E-ISSN: XXXX-XXXX
P-ISSN: XXXX-XXXX
VIDYANTARA
Jurnal Humaniora dan Ilmu Sosial
https://lenterajournals.com/index.php/VJHIS

Cyberflashing as a Form of Online Gender-Based Violence: Its Impact on User Behavior X

Clarrise Michelle Effendi[1], Louise Alberto Emmanuel[2], Muhammad Rafif Dzakwan Rafa[3], Shakila Nur Azzah Afifa[4], Vanessa Elvaretta[5], Abdul Haris Faisal[6]
Program Studi Manajemen, Universitas Multimedia Nusantara, Indonesia[1,2,3,4,5,6]
Corresponding author: clarrise.michelle@student.umn.ac.id

Abstract

This study examines the phenomenon of cyberflashing as a manifestation of Online Gender-Based Violence that is increasingly prevalent on Platform X (formerly Twitter), with a focus on differences in responses between male and female victims. The research methodology employs a qualitative-descriptive approach through data triangulation, including the distribution of questionnaires, social media content analysis, document studies, and in-depth interviews. The participants consist of 25 respondents, all of whom have experienced cyberflashing. The findings reveal that the majority of victims respond with defensive strategies, such as blocking perpetrators and adjusting account privacy settings. Additionally, significant psychological impacts were identified, including feelings of disgust, fear, and trauma. A comparative analysis indicates that female victims tend to exhibit more intense emotional reactions and take more proactive measures compared to male victims.

Keywords: Cyberflashing, Online Gender-Based Violence, X, Communication Privacy Management

Abstrak

Penelitian ini mengeksplorasi fenomena *cyberflashing* sebagai salah satu manifestasi Kekerasan Berbasis Gender *Online* yang semakin prevalen di platform X (sebelumnya dikenal sebagai aplikasi Twitter), dengan fokus pada perbedaan respons antara korban laki-laki dan perempuan. Metodologi penelitian menggunakan pendekatan kualitatif-deskriptif melalui triangulasi data, meliputi penyebaran kuesioner, analisis konten media sosial, studi dokumen, dan wawancara mendalam. Partisipan penelitian terdiri dari 25 responden yang semuanya memiliki pengalaman sebagai korban *cyberflashing.* Temuan penelitian mengungkapkan bahwa mayoritas korban merespons dengan strategi defensif, seperti memblokir pelaku dan memodifikasi pengaturan privasi akun. Selain itu, ditemukan dampak psikologis yang signifikan, termasuk perasaan jijik, ketakutan, dan trauma. Analisis komparatif menunjukkan bahwa korban Female cenderung menunjukkan reaksi emosional yang lebih intens serta mengambil tindakan yang lebih proaktif dibandingkan dengan korban laki-laki.

Kata Kunci: *Cyberflashing*, Kekerasan Berbasis Gender *Online*, X, *Communication Privacy Management*

Introduction

In the rapidly evolving digital era, human interaction often occurs through social media and online communication platforms. Communication in the modern world is increasingly shifting from in-person to online formats, thus acquiring characteristics such as virtuality, transience, multidimensionality, anonymity, isolation, and so on (Doni, 2023). The transition from in-person to online communication is facilitated by technological advances that transcend geographical boundaries. However, despite the benefits of ease of communication, social media also has a significant impact on cybercrime (Baizat et al., 2022).

One increasingly prevalent form of digital crime is Online Gender-Based Violence, which not only impacts individual privacy but also affects users' sense of security and behavior online. Online Gender-Based Violence is an act of gender-based violence that utilizes digital technology for sexual or financial gain (Moulita et al., 2023). This form of violence reflects how gender norms and power operate in the digital world. Along with the increasing use of social media, the trend of Online Gender-Based Violence cases has also seen a significant spike. Based on the SAFENet Indonesia (Southeast Asia Freedom of Expression Network) report, the number of complaints of Online Gender-Based Violence in the last three years.

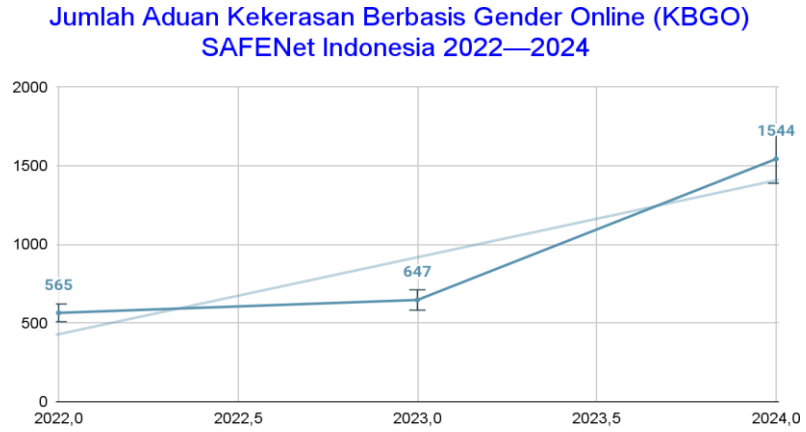


Chart 1. Number of KBGO Complaints from SAFENet Indonesia 2022-2024
Source: SAFENet Indonesia

Based on data reported by SAFENet Indonesia, the number of complaints of Online Gender-Based Violence increased from 2022 to 2024. In 2022, 565 reports were recorded, which then increased to 647 reports in 2023. This upward trend became even more significant in 2024, with the number of reports reaching 1,544 cases. This data reflects that GBV was reported by individuals of various genders, indicating that this phenomenon is not limited to one specific group. With the increasing number of reports each year, further study is needed to understand its characteristics and impact on victims' online behavior.

Online Gender-Based Violence in the digital realm takes various forms, evolving with technological advances. A study by De Araújo et al. (2022) identified nine main categories of Online Gender-Based Violence: digital dating abuse, revenge porn, sexting, online misogyny, digital sexual harassment, gender-based hate speech, cyberbullying, sextortion, and the distribution of aggressive photos. These various forms of online gender-based violence not only threaten victims' safety online but can also impact their

mental and social health.

The increase in cases of online gender-based violence contributes to gender inequality in the digital space, which contradicts Sustainable Development Goal (SDG) 5, which aims to achieve gender equality and empower women and girls (United Nations, 2015). SDG 5 emphasizes the importance of eliminating all forms of violence against women in public and private spaces, including technology-based violence. However, the reality of online violence shows that this form of violence can also be experienced by individuals of all genders, including men, although with different patterns and impacts. Therefore, it is important to examine how victims of different genders respond to and deal with this form of violence. Furthermore, this phenomenon is also related to SDG 16 (Peace, Justice, and Strong Institutions), which emphasizes legal protection and access to justice for all individuals without discrimination (United Nations, 2015). This includes victims of sexual violence in the digital realm.

One form of online gender-based violence that has become increasingly prevalent with the rise in social media use is cyberflashing, the sending of images of genitals without the other person's consent. This harassment often occurs in digital spaces that enable instant communication, such as social media platforms. The term cyberflashing is derived from the words "cyber," which refers to technological practices, and "flashing," which means the act of indecently exposing body parts. A study by McGLYNN and Johnson (2021, p. 2) shows that the majority of cyberflashing perpetrators are men who send images of their genitals without prior consent or agreement.

Cyberflashing often occurs through direct messages or anonymous file sharing. Twitter, now known as X, has become a primary platform for cyberflashing due to its text-based nature, image-based nature, and its Direct Message (DM) feature, which allows for instant communication. Furthermore, its open algorithms and high degree of anonymity are often exploited by perpetrators to send indecent content without immediate consequences. This situation not only disrupts users' comfort while interacting on social media but can also have various psychological impacts on victims, ultimately influencing their online behavior in response to cyberflashing.

While cyberflashing is often associated with the experiences of female victims, studies on the responses of male victims are still limited. Most studies focus more on the psychological impacts and resilience strategies employed by women, while men's experiences in dealing with cyberflashing are rarely discussed. Previous research conducted by Athirah and Hidayana (2023) from the University of Indonesia explored women's agency and resistance to cyberflashing on Twitter, highlighting how women interpret their experiences and the resistance they employ. However, this research did not address the experiences of male victims or compare responses by gender. Therefore, a more inclusive analysis is needed to understand how gender differences influence responses to cyberflashing on social media, particularly on platform X. Given the increasing number of cyberflashing cases on social media, it is crucial to understand how victims, both female and male, respond to this form of harassment in the digital space. This study aims to analyze gender differences in responses to cyberflashing in X, as well as its impact on victims' online behavior. The findings of this study are expected to contribute to efforts to raise public awareness in line with the Sustainable Development Goals (SDGs), particularly SDG 5 on gender equality and SDG 16 on peace, justice, and strong institutions (United Nations, 2015).

The literature review in this study covers the definition and phenomenon of cyberflashing on social media, as well as its relationship to the Sustainable Development

Goals (SDGs), particularly in the prevention of digital sexual violence. A theoretical approach is used to analyze changes in victim behavior, including Communication Privacy Management Theory, which explains how individuals manage privacy boundaries after online harassment.

Over time, cybercrime has become increasingly prevalent, one of which is cyberflashing. Cyberflashing, the sending of sexually explicit images or videos without the recipient's consent, is a form of Online Gender-Based Violence. Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence, specifically Article 14 concerning the threat of punishment, is expected to provide justice and legal protection for victims (Salsabila, 2023).

SDGs No. 5. "Gender Equality aims to achieve gender equality and empower all women and girls. This includes the elimination of all forms of discrimination and violence against women" (Sudirman & Susilawaty, 2022). In this context, cyberflashing is a form of online sexual harassment that violates an individual's right to privacy and security. It can cause psychological trauma, shame, and profound fear in victims.

SDG No. 16 "Peace, Justice, and Resilient Institutions" aims to build peaceful, just, and inclusive societies for sustainable development and provide access to justice for all (Febri, 2021, p. 2). In this context, cyberflashing, as a form of online sexual violence, causes victims to experience psychological trauma, fear, and feelings of insecurity, and compromises security in digital spaces.

Communication Privacy Management Theory (CPM), developed by Petronio (2002), suggests that individuals operate within a framework of normative constraints and a number of criteria that influence their decisions to disclose personal information. These criteria encompass a broad spectrum of cultural factors. such as culture (customs, norms, religion), gender (expression and dress), motivation (drives and feelings), context (appropriateness and positive impact), and consideration of risks and benefits. In this context, cyberflashing can be conceptualized as a very serious and significant privacy violation, forcing victimized individuals to revise their privacy rules regarding the control of the information they possess (Kamilah & Lestari, 2020). Disclosure of personal information is dialectical, where people make choices to reveal or conceal information based on criteria and conditions they deem important. This theory also states that individuals fundamentally believe that they have the right to own and regulate access to their personal information (Petronio, 2002). The consequences of these violations often result in privacy turbulence, which can encourage victims to reduce their activity on social media platforms such as X or even block the perpetrator's account..

Method

This study employs a qualitative approach utilizing descriptive analysis methodology grounded in postpositivist philosophy (Sugiyono, 2013) to obtain in-depth and meaningful data regarding victims' experiences of cyberflashing on social media and their responses to such incidents. The research population consists of users of social media platform X, both male and female, who have experienced cyberflashing. As Sugiyono (2017) defines, population represents a generalization area comprising objects or subjects with specific characteristics determined by the researcher. In this context, the general population includes all platform X users regardless of gender, while the target population specifically comprises individuals who have experienced cyberflashing on this

platform. The sampling technique employed nonprobability sampling, selecting participants based on relevance, availability, and willingness to participate.

Data collection was conducted through social media analysis, document studies, questionnaires, and semi-structured interviews. Social media analysis and document studies were used to examine public discourse and relevant literature, while questionnaires and in-depth interviews served to explore victims' experiences and expert perspectives. Data analysis followed the stages of data reduction, data presentation, and conclusion drawing, focusing on patterns of behavioral changes among victims regarding privacy protection, digital interactions, and resistance strategies.

Social media analysis was employed to examine user behavior patterns and interactions (Murthy, 2018), while document studies analyzed relevant academic literature, articles, and reports concerning digital harassment (Bowen, 2009). Questionnaires were used to collect written data about participants' experiences and responses, as this instrument can systematically measure opinions, attitudes, and participant characteristics (Creswell, 2014). Additionally, interviews with gender experts were conducted to obtain direct and contextual information (Kvale & Brinkmann, 2009).

The data analysis process followed Brannen's (2005) stages: data reduction, organized narrative presentation of data, and drawing preliminary conclusions that remain open to modification based on new findings. The analytical focus examined patterns in victims' online behavioral changes, including account privacy protection, digital social interaction modifications, digital resistance strategies, and migration to alternative social media platforms.

Results and Discussion

This section presents the main findings of the research, obtained through questionnaires, document studies, social media analysis, and interviews with expert sources. The discussion begins with a presentation of the questionnaire data to provide an overview of the respondents' profiles and their response tendencies to the phenomenon of cyberflashing. This data serves as the basis for understanding emotional reaction patterns, changes in digital behavior, and differences in perception between male and female respondents. The discussion then proceeds thematically according to the analytical focus designed in the research.Tabel 1 Data Responden

No.	Initials	Age	Gender
1.	EDF	19	Male
2.	J	21	Male
3.	KZS	19	Female
4.	TD	19	Female
5	MIH	22	Male
6	SS	19	Female
7	AY	20	Female
8	GA	22	Female
9	ID	24	Female
10	RY	20	Female
11	AP	20	Female
12	NS	23	Female

No.	Initials	Age	Gender
13	NL	23	Female
14	AZ	19	Female
15	SS	22	Female
16	HR	23	Female
17	NA	19	Female
18	TP	22	Female
19	LM	26	Female
20	WF	28	Female
21	BA	25	Male
22	DA	27	Male
23	AR	28	Male
24	BT	27	Male
25	LS	30	Male

The results of a survey of 25 respondents showed variations in the duration of daily use of Platform X. The majority of respondents (48%) reported spending between 3 and 4 hours per day. Twenty-eight percent of respondents used the platform for 1 to 2 hours per day, followed by 12% who spent 5 to 6 hours per day. Meanwhile, 8% of respondents used the platform for less than 1 hour, and only 4% accessed it for more than 6 hours per day. Regarding the primary purpose of using Platform X (respondents were allowed to select more than one), the survey of 25 respondents showed that "for entertainment" was the dominant choice, with 23 answers (92%). "For education/seeking information" and "To express opinions" were each chosen by 16 respondents (64%). On the other hand, "For work" was chosen by 4 respondents (16%).

68% of the 25 respondents stated that they did not recognize the account from the message they received. 28% of respondents knew the sender as a mutual or follower, while only 4% knew the sender personally. Regarding experiences with cyberflashing on platform X (Twitter), all respondents (100% of 25 respondents) stated they had experienced it.

When experiencing cyberflashing, the majority of respondents (68% of 25 respondents) had private accounts. Meanwhile, 32% of respondents had public accounts. Based on reports from the 25 respondents who experienced cyberflashing, the most common form of image received (64%) was an explicit image of genitalia. Twenty percent of respondents received photos of naked bodies, and 16% received illustrations or non-realistic sexual content.

A survey of the 25 respondents who experienced cyberflashing revealed various actions taken after receiving the image (respondents were allowed to select more than one). The most common actions were blocking the sender's account (21 respondents (84%)), ignoring the message (11 respondents (44%)), reporting the incident to platform X, and sharing the experience with friends/family, each chosen by 10 respondents (40%). Meanwhile, five respondents (20%) chose to speak up or create a "spill tweet." No respondents chose to reply to the message (0%).

After experiencing cyberflashing, some respondents (out of 25) experienced changes in their behavior when using platform X. Fifty-two percent of respondents chose to change their account settings to private. Furthermore, 32% of respondents opened platform X less frequently. Twelve percent of respondents reported no significant

changes, and 4% of respondents chose to delete their old account and create a new one with private settings to access information.

Of the 25 respondents, the majority (17 respondents, or 68%) reported that the perpetrator did not include a specific message or wording before or along with the image. However, eight respondents (32%) received messages that varied; from short, uncomfortable phrases like "look here" or "want to see a surprise?" to messages that were explicitly harassing, vulgar, contained profanity, or even promoted paid pornography. This demonstrates that cyberflashing incidents can occur with or without verbal harassment.

Upon first receiving the image, disgust was the most predominant reaction, experienced by 21 respondents (84%). Furthermore, 19 respondents (76%) felt shocked, and 8 respondents (32%) experienced fear. Other negative emotional responses included anger (6 respondents, 24%), confusion (2 respondents, 8%), and shock (2 respondents, 8%). Specifically, 1 respondent (4%) felt "harassed" and 1 respondent (4%) felt "invaded." Although 2 respondents (8%) reported their reactions as "normal," the vast majority expressed strong, negative emotional reactions to the experience.

Universally, all 25 respondents (100%) immediately took defensive action by blocking the sender. Furthermore, 17 respondents (68%) also reported the sender's account to the platform. Another common action was deleting the message or image (6 respondents, 24%). A small number of respondents (2 respondents, 8%) chose to share their story with friends or loved ones, seeking social support after the incident. Five respondents (20%) stated that they ignored the message after blocking.

Detailed responses revealed a strong tendency to immediately stop the interaction and report the incident. Seven respondents (28%) stated that they immediately blocked the sender's account because they felt uncomfortable and didn't need to respond. Furthermore, nine respondents (36%) explicitly stated that they blocked and reported the account simultaneously, often citing harassment or sensitive content. Five respondents (20%) also cleared their digital footprint by deleting messages or chat history. Only one respondent (4%) responded with insults before blocking, while four respondents (16%) chose to ignore messages after blocking. Two respondents (8%) sought support by sharing their stories with friends.

These cyberflashing experiences had a significant personal impact on most victims. Twenty-one respondents (84%) reported increased vigilance and caution in using social media. Furthermore, twelve respondents (48%) revealed emotional and psychological impacts such as paranoia, anxiety, insecurity, feelings of personal space being violated, trauma, overthinking, and persistent anger. One respondent (4%) even reported experiencing nightmares. Only 3 respondents (12%) stated there was no significant personal impact.

This cyberflashing experience significantly impacted how 22 respondents (88%) interacted on platform X. The most frequently mentioned behavioral change was becoming more selective in accepting DM requests and responding to mentions from strangers. A number of respondents also decided to limit DMs to people they follow or even lock their accounts and disable DM requests from non-mutuals. This reflects a tendency to withdraw from public interactions and become "silent readers," fundamentally changing their social media usage patterns. Only 3 respondents (12%) stated that this experience did not affect the way they use social media.

Perceptions regarding control over privacy following this incident were divided. Twelve respondents (48%) felt they retained control or increased their control through

stricter privacy measures such as privatizing their accounts. However, 10 respondents (40%) felt a loss of control or realized that control on social media was an illusion. They argued that despite tightened privacy settings, malicious intent from perpetrators and limited platform features remained a threat to their sense of security and privacy online. One respondent (4%) did not explicitly answer this question.

Regarding platform X's response to cyberflashing reports, the majority of respondents (13 respondents, or 52%) explicitly stated that the platform was not responsive enough. Complaints included automated responses without clear follow-up, the perpetrator's account remaining active, and a lack of transparency in the reporting process. Conversely, 10 respondents (40%) considered platform X to be sufficiently responsive due to the availability of account blocking and reporting features. One respondent (4%) was unaware of the platform's response because they did not report it.

Respondents provided several important suggestions for increasing awareness of cyberflashing and other forms of digital violence. Key recommendations include being cautious when posting personal content, maintaining account privacy, enabling privacy features that limit DMs from unknown individuals, and not hesitating to immediately block and report suspicious accounts. They also collectively emphasized the importance of not taking incidents lightly, speaking up and seeking support from trusted individuals, and understanding that victims are not to blame for the perpetrator's actions.

Practitioner's Perspective on Cyberflashing in the Context of Online Gender-Based Violence

In an interview, the Expert Resource Person, a practitioner active in issues of sexual and gender-based violence, provided an in-depth analysis of the phenomenon of cyberflashing within the framework of Online Gender-Based Violence. The Expert Resource Person emphasized that cyberflashing is a form of harassment because it does not require the consent of the recipient. He stated, "In my opinion, actions like sending unsolicited images of genitals are a form of harassment because they are non-consensual, and that's the most important thing."

The Expert Resource Person further emphasized that the definition of cyberflashing focuses on the perpetrator's act of sending the image without consent, regardless of the victim's emotional response. He stated, "Is it our emotions when receiving the image that determine whether it is cyberflashing or not? Or is it the act of sending the image without our consent that is called cyberflashing? Regardless of whether we like it or not, the act of sending unsolicited images is still unethical."

The Expert Resource Person also explicitly linked cyberflashing to Online Gender-Based Violence, stating:

> *"This falls under Online Gender-Based Violence, a form of gender-based violence that emerged due to the development of digital communication technology, especially after the 2000s. There are still few references to it in academic journals, as it is a relatively new issue."*

He emphasized that cyberflashing meets two key criteria for Online Gender-Based Violence: the lack of consent from the victim and the resulting negative impact:

> *"Yes, cyberflashing is definitely categorized as online gender-based violence because it meets two aspects of gender-based violence: the lack of consent from the victim and the resulting impact."*

Regarding the differences between online and offline flashing, the Expert Resource Person explained that victims' perceptions of risk differ in the two contexts:

> *"A person's reaction to online and offline cyberflashing can differ because of the concept of perceived risk. Online, the perpetrator feels more distant and unable to physically harm them, while offline, the risk feels more real."*

The Expert Source also highlighted the perpetrator's tactic of often concealing their identity through anonymous accounts:

> *"There are degrees of flashing, right? Some people only flash their genitals or genitals, so their faces and identities are unknown. They even use anonymous accounts. That means they still feel that it would be dangerous if people found out. But they still do it. The perpetrator could be anyone if that's the case. And the perpetrator has to be careful when doing that."*

In his observations, the Expert Source also found that cyberflashing isn't always an impulsive act:

> *"I've also encountered cases where cyberflashing wasn't just a prank, but part of a planned action or even a form of revenge. So, cyberflashing might not be the disease, but just a symptom."*

Regarding initial treatment for victims, the Expert Source recommended practical steps:

> *"From my experience as a practitioner quite active in sexual violence issues, the most basic response to cyberflashing is to block the perpetrator, report them, document the evidence, and, if necessary, involve a legal aid organization."*

He also highlighted technology's dual role in facilitating crime while also serving as a preventative tool:

> *"Technology is always a two-way street. It facilitates crime, but at the same time, it must also be able to prevent it. AI is now so advanced that it can identify whether an image is real or not."*

However, the Expert Source questioned the readiness of social media platforms to address this issue:

> *"Do social media platforms have strong policies for banning users or IP addresses of cyberflashing perpetrators? So, it can be prevented? Yes. But there need to be clear boundaries for what that prevention entails."*

Cyberflashing as a Form of Online Gender-Based Violence

Cyberflashing is a manifestation of Online Gender-Based Violence that frequently occurs in digital interactions, particularly on platforms with high levels of anonymity such as Twitter (now X). This anonymity allows perpetrators to easily conceal their identities, facilitating the sending of sexually explicit images or videos without the recipient's consent. An anonymous expert, a practitioner in the field of sexual violence and Online Gender-Based Violence, emphasized that cyberflashing is a form of harassment because it occurs without the victim's consent. The expert stated,

> *"Actions like sending unsolicited images of genitals are a form of harassment because they are non-consensual, and that's the most important thing."*

This principle of non-consensualism was directly evident in the experiences of the 17 female and 8 male respondents in this study. They consistently reported receiving

unsolicited images of genitals, confirming that cyberflashing is a completely one-sided act. For example, RY (female) described receiving the image accompanied by a text message that made her uncomfortable, such as "look at this." Similarly, EDF (Male) and several other male respondents also experienced the sudden, unsolicited sending of graphic images. The collective experiences of these victims clearly demonstrate that the essence of cyberflashing is a deliberate violation of consent, with explicit content being forced upon the recipient without their consent.

In the context of gender-based violence, cyberflashing fulfills two crucial elements that define GBV: the lack of consent from the victim and the resulting negative impact. The expert informant explained that in the context of gender-based violence, cyberflashing fulfills two crucial elements that define GBV: the lack of consent from the victim and the resulting negative impact. From a feminist criminology perspective, online GBV is understood as a form of violence perpetuated by gender-based power imbalances. Rossettini (2025) emphasizes that digital technology has become a tool for reinforcing this dominance, and that anonymity on digital platforms exacerbates this inequality by weakening perpetrator accountability.

Cyberflashing also demonstrates how victims' experiences and responses are strongly influenced by gender. Stevens et al. (2024) revealed that females are more frequently targeted by these acts than males and experience more significant psychological impacts. This is closely related to the social construct inherent in female bodies, which are often viewed as objects in public and digital spaces. An expert source stated,

> *"Cyberflashing is included in KBGO, a form of gender-based violence that emerged due to the development of digital communication technology, especially after the 2000s."*

Cyberflashing, the sending of sexually explicit images or videos without the recipient's consent, is a form of Online Gender-Based Violence. Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence, specifically Article 14 concerning the threat of punishment, is expected to provide justice and legal protection for victims (Salsabila, 2023).

Most of the 25 respondents (17 females and 8 males) expressed negative emotional reactions to these acts. For example, J (male) admitted to feeling "disgusted and angry," while TD (female) said she felt "disgusted, shocked, and goosebumps." This confirms that cyberflashing has a significant psychological impact on victims.

This phenomenon demonstrates that cyberflashing is not simply physical harassment, but a form of violence that violates individual privacy and rights in the digital realm. With technological advances and the anonymity offered by social media, cyberflashing has become increasingly easy to commit without any immediate visible consequences for the perpetrator. The experiences of respondents, both female and male, who generally did not know the sender of the image, illustrate how anonymity on digital platforms is exploited to commit transgressive acts. Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence, particularly Article 14 concerning the threat of punishment, is expected to provide justice and legal protection for victims (Salsabila, 2023).

Forms of Cyberflashing and Characteristics of Perpetrators

Cyberflashing is the sending of sexually explicit images or videos without the recipient's consent and is considered a form of Online Gender-Based Violence (KBGO). Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence, specifically Article 14 concerning the threat of punishment, is expected to provide justice and legal protection for victims (Salsabila, 2023, p. 2). Based on questionnaire data from 25 respondents (17 females and 8 males), the majority received explicit images of genitals (64%). Respondents such as EDF (male), KZS (female), AY (female), and LS (male) were all targets of unsolicited and vulgar visual content.

From the perpetrator's perspective, cyberflashing does not always occur impulsively but can be planned according to a specific pattern. This aligns with the findings of Henry and Powell (2015), who stated that perpetrators of technology-based sexual violence can act in a structured, planned manner, and are motivated by dominance or control over the victim. Even LS (Male) received "vulgar language and promotions about paid accounts for pornographic content," suggesting a deliberate economic intent. The expert informant also highlighted that cyberflashing perpetrators often attempt to maintain their anonymity, either by using anonymous accounts or by hiding their faces. This phenomenon is also related to toxic online masculinity, where anonymity on digital platforms is used as a shield to express aggressive and sexually dominant forms of masculinity (Barker & Jurasz, 2018). The experiences of respondents who generally did not recognize the sender support this assertion. Furthermore, AP (Female)'s experience of receiving the message "Yes, the message is 'want to see a surprise?'" before the image was sent suggests an element of psychological control, confirming that not all cyberflashing is impulsive but can also be manipulative.

Victims' Perceptions of Cyberflashing Experiences

The questionnaire, which involved 17 female and 8 male respondents, showed that victims' reactions to cyberflashing varied, but most experienced negative emotions. J (Male) felt "disgusted and angry," TD (Female) experienced "disgust, shock, and goosebumps," and RY (Female) felt "really shocked, disgusted, and a little scared because it was so sudden." Even though they didn't know the perpetrator, feelings of shock and discomfort still arose, indicating that cyberflashing can have not only physical but also emotional impacts.

Based on these statements, the perpetrator's act of sending an image without permission is enough to categorize the incident as cyberflashing, regardless of whether the victim felt threatened or not. This perspective aligns with the theory in Communication Privacy Management by Petronio (2002). This means that while emotional reactions may differ, a violation still occurs due to the unauthorized overstepping of digital privacy boundaries.

Emotional Impact and Changes in Online Behavior of Cyberflashing Victims

Cyberflashing not only affects victims' emotional well-being but also changes their social media habits. Based on a questionnaire from 17 female and 8 male respondents, it was found that after experiencing the incident, 52% of respondents chose to set their accounts to private. For example, AP (female) stated, "Yes, I've become very careful and decided to limit DMs to only people I follow." Meanwhile, 32% of respondents accessed the platform less frequently, as BA (male) stated, "I rarely open messages from strangers on X." These actions indicate fear and discomfort that impact the way victims interact online.

These changes can be explained through the concepts of media trauma, Communication Privacy Management (CPM) Theory, and perceived risk. In CPM theory (Petronio, 2002), individuals manage personal information by setting privacy boundaries. When a violation such as cyberflashing occurs, victims perceive a threat to their privacy and respond by restricting access (e.g., making accounts private or restricting direct messages) as a form of protection against potential further risks.

Victims interpret cyberflashing as a highly unpleasant and disturbing experience, often traumatic. The dominant initial responses are disgust, shock, anger, and fear, with some also experiencing goosebumps and disgust. The accompanying messages, often vulgar, harassing, or provocative, such as "look at this" or "want to see a surprise?", further reinforce the perception that this act is a form of harassment and a deliberate invasion of privacy. Thus, the significant emotional impact prompts changes in online behavior in victims, both male and female, as a form of self-protection against similar threats in the future.

Conclusion

Based on the results of this study, it can be concluded that cyberflashing is a form of Online Gender-Based Violence (OGBV) frequently experienced by users of platform X (Twitter), both female and male. Most respondents reported receiving sexually explicit content without consent, indicating that the digital space is far from safe for all users. Although cyberflashing is more often associated with female victims, these findings suggest that males also experience similar experiences, albeit with different patterns and impacts.

The differences in responses between males and females to cyberflashing are a key finding in this study. Females exhibited more intense emotional reactions, such as fear, disgust, shock, and even prolonged trauma, and were more likely to take active action, such as reporting the perpetrator. Meanwhile, males responded more neutrally, feeling indifferent, or simply blocking and ignoring the perpetrator. They were also less likely to change their account settings or report the incident. These findings suggest that gender constructs influence how victims process and respond to these invasive incidents.

Communication Privacy Management theory helps explain these differences by demonstrating how victims manage their privacy boundaries in the digital space. After experiencing cyberflashing, many women change their online behavior, such as making their accounts private or limiting direct messages (DMs), in an effort to regain control over the personal information that was breached. On the other hand, men generally feel they haven't lost control of their privacy, so they don't make many changes. Awareness that victimization isn't limited to one gender, and understanding how victims manage the impact, are important first steps in creating a safer and more inclusive digital ecosystem.

References

Athirah, S., & Hidayana, I. (2023). Women's agency and resistance to cyberflashing on Twitter. Masyarakat: Jurnal Sosiologi, 28(1). https://doi.org/10.7454/mjs.v28i1.13562

Baizat, F., Rahma, Z., & Abusaid, S. (2022). The dark side of IT: The negative aspects of information technology. International Journal of Technology and Systems, 1(1). https://doi.org/10.47604/ijts.1709

Barker, K., & Jurasz, O. (2018). Online misogyny as a hate crime. https://doi.org/10.4324/9780429956805

Bowen, G. A. (2009). Document analysis as a qualitative research method. Qualitative Research Journal, 9(2), 27-40. https://doi.org/10.1108/19410870910953548

Brannen, Julia. (2005). Memadu Metode Penelitian: Kualitatif & Kuantitatif. Yogyakarta: Fakultas Tarbiyah IAIN Antasari Samarinda & Pustaka Pelajar.

Connell, R. W., & Messerschmidt, J. W. (2005). Hegemonic masculinity: Rethinking the concept.

Creswell, J. W. (2014). Research design: Qualitative, quantitative, and mixed methods approaches (4th ed.). SAGE Publications.

De Araújo, A., Bonfim, C., Bushatsky, M., & Furtado, B. (2022). Technology-facilitated sexual violence: A review of virtual violence against women. Research, Society and Development, 11(2). https://doi.org/10.33448/rsd-v11i2.25757

Donii, V. (2023). Specifics of the communication space of modern social media. Mižnarodnij filologìčnij časopis, 14(3). https://doi.org/10.31548/philolog14(3).2023.09

Gender & Society, 19(6), 829–859. https://doi.org/10.1177/0891243205278639

H. Z. (2024). Women are less comfortable expressing opinions online than men and report heightened fears for safety: Surveying gender differences in experiences of online harms. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2403.19037

Henry, N., & Powell, A. (2015). Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. Australian & New Zealand Journal of Criminology, 48(1), 104–118. https://doi.org/10.1177/0004865814524218

Junior, K. G. (2021). Manajemen privasi komunikasi pengguna aplikasi kencan online "Tinder" di kalangan mahasiswa UNS. Jurnal Kommas. https://www.jurnalkommas.com/docs/Jurnal%20D0216052.pdf

Kamilah & Lestari (2020). Manajemen privasi pada pengguna media sosial Instagram. Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Diponegoro. https://ejournal3.undip.ac.id

Kvale, S., & Brinkmann, S. (2009). Interviews: Learning the craft of qualitative research interviewing (2nd ed.). SAGE Publications.

McGlynn, C., & Johnson, K. (2021). Cyberflashing: Recognising harms, reforming laws. Bristol University Press. https://www.amazon.com/Cyberflashing-Recognising-Harms-Reforming-Laws/

Misoch, Sabina. 2014. *Card Stories on Youtube: A New Frame for Online Self Disclosure. Media and Communication*. Vol.2 No.1. 2-12.

Murthy, D. (2018). Social media research: An introduction. SAGE Publications.

Muryatini, N. (2024). Perlindungan terhadap Female korban kekerasan berbasis gender online dalam era digital. *Jurnal Interpretasi Hukum, 5*(2), 969–976. https://doi.org/10.22225/juinhum.5.2.10396.969-976

Petronio, S. (2000). *The boundaries of privacy: Praxis of everyday life* (1st. Balan). Lawrence Erlbaum Associates Publishers.

Petronio, S. (2002). *Boundaries of Privacy:Dialectic of Disclosure*

Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior*, 28(5), 1859–1872. https://doi.org/10.1016/j.chb.2012.05.004

Rossettini, S. (2025). *Breaking the web of abuse: The realm of technology-facilitated gender-based violence*. European Student Think Tank.

Safenet. (2022, August). Analisis pelanggaran hak-hak digital triwulan II 2022.

Safenet. (2023, April). Laporan pemantauan hak-hak digital triwulan I 2023.

Safenet. (2023, August). Laporan pemantauan hak-hak digital triwulan II 2023.

Salsabila, N. A. (2023). *Cyberflashing dan hukum pidana di Indonesia*. Jurnal Ilmu Hukum, 8(2), 1–10.

Stevens, F., Enock, F. E., Sippy, T., Bright, J., Cross, M., Johansson, P., Wajcman, J., & Margetts,

Sudirman, F. A., & Susilawaty, F. T. (2022). Kesetaraan gender dalam tujuan pembangunan berkelanjutan (SDGs): Suatu reviu literatur sistematis. *Journal Publicuho, 5*(4), 995–1010. https://doi.org/10.35817/publicuho.v5i4.41

Sugiyono. (2010). *Metode penelitian kuantitatif, kualitatif dan R & D*. CV Alfabeta.

Syahda, A., & Ramaiah, A. (2024). Sexual violence in virtual world: The unaddressed legal protection issue for victims. *Neoclassical Legal Review: Journal of Law and Contemporary Issues, 2*(2). https://doi.org/10.32734/nlr.v2i2.14057