

2023 REPORT

Protection of minors on the Internet

Risks and need for action

Contact us

jugendschutz.net
Kaiserstraße 22, 55116 Mainz
Tel.: 06131 3285-20
buero@jugendschutz.net
www.jugendschutz.net
www.x.com/jugendschutznet

Responsible

Stefan Glaser

Editorial office

Steffen Eisentraut, Andreas Hautz, Murat Özkilic

Graphic design

elements of art

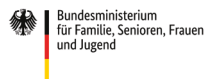
As of

July 2024

Financed by:



Gefördert vom:



Im Rahmen von:



Kofinanziert von der Europäischen Union



Digital upheaval requires concerted youth media protection

The world of games, challenges and shorts entices children and young people to use the Internet every day. Unfortunately, the diversity of use and attractiveness of Internet services has long been offset by negative experiences: Sexualised violence and bullying, posts that turn against our democracy and a diverse society or incriminating images of violence are the norm in the user-generated cosmos. For some time now, the rapid development and spread of AI systems has also been raising questions about the risks that arise for those who grow up using them. The downside of helpful tools are phenomena such as deepfakes, which can hardly be distinguished from real content.

Looking back at the past year, it is clear that the problems for children and young people in the digital world are not getting any smaller. It is also evident that providers are still not effectively protecting the youngest users from being confronted with harmful content and offences when using their services: Reporting systems fail and do not lead to the deletion of offences quickly enough, if at all. Age-differentiated approaches are ineffective because there is no reliable verification of how old the users actually are. This is incomprehensible given the potential dangers that exist in popular services.

It is not only online worlds that are currently undergoing major changes and creating new risks of use. The Digital Services Act (DSA), which aims to create a safe space for internet users and protect their fundamental rights, is also changing the system of child and youth media protection across Europe. The large, internationally operating platforms are now regulated by the EU. In order for this positive approach to work and for the Commission's measures to take effect, nationally responsible specialised and supervisory bodies must be involved and work well together.

With jugendschutz.net, the youth ministries of the federal states created a centre many years ago that has its finger on the pulse of the times. It quickly picks up on developments in the field of work, assesses youth protection problems precisely and with foresight and derives recommendations for action for politics, supervision and practice. It supports the media supervisory authorities of the federal states and the federal government with case-by-case and structural reviews of programmes. And it is networked with important players both nationally and internationally. With its many years of experience and expertise, jugendschutz.net is an important constant in the changing system and can continue to help children grow up well online in the future.

Stefan Glaser
Head of jugendschutz.net

Pages 6 - 17

DANGERS AND RISKS

Generative AI:

Deepfakes and realistic counterfeits exacerbate risks

Hate content:

Extremists capitalise on war suffering and climate change for propaganda

Sexualised violence:

Video chats with children misused for intimate recordings

Challenges, pranks and fitness:

Trends with dangerous consequences

Roblox gaming platform:

Extremism, harassment and cost traps

Pages 18 - 26

PROTECTION AND PARTICIPATION

Over 7,600 offences registered

90 % of offences removed by the end of the year

Review of preventive measures by providers

Lack of age verification remains the biggest problem

Inadequate response to the reporting of violations

Security settings: Basic protection with gaps

Utilisation guidelines and support services further developed

Current findings and further information



www.jugendschutz.net

DANGERS AND RISKS

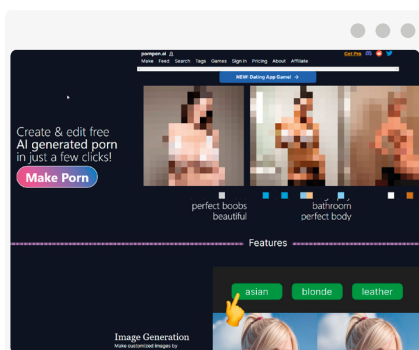
Generative AI: deepfakes and realistic fakes exacerbate risks

The development of artificial intelligence systems, particularly generative AI, has seen significant advancement in 2023. The new technologies dominated media debates and found their way into the everyday lives of children and young people. Many applications are easy to use, freely accessible and require no programming skills. With just a few text instructions ("prompts"), ChatGPT and similar programmes generate texts, images, speech and videos on any topic. Applications are integrated into smartphones and social media services.

While technology can support young people with schoolwork and promote creative skills, it exacerbates existing risks on the internet such as sexualised violence, bullying and extremism.

So-called deepfakes can now be created and distributed in no time at all. Many of the fakes generated look deceptively real and can hardly be distinguished from actual photos. Combined with nudity (deepnudes) or pornography (deepporn), this can quickly lead to cyberbullying or sexualised violence. Cases from Spain show how easily young people can become victims. Pupils there used AI to create nude images of their classmates and circulate them - with dramatic consequences for those affected.

Social media providers block key terms in their AI systems for content such as depictions of abuse, violence and pornography in order to prevent the generation of such content. However, users can easily circumvent this protection by using alternative descriptions. There are also services that specialise in creating pornographic material: After entering characteristics such as age, size or gender, porn is created as desired and can be downloaded.



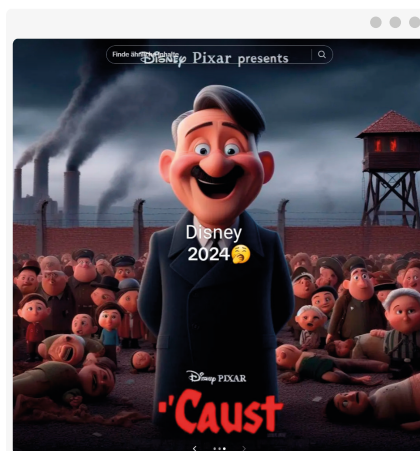
On pages for AI image creation users create their own pornographic content. (original unpixelated)

In online communication, it is becoming increasingly difficult to recognise whether the other person is a real person or an AI system. This makes it more difficult for children and young people in particular to assess how trustworthy transmitted information is or which personal data they can disclose without any problems. With the help of chatbots and voice generators, strangers can impersonate people of the same age even more easily. This makes it easier for them to build trust, access sensitive personal information and misuse it for grooming purposes.

AI systems also deliver incorrect or inappropriate results, putting children at risk: tests carried out by jugendschutz.net with Snapchat's MyAI chatbot led a supposedly 14-year-old user, to the alcohol drinking game "Flunkyball" and the horror film "Saw" (FSK 18).

AI-generated posts and identities are also used to spread extremist propaganda and disinformation. This is particularly effective when the actors combine entertainment with manipulative content. In the course of a youth-oriented challenge for AI-generated images, right-wing extremists relativised the Holocaust or trivialised terrorism. E.g. the poster for a supposedly new Disney film entitled "Caust", which was deceptively realistically generated by AI in Pixar style, has already been shared thousands of times. The image shows Adolf Hitler, animated as a figure, smiling in front of a concentration camp.

Hitler and concentration camps in the popular "Pixar" film style: the Holocaust is trivialised using image-generating AI.
(Source: TikTok)



Hate content: Extremists use war suffering and climate change for propaganda

Extremists are using current crises to indoctrinate and radicalise children and young people online. Climate change and the wars in Ukraine and the Middle East are important topics for young people to find out about online. They quickly come across disinformation, hate content and depictions of violence.

Young people who campaign for climate protection on platforms such as TikTok, Instagram or YouTube quickly become the target of derogatory posts. Comments portray them as unaccountable and "mentally ill", and suggest that they should seek psychiatric treatment.

Misogynistic defamation, sexualised comments and even rape fantasies are uttered against female activists.

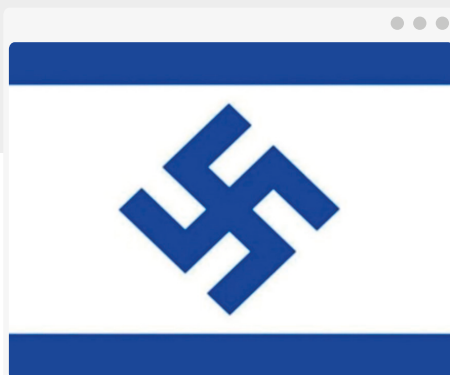
Exposure to such derogatory and hateful statements can have a negative impact on children and young people. On social media, they experience a highly emotional and polarising culture of debate that influences fundamental social values. A poisoned atmosphere when discussing political issues is contrary to development goals such as respect for other people and opinions.



Climate activists are asked to publish erotic or pornographic content, e.g. on the relevant platform OnlyFans.
(Source: Twitter/X; original unpixelated)

Hamas' terrorist attack on Israel on 7 October 2023 is also being misused to stir up public opinion and spread extremist ideologies. In the days and weeks following the attack, youth oriented services such as Instagram and TikTok were used to spread drastic depictions of violence, disinformation and anti-Semitic and anti-Muslim propaganda. Disturbing images and videos of abduction and mistreatment, some of them showing children, were distributed en masse. Both pro-Palestinian as well as pro-Israeli groups shared drastic images of victims.

Referring to the Israeli settlement policy, many actors trivialised the Hamas attack and attempted to justify it. jugendschutz.net found anti-Semitic conspiracy narratives, threats of violence and incitement to hatred in the posts, especially after the military counterattack. Users relativised the Holocaust, e.g. by equating Israel's actions with the crimes of the Nazis in Germany. AI-generated content was also used. Some showed Jews as vampires, who were after the blood of innocent babies. At the same time, there was also derogatory and inflammatory content against Muslims or people who were thought to be Arab.



Israel is equated with the German Nazi regime.
(Source: Instagram)

Under the pretext of solidarity with Israel, extremists fuelled resentment against Muslim population groups and portrayed them as a threat.



jugendschutz.net has been cooperating for over 20 years in the International Network Against Cyber Hate (INACH), which currently has 35 members from 28 countries. The network aims to quickly delete illegal hate speech, exchange knowledge and strengthen civil courage online.

Since 2016, INACH and European hotlines have been checking on behalf of the EU Commission how social media services that have signed up to the EU Code of Conduct on combating illegal hate speech online respond to reports of hate content. (inach.net)

The image shows a light gray rectangular frame with three small circles in the top right corner. Inside the frame, the INACH logo is displayed at the top. The logo consists of the letters 'I', 'N', 'A', and 'C' in a dark blue, sans-serif font, followed by the letter 'H' in a larger, bold, dark blue font. The 'A' is white and is set against a solid orange circular background. Below the logo, there is a paragraph of text in a dark gray, sans-serif font. At the bottom of the frame, there is another paragraph of text in the same font.

Sexualised violence: video chats with children misused for intimate recordings

In 2023, jugendschutz.net documented 4,983 cases with depictions of sexualised violence.

A large proportion of the recorded offences are recordings of video chats. They predominantly show underage girls - often before the onset of puberty - alone or together with their peers in front of the camera. Scantily clad or naked, they adopt sexualised poses or perform sexual acts on themselves.

The recordings are often made as a result of cybergrooming. Images and videos that were probably created consensually as part of sexting are also made available in an abusive manner. There have been isolated reports of criminal AI-generated images showing sexualised violence against children and young people.

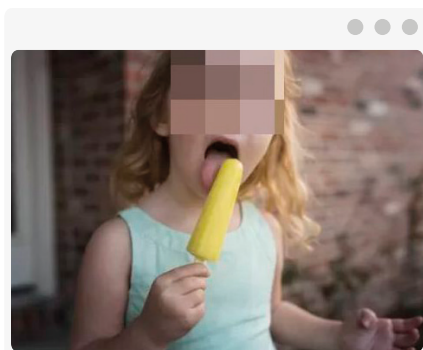
A persistent problem is the networking of paedocriminals via the internet. In addition to the publication of depictions of sexualized violence, perpetrators also use comments to turn everyday images of children in a sexualized context. The keywords, tags and album titles used associate children with sexualised acts and make the intention clear.

2023

4.983

Cases of depictions of sexualised violence

In some cases, there are direct requests to share images of sexualised violence. Perpetrators use services such as Telegram or other messengers to network with like-minded people.



An example from a collection of pictures entitled "Little girls licking ice cream", which are commented on sexually. (Image in original unpixelated)

DANGERS AND RISKS

"Sugardating" is a phenomenon that has a considerable potential to endanger children and young people: They come into direct contact with adults who have sexual intentions. On portals such as mysugardaddy.eu, older (mostly male) users can arrange to meet younger people for pseudo-romantic encounters in exchange for money, gifts or other benefits. During a test with a profile on mysugardaddy.eu that was recognisably created as a minor, jugendschutz.net received private messages from adults within 30 minutes. They asked directly "for casual dates and sex for money".

Although the platform's terms and conditions exclude the use of users under the age of 18, there is no age check when registering. jugendschutz.net came across profilnames such as "KLEINESMÄDCHEN_MA" or "13JAHREJUNGE", which indicated that minors also use the service.

The use of corresponding hashtags on TikTok or Instagram shows that the topic is present among children and young people. When viewing livestreams on TikTok and Likee, jugendschutz.net repeatedly observed comments such as "Meet for money" or "Earn extra money". Some of the comments were combined with requests for private contact via the internal messaging function or messengers such as WhatsApp or Snapchat.

INHOPE

As a founding member, jugendschutz.net works together with the partners of the International Association of Internet Hotlines (INHOPE). The aim is to combat depictions of sexualised violence against children online.

The participating organisations report violations via a joint database. They develop best practices and exchange expertise and technical know-how. The network currently has 54 members from 50 countries worldwide. (inhope.org)

Challenges, pranks and fitness: trends with dangerous consequences

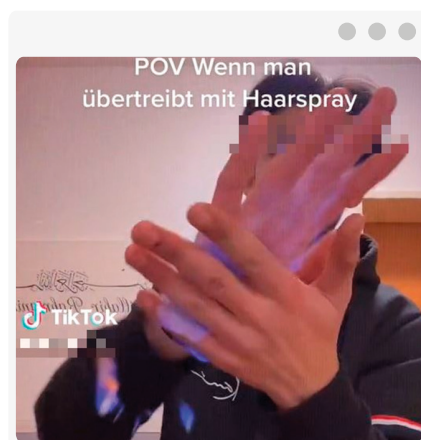
There are many trends on social media services such as TikTok that encourage children and young people to join in and go viral quickly. The spectrum is diverse and ranges from fun competitions to lifestyle tips on nutrition, health and body awareness. Posts with challenges and pranks in particular achieve many clicks on social media.

The hot chip challenge was very popular last year. This involves eating an extremely hot tortilla chip. Afterwards, nothing should be drunk for as long as possible so as not to neutralise the spiciness. This can have serious consequences such as shortness of breath, stomach cramps and circulatory problems. jugendschutz.net observed many posts in which

young people in particular were called upon to show courage and join in. For a long time, the chips could be purchased at many kiosks without an access barrier, but some federal states have now banned their sale.

The Firefinger Challenge has become a similarly dangerous trend. It involves young people wetting a finger with flammable liquid and lighting it on fire. The flame is then extinguished with the other hand during a certain line of a song. Videos show how the fire gets out of control and spreads to the entire hand or takes hold of other parts of the body. In the case of obviously dangerous challenges, users often distribute tutorials that give the deceptive impression that it is safe to take part. The supposedly fun idea and mass documentation of the tests of courage also encourage imitation.

TikTok and other services usually block hashtags for dangerous challenges quickly. However, the videos can still be accessed via other keywords.



Highly dangerous: During a firefinger challenge, a user accidentally ignites his whole hand and parts of his jacket.
(Source: TikTok; original unpixelated)

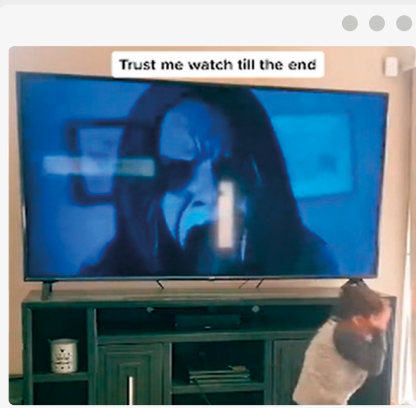
DANGERS AND RISKS

Posts that portrayed trend drugs such as laughing gas as supposedly harmless and promoted their use also quickly went viral. Utensils, e.g. cream dispenser capsules filled with added flavour, were available via online shops and associated social media accounts. What is presented as a harmless and legal party drug is highly dangerous: frequent inhalation can lead to severe neurological damage. There is hardly any critical discussion of the risks and consequences of abuse in the offers.

There are many imitators of pranks in which children are deliberately put into emotional states of emergency for the amusement of the community. Often young people (e.g. older siblings), parents or other caregivers take on the role of the prankster. They place their victims in scary, supposedly dangerous or unpleasant situations in order to cause fear, disgust or even despair.

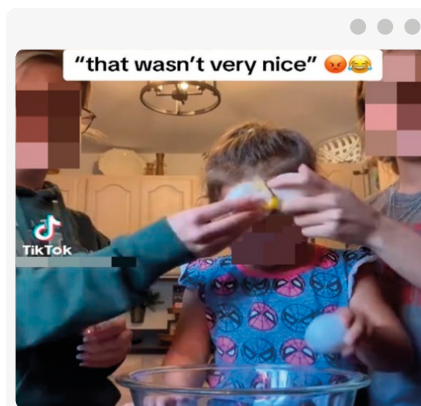
In some “pranks”, pranksters use app effects and filters to create, e.g. ghostly apparitions, monsters or spiders over their victims’ videos to scare them. The smartphone is positioned in such a way that the pranked children notice the changes on the screen. In this way, children are led to believe that spiders are crawling across their faces or that there are ghosts in the room.

In the TV scare prank, children are frightened by a horror figure that suddenly appears on the TV screen during a harmless video. The children are shocked and run away in panic.



A calm video is followed by a horrifying image: the boy who has been pranked puts his hands to his face in panic.
(Source: TikTok)

The Eggcrack challenge on TikTok had a strong pull effect: Parents crack a raw egg on their children's heads for fun, film the reaction and post the video online. The act is intended to amuse viewers and generate clicks. Children often react in horror, cry or lash out.



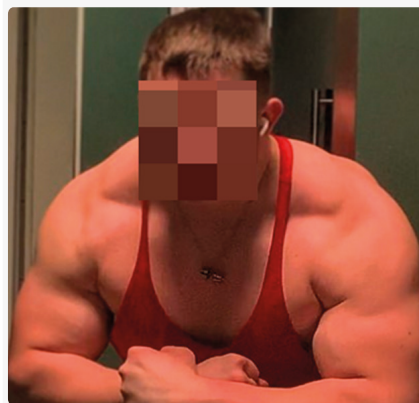
Pranked child reacts to eggcrack challenge: The reaction is ridiculed by laughing faces.
(Source: TikTok; original unpixelated)

All of the pranksters' "pranks" are aimed at triggering emotional reactions in the children. They are defencelessly at the mercy of the unpleasant or frightening situation. It is particularly worrying because very young children actually feel safe in the presence of their parents or siblings and trust them to protect them. This trust is shaken by the pranks. Their emotions are publicly exposed. In addition, the posts can be misused and misappropriated in other contexts, e.g. for cyberbullying.

Trends in social media do not necessarily have to be aimed at short-term thrills or crossing boundaries in order to be risky. "Fitfluencing", which is becoming increasingly popular, has a lower-threshold approach. Children and young people are attracted by the idea of earning money and recognition by optimising their own bodies. (Strength) sport in particular is often elevated to the status of an all-encompassing lifestyle. The images of well-trained peers can lead to high pressure to achieve a comparable appearance.

Training methods and diets of fitfluencers and the public self-presentation through clothing, language and gestures are copied. The protagonists often recommend the following to achieve the goals: unhealthy dietary supplements and training sessions far beyond the limits of endurance. A hobby that should be fun, can be so quickly detrimental to health and promote exaggerated and unrealistic body ideals.

Fitfluencers are increasingly posting images in a visually perfect form, e.g. through the use of "beauty" filters, AI or image editing. These further distort the idea of the ideal body and increase the pressure of expectations.

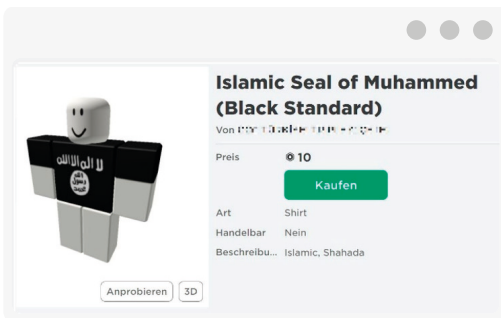


A 15-year-old Fitfluencer shows off his muscles to his followers.
(Source: Instagram; original unpixelated)

With over 70 million active users every day, Roblox is one of the most popular gaming platforms worldwide. The service is particularly popular among children and young people: at the beginning of 2023, almost half of all players were under 13 years old.

What makes the platform particularly attractive is the wide range of gaming, design and communication options. Users can create and visually design their own virtual gaming worlds (called “experiences”) as they wish. However, Roblox not only encourages creativity and playfulness, but also harbours dangerous content.

jugendschutz.net found right-wing extremist content in groups, experiences or on avatar clothing and Islamist content, including unconstitutional symbols such as the black banner of the terrorist organisation Islamic State (IS), swastikas and SS runes. In one specific gaming world, users were able to play on a replica of the Norwegian island of Utøya, shooting other people while heavily armed. The right-wing extremist Anders Breivik carried out an attack there in 2011, murdering 77 young people. There were also detailed Nazi concentration camps, as well as the option to give the avatar the appearance of Nazi officers.



Shirt with IS flag: Users can buy clothes, put them on their avatars and thus also spread symbols that are banned (in Germany).
(Source: Roblox; original unpixelated)

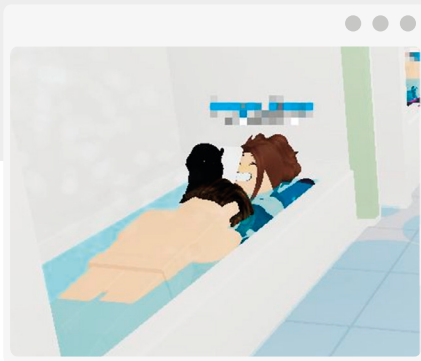
DANGERS AND RISKS

Protection against harassment and cyber-grooming is also inadequate. Users draw attention to themselves with relevant keywords and sexualise conversations with explicit smileys. In addition, movements and actions (e.g. push-ups) of avatars are misappropriated to imitate sexual acts during interactions. Roblox prohibits all of this in its community guidelines and uses a strict word filter. Nonetheless, there are still documented incidents of abuse.

Effective reporting systems can at least provide a quick remedy in such cases and protect against further confrontations. However, Roblox did not perform very satisfactorily in tests: of 26 reported contents that violated the "Interstate Treaty on the Protection of Minors in the Media", the service only removed five after a user report.

Roblox is basically free of charge. However, in-game purchases can be made. To do this, users must purchase the platform's own currency (Robux). This allows them to equip their avatar with special skins and items to customise it and make it more personal. The incentive can quickly become a pull and thus a considerable cost trap. Although purchases are only permitted from the age of 18 or with the consent of a parent or guardian, the service does not actively request this.

Roblox has taken precautionary measures to protect children and young people: Parents can accompany the account to control access to content and in-app purchases. However, these precautions are not enough, as they hardly offer any protection from the dangers



In the "Public bathroom" experience, users imitate sexual acts in bathtubs.

(Source: Roblox; original unpixelated)

of user-generated content. Roblox shares a core problem with many child- and youth-relevant services: there is no reliable age check during registration. As long as users can easily register by providing a false age, even the best age-differentiated precautionary measures are ineffective.



With the "Safer Internet Centres", the EU promotes secure communication on the Internet, in Germany bundled under saferinternet.de: the awareness centre klicksafe.de, the hotlines of jugendschutz.net, [eco](https://eco.de) and [FSM](https://FSM.de) as well as the children and youth helpline "Nummer gegen Kummer". (saferinternet.de)

PROTECTI ON AND PARTICI PATION

Over 7,600 offences registered

jugendschutz.net checks online content that is discovered during research or reported via the online complaints office, authorities and partner organisations. In 2023, 7,645 offences were processed (2022: 7.363).

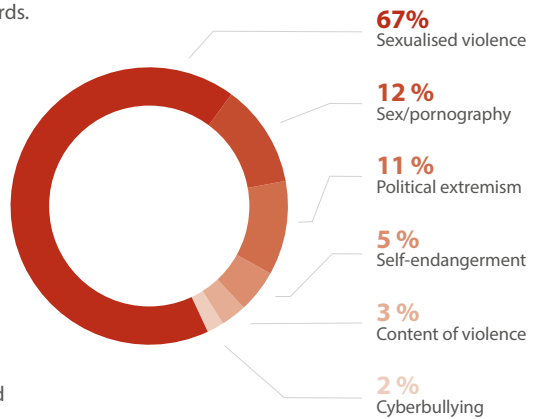
The thematic distribution is comparable to previous years. Sexualised violence continues to account for the lion's share, at two thirds.

The majority of offences involved content whose distribution is absolutely prohibited under the Interstate Treaty on the Protection of Minors in the Media (JMStV). Providers are not permitted to distribute this content, not even to adults. In 2023, this applied to 82 % (2022: 84 %). These were mainly criminal offences such as the Distribution of child pornography (73 %), symbols of unconstitutional organisations (9 %) and youth pornography (5 %).

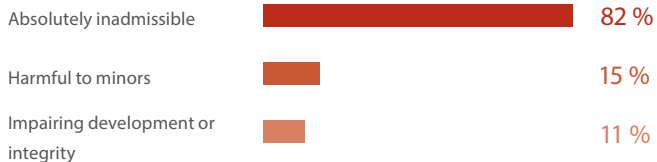
REGISTERED OFFENCES 2023

7.645

Another increase compared to previous years.



Sexualised violence accounts for the majority of cases.



The focus of the work: Absolutely unauthorised cases.

90% of offences removed by the end of the year

jugendschutz.net informs service providers and self-regulation bodies about violations of the youth media protection. The aim is to take swift remedial action and thus immediately eliminate the impairment or danger to children and young people. This activity took place in 3,210 cases of offences last year.

If a responsible provider can be identified, jugendschutz.net forwards the case to the Commission for the Protection of Minors in the Media (KJM) or the responsible state media authority to initiate proceedings. In 2023, this was the case for 105 offences. In addition, 252 cases were forwarded to the KJM for indexing by the Federal Agency for the Child and Youth Protection in the Media (BzKJ).

If content contains child or youth pornography or poses a risk to life and limb, law enforcement is informed directly by jugendschutz.net. This was necessary for 3,582 offences. This activity thus accounted for the largest share in 2023. Cases of child sexual abuse material (CSAM) or other sexualised violence against minors not under investigation in Germany are forwarded to the relevant INHOPE partners.

At the end of the year, 6,902 cases (90 %) of the offences had been rectified.

Information for providers and self-regulation bodies

3.210

Mainly sexualised violence and political extremism.

Supervisory cases to KJM

105

Mostly pornography and indexed content.

Indexing cases to KJM

252

Mainly animal pornographic content.

Disclosure to law enforcement

3.582

Sexualised violence.

Passing on to INHOPE partners

280

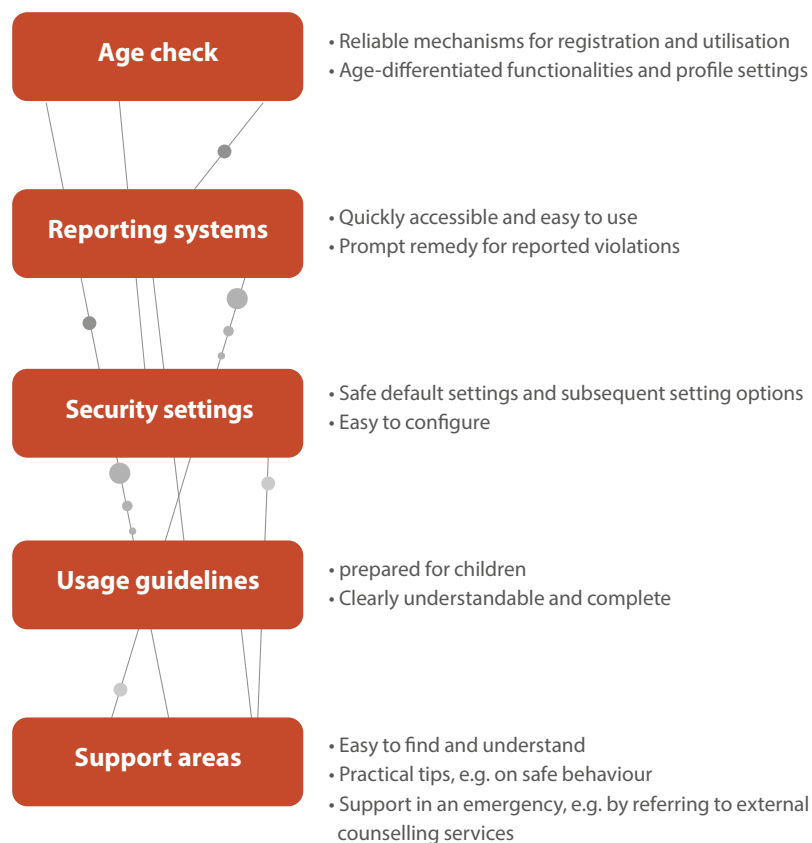
Sexualised violence.

Review of preventive measures by providers

In order to enable children and young people to participate safely and age-appropriately online, platform operators are now legally obliged to take appropriate precautionary measures. In Germany, the Youth Protection Act (JuSchG), which was amended in 2021, formulates regulations for better protection of minors. With the Digital Services Act (DSA), there is also an EU-wide set of rules that obliges internet service providers to minimise systemic risks on their platforms.

jugendschutz.net continuously monitors precautionary measures for services that are particularly relevant for children and young people. In 2023, this included TikTok, Instagram, YouTube, Snapchat and Facebook. Other services were reviewed on an ad hoc basis.

**jugendschutz.net examines precautionary
measures in various areas:**



Lack of age verification remains the biggest problem

Reliable age verification of users in online services is in short supply and remains the central weak point in providers' protection concepts. Almost all platforms monitored by jugendschutz.net set a minimum age and offer age-differentiated access. However, the providers do not or only insufficiently check the age. When registering, the platforms generally only ask for the date of birth and trust the information provided. If you try to register with an age below the set minimum age, the process is often only interrupted. In most cases, the date of birth can be corrected directly and registration can be continued.

A reliable age check is essential for the most precautionary measures. E.g. Protection mechanisms that are intended to prevent third parties from contacting or accessing your own content are ineffective if the age is incorrect. The same applies to filters that providers use for accounts of minors. They are intended to prevent confrontation with harmful or dangerous content. This protective function is also cancelled out if children and young people can pretend to be 18 years or older. They are then defencelessly exposed to all risks on the service.

The use of artificial intelligence in age verification could help to improve the level of protection in the medium term. Some services already use AI-supported "age estimation" in some cases, but only to determine the age of majority. In this process, the user's age is determined by taking a real-time image of their face via the webcam. At present, age estimation systems still have difficulties in accurately determining small differences in age. If developments in the field of AI continue to progress, a sufficiently accurate and data-efficient approach could emerge. Documents and extensive data would then no longer be necessary.

Inadequate response to the reporting of violations

An easy-to-use and effective reporting system that ensures rapid remedial action in the event of offences is particularly important for the protection of children and young people. Reporting is often the only way to draw attention to harmful content or contacts. This makes it all the more important that providers examine complaints promptly and take consistent action in the event of violations. This usually involves deleting or blocking the content.

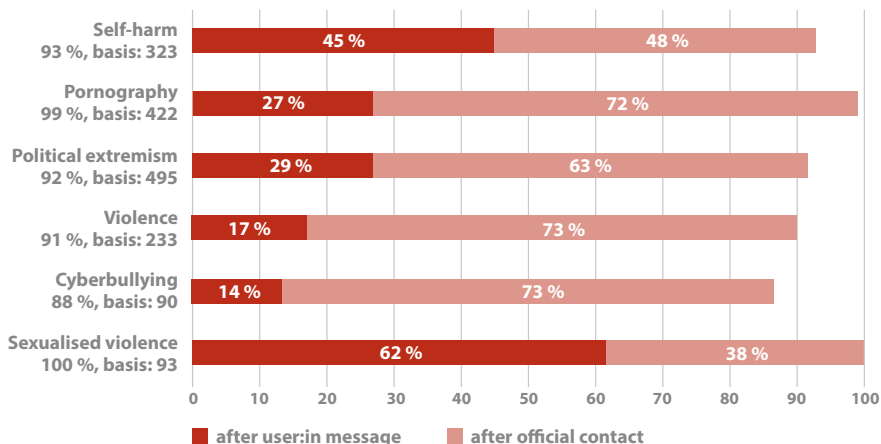
The results of the 2023 tests show once again that services with an affinity for young people do not take their duty to take remedial action seriously when offences are reported. For several phenomena the average deletion rate according to user reports was only less than a third - including violence, pornography and political extremism. For content of self harm, the response rate was only 45 %.

Slightly better: in the case of sexualised violence, 62 % of reports were deleted.

jugendschutz.net uses a two-step procedure to check the reporting systems: In the first step, offences are submitted as regular user reports. This means that jugendschutz.net cannot be recognised as the sender. If the reported content has not been deleted or blocked after seven days, jugendschutz.net officially requests as an institution for removal. Whether the service has taken any action is checked after a further seven days.

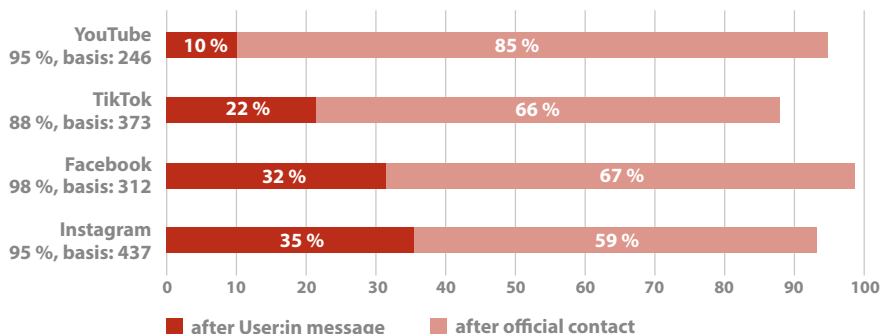
Cancellation rates via Reporting systems

Test results by topic



Cancellation rates via Reporting systems

Total test results



YouTube has disappointing deletion rates overall following reports from users. In the area of pornography, there was a drastic drop compared to the previous year (4 %; 2022: 62 %). The poor reactions to offences in the context of political extremism (14 %) are also difficult to understand: The vast majority of the content reported for this was criminal content, which is usually easy to recognise as an offence.

While **TikTok** achieved the best result for self-harm content in 2022 with 42 % of cases removed according to user reports, the rate in 2023 was only 22 %. This is particularly problematic as dangerous challenges spread rapidly via TikTok and have a wide reach among children and young people.

Facebook responded particularly poorly to cases relating to violence and political extremism: the service removed only 8 % of reported depictions of violence, only 13 % of content showing human dignity violations and only 22 % of right-wing extremist criminal offences. It also remains incomprehensible that only 32 % of pornographic content was removed.

While **Instagram** was better at deleting self-harm than in the previous year (68 %; 2022: 49 %), the rate for cyberbullying fell significantly (24 %; 2022: 62 %) and political extremism (17 %; 2022: 36 %). The service performed particularly poorly when it came to depictions of violence (0 %) and violations of human dignity (8 %).

Security settings: Basic protection with gaps

Safe default settings in online services are a key requirement for enabling children and young people to participate in an age-appropriate manner. Basic protection is now offered by all services, which are checked on an ongoing basis. However, this only applies if the age is truthfully stated. Young people should also be able to make additional safety settings quickly and easily themselves. In 2023, some providers made improvements and some things got worse:

TikTok



Minors have more control over their posts and data. They can now see in the settings whether videos from other users have been combined and shared with their own content (so-called duets and stitches). These can be deleted, including the originals.



The direct messaging function is open to a wider audience. In addition to "Friends" and "Nobody", young people aged 16 and over now have a third option for receiving private messages: "Suggested contacts and friends from Facebook".

Instagram



Users can better control who can and cannot see posts. Posting content can now be restricted to "Close friends" (up to 100 people). Previously, posts could only be shared with all followers or completely publicly.



For public profiles, the dangers of losing control over one's own data and the misuse of data by unauthorised parties have become increasingly apparent. Reels can now be downloaded there by one click - even if the accounts in question are those of minors.

Snapchat



If minors are contacted by a person with whom they have no or only a few contacts in common, they now automatically receive a warning message that they probably do not know them and that caution is advised. They can then block or report the account directly from the chat window or agree to the conversion.

Utilisation guidelines and support services further developed

Some services have improved their utilisation guidelines and offers of support. However, it is crucial that violations of their own guidelines are consistently sanctioned. The providers still have a lot of room for improvement here, as the analysis of the reporting tests shows.

YouTube



Live streams in which firearms are shown are now prohibited. In addition, external links to third-party content that violates the YouTube guidelines may no longer be placed in videos. This also applies to non-clickable links, e.g. verbal mentions and superimposed images in the video.



According to the renewed guideline on self-harm, certain content relating to eating disorders is only permitted from the age of 18. However, this measure is ineffective if the wrong age is specified. Corresponding to the guideline, help and counselling services are referred to directly under the relevant videos.

TikTok



Underage users now see short videos with information during the registration process, e.g. on protective functions and offers of support. This age-appropriate introduction contributes to the safe use of the service.



The new information hub on fake news offers users tips on how to recognise and check fake news and other disinformation. However, the hub is not integrated into the support portal, but can only be found via a targeted keyword search.

About jugendschutz.net

jugendschutz.net acts as the joint centre 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. 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 Supervisory Bodies and the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth.

jugendschutz.net runs a hotline accepting reports about violations of youth media protection laws.

jugendschutz.net/make-a-report