Council of the European Union
General Secretariat

Interinstitutional files:
2022/0155 (COD)

Brussels, 10 April 2024

WK 3036/2024 REV 2

LIMITE

JAI	**FREMP**
ENFOPOL	**TELECOM**
CRIMORG	**COMPET**
IXIM	**MI**
DATAPROTECT	**CONSOM**
CYBER	**DIGIT**
COPEN	**CODEC**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Presidency
To:	Law Enforcement Working Party (Police)
Subject:	Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse - draft methodology and criteria for the risk categorisation of services

The Presidency provides delegations in the Annex with a working document outlining the draft methodology and criteria for the risk categorisation of services to facilitate discussions at the meeting of the Law Enforcement Working Party (Police) on 15 April 2024.

ANNEX

Methodology and criteria for the risk categorisation of services

1. Scoring based on the size of the service

A. Services defined as "VLOPs" (= very large online platforms), and services defined as "VLOSEs" (very large online search engines)[1].

a. Definition: Online platforms and online search engines which have several average monthly active recipients of the service in the Union equal to or higher than 45 million, and which are designated as very large online platforms or very large online search engines

B. Other services

2. Scoring based on the type of service

Is the service one or more of the following service types?

A. Social media platform (services that connect users and enable them to build communities around common interests or connections)

B. Electronic messaging service *(service that is typically centered around allowing users to send messages that can only be viewed or read by a specific recipient or group of people)*

C. Online gaming service *(services that allow users to interact within partially or fully simulated virtual environments)*

D. Adult service[2] *(services that are primarily used for the dissemination of user-generated adult content)*

a. For instance, adult services could comprise one or more of the following services:
   i. Camming Services: These platforms facilitate the live streaming or webcam performances by individuals typically engaged in adult-oriented activities such as explicit conversations, striptease, or sexual acts for an audience.
   ii. Pornographic Websites: These are platforms that primarily host or distribute sexually explicit videos, images, or other adult content for viewing or downloading.

[1] Art. 33 and 34 of Regulation (EU) 2022/2065 (Digital Services Act).

[2] An "adult service" typically refers to an online platform or service that primarily deals with or facilitates the dissemination of adult content. This content may include, but is not limited to, explicit imagery, videos, or text that is intended for mature audiences and may contain nudity, sexual content, or explicit language. Adult services encompass a wide range of platforms, including adult websites, adult social media networks, adult chat rooms, adult streaming services, and adult dating or hookup platforms. These platforms are designed to cater to individuals seeking adult-oriented content, entertainment, or interactions. Note that adult services may vary in terms of the types of content they offer, the audience they target, and the services they provide. However, they share a common characteristic of providing access to adult-oriented material and often require users to confirm their age before accessing such content.

iii. Adult Gambling Services: These services involve online betting or gambling activities that are explicitly geared towards adults and may include adult-themed games or gambling content.
iv. Escort Services: These services connect individuals with escorts or companions for adult-oriented activities, which may include companionship, intimacy, or sexual services in exchange for payment.
v. Adult Social Networking Sites: These are platforms like mainstream social networking sites but cater specifically to adults interested in connecting with others for adult-oriented interactions, such as dating, casual encounters, or discussions about sexual topics.
vi. Adult Dating Services: These mobile applications focus on facilitating connections between adults interested in casual or intimate relationships, often emphasizing physical attraction and sexual compatibility, typically through profile creation, matching algorithms, and messaging features.
vii. Adult Content Subscription Services: These platforms offer access to exclusive or premium adult content through subscription-based models, providing users with a variety of adult-oriented media such as videos, images, or stories.

E. Discussion forum or chat room service *(services that allow users to send or post messages that can be read by the public or an open group of people)*

F. Marketplace or listing service *(services that allow users to buy and sell their goods or services)*

G. File-storage and file-sharing service *(services whose primary functionalities involve enabling users to store digital content and share access to that content through links)*

H. Web and server hosting services[3] *(services that provide individuals or organisations with the infrastructure and technology needed to host websites or web applications on the internet, including server space, bandwidth, and technical support).*

I. *Online search engines*[4]

J. *Services directly targeting children*

K. *Other information society services*[5]

[3] See also article 3 (g), point (iii) of Regulation (EU) 2022/2065.
[4] See article 3 (j) of Regulation (EU) 2022/2065.
[5] 'Information society service' means a 'service' as defined in Article 1(1), point (b), of Directive (EU) 2015/1535.

3. Scoring based on the core architecture of the service.

A. Does the service allow child[6] users to access a part or the entirety of the service?

YES/NO

B. User identification

1. Can users display identifying information through a user profile that can be viewed by others (e.g. images, usernames, age)?

   YES/NO

2. Can the platform be used anonymously?

   YES/NO

3. Can users share content anonymously (e.g. anonymous profiles or access without an account)?

   YES/NO

4. Are there functionalities that prevent users from accessing the website(s) in another geographic region where the legislation is less strict?

   YES/NO

5. Does the service require multi-factor authentication and user signup information, where users register for the service using a phone number, email address, or other identifiers?

   YES/NO

C. User connection

1. Can users connect with other users?[7]

   YES/NO

2. Can users form closed groups or send group messages?

   YES/NO

3. Can users search for other users by specific categories (place, gender, hobbies, etc.)?

   YES/NO

[6] Users not having reached the age of adulthood in the country of establishment of the service provider. The assessment of this criteria should consider not just whether children can access the site but whether they do access the site.

[7] 'User connection': a user-to-user service functionality that allows users to follow or subscribe to other users. Users must sometimes be connected to view all or some of the content that each user shares. (UK safety act)

D. *User communication*[8]

1. Can users communicate via livestreaming?

   YES/NO

2. Can users communicate via direct messaging (including ephemeral direct messaging)?

   YES/NO

3. Can users communicate via encrypted messaging (YES/ NO) and are there functionalities to "opt-in/opt-out"? [9]

   YES/NO

4. Can users post or send images or videos (either open or closed channels)?

   YES/NO

5. Can users re-post and forward content (either open or closed channels)?

   YES/NO

6. Can users share content via hyperlinks and plain-text URLs?

   YES/NO[10]

7. Can users comment on content (open and/or closed channels)?

   YES/NO

8. Can users post/share (visible) location information?

   YES/NO

9. Can users search for user-generated content?

   YES/NO

[8] These criteria have been presented ranked to help for the future scoring system (to be developed). These ranking places activities involving direct real-time communication (livestreaming, messaging) at the highest risk due to their immediate and potentially unfiltered nature. Encrypted messaging follows closely due to privacy concerns and the potential for misuse. Posting and sharing of multimedia content are also high-risk activities, as they can easily disseminate harmful material. Reposting, forwarding, and sharing via hyperlinks carry a moderate risk, while commenting, sharing location information, and searching for user-generated content are deemed lower risk, though they still warrant attention in terms of potential risks.

[9] Making design choices such as ensuring that E2EE is opt-in by default, rather than opt-out would require people to choose E2EE should they wish to use it, therefore allowing certain detection technologies to work for communication between users that have not opted in to E2EE.

[10] Link to encrypted services is often shared on unencrypted online spaces to facilitate the exchange of CSAM.

E. Does the service allow users to post goods and services for sale[11][12]?

1. Does the service allow the use of cryptocurrency to buy service/material (promotes anonymity)?

   YES/NO

2. Does the service allow for gift-card-related transactions?

   YES/NO

F. Does the service allow payments through its system?

YES/NO

G. Can users download/save/screenshot/screen video content?

YES/NO

H. Does the service apply recommendation algorithms?[13]

YES/NO

I. Possibility to limit the number of downloads per user to reduce the distribution of illegal content

- Absent
  - The platform lacks functionalities to limit the number of downloads per user to reduce the dissemination of harmful content.
- Basic
  - The platform has basic functionalities in place to limit the number of downloads per user to reduce the dissemination of harmful content. Their scope and effectiveness are limited.

[11] The UK online safety act includes this because: "*Potential perpetrators may try to promote illegal goods or services by posting them for sale using this functionality. Often illegal items such as drugs and firearms are posted for sale using code names. In certain contexts, the ability to post goods or services for sale, such as through user-generated advertisements, also enables potential perpetrators to advertise and broadcast the sexual services of adults in exploitative environments. The risk of harm can be increased if your services also allow users to make online payments directly.* "

[12] 'Posting goods and services': "*a user-to-user service functionality allowing users to post content dedicated to offering goods and services for sale. This does not include paid-for advertisements but may serve the function of allowing users to promote goods or services*." (UK online safety act).

[13] Algorithms that recommend content like that already viewed may potentially expose users to inappropriate content if they have already been exposed to child pornography.

- Effective
    - The platform has effective functionalities in place to limit the number of downloads per user to reduce the dissemination of harmful content. They significantly reduce the risk of the dissemination of harmful content, contributing to a safer online environment.
- Comprehensive
    - The platform has comprehensive functionalities in place to limit the number of downloads per user to reduce the distribution of harmful content. These robust measures leave minimal to no room for the dissemination of harmful content, thereby ensuring a safe online environment for users.

J. Storage functionalities

- Absent
    - The platforms' storage functionalities do not allow sharing information with law enforcement authorities.
- Basic
    - The platforms' storage functionalities allow sharing information with law enforcement authorities, but only for a limited amount of information and for a limited amount of time.
- Effective
    - The platforms' storage functionalities allow sharing information with law enforcement authorities for a large amount of information and for a long time.
- Comprehensive
    - The platforms' storage functionalities allow sharing information with law enforcement authorities for all information and for an indefinite period.

K. Functionalities preventing users from making recordings and screenshots of shared content or saving a local copy of shared content

- Absent
    - The platform lacks functionalities to prevent users from saving harmful content (by making recordings, screenshots etc.) for the purpose of the dissemination thereof (such as for example not allowing recording and screenshotting content shared by minors).
- Basic
    - The platform has basic functionalities in place to prevent users from saving harmful content (by making recordings, screenshots etc.) for the purpose of the dissemination thereof, but their scope and effectiveness are limited.

- Effective
    - The platform has effective functionalities in place to prevent users from saving harmful content (by making recordings, screenshots etc.) for the purpose of the dissemination thereof. These measures significantly reduce the risk of the dissemination of harmful content, contributing to a safer online environment.
- Comprehensive
    - The platform has comprehensive functionalities in place to prevent users from saving harmful content (by making recordings, screenshots etc.) for the purpose of the dissemination thereof. These robust measures leave minimal to no room for the dissemination of harmful content through saving, thereby ensuring a safe online environment for users.

4. Scoring based on policies and safety by design functionalities in place to address identified risks.

A. Effectiveness of CSA Risk Policies

- Absent
    - The platform lacks explicit policies specifically addressing child sexual abuse risks.
- Basic
    - While the platform has policies related to CSA risks, they are not regularly updated, and users find them unclear.
- Effective
    - Clear policies addressing CSA risks are in place, updated regularly, and users understand them.
- Comprehensive
    - The platform boasts explicit and user-friendly policies on CSA risks, which are not only regularly updated, but also enforced in a manner that users can easily comprehend.

B. Measures for Promoting Users' Media Digital Literacy and Safe Usage Scoring System

- Absent/limited
    - The platform does not offer (or only to a limited extent) educational materials dedicated to promoting media digital literacy (for example, links to educational information). The materials do not contribute to an observable user awareness of CSA risks.

- Basic
    - The platform offers some educational content dedicated to promoting media digital literacy. The materials only contribute to a limited extent to an observable adequate level of user awareness of CSA risks.
- Effective
    - The platform offers a robust set of educational content dedicated to promoting media digital literacy. The materials lead to an observable improvement in user awareness of CSA risks.
- Comprehensive
    - The platform offers a robust set of educational content dedicated to promoting media digital literacy. The materials lead to an observable improvement in user awareness and engagement. The commitment to fostering a deep recognizing of safe media usage is evident.

C. Definition of CSA in Terms of Services

- Absent/limited
    - Terms and conditions related to CSA risks are lacking or unclear, leading to potential misinterpretation by users.
- Basic
    - While terms are clear, the enforcement mechanisms related to CSA risks are weak and may not deter violations effectively.
- Effective
    - The platform has comprehensive terms addressing CSA risks, and enforcement is moderate.
- Comprehensive.
    - Terms are strictly enforced, and the platform is transparent about the consequences for violating CSA-related terms.

D. Functionalities enabling Users to Share Potentially Harmful Content

- Absent/Very Limited
    - Platforms lack adequate functionalities (for example: Hashing/photo DNA) to prevent the sharing of potentially harmful content by users. This absence raises concerns about the platform's ability to mitigate the dissemination of harmful material effectively.

- Limited
    - Platforms have limited functionalities to prevent users from sharing potentially harmful content. While some measures may be in place, they are not comprehensive, leaving room for the dissemination of harmful material.
- Effective
    - Platforms in this category demonstrate effective functionalities to prevent users from sharing potentially harmful content. These measures significantly reduce the risk of harmful material dissemination, contributing to a safer online environment.
- Comprehensive
    - Platforms in this category have comprehensive functionalities in place to prevent users from sharing potentially harmful content. These robust measures leave minimal to no room for the dissemination of harmful material, ensuring a safe online environment for users.

E. Possibility to use peer-to-peer downloading (allows direct sharing of content without using centralised servers)

- Absent
    - Platforms offer comprehensive support for peer-to-peer downloading, allowing seamless and efficient direct sharing of content among users, promoting decentralised distribution, and reducing reliance on central servers for content dissemination.
- Limited
    - Platforms provide effective support for peer-to-peer downloading, enabling users to directly share content without dependence on centralised servers, enhancing efficiency and user autonomy.
- Effective
    - Platforms offer limited support for peer-to-peer downloading, but it may not be widely available or may come with significant limitations, potentially increasing the risk associated with centralised content distribution.
- Comprehensive
    - Platforms lack the option for users to utilise peer-to-peer downloading, restricting direct sharing of content without relying on centralised servers.

F. Functionalities Assessment of Potential Dissemination Risks

- Absent
    - Platforms fail to assess potential dissemination risks associated with shared content adequately. This lack of assessment raises concerns about the platform's ability to proactively identify and mitigate dissemination risks, potentially exposing users to harmful content.
- Limited
    - Platforms conduct partial assessments of potential dissemination risks related to shared content. While efforts are made to evaluate risks, the assessment may not be comprehensive, leading to gaps in identifying and mitigating dissemination risks.
- Effective
    - Platforms conduct effective assessments of potential dissemination risks related to shared content. Through proactive evaluation mechanisms, these platforms identify and mitigate dissemination risks, contributing to a safer content-sharing environment.
- Comprehensive
    - Platforms conduct comprehensive assessments of potential dissemination risks related to shared content. With thorough evaluation processes in place, these platforms effectively identify and mitigate dissemination risks, ensuring a safe content-sharing environment for users.

G. Possibility to delete shared content for all users it has been shared with

- Absent
    - The service provider lacks the ability for children to delete shared content.
- Limited
    - The service provider has a limited functionality for children to delete shared content. Only for a certain period and under certain circumstances, avoiding the proper possibility of children to delete shared content when necessary.
- Effective
    - The service provider has a limited functionality for children to delete shared content. For an extensive period and under relevant circumstances, succeeding in allowing deleting shared content in most of the cases.

- Comprehensive
    - The service provider has an efficient functionality for children to delete shared content when necessary. For an extensive period and under every circumstance, succeeding in allowing deleting shared content in all relevant cases.

H. Systems for selecting and presenting advertisements

- Absent
    - The platform does not propose any safety by design functionalities on advertisement systems, like age-based ad filtering or parental control, allowing potentially harmful content to be shown to children.
- Limited
    - The platform proposes limited safety-by-design functionalities on advertisement systems, but it is not comprehensive enough to effectively prevent harmful content to be shown to children.
- Effective
    - The platform proposes effective safety by design functionalities that reduces the likelihood of harmful content being shown to children.
- Comprehensive
    - The platform provides comprehensive safety by design functionalities on advertisement systems that thoroughly prevent harmful content from being displayed to children.

I. Usage of Premoderation functionalities

- Absent
    - Platforms lack a premoderation system, allowing potentially harmful content to be posted without oversight or moderation.
- Limited
    - Platforms have a limited premoderation system in place, but it is not comprehensive enough to effectively filter out all inappropriate content.
- Effective
    - Platforms utilise an effective premoderation system that significantly reduces the likelihood of inappropriate content being posted, enhancing user safety.
- Comprehensive
    - Platforms have a comprehensive premoderation system in place that thoroughly screens all content before it is posted, minimising the risk of harmful content reaching users.

J. Usage of Delisting Content System

- Absent
    - Platforms lack a delisting content system, making it challenging to remove harmful or inappropriate content once posted.
- Limited
    - Some platforms have a limited delisting content system, but it is not consistently applied or may not effectively remove all inappropriate content.
- Effective
    - Platforms utilise an effective delisting content system that promptly removes harmful or inappropriate content upon identification, reducing its visibility to users.
- Comprehensive
    - Platforms have a comprehensive delisting content system that efficiently identifies and removes harmful or inappropriate content, ensuring a safer online environment for users.

K. Usage of Image Masking

- Absent
    - Platforms lack image masking capabilities, potentially exposing users to sensitive or explicit content without adequate protection.
- Limited
    - Platforms have limited image masking capabilities, but they may not be consistently applied or may not effectively conceal sensitive or explicit content.
- Effective
    - Platforms utilise effective image masking techniques that appropriately conceal sensitive or explicit content, enhancing user privacy and safety.
- Comprehensive
    - Platforms have comprehensive image masking capabilities in place that consistently and effectively conceal sensitive or explicit content, providing robust protection for users.

5. Mapping of user tendencies

A. Assessing User Patterns

- Absent
    - A portion of users demonstrate frequent engagement with content that could pose risks. This includes but is not limited to content that may be inappropriate, harmful, or potentially unsafe. A high frequency of user interaction with such content raises concerns about the overall safety of the platform.
- Limited
    - Platforms falling within this range demonstrate a certain level of user engagement with potentially risky content. While harmful activities are not widespread, occasional instances raise concerns about the need for enhanced moderation and content filtering mechanisms to ensure a safer environment for users.
- Effective
    - Users in this category engage with risky content in a limited manner. Instances of harmful activities are infrequent, suggesting a healthy user environment. However, ongoing monitoring and preventive measures are still essential to maintain this positive trend and further reduce potential risks.
- Comprehensive
    - This represents the most favourable scenario where users rarely engage in activities that pose risks. The platform enjoys an elevated level of user responsibility, and harmful content is a rare occurrence. This indicates a strong community's commitment to maintaining a safe and secure online environment.

B. Service's Popularity Among Different Age Groups

- Absent
    - The platform lacks adequate monitoring and assessment of its popularity among different age groups. There is a lack of data collection and analysis regarding user demographics, particularly related to age groups, raising concerns about the platform's understanding of potential vulnerabilities.
- Limited
    - Platforms have limited data on the popularity among different age groups. While there may be efforts to collect and analyse user demographics, the data may not provide an understanding of potential vulnerabilities associated with age groups.

- Effective
    - Platforms in this category effectively monitor and analyse the service's popularity among different age groups. Through comprehensive data collection and analysis, these platforms gain insights into user demographics, allowing for targeted risk assessment and mitigation strategies.
- Comprehensive
    - Platforms in this category have comprehensive monitoring and analysis of the service's popularity among different age groups. With data collection and analysis mechanisms in place, these platforms possess detailed insights into user demographics, facilitating targeted risk assessment and effective mitigation strategies.

C. Analysis of Grooming Risks Based on User Mapping

- Ineffective
    - Platforms fail to conduct a comprehensive analysis of solicitation risks based on functionalities and user mapping. This lack of assessment raises concerns about the platform's ability to proactively identify and mitigate solicitation risks, potentially exposing users to harmful interactions.
- Limited
    - Platforms conduct a partial analysis of solicitation risks based on functionalities and user mapping. While efforts are made to evaluate risks, the analysis may not be comprehensive, leading to gaps in identifying and mitigating solicitation risks.
- Effective
    - Platforms conduct an effective analysis of solicitation risks based on functionalities and user mapping. Through proactive evaluation mechanisms, these platforms identify and mitigate solicitation risks, contributing to a safer online environment.
- Comprehensive
    - Platforms conduct a comprehensive analysis of solicitation risks based on functionalities and user mapping. With thorough evaluation processes in place, these platforms effectively identify and mitigate solicitation risks, ensuring a safe online environment for users.

D. Analysis of tendencies based on account's information:

Use of Anonymous Account:

- **Frequent use of anonymous accounts**
  - Less than 25% of accounts have identifiable information.
- **Moderate instance of anonymous accounts.**
  - 25 to 60% of accounts have identifiable information.
- **Minimal or no use of anonymous accounts**
  - More than 60% of accounts have identifiable information

Consecutive and Repetitive De- and Re-Activation of Accounts

- **Frequent de- and re-activation patterns observed.**
  - More than 60 % of accounts undergo repetitive activation and deactivation.
- **Moderate instances of de- and re-activation**
  - 25 to 60 % of accounts undergo repetitive activation and deactivation.
- **Minimal or no repetitive de- and re-activation**
  - Less than 25% of accounts undergo repetitive activation and deactivation.

Fake or Imposter Accounts

- **Frequent fake or imposter accounts identified.**
  - Less than 25% are genuine accounts.
- **Moderate instances of fake or imposter accounts**
  - 25 to 60% are genuine accounts.
- **Minimal or no fake or imposter accounts**
  - More than 60 % are genuine accounts.

Identity Verification Tools for Opening Accounts

- **Lack of identity verification tools**
  - More than 60% of accounts can be created without verifying identity.
- **Moderate identity verification measures**
  - 25 to 60% of accounts can be created without verifying identity.
- **Comprehensive identity verification tools**
  - Less than 25% of accounts can be created without verifying identity.

Pseudonymity

- **Frequent Pseudonymous behavior**
  - More than 60% of users use aliases or pseudonyms.
- **Moderate instances of pseudonymity**
  - 25 to 60% of users use aliases or pseudonyms.
- **Minimal or no pseudonymous behavior:**
  - Less than 25% of users use aliases or pseudonyms.

Temporary Accounts

- **Frequent creation of temporary accounts:**
  - More than 60% of accounts are created for short-term use.
- **Moderate instances of temporary account:**
  - 25 to 60% of accounts are created for short-term use.
- **Minimal or no temporary account creation:**
  - Less than 25% of accounts are created for short-term use.

Frequent Changing of Account(s) or Profile Details:

- **High frequency of changing accounts or profile details:**
  - More than 60% of users update account(s) information/ details at least every 7 days.
- **Moderate instances of changes:**
  - 25 to 60% of users update account(s) information/ details at least every 7 days.
- **Minimal instances or no changes of accounts:**
  - Less than 25% of users update account(s) information/ details at least every 7 days.

Unmatching or Defriending Victims on Social Media Accounts

- **Frequent unmatching or defriending of victims observed:**
  - More than 60% of users maintain consistent social connections.
- **moderate instances of unmatching or defriending:**
  - 25 to 60 % of users maintain consistent social connections.
- **Minimal or no unmatching or defriending:**
  - Less than 25% of users maintain consistent social connections.

Switching Between Private and Public Platforms

- **Frequent switching between private and public platforms:**
  - More than 60% of accounts switch between private and public settings.
- **Moderate instances of platform switching:**
  - 25 to 60 % of accounts switch between private and public settings.
- **Stable behavior with minimal platform changes:**
  - Less than 25% of accounts switch between private and public settings.

Moving Public Conversations to Private Channels

- **Frequent movement from public to private channels:**
  - More than 60% of users often transition discussions from public to private spaces.
- **Moderate instances of conversation shifts:**
  - *25 to 60 % of* users often transition discussions from public to private spaces.
- **Minimal or no movement to private channels:**
  - Less than 25% of users often transition discussions from public to private spaces.

Obfuscation of I.P. Addresses

- **Frequent use of VPN or proxy servers to mask IP addresses:**
  - More than 60 % of users employ VPNs or proxies and don't typically use their real IP addresses.
- **Moderate instances of IP address obfuscation:**
  - 25 to 60% of users employ VPNs or proxies and don't typically use their real IP addresses.
- **Minimal or no obfuscation of IP addresses:**
  - Less than 25% of users employ VPNs or proxies and don't typically use their real IP addresses.

Use of Unsecure Public WIFI Hotspots

- ***Frequent use of unsecure public WIFI hotspots:***
  - *More than 60% of users connect from unsecured public networks.*

- ***Moderate instances of connecting to unsecure WIFI:***
    - *25 - 60 % of users connect from unsecured public networks.*
- ***Minimal or no use of unsecure public WIFI:***
    - Less than 25% *of users connect from unsecured public networks.*

Creation of Private Group or Chatboxes

- **Frequent creation of private groups or chatboxes:**
    - More than 60% of users create private communication spaces and groups.
- **Moderate instances of creating private spaces or chatboxes:**
    - 25 to 60 % of users create private groups for communication.
- **Minimal or no creation of private groups or chatboxes:**
    - 25% of users predominantly engage in public communication.

"Cyber Flashing" (Unsolicited Intimate Messages)

- **Frequent incidents of cyber flashing:**
    - More than 60% of users send unsolicited intimate messages.
- **Moderate instances of unsolicited intimate messages:**
    - 25 to 60% of users send unsolicited intimate messages.
- **Minimal or no incidents of cyber flashing:**
    - Less than 25% of users send unsolicited intimate messages.

E. Number of reporting during the previous period[14]

- **Large amount of reporting during the previous period:**
    - More than 160% of reports compared to the current period.
- **Moderate amount of reporting during the previous period:**
    - Between 125 to 160% of reports compared to the current period.
- **Minimal amount of reporting during the previous period:**
    - Less than 125% of reports compared to the current period.

---

[14] The number of NCMEC reports being made in respect of a service. These reports provide a stable indicator of what services and platforms are being used for CSA.