

Harassment As Infrastructure

How Telegram's design enables technology-facilitated gender-based violence in Italy and Spain.

AI FORENSICS



Table of content

Table of content	2
Executive summary	2
Credits	5
Disclaimer	5
Introduction	6
1. Context	7
1.1 The growth of technology-facilitated gender-based violence	7
1.2 Telegram as a preferred platform for image-based sexual abuse	8
1.3 Italy and Spain as comparative case studies	9
2. Methodology	10
2.1 Data collection	11
2.2 Ethical considerations	12
2.3 Qualitative analysis	12
2.4 Quantitative and network analyses	12
2.5 Limitations	14
3. Results	14
3.1 The scale and architecture of the network	14
Italian context	15
Spanish context	17
3.1.1 Shared links across countries	18
3.1.2 Shared message senders across countries	20
3.1.3 Shared media across countries	21
3.2 A taxonomy of violence	23
3.3 Types of perpetrators	29
3.4 Types of victims	32
3.5 Telegram as a cross-platform infrastructure for abuse	33
3.6 An organized economy of abuse: automation, archives, and monetization	39
The automatization of violence	39
Monetization practices	43
4. Telegram's role	53
5. Recommendations	54
5.1 National level (Italy and Spain):	55
5.2 European level:	56

Executive summary

This report presents findings from the first systematic, cross-national analysis of Telegram communities dedicated to inciting technology-facilitated gender-based violence (TFGBV) in Italy and Spain. Drawing on nearly **2.8 million messages** collected across 16 different groups and channels over a period of six weeks, the study reveals that what is commonly framed as peer-to-peer misconduct is, in reality, a **structured, monetized, and largely automated ecosystem of abuse** operating at scale:

- Across the two national contexts, researchers identified **24,671 active users perpetrating violence** (accounts sending at least one message during the observation period), with individual groups reaching 27,000 members in Italy and 25,000 members in Spain.
- Abusive material does not remain confined to linguistic or geographic borders. 72% of Spanish content also appeared within Italian groups, while **8% of all media files were seen circulated across both national environments**.
- Perpetrators are **predominantly young heterosexual men**, who exploit Telegram's infrastructure, including features available through its Premium subscription, to organize content through tagged folders, deploy automated bots, and charge for access to private archives and channels.
- Non-consensual content is often monetized through one-time fees of **€20-€50 for lifetime access to full channels and archives of abusive material**, or recurring monthly subscriptions starting at €5. Payments for these services are typically organized through **digital payment systems**, including PayPal, cryptocurrencies, and Bizum.
- These archives contain not only non-consensual intimate images but also **child sexual abuse material (CSAM)** and content depicting incest and rape.
- Among the most sought after and advertised services within these communities are **nudifying bots**, i.e., tools that generate synthetic non-consensual intimate imagery (NCII) from non-intimate source images or audios. The growing use of automation has scaled up the volume, speed, and ease with which TFGBV can be perpetrated, lowering barriers to participation and expanding the pool of potential victims.
- **Victims are predominantly women**, and include partners, acquaintances, and former partners of perpetrators, as well as public figures, particularly

influencers. Victims are often named, tagged, and locatable via shared profile links. Non-consensual sharing of intimate content often intersects with **cyberharassment** practices, the use of **spyware** and **hacking tools, gamified forms of violence,** and **doxing.**

- Telegram is used as a repository and redistribution layer for content extracted from other platforms: TikTok is the most frequently cited source, mentioned **19,625 times** across the dataset. Instagram appears **2,181 times,** frequently in connection with direct links to personal profiles or screenshots of private conversations; dedicated channel sections exist for the redistribution of private exchanges originating from **Instagram and WhatsApp. Reddit** also emerges as a key source, used to disseminate invitation links to Telegram channels. This cross-platform continuity, combined with the large-scale, structured, monetized, and largely automated abuse ecosystem, requires a more holistic approach to limit image-based sexual abuse (IBSA).

During the observation period, several groups were shut down by Telegram only to reopen under the same names just a few hours later, suggesting that Telegram's moderation mechanisms are insufficient. We reported the most recent, available links of all Telegram channels identified in the study directly to Telegram.

Credits

Project Lead: Dr. Silvia Semenzin, Salvatore Romano

Research & Report: Silvia Semenzin, Natalie Kerby, Miazia Schüler, Salvatore Romano

Data collection: Mario Baldi, Silvia Semenzin

Policy and Recommendations: Silvia Semenzin, Katya Viadziorchyk

Publication Review and Approval: Salvatore Romano

Many thanks to Jacinto Gutiérrez Lorca (UCM) for supporting the data collection.

All other content (c) AI Forensics 2026 | <http://aiforensics.org/>

The contribution from AI Forensics is funded by core grants from [Open Society Foundations](#), [Luminate](#), and [Limelight Foundation](#).

Email : info@aiforensics.org

Social Media: [Linkedin](#) | [Bluesky](#)

Disclaimer

This technical report is based on an experiment conducted in December 2025 under macOS Tahoe 26.1, the underlying model and guardrails could have evolved since. We acknowledge that manual errors may have occurred, and we do not claim to have carried out an exhaustive analysis of all biases that Apple Intelligence may harbor. We refer the reader to the companion scientific article for further details about the methodology and results [LINK]. Finally, at no point does this report provide, attempt to provide, or purport to offer a legal assessment of non-compliance with applicable regulations.

Introduction

In February 2019, Italian journalist Luca Zorloni [published an investigation in *Wired Italy*](#) exposing an extensive network of private Telegram groups and channels where thousands of users were collecting and sharing non-consensual intimate images of women and girls, many of them minors, and many of them former or current partners of the men sharing the images. The scandal prompted great outrage in Italy, contributing to the approval of a law criminalising the non-consensual sharing of intimate content (Art. 612-ter c.p.), but it did not stop the practice.

In the years that followed, similar networks came to light in France, Germany, Portugal, Spain, and beyond, yet the public and media response to each new revelation tended to focus narrowly on the perpetrators, often framing them as deviant or pathological individuals, and rarely questioning why these networks kept reappearing on the same platform across different countries, largely undisturbed. In doing so, the potential responsibility of Telegram itself — its design choices, its moderation failures, and its role as an enabling infrastructure — remained almost entirely out of the conversation.

This report returns to this persistent, disturbing issue, presenting the findings of a systematic analysis of Italian and Spanish Telegram groups and channels where non-consensual intimate images continue to circulate today alongside many other forms of technology-facilitated gender-based violence (TFGBV). The two countries have been selected because both present rich Telegram ecosystems in which the phenomenon can be systematically documented, and because their broadly comparable socio-legal contexts — as Southern European countries that have each recently criminalized image-based abuse — allow us to look at the patterns identified across the two cases in unison rather than merely parallel descriptions.

The report documents how these practices have not simply persisted but also evolved and adapted to the environment offered by the platform, responding to moments of public scrutiny by **privatizing violence** and integrating new AI tools to shape new forms of **automated abuse**. It also reveals a troubling **economic dimension** that has received almost no attention in policy or public debate. In both the Italian and Spanish contexts, the analyzed users do not only share abusive content targeting women and girls, but increasingly monetize it through archives and packs of non-consensual images, access to private channels with illegal content, AI-generated intimate content, and tools and services for partner surveillance. This points to a double layer of economic activity: perpetrators profiting from the abuse of women and girls, and Telegram itself indirectly (and unintentionally) but structurally profiting from the scale and engagement these networks generate on its platform.

Finally, this report demonstrates that TFGBV practices and the norms that sustain them **are not restricted by national borders or platform boundaries**. In observing TFGBV practices across platforms and countries, what we find is a dynamic problem, in which a set of abusive practices are actively shaped by, and in turn shape, the sociotechnical environment that Telegram provides. The same dynamics, content typologies, and user behaviors appear in both Italy and Spain, pointing to a structural problem that is European in scope and demands a European response. By refocusing on platforms' responsibilities, rather than on individual users' conduct, this report aims to contribute to a more effective policy exchange about what it will take to make online spaces safer for women and girls.

1. Context

1.1 The growth of technology-facilitated gender-based violence

Technology-facilitated gender-based violence (TFGBV) refers to acts of gender-based abuse that are committed, assisted, or amplified through digital technologies¹. In recent years, TFGBV has emerged as a global human rights challenge, fueled by the rapid expansion of social media platforms, messaging services, and algorithmically driven content ecosystems.

Reports from international organizations consistently show rising patterns of online harassment, non-consensual image sharing, cyberstalking, and coordinated abuse campaigns. These forms of violence disproportionately target women and girls, as well as journalists, activists, and politicians with a public voice. According to UNESCO, [73% of women journalists](#) have experienced online violence in the course of their work, while global surveys suggest that [58% of women and girls](#) have experienced some form of harassment on social media.

Across Europe, institutions increasingly recognise TFGBV as both a digital safety issue and a threat to democratic participation. According to the [European Institute for Gender Equality](#), **one in three** women in the European Union (EU) has experienced some form of sexual violence since the age of 15, including cyberviolence. However, data collection remains uneven across member states, and many incidents likely go unreported due to stigma, limited legal recourse, and the normalization of misogynistic behavior online.

¹ UN Women 2023:

<https://unric.org/en/how-technology-facilitated-gender-based-violence-impacts-women-and-girls/>

At the same time, online misogyny [has amplified](#) with the growing visibility of anti-feminist and far-right online communities that use digital platforms to spread misogynistic narratives, coordinate harassment campaigns, and mobilize against gender equality policies. Altogether, these dynamics have created an online environment where gender-based abuse can scale rapidly and circulate across borders, producing a significant chilling effect on women's participation in the digital realm.

1.2 Telegram as a preferred platform for image-based sexual abuse

TFGBV occurs across a wide range of online spaces and platforms. Recent scandals, such as [the Grok deepfake controversy](#) exposed by AI Forensics or the Facebook group "[Mia Moglie](#)" where allegedly 30,000 users shared non-consensual intimate images of their wives and girlfriends, demonstrate that even the platforms most exposed to regulatory scrutiny such as the Digital Services Act (DSA) continue to be used for gender-based violence. This also raises serious concerns about the situation for platforms that fall outside or at the margins of the DSA's regulatory reach: what kind of obligation do they have to prevent such abuse? Telegram is an instructive case, a platform with [over one billion monthly active users](#) that has not been the subject of a DSA investigation by the European Commission yet, compared to its Very Large Online Platform (VLOP) counterparts.

Across Europe, media investigations and civil society organizations have documented large Telegram communities dedicated to the circulation of abusive material. [In Portugal](#), media and civil society reporting has drawn attention to a Telegram group with more than 70,000 members that circulated non-consensual intimate images of women. [In Germany](#), a comparably large group was identified in 2024 in which users shared suggestions on how to rape and assault women. In France, the association [StopFisha](#) has repeatedly denounced the presence of IBSA²-focused Telegram groups, noting that the largest of these has been reported to reach approximately 233,000 members. Together, these cases illustrate how the issue of large, networked Telegram communities distributing image-based sexual abuse (IBSA) content is not just episodic.

[Previous research](#) has described Telegram as an especially enabling environment for the circulation of non-consensual intimate content and the normalization and

² IBSA is an umbrella term that is increasingly preferred to "revenge porn" because it captures a wider range of harms: not only the sharing of intimate images without consent, but also their creation, theft, and manipulation, as well as harassment perpetrated through non-consensual sexual content (for example, cyberflashing).

scaling of IBSA, owing in large part to the platform's specific technical affordances. Telegram combines strong privacy features — including end-to-end encrypted messaging and pseudonymous accounts — with large-scale distribution capabilities, shaping the conditions under which abusive behaviour can develop with a relatively high sense of security and impunity. Moreover, the platform supports group chats of up to 200,000 members and channels with unlimited audiences, facilitating the rapid circulation and replication of large volumes of content across interconnected networks. These structural features are further compounded by Telegram's Premium subscription tier, which grants users access to a wider number of channels, faster download speeds, promotional tools for their own channels, and enhanced content organization features — capabilities that can serve to professionalize and systematize the distribution of abusive material. All of this goes to show that the conditions enabling IBSA on Telegram are therefore, to a significant degree, embedded into the platform's architecture and business model, though it is important to note that these same features reflect deliberate design choices prioritizing user privacy, and that their role in facilitating IBSA should not be taken as evidence that enabling such harm is, in itself, the platform's intent or purpose.

1.3 Italy and Spain as comparative case studies

Italy and Spain provide two particularly relevant, complementary national contexts for examining the evolution of Telegram-based abuse networks. Both countries have seen significant public debate around TFGBV, yet each has followed a distinct institutional and political trajectory in responding to it, providing an analytically rich basis for comparison.

In Italy, IBSA has unfolded across an interconnected ecosystem of platforms and spaces, with Telegram groups operating alongside external archives, such as "[La Bibbia](#)", and repositories of stolen material, frequently including content depicting minors. Despite growing media attention, and even the approval of a law to criminalize the non-consensual sharing of intimate images in 2019 (Art. 612 ter c.p. inserted in the so-called "Red Code"), these networks continued to expand in scale and organization. In August 2025, the forum [Phica.net](#) was shut down following a public callout on social media; at that point, the platform counted over 700,000 registered users and had become an extensive hub for the cataloging and circulation of non-consensual images and videos, deepfake content, and other abusive material targeting women and girls. Law enforcement interventions have followed, with police investigations and charges brought against administrators of channels operating within this ecosystem. However, as this report documents, the closure of these spaces has not eliminated these communities, and users have

consistently migrated to environments perceived as having less scrutiny, with Telegram functioning as a primary destination where non-consensual material continues to circulate.

In Spain, the Ley Orgánica de Garantía Integral de la Libertad Sexual (also known as “Ley Sí es Sí”) introduced an ad-hoc article in 2022 criminalizing the non-consensual dissemination of intimate images, similar to Italy. However, headline scandals explicitly naming Telegram as a vector of IBSA have been less prominent, though the platform has become politically contentious in its own right. Public clashes between the Spanish government and Telegram’s leadership — prompted by the [government’s proposals to restrict certain social media functions](#) for minors and to increase platform accountability for harmful content — have placed Telegram at the center of broader debates about digital regulation. Separately, growing attention has been directed at online violence targeting women with public profiles, including feminist activists, journalists, politicians, and content creators. Yet the everyday experiences of ordinary women and girls remain comparatively underexamined, despite [recent data published by the Ministry of Equality](#) indicating that 80% of young Spanish women between the ages of 16 and 24 have experienced some form of online attack or harassment.

These two national contexts illustrate the transnational character of IBSA networks and the structural limitations of platform accountability under current regulatory frameworks. Comparing them allows us to identify patterns that transcend national specificities, and to formulate policy recommendations relevant at both national and European levels. In the Italian case, the research maps how abusive communities have evolved and adapted following recent deplatforming events, tracking the migration of these practices onto Telegram. In the Spanish case, it contributes new empirical data on IBSA circulation, situating it within a national context where regulatory and political debate around platform responsibility is still developing.

2. Methodology

The methodology employed in this study combines digital ethnographic observation with systematic data extraction and analysis of Telegram communities. This mixed approach allowed us to examine both the qualitative dynamics of user interactions and the structural patterns of content circulation and networked activity within image-based sexual abuse (IBSA) ecosystem.

2.1 Data collection

Data was collected through a multistep exploratory process aimed at identifying Telegram groups, channels, and bots associated with the circulation of IBSA content.

First, we conducted a manual search directly on Telegram using relevant keywords (see: Taxonomy of violence), including misogynistic slurs and commonly used terms associated with IBSA communities, as well as the names of previously documented groups. This search was complemented by manual queries on external platforms where links to Telegram communities are often shared, including **Google and Reddit**, following a sample based on IBSA-related groups and channels.

Second, we employed a snowball sampling strategy, where we followed invitation links, cross-posted messages, and internal references shared within identified communities to locate additional groups, channels, and related infrastructures.

The final sample consisted of **16 Telegram private groups and channels**, eight Italian and eight Spanish, and **19 Telegram bots** that were identified and manually analyzed as part of the broader ecosystem facilitating access to, and circulation of, IBSA content. Messages from these groups were collected **over the course of six weeks** (from December 22, 2025 to February 10, 2026).

Data collection followed a snapshot-based approach: for each entity, such as a message, user, or channel, a unique identifier was recorded together with a snapshot of the metadata available at the time of collection. Messages were periodically revisited in order to detect possible changes. When an entity was modified, for example when a message was edited or a channel changed its name, a new snapshot was created. This approach allowed us to reconstruct the historical evolution of individual entities over time.

Difference between groups and channels on Telegram

Groups: Can be public or private and host up to 200,000 members. Groups enable many-to-many communication, allowing users to engage in conversations and interact directly with one another.

Channels: Can be public or private and have no limit on the number of subscribers. Channels operate as one-to-many communication spaces, where only administrators can post content. Users can nevertheless interact with posts through reactions and, where enabled, comments.

For each channel or group, the following metadata was collected: channel identifier, title, type of entity (group, forum, or channel), and related discussion topics where available.

2.2 Ethical considerations

Because of their sensitive and non-consensual nature, media files were never downloaded or stored, and only the file hash was recorded in order to detect whether the same media files were reposted across different groups or channels. All data will be deleted upon the publication of the project. User identifiers were also anonymized, and instead of storing Telegram's original user IDs, the system recorded a hashed version of the identifier that could be used to identify users who participate in multiple groups or channels.

In order to avoid facilitating harassment or retaliation, the **names of the analyzed groups, channels, and bots will not be disclosed in the report.**

2.3 Qualitative analysis

The analysis combined elements of digital ethnography with a manual exploration of Telegram's platform affordances.

After gaining access to the identified groups, channels, and bots, we carried out **non-participant observation** to examine how users interacted, shared content, and navigated Telegram's infrastructure. Particular attention was paid to the role of specific platform features, including bots, invitation links, message forwarding, and the forum function in facilitating circulation of IBSA material.

During the observation process, we took note of relevant interactions for analytical purposes; images contained in the original messages were never captured. In addition, a qualitative content analysis was conducted on a subset of keyword-driven discussions extracted from the dataset. Relevant messages were identified and extracted through a combination of keyword searches and manual review of conversations within the sampled groups and channels. This process allowed us to identify discussions related to the sharing, requesting, and redistribution of IBSA content, as well as conversations reflecting community norms, motivations, and patterns of interaction.

2.4 Quantitative and network analyses

In addition to qualitative observation, we employed quantitative metrics and network analysis techniques to examine patterns of interaction and content circulation across the sampled Telegram communities.

AI Forensics' data scraping tools were used to extract message-level metadata from the selected groups and channels. This data was then used to produce descriptive statistics and network visualizations illustrating relationships between users,

groups, and key discussion topics. Network graphs generated using Gephi were used to analyze how users and discussions connect across multiple groups, and to identify patterns of content circulation within the broader ecosystem.

To analyze the connections between Telegram communities and other online environments, messages containing hyperlinks were examined. All messages including text strings such as “http” or “www” were extracted from the dataset. From these messages, we isolated individual links, including cases where multiple links appeared within a single message. Each link was then manually coded by a researcher according to the external platform it directed to, such as TikTok or other social media services. These platforms were subsequently grouped into broader categories and analyzed according to frequency, group membership, and language. This process allowed us to identify which external platforms were most frequently referenced within the analyzed Telegram communities and how they were integrated into IBSA-related practices.

Platform Type	Definition
Archive/File Hosting	Platform where someone can host files
E-Commerce	Shopping platform
Gambling	Gambling platform
Government Site	Page from a government website
Messenger	Messenger apps
NCII AI Image & Video Generator	AI apps that enable users to create sexually-explicit imagery (comprising both platforms specifically designed for that purpose and platforms that allows it without explicitly permitting it)
Porn Site	Typical porn hosting site with videos
Search Engine	Search results for a specific query from a search engine
Sex Games	Game site with sexually explicit games
Social Media	Platforms such as TikTok, Reddit
Streaming Site	Site to watch films, not specifically porn
Telegram Redirect	Link that appears to be external but redirects back to Telegram

Table 1. A typology of linked external platforms on Telegram

2.5 Limitations


Telegram's structural features restrict access to complete membership lists, meaning that it is impossible to determine the total number of unique users, and only active members of the groups, namely senders, could be recounted.

It should be noted that, after the conclusion of the data collection period, additional Telegram groups and channels with larger user numbers were identified in the Spanish context, but not included in the analysis. Thus, the selected 16 groups are not representative of all Telegram IBSA communities in either country, and the findings presented in this report should be understood as a snapshot of a rapidly evolving ecosystem rather than an exhaustive mapping of all existing communities.

3. Results

3.1 The scale and architecture of the network

The analyzed dataset consisted of a total of **2,788,751 messages** exchanged across 16 sampled Telegram communities. Groups were included if they showed active IBSA content exchange during the observation period. A total of **82,723 media files** were shared across the analyzed groups and channels, highlighting the central role of image and video circulation within these communities. Within these groups, **24,671 active senders** were identified based on participation in conversations during the observation period. Table 2 below summarizes the results, noting that channels only have one sender (the admin) whereas groups have multiple senders:



Index	Language	Type	Accessibility	Total members	Active senders	Percentage of senders on total members
1	ES	Channel	public	21,537	1	
2	IT	Group	private	27,058	2813	10%
3	ES	Channel	private	11,430	1	
4	IT	Channel	private	268	1	
5	ES	Group	private	2002	544	27%
6	ES	Group	private	1312	428	32%
7	IT	Group	private	865	129	15%
8	IT	Group	Public	8700	5902	67%
9	ES	Group	private	478	59	12%
10	IT	Channel	private	1067	1	
11	ES	Group	private	826	562	68%
12	IT	Group	Public	26,539	15.554	58%
13	IT	Group	Private	13,485	9.195	68%
14	IT	Group	Private	7862	3.375	43%
15	ES	Group	Private	322	174	54%
16	ES	Group	Private	1471	348	24%

Table 2. Characteristics of the 16 groups analyzed in the report

Italian context

Italian groups showed a higher number of users (**up to 27,000**) and higher number of messages (2,7 million). Message activity within these groups is characterized by a high degree of repetition, with users frequently broadcasting identical or near-identical content across multiple posts in rapid succession. Despite the large volume of messages, non-participant observation revealed that group-level interaction remains comparatively low: messages generate limited responses in the chats, and direct content sharing within the shared chat space appears relatively lower compared to message frequency. Users still share IBSA content

(approximately 175k media content shared), but with higher attention to potential public scrutiny. This pattern suggests a relocation of substantive exchanges to private communication channels, a dynamic supported by quantitative and qualitative evidence from the dataset. The term "private" appears 21,045 times across all messages, encompassing a range of uses: direct solicitations to move exchanges out of the group (e.g., "Venite in privato", "come in private"), requests for access to private groups, and inquiries about privately held archives (Figure 1).

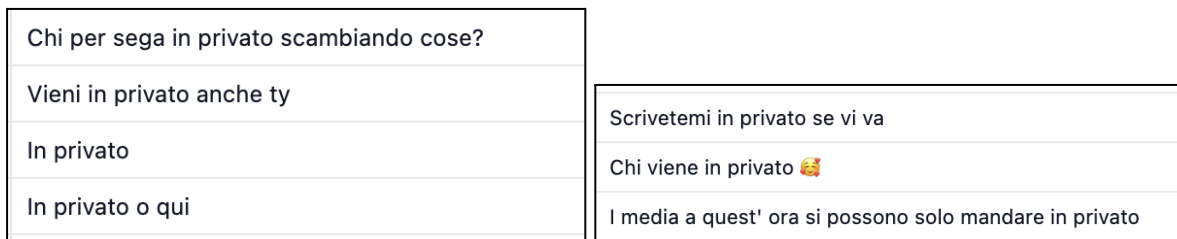


Figure 1. Examples of messages in Italian groups containing the word "private"

[Previous research](#) on Italian IBSA communities documented higher levels of user interaction and content dissemination in the chats. The dynamics observed in this study may therefore indicate a structural shift in how these communities operate, with public groups functioning increasingly as recruitment and coordination environments, while circulation of the majority of material seems to have relocated to less visible, less monitorable, private channels. This possible shift may be linked to the series of media scandals and law enforcement interventions in Italy in recent years. The finding of decreased content sharing in group chats should therefore not be interpreted at face value as a decline in abusive practices, but further scrutinized as a sign of their **privatization and strategic relocation** toward less visible communication channels.

Smaller Italian private groups, however, maintained the rule of mandatory sharing of content in the chats:

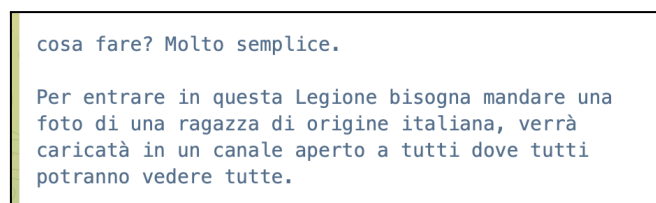


Figure 2. A message from one of the Italian groups. Translation: "What to do? Very simple. To enter this Legion you need to send a photo of a girl of Italian origin, it will be uploaded in a channel open to everyone where everyone will be able to see them all."

Spanish context

Spanish groups, on the other hand, tended to have fewer participants than their Italian counterparts, although one of the observed groups reached approximately **25,000 users**. A total of 19,102 messages were observed in the Spanish context. Despite their smaller size, these groups display significantly higher levels of engagement, with more frequent interactions among users and a greater volume of content being shared directly within the group chats (**approximately 10k media content shared**). In several Spanish groups with **800-1,000 members**, we observed **dozens of abusive images being shared every hour**, creating a constant flow of content accompanied by requests for additional material.

Notably, most Spanish groups explicitly regulate participation through community rules that prohibit the use of private messages for exchanging material (Figure 3). Members are instead required to share content directly within the group, like in the smaller Italian communities. Users who fail to contribute or who attempt to move exchanges to private conversations are often warned or threatened with expulsion. These rules suggest that, in these contexts, visibility and continuous contribution function as mechanisms of participation and status within the community, encouraging users to maintain a steady stream of abusive material within the shared space (Figure 3).

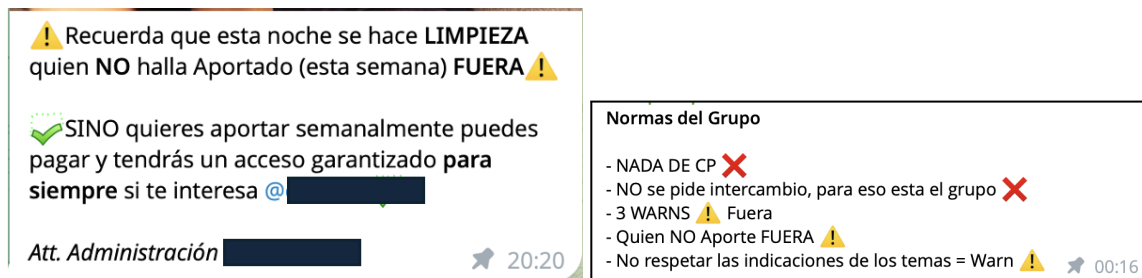


Figure 3. Examples of Spanish messages asking users to share content in the group directly and not in private.

These patterns indicate that the dynamics of IBSA content posted on Telegram may vary depending on the size of the groups, with smaller communities privileging open circulation within groups while the bigger ones rely more heavily on private exchanges.

Across both the Italian and Spanish contexts, **large channels** (those in which only the admin sends messages), particularly those with more than **20,000 members**, appear to function primarily as **distribution hubs**. Rather than hosting extensive conversations, these channels are mainly used to disseminate images and videos, repost content from other communities, and share curated lists of invitation links directing users toward additional groups, channels, archives, or external platforms

(see Figure 4). In this sense, large channels operate as infrastructural nodes within a broader network, facilitating the discovery and circulation of abusive content across multiple spaces.



Figure 4: Example of channels distributing links to other Telegram groups.

Moreover, these communities are highly dynamic. Groups are frequently closed, deleted, or recreated under new names and links, often in response to reporting, moderation actions, or external scrutiny. In the Italian context in particular, several of the observed groups were shut down and re-established multiple times during the six-week research period. This constant cycle of closure and reappearance allows abusive communities to persist while complicating efforts to monitor or disrupt them.

3.1.1 Shared links across countries

Among all the links redirecting users back to Telegram (which accounted for 38.98% of all links shared within the 16 sampled groups), 39% linked to channels, 36% to bots, and 25% to private groups, suggesting similar levels of adoption of the different interaction options offered by the platform. Most Telegram links circulated primarily within their country of origin, with relatively limited cross-country overlap. However, **two links were shared across both countries**, one directing users to a bot and the other to a private Telegram group, indicating at least one connection between the Italian and Spanish networks.

At the network level within countries (Figure 5), four **Italian groups appeared to be interconnected** through the sharing of private group links among each other, indicating a level of internal coordination. By contrast, the **Spanish groups appeared to operate in a more fragmented network**, with fewer direct connections established through link sharing.

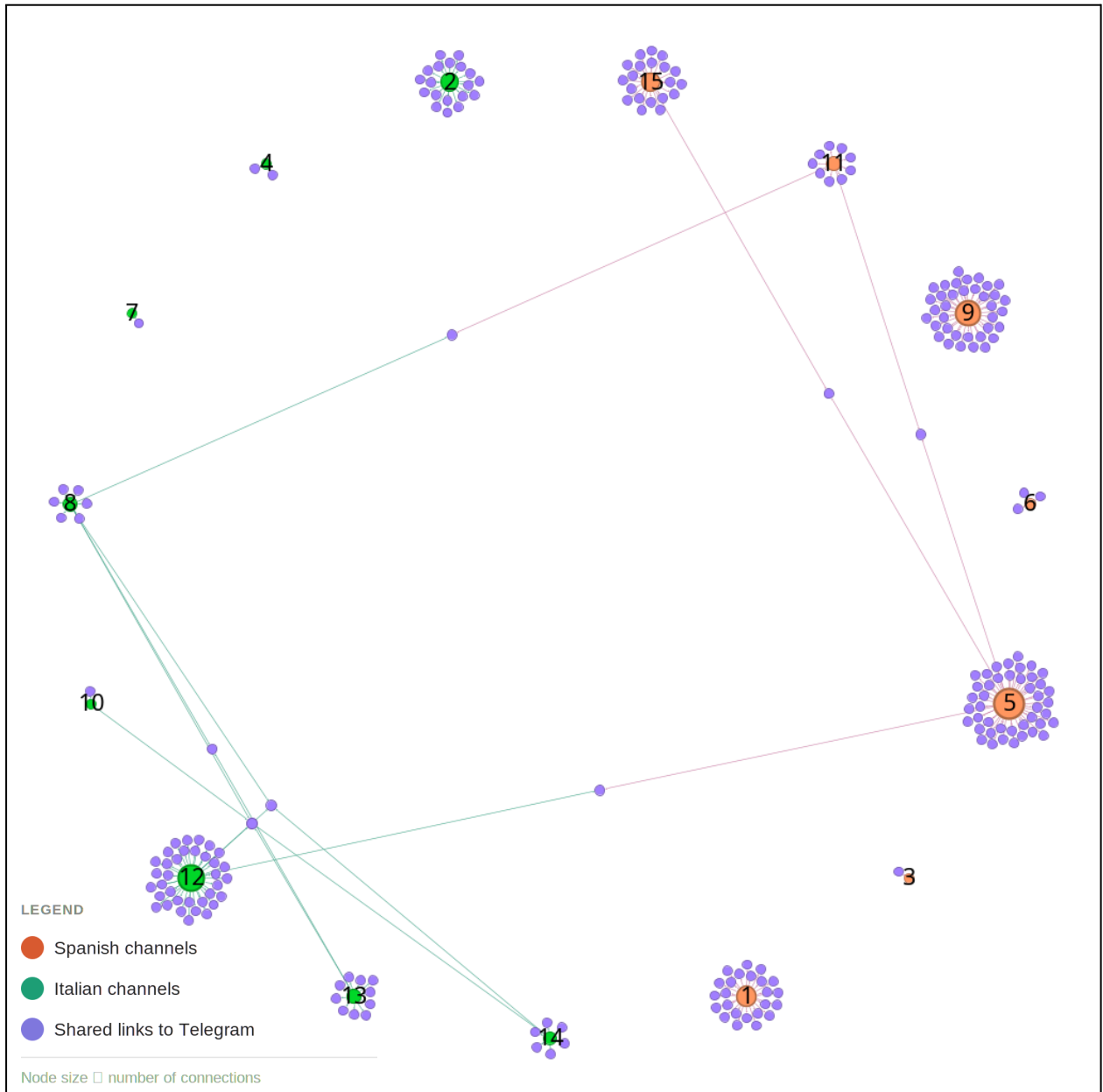


Figure 5: Channels are displayed in a circle using the Circular Layout plug-in. Italian channels are in green, while Spanish channels are in orange. Shared links to other telegram bots/channels/groups are in violet and are connected to the channel(s) that shared them. We can observe that only two links are shared in both Italy and Spain. Group 16 didn't share any link.

3.1.2 Shared message senders across countries

A similar pattern emerges in the analysis of message senders across groups (see Figure 6). Italian groups show a higher degree of cohesion, with many senders participating across multiple groups and creating dense cross-group connections. Spanish groups, by contrast, appear to operate more independently, although some clusters can still be identified. In particular, four Spanish groups share a relatively large number of senders, suggesting a degree of overlap between their participant bases, while the remaining three groups appear more isolated and share only a limited number of senders with other communities.

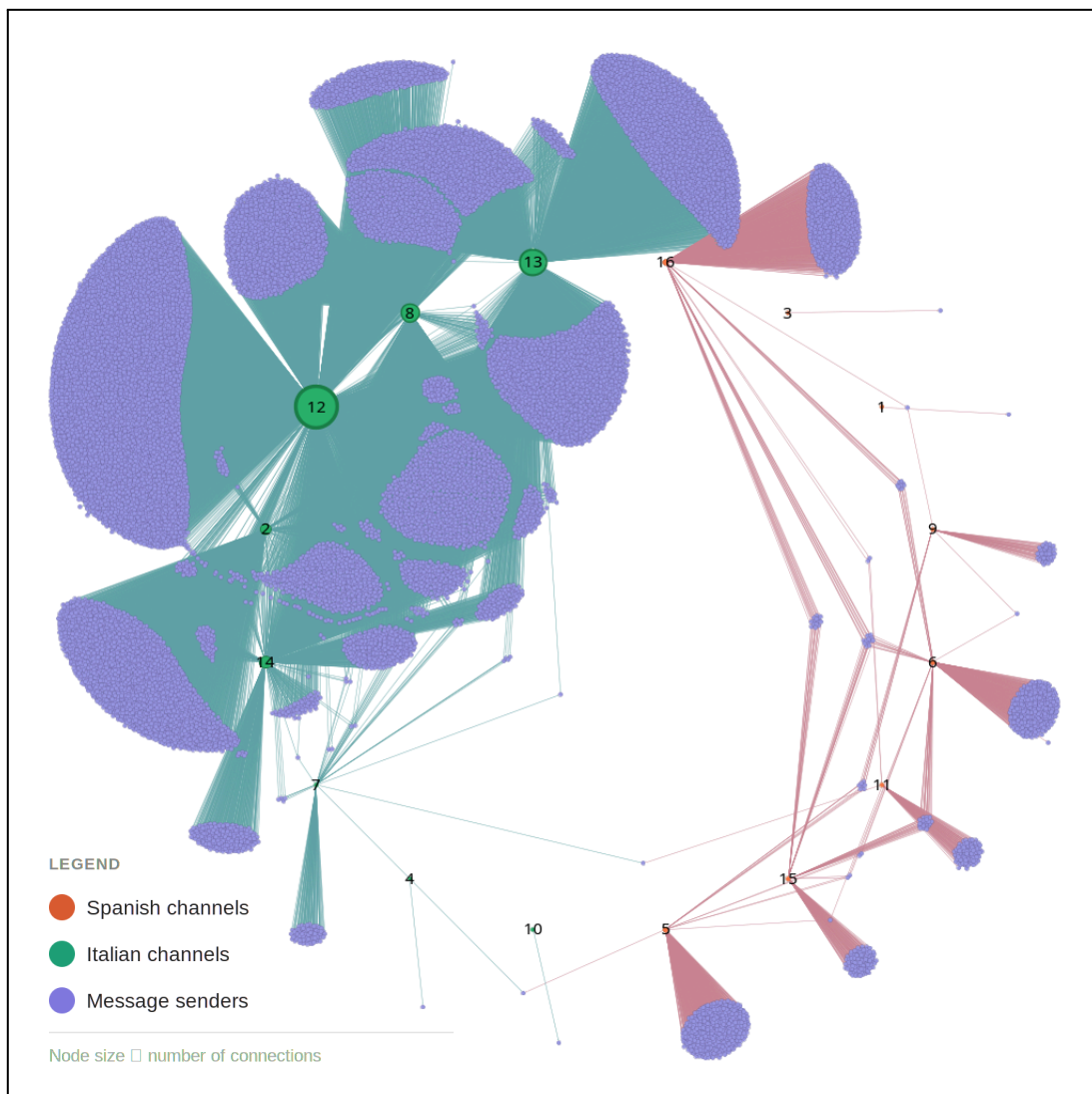


Figure 6: Network of message-sending users (not all users in the channels). Each message-sending user is connected to the group where they sent messages. Only two users posted in both countries, while many posted across channels within the same country.

3.1.3 Shared media across countries

Despite the limited overlap in links and senders, our analysis of the media circulation shows that the content itself travels more widely across national boundaries.

Approximately **8% of all analyzed media files were seen circulated across both the Italian and Spanish environments**. This corresponded to 72% of the Spanish content but represented only around 8% of the total Italian content, reflecting the larger size of the Italian dataset.

The network depicted in Figure 7 represents the cross-national media sharing structure across Italian (green nodes) and Spanish (orange nodes) channels. Purple nodes represent individual media items (photos and video notes, $N = 4,916$) that appear in at least one channel from each country (the exclusive condition for inclusion in this graph). Edges are colored by the community of origin: teal edges represent content originating from Italian channels, while pink edges represent content originating from Spanish channels.

Channel 6 (from Italy) and channel 12 (from Spain) emerge as dominant hubs, distinguished by substantially larger node sizes, and by the notable thickness of the edges connecting them, encoding a high-degree of participation in the cross-national media sharing ecosystem. The biggest resharing hub among the Spanish channels is represented by node 6, which appears to propagate content from both Italian and Spanish ecosystems, becoming a superspreader channel. On the other hand, channels 1, 2, 3, 4, 9, 14, and 16 show smaller node sizes and thin connecting edges, suggesting marginal participation in the cross-national media sharing ecosystem.

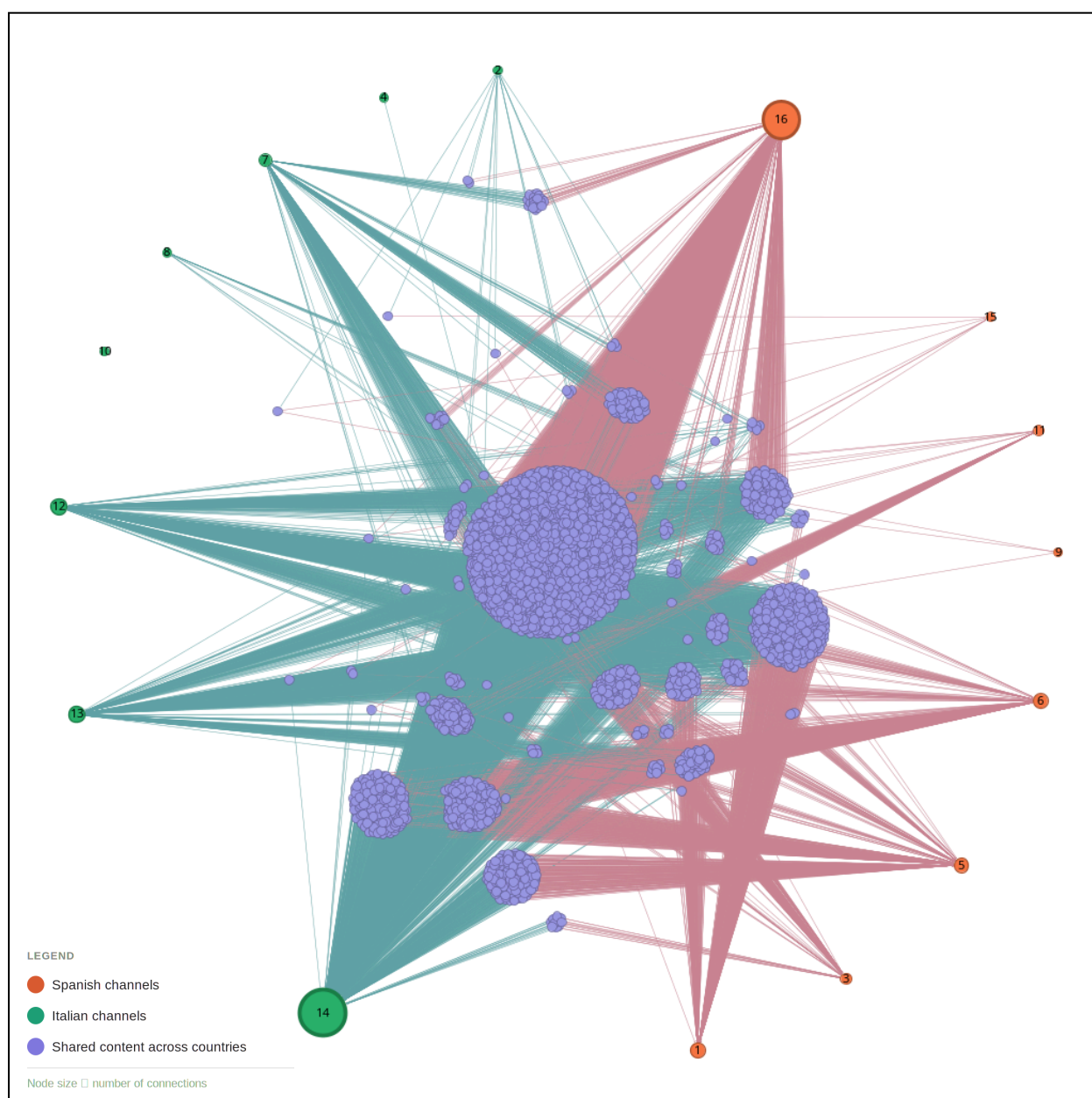


Figure 7: Median sharing network representing 8% of content shared across both Italian and Spanish channels and groups, despite not having any shared media senders.

The analysis of shared media also shows that **photos constitute the vast majority of circulated content, accounting for 74% of all media files**, followed by videos (25%), and a small proportion of other file types, such as audio (1%). The types of media shared across both the Italian and Spanish contexts, including photos and videos, appear proportionally similar.

Taken together, these findings indicate that abusive material does not remain confined to individual groups but potentially circulates across a much larger network of interconnected communities and archives, where Telegram's channels, bots, and private groups function as infrastructural nodes enabling the

redistribution and persistence of content across different spaces. Beyond the structural dimensions of these networks, the analysis also documents the specific forms of violence that circulate within them.

3.2 A taxonomy of violence

Across both countries, the analyzed Telegram groups and channels are primarily used to seek and disseminate non-consensual sexual images of women and girls. However, our content analysis also reveals the presence of multiple, overlapping forms of TFGBV. These practices extend beyond the circulation of non-consensual intimate images and include broader forms of IBSA, as well as behaviors aimed at controlling, degrading, or humiliating women and girls online.

It is important to note that the **sharing of non-consensual intimate images rarely occurs as an isolated practice**, but forms part of a wider ecosystem of gender-based violence enabled by digital technologies.

In order to better understand the complexity of these dynamics within Telegram communities, we developed a categorization of the different abusive practices we observed across the analyzed groups and channels. Practices have been categorized using in-depth content analysis and manual searches through the dataset using relevant keywords. Table 3 below shows the different categories of abusive practices observed:

Practice	Description	Number of messages containing a related keyword	Italian language	Spanish language
Tribute / "Pisellare"	<p>"Tribute": non-consensually ejaculating on someone's picture, also called "semen picture"³.</p> <p>"Pisellare" or "cocking": non-consensual</p>	<p>"Tributo/Tributare": 18,000</p> <p>"Pisella/Pisellare": 11,304</p>	<p>"qualcuno per pisellare mia cugina?"</p> <p>"chi con doppio dispositivo per pisellare amichette"</p>	<p>"Alguien le hace tributo a mi amiga?"</p> <p>"Busco pajabro para tributo"</p>

³ McGlynn, C. (2026) Exposed: The Rise of Extreme Porn and How We Fight Back. Oneworld Publications

	ly using someone's picture to perform masturbation on it. Requires using double devices.			
Roleplay/Morbo	A gamified form of violence in which two users chat privately: one impersonates a woman, uses her intimate content without consent (often synthetic or AI-altered, including audios), and engages in sexting with another user.	"Roleplay": 43,066 "Morbo": 631	"Chi fa f in roleplay ho foto tipa e trama, mi adatto a qualsiasi richiesta ho cazzo duro" "Chi interpreta una troia milf in roleplay? Ho anche foto"	"Morbo a mi novia?" "Alguen morbo de amigas, influ, etc?" "Dm para morbo a mis conocidas"
Non-consensual dissemination of intimate images	Non-consensual sharing, seeking, or selling of intimate imagery (including pictures and videos, creepshots, and non-consensual ly taken or stolen content).	"Ex": 106,013 "Girlfriend"- (Novia/Mia ragazza/Fidanzata): 101,153 "Wife" (Moglie/Mi mujer): 15,521 "Sputtana/Sputtana ta": 17,757	"chi sputtana la mia ragazza? VISO E COSTUME" "Chi conosce V. O. di milano?" "🔥🤔🚫 Troie sputtante in descrizione"	"Exponiendo a mi ex. Dm" "Alguno me presta su novia para humillarla y pajearme?" "Alguen para paja en autodestrucción de amiga ex o novia m d"

Sexual deepfakes	Altered images, sometimes accompanied with synthetic audio of the victim's voice.	<p>"Deepfake": 170</p> <p>"Denudare/desnuda r": 777</p>	<p>"scambio deepfake di XXX solo se mi mandate sue foto o video"</p> <p>"ho fatto dei deepfake della mia ragazza, chi vuole vedere?"</p>	<p>"alguien que haga tributos o deepfakes"</p> <p>"Alguien puede desnudarlas?"</p>
Doxxing	Non-consensual sharing of a victim's personal information, such as personal number, email address, social media profiles, or home address.	<p>"Indirizzo/Dirección": 391</p> <p>"Telefono": 1865</p> <p>"Numero": 1979</p>	<p>"+39 3XX XXX XXXX questo è il numero dove contattare"</p> <p>"Do il numero di mia sorellina se le mandate il cazzo"</p> <p>"375XXXXXXX numero ragazzina ricattata fa pompini scrivetele"</p> <p>"CHI VUOLE INDIRIZZO CASA TIPA 29 TETTONA PALERMO PER ANDARLA A TROVARE CON AMICI ANIMALI"</p> <p>"Scambio numero troia"</p>	<p>"Tienes su número de teléfono?"</p> <p>"Comparto numero de putas para morbosear"</p>
Hacking	Seeking,	"Hack": 441	"Qualcuno	"Hackeo y

	offering, or selling services to gain unauthorized access to data on a smartphone, computer, system, or social media profiles.		<p>riesce a recuperare numero di telefono da ig?”</p> <p>Cerco real hacker o bot per hackerare chi mi insegna ad hackerare?</p> <p>“Scambio mia amica 2008! Le sono entrato nel telefono e ho rubato moltissime foto e video di ogni genere! Scrivetemi che scambiamo!”</p>	recupero cualquier tipo de servicio de redes sociales.y puedo espiar la cuenta de tu pareja envíame un mensaje privado”
Spycams	Sharing or seeking non-consensually taken material, recorded with a hidden camera in public and private spaces (e.g. gyms, schools, shops, hotels, houses)	“Spy”; “Espiađa”: 18.824	<p>“Chi scambia foto e video Spy? Camerini, fatti in casa”</p> <p>“Cerco video porno spy chi ha mi scriva ho teen”</p> <p>“Mostro spy donne vestite”</p>	<p>“a quien le gustan las espiadas en la calle? Dm”</p> <p>“Quien cambia videos espiados en el instituto?”</p>
Spywares	Offering spyware or malware to spy on victims.	Ibidem	<p>“Accesso alle chat Accesso alla galleria Accesso alla telecamera</p>	“Quieres acceder a Facebook, Whatsapp, Instagram o Google photos

			<p>Spiare senza che lei se ne accorga? Scrivimi in privato.”</p> <p>“Ciao hai il desiderio di spiare la galleria di una tipa? 😊 Vendiamo BOT che lo fa per info dm👉”</p>	<p>de tus conocidas? Manda mensaje a ***”</p> <p>“Contenido IPCam”</p>
Coordinated attacks/targeted harassment	Channels and conversations targeting specific victims (e.g., influencers, content creators) for harassment.	“Influencer”: 2051	“Chi sputtana influencer? O crea un gruppo su ***”	“Aquí teneis de regalo un canal con filtrados de influencers, chicas españolas parejas y de todo.”
Child sexual abuse material (CSAM)	Non-consensual sharing and seeking of underage girls.	”Teen”: 61.936	<p>“cerco qualcuno con cui scambiare foto di amiche/conoscenti 2010-2013”</p> <p>“chi ha 2010 magra”</p> <p>“SCAMBIO TEEN ITA RARI 07/08”</p>	<p>“Tengo sexo con mi hijastra de 14, busc0 alguien que haga lo mismo y tenga pruebas, yo tengo demasiado”</p> <p>“who can facetime my asian teen girl and flash their dick to her. imessage only”</p> <p>“quien pasa teens??”</p>
Sexist hate speech	Use of misogynist	“Puttana/Putta(s)”: 20.904	“SEGO E SBORRO LA	“K zorra”

	slurs, insults, and attacks.	“Troia/Troie/Zorra(s)”: 90.039 “Guarra”: 45	TUA PUTTANELLA” “Chi odia le troie come me? Scrivimi” “Chi trova IG di sta troia?”	“Soy yo, o esta tiene una cara de adicta al sexo...Madre mía que cara de guarra tiene...” “se ve muy puta”
Sexual solicitation	Seeking, offering, or enticing another person to engage in sexual acts, including engaging in technology-mediated or offline sexual interactions.	“Cerco/Busco” (<i>I seek</i>): 27.2790	Ragazza x sesso reale sta sera prov di Treviso?	N/A
Rape	Incitation to rape, offering/seeking women to rape, sharing rape fantasies.	“Rape” (Stupro/Violación): 1447	“Chi vorrebbe stuprare una ragazza?” “Voglio stuprare una moglie” “Troia veneta da stuprare in bio” “Vorrei fare stuprare la mia ragazza”	“Videos de violación?” “Estoy agregando personas a la nueva mega carpeta, incluidos todos los grupos de incitación a la violación de adolescentes, homosexuales, mamás y hijos. Envíenme un mensaje privado para que los agreguen.”

Table 3. Observed categories of abusive practices on Telegram groups and channels

As our findings show, misogynistic language cuts across all categories of abusive behavior and acts as a shared cultural and discursive framework that sustains these

communities. Our analysis also demonstrates that TFGBV can manifest in multiple, interconnected forms extending beyond the circulation of non-consensual intimate images, such as harassment, surveillance, humiliation, and privacy violation of women and girls, including underage girls. Notably, **these dynamics are largely consistent across the analyzed Italian and Spanish communities**, showing similar norms and practices among IBSA networks across national contexts.

3.3 Types of perpetrators

Across both the Italian and Spanish groups, several recurring user roles can be identified, suggesting that these communities operate through relatively structured patterns of participation.

A first category consists of **uploaders**, users who explicitly present themselves as providers of material through expressions such as “I exchange” (243,758 messages) or, less frequently, “I sell” (1,483 messages).

A second category includes **requesters**, whose activity is reflected in messages such as “who sends” (7,443 messages) or “I seek...” (272,915 messages). These requests frequently appear to lead to private conversations rather than continuing within the public chat space.

A third category can be described as **administrators or mediators**, users who perform organizational functions by communicating group rules, advertising related channels, or archives, and moderating participation (Figure 8).

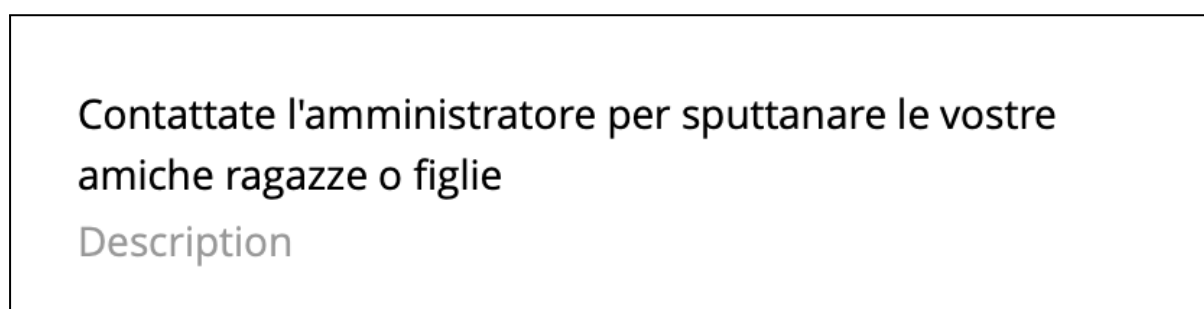


Figure 8. Translation: “Reach out to the administrator to expose your friends, girlfriends, or daughters”

Finally, the groups include a large number of **lurkers**, users who remain present in the communities without visibly contributing content (and who therefore could not be captured through measures of active participation).

These participation dynamics indicate that IBSA communities on Telegram function as active, socially-organized environments. The presence of differentiated roles and rules, the concentration of content production among a minority of users, and the

role of central actors who maintain cohesion, all point to the existence of relatively stable peer networks structured around the exchange of abusive material.

Because Telegram allows users to operate under pseudonymous identities, it was not possible to conduct a comprehensive **sociodemographic analysis of participants**. However, some indicators could be inferred from usernames, internal group sections, conversational cues, and occasional self-disclosures. These include references to gender, age, nationality, or location, e.g., statements such as “*soy H 25 años*” (“I am a 25-year-old man”), “*sono 2011*” (indicating year of birth), or references to specific locations such as “*sono di Palermo*” or “*io veneto*”. In several groups, internal polls, hashtags, and symbolic markers such as national flags also suggest a predominance of Spanish or Italian users depending on the context (e.g., #MadridViral), as shown in Figure 9 below.

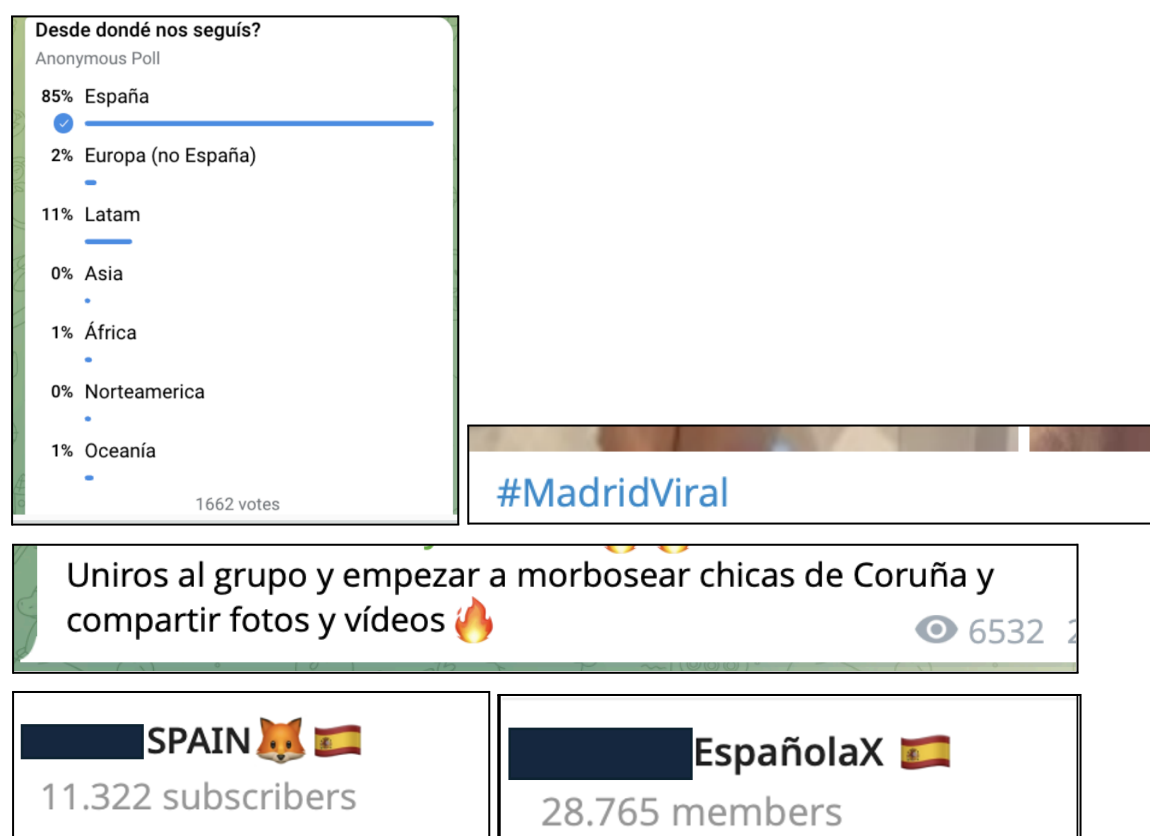


Figure 9. Examples of clues identifying the origin of Spanish users.

Overall, the observed practices appear to be **predominantly shaped by heterosexual male participation**, reflecting a broader pattern of male homosocial interaction in which the circulation and evaluation of women’s bodies functions as a form of bonding and status-seeking among participants (Figure 10).

Siamo un gruppo hot 🍆 (etero) dedicato a chi vuole condividere racconti e temi di natura sessuale senza sentirsi giudicato, un posto dove lasciarsi andare e godere di questi brevi ed intensi piaceri 🔥

Figure 10. “We are a hot 🍆 (hetero) group dedicated to those who want to share stories and topics of a sexual nature without feeling judged, a place to let yourself go and enjoy these brief and intense pleasures 🔥”

At the same time, the dataset also reveals the presence of bisexual and homosexual male users. However, these participants do not appear to be primarily engaged in sharing non-consensual intimate images of men. Instead, their activity is more often oriented toward seeking offline encounters or sexting interactions within the group environment. This tension is occasionally made explicit through homophobic remarks posted by other users, such as “Non scrivere in privato... mi piace la figa, no il cazzo” (“Do not write to me in private... I like pussy, not dick”), illustrating how heteronormative norms are actively enforced within these communities.

Non scrivere in privato ... mi piace la figa no il cazzo

Mandamelo in privato se non ti da fastidio... tranquillo mi piace la figa 🤔🤔🤔

Figure 11. Conversations among Italian users restating their heterosexuality.

In the Italian case, [prior research](#) has shown that abusive practices on Telegram are actively shaped and reinforced by social dynamics such as homosocial peer validation, status-seeking, and sexual objectification of women, all of which, facilitated by Telegram’s affordances, allow image-based sexual abuse to be systematized and normalized within online male peer networks. In this context, users, for instance, incite and congratulate each other for contributing to the sharing of such content (Figure 12).

gracias por aportar [REDACTED] eres un crack 22:30

Figure 12. “Thank you for contributing, you’re a genius”

Finally, the data also indicates a **limited but visible participation of women** within these chats, both as subjects of discussion and as users who are actively sought by other participants. In several instances, women appear to promote their own channels, either on Telegram or on external platforms such as OnlyFans, where they advertise erotic services including camming, online performances, or offline meetings. These interactions point to a complex gendered ecology within the

groups, in which abusive exchanges coexist with forms of sexual self-promotion and commercial activity.

3.4 Types of victims

The analysis shows that the primary targets of these communities are ordinary women and girls, including girlfriends, friends, acquaintances, and former partners whose images are shared without their consent. At the same time, users also frequently refer to more visible figures, including influencers (mentioned 2,051 times across the chats), “famous” women (363 mentions), feminist activists (351 mentions, primarily within Italian groups), and also “tradwife” influencers (within Spanish groups). Victims are often named, tagged, and locatable via shared profile links, with groups featuring dedicated sections to influencers, and specific rules for disseminating content or requesting synthetic content.

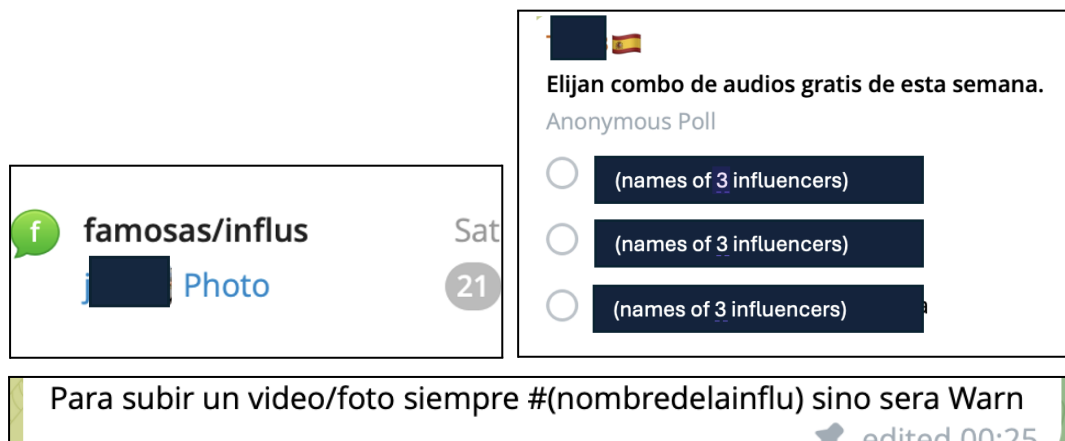


Figure 13. Groups targeting women influencers across Spain, with rules for disseminating content.

While public figures attract particular attention, with entire groups created with the aim of disseminating (real or synthetic) pictures of influencers, the data suggests that **ordinary women constitute the central focus of these practices**. This can be seen, for instance, in sections of the groups targeting “girlfriends” or “friends” (Figure 14), but also in conversations leaked from social media (see also paragraph 3.4). This highlights the importance of examining IBSA not only as a phenomenon affecting high-profile individuals but also as **a form of everyday gender-based violence**.

In many cases, the women targeted appear to be unaware that their images are being collected, exchanged, or discussed within these networks, as **perpetrators also share images and videos taken with hidden cameras or filmed while the victims are asleep** (Figure 15). The circulation of such material often occurs within a broader environment where lack of consent is normalized and misogynistic discourse is pervasive.

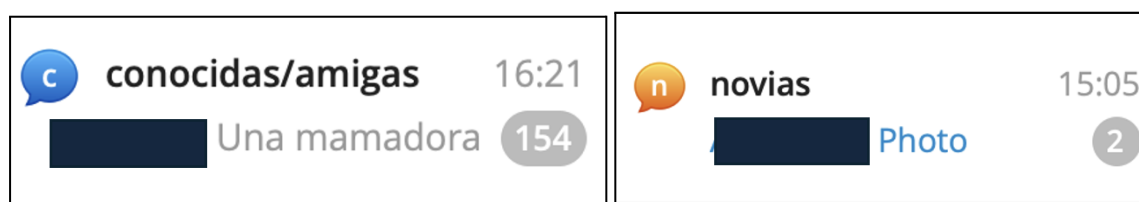


Figure 14. Groups' sections targeting members' acquaintances, friends, and girlfriends.

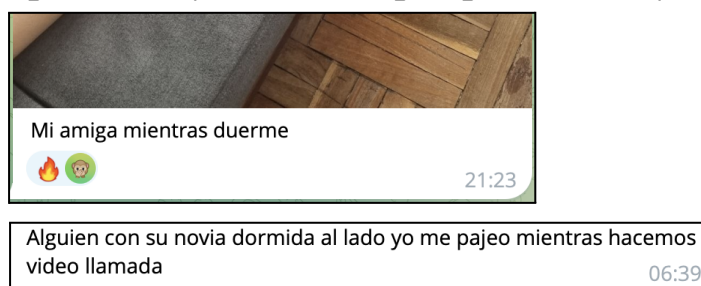


Figure 15. “My friend while sleeping” - “Does somebody have a sleeping girlfriend to do a video call while I masturbate?”

Across both the Italian and Spanish contexts, these dynamics point to a structured and socially embedded form of violence, in which the non-consensual sharing of women’s images is treated as routine practice within male peer networks and consent is constantly negotiated or denied.

3.5 Telegram as a cross-platform infrastructure for abuse

Our analysis shows that IBSA practices are not confined to Telegram but draw systematically on content extracted from other platforms. To date, relatively little research has looked into how dissemination of IBSA content unfolds across different online networks, both within Telegram and through connections to other environments.

While many links shared through Telegram keep users on the platform, directing them to internal channels, groups, or bots, Telegram is also a repository for external links. Several messages also direct users to external platforms, such as those sharing porn, non-consensual images, and nudifying apps. Our dataset contained 510 messages that had one or more links directing users to an external platform, with a total of 76 unique URLs that were shared 898 times. In total, 11 out of the 16 analyzed channels and groups shared external links.

More external links were shared in Spanish channels and groups (55 unique URLs shared 861 times) than Italian (21 unique URLs shared 37 times). However, the majority of the Spanish-language links were shared in one channel.

In this sense, Spanish groups appeared more networked with external platforms. In terms of overall frequency, Spanish channels and groups tended to share **small porn sites** most often, followed by Telegram redirect links, and to a lesser extent sites for gambling, sex games, archives/filehosting, non-consensual intimate images (NCII) and video generators, social media, and, lastly, a messenger app (see Table 4).

Italian channels and groups appeared to stay more in-platform. In terms of overall frequency, they tended to share Telegram redirect links most often, followed by social media links. Further, we see that Spanish groups linked to more participatory external platforms (e.g., games or gambling sites).

Platform Type	Percentage of links shared		
	Spain	Italy	Total
Porn Site	45.88%		43.99%
Telegram	38.33%	54%	38.98%
Gambling	5.23%		5.01%
Sex Games	5.23%		5.01%
Archive/File Hosting	2.56%		2.45%
NCII AI Image + Video Generator	2.09%	2.7%	2.12%
Social Media	0.58%	27.03%	1.67%
Search Engine		5.41%	0.22%
E-Commerce		2.7%	0.11%
Government Site		2.7%	0.11%
Messenger	0.12%		0.11%
Streaming Site		2.7%	0.11%

Table 4. A breakdown of how often certain platform types were shared in Spanish and Italian channels and groups.

When we break this down across groups, however, **NCII AI image and video generators appear in five of the Spanish groups**, despite constituting only a small percentage of platforms shared overall (see table 5). Telegram redirects follow a

similar pattern, also appearing in five of the Spanish groups and four of the Italian ones. **While porn sites were shared frequently, they only appeared in two Spanish groups**, and more predominantly in one of them. However, these sites remained particularly relevant as they often featured non-consensual intimate images and videos of women and girls, including AI-generated content.

Language	Spain						Italy				
Group Index	1	5	6	9	11	15	2	8	12	13	14
Platform Type											
Porn Site	43.76%			0.22%							
Telegram	22.94%	0.45%		0.33%	1%	12.03%	1.89%		0.11%	0.11%	0.11%
Gambling	5.01%										
Sex Games	5.01%										
Archive/File Hosting	2.45%										
NCII AI Image + Video Generator		1.11%	0.11%	0.33%	0.33%	0.11%				0.11%	
Social Media					0.56%		1%		0.11%		
Search Engine							0.22%				
E-Commerce							0.11%				
Government Site							0.11%				
Messenger				0.11%							
Streaming Site								0.11%			
N/A											

Table 5. Overall percentage of links redirecting to different platform types, broken down across groups.

While no specific URL showed up across different groups or channels, there were specific platforms that did. As seen in Table 5 above, social media platforms, more specifically Instagram and TikTok, were shared in both Spanish and Italian groups. These social media links are a way to share sexually suggestive but sometimes also humorous or entertaining content. Similarly, NCII AI image and video generators were shared in both country contexts, although more so in Spanish groups. There was one specific image generator app that was observed across both countries (for the rest, the cross-country groups shared different apps with the same function).

All but two of the groups utilized external links to redirect to Telegram. These are links where the URL appears to be “external” but ultimately redirects to Telegram — typically to nudifying bots. Likely, disguising these links as external ones helps evade moderation of sexually explicit content from nudifying bots or channels (see Figure 16). Further, disguising links appears to be a cross-country practice, but each country had a predilection for specific apps.

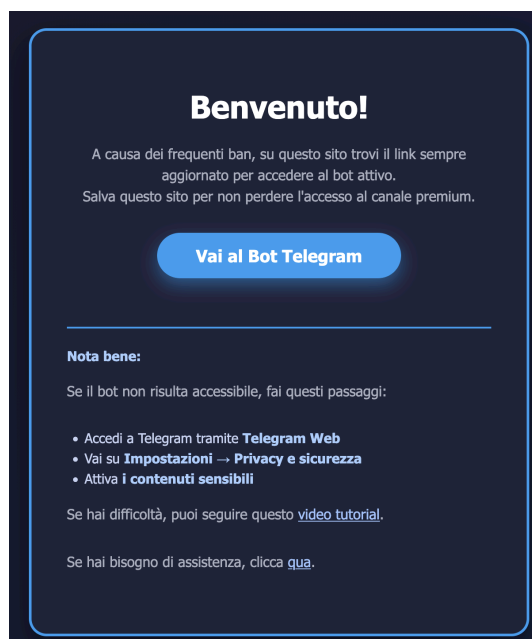


Figure 16. Screenshot of a webpage that hosts the most updated link to a Telegram bot to evade bans.

More importantly, our analysis reveals that the circulation of abusive material on Telegram is also deeply embedded in the broader cross-platform ecosystem. Rather than relying exclusively on content produced within Telegram itself, users frequently **scrape, collect, and redistribute material originating from other social media platforms.**

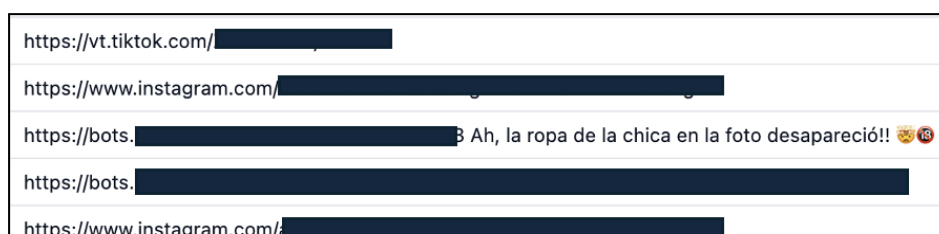


Figure 17. Example of external links extracted from Telegram messages.

Among the platforms most frequently referenced, **TikTok appears as the primary source of content**, mentioned **19,625 times** across the dataset. Conversations often frame TikTok as a pool from which images, videos, or personal accounts of women can be identified and subsequently shared, altered, or targeted for harassment. In

several cases, references to TikTok content are accompanied by requests for screenshots, recordings, or other forms of content capture, including the extraction or AI-creation of audio or video clips. Here are an example messages:

“Chi mi fa segare tiktoker fighe? Sborro in cam solo a chi manda foto e interpreta senza mostrarsi”

Translation: “Who will help me masturbate to hot TikTokers? I will ejaculate on cam only to those who send photos and play along without showing themselves.”

“chi ha tik tok per segare e sputtanare mie amiche??”

Translation: “Who has TikTok to masturbate to and expose my female friends?”

The presence of hashtags such as **#PornoTok** further suggests that some users explicitly reinterpret the platform as a space from which sexualized material can be extracted or repurposed. #PornoTok consists mainly in creating and sharing synthetic content (including audio) of specific TikTok influencers (Figure 18).

#PornoTok : Combinación de tiktoks y porno.
#Series : Aquellos audios IA que tengan más de 2 partes.
#Conversaciones : Aquellos audios que tengan más de una voz en el mismo audios.

Figure 18. Explanation of rules of #Pornotok and the creation of synthetic audio.

Instagram is mentioned 2,181 times, often in connection with direct links to personal profiles or screenshots of private conversations. In some groups, entire sections are dedicated to the redistribution of **private exchanges originating from Instagram or WhatsApp**, which are shared without the knowledge or consent of the individuals involved. Messages observed in the dataset indicate that users sometimes deliberately collect screenshots of women’s profiles or conversations and repost them within the Telegram groups (Figure 19). Moreover, users often ask to contact women on social media, such as Instagram or Snapchat, to cyberharass them, for example through cyberflashing (Figure 20).

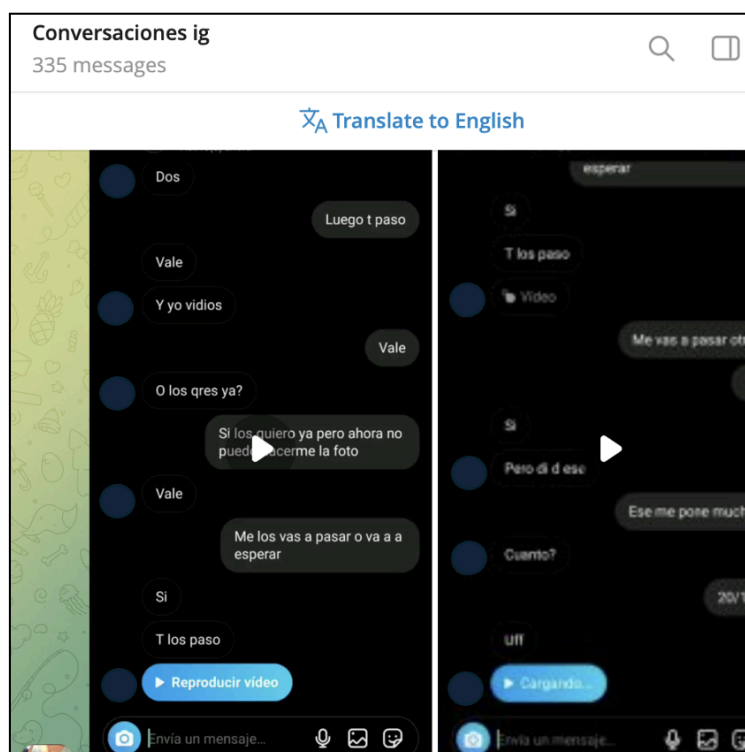


Figure 19. Example of a screen recording and sharing of an Instagram private conversation where explicit sexual material is consensually shared.

Chi manda foto del cazzo a mia amica su Instagram ? Con profilo fake va bene

Figure 20. "Who sends a dickpic to my friend on Instagram? With a fake account it works"

Other platforms are also integrated into these practices. **Snapchat is referenced 545 times**, frequently in relation to the circulation of captured or recorded ephemeral content. Users sometimes discuss sending messages to women through Snapchat in order to provoke reactions or obtain material that can then be shared within the groups.

LO ESCO ALLE VOSTRE AMICHE SU SNAPCHAT E VI MANDO REAZIONE

Chi vuole nick Troia Snapchat

Figure 21. "I show it (*penis*) to your friends on Snapchat and I'll send you the reaction" - "Who wants the nickname of a Snapchat sl*t?"

OnlyFans is mentioned 1,323 times, often in relation to the collection and redistribution of material produced by content creators. Several groups include sections or archives explicitly dedicated to sharing leaked or redistributed OnlyFans content, as well as requests for specific creators' material.

Overall, these findings highlight how the IBSA ecosystem operates as cross-platform infrastructures of abuse. In this environment, social media platforms or other messaging apps function as sources of raw material, while Telegram appears to serve as a hub for the organization, amplification, and circulation of abusive content across interconnected communities.

Finally, several links to the analyzed Telegram groups were traced back to **Reddit**, where dozens of subreddits appear to function as intermediary spaces for discussing and promoting tools and practices connected to IBSA. These communities often host discussions about nudifying apps, methods for jailbreaking generative AI chatbots, and techniques for generating or manipulating explicit content. In many cases, these discussions also include **direct invitation links** to Telegram groups and channels, where more explicit material is circulated and where users gather around specific practices (such as roleplay or “tribute” activities). This suggests that Reddit operates as a key gateway platform, facilitating the discovery and recruitment of users into Telegram-based networks where abusive content is stored, exchanged, and monetized.

3.6 An organized economy of abuse: automation, archives, and monetization

What was previously mainly peer-to-peer image sharing has evolved into a structured informal economy with multiple revenue streams, automated service delivery, and platform-enabled payment infrastructure. Our analysis, in fact, reveals the growing role of automation tools and bots in facilitating and scaling TFGBV within Telegram communities.

The automatization of violence

The use of internal and external **bots** play a significant organizational role within these IBSA ecosystems. Among the analyzed groups, bots were often used to automatically generate invitation links to private groups, archives, or cloud storage spaces; communicate group rules to new members; and moderate participation by banning users who engage in spam or violate internal regulations.

In three of the Spanish groups analyzed, access to the group was also conditional upon promotional actions, such as sharing the invitation link across multiple other channels, practices that effectively help expand the visibility of these networks (see Figure 22).



Figure 22. Examples of propagation of material with bots resharing requests.

The widespread presence of these automated tools suggests an organizational structure that goes beyond spontaneous peer-to-peer exchanges, enabling the coordination and maintenance of abusive communities at scale. Bots, in fact, represent a key infrastructural element of these ecosystems, enabling users to access, generate, and distribute abusive content with minimal effort.

On Telegram, users discuss bots both for offering/selling or seeking different AI tools embedded into Telegram channels. The word “bot” is mentioned 16,232 times across the analyzed messages, and encompasses different practices, including AI-manipulation of images, hacking or spy bots, and doxing bots (Figure 23; Table 6).

ho bot che denuda se volete scrivetemi

Qualcuno che crea video bot con mia ex

Regalo bot per spammare foto

Chi ha bot denudatori?
Chi vuole bot che modifica immagini e fa fare alle tipe quello che volete?
BOT PER SBORRARE VISO SCRIVETE
Ciao hai il desiderio di spiare la galleria di una tipa? 😊 Vendiamo BOT che lo fa per info dm 🤝
Cerco bot per hackerare o real hacker
Chi vuole nuovo bot che fa deep fake perfetti gratis?
🔥 ¡Bot AI para desvestir gratis! Super realista
Bot GRATIS para hacer videos porno desde una foto
CHI HACKERA O HA BOT PER TROVARE PERSONE?

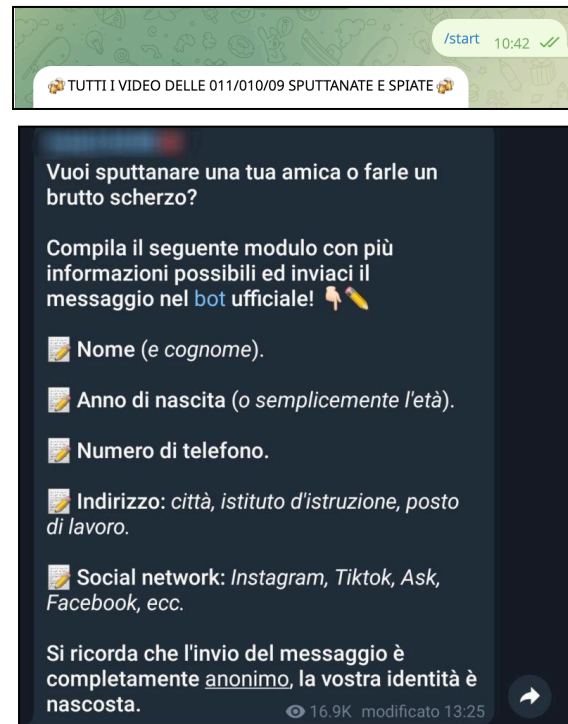


Figure 23. Example of doxxing bots.

Table 6. Example of messages discussing bots

In addition to the bots identified during qualitative observation, we detected further use of automated tools through the analysis of shared links. We manually analyzed 19 bots in total to understand their functioning.

A significant portion of these links were disguised, presenting themselves as external websites while actually redirecting users to Telegram-based services. These links comprised several recurring categories of automated services, including **AI girlfriend generators**, **nudifying bots** capable of producing synthetic sexual images, and **video archives** containing leaked material from platforms such as OnlyFans.

Among the disguised links, AI girlfriend bots were the most frequently shared, followed by nudifying bots, and video archives containing collections of OnlyFans material (see Table 7):

Telegram Redirect Links	Link Sharing Frequency
AI Girlfriends	49.71%
Nudifying Bots	19.14%
Videos Archive OnlyFans	4.86%
Video Archives (other)	0.29%

Table 7. Breakdown of the frequency of disguised Telegram redirect links. Broken links comprise the remaining percentage.

These tools were also identified in other parts of the dataset outside of disguised links, suggesting that they constitute a widely recognized infrastructure already integrated within these communities or advertised by users (Figure 24). Moreover, users were also observed sharing tips regarding prompts to generate sexualized or nudified images on chatbots such as Grok, Gemini, or similar (Figure 25).

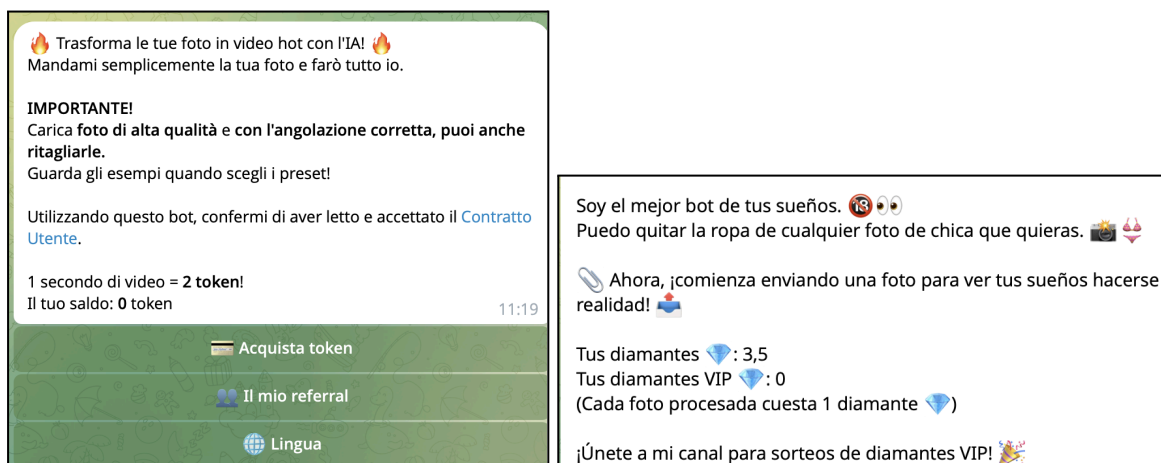


Figure 24. Telegram bots for nudifying women and girls integrated into IBSA groups.

Sapete se esiste un ai tipo grok ma che non censura le foto?

Alguien sabe de promts buenos para grok?

Chi con gemini modifica la foto per segarci sopra?

Descarga la app de grok, y hay una sección que se llama imagine, ahí subes la foto y le pones el prompt

"Convierte su blusa en un top que muestre mucho del abdomen incluyendo el ombligo. Recoge el top para que muestre la parte inferior de los pechos sin mostrarlos por completo"

Figure 25. Example of messages sharing or seeking prompts to manipulate images on chatbots like Grok or Gemini.

The presence and frequent promotion of these bots and tools across both the Italian and Spanish groups illustrates how automation is increasingly integrated into the organization of abusive practices, allowing users not only to redistribute existing material but also to produce new forms of synthetic sexual content — including audio — without the consent of the individuals depicted. By lowering the technical barriers to generating or accessing abusive content, these services contribute to the **scaling and normalization of TFGBV**, transforming what might otherwise require individual effort into a semi-automated process embedded within the platform’s infrastructure.

Monetization practices

Image-based sexual abuse within Telegram ecosystem is also increasingly tied to forms of monetization. Evidence of commercial activities related to abusive content was observed across both the Italian and Spanish groups, suggesting that these communities operate not only as spaces of voluntary exchange of material, but also as informal marketplaces where abusive material and related services are offered for sale.

Several types of content and services are exchanged, promoted, or sought within the Telegram chats. These include large **archives of images and videos**, **access to private Telegram channels** containing curated collections of leaked material, **packs of images, or videos** featuring specific women, and bots.

The circulation of so-called “archives”, i.e., large collections of intimate images and videos gathered without consent, represents a **key element** of many IBSA ecosystems. However, direct links to these repositories are often guarded, and users are typically required to engage in exchanges or payments to demonstrate credibility within the community in order to gain access.

The analyzed dataset contained 2,011 messages using the word “archive,” wherein the discussion often treated archives as commodities to be exchanged, promoted, or sought (see Table 8).

Example	Translation	Code	Definition
<p>**😄 PRIVATE XXX ARCHIVES NOW FOR FREE</p> <p>👉👉** https://xxxxxx https://xxxxxx https://xxxxxx</p>		Promotion of archives	A message that shares an archive link. This includes messages where archives are accessible for free or for a monetary value.
<p>Cerco footjob o teen ita Scambio per archivio 500 video</p>	“Looking for a footjob or Italian teen Exchange for 500 video archive”	Exchange of archive material	A message that suggests an archive can be exchanged for access to something else. Treats an archive as “currency”.
<p>Cerco archivio a pagamento</p>	“I’m looking for a paid archive”	Requests or attempts to obtain access to archives	A message looking for access to an archive or inquiring about an archive. Includes seeking contributions to an archive or to create an archive.

Table 8. Classification of archive-related messages.

Of these 2,011 messages mentioning archives, 55% were about **exchanging** archives, 36% were **promoting** either free or paid archives, and 8.5% of messages were from users **seeking** archives, including seeking contributions for existing or new archives.

Overall, **56% of the analyzed groups and channels contained references to archives**, confirming that the storage and redistribution of large collections of images and videos represents a key practice within these communities. Among these, Italian groups accounted for around 67% of the conversations, while Spanish groups represented approximately 33%.

The ways in which archives are discussed differ across country contexts. In the analyzed Spanish groups, references to archives were almost exclusively promotional, often advertising access to external collections or directing users to other channels where such material could be obtained. However, we did find two **direct links to free archives** in the Spanish groups in our ethnographic analysis (see Figure 26).

In our dataset, messages mentioning “archives” were spread by **89 unique users**, with two main super-posters, who, taken together, posted around 40% of the archive-related messages. These two users were active in both the public and private versions of two Italian groups and sent the same, repetitive messages looking for exchanges or promoting archives. While no relevant connection was observed between Italian and Spanish users discussing archives, there is some permeability between Italian groups, reinforcing earlier findings that show more diversified archive-related activity among Italian groups.

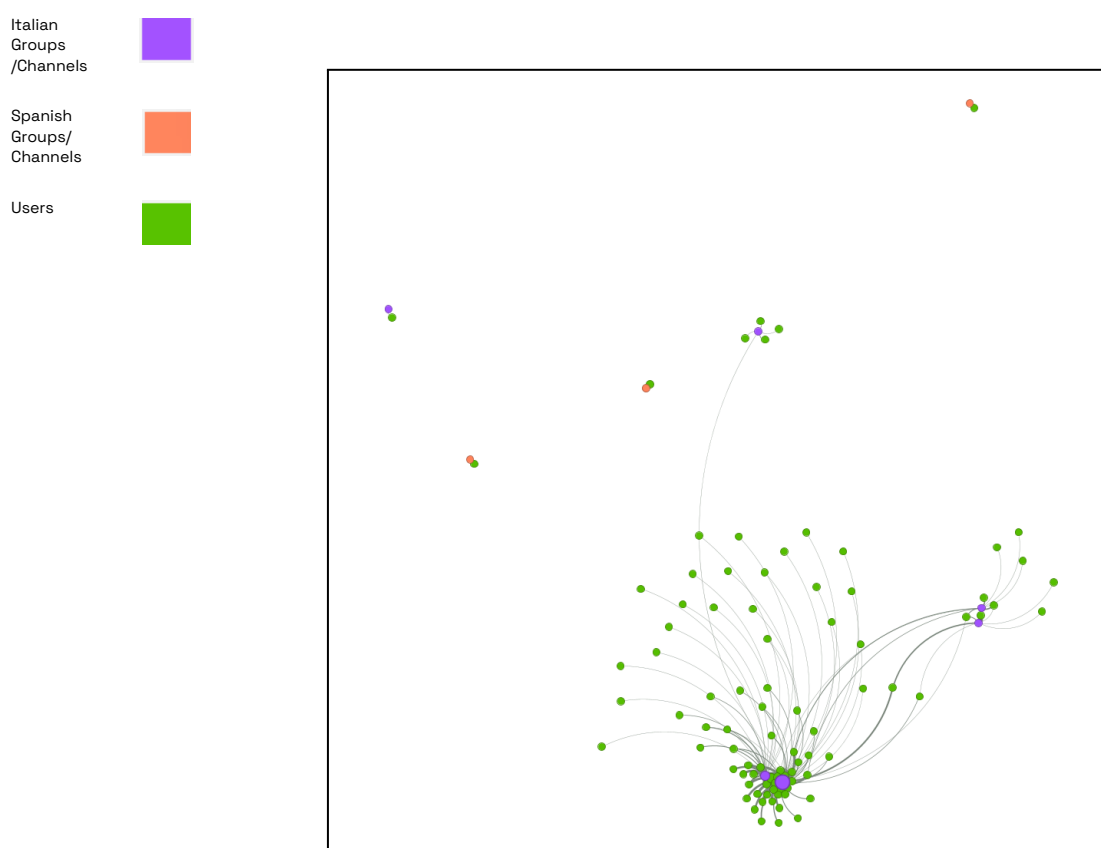


Figure 27. A network analysis between users and groups who send archive-related messages.

Users frequently advertise or seek such archives and packs by specifying the type of material included, e.g., asking whether others possess “complete packs” containing different types of images and videos of specific women or suggesting exchanges (see Figure 28). Non-consensual content is often monetized on Telegram through a one-time fee of **€20-€50 for lifetime access to full channels and archives of abusive material**, or recurring monthly subscriptions starting from €5 (Figure 29).

Vendo pack 12gb foto di una tipa a 5€

Pack con foto e video di tipe disponibile per info privato

Grupo Vip PACKS muy top de amigas , exs, novias todo españolas 🇪🇸🇪🇸🇪🇸

Grupo de nudes de ig, caseros, packs, etc. Se aporta antes de entrar, quien quiera entrar q me hable

Cambio packs x packs sevilla o huelva

Figure 28. Examples of Italian and Spanish messages seeking or offering packs of non-consensual content.

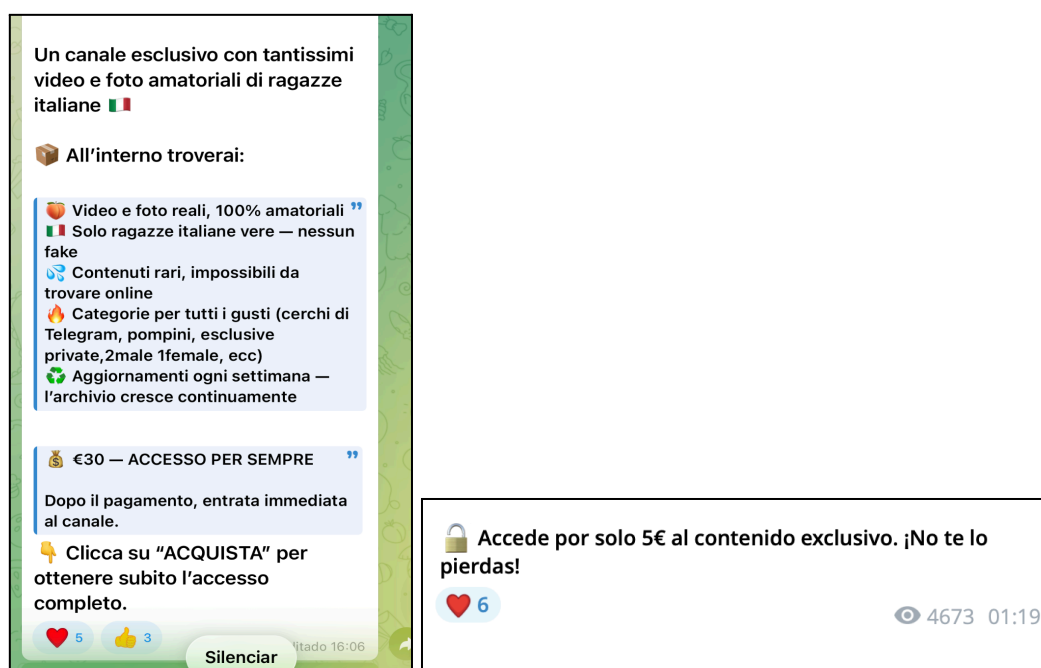


Figure 29. Example of messages containing prices for accessing channels and archives.

Archives remain the most sought after and monetized content, with all channels in Spain and Italy advertising their own archives (Figure 30). Moreover, multiple distinct archives across both Italian and Spanish groups were advertised as containing illegal content such as child sexual abuse material (CSAM), rape, or incest (see Figure 31). Users offer them in the chats through private exchanges.



Figure 30. Channels advertising archives with price offers and content explanation.

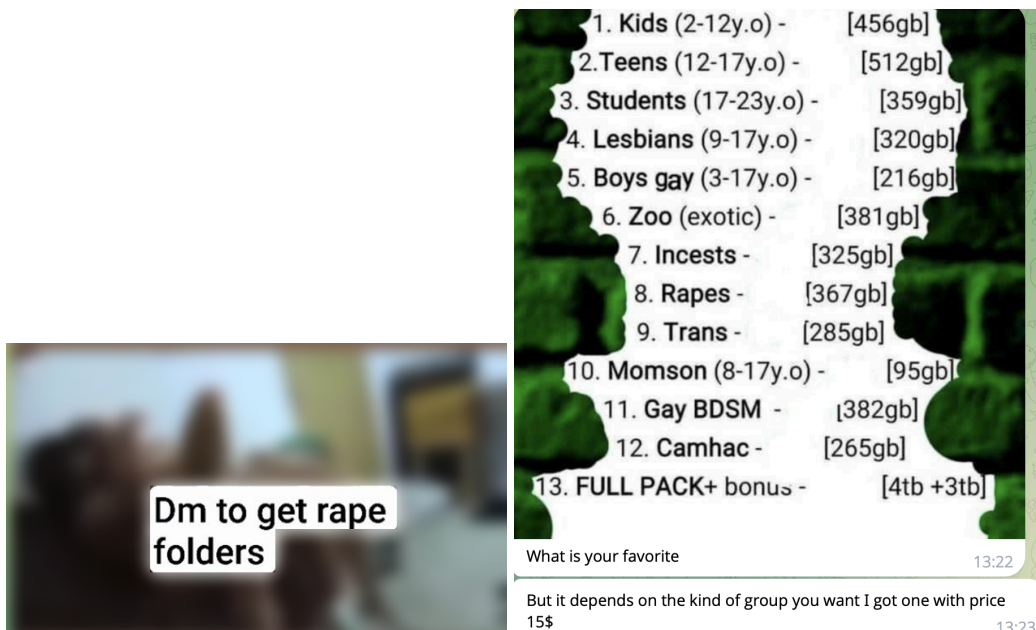


Figure 31. Example of sold archives containing rape, incest, CSAM, and other types of illegal content.

In addition to the sale of existing material, we also identified the promotion of technical services aimed at producing or obtaining abusive content, including hacking services and spyware tools (see Figure 32).

Fornisco servizio di hacker a prezzi bassissimo , solo per oggi i primi 2 che mi scriveranno per hackerare qualsiasi cosa vogliono é gratuita

Hackeo y recupero cualquier tipo de servicio de redes sociales.y
puedo espiar la cuenta de tu pareja envíame un mensaje privado

16:52

I'M AVAILABLE FOR ALL KINDS OF HACKING SERVICE :

- 📱 SNAPCHAT HACK
- 📱 TELEGRAM HACK
- 📱 INSTAGRAM HACK
- 📧 GMAIL HACK
- 📱 WHATAPP HACK
- 📱 PHONE HACK
- 👤 BLACKMAIL HELP
- 📱 FACEBOOK HACK

FOR MORE INFORMATION INBOX

16:17

NEW MEGA CONTENT Menu

- 👤 Mom and kids /pedo mom
- 👤 Rape
- 👤 Incest
- 👤 White teen
- 👤 Black teens
- 👤 CP (all types)
- 👤 Gay
- 👤 Lesbian
- 👤 High school
- 👤 Asia
- 👤 Teen girls
- 👤 Teens blow job
- 👤 Black Cp girls
- 👤 Zoo
- 👤 Kids together

Figure 32. Example of hacker services offered by users.

Messages translations: "I provide hacker services to very low prices, only for the first two people who will write me to hack anything, it's free" - "I hack and get into any type of social network, and I can spy on your partner, send me a message"

Nudifying bots remain the most sought after and offered among the advertised services. In some cases, bots become a source of gain for users, who explicitly recruit affiliates to promote AI-based image manipulation bots to increase their credits, often needed to create images (Figure 33).

📊 Dettagli Referral:

- Guadagno da pagare: €0.00
- Totale guadagnato: €0.00
- Prelievi: €0.00
- Clienti portati: 0

🔗 Your referral link: [REDACTED]

Guadagna il 40.00% Per ogni acquisto!

⚠️ **Disclaimer:** I guadagni da referral sono soggetti a verifica e possono essere annullati in caso di attività fraudolente o violazioni dei termini del servizio, prima di iniziare, contatta l'assistenza

11:20

← Indietro

What can this bot do?

Free removals for everybody! 🗑️ Earn money by inviting friends! 🤖

Cercasi affiliati per bot ai (photo to porn), provvigioni del 40%, info in dm, **NESSUNA SPESA INIZIALE**
Guadagno giornaliero dai 30-60\$ dai primi giorni (dopo sale)

Figure 33. Monetization through bots.

Translation: "I seek affiliates for bot ai (photo to porn) with 40% gain, info in dm, no initial spending, daily rate from 30-60\$ during the first days (then it grows)"

Payments for these services are typically organized through **digital payment systems**, including Apple Pay, Bizum (a Spanish bank-linked payment system), PayPal, and other online transfer methods like cryptocurrency, indicating that these exchanges are embedded within broader digital financial infrastructures (Figure 34). While cryptocurrency transactions offer relative anonymity, Bizum and Paypal potentially leave a traceable financial record, which should be further investigated. All digital financial service providers should consider disallowing, or should be required to ban, transactions that feed into the IBSA ecosystem.

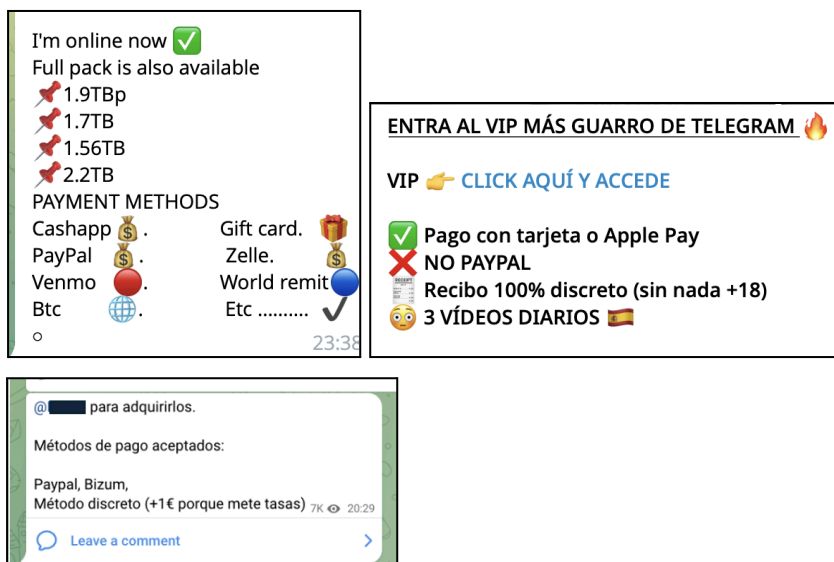


Figure 34. Example of digital payment systems used.

Additionally, the circulation of abusive content is often connected to adjacent Telegram economies, including channels dedicated to cryptocurrency trading, gambling, finance advice, or sports betting, which are often advertised in the groups. In two of the analyzed Italian groups and one Spanish channel, users were required to subscribe to such external channels in order to obtain an invitation link to IBSA groups (see Figure 35).

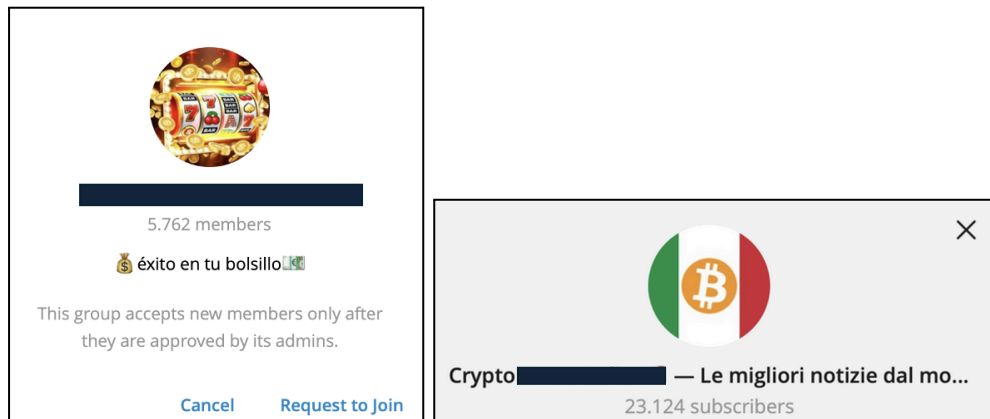


Figure 35. Examples of trading channels advertised in IBSA groups.

Some channels openly claim that content monetization is what allows the channel to remain active, thus inviting users to purchase content and support activities related to AI-fabricated content that “are not for free” (Figure 36). In this way, the circulation of non-consensual intimate images becomes intertwined with profit-seeking activities, transforming abusive practices into economic opportunities for some users. This dynamic also highlights the broader entanglement between user-driven economies and platform infrastructures, where Telegram’s features, including channels, bots, invitation links, and payment redirection systems, enable the organization and scaling of monetized forms of abuse.

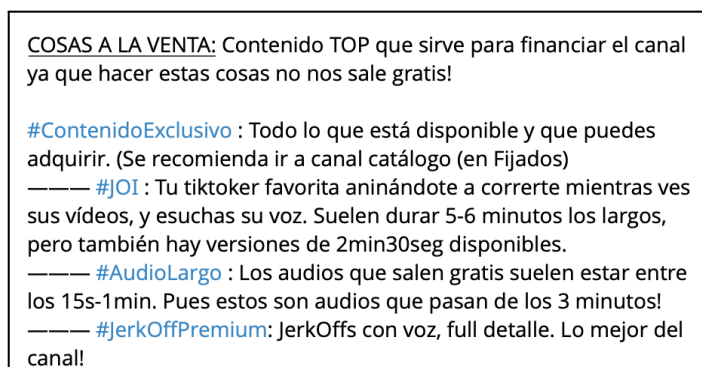


Figure 36. Message asking users to contribute to funding the channel by acquiring content for sale.

4. Telegram as a repository of illegal content across different countries

Our findings show that Telegram offers all the enabling conditions to function as a repository and infrastructural hub for TFGBV, as the platform is used to store, organize, and redistribute abusive material at scale, including through the sharing of invitation links to IBSA groups, embedding of automated bots, circulation of curated archives, and the exchange or sale of packs of intimate images and videos. In this sense, Telegram is a central node where abusive content can be accumulated,

cataloged, and continuously recirculated across interconnected groups and channels. Therefore, the groups analyzed in this study should not be understood as marginal or deviant online spaces, but seen as part of **structured and socially organized environments** that sustain the circulation of image-based sexual abuse and other forms of TFGBV.

The analysis also highlights the **transnational character of these networks**, with Italy and Spain functioning as interconnected hubs, where practices, discourses, and a certain portion of shared content overlap. Shared languages, similar forms of interaction, and the circulation of non-consensual sexual media across groups suggest that these communities are embedded within broader cross-border ecosystems of abuse that should be further investigated and analyzed.

For this reason, the scale of the phenomenon cannot be assessed solely through the number of users present in individual groups or channels. Instead, it must also be understood in terms of the **organization and persistence of abusive activity**, including the volume of content circulating, the frequency of interactions, and the infrastructures that sustain these exchanges. What emerges clearly from this study is that the analyzed communities represent **only the visible layer of a larger ecosystem**, much of which remains difficult to access due to invitation-only mechanisms, private archives, and constantly shifting groups.

These barriers highlight the structural challenges involved in systematically mapping Telegram-based abuse networks, while the platform's features appear to facilitate the development and persistence of this architecture. As we have seen, Telegram in fact offers technical affordances that allow users to organize and scale abusive practices, including integration of bots that automate access to content, generate invitation links, or provide related services. In addition, Telegram's premium features (available at €3 per month) enable users to categorize and organize channels through folder tags, effectively transforming collections of channels into structured repositories that resemble organized forums of content. Other affordances related to privacy and ephemerality further reinforce a **sense of security and impunity** among participants. For example, many groups adopt mechanisms such as automatic deletion of messages after 24 hours, which reduces the traceability of interactions while allowing abusive material to circulate rapidly.

Further, within the broader cross-platform infrastructures sustaining IBSA communities and activities, Telegram is frequently used as a **redistribution hub**, where material scraped, leaked, or captured from other platforms is aggregated, archived, and recirculated across multiple communities. Content originating from social media platforms such as Instagram, Snapchat, or TikTok is systematically imported into Telegram spaces, where it becomes part of a steady repository that can be reshared, repackaged, or monetized, while Reddit remains a central platform to find and share direct links to Telegram's groups and channels.

Despite growing public attention to the issue of image-based sexual abuse in both the Italian and Spanish contexts, user conversations observed within these communities still reveal a high degree of normalization of violence. In many cases, users frame these practices as legitimate forms of entertainment or peer exchange, and occasionally present themselves as victims of censorship when abusive spaces are removed. This dynamic is particularly visible in the Italian context, where participants frequently refer to previously banned archives or websites such as PHICA.net, Mia Moglie, or La Bibbia, lamenting their closure and seeking alternative spaces where similar material can continue to circulate (see Figure 37).

Qualcuno sa se phicanet ha riaperto o qualcuno di simile?
Conoscete altri siti come phica?
Siti come phica?
Ma qualcosa simile a phica esiste?
Qualcuno conosce forum come era Phica?
chi mai stato su phica?
Qualcuno sa qualcosa di phica?
Vi manca il sito phica?
Esistono altri siti tipo phica?
cerco gruppo phica
Ma siti tipo phica non ci stanno?
Scambio gruppo phica

Cosa contiene il MAXIARCHIVIO:
Archivi MEGA 📁 (anche i più famosi come "La B***ia 4.0 & 5.0", "Pack Deep Porn", "Passion Fruit", tanti archivi amatoriali italiani presi dal gruppo FB "Mia moglie", ecc...), **porno a pagamento** (tra cui molti video a pagamento delle pornstar piu' famose, Max Felicitas, Brazzers, Blacked, Bangbros, ecc...), **Spy** 📹 (video rubati delle telecamere di sorveglianza, spogliatoi, camerini), archivi **Onlyfans** 📁 (delle ragazze piu' famose), archivi con porno amatoriale di coppie, nudes e video di ragazze, e tanto altro ancora.

17:01

Figure 37. Example of Italian messages seeking or offering content from Phica.net

Overall, these narratives illustrate how Telegram is perceived by many users as **one of the remaining infrastructures where these practices can persist** and where illegal content can be disseminated, reinforcing the platform's role as a key environment in the contemporary landscape of TFGBV.

4. Telegram's role

This study across two distinct European contexts shows how Telegram plays a role in facilitating forms of abuse against women and girls, revealing the complex interplay between platform governance and the social norms and behaviors of users. In terms of potential platform responsibilities, this analysis makes visible that certain abusive practices are not incidental or episodic, nor are they deviant cultural exceptions. Instead, they appear to be structurally enabled by Telegram (even if not authorized) and transcend geographical borders, aligning with broader global trends in the growth of TFGBV and organized online misogyny. In this context, regulation

has not as of yet adequately addressed the role of Telegram in facilitating gender-based violence.

In 2024, Telegram's premium subscriptions [generated USD 292 million](#), with the subscriber base growing to 15 million by May 2025. Aligning with the platform's business model, these large and very active IBSA channels can generate more advertising and more revenue from premium subscriptions. It is therefore not in the platform's interest to proactively and aggressively moderate content.

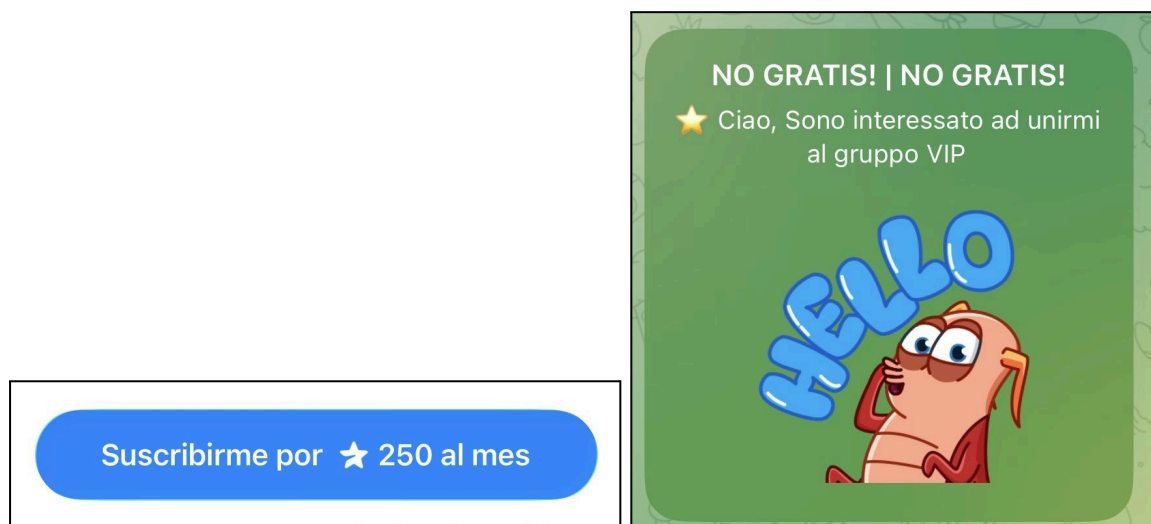


Figure 38. Examples of Telegram features used for monetization inside IBSA channels and groups.

Moreover, Telegram continues to be used as a permissive space where abuse actively connects with other online environments. Crucially, understanding TFGBV in this context requires investigating two dimensions simultaneously: on the one hand, the normalized misogynistic attitudes and behaviors that users bring to and reinforce within these spaces and that require media literacy and education; and, on the other, the structural and design decisions made by Telegram itself, including its moderation choices, privacy architecture, and selective enforcement of its own policies, which together create the conditions for abuse to persist and scale. Addressing IBSA and other forms of TFGBV demands responses that operate at both levels, targeting not only individual perpetrators and their conduct, but also the platform infrastructures and regulatory vacuums that allow such conduct to go largely unchecked.

5. Recommendations

The following recommendations are addressed to national governments and European Union (EU) institutions and reflect the cross-border, multiplatform, and technologically evolving nature of the abuse documented in this research.

5.1 National level (Italy and Spain):

[Legal frameworks](#)

- Ban the **creation** of non-consensual deepfake sexual content, following the EU Directive on violence against women, and mandate that online platforms have automated detection and reporting tools for image-based sexual abuse (IBSA), including abusive synthetic images.
- Amend existing legal frameworks to reflect the technologically evolving nature of IBSA, reconceptualizing it not merely as an individual act of violence, but as a form of **platform-mediated, systematized, and monetized sexual violence** capable of causing continuous and compounding harm to victims. Specifically:
 - In **Italy**, Article 612-ter of the Penal Code (*revenge porn*) should be expanded beyond its current focus on the unauthorized dissemination of sexually-explicit images to also encompass automated distribution mechanisms, algorithmic amplification, and commercial monetization of non-consensual intimate imagery (NCII), recognizing these as aggravating factors that heighten victim harm and perpetrator culpability.
 - In **Spain**, the provisions of Ley Orgánica 10/2022 (*Ley Sí es Sí*), which situate sexual violence within a framework of consent and structural gender-based harm, should be extended to **explicitly codify digital sexual violence** as a distinct and standalone legal category, one that captures not only individual perpetrators but also **platform liability**, duty-of-care obligations, and the role of intermediaries in enabling or profiting from IBSA content.
- Establish **statutory civil liability** for platforms that fail to action verified reports of TFGBV within prescribed mandatory timeframes, with non-compliance leading to compensatory damages and regulatory penalties enforceable by both individual victims and designated public bodies. This should be complemented by a **statutory trusted flagger accreditation regime** granting verified civil society organizations enhanced procedural standing to report TFGBV content.

[Law enforcement and tracing violence](#)

- Train **specialized police units** in platform-specific investigation techniques, including monitoring open or semi-public Telegram channels, tracing links to external archives, and preserving evidence from ephemeral content.

- Establish dedicated **fast-track prosecution pathways** for IBSA cases, reducing the time between reporting and takedown orders, given how rapidly content spreads across interconnected platforms.
- Develop **judicial training programs** to ensure prosecutors and judges understand the impact of AI-generated IBSA, CSAM, and other automatized forms of TFGBV, which may fall into legal gray areas under current national frameworks.
- Create **multi-agency task forces** combining legal experts, victim support services, and digital forensics expertise to handle cases that span multiple platforms simultaneously:
 - [In Italy](#): Create a TFGBV observatory for independent research and data collection.
 - [In Spain](#): Add Telegram to the list of the platforms monitored by [HODIO](#) and specific lines of research and evidence collection about TFGBV.

[Victim support & reporting infrastructure](#)

- Fund dedicated **national hotlines and online reporting portals** staffed by trained operators who can simultaneously advise victims legally, initiate emergency takedown requests, and offer psychological support services (such as [the SIE Digital in Catalonia](#)).
- Introduce statutory obligations requiring the integration of **digital literacy, gender equality, and media literacy** curricula into national education frameworks at all levels, with specific content addressing IBSA, consent, and online sexual violence.

5.2 European level:

[Digital Services Act, EU Directive, and AI Act:](#)

- Designate **Telegram as a Very Large Online Platform (VLOP) under the Digital Services Act (DSA)** as subject to enhanced obligations, including algorithmic transparency, risk assessments for TFGBV, and mandatory trusted flagger programs. Telegram's current semi-ambiguous status has allowed it to avoid the highest tier of DSA scrutiny.
- Extend EU minimum standards for detection, reporting, and removal of IBSA content to messaging platforms operating public or semi-public channels, requiring platforms such as Telegram to apply **proactive content moderation, user reporting mechanisms, and algorithmic transparency obligations** on the same basis as other content-sharing platforms. For private encrypted communications, obligations should be limited to metadata-based risk indicators and robust user reporting channels, preserving encryption integrity while maintaining a meaningful duty of care. The European

Commission should also assess whether the 45 million monthly active user (MAU) threshold for VLOP designation under the DSA remains fit for purpose, given that mid-scale platforms hosting high-density IBSA content may fall below these numbers while causing inordinate harm.

- Mandate that Telegram provide **meaningful victim redress mechanisms** in all EU languages, with maximum 24-hour takedown timelines for verified reports of non-consensual dissemination of intimate images (NCII) and automatic cross-platform notification to prevent reupload. Additionally, mandate proactive risk assessments specifically for coordinated NCII distribution networks, and not only for individual item reports.
- **Harmonize TFGBV criminal definitions** and minimum sentencing thresholds across member states, so that offenders cannot exploit jurisdictional gaps between EU countries, following the EU Directive.
- **Strengthen the AI Act's provisions** on synthetic CSAM and NCII to require that AI model developers and deployers implement technical safeguards preventing the generation of non-consensual and abusive intimate imagery, with mandatory independent auditing.
- Ban the **development, distribution, and commercial use of AI tools** marketed explicitly or functionally for generating NCII across all EU member states, with penalties for operators.
- Establish a dedicated **EU Cross-Platform TFGBV Enforcement Unit** within Europol, with a specific mandate to investigate networks that use Telegram as a coordination hub and other platforms (Reddit, Discord, forums) as source or redistribution nodes.
- Assess whether existing regulation for payment services adequately addresses **the role of payment processors in facilitating the monetization of IBSA content**, and where gaps are identified, issue guidance or legislative proposals obliging payment service providers to implement merchant due diligence and transaction monitoring protocols for known IBSA-facilitating services.

[Research and monitoring](#)

- Commission independent NGOs to produce **regular, systematic monitoring reports on TFGBV** trends across platforms, including Telegram, using standardized metrics to track whether interventions are working.
- **Fund research** on detection technologies for IBSA content and the sociological dynamics of platform-hopping TFGBV networks, to directly inform future regulatory updates.