JUGENDSCHUTZ.NET

2024 Report

Protection of minors on the Internet

Risks and need for action

Dear readers,

We live in turbulent times. Not only are the wars in Ukraine and the Middle East unsettling us and fueling fears about the future, but the volatile transatlantic relations are also undermining our previous understanding of a peaceful and stable world order. Central social values such as freedom and equality, as well as the veracity of facts and scientific findings, are being called into question.

The internet holds up a mirror to us here: Online debates are becoming increasingly heated, polemical, and reckless. Services like Facebook and X are full of hateful posts that denigrate groups of people and discredit democratic institutions. On Instagram and TikTok, we see images of graphic violence and risky behavior. Even the inhibition threshold for sexual assault, including against minors, is lowering.

Our report vividly demonstrates the risks children and young people face when using digital services. Many of these risks could be reduced if providers finally implemented effective protection concepts. Instead, they prefer to focus on innovation through generative artificial intelligence. The safety of children and young people is not a priority.

At German and European level, legislators have laid a solid foundation for regulating large, internationally operating tech companies. Now it's time to use these instruments effectively and join forces to force providers to act.

Stefan Glaser

Head of jugendschutz.net

Our mission

jugendschutz.net is committed to ensuring that children and adolescents can use the internet as safely as possible. We act on a legal mandate. Our responsibilities are defined in the Interstate Treaty on the Protection of Minors in the Media (JMStV) and the Youth Protection Act (JuSchG).

Identify risks

We research online platforms popular with children and young people to identify dangerous phenomena and trends early on. We share our findings with educational practitioners and the general public, as well as policymakers and regulatory authorities.

Combat violations

We investigate reports of violations of child protection laws that reach us via our online complaints office or partner organizations. We notify providers of violations so they can quickly remedy the situation, and refer cases to the media supervisory authority.

Evaluate prevention

We examine digital services and evaluate precautionary measures to reduce risks. Our assessments provide regulators, youth policymakers, and providers with important information on structural deficits and areas for action.

Identify risks

Threats and risks

jugendschutz.net examines the internet for risks to children and young people, focusing on popular social media services, messaging apps, video platforms, and games. Furthermore, jugendschutz.net continuously monitors new technological and content-related developments that could create or exacerbate risks. This also includes the effects of social or political crises.

The focus of the 2024 work was on research and analysis on extremism, gaming, violence, cyberbullying, pressure to buy and play, challenges, as well as deep nudes and sexualized violence.

Topics at a glance (only available in German)

- **Report** - Der Israel-Hamas Konflikt online
- **Report** - Islamistisches Influencing
- **Report** - Demokratiefeindliche Anbahnungsrisiken auf Discord
- **Report** - Gore im Wandel
- **Report** - Straßenumfragen auf Social Media
- **Report** - Lootboxen
- **Report** - Wie sicher ist Fortnite?
- **Article**- Kurzvideo-App Likee
- **Article** - Pädokriminelle Vernetzung auf Telegram
- **Article** - Sexualisierte Deepnudes Minderjähriger
- **Article** - Porno-Deepfakes fördern digitale Gewalt
- **Article** - Sephora-Kids, Ohnmachtsspiel, Mukbangs und Superman-Trend

Islamist influencers spread hate

Both the ongoing Middle East conflict and political events such as the US election had a noticeable impact on the digital space in 2024. Extremist groups are exploiting these developments to negatively influence young users with their posts. Islamist influencers, for example, are mixing everyday topics and advice on religious living with anti-democratic and anti-human statements directed against queer people or the State of Israel. These posts and videos sometimes achieve considerable reach.

Extremists use crises and everyday issues to influence young people on social media.

Read reports: “Der Israel-Hamas-Konflikt online" and "Islamistisches Influencing"

Discord: Gamers targeted by extremists

Right-wing extremists and Islamists are using Discord, a service popular among young gamers, for their own purposes. Due to the provider's inadequate precautionary measures and lack of moderation, they can spread their ideas unhindered and specifically reach young people with an affinity for gaming. Their goal is to engage in dialogue with young users and win them over to their extremist views. The possibility of direct contact in seemingly harmless chat rooms poses a particular risk.

> Lack of moderation in chats opens the door for extremists to target young gamers.

Read the report

Drastic violence as a test of courage

Gore sites with disturbing violent content exert a strong fascination on young people and often serve as a test of courage. Social media have added new channels of distribution and reception, as well as new forms of representation. Confrontation can occur, for example, via the platform's own recommendation pages or by clicking on a hashtag. Although many platforms prohibit the uploading of graphic content and take action against it, it still spreads. Users publicize such content through reaction videos, so-called "Don't Google" warnings, or by showing the content with graphic scenes omitted.

Gore content is being distributed in new formats and as a playful challenge.

Read the report

Street polls:
Gateway to cyberbullying

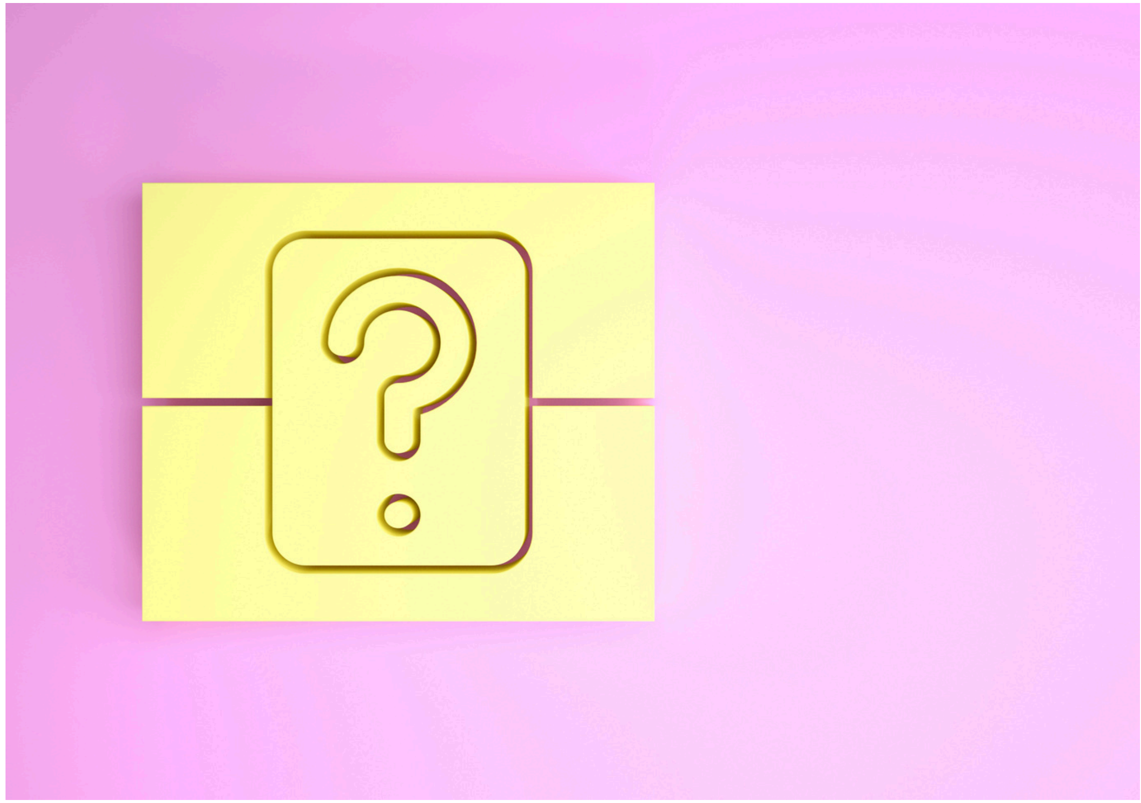
Street polls were among the most popular social media formats in 2024. These spontaneous surveys of passersby, similar to TV formats like TV Total, often generate laughter at the expense of the participants – including teenagers and children. Some of these videos aim to embarrass people, spread racist stereotypes, or encourage risky behavior such as eating extremely spicy foods with rewards. As a result, respondents are often subjected to ridicule and defamatory comments.

Creators expose children and young people to increase their reach on social media.

Read the report

Pressure to buy and play through loot boxes

As part of the debate surrounding computer game addiction, gambling, and cost traps, jugendschutz.net analyzed loot box systems in approximately 20 online games. The results showed that not all of them are equally risky. A loot box becomes problematic if it contains rare, sought-after items and is integrated into the game's reward system. The problems are exacerbated if they are collected and opened outside of gameplay and are emotionally charged by animations and sounds. When these factors come together, loot boxes can encourage excessive gaming and become a cost trap.



Loot boxes can become problematic in games with high emotional engagement.

Read the report

Risky trends and challenges

In 2024, children and teenagers filmed themselves jumping and being caught by friends in the "Superman Challenge." However, the viral TikTok trend carried a high risk of injury. The "stunt" often failed, resulting in accidents that also went viral in fail compilations. Risky challenges such as the "choking game" and the "deodorant challenge" also claimed the lives of minors. Furthermore, high-profile creators in "mukbangs" demonstrated unhealthy eating behaviors such as excessive gorging or the consumption of extremely spicy foods. The Sephora Kids trend, in which children advertised expensive cosmetics, also promoted unrealistic beauty ideals.

Dangerous tests of courage quickly go viral and have a strong pull effect on children and young people.

Read snippets: "Sephora-Kids, Ohnmachtsspiel, Mukbangs" and the "Superman-Trend"

Deepfakes and the sexualization of minors

Due to advancements in artificial intelligence, deepfakes and deepnudes can now be created quickly and without technical expertise. Not only are there numerous freely accessible deepfake generators for pornography that enable sexualized violence, but some services also allow the creation of sexualized images of minors, opening the door to abuse. These images can be shared and used as often as desired to expose, bully, and blackmail minors online and offline. Victims of digital sexualized violence can suffer long-term physical, psychological, and social consequences.

AI can easily be used to sexualize everyday images of children.

Read articles: "Sexualisierte Deepnudes Minderjähriger" and "Porno-Deepfakes fördern digitale Gewalt"

Alternative platforms for sexualized violence

The video portal **Likee** offers similar functions to TikTok, but implements fewer precautionary measures. It is also used by children who fear being blocked on other platforms due to their age. jugendschutz.net identified significant risks such as sexual harassment and grooming in live streams and comments. Pedo criminals also used the platform to trade and exchange images of sexual abuse.

The messenger service **Telegram** is also a hub for depictions of sexualized violence. Unhindered by the operator, perpetrators spread sexual images of minors there.

Services like Likee and Telegram allow pedo criminals to operate unhindered.

Read articles: Likee, Telegram

Combat violations

Handling violations

jugendschutz.net examines and investigates violations of youth protection regulations online and works to ensure their prompt removal. jugendschutz.net accepts reports of content that may violate the Interstate Treaty on the Protection of Minors in the Media (JMStV) through its online complaints office. Furthermore, the office processes reports of digital sexualized violence with a German context submitted by partners of the Association of Internet Hotline Providers (INHOPE).

Since jugendschutz.net's processing of reports and violations depends both on the activities of external information providers and its own thematic priorities, the reported figures only allow limited conclusions about actual empirical overall developments.

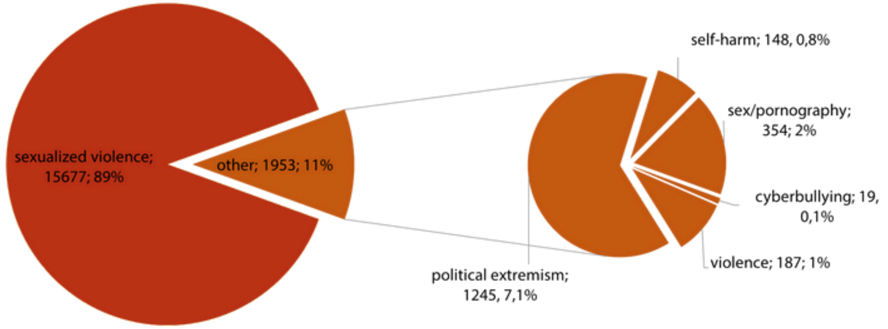
Total registered violations

17.630

jugendschutz.net registered a total of 17,630 violations in 2024. Compared to previous years (2023: 7,645; 2022: 7,363; 2021: 6,865), the number has thus more than doubled compared to the average of previous years (7,291). This development is due to the enormous increase in cases of sexualized violence reported to jugendschutz.net.

🟥 Sexualized violence dominated work.

Violations by topic



Sexualized violence accounted for around 90% of the violations processed by jugendschutz.net (2023: 5,112/67%; 2022: 4,866/66%).

A significant increase was also recorded in **political extremism**, even though it only accounts for 7% of the total: 1,245 violations were registered, almost 400 more than in the previous year (2023: 852/11%; 2022: 945/13%). Of these, 732 were related to right-wing extremism and 513 to Islamism. 1,221, or 98%, were absolutely inadmissible (2023: 96%; 2022: 98%).

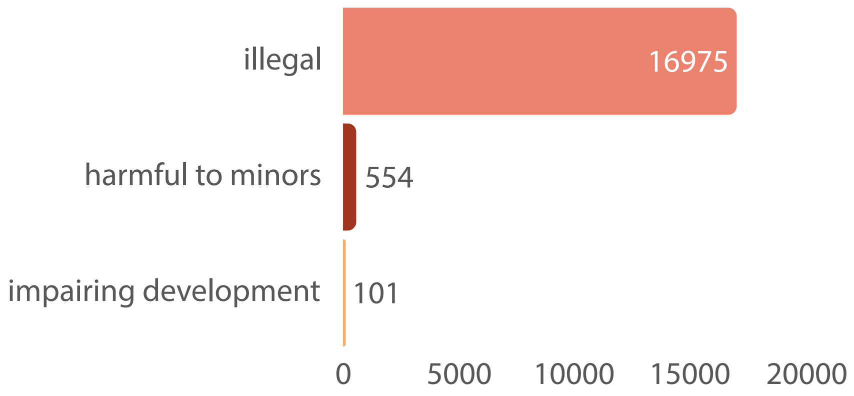
Services related to **sex/pornography** accounted for only 2%. A sharp decline was also recorded here: 354 cases were attributable to this (2023: 915/12%; 2022: 575/8%). Fifty-nine violations (17%) were classified as absolutely inadmissible (primarily animal and violent pornography). The majority, 252 cases (71%), involved content harmful to minors (primarily simple pornography); 43 were content harmful to development.

A decrease can also be observed in the area of **violence**, with 187 violations and a proportion of 1% (2023: 266/3%; 2022: 398/5%).

jugendschutz.net also registered fewer cases of **self-harm** and **cyberbullying** than in previous years.

Sexualized violence and political extremism are on the rise.

Violations by degree



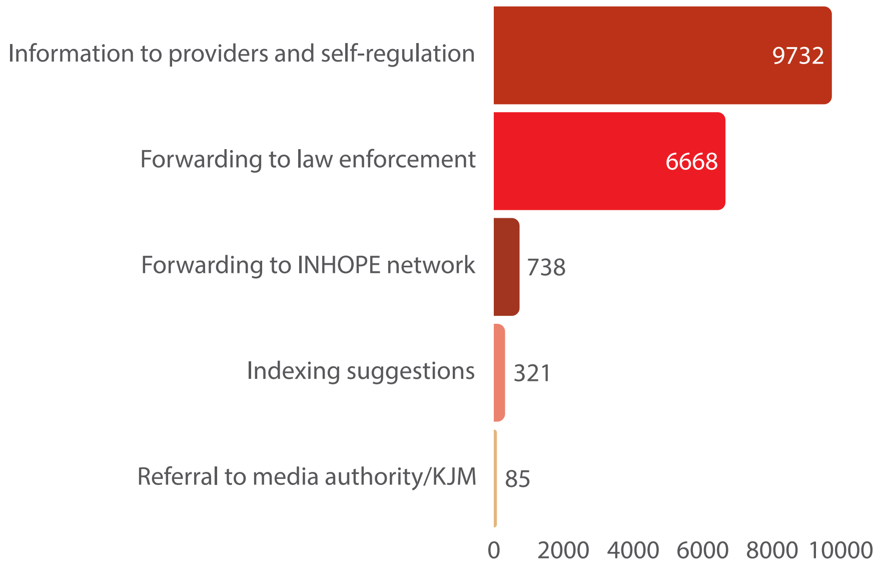
16,975 of the violations (96%) involved content whose distribution is strictly prohibited under the Interstate Treaty on the Protection of Minors in the Media (JMStV) (2023: 82%; 2022: 84%). These primarily included so-called child pornography (14,567) and youth pornography (825), as well as symbols of unconstitutional organizations (1,099).

jugendschutz.net classified 554 violations (3%) as harmful to minors (2023: 15%; 2022: 14%). 210 concerned simple youth endangerment, 243 simple pornography, and 88 obviously serious youth endangerment or indexed content.

In 101 violations (1%), a possible impairment of development or integrity was assumed (2023: 3%; 2022: 2%), of which 89 were considered to be developmentally detrimental to young people.

96% of the registered violations were classified as absolutely inadmissible.

Activities against violations



In 9,732 of the 17,630 registered violations, jugendschutz.net alerted providers and self-regulatory bodies to violations and demanded their removal. This action was successful in 9,624 cases (99%).

In 6,668 cases involving so-called child or youth pornography, as well as in cases of danger to life and limb, jugendschutz.net directly informed law enforcement. jugendschutz.net forwarded 738 cases involving abusive content without a German investigation to INHOPE partners.

jugendschutz.net forwarded 85 cases to the Commission for the Protection of Minors in the Media (KJM) and the State Media Authorities so that they could examine whether to initiate supervisory proceedings. In addition, the agency forwarded 321 cases to the KJM or directly to the Federal Agency for the Protection of Children and Youth in the Media (BzKJ) for content indexing.

In 99% of cases, providers responded to deletion requests from jugendschutz.net.

Evaluate prevention

Precautionary measures under scrutiny

To enable children and young people to participate in the internet in an age-appropriate manner, platform operators are legally obligated to take appropriate precautionary measures. In Germany, the Youth Protection Act (JuSchG) formulates regulations for better protection of minors. Furthermore, the Digital Services Act (DSA) is an EU-wide set of rules that obliges digital services to minimize systemic risks on their platforms.

jugendschutz.net monitors precautionary measures, new features and functions on services that are particularly popular with minors. In 2024, the focus was on **TikTok**, **Instagram**, **YouTube**, **Snapchat**, **X**, and **Facebook**. The gaming platform **Fortnite** was also examined (see report).

Test areas 2024 at a glance

Verified precautionary measures

- Age assurance: key to safe participation
- Security settings
- Community Guidelines
- Help and guidance
- Reporting systems

New risky features

Labeling AI-generated content

Fortnite: Service in focus

Age assurance: key to safe participation

Reliable age assurance during registration for a digital service is the necessary basis for many precautionary measures to protect minors. Only if it is known which age group users are in can their different protection needs and constantly growing abilities be taken into account.

All popular services set a minimum age and offer age-based access. **However, age assurance is still either not or inadequately performed**. Registration usually only requires the user's date of birth. If the information is below the minimum age for the service, the process is usually interrupted and can be easily restarted.

Social media services are increasingly using **artificial intelligence** to assess age based on user behavior. Users below the specified minimum age are identified and excluded from the service—or the age specified during registration is corrected, and age-appropriate default settings are subsequently activated. However, this requires analyzing usage over a certain period of time; the protection solution does not take effect immediately.

A system that enables reliable and data-efficient age assurance would be a central building block for effective youth media protection.

Security settings

Secure default settings in digital services are a key prerequisite for enabling age-appropriate participation for young people. All regularly reviewed services offer basic protection. However, this only applies if the age information is truthfully stated.

With the introduction of "teen accounts" last year, **Instagram** improved its protection concept. This provides minors' accounts with secure default settings; changes to those under 16 are only possible with parental supervision. Private profiles allow only confirmed followers to view posts. There are also strict content filters and options to prevent unwanted interactions, as well as pause and sleep functions designed to encourage conscious use.

“Teen accounts” on Instagram are intended to protect young users from unwanted contacts.

Community Guidelines

Some services have improved their community guidelines. However, it is crucial that violations of their own policies are consistently sanctioned.

YouTube's harassment and cyberbullying policy now prohibits content that uses realistic simulations to depict the circumstances of death or the suffering of deceased minors or victims of serious violent crimes.

TikTok has tightened its community guidelines by introducing new definitions of hate speech. The service is also now imposing stricter sanctions for risky behavior in LIVEs by removing monetization options.

YouTube is tightening rules for violent simulations, TikTok is taking stronger action against hate speech and risky behavior in LIVEs.

Help and guidance

Young users need guidance on safe online behavior, information on how to deal with stressful content, and support in emergencies. The services offered by providers are important, but resources for parents can also be helpful.

TikTok now offers users who report content related to suicide, self-harm, hate speech, or harassment on the app information about support and counseling services immediately after the report. In Germany, the TikTok account of the Helpline Nummer gegen Kummer is linked, among others.

Snapchat's Family Center now allows parents to request their child's location. However, this has a risky side effect: This request could potentially result in the child's location being inadvertently shared with all of their friends.

TikTok improves support after reports, Snapchat implements risky location query.

Reporting systems

An easy-to-use and effective reporting system that provides rapid remedial action in the event of violations is particularly important for the protection of children and young people. Reporting is often the only means for users to alert providers to dangerous content or contacts. Therefore, it is important that these systems promptly investigate complaints and take consistent action in the event of violations. This usually involves removing or blocking the content.

In 2024, jugendschutz.net conducted systematic tests on the major social media services Instagram, YouTube, TikTok, Facebook, and X. Due to its particular relevance, **the focus was on the topic of political extremism**. A total of 1,087 cases of this kind were recorded on the services examined.

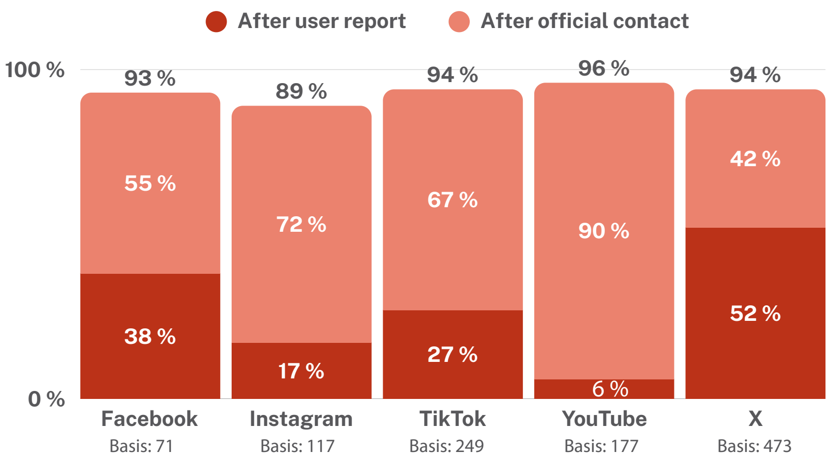
Procedure

To review the reporting systems, jugendschutz.net uses a two-stage process:

In the first step of the reporting tests, violations are submitted as user reports. This means that jugendschutz.net is not identifiable as the sender.

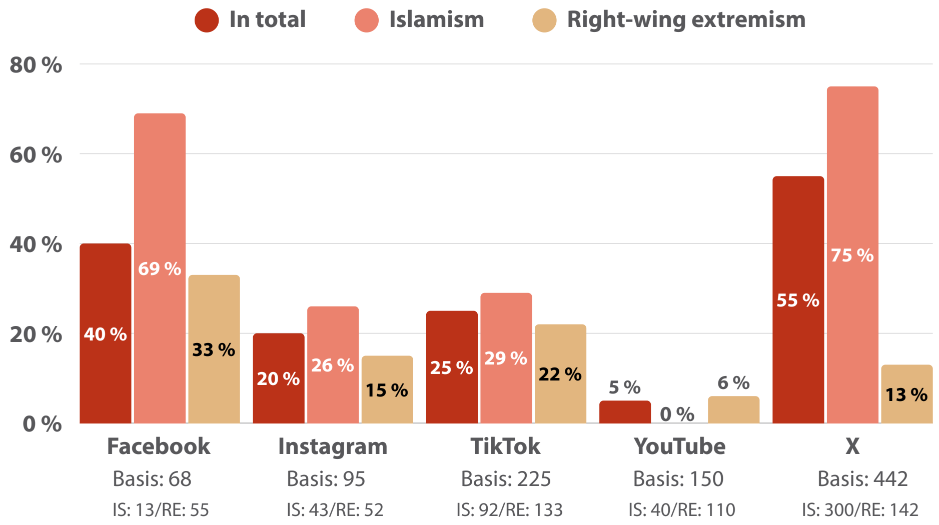
If the reported content hasn't been deleted or blocked after seven days, jugendschutz.net officially requests its removal. Whether the service has taken action will be reviewed after another seven days.

Extremism removal rates



The results of the reporting tests show that the services deleted the majority of violations only after official contact from jugendschutz.net. They removed content that the agency reported as a user significantly less frequently. The results are particularly sobering for YouTube (6%), Instagram (17%), and TikTok (27%). This shows that services continue to neglect their obligation to promptly remedy reported violations.

Ninety percent of the **extremist** violations involved criminal symbols (980 of 1,087). Those related to Islamism were, on average, more effectively removed than those related to right-wing extremism (Islamism: 272 of 488, or 56%; right-wing extremism: 81 of 492, or 16%).



New risky features and functions

New features in digital services not only offer users advantages. They can also pose risks or increase dangers, especially for minors. This creates gateways that are not yet or only inadequately covered by existing precautionary measures.

On **YouTube** Shorts, the new "Remix" feature lets you embed other users' videos into your own. This is available to everyone by default, and you won't receive any notifications about the use of your video. Even if you delete the original, the remixes remain. This results in a loss of control over your own content and creates a gateway for cyberbullying.

Snapchat's new "Sponsored Snaps" advertising format delivers direct ads to users' inboxes. In addition, certain locations are displayed as "Promoted Places" by advertising partners on users' Snap Maps. This brings advertising into central and previously private areas of the service.

Giving a "Team Heart" on **TikTok** can create pressure to buy or contribute to excessive use. Users can purchase Team Hearts with TikTok's native currency and send them to creators to join their team. Sending additional gifts, commenting, or watching live streams increases the team membership level.

Labeling AI-generated content

In 2024, the question of how to deal with artificially generated content and its recognizability - for example in the form of a label - played a role in almost all popular services. The following measures were taken:

TikTok relies on automated labeling of AI content. In collaboration with the Coalition for Content Provenance and Authenticity (C2PA), video metadata is used to determine whether the content is AI-generated. The method works if the provider of the AI software used is part of the initiative and has marked the content accordingly. The metadata must also not have been manipulated by users.

At the beginning of the year, **Facebook** and **Instagram** introduced the highly visible "Made with AI" label, which was changed several times over the course of the year.

Users can label the content when uploading, and the services also work with C2PA to recognize and label AI-generated content.

YouTube's guidelines stipulate that users must flag heavily modified or synthetically generated content when uploading. If this option is enabled, a notice appears in the accompanying text of the video. For selected topics such as news, health, or finance, YouTube displays the notice directly in the video.

The service also uses a positive label for "real" content: Videos recorded with a camera from a company affiliated with C2PA are automatically labeled "Recorded with a camera." As of the end of 2024, this standard had not yet been widely rolled out.

Fortnite: Service in the spotlight

Fortnite has been one of the most popular online games among young people for years. The service has now evolved into a comprehensive gaming platform. To protect young people, Fortnite relies on strict default settings that automatically activate restrictions, such as chat and purchase bans, for users under 16 years of age. Full use is only possible with parental supervision. The use of the IARC age rating for user-generated "islands" on Fortnite provides guidance.

However, Fortnite shares a core problem with many popular services: There's no reliable age assurance during registration, which means the precautionary measures already implemented aren't effective. The reporting system is also overly complicated.

> As with many services, the lack of reliable age assurance is the biggest problem with Fortnite.

Read the report: Fortnite

About jugendschutz.net

jugendschutz.net serves as the joint competence center of the federal government, the states, and state media authorities for the protection of children and young people on the internet. jugendschutz.net looks closely at dangers and risks in internet services specifically popular among young people. The centre works to ensure that violations of youth protection laws are removed and urges providers and operators to design their content in a way that allows children and young people to use the internet free of troubles.

The German youth ministries founded jugendschutz.net in 1997. The tasks were laid down in the Interstate Treaty on the Protection of Minors (JMStV) in 2003. Since then jugendschutz.net has been organizationally linked to the Commission for the Protection of Minors in the Media (KJM).

In 2021, the Federal Government also assigned jugendschutz.net a statutory mandate in the Protection of Young Persons Act (JuSchG).

The work of jugendschutz.net is funded by the Supreme Youth Protection Authorities of the federal states, the state media authorities and the Federal Ministry for Education, Family Affairs, Senior Citizens, Women and Youth and the European Union. jugendschutz.net runs a hotline accepting reports about violations of youth media protection laws.

jugendschutz.net accepts reports of violations of youth media protection via its Online complaints office.

Imprint

Contact

jugendschutz.net
Kaiserstraße 22
55116 Mainz
buero@jugendschutz.net
www.jugendschutz.net

Responsible

Stefan Glaser

Editorial staff

Dr. Steffen Eisentraut, Murat Özkilic

Stand

May
2025

jugendschutz.net is funded by

kjm Kommission für Jugendmedienschutz

die medienanstalten

Gefördert vom:

Bundesministerium für Familie, Senioren, Frauen und Jugend

Im Rahmen des:

KJP Kinder- und Jugendplan des Bundes
STÄRKEN, WAS DIE ZUKUNFT TRÄGT.

GAmM Gutes Aufwachsen mit Medien

Kofinanziert von der Europäischen Union