminan kenyataan yang tidak sejalan dengan Undang-undang Nomor 40 Tahun 1999 tentang Pers. Pasal 4 UU Pers No 40 Tahun 1999 ayat 2 yang menyatakan, "terhadap pers nasional tidak dikenakan penyensoran, pemberedelan atau pelarangan penyiaran". Melakukan teror atau ancaman terhadap kerja jurnalistik berarti menghalangi jurnalis untuk bekerja secara profesional.

Sementara itu keterhubungan lainnya yaitu pada jaminan keamanan digital dari perusahaan media masing- masing informan. Berdasarkan pengalaman para informan, pengamanan personal maupun perusahaan media dilakukan setelah terjadi serangan siber. Langkah antisipasi bergerak tidak linier dengan potensi serangan digital yang bisa terjadi kapan saja. Perusahaan media juga belum menyediakan sebuah Standart Operational Procedurs (SOP) bagi keamanan siber untuk jurnalisnya maupun bagi perusaan media secara umum. Temuan riset ini menunjukkan bahwa tantangan yang dihadapi para jurnalis dalam menjalankan kerja profesionalnya masih belum sepenuhnya mendapatkan perlindungan dan jalan keluar serta belum juga mengawali sebuah langkah mitigasi dari serangan digital yang sewaktu-waktu bisa mencelakai secara personal dan mengganggu tugas kerjanya.

Saran

Saran untuk penelitian lanjutan akan lebih komprehensif apabila dilanjutkan dengan penelitian pengaruh literasi keamanan digital kepada para jurnalis dan perusahaan media massa, dengan mix methods, untuk mengetahui sugnifikansi kenaikan tingkat kemanan siber para jurnalis.

Oleh karena itu masih diperlukan penyadaran tentang keamanan kemanan siber dalam profesi jurnalis, mengingat hingga hari ini masih belum terlihat secara maksimal perlindungan dan tindak lanjut terhadap serangan siber. Jurnalis juga secara sadar memerlukan penambahan keilmuan mengenai keamanan digital, sebagai salah satu langkah untuk mengantisipasi kejahatan siber.

Ucapan terimakasih

Terimakasih kepada LPPM USM yang membiayai penelitian ini, juga kepada jurnalis multiplatform Semarang yang menjadi informan riset.

Daftar Rujukan

Adinda, P. (2021). *Magdalene.co dan Konde.co Kena Serangan Digital, Peran Pers Mempromosikan HAM dan Keberagaman Dihalangi.* https://www.asumsi.co/post/59168/magdaleneco-dan-kondeco-kena-serangan-digital-peran-pers-mempromosikan-ham-dan-keberagaman-dihalangi/

Amri, S., Maulina, P., & Zuhri, A. (2021). PRO DAN KONTRA UNDANG-UNDANG NOMOR 40 TAHUN 1999 TENTANG PERS SEBAGAI LEX SPECIALIS (Memaksimalkan Profesionalitas Pers dalam Menjalankan Aktifitas Jurnalistik). *SOURCE: Jurnal Ilmu Komunikasi*, *7*(1), 87–94.

Buana, B. S. S., & Rijal, S. (2021). *Kekerasan Terhadap Pers Melalui Serangan Siber: Studi Kasus Pada Media Online Tempo.Co*. https://repository.uinjkt.ac.id/dspace/handle/123456789/65695

Creswell, J. W. (2016). *Research Design: Pendekatan Kualitatif, Kuantitatif, dan Mixed* (3rd ed.). Pustaka Pelajar.

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

Dr. Drs. Ido Prijana Hadi, M.Si Megawati, Wahjudianata, S.Sos., M.Med.Kom Inri, & Inggrit Indrayani, S.I.P., M.Si. (2021). *Buku Ajar Komunikasi Massa*. CV. Penerbit Qiara Media - Pasuruan, Jawa Timur.

Persekusi Doxing sebagai Pola Baru Viktimisasi terhadap Jurnalis di Indonesia | Sari | Deviance Jurnal Kriminologi. (n.d.). Retrieved December 31, 2023, from https://journal.budiluhur.ac.id/index.php/deviance/article/view/1139

Rianto Rahadi, D. (2021). *KONSEP PENELITIAN KUALITATIF PLUS TUTORIAL NVivo*.

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

Sugiyono, P. (2017). *Metodologi penelitian kuantitatif kualitatif dan R&D*. Alpabeta, Bandung.

Syahruddin, N. I. (2022). *TINJAUAN VIKTIMOLOGIS TERHADAP JURNALIS YANG MENJADI KORBAN PENYEBARAN DATA PRIBADI (DOXING) MELALUI MEDIA ONLINE* [Other, Universitas Hasanuddin]. http://repository.unhas.ac.id/id/eprint/13657/