2021 REPORT

Protecting Minors on the Internet

Risks and the Need for Action

JUGEND
SCHUTZ.NET

IMPRINT

Contact
jugendschutz.net
Bahnhofstraße 8a, 55116 Mainz
Tel.: 0049 6131 3285-20
buero@jugendschutz.net
www.jugendschutz.net
twitter.com/jugendschutznet

Legally responsible
Stefan Glaser

Editor
Andrea Kallweit

Translation
Susan Jones

Graphic design
elements of art

As of
June 2022

Supported by

kjm Kommission für Jugendmedienschutz

die medienanstalten

Funded by

Federal Ministry for Family Affairs, Senior Citizens, Women and Youth

as part of the federal programme

Live Democracy!

GUTES AUFWACHSEN MIT MEDIEN

This publication does not represent a statement of opinion by the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth or the Federal Office for Family and Civil Society Work. Responsibility for the content is borne solely by the authors.

MKFS MEDIEN KOMPETENZ FORUM SÜDWEST

STIFTUNG

Providers' Measures towards Protecting Children and Adolescents are Insufficient

Fun and entertainment, information, communication, creativity: for children and adolescents, there is much to be experienced and discovered on the internet. They can game there, watch videos, chat with others, and try out new ideas. During the pandemic, as contact restrictions affect social life and learning, the net presents itself primarily as a source of opportunities. However, as this report shows, the web continues to harbor dangers and a wide range of risks.

Extremists circulate anti-democratic and misanthropic propaganda in such contexts as Let's Play videos or on TikTok. Depictions of sexualized violence toward children are uploaded by the score onto file-hosting services and are further disseminated from there. Risky and sometimes life-endangering challenges go viral and are taken up unthinkingly by other users. Providers of games that attract children employ manipulative strategies to fetter young people to their product – along with its cost traps and data security risks. These are only a few of the existing problems we are faced with.

As in previous years, jugendschutz.net examined the preventive measures implemented by service providers – and the outcome is sobering. Although a few providers have improved their default settings or support functions, they are still lacking a reliable means of differentiating access according to age, which would be a reasonable measure of "basic protection" from endangerment.

On social media, the response to user complaints remains unsatisfactory: far less than half of the violations reported are actually removed in a timely manner. There are still no easy-to-use technical systems in place that could enable parents and guardians to reduce, in accord with children's age, the risks that they are exposed to. All in all, the industry has a long list of improvements to attend to.

This year, jugendschutz.net is celebrating its 25th anniversary. Since 1997, our staff has been evaluating content and phenomena on the net and providing valuable assessments for supervisory authorities, politicians, and everyday practice – urging providers to remove material that violates youth protection laws, and referring cases for investigation to the Commission for the Protection of Minors in the Media and to the media authorities of the German states. Our teams also develop ideas toward optimizing the standards for protecting young people on popular websites. The work undertaken by jugendschutz.net is often burdensome due to the content encountered, but at the same time it is extremely valuable. For it supports children and adolescents coming of age in the internet age, unscathed by it. My heartfelt thanks to my colleagues for their untiring commitment!

Stefan Glaser

Stefan Glaser
Head of jugendschutz.net

CONTENTS

DANGERS AND RISKS

In the course of its continuous monitoring of online risks, jugendschutz.net identifies dangers for children and adolescents. The focus is on popular social networks, messaging services, video platforms, and games. In all of these, political extremism, hate, and violence are to be found. Minors are also exposed to the threat of sexualized violence via risky contacts and of self-endangerment in various forms.

Extremists take advantage of the topic of Corona vaccinations to advance conspiracy myths about thought control or the decimation of the population. They attempt to normalize anti-democratic and rassist attitudes by presenting themselves as typical young people on platforms such as TikTok.

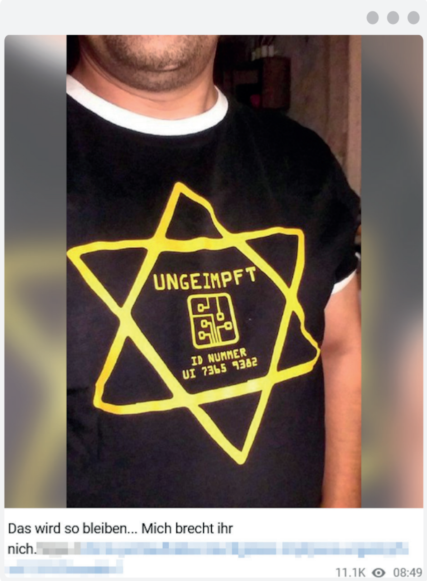
jugendschutz.net has observed a significant increase in the number of depictions of sexual abuse online. Young people encounter violence on the net in many different contexts: jugendschutz.net pursued research, for example, on the hype surrounding the series Squid Game, which raises concerns about the protection of minors. Other questionable websites can mislead unstable children and adolescents to engage in unhealthy eating habits. Furthermore, young people are lured into reckless dares.

Youngsters are often entirely unprotected due to the fact that platform providers and the gaming industry have no age-appropriate access restrictions or effective age varification in place. Providers cause additional risks by creating manipulative designs for games and thus paving the way to excessive use. In general, children and adolescents cannot see through this strategy.

Conspiracy myths: Right-wing extremists take advantage of the pandemic

Hate and vilification in the context of the Corona pandemic and its countermeasures continue to figure as a dominant topic. Where the virus had previously been portrayed as a biological weapon, and the "plandemic" as a deceptive maneuver of politicans and the media seeking to establish a new world order, more emphasis in 2021 was placed on the Corona vaccinations as a subject of conspiracy myths. The vaccinations were said to serve as a means of thought control or of decimating the population.

Right-wing extremists and conspiracy followers inhabit a protest milieu in which anti-semitic slander is circulated. At the same time, anti-vaxxers compare themselves with the Jews persecuted by the Nazi regime – and by doing so, they downplay the Holocaust. They see themselves as faced with an existential threat scenario being enacted by an international "Corona regime", and they call for "resistance" and for violence, for example against politicians.



Das wird so bleiben... Mich brecht ihr nich. [redacted]

11.1K 08:49

Anti-vaxx t-shirt advertised online: asserting a status equal to that of persecuted Jews, and claiming that the vaccine contains a microchip.
(source: Telegram; original not pixelated)

Taking effective measures against hate, rabble-rousing, and propaganda is an international task. jugendschutz.net cooperates in the International Network Against Cyber Hate (INACH) with 31 members in more than 20 countries.

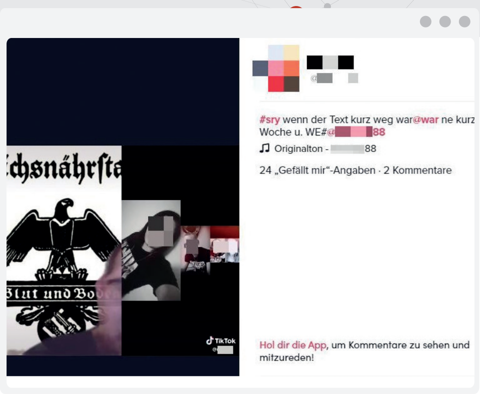
The aims are to delete illegal hate content as quickly as possible, to exchange knowledge, and to strengthen civil courage on the net.

INACH is also the main dialogue partner for the European Commission in matters concerning hate speech. As a result, the EU behavioral code against illegal hate speech on the internet is reviewed on a regular basis. INACH members across Europe monitor the response of platform providers when hate content is reported.
(inach.net)

Online rabble-rousing: TikTok is trending

TikTok is currently one of the most popular social media services among children and adolescents. It features the option to post videos online or to stream videos live. Right-wing extremists exploit the popularity of the platform to present themselves and their ideology as appealing to young people.

They make a pitch for the life-style of right-wing extremism by engaging topics such as vacation trips, cooking, or clothing. Videos provide clips of right-wing rock bands, Neo-nazi ballads, and right-wing extremist rap. The right-wingers use hashtags auch as #heimat-liebeistkeinverbrechen (love-of-your-land-is-not-a-crime) for networking, with typical insider codes. There are also profile names and descriptions that include vilification and forbidden slogans.



[redacted]
@[redacted]

#sry wenn der Text kurz weg war@war ne kurz Woche u. WE#@[redacted]88

♫ Originalton - [redacted]88

24 „Gefällt mir“-Angaben · 2 Kommentare

Hol dir die App, um Kommentare zu sehen und mitzureden!

Right-wing extremists networking via TikTok and revealing their ideological affiliation by using unmistakeable symbols. (source: TikTok; original not pixelated)

Islamists, as well, have been discovering TikTok's usefulness for their pernicious aims. Activist groups such as “Muslim Interaktiv” promote upcoming events. They stylize forbidden organizations as supposed victims of anti-Muslim political policies. Clips from live activities are posted online to extend the audience range of extremist actions and campaigns.

TikTok is also used to attract young people to content on other platforms. There, they are then confronted with extremist propaganda.

"Fleeting" content: Hate in real time

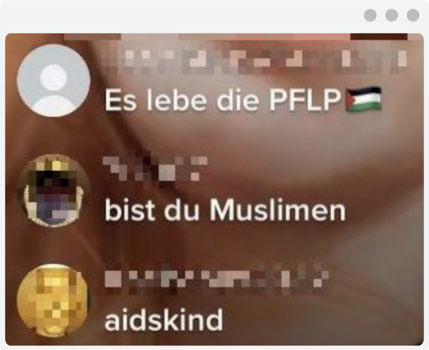
Quite a few services now enable posting of stories that will only be available for a limited time, or of live streams with simultaneous live chats. Children and adolescents love this type of function: it offers the immediacy of an event and the possibility of (live) interaction with streamers. Similarly, streaming their own material and experiencing direct contact with others provides a certain thrill.

Such real-time functions were used by right-wing terrorists in Christchurch, New Zealand, and in Halle (Saale), Germany, to disseminate videos of their attacks. Young users can also be confronted with hate and vilification in places such as chats that run alongside live debates on YouTube. Particularly when the topic or event tends to polarize opinions, the comments can escalate starkly, extending to fantasies of violence against, e.g., refugees, Muslims, or Jews.

Popular formats such as Let's Play (video documenting the playthrough of a game with commentary options) are "hijacked" by right-wing extremists via the chat, which they misuse to propagate their slogans. Often, children and adolescents themselves become the target of hostilities when they publicly present live video appearances.

Several services only allow public streaming for users over 16 years of age. However, there is no definitive process for verifying a user's date of birth. And usually, immediate reporting options are only available to users who are logged in – even though it is possible to view the streams without an account. It can happen that the moderation of a chat running parallel to a stream is left entirely in the hands of an underage streamer, with no support.

Real-time content formats call for rapid intervention to protect the live audience and the protagonists. Service providers therefore must delete offensive material promptly and must provide support in moderating the chats, particularly when those streaming are minors.



Es lebe die PFLP 🇵🇸

bist du Muslimen

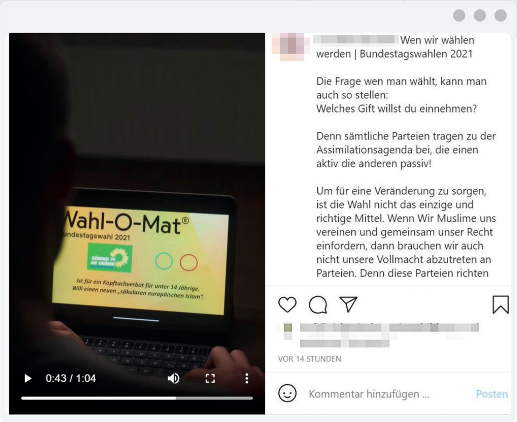
aidskind

Hate comments in the live stream of a Jewish girl (excerpt).
(source: TikTok; original not pixelated)

Democracy in the crosshairs: Extremist propaganda ahead of federal election

The federal election of 2021 was misused by extremists for their anti-democratic propaganda. In advance of the election, right-wing extremists and conspiracy adherents spread rumors about election manipulation. In this way, they attempted to sow doubt about the legitimacy of the election outcomes.

Islamist groups called for an election boycott. Only God, they claimed, had the right to declare the law; for true Muslims, participating in the election was irreconcilable with their religion. This line of argumentation is used again and again by Islamists to undermine democratic principles. With it, they exert pressure on younger people of Muslim faith who are, as is typical at that age, addressing issues of how to harmonize religion and daily life.



[redacted] Wen wir wählen werden | Bundestagswahlen 2021

Die Frage wen man wählt, kann man auch so stellen:
Welches Gift willst du einnehmen?

Denn sämtliche Parteien tragen zu der Assimilationsagenda bei, die einen aktiv die anderen passiv!

Um für eine Veränderung zu sorgen, ist die Wahl nicht das einzige und richtige Mittel. Wenn Wir Muslime uns vereinen und gemeinsam unser Recht einfordern, dann brauchen wir auch nicht unsere Vollmacht abzutreten an Parteien. Denn diese Parteien richten

[redacted]

Claiming that all the parties are anti-Muslim: video with fake voter information. (source: Instagram; original not pixelated)

The federal election was also used to circulate the Islamist narrative of the purported war of "the West" against "the Muslims". It claims that all the political parties are pursuing an anti-Muslim agenda. To support this false assertion, fake images were posted of the Wahl-O-Mat – an online voting advice tool featuring key positions of the parties on the ballot, which is popular among young voters and in its real version was created by the Federal Agency for Civic Education (bpb).

Since 2021, jugendschutz.net has been receiving funding as a partner in the Competence Network against Hate on the Net through the federal program "Live Democracy!" of the Ministry for Family Affairs. The other partners are HateAid, New German Mediamakers, and NETTZ (as coordinator).

The network aims to consolidate expert knowledge relating to hate speech and support institutions across Germany in the work to combat it. jugendschutz.net contributes to this effort through its continuous monitoring of extremist online phenomena and through international networking. (kompetenznetzwerk-hass-im-netz.de)

Sexualized violence: Depictions circulated widely

Acts of sexual abuse committed against children and adolescents are frequently documented by the perpetrators themselves in photos and videos that are posted online. Also, images of consensual acts among adolescents are posted without the consent of the persons shown. The widespread circulation of these images presents an ongoing problem.

Of the 3,948 cases of sexualized violence documented online by jugendschutz.net (58 % of violations overall), the number involving minors in sexual acts or showing them in sexualized poses was 3,834: more than double the number observed the previous year (2020: 1,896). Among these, 2,433 were of German origin (2020: 645). The number of cases coming from foreign servers, 1,401, was comparable with the previous year (2020: 1,251). The reason for the increase is the high number of cases reported through the hotlines of the INHOPE network.

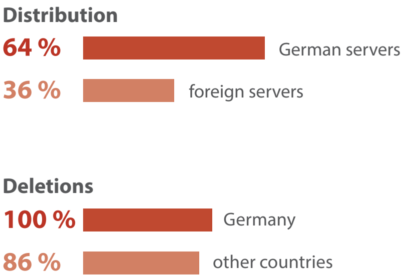
jugendschutz.net works together internationally with hotlines from the INHOPE network. In addition to the referral of cases among countries, the network develops guidelines for best practice and cultivates exchange on professional expertise and technical know-how.

The network has 50 members in 46 countries and is growing steadily.
(inhope.org)

2021

3,834

Cases of depiction
of sexualized violence



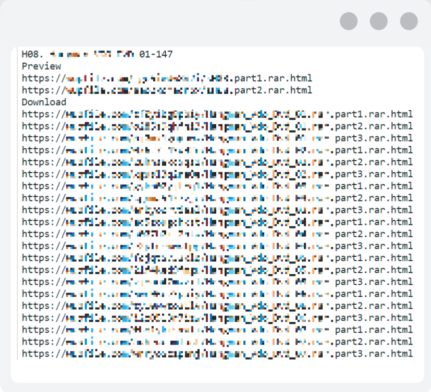
Once content hosted in Germany has been assessed and deemed illegal, the URLs with depictions of sexualized violence are forwarded to the Federal Criminal Police Office. There, the evidence is secured, options for investigation are weighed, and the provider is called upon to delete the content. In most cases, it is removed quickly. In a number of cases, providers transfer the material to servers in other countries and in this way avoid prosecution measures on the national level in Germany.

File hosters: Hardly any protection against circulating images of abuse

72 % of the cases with depictions of sexual abuse documented by jugendschutz.net were distributed via file-hosting services. There is no individual file hoster leading the pack: the phenomenon extends to all the services available. The reason why file hosters are of essential relevance for the abuse milieu is simply that they make it so easy to upload photos and videos onto a central data storage space, while the content or links to it can be posted on websites or forums.

jugendschutz.net has documented cases in which those using this method have integrated hundreds of photos into a forum, or provided links to downloads containing thousands of abusive depictions. An important detail: many of these images are re-posted and may have already been reported on elsewhere.

It may well be that the file hosters' terms of use explicitly forbid the distribution of "child sex abuse material", and that some of the services offer reporting options. But this is in no way sufficient. Far too seldom do providers employ technical mechanisms for protection, e.g. blocking the upload of abusive images that have previously been identified – which would stem the tide of further distribution.



```
H08. [redacted] 01-147
Preview
https://[redacted].part1.rar.html
https://[redacted].part2.rar.html
Download
https://[redacted].part1.rar.html
https://[redacted].part2.rar.html
https://[redacted] part3.rar.html
https://[redacted].part1.rar.html
https://[redacted].part2.rar.html
https://[redacted].part3.rar.html
https://[redacted] part1.rar.html
https://[redacted].part2.rar.html
https://[redacted].part3.rar.html
https://[redacted].part1.rar.html
https://[redacted] part2.rar.html
https://[redacted].part3.rar.html
https://[redacted].part1.rar.html
https://[redacted].part2.rar.html
https://[redacted] part3.rar.html
https://[redacted].part1.rar.html
https://[redacted].part2.rar.html
https://[redacted].part3.rar.html
https://[redacted] part1.rar.html
https://[redacted].part2.rar.html
https://[redacted].part3.rar.html
```

An array of multiple links to previews and downloads. (original not pixelated)

An active contribution toward blocking images of sexualized violence comes from the "Project Arachnid". The core of the system is a data base listing the hash values of abusive images that have been reported or observed. In an automated process, providers can compare uploads with this list and weed out images known to be offensive. Another option: they can register their file-hosting service with the Canadian Centre for Child Protection.

In this way, the cycle is interrupted that enables images deposited on servers to be downloaded onto numerous computers and re-distributed from there. (projectarachnid.ca)

Drastic content: Violence and horror as entertainment

Devoting too much of their attention to crime can have a detrimental effect on young people and become a psychological burden – for example, when they become active as ”lay investigators” in a true-crime context. Online, they engage in lively exchanges about crime. Activities of this type were observed by jugendschutz.net in mid-2021 after the homicide in the USA of the influencer Gabby Petito. Would-be leads and suspicions were shared and discussed in social media or forums.

A depiction of violence deleted on TikTok but then circulated on an indexed website. (source: indexed gore page; original not pixelated)

Children and adolescents often fail to perceive the risks inherent to this trend: descriptions and images of crime can become an emotional burden. Moreover, suspicions voiced about innocent persons can lead to legal consequences and can interfere with police investigative work.

In the same context, jugendschutz.net examined the phenomenon of chain letters that can trigger anxieties. Most often, they are sent via messaging services, such as WhatsApp. As a means of reaching as many recipients as possible, they include threats that terrible things will occur if the letter is not forwarded. The envisioned horror scenarios generally include monsters or (fictitious) criminals, e.g. Jonathan Galindo, Momo, or the Slender Man. Often there is a claim that the recipient or their family member or friend will die. For children, such threats are a significant burden.

Even if providers quickly delete such drastic depictions on social media, the content nonetheless continues to be distributed. During the summer of 2021, a brutal video was circulated on TikTok and also recommended to minors via their feed. It showed a young woman being beheaded. jugendschutz.net was made aware of it through a complaint on its online reporting system. Although the video could no longer be located on the platform, later in the year it re-surfaced with the keyword “TikTok” in the title on a gore page, which was later placed on the index.

Squid Game: Hype with risks for young people

Media phenomena spread like lightning via the internet – as did, in 2021, the hype over a Korean Netflix series called "Squid Game". Although the series was classified by the streaming service for users 16 years of age or older, it was nonetheless on the screens of younger children in schoolyards and even in kindergartens.

As a result, Squid Game has been co-opted any number of times, altered and used to generate attention, clicks, or financial turnover. jugendschutz.net found many gaming apps, Roblox games (home-made computer games to be played together), Let's Plays (videos documenting the playthrough of a game with commentary options)), and challenges that were spin-offs from the series. The focus was most often on the game "Red light, green light" from the series, where avatars who move at the wrong moment are shot dead.

The apps and Roblox games involve an element of suspense or thrill due to ticking timers and the constant danger that an avatar will be executed. Particularly for younger users, this can cause extreme stress or lead to excessive gaming.

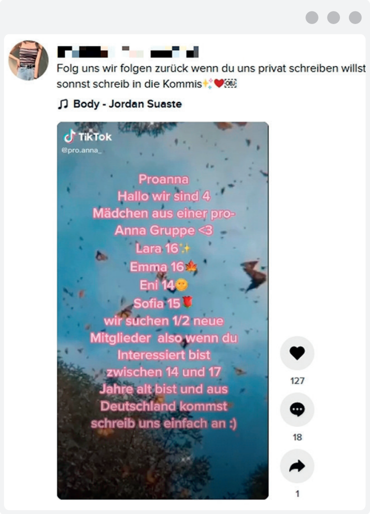
Squid Game: Players who are highly in debt participate in a contest. The winner is promised a great amount of money provided by an anonymous group of super-rich people. The participants compete with one another in various "children's games", in which failure is punished by death.

In videos on YouTube and TikTok, these games have been reduplicated, and some of the videos have had millions of viewers. The candidates are young adults, the prizes are large sums of money. As in Squid Game, losing the game leads to punishment. It could mean being forced to eat extremely spicy food, having cold water poured over one's body, or being shot at with soft-air or paint-ball weapons.

What is problematic is that the punishments are not depicted as cruel or inhumane, as they are in the original series. Instead, they serve to heighten the suspense. The protagonists treat them as "amusing" highlights, completely ignoring health risks and the probability of physical injury.

Eating disorders: Social media can generate risky contacts

Children and adolescents are confronted with self-endangering behavior, especially on social media and in blogs. Drug use, eating disorders, and self-harm extending as far as suicide are trivialized or even glorified. These depictions can lead to imitation, cause emotional stress, and reinforce unstable persons in their self-destructive behavior. Inexperienced users can easily underestimate the consequences of self-endangering behavior.



[redacted]

Folg uns wir folgen zurück wenn du uns privat schreiben willst sonnst schreib in die Kommis✨❤️

♫ Body - Jordan Suaste

TikTok
@pro.anna_

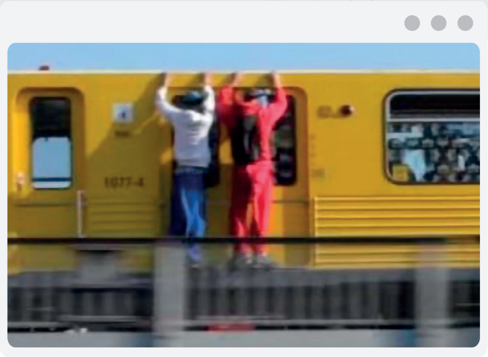
Proanna
Hallo wir sind 4
Mädchen aus einer pro-
Anna Gruppe <3
Lara 16✨
Emma 16🍁
Eni 14🌞
Sofia 15🌹
wir suchen 1/2 neue
Mitglieder also wenn du
Interessiert bist
zwischen 14 und 17
Jahre alt bist und aus
Deutschland kommst
schreib uns einfach an :)

Search for like-minded others: young people using social media to advertise their "hunger groups".
(source: TikTok; original not pixelated)

Particularly when eating disorders are the topic, digital exchanges tend to be continued in private communication, for example in pro-ana/pro-mia WhatsApp groups. In such "hunger groups", the dynamic and sense of community can have the devastating effect of reinforcing self-endangering behavior among the participants. These platforms are therefore a risky area for making contacts. There are strict criteria for acceptance, e.g. reporting one's body weight on a daily basis. Among the 166 cases examined by jugendschutz.net in 2021, almost one third (51) were related to such contact requests or offers.

So-called pro-ana/pro-mia coaches present a particularly high risk for children and adolescents who are unstable or suffer from eating disorders. Posing as weight-loss advisors, they offer support on social media or in guest books of topical blogs. But these are not offers to be taken seriously; the coaches are in fact interested in manipulating and exerting power over inexperienced minors. Also, it cannot be ruled out that there may be an intent of sexual abuse, since the coaches often call for nude photos. Moreover, humiliations are a standard component in their communication.

Challenges: Dangerous games played on a dare



Risky ride: adolescents filmed while train surfing in Berlin. (source: YouTube)

Popular among adolescents: risky, sometimes life-endangering tests of courage, such as “roofing” (climbing high buildings with no safeguards) and “train surfing” (riding on the roof or the outside ledge of a train car). In the photos and videos that are posted online, dangers are disregarded. Usually, they convey a feeling of carefree abandon and freedom from restriction. Risky actions are presented as athletic achievements that are acknowledged by the community. That heightens the pressure on children and adolescents to take on dangerous dares in the hope of positive feedback.

Participating in so-called challenges and publishing the outcomes online is another aspect of young users’ behavior on social media. Many of these playful competitions are original and creative. But things become problematic when ill-considered, risky behavior is shown and imitation encouraged, as in the “milk crate challenge”. Here, young people climb over a makeshift staircase of stacked milk crates.

There has been an increase in posting of so-called “fail compilations”. These videos consist of a series of clips of challenges that failed. Their participants are exposed to public ridicule, and often, serious injuries are shown in the videos. For adolescents and particularly for children, seeing such depictions can be disturbing and shocking.

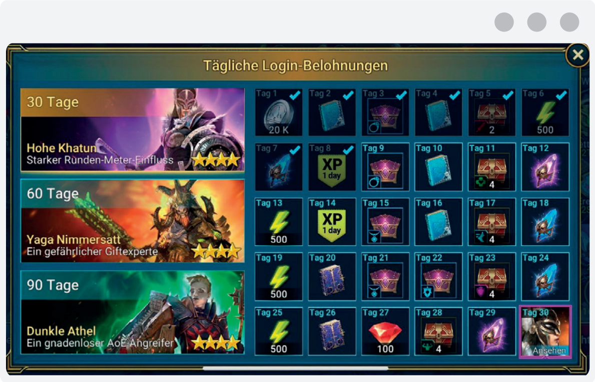
Manipulative game design: Risky fun in free2play apps

“Dark patterns” is a concept applied in online shopping, resp. online marketing. It designates mechanisms used to trick users: they are enticed to do something that is not in their own interest, but in the interest of the provider. Such manipulative design is also used in games, particularly in free2play apps. They animate users to buy things, reveal personal data, take in advertising, or simply play the game as often and as long as possible.

Research on gaming apps shows that dark patterns play on the users’ enjoyment and interest in interaction, while relying on their credulousness. One trap for children and adolescents, who form the majority among gamers: due to their lack of experience, they often cannot see through the strategy of providers.

The apps that were examined are not exceptional. The majority of available free2play apps work with dark patterns in various forms. This therefore must be regarded as a phenomenon that has been standardized among gaming providers and is incorporated systematically in their products.

In order to protect children and adolescents without restricting their right to participation, providers would be required to change their policy. A logical solution would be to refrain completely from integrating dark patterns into games that attract children and adolescents. Whenever certain functions are associated with cost traps or enticement to excessive use, these risks should be taken into consideration when setting the age recommendation.



Playing daily is rewarded with gifts.
(source: Raid)

Manipulative design in gaming apps can be roughly described in four categories, which overlap in part. Some examples to illustrate the strategies:

Time Patterns

An "artificial tug" draws the user back to the app and/or keeps them in the app for as long as possible.

- Playing daily brings rewards, and their values rise if the user picks them up regularly.
- A player who comes back frequently and regularly accumulates more resources and advances more quickly.
- Push notifications come up constantly about new lives, replenished resources, events, rewards to be picked up, etc.

Money Patterns

Subliminal pressure entices users to make in-app purchases.

- Rare resources necessary for gaming actions are hard to achieve through playing, but easy to purchase.
- Various currencies, offers, and packages in the game shop make it difficult to judge the actual value of a purchase.
- "Loot boxes" (surprise packets) lure users hoping to get resources they need and other useful items.

Social Patterns

The interaction among gamers is exploited to create social pressure.

- A sense of competition is produced by constantly displaying the success of other players.
- Group pressure builds up due to cooperative playing options within alliances or clans that have their own rules (e.g. regarding game-wins or playing times).

Psychological Patterns

The disruption of familiar patterns fools the brain.

- Irritation results when the color, form, function, or position of a button suddenly changes.
- The player has to make decisions under time pressure or immediately after completing a time-limited move.

Cloud-Gaming services: No reliable age restrictions

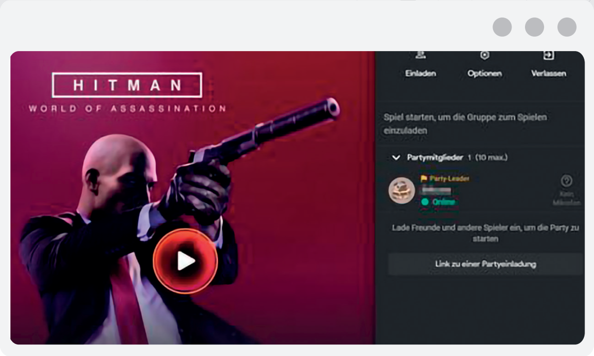
Cloud-gaming is a growing sector of the gaming industry. The games are located on external servers, meaning that a user can access his or her games on various (mobile) devices to which they are streamed. jugendschutz.net examined the cloud-gaming services Google Stadia and NVIDIA GeForce Now with a focus on risks and the protection of children and adolescents.

GeForce Now offered a free version in which the time per game was limited to one hour. Paying users were given priority for beginning a game. In order to play on demand and for an unlimited time, a subscription was offered at 5.49 € per month, payable via credit card or PayPal.

Although GeForce Now, in its Terms of Use, set a minimal age of 18 years for users, or alternatively requires permission of a legal guardian, there is no reliable assurance of age. It was possible to create an account while claiming to be 16 years old.

The platform only offered the option to stream games of other providers. In order to download or buy a game, it was necessary to create an additional account at the third-party service.

GeForce Now listed games in its library without any differentiation by age. Therefore, the 16-year-old was being offered games labelled "18 and over" such as "Blair Witch" or "The Surge". Whether these games could also be purchased depending on the protective measures taken at the third-party platform. The catch here: many providers (e.g. Steam) did not verify the customer's age reliably. In effect, minors had access to games that are not approved for them. And payment could be made with pre-paid cards that are available in stores everywhere.



Spiel starten, um die Gruppe zum Spielen einzuladen

[redacted]

Lade Freunde und andere Spieler ein, um die Party zu starten

Game not approved for minors, but available for 16-year-olds free of charge. (source: Stadia; original not pixelated)

At Google Stadia, all the games were accessible via this service only. In a free version, individual games could be purchased at full price, and several were available free of cost. Payment required a credit card. With a subscription for 9,99 € per month, it was possible to access more games.

Google Stadia sets a minimum age of 16 years for a self-administered Google account (which can also be used for Gmail or YouTube). For younger users, Google offers Family Link as a tool for parental supervision. There was no reliable age verification. During the research period, accounts listing the owner's age at 16 were able to download, free of charge, one game with the age label "18 and above", while others were available on payment.

Google Stadia presents numerous interactive options, for example via individual text or voice message, or in a group chat. Using the search function of the platform, other players are easy to find as long as they, after creating their account, have not actively restricted access to details including e-mail address or online status. This means that inexperienced users may inadvertently expose themselves to risks such as harassment or mailings of harmful content.

It was possible to report or block users, as well as comments in the chat. However, it was only foreseen that images would be attached to the complaint (for example, a screenshot showing a violation), but no space was provided for an explanatory text.

While brick-and-mortar stores selling hard copies of games intended for adults verify the buyer's age, minors have direct and often cost-free access on all their devices via cloud-gaming services. Only a reliable means of age verification and access differentiated by age, with safe default settings, can ensure both protection and participation for young users.

PROTECTION AND PARTICIPATION

Violations of the regulations protecting minors on the internet need to be deleted in short order. To this end, jugendschutz.net establishes contact to providers. Cases that fall under German jurisdiction are forwarded to the Commission for the Protection of Minors in the Media (KJM), so that supervisory proceedings can be initiated. Where there is imminent danger to life and health, jugendschutz.net informs police authorities. In individual cases, there is cooperation with foreign partners and their reporting systems.

For eight social media services, jugendschutz.net researched the status of their preventive measures. Thankfully, several providers have improved their precautions. What is still lacking across the board – on all the platforms – is a reliable procedure for age verification. This, however, is a basic prerequisite for the age-appropriate protection of youngsters.

Research on four parental control apps revealed that their functions do not provide effective protection. They rather couch the legal guardians in an illusion of security. It is still too seldom that modern technology, such as machine learning, be employed for the protection of minors in the media.

Children have a right to protection and participation on the internet. With its study outcomes, jugendschutz.net has continued its support for media education and has contributed its expertise to numerous events on national and international levels.

Almost 7,000 violations: 84 % deleted by the end of the year

In 2021 jugendschutz.net processed 6,865 violations (2020: 5,056). Of these, 2,436 (36 %) occurred on social media services, with a breakdown as follows: 17 % on Instagram, 16 % on Twitter, 15 % on YouTube, 14 % each and Facebook und Pinterest, 12 % on TikTok and 5 % on Telegram.

58 % of the violations lay in the topical area of sexualized violence. The second most frequent area was political extremism at 15 %. Pornography was represented with 14 %, self-endangerment with 6 %, violence with 5 % and Cyberbullying with 2 %.

Depictions of child abuse most common on file-hosting services

3,093 violations (45 %) were related to a file-hosting service – a considerable increase in comparison to the previous year (1,311 cases, 26 %). Without reservation, this is due to the high number of child pornography cases being disseminated predominantly (at 84 %) over these platforms.

By the end of the year, in 5,784 of these cases (84 %) the violations had been deleted.

Media supervisory bodies: More than 500 cases referred to the KJM

To initiate investigations, in 2021, 132 cases (2020: 78) were referred to the KJM (Commission for the Protection of Minors in the Media) for further proceedings. These pertained largely to pornography (63 cases), indexed material (35 cases), and developmentally harmful content (19 cases).

In addition, jugendschutz.net referred 385 cases (2020: 216) to the KJM to be indexed by the review board within the newly established Federal Center for Youth Media Protection. Again, most of these cases contained pornographic material (276 cases).

132 supervisory referrals and 385 requests for indexing

2,242 cases were forwarded directly to the Federal Criminal Police Office because child pornography was being disseminated, or there was imminent danger to life and health (e.g. threat of violence, announcement of suicide). Additionally, 493 cases were transferred to the INHOPE partners in other countries for assistance.

Social Media: Precautions are still insufficient

jugendschutz.net tracks the precautionary measures taken by providers whose services are frequently used by children and adolescents. In 2021, these were Instagram, YouTube, TikTok, Snapchat, WhatsApp, Pinterest, Facebook and Twitter. The aspects that were examined: reporting systems (e.g. easy access, rapid assistance), settings (pre-configuration, easy handling of protective options), guidelines (completeness, clarity), support systems (practical assistance in an emergency, information on professional help), and technical measures (access differentiated by age, employment of recognition technology).

It remained the case that providers do not take sufficient measures toward the protection of children and adolescents. However, certain improvements were to be observed, for example in the default settings, guidelines, and support structures.

All eight of the services examined offer reporting options of some kind. The most apparent structural deficit was to be found on Twitter: it was not possible to report pornographic remarks made in tweets, although these presented the most prevalent problem on the platform. In matters relating to sexualized violence, extremism, violence, and cyberbullying, it was only possible to report violations of the Network Enforcement Act (NetzDG); tweets endangering minors could not be addressed.

On YouTube, the problem was still unresolved that content cannot be reported by users who have no account, although most content is freely available for unregistered users. Pinterest, Facebook, and Snapchat still fail to offer the option of reporting profiles.

Deficits in reporting systems

jugendschutz.net monitors the response to complaints in a two-fold procedure. In the first step, violations of regulations protecting minors on the media that cannot be traced to a responsible party in Germany are reported as normal user complaints. If, after seven days, the content has not been deleted or blocked, jugendschutz.net identifies itself as an institution and formally requests that the material be removed. The violation is checked one last time after seven more days, and the outcome is documented.

The reporting systems checked on were those of YouTube, TikTok, Instagram, Facebook, Pinterest and Twitter. Result: out of 1,974 reported violations, the service providers deleted/blocked only 41 % on the basis of a user complaint. An additional 41 % was deleted after an official complaint.

In the first step, YouTube, TikTok and Instagram removed less than one third of the violations, while Twitter and Facebook removed less than half. Only Pinterest responded adequately with a quota of 84 %. It was clear to be observed that the services responded differently to user complaints, depending on the topic: in cases of violence, for example, YouTube deleted only 9 %, Instagram 17 %, and TikTok 20 %. By contrast, Pinterest already removed all the reported cases of violence in this first step.

Forbidden insignia from the right-wing extremist milieu were removed in 50 % of reported cases. In contrast to a low rate of deletion on TikTok (18 %), YouTube (24 %), and Instagram (39 %), the deletion quota was relatively high on Facebook (59 %), Twitter (68 %) and Pinterest (83 %).

	cases	deleted after user complaint	deleted after official complaint	not deleted	deletion quota
Pinterest	345	84 %	5 %	11 %	89 %
YouTube	346	24 %	60 %	16 %	84 %
TikTok	278	26 %	56 %	18 %	82 %
Facebook	324	45 %	36 %	19 %	81 %
Twitter	294	37 %	40 %	23 %	77 %
Instagram	387	28 %	48 %	24 %	76 %
total	1.974	41 %	41 %	18 %	82 %

The minimum age for users is set at 13 years by most of the services that were monitored. YouTube and WhatsApp stipulate 16 years as the minimum age for self-administered accounts. For all those under 18 years of age, the prerequisite for use is permission from the legal guardian. However, the age recommendations given elsewhere for individual apps often diverge from the stated age minimum on the app itself. For WhatsApp, as an example, Google Play Store lists a minimum age of 0 years.

There is still no provider with a reliable system of age verification in place. This is, however, the prerequisite for any age-appropriate protection for children and adolescents. Up to now, a number of services base their age-differentiated preventive measures simply on the information given by the users themselves during registration.

Pre-settings improved by several providers

Default settings have been improved by several providers. YouTube videos uploaded by users under 18 years of age are no longer automatically available to the general public.

On TikTok, accounts of users under 16 years of age are set to "private" when they are created. Comments can only be added to posts by followers who are also followed by the author of the post. Comments that TikTok classifies as spam or as insulting are filtered out. Authors over 16 years of age can view them and de-classify them, thus releasing them. Private messages cannot be received by those under 16 years of age.

On Instagram, as well, accounts newly created by minors are now "private"; users with existing accounts are informed about options to protect the private sphere. Moreover, adults can no longer send messages to minors if they are not listed as followers.

There are also new options to alter settings on some of the services. On TikTok, users over 16 years of age can activate pre-moderation of comments they receive. And Instagram has integrated a new safety check which helps to set up an account with the best available protection.

Some of the services have tightened up their guidelines on certain types of content and behavior. Instagram is objecting more strictly to the dissemination of hate speech in direct messages and reserves the right to deactivate the relevant account if there is a repeated offense after a warning. Twitter has forbidden sharing images of persons without their permission. On the topic of eating disorders, Pinterest has banned advertising that promotes or idealizes weight-loss.

Several services have also improved their support structures. TikTok expanded its "safety center" to include the topics of challenges and hoaxes. It also added information for users who have been the object of sexual infringements. What's still lacking is specific information about where to find supportive help in Germany.

Facebook set up an information center on emotional health, with topics such as depression or dealing with stress and mourning. It also, in cooperation with klicksafe, developed a guideline for parents and guardians on using Facebook safely. Snapchat established a channel ("Safety Snapshot") covering safety issues and data protection.

Some progress in guidelines and support

Parental Controls: Scant protection on social media

Children and adolescents spend a major part of their everyday life online. Usually, they use social media and mobile devices. To protect their children against unsuitable content and dangerous contacts, parents and guardians rely in part on technical aids.

jugendschutz.net pursued research on the parental control apps KROHA, Safe Lagoon, Kaspersky Safe Kids and FamiSafe. Their product descriptions all promised, among other things, protection on social media. The research outcomes on this point were sobering.

All of the apps fulfilled the standard functions of programs to protect youth: limiting media time, setting website filters, denying access to certain apps. Kaspersky Safe Kids enables blocking of YouTube searches.

With KROHA and Safe Lagoon, the focus was on surveillance. They both allow GPS tracking and documentation of chat exchanges, contact requests, and viewed content. Safe Lagoon can produce screen shots from the child's device. This is questionable inasmuch as reading private chats is an incursion into the child's privacy.

The four alternatives examined provided little or no specific protection for the use of social media and apps. In some cases, not even the simplest options were activated, such as the safe search function in search engines. The functions that were offered did not contribute to effective protection. Instead, they create an illusion of security for parents and guardians.

A parental control app adequately adapted to social media would need to take interactive risks into account, activate security settings along with blocking and filter tools, and thus prevent confrontations with dangerous and detrimental content.

Parental control apps don't deliver on their promises

On large social media platforms, options for parental supervision are seldom offered. Since no reliable age verification is undertaken, younger children also move around on these platforms. They often claim to be older than 18 so that they can use all the functions, and thus unfortunately circumnavigate any other age-differentiated settings that might be in place.

Services designed especially for children usually offer the option of a parental escort. Such services are not always easy to find. But when they are up and running, they enable such things as control over exchanges with strangers. In the children's communities Momio and MovieStarPlanet, for example, risky communicative functions including chats and messages can only be used after being activated by a parent. Alongside such a blanket solution, the gaming platform Roblox also permits individual exceptions. In this way, at least to a certain degree, safety settings can be adjusted to the age and cognitive level of an individual child.

A comparable conception could be adopted by the large social media platforms. Options for parental permission and adjustments are an essential element for safe use of the services.

Combination of provider measures and parental control can improve safety

Machine learning: Potential for protecting minors

Self-learning systems are very widespread: search engines, suggestions for purchases, and navigation systems are just a few examples of areas in which this technology is applied.

The large social media services invest heavily in the development of methods for automatic recognition of content. It enables them to analyze user-generated material, predict user behavior, and introduce targeted advertising. All this goes on in the background. It only becomes visible in the form of recommendations to buy or view something, or in the so-called "Facebook bubble": content comes up that "might possibly be relevant for" the user. Children and adolescents are constantly exposed to these mechanisms.

Advanced recognition technologies can, however, also help to assess dangerous content quickly and filter out harmful posts unsuited for a particular age group. In view of the enormous amount of user-generated content to be dealt with, the service providers hardly have any choice but to rely on automatic classification systems.

How does machine learning work?

Many of today's recognition systems are so-called "neural networks". They imitate the functionality of the human brain. They learn by identifying patterns in the material they are presented with.

This process requires large quantities of training material (e.g. images). During training, the system views the samples, calculates an outcome (e.g. "cat"), and then compares it with the actual content (e.g. image in fact shows a dog).

Then the "neural network" is fine-tuned in small steps so that, on the next attempt, it will be more likely to produce a correct result. This process is repeated with an enormous number of examples until the likelihood of correct recognition is sufficiently high. Then, the algorithm can reliably assess material it has never encountered before.

The quality of the training material and the manner in which training is conducted determine the reliability of the recognition system.

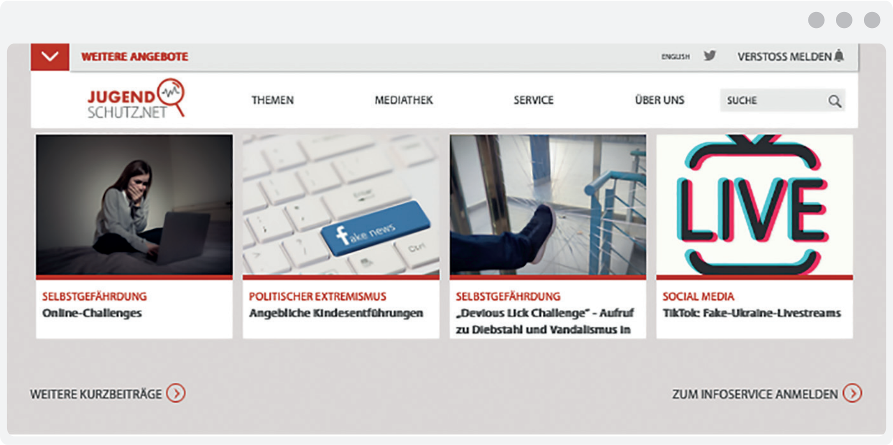
Until now, youth protection programs have been called upon when parents want to protect their children from certain content on the net. These programs have been oriented toward filtering classically constructed websites. When it comes to user-generated content on social media, there has not yet been a system developed that would be capable of filtering out individual elements of content in a differentiated manner. In most cases, all the systems can do currently is to block the service completely or allow it to be viewed.

Whereas pornographic content can be reliably identified with simpler methods, such as recognition of keywords, machine learning can achieve reasonably high recognition quotas in other areas of endangerment, including violence and self-harm.

Particularly in the field of (spoken) language and text recognition, machine learning has been making considerable progress. Language assistents are expected, in the future, to be able to carry on dialogues and take the previous course of a given conversation into account. For reporting systems or for technical support in moderating chats, but also towards successful recognition of risky communication, technologies of this type could contribute to ensuring safer internet use for children and adolescents.

Machine learning can contribute to better protection in the future

Transferring insights:
Practical aids available online



SELBSTGEFÄHRDUNG
Online-Challenges

POLITISCHER EXTREMISMUS
Angebliche Kindesentführungen

SELBSTGEFÄHRDUNG
„Devious Lick Challenge" - Aufruf zu Diebstahl und Vandalismus in

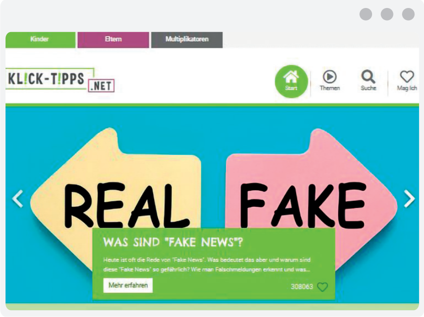
SOCIAL MEDIA
TikTok: Fake-Ukraine-Livestreams

Relaunch of the jugendschutz.net website

In the **Mediathek** all the major publications of jugendschutz.net are available. This includes materials for practical use (e.g. on the topic of cybergrooming), study reports with insights into current phenomena (e.g. dark patterns), and status reports with a wide range of research outcomes on topics such as political extremism.
All the publications are available free of charge, they are intended to support practical efforts in education and advanced training.
jugendschutz.net/mediathek

The **Infoservice** publishes short news items about risks within apps, political extremism, depictions of abuse, self-endangerment, and violent content, as well as other relevant topics.
jugendschutz.net/service/infoservice

Violations of regulations for the protection of youth can be reported online using the form provided.
jugendschutz.net/verstoss-melden

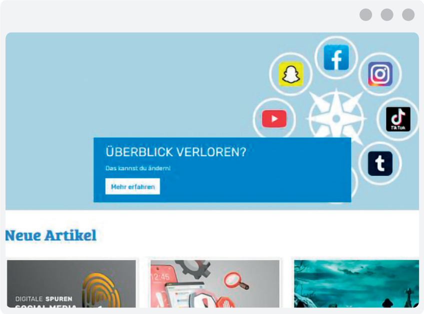


WAS SIND "FAKE NEWS"?

Heute ist oft die Rede von "Fake News". Was bedeutet das aber und warum sind diese "Fake News" so gefährlich? Wie man Falschmeldungen erkennt und was...

klick-tipps.net presents websites and apps relating to topics that children are often curious about, e.g. puberty, arguing, or time-travel. For parents, there are news articules and tips on safe behavior for children on the net. Teachers are provided with instruction materials for media education in elementary schools.

klick-tipps.net/multiplikatoren/kinder-sicher-online



ÜBERBLICK VERLOREN?

Das kannst du ändern!

kompass-social.media examines service platforms popular among children and adolescents. It uses a ‘traffic signal’ system to assess safety settings, data security, and reporting options at a glance: green, yellow, or red. Articles on current topics provide insight into the workings of large platforms and tips on using them safely.

kompass-social.media

Bericht 2020/2021: Rechtsextremismus im Netz

Corona, Livestreams, Gaming: Krisen und jugendaffine Medien werden für Hasspropaganda genutzt.

hass-im-netz.info (‘hate-on-the-net’) covers political extremism from the point of view of protection for minors. Focus articles, “HiNweise” (up-to-date tips), reports and more explain background and developments. Practical suggestions are provided to encourage critical discussion on right-wing extremism, Islamism, hate and propaganda, and to support civil courage on the net.

hass-im-netz.info

Supporting media protection for youth: Major initiatives and portals

saferinternet.de
With the "Safer Internet Centers" in its member states, the European Union provides contact points across the continent to promote safe communication on the net. The Center for Germany is saferinternet.de. It presents the services of various partners working to transfer knowledge about media literacy to children, parents and educators and to raise awareness of online risks, while also providing telephone counselling and addresses for submitting complaints.

klicksafe, FSM – Voluntary Self-Monitoring of Multimedia Providers, eco – Association the German Internet Industry, Nummer gegen Kummer e.V., jugendschutz.net

gutes-aufwachsen-mit-medien.de
The initiative "Gutes Aufwachsen mit Medien" (Growing up well with media), with funding by the Federal Ministry for Family Affairs, offers practical support for educational professionals and parents in the area of media literacy and media education, as well as age-appropriate media access for children and adolescents. Among the topics are practical tips for educational work with media, qualification options for educators, and advisories for media education.

**Digital Opportunities Foundation,
Federal Ministry for Family Affairs, Senior Citizens, Women and Youth**

schau-hin.info
Media advisory for parents and educators covering current developments in the media world and general information on various media topics, such as smartphones and tablets, social networks, games, apps, time spent on media, and streaming. It offers practical tips on competent supervision of media use by children and adolescents. Media coaches respond to questions that are submitted.

**Federal Ministry for Family Affairs, Senior Citizens, Women and Youth,
Das Erste (national TV network), ZDF German Television,
AOK – Die Gesundheitskasse (health insurance provider)**

klicksafe.de
EU initiative to support media education for children and adolescents, as well as parents, teachers and educators. It provides up-to-date information, practical tips and helpful materials relating to digital services and topics. It also conducts information campaigns and develops conceptions for nationwide qualification schemes for teachers and educational professionals. klicksafe works in close cooperation with national and European partners.

Central Authority for Media and Communication Rhineland-Palatinate,
Media Authority of North Rhine-Westphalia (co-financed by the European Union)

medien-kindersicher.de
Portal for technical protection of minors in the media. Informs parents about technical protective measures on devices, services, and apps used by their children. Complicated settings are presented in easy steps, explained and assessed. An assistance system helps in finding a tailored solution for protection, based on a child's age and the devices and services being used.

State Media Authorities of the federal states Bremen, Baden-Wuerttemberg,
Mecklenburg-Western Pomerania, Rhineland-Palatinate, klicksafe

jugend.support
Advice and assistance for children aged 10 and older, and for adolescents. Support and tips for self-help in cases of acute problems or stress on the net. Covers the full range of risks encountered by children and adolescents online, e.g. bullying, harassment, privacy issues, cost traps, hate speech, violence, or self-endangerment. Provides information on confidential counselling services and contact addresses for emergencies.

juuuport e.V.

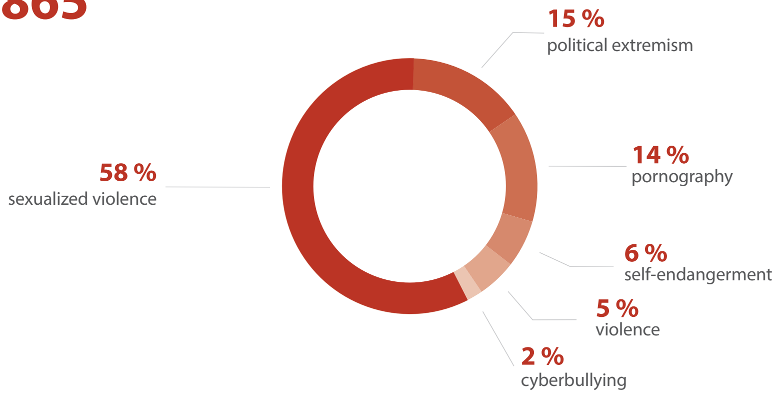
fragzebra.de
Counselling platform responding to questions and providing practical support on topics in the field of media, everyday digital life, and media competency, e.g. on false information found on the net. Includes a large knowledge data-base. New questions can be submitted easily online and are responded to promptly by experts in the areas of media education, media competency, communication studies, media law, and media research.

Media Authority of North Rhine-Westphalia

KEY FIGURES

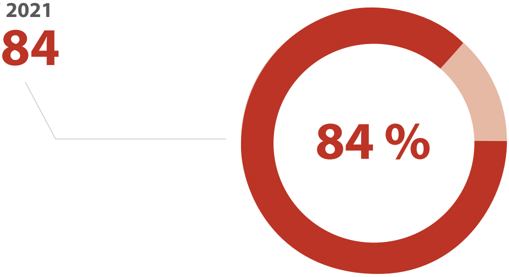
VIOLATIONS REGISTERED

6,865

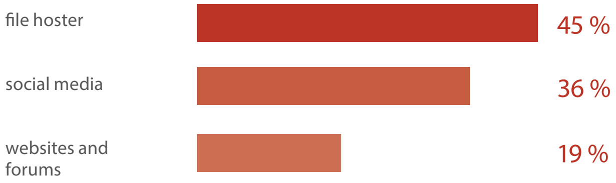


DELETED BY END OF 2021

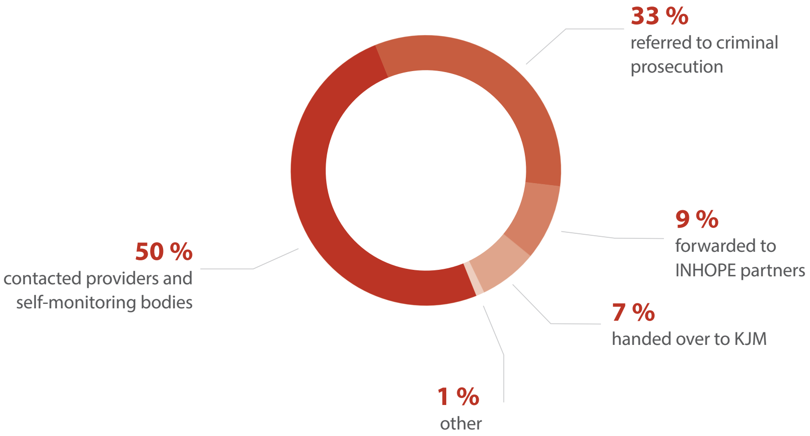
5,784



Distribution of violations



Activities towards deletion and prosecution of 6,865 violations



Allowing Children and Young People to Grow Up Well in a Digital World

jugendschutz.net is the joint center of the German Federal Government and the federal states tasked with 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 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. Since 2003, jugendschutz.net has been organizationally linked to the Commission for the Protection of Minors in the Media (KJM). The work of jugendschutz.net is funded by the Supreme Youth Protection Authorities of the federal states, the State Supervisory Bodies and the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth.

jugendschutz.net's hotline accepts reports about violations of youth media protection laws.

jugendschutz.net/verstoss-melden

JUGEND
SCHUTZ.NET