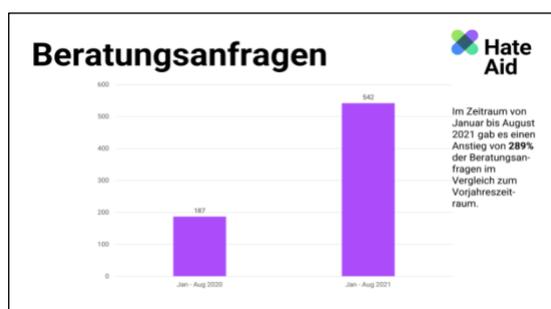


## 9 months after the Capitol Hill insurrection, Big Tech puts the German election at risk

“Today I was called a bastard and a murderer at the election stand, yelled at and followed up to my car. Already common on the Internet, we can now see it on the street. Take care of yourselves!”  
(Torbjörn Kartes, CDU, on 30.07.)

Two years have passed since the political assassination of Walter Lübcke, a member of the Christian Democratic Union (CDU) party in Germany. His assassin had ‘consumed far-right extremist propaganda’<sup>1</sup> on social media for years. Today, research repeatedly shows that hate on the Internet is growing at an alarming rate—especially on social media platforms like Facebook and YouTube. The President of the BKA (Federal Criminal Police Office), Holger Münch, recently warned that “this development could endanger democracy”.<sup>2</sup> Requests for help against online threats, including requests from many local politicians, have tripled in the past year.

Social media platforms hosting these targeted hate comments, like Facebook and YouTube, do not simply “mirror” the sentiments and opinions of their users. They are not neutral transmitters of human or political communication. On the contrary, their algorithms select and amplify hate and disinformation to users who otherwise may never be exposed to it. While social media platforms profit from keeping people hooked on their product, they simultaneously polarise and divide the public debate.



One need not look far to find other examples of social media driving deep cuts into society. In 2020, Big Tech pushed US democracy to the brink of disaster when an angry mob, disinformed by online media, attacked the US Capitol in the unwavering, albeit false, social media-fueled belief that paedophile elites had stolen Donald Trump's election victory. In the end, five people were dead. Once again, Facebook and Twitter promised to do better after a multitude of

researchers demonstrated their complicit role in the insurrection—but shortly before the federal election in Germany, we see that major platform operators are neither complying with legal requirements nor enforcing their own community standards e. g. on hate or disinformation in the run-up to our federal election. To make matters worse, the legal framework in place to constrain Big Tech, like the Network Enforcement Act (NetzDG), are failing to protect our democracy or individuals from online harms.

Social Media Platforms only take insufficient action against manifestly illegal content, even if it is reported by the users.

<sup>1</sup> [Father, Neighbor, Killer: Germany's New Far Right Terror](#)

<sup>2</sup> [BKA-Präsident Holger Münch: Der Hass im Netz nimmt weiter zu](#)

## Insufficient protection against criminal content

A recent nation-wide survey amongst eligible voters shows that three out of four Germans expect platform operators to do more against hateful content on social networks.<sup>3</sup> Meanwhile, Facebook does not even comply with the existing legal requirements of the NetzDG. We reported 100 manifestly illegal comments from public Facebook pages and groups of the AfD, a right wing party in the German parliament, according to the NetzDG. In 33 cases, Facebook saw no violation and comments remained on the platform. Especially in the case of high-ranking politicians, we found that comments were only deleted in a few cases, even if they contained massive insults.<sup>4</sup> This included the following comments:

Horst du hurensohn ich fick deine mutter.

Es lebe die fette muschie von deiner nazi junkie mutter!

Like · Reply · 5y

Ich kotz auf dich du grüne fotze 🤢🤢

Like · Reply · 12w

However, Facebook deleted almost all of the remaining 67 comments with reference to its own community standards, and not according to the law. This way Facebook evades the legal obligations according to the NetzDG, such as to provide a statement of reasons or include the decision in their transparency report. Instead Facebook made them disappear.

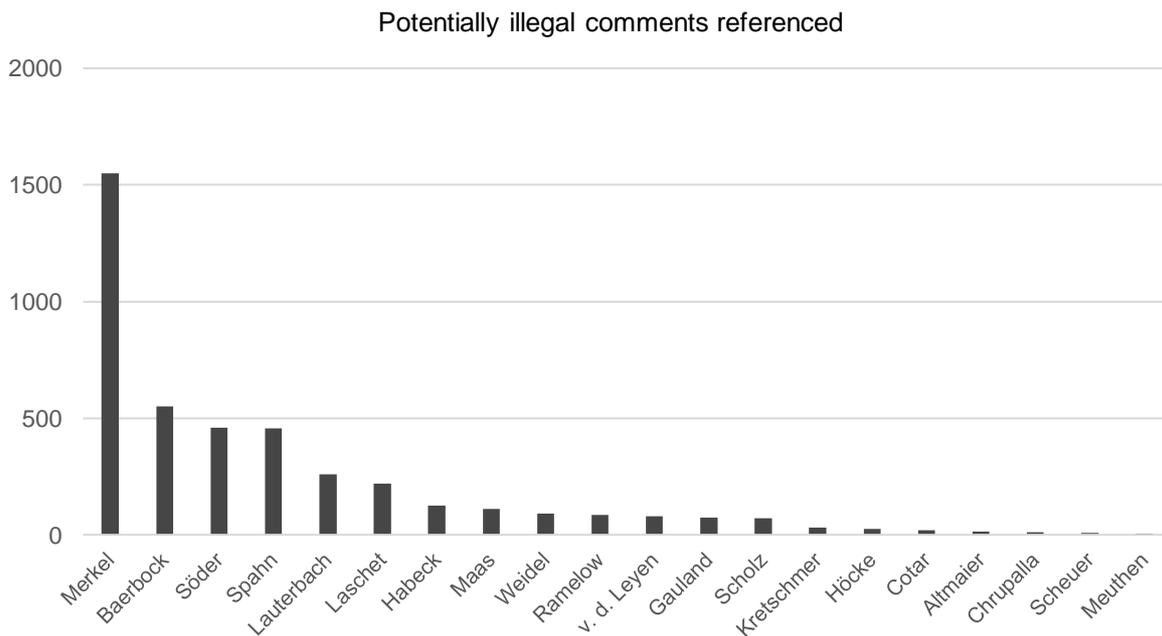
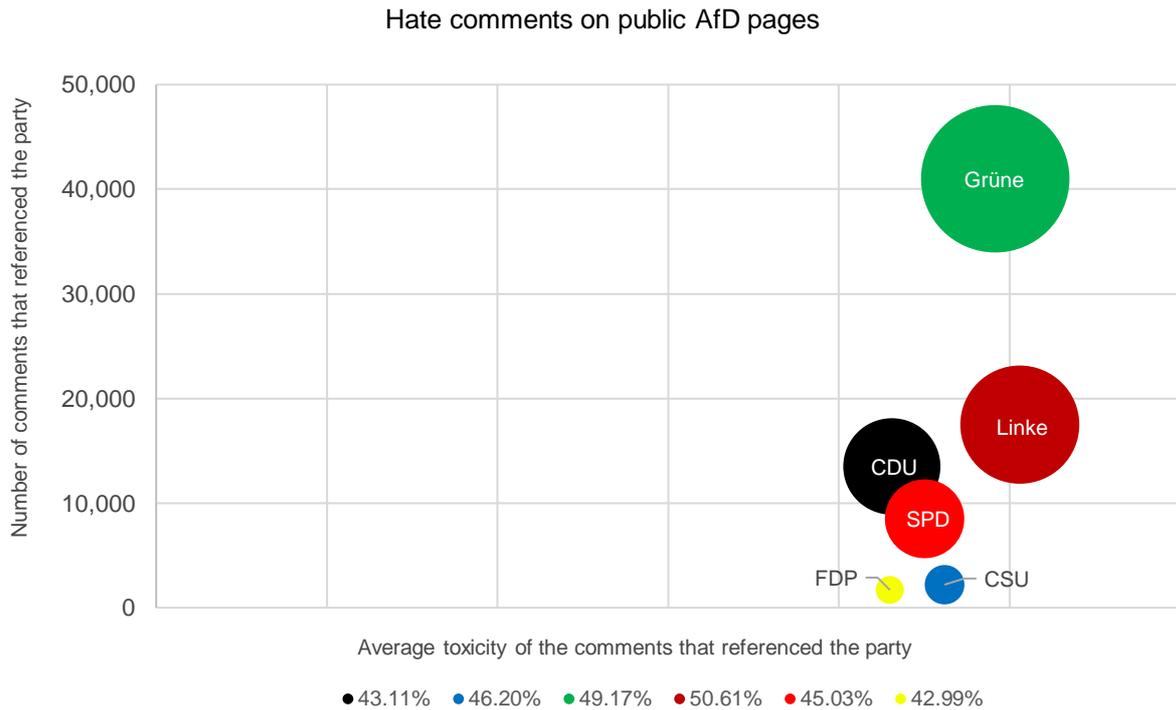
In any case, Facebook only took action against the illegal content upon notification by us. On average, the 100 manifestly illegal comments had been on the platform for **409 days** at that point. Even if Facebook conscientiously complied with the requirements of the NetzDG, the law would hardly offer any protection against criminal content. Due to European law, Facebook is not liable for content uploaded by users unless the “actual knowledge” of the item. This shows impressively that Facebook is not willing to protect users from manifestly illegal content beyond the minimum legal requirements, even if serious crimes are committed on the platform. For example, the following content was accessible public Facebook groups for five years:



<sup>3</sup> [Social Media in Germany: Effects on the Culture of Debate, Disinformation, and Hate](#)

<sup>4</sup> Statements against high-ranking politicians are not automatically covered by the freedom of expression in the “political battle of opinions”, so that an insult can also be present here. This was also clarified by the Federal Constitutional Court in May 2020 (decisions of 19 May 2020 - 1 BvR 2459/19, 1 BvR 2397/19, 1 BvR 1094/19 and 1 BvR 362/18).

## Hate comments on public AfD pages

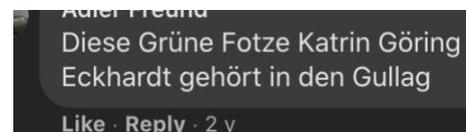
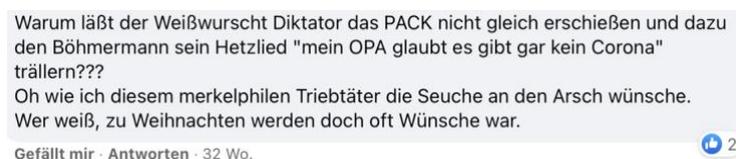


## Insufficient enforcement of community standards

“We don’t allow hate speech on Facebook. It creates an environment of intimidation and exclusion, and in some cases may promote offline violence.” (Facebook Community Standards)<sup>5</sup>

Comments that we reported for violations of Facebook’s hate speech policy, were deleted by the platform only in 50 percent of the cases—if the company reacted at all.

A sample of reported content available on the platform up to this point:



The AfD in particular is benefitting from the negligent enforcement of the community guidelines. While Facebook claims that they learned their lessons from the US elections, they allow the AfD to gain an enormous reach with content that promotes conspiracy theories, disinformation, denial of the covid 19 pandemic or manipulation of elections although this content clearly violates their community standards. Because Facebook’s recommender systems are built to maximise attention, the spread of disinformation and inflammatory content is automated for profit. That is why AfD pages achieve on average five times as many interactions as the pages of the Christian Democrats (CDU), Greens or Social Democrats (SPD), according to research from the NGO *Hope not Hate*. In the example attached, a post by an AfD candidate which denies the covid-19 pandemic and spreads conspiracy narratives of the militant *QAnon* cult gained viral reach. With automated recommendations of political groups, pages and posts, Facebook not only increases the reach of harmful content, but also creates an environment where political parties are no longer treated equally.



On the Facebook pages of the AfD, there are many indications of potential “Coordinated Inauthentic Behaviour”, a practice where disinformation about political actors is spread to intentionally mislead users and that violates Facebook’s policies. For example, 250,000 of the 1 million comments from our research sample were attributed to only 1 per cent of the user accounts. In addition, presumably authentic user profiles spread hundreds of misquotations from Green politicians<sup>6</sup>, thus violating

<sup>5</sup> [https://www.facebook.com/communitystandards/objectionable\\_content](https://www.facebook.com/communitystandards/objectionable_content)

<sup>6</sup> <https://twitter.com/benheubl/status/1422922869840007171>

Facebook's community standards. Already during the state elections in Saxony-Anhalt, disinformation about a supposed "election fraud" went viral, multiplied thousands of times by the automated recommender systems of Facebook and Twitter. (This happened despite claims that they will not tolerate disinformation about the course and results of elections).<sup>7</sup>

The fact that Facebook does not even assume responsibility for the content of paid advertisements was proven by another investigation: Facebook recently authorised advertisements for conversion therapies, which were specifically displayed to LGBTIQ youth.<sup>8</sup> Facebook, contrary to its own guidelines, also allowed accounts associated with the AfD to place inflammatory and defamatory ads about the Bundestag candidate Tareq Alaows, who eventually withdrew his candidacy.<sup>9</sup> In June, Facebook also placed racist and defamatory ads of the far right party NPD, which clearly violated Facebook's own guidelines.<sup>10</sup> Meanwhile, Facebook is harassing and censoring researchers conducting studies on online political advertising in the run-up to the federal elections.<sup>11</sup>



<sup>7</sup> [Desinformationskampagnen gegen die Wahl: Befunde aus Sachsen-Anhalt - ISD](#)

<sup>8</sup> The ads were deleted before they would have actually gone "live". [Facebook lässt problematische Werbeanzeigen für Minderjährige zu](#)

<sup>9</sup> <https://www.facebook.com/ads/library/?id=327525171956480>

<sup>10</sup> [Facebook Community Standards](#)

<sup>11</sup> [Wegen Facebook-Sperre: Aus für Datenprojekt zur Bundestagswahl](#)

## Recommendations for protecting the German election

In the medium term, the German federal government should advocate for systemic regulatory approaches at the EU level, such as those contained in the EU Commission's proposals for a “Digital Services Act” and for AI regulation.

The federal government and all parties should push platforms to implement the following measures (the proposals are based on the experience of the US elections, the work of *HateAid* and other NGOs and other NGOs and the expertise of various international research institutions):

*Above all else, Facebook must comply with the law and the associated obligation to delete and report illegal content. Content that is reported by users as breaking the law must be recorded and processed as such, instead of letting it “disappear” with reference to the company's own guidelines. Lawmakers should ensure the supremacy of legal regulation over private company rules.*

### Prevention of (digital) violence

- The platform operators carry out risk analyses and inform parties, candidates and authorities about which persons or groups of persons are particularly affected by hate and provide early information, for example about increased calls for violence.
- Use of human moderators in groups and on pages with more than 20,000 members where the risk of hate speech, disinformation, verbal or actual violence is particularly high.
- No automated recommendations for political pages, groups and profiles or from websites that spread disinformation or incite hate and violence.
- All corporate policies to protect the federal election come into effect before September—not after problems are already out of control. Consistent and comprehensible effective enforcement of own policies by psychologically supervised and trained staff who speak German and understand cultural and contextual nuances of speech.
- Protection of women from image-based sexualised violence in particular: If intimate photos or manipulated images get on the Internet (including deep fakes), it is often almost impossible to stop them from spreading. Even if they are removed, they are reuploaded over and over again. Tech companies have all the possibilities to prevent this, but they do not make use of them. Companies should therefore immediately set up a cross-platform database of images marked as illegal. Databases for terrorist and child pornography content could serve as a role model.
- Real-time transparency of online election advertising<sup>12</sup>, including all targeting parameters and friction in the advertising system that would not allow profits from ads that are clearly inflammatory and racist.
- Use of the News Ecosystem Quality Score to curate and recommend newsworthy content, as Facebook did before the US election.<sup>13</sup>

---

<sup>12</sup> Users should be able to find out on the basis of which data or information they are being contacted and whether they have actually consented to the use of such data and information.

<sup>13</sup> [Facebook Struggles to Balance Civility and Growth](#)

## Documentation and sanctioning of (digital) violence

- To ensure the documentation and reporting of offending content, independent researchers and auditors are given access to all posts and comments on public pages and public groups associated with political parties or dedicated to political issues<sup>14</sup> via programming interfaces.
- Improved cooperation with law enforcement, especially regarding fake and multiple profiles, that spread the majority of illegal content according to our research. So far, requests from law enforcement authorities are answered only arbitrarily. In most cases, reference is made to the headquarters in Ireland or even the USA as the place of data storage. If data is obtained, it is usually worthless.
- Systematic recording of contributions that contain digital violence via an independent agency (e.g. Lumendatabase). In addition, platforms should offer differentiated transparency reports with thematic breakdown.
- Weekly reporting on the measures taken to prevent the (automated) dissemination of punishable content, as Twitter has done recently.<sup>15</sup>

---

*Reset* is an initiative engaged in programmatic work on technology and democracy. Reset provides grants and contracts while working alongside partners with a shared policy, technology, and advocacy agenda in countries with immediate opportunities for change. Reset's goal is to stop Big Tech companies from profiting off public harm by resetting the rules for online media.

*HateAid* is the first point of contact for victims of digital violence in Germany. Since founding in 2018, HateAid has supported more than 1300 victims through counselling, security and communication consulting. Besides, organisation offers litigation financing so affected persons can access justice and enforce their rights against online platforms and perpetrators in the digital space. With campaigns, workshops and other public engagements, HateAid's team also creates social awareness of the destructive effects of digital hatred on our democracy. In 2021 HateAid joined forces with the Alfred Landecker Foundation, launching the "Landecker Digital Justice Movement" to stand up for a democratic internet by financing landmark cases against the digital platforms and advocating for a hate-proof EU legislation that protects victims of digital violence.

---

<sup>14</sup> In the sense of Facebook's own definition: [About ads about social issues, elections or politics](#)

<sup>15</sup> [Combatting online racist abuse: an update following the Euros \(blog.twitter.com\)](#)