Jurnal
Komunikasi
https://journal.trunojoyo.ac.id/komunikasi

EISSN 2549-4902, **ISSN** 1978-4597
Volume 18 No 1 Maret 2024

Cybersecurity Literacy Among Mass Media Journalists In Central Java

Retno Manuhoro Setyowati[1,a)], Citra Safira [2], Sinta Pramucitra[3]

1)2) 3) **Communication Science Study Program, Universitas Semarang**
[a)] author correspondence : retnomanuhoro@usm.ac.id

DOI:https://doi.org/10.21107/ilkom.v18i1.21712

ABSTRACT

Notes of the Alliance of Independent Journalists (AJI Indonesia) at the end of 2022, the number of digital attacks on journalists increased compared to 2021. There were 15 digital attacks in 2022, while in 2021, there were only 5 cases recorded. Attacks, or what is commonly referred to as digital violence, refer to the notion of violence in which the perpetrator attacks network infrastructure or uses digital technology. Meanwhile, digital attacks becoming a trend during 2022 are hacking experienced by journalists and DDoS targeted at media organization sites. However, not all mass media have prepared anticipation for the potential for digital violence, including not all journalists who understand cybersecurity's importance in carrying out their duties. This research seeks to explore the meaning of journalists related to cyber security in their journalistic work and to record real experiences of how anticipation and strategies are carried out so that they do not just become victims of cyber-attacks. The method used is qualitative with an interpretive phenomenological analysis (IPA) approach. An approach where data is obtained and studied in an in-depth way, and sees each case is something that has its characteristics. The key word of this research lies in the technique of analysis and interpretation of data that is descriptive, which is presented using a distinctive language and does not aim to generalize the results. The research location is in the city of Semarang, with data collection techniques through in-depth interviews, surveys, observations, and documentation of the research subjects, in this case, journalists from various mass media in Central Java.

Keywords: *cyber violence; digital violence; doxing; DDos, cyber security; journalists*

Article History:
Received
July 31th 2023

Revised
December 18th 2023

Accepted
February 28th 2024

ABSTRAK

Catatan Aliansi Jurnalis Independen (AJI Indonesia) di akhir tahun 2022, jumlah serangan digital kepada jurnalis menunjukkan kenaikan dibanding tahun 2021. Serangan digital di tahun 2022 adalah sebanyak 15 kali sedangkan untuk tahun 2021 hanya tercatat sebanyak 5 kasus. Serangan atau juga yang biasa disebut dengan kekerasan digital merujuk pada pengertian kekerasan dimana pelakunya menyerang infrastruktur jaringan atau menggunakan teknologi digital. Sedangkan serangan digital yang menjadi tren selama tahun 2022 berupa peretasan yang dialami oleh jurnalis dan DDoS yang ditargetkan ke situs organisasi media. Meski demikian, tidak semua media massa sudah menyiapkan antisipasi terhadap potensi kekerasan digital, termasuk juga para jurnalisnya juga belum semuanya memahami pentingnya keamanan siber dalam menjalankan tugasnya. Penelitian ini berupaya mengeksplorasi pemaknaan jurnalis terkait dengan keamanan siber dalam kerja jurnalistik mereka, juga mencatat pengalaman nyata bagaimana antisipasi dan strategi yang dilakukan agar tidak hanya berhenti sebagai korban serangan siber. Metode yang digunakan adalah kualitatif yang dengan pendekatan fenomenologi intepretatif atau Interpretative Phenomenological Analysis (IPA). Sebuah pendekatan di mana data diperoleh dan dikaji dengan cara yang mendalam serta melihat tiap kasus sebagai sesuatu yang memiliki kekhasan tersendiri. Kata kunci penelitian ini terletak pada teknik analisis dan interpretasi data yang bersifat deskriptif yang disajikan dengan menggunakan bahasa yang khas serta bukan bertujuan untuk menggeneralisasi hasil. Lokasi penelitian berada di Kota Semarang dengan teknik pengumpulan data melalui wawancara mendalam, survei, observasi, dan dokumentasi terhadap subyek penelitian dalam hal ini adalah para jurnalis dari berbagai media massa di Jawa Tengah.

Kata Kunci: *kekerasan siber; kekerasan digital; doxing; DDos; keamanan siber; jurnalis*

Cite this as (APA Style):
Setyowati, R. M., Safira, C., & Pramucitra, S. (2024). Cybersecurity Literacy Among Mass Media Journalists In Central Java. *Jurnal Komunikasi*, 18 (1), 47-60. doi: https://doi.org/10.21107/ilkom.v18i1.21712

INTRODUCTION

The Alliance of Independent Journalists (AJI Indonesia) notes that journalists in Indonesia will not be safe at work throughout 2022. Increased cases of violence mark this as the issuance of various laws that endanger the safety of journalists and weaken economic security that, affects welfare. When viewed from the level of violence that occurred, throughout 2022, 61 cases attacked 97 journalists and media workers, as well as 14 media organizations (Annur, 2023). The number of cases has increased from 2021, which reached 43 cases. Types of attacks include digital violence (15 cases), physical violence and destruction of work tools (20 cases), verbal violence (10 cases), gender-based violence (3 cases), criminal arrest and reporting (5 cases), and censorship (8 cases) (Rahmanda, 2023).

In releasing a cyber-attack report at the end of 2022, AJI stated that the number of digital attacks on journalists 15 times increases compared to 2021, which only recorded 5 cases. Attacks, or digital violence, refer to violence in which the perpetrator attacks network infrastructure or uses digital technology (Marsiela et al., 2023). Meanwhile, digital attacks becoming a trend during 2022 are hacking experienced by journalists and DDoS targeted at media organization sites. The biggest hack in all the recording of digital attacks was experienced by 37 Narasi editorial staff from 24-29 September 2022 (Sinaga, 2022). The hacking and attempted hacking of Narasi's media crew spanned multiple platforms such as Facebook, Instagram, Telegram, and Whatsapp accounts. The editorial crew that became the target came from various levels, from the editor-in-chief, managers, finance department, and producers to reporters. The hacking occurred on the WhatsApp number belonging to Akbar Wijaya or Jay Akbar, a Narasi producer, on Friday, 23 September 2022. He received some unknown links via Whatsapp at around 15.29 WIB. Even though Jay did not click on any of the links in the text message, 10 seconds later, he had lost control of his account or personal Whatsapp number. Not only the WhatsApp account, but Jay also cannot access the private phone number. Since then, the social media accounts of Narasi's editorial team have been hacked one by one. Those who have implemented more stringent digital security can prevent or take over their digital assets more quickly after receiving notification of another party's attempt to take over their account. Apart from the Narasi editorial staff, five other hacking incidents were experienced by journalists from CNN Indonesia, Jaring.id, the Chairperson of AJI Indonesia, as well as the YouTube account Suara Kita and the Facebook account Nuusdo.

The alternative media actively voicing the rights of women and minority groups, Magdalene.co and Konde.co, also reported that their sites and social media were attacked until they were inaccessible. Magdalene.co suffers a DDoS (distributed denial-of-service) attack, which is an attack by flooding the internet network traffic on servers, systems, and networks which makes the site inaccessible. Meanwhile, the digital attack on Konde.co-occurred on Monday, October 24, 2022, after writing news about a rape at the Ministry of Cooperatives and Small and Medium Enterprises (UKM) (Adinda, 2021). The Konde.co site was inaccessible after receiving a DDoS attack and was only entirely normal on October 26, 2022. During those two days, the editors were hampered from publishing other articles and incurring extra costs to pay IT, consultants, install additional devices, and replace damaged plug-ins. The primary loss fell on the public because it was difficult to access information, especially regarding stories of the steep path of sexual violence survivors seeking justice.

This cyber attack occurs on ordinary days and can increase during political momentum or ahead of the 2024 Election. It is feared that cyber-attacks against journalists will increase. Digital attacks are a new threat to the press's independence and journalists' safety. The story of journalist Detik, Isal Mawardi, became the target of anger from government supporters because his news was also one of the victims of cyber-attacks. Isal's data is widely distributed on social media with the aim of damaging reputation (doxing) (Yuniati, 2023).

Every year journalists receive various attacks by perpetrators from state and non-state actors. The Journalist Safety Index 2023 scores 59.8 out of 100 or falls into the 'Somewhat Protected' category. This score is partly contributed by the number of violence experienced by journalists both collected through surveys and from cases handled by the Alliance of Independent Journalists (AJI) throughout 2023. Through a survey of 536 respondents, 45% of respondents claimed to have experienced violence. Meanwhile, AJI data shows that the number of violence against journalists reached 87 cases, up 16 cases from the previous year. The most common forms of violence are coverage prohibition (45%), news prohibition (44%) and terror and intimidation (39%). The survey also noted that one journalist can experience various forms of violence and female journalists are more vulnerable. Threats to journalists' safety come from various parties. When asked about potential safety threats, journalists mentioned mass organizations (29%), the state through the police (26%) and government officials (22%), political actors (14%) and the media company itself (7%). The remaining 4% mentioned other actors (MediaIndonesia.com, 2024). Uli Parulian Sihombing, Coordinator of the Sub-Commission on Human Rights Enforcement of Komnas HAM, revealed that from 2018-2024, there were seven cases of violence reported to Komnas HAM, five cases of verbal violence and two cases of torture, five cases of defamation and violations of the ITE Law (Feisal, 2024). However, the protection mechanisms provided by state institutions to protect journalists who are victims of violence, such as the availability of emergency assistance, safety funds, or legal assistance, are not visible

The protection mechanism is still the initiative of civil society organizations such as AJI, LBH Pers, and the Journalist Safety Committee. The Press Council does have a mechanism to protect journalists from criminalization, marked by an MoU with the Police and this year has been followed up with a cooperation agreement (PKS) on the protection of press freedom (Dewan Pers, 2022). In addition, there is no mechanism for quick response and comprehensive protection if a journalist is still punished for his journalistic work, such as no hotline that is easily accessible to victims of criminalization, no litigation funding assistance, no lawyers provided by the Press Council, and how litigation advocacy provided by the Press Council so that the Police stop criminal cases. On the other hand, media organizations are also considered to have not provided holistic protection for their journalist.

As online activities are increasingly inseparable from the work of journalists, digital security, at least the most basic, is becoming a necessity. When journalism penetrates the internet, journalists are required not only to be able to adapt to digital ways of working but also to understand that risks to security and privacy are higher than before. Therefore, journalists are considered essential and urgent to implement digital security to reduce risk (mitigation). Seeing the background of this problem, the researcher considers that research on digital safety for journalists is essential.

METHODS

This study uses a qualitative method described descriptively with a phenomenological approach. Phenomenological research is a philosophical approach that explores an experience's meaning. The object, event, or condition is called a phenomenon and is the study of phenomenology. As a scientific method, phenomenology shows how to formulate knowledge through certain stages where the subject of study is a phenomenon experienced by humans, as he/she experiences it through thoughts, imagination, emotions, desires and so on (Hasbiansyah, 2008; Tamangkeng & Maramis, 2022).

Researchers used an interpretive phenomenological approach or Interpretative Phenomenological Analysis (IPA). The approach put forward by Jonathan Smith in 1996 is an approach in which data is obtained and studied in-depth (Sudarsyah, 2013). At the same time, the paradigm used is the constructivist paradigm. According to Guba and Lincoln, this paradigm seeks to see a phenomenon as a result of social construction that is specific and relative (Hajaroh, 2010).

The subjects of this research are journalists who work for various mass media in Central Java. This subject is intended to learn about the implementation of digital security, carried out while working through in-depth interviews. The criteria for research subjects are:

a) Journalists who have worked for more than five (5) years.
b) Journalists whose working area covers the whole of Central Java
c) Journalists from various mass media platforms.
d) Journalists with specific experience related to cybersecurity.

The informants were interviewed personally and through a Forum Discussion Group. The theme of the FGD was "Cybersecurity Literacy in The Journalistic Work Process". Personal interviews were conducted via direct phone calls and face-to-face opportunities, as well as email. Each informant produced different data according to their experiences with cybersecurity. The data analysis technique used in data analysis uses the Smith, Flowers, and Larkin models. Namely, the steps taken after the data is collected are as follows: (1) Reading and re-reading; (2) Initial recording; (3) Developing emerging themes; (4) Looking for relationships between emerging themes; (5) Moving to the next cases; and (6) Looking for patterns between cases. Each stage of analysis is described as follows:

(1) Reading and re-reading

After transcribing the audio interviews into written form. The researcher conducted the reading process repeatedly and continuously. This is done to avoid the process of interpretation or interpretation that is wrong or seems hasty so that the analysis process becomes less sharp or even inappropriate. Repeated reading allows researchers to find interesting data and then mark it either to explore further in the next interview process or to analyze further.

(2) Intial Recording

Initial noting or initial recording by analyzing data in the context of semantics and using the informant's language. There are three categories in initial noting: making descriptive comments, linguistic comments, and conceptual comments. Initial noting or marking the transcript is that after the transcript process, the researcher marks the data that the researcher finds interesting or interesting findings and is related to the research focus. This is done to identify what is expressed by the participant, which is a description of the phenomenon, be it feelings, understanding, or the participant's point of view. At this stage, the researcher can provide comprehensive and detailed comments on the data.

(3) Develop emerging themes

The next step is to conduct a theme or coding process which is then developed into themes. The material or information that has been obtained from informants is selected in accordance with the research objectives, then the researchers interpret it. At this stage there is no attempt to remove or select certain parts because of special attention, so that the entire transcript is addressed as data. At the same time there was no requirement to theme all the words, the number of themes that emerged reflected the richness of the section in question. The coding process was carried out using the Nvivo tool, however, the coding must be done by the researcher first so that this is not a technical part done by Nvivo.

Coding is needed to process data, which is preceded by analytical thinking by the researcher. The process of giving codes to words, phrases, sentences, or paragraphs that represent the code is called coding. Codes are in the form of concepts or terms. First cycle coding departs from field data, with codes that represent the conditions as they are. After that, second cycle coding is carried out, namely codes that are born from the process of generalizing field conditions. These two stages move dynamically so that they can maximize results. In Nvivo, the space for coding is named as nodes. Nodes are used to classify the data in this research.

Files related to this research that have been imported are then read to find the sentences to be analyzed. There are 3 files used for data processing in Nvivo, namely 1 file of personal informant interviews, 1 file of written interviews, and 1 file of transcripts of informant interviews through Focus Group Discussions (FGDs).

Based on these files, sentences are found which are then grouped according to the nodes created. This feature will make it easier for researchers to review the literature, as well as to classify the data used in their research. The nodes that have been determined to get visualization results are as follows:

1. Doubt about digital security guarantees
2. Doubt about legal protection
3. Have received threats of personal attacks
4. Stay professional but also remain vigilant
5. Have secured personal accounts
6. Have not secured personal accounts / ignored
7. There is no security guarantee from the media company/workplace
8. Have experienced data leaks and been harmed
9. There is no security mechanism from the workplace
10. Cybercrime happens unexpectedly
11. High awareness of securing personal and corporate media accounts
12. High awareness of personal data leakage but helplessness

The data that has been classified is then processed using the Query feature. This feature contains Text Search facility to search for the same words in some data, while Word Frequency to search for words that often appear either in 1 nodes or all data, and Word Tree to see the relationship tree between words that often appear with other words. Query is a suitable feature to analyze the tendency of words written by someone in their social media

The most frequent words that appear are "digital" mentioned 17 times, "security" 16 times, "own" 12 times, "assurance" 11 times and "reporting" 10 times. These are the top 5 most frequently found words. The further down the table you go, the fewer times the word is mentioned. Next, the recorded data was visualized in a word cloud. The words with the largest size are the most frequently occurring words as recorded in the word frequency. The further to the edge, the less mentioned. This word cloud then becomes a guide or understanding of the existing data, not the final result of the analysis.

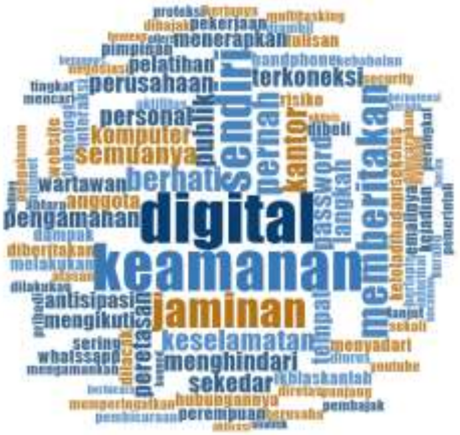

Figure 1. Data visualization in Word Clou

Through the Nvivo, the data analysis step using Interpretative Phenomenological Analysis (IPA) can simultaneously work on the fourth stage

(4) Look for relationships between themes

Namely searching for connections a cross emergent themes or the next stage that relates emerging themes as well as working on the fifth stage

(5) Move on to the next case

namely moving the next cases. The order used initially is the chronological order in which the themes appear. Then the next stage is sorting with a more analytical or theoretical nature, with the aim of finding relationships between emerging themes until the final stage of analysis is to look for patterns that emerge between cases / informants. From the coding through the nodes in NVivo, major themes or message content can emerge which is the essence of the informant's interview. The message themes that emerged were:

a. Personal threats in journalistic work
b. Journalists' security guarantees from media companies
c. Awareness of personal and company digital data security

(6) Look for patterns between cases.

After conducting five stages of analysis, common themes were finally found. The first theme is personal threats in journalistic work. This theme was obtained from repeated statements related to work threats both directly and digitally, insecurity after sensitive coverage and hacking of the personal social media accounts of the journalists concerned. The second theme in general is the guarantee of digital security from each informant's media company. This was built from a series of statements regarding the absence of protection from media companies related to the safety of journalists after coverage, media companies not willing to bear the risks of their journalists, and unclear handling and follow-up of existing cases. The third theme that patternically emerged from the interviews was awareness of personal and corporate digital data security. This emerged from informants' statements about the efforts made by journalists after the hacking of personal accounts, and the anticipation of cybercrime

RESULT AND DISCUSSION

Experience of Journalists Related to Cyber Security in Carrying Out Journalistic Duties.

Based on the data analysis that has been carried out, the researcher records statements from the informants' real experiences while carrying out their journalistic duties. Researchers also asked whether they had ever received cyberattacks while carrying out their duties as journalists. Informants with various experiences answered them, but most said they had received cyberattacks and threats. The following is a quote from an informant who stated that he had received threats that led to personal losses because someone hijacked his WhatsApp (WA) account.

> *“My WA was hacked - apparently it was related to the coverage related to flashbacks to the G.30 S PKI case. At that time, suddenly my WA was pending for a long time, it was difficult to get out and it was difficult to enter or exit WA. Finally I changed my number and deleted my number. That's my experience, okay?"*

As a result of this incident, the informant suffered losses because the source's contact and all chat history on the WhatsApp application related to his work had to be lost because he changed or even deleted numbers. The impact of the cyber threat on his account made the informant decide not to re-install WhatsApp and use another chat application, namely Signal.

The professional risk of a journalist who experiences threats while carrying out his journalistic duties also occurs directly. Journalists sometimes experience double threats, such as cyber-attacks and direct mental terror. This was also expressed by an informant who told about the case of his best friend who was terrorized after writing about criticizing the authorities.

> *"There is also the experience of a friend of mine whose FB was hacked. My friend is a blogger who often criticizes the government. Inbox messages on FB can also be pending for a long time. In fact, it was finally discovered that the messages that entered his inbox didn't arrive until the following year. My friend also got a call from an unknown number and he didn't know where the number came from. On the other end of the phone, a woman's voice questioned my friend and indicated that she knew exactly what my friend was doing. For example, the woman's voice says "oh sir, your house is here, right?" "So it was like threatening, he called but he was able to state in detail my friend's house, starting from what RT RW, down to the house number."*

The experiences of other informants who work in online media also show that the threats that occur after reporting are not only experienced by themselves. It was as if it was familiar and commonplace when a source gave an early warning of the results of his coverage.

> *"If it's actually normal with friends, what becomes a threat is that when we interview, the source sends a message via WhatsApp "mbok ojo has been reported" or "how can you say that? Yes, even though we already have guarantees under the Press Law, we can only think about security too. We report something wrong, if we don't report it, it's wrong because we are journalists, our job is to report. So you really have to be careful."*

Messages with threats sometimes do not appear in the form of sentences that suppress and terrorize but can also use sentences that are felt to be soft but still put pressure on journalists not to be reckless in writing and reporting. Terror or threats also appear in the form of calls to messages on WhatsApp and telephone calls to journalists' private numbers, which are also used as work tools.

> *"If it's about personal security after coverage or perhaps advocacy, there's a little story, namely right after the Regional Deliberation or Musda finished. There are around 50 unknown numbers coming to members, WA and telephone. Yes, I don't know, maybe it's a kind of terror or something like I don't know, what's clear is that it also makes me feel uncomfortable."*

It is undeniable that carrying out journalistic duties professionally in the new media era has increasingly complex challenges. As described in the experience of journalists facing threats after field coverage, this is not in line with Law Number 40 of 1999 concerning the Press. Article 4 of the Press Law No. 40 of 1999, paragraph 2 states, "the national press is not subject to censorship, banning or banning of broadcasting." The Press is free from precautions, prohibitions, and/or suppression so that the public's right to obtain information is guaranteed. Censorship, banning, or prohibition of broadcasting does not apply to print and electronic media. Broadcasts that are not part of the implementation of journalistic activities are further regulated by the provisions of the applicable law (Pers, 2021). The article provides an opportunity for the Press and every citizen to use the opportunity to distribute information and ideas as widely as possible. However, in reality, in the reporting process or early stages of collecting field data, a journalist must face various threats. For journalists in the current cyber era, threats to press freedom, apart from an authoritarian system of power, can also come from society. There are still groups in society whose interests are disturbed by freedom of the Press. They try to do things that threaten press freedom.

Guaranteed Digital Security from Each Informant's Media Company.

In this section, informants from various mass media platforms share their experiences related to the lack of protection from media companies. The protection referred to, on average, talks about the impact of post-coverage by journalists. Several cases of account hacking that had to be suffered by journalists ended up just being ordinary chats in the newsroom. The following is a statement from an informant (informant 2) who works in online and print media.

> *"If we talk about it officially, no way. Discussions about security were only informal. Most of the time, friends just talk about it, formally, I don't mean in an editorial meeting. Personally, when dealing with cases, I prefer to chat face to face with my redpel, the redpel are already seniors, they are more experienced. But sometimes I also chat with city friends too, younger ones too."*

Editorial leaders and in charge who are aware of the incident also rarely discuss personal security measures from cyber-attacks and do not provide a Standard Operational Procedure (SOP) so that journalists are guaranteed calm and security while on duty.

> *"Regarding security guarantees from media companies, it could be said that there are none, at least sharing"*

Meanwhile, experience with the theme of security guarantees provided by media companies has also developed on the issue of decision-making responsibilities regarding the hierarchy in the newsroom. One of the informants stated that there had been a case of burglary in a bank account by one of his co-workers, which resulted in bills that were not supposed to be paid by the person concerned because he had indeed not purchased several bills that had soared beyond his ability to pay at the market place. The co-worker of this informant suddenly received a bill of Rp. 18 million rupiah. Even though he only bought an item with a value that was not that big, up to tens of millions of rupiah. The informant's colleagues then asked the leaders for help to solve the problem, but in the end, they also could not get it.

> *"Finally, I went to the office, had a meeting with the office, and reported to my superiors and the superiors raised their hands, meaning they didn't provide protection or guarantees. In fact, the people who have the problem - sorry - are not people who have a lot of money, not rich people. Maybe the leadership saw that what my friend bought had nothing to do with office work so the office felt there was no need to help."*

From within the editorial office itself, the responsibility and protection of the editor-in-chief or media company for journalists who have been hacked or cyber-violent in several cases that have occurred is lacking or even non-existent. Meanwhile, the informants also assessed the aspect of legal protection from the government or the state as a step that was still shy and barely followed up. One of the informants (informant 1) questioned the follow-up of the cyber-attack case that hit the "Narasi News" website.

> *"Finally the question arises, are we actually safe or not? Everyone wants to send news using technological devices, but is technology itself safe or not? An example is the "NARASI" case that happened previously, 11 people were hacked. The device is not safe, the application is not safe, you already know it is not safe, so what should the follow-up be? but until now it's never been found out who hacked it. Narrative. Or when public policy activists used to speak, it was true that it was proposed, it was also reported... but we know there was no follow-up action. It's not tracked down... or it's taken care of further... there's no such thing, right... That means there's no guarantee of safety. There are actually other cases, such as site piracy, which are rarely tracked. This means there is also no guarantee of security."*

Awareness of Personal and Corporate Digital Data Security (Strategy)

From interviews with informants, it was found that not all journalists had made efforts to prevent cyber-attacks/violence. Out of the eight journalists interviewed, only three (3) journalists have implemented double security for their accounts-minimum security to prevent WhatsApp leaks or hacking as a communication application that supports work. The following is a statement from informant two, who secured his account after threats and terror occurred.

> *“I personally sometimes don't secure my personal accounts. I realize I often forget this. Sometimes it's lazy, it's complicated because as women we are multitaskers, so it's like we don't have time, just ignore it. Sometimes when you go to the shop or buy something like that, you are asked for a telephone number, just give it. Now, let's think again, okay?"*

It is different with informant one, who has tried to secure his account to support personal safety.

> *"For personal activities, what is needed is to take 2 security steps. For WhatsApp, apart from using fingerprints, every activation also requires authorization. From WhatsApp itself it also actually suggests it. Avoid hacking attempts. "Email is not just a password, but also where it is connected from, for example if we use a computer in a public place, especially, everyone has to be careful."*

Informant 2, who had experienced hacking of his WhatsApp account, stated that he is now more careful in anticipating protecting his identity in mobile applications and social media on his digital devices.

> *"When it comes to email, I secure it via a complicated password, for example my child's name is long and I think that's enough to keep my email safe."*

From the side of media companies, steps to anticipate cyber attacks are carried out after the attack. It is because the average incident is categorized as an unexpected event even though they have taken some security measures as an anticipatory strategy. The security strategies implemented by media companies, as explained by informant 4.

> *"This happened not just once but up to 2-3 times, so for our own protection, we implemented several models. There is a 3-step double security and it is not certain that we can guarantee the security of our website either, because thieves are always more advanced in looking for loopholes. Well, that's just the same as our own website, even people like the government's website can be hacked. That's why we have to anticipate and manage ourselves carefully, even though sometimes it happens again."*

Media companies also carry out website security or digital security strategies on various scales, bearing in mind that the impact is very detrimental to business and achievements. Losing an account cause losing followers or audience from the media automatically. Therefore, cyber security is carried out by companies in various ways and in layers to anticipate attacks or hacks.

> *"Our media is still small. Not very powerful yet. For website security there are 3 applications. One way is through two-step authentication. Meanwhile, access to analytical data is only given to a few people, then backing up any important data must be backed up either by journalists because we never know, recording it on their cell phone will only be a hassle. The website is also backed up. There have also been times when some content was lost, whether it was hacked or not, because IT didn't even know. Since that incident, in our office there is always a back up for everything, including billing, the website is also backed up. News is backed up because if it's lost it won't come back. Websites are given additional protection."*

The era of digital journalism is evidence of Mc Luhan's Theory of determinism. This era is an extension of human interests that require speed. Therefore, there are cases of digital attacks that affect the cyber security of each mass media company, as well as being a "double-edged knife." On the one hand, online media, the internet, and the speed of information are currently helping human needs. However, on the other hand, if hacking or digital attacks occur, they may also affect the image or reflection of the credibility of a mass media company. However, the media is the main factor influencing other things because each has different and unique characteristics. From the various opinions of informants, journalists' digital security strategies are essential things that ideally get significant attention. Informant 7 stated that if the media company where he works wants to provide training, then as a worker, he also has the right to be protected and get knowledge. Informant seven (7) also stated that his office had never provided cyber safety training for its workers.

> *"Regarding digital safety guarantees from my media company, there are none, especially digital security."*

Informant two (2) also expressed his desire to protect himself through the opportunity to increase his cybersecurity knowledge.

> *"Personally, I feel I have to update my knowledge about digital security by taking part in workshops"*

CONCLUSION

Based on in-depth interviews with informants, it was found that the patterns of themes and the interrelationships between themes were the flow of data processing using Interpretative Phenomenological Analysis (IPA). To get connected themes, the researcher uses the help of the NVivo 12 Plus tool, namely by doing a series of coding first. From the coding that was done, it was found that the word that was mentioned the most and most frequently was "digital" 17 times, "security" 16 times, "self" 12 times, "guarantee" 11 times, and "report" 10 times. These are the top 5 most frequently encountered words. Coding through the nodes in NVivo raises major themes or message content which is the essence of interviews with informants. The message themes that emerged were: (a) Journalists experience feelings of insecurity when doing sensitive coverage. They feel anxious about threats from sources and parties related to the source of the news. Threats are also made by hacking into journalists' personal social media accounts; (b) Regarding digital security guarantees, journalists admit that they have not received protection from the media companies where they work regarding the safety of journalists after coverage. Media companies do not want to bear the risks of their journalists, so there is no clarity or good handling when a case occurs; (c) Journalists are finally starting to realize the security of personal and company digital data by starting to install security or double passwords in each journalist's personal account.

From these themes emerged connectedness that converged into research finding and answering research questions. Personal threats experienced by journalists in connection with their journalistic duties occur because journalists also have not secured accounts in their various applications. Not all journalists who become informants have carried out security because they previously felt it was unnecessary. Of the eight (8) informants interviewed in-depth, only three had secured their accounts to support their journalistic work. Threats of violence or terror and even hacking of accounts belonging to journalists reflect a reality that is not in line with Law Number 40 of 1999 concerning the Press. Article 4 of the Press Law No. 40 of 1999, paragraph 2 states, "the national press is not subject to censorship, banning or banning of broadcasting." Terrorizing or threatening journalistic work means preventing journalists from working professionally.

Meanwhile, another connection is the guarantee of digital security from each informant's media company. Based on the informants' experience, personal and media company security is carried out after a cyber-attack. Anticipatory steps are non-linear, with the potential for digital attacks that can occur anytime. Media companies have also not provided a Standard Operational Procedure (SOP) for cybersecurity for their journalists or media companies. Therefore, there is still a need for awareness regarding cyber security in the journalism profession, bearing in mind that, to this day, there still needs to be maximum protection and follow-up action against cyber-attacks. Journalists also consciously need additional knowledge regarding digital security as one of the steps to anticipate cybercrime.

REFERENCES

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/

Annur, C. M. (2023). *Ada 61 Kasus Kekerasan terhadap Jurnalis pada 2022, Pelakunya Mayoritas Polisi*. https://databoks.katadata.co.id/datapublish/2023/12/12/ada-61-kasus-kekerasan-terhadap-jurnalis-pada-2022-pelakunya-mayoritas-polisi#:~:text=Menurut data Aliansi Jurnalis Independen,media%2C serta 14 organisasi media.

Dewan Pers. (2022). *Siaran Pers Dewan Pers-Polri Tanda Tangani Kerja Sama Perlindungan Kemerdekaan Pers*. https://dewanpers.or.id/publikasi/siaranpers_detail/580/Dewan_Pers-Polri_Tanda_Tangani_Kerja_Sama_Perlindungan_Kemerdekaan_Pers

Feisal, R. (2024). *Komnas HAM: Jurnalis Paling Banyak Melapor Terkait Kekerasan yang Dialami*. https://manado.antaranews.com/berita/248388/komnas-ham-jurnalis-paling-banyak-melapor-terkait-kekerasan-yang-dialami

Hajaroh, M. (2010). Paradigma, pendekatan dan metode penelitian fenomenologi. *Jurnal Pendidikan Universitas Negeri Yogyakarta*, 1–21.

Hasbiansyah, O. (2008). Pendekatan Fenomenologi Pengantar Praktik Penelitian. *Mediator*, *9*(56), 163–180.

Marsiela, A., Can, E., Faisol, E., Ningtyas, I., Musdalifah, Afrida, N., & Sasmito. (2023). *Serangan Meningkat, Otoritarianisme Menguat: Laporan Situasi Keamanan Jurnalis Indonesia 2022*. https://aji.or.id/data/serangan-meningkat-otoritarianisme-menguat-laporan-situasi-keamanan-jurnalis-indonesia-2022

MediaIndonesia.com. (2024). *45% Jurnalis Pernah Mengalami Tindak Kekerasan*. https://mediaindonesia.com/politik-dan-hukum/661934/45-jurnalis-pernah-mengalami-tindak-kekerasan

Pers, D. (2021). *Undang-undang No 40 tahun 1999*. https://dewanpers.or.id/kebijakan/peraturan.

Rahmanda, S. K. (2023). *AJI: Kekerasan Terhadap Jurnalis Meningkat, Siapa Pelaku dan Kota Mana Kasus Tertinggi?* https://nasional.tempo.co/read/1771386/aji-kekerasan-terhadap-jurnalis-meningkat-siapa-pelaku-dan-kota-mana-kasus-tertinggi#:~:text=Pada tahun 2021%2C AJI mencatat,66 kasus kekerasan terhadap jurnalis.

Sinaga, T. M. (2022). *Serangan Digital terhadap Media dan Jurnalis Ancam Kebebasan Pers*. https://www.kompas.id/baca/humaniora/2022/10/27/serangan-digital-terhadap-media-dan-jurnalis-mengancam-kebebasan-pers

Sudarsyah, A. (2013). Kerangka Analisis Data Fenomenologi (contoh analisis teks sebuah catatan harian). *Jurnal Penelitian Pendidikan*, *13*(1).

Tamangkeng, S. Y. L., & Maramis, J. B. (2022). Kajian Pendekatan Fenomenologi: Literature Review. *Jurnal Pembanguan Ekonomi Dan Keuangan Daerah*, *23*(1), 14–32.

Yuniati, I. (2023). *Kebebasan Pers di Bawah Bayang-Bayang Kekerasan Digital*. https://news.solopos.com/kebebasan-pers-di-bawah-bayang-bayang-kekerasan-digital-1552202