

# Germany

## C Violations of User Rights

*New legislation empowers law enforcement agencies on the federal and state levels to access personal user data and install malware on electronic devices for the purpose of criminal investigations. In a landmark decision, the Federal Constitutional Court ruled that the German Basic Law applies to foreign surveillance operations, not only domestic surveillance. In the aftermath of the 2015–16 refugee crisis, there has been a surge in investigations for online “incitement to hatred.”*

C1 1.00-6.00 pts0-6 pts

Do the constitution or other laws fail to protect rights such as freedom of expression, access to information, and press freedom, including on the internet, and are they enforced by a judiciary that lacks independence?	5.005 6.006
--	----------------

Article 5 of Germany’s Basic Law guarantees freedom of expression and freedom of the media. Judicial bodies operate independently, and generally support the protection of basic rights.

Since 2016, the Office of the Federal Commissioner for Data Protection and Freedom of Information has been an independent supreme federal authority, a clear upgrade from its former status as a subdivision of the Federal Ministry of the Interior.<sup>139</sup> This change of constitutional status entailed a significantly larger budget and staff.<sup>140</sup> Since its founding, the agency has tripled its capacities, and recently enlarged its staff to strengthen the supervision of security authorities.<sup>141</sup>

Online journalists are largely granted the same rights and protections as journalists in print or broadcast media. However, the official press card remains available only to “professional” journalists, meaning those whose journalistic activities account for at least 51 percent of their income.<sup>142</sup> This card is often connected to granting rights of privileged access for journalists, for example, to demonstrations. Similarly, the German code of criminal procedure grants the right to refuse testimony solely to individuals who have “professionally” participated in the production or dissemination of journalistic materials.<sup>143</sup>

After two journalists from the online outlet Netzpolitik briefly faced criminal proceedings for alleged treason in 2015, Federal Minister of Justice and Consumer Protection Heiko Maas announced a bill with the aim of explicitly excluding journalists from the scope of the treason provision in the criminal code. However, the promised reform had not made any as of the end of the coverage period.<sup>144</sup>

## C2 1.00-4.00 pts0-4 pts

Are there laws that assign criminal penalties or civil liability for online activities?	3.003 4.004
---	-------------

The German criminal code includes numerous prohibitions that apply to the online realm, such as Section 130, which penalizes calls for violent measures against minority groups and assaults on human dignity.<sup>145</sup> This provision is seen as legitimate in the eyes of many Germans, particularly because it is generally applied in the context of Holocaust denial.<sup>146</sup> NetzDG defines illegal online content in relation to 22 provisions in the German criminal code, including Section 130. Other provisions prohibit defamation, forming a criminal or terrorist organization, and “using symbols of unconstitutional organizations.”<sup>147</sup> In the context of NetzDG, many activists, politicians, and officials have expressed concern that these provisions are too broad. In addition to facilitating content removals, these provisions carry penalties in the form of fines and, in some cases, jail time.

After the satirist Jan Böhmermann came under criminal investigation in 2016 for a provocative poem mocking Turkish president Recep Tayyip Erdoğan, the federal parliament abolished a provision of the criminal code that penalizes insulting foreign leaders.<sup>148</sup> Erdoğan also filed a civil libel lawsuit against Böhmermann, which led to a ban on three-fourths of the controversial poem and its deletion from the website of the television channel on which Böhmermann performed.<sup>149</sup> Both parties appealed the judgment. In May 2018, the judgement was upheld, with an appellate court rejecting Böhmermann’s request to repeal the partial ban. At the same time, the court ruled that Erdoğan had no right to have the entire poem prohibited.<sup>150</sup> In January 2019, Böhmermann launched a complaint with the Federal Court of Justice challenging the rejection.<sup>151</sup> The Federal Court of Justice dismissed the appeal in July 2019, after which Böhmermann filed a complaint with the Federal Constitutional Court, Germany’s highest court, which had not yet ruled as of June 2020.<sup>152</sup>

## C3 1.00-6.00 pts0-6 pts

Are individuals penalized for online activities?	5.005 6.006
--	-------------

In the context of the 2018 refugee crisis, previous years saw a surge in law enforcement investigations invoking the provision on “incitement to hatred” in the German criminal code, mostly related to hate speech against asylum seekers on social media platforms such as Facebook. As a result, there have been considerably more convictions for incitement to hatred.<sup>153</sup> Official crime statistics document 4,486 such cases of in 2018.<sup>154</sup> In 2019, the BKA documented 1,524 posts that fit the criminal code definition of hate speech from that year, 73 percent of which were categorized as being politically right-wing.<sup>155</sup> In June 2018, police in 10 German states conducted raids against 29 social media users for alleged hate speech.<sup>156</sup> The adopted amendment to the NetzDG will require larger platforms to disclose personal user data associated with postings of certain illegal content, including online hate speech, to the BKA (see C6).<sup>157</sup>

## C4 1.00-4.00 pts0-4 pts

Does the government place restrictions on anonymous communication or encryption?	3.003 4.004
--	-------------

User anonymity is compromised by SIM card registration rules under the Telecommunications Act of 2004, which requires purchasers to submit their full name, address, international mobile subscriber identity (IMSI number), and international mobile station equipment identity (IMEI) number.<sup>158</sup> Nonetheless, the principle of anonymity on the internet is largely upheld as a basic right. A 2014 decision by the Federal Court of Justice further strengthened this right, confirming that an online ratings portal was under no obligation to disclose the data of anonymous users.<sup>159</sup>

Website owners and bloggers are not required to register with the government. However, most websites and blogs need to have an imprint naming the person in charge and providing a contact address. The anonymous use of email services, online platforms, and wireless internet access points is legal. However, in May 2019 the Federal Ministry of the Interior brought forward a new initiative on mandatory backdoors for encrypted messaging services.<sup>160</sup> The proposal has been widely criticized by civil society organizations and industry professionals, including the iRights.Lab, as it would mark the departure from longstanding proencryption policy. Experts also criticized a 2017 legislative proposal by the governing coalition to allow civil lawsuits to gain knowledge of an alleged offender's real name in the case of violations of the right of personality online, especially defamation. Observers voiced concern that this might infringe on the right to anonymity online, if interpreted broadly.<sup>161</sup> Discussions on this topic were still ongoing at the end of the reporting period.<sup>162</sup>

In October 2019, a man live streamed an antisemitic attack on a synagogue in Halle, Saxony-Anhalt, via the gaming platform Twitch. Following the attack, politicians from several states introduced legislation to the Bundesrat in February 2020 to require social networks and gaming platforms to collect users' names, addresses, and date of birth, as well as proof of identity, and to hand them over to the police upon request.<sup>163</sup> As of June 2020 the draft was passed on to the Bundestag and assigned to an expert committee.<sup>164</sup> With further amendments to the NetzDG implemented in 2020 (see C6), the federal government has been criticized for establishing an overextended ability to access to personal user data for the BKA through private companies. In an open letter, 13 associations concerned with digital rights urged the Ministry of Justice and Consumer Protection to focus on the origin of hate crimes in general, and to stop outsourcing government's responsibility to prevent hate speech to foreign companies.<sup>165</sup>

In March 2019, the Federal Council proposed a bill against illegal online marketplaces. It will add a new criminal penalty for offering services in Germany on the Darknet that contribute to or enable other crimes such as the spread of illegal drugs, explosives, or child sexual abuse imagery.<sup>166</sup> The bill specifically mentions the use of the Tor browser as a vehicle to access such services. Due to its broad language, legal observers argue the scope of the bill would encompass potentially all Darknet services and therefore severely hinder the effective use of the Tor services to anonymize users' online communication.<sup>167</sup> Public criticism increased following the draft's first approval by the Bundesrat in summer of 2019, and the bill was still stalled at the end of the coverage period.<sup>168</sup>

C5 1.00-6.00 pts0-6 pts

Does state surveillance of internet activities infringe on users' right to privacy?	2.002 6.006
---	-------------

Article 10 of Germany's Basic Law guarantees the privacy of letters, posts, and telecommunications. These articles generally safeguard offline as well as online communication. A groundbreaking 2008 ruling by the Federal Constitutional Court established a new fundamental right regarding the “confidentiality and integrity of information technology systems” as part of the general right of personality under Article 2 of the Basic Law.[169](#)

A German parliamentary commission of inquiry on intelligence practices—established after former US National Security Agency (NSA) contractor Edward Snowden leaked documents exposing the various activities of US, British, and German intelligence services in 2013—completed its work in 2017.[170](#) While the governing coalition concluded that the conduct of both the allied foreign intelligence services and the German Federal Intelligence Service (BND) had been and continued to be within the bounds of the law, the opposition argued that ongoing mass surveillance was unlawful. Both sides drew criticism for not demanding sufficient steps to end the practice in Germany.[171](#) Meanwhile, the German government has taken further steps to significantly expand online surveillance.

In May 2020, the Federal Constitutional Court ruled that the BND is still bound by the fundamental rights of the Basic Law when conducting telecommunications surveillance of foreigners in other countries, finding that the BND had acted unlawfully in monitoring the communications of foreign journalists.[172](#) A 2016 law granted the BND explicit permission to monitor domestic internet traffic as long as they target foreign citizens.[173](#) Press freedom groups argued that the law threatens the constitutionally protected work of foreign journalists reporting in Germany<sup>174</sup> and, in January 2018, a number of nongovernmental organizations (NGOs) and foreign investigative journalists filed a constitutional complaint.[175](#)

Public perception of the May 2020 ruling has been largely positive, welcoming the courts verdict as a reinforcement of the Basic Law.[176](#) The consequences for BNDs operations remained to be seen, as the BND has until the end of 2021 to implement the ruling.

The late-2016 BND law has also been scrutinized for its impact on the privacy of German internet users.[177](#) While the BND is mainly tasked with foreign intelligence collection, one of the main concerns is that the law permits monitoring of all network traffic channeled through the DE-CIX in Frankfurt—the world's largest internet exchange point—which would at least unintentionally affect communications by German citizens as well. In 2016, before the new law's enactment, the operators of DE-CIX had sued the BND in the Federal Administrative Court, arguing that the intelligence service's practices were unconstitutional.[178](#) In May 2018, the court dismissed the claims, declaring that monitoring of the exchange point was lawful.[179](#)

The BND had also been storing and processing bulk metadata records of phone calls via its traffic-analysis system VerAS. In response to a lawsuit filed by Reporters Without Borders Germany,[180](#) in December 2017 the Federal Administrative Court outlawed such intelligence gathering, prohibiting the BND from collecting and processing communications metadata due to a lack of sufficient legal basis for the conduct.[181](#) In May 2018, the BND officially announced that it would end the practice.[182](#) Reporters Without Borders Germany also lodged a parallel complaint

with the European Court of Human Rights, alleging that the intelligence service had been unlawfully monitoring the NGO's own email correspondence.[183](#)

Surveillance conducted by intelligence services under the Act for Limiting the Secrecy of Letters, Posts, and Telecommunications (also known as the G10 Act) has continued to decline.[184](#) With respect to international terrorism, the international arms trade, human smuggling, and international cybercrime, the German intelligence services in 2018 (the latest year for which data is available) conducted 9,927 interceptions of telecommunications in total, of which just 48 were deemed relevant for further inquiry by the BND. The BND's practice of monitoring communications between Germany and foreign countries in accordance with the G10 Act has come under legal scrutiny. Amnesty International has filed a complaint before the Federal Constitutional Court, arguing that the authorities granted by the G10 Act are overly permissive and thus unconstitutional.[185](#) The court's judgement made in May 2020 regarding the BNDs surveillance of domestic communication traffic involving foreigners has raised hopes for a successful ruling against the G10 Act,[186](#) The appeal against which was accepted for decision in Karlsruhe. At the end of coverage period no verdict had been reached.

Telecommunications interception by state authorities for criminal prosecutions is regulated by the code of criminal procedure and may only be employed for the prosecution of serious crimes for which specific evidence exists and when other, less intrusive investigative methods are likely to fail.

The 2008 Federal Constitutional Court ruling establishing a new fundamental right to the “confidentiality and integrity of information technology systems” also found that covert online searches are only permitted “if factual indications exist of a concrete danger” that threatens “the life, limb, and freedom of the individual” or “the basis or continued existence of the state or the basis of human existence.”[187](#) Based on this ruling, the federal parliament in 2009 passed a law authorizing the Federal Criminal Police (BKA) to conduct—with a warrant—covert online searches to prevent terrorist attacks.[188](#) The law also authorizes the BKA to employ other methods of covert data collection, including dragnet investigations, surveillance of private residences, and the installation of software on a suspect's computer that intercepts their communications at the source. Separately, antiterrorism legislation that was first passed after the terrorist attacks in New York City on September 11, 2001—which, among other provisions, obliges banks or telecommunications operators to disclose customer information to the authorities—was once again extended in 2015 through 2021.[189](#)

In June 2017, the federal parliament enacted the “law for more effective and more practical criminal proceedings.” Most significantly, it included an extensive list of criminal offenses that would allow for the deployment of surveillance software (spyware) on suspects' mobile phones, tablets, and computers in order to enable monitoring of written and spoken text as well as the copying of data.[190](#) Critics consider the law unconstitutional due to its expansive scope and long list of applicable offenses.[191](#) In accordance with the law, the BKA has been permitted to install monitoring software (the so-called *Bundestrojaner*, or “federal Trojan horse”) on suspects' devices since January 2018.[192](#) So far, three different types of Bundestrojaner have been developed.[193](#) BKA hackers have reportedly breached the encrypted messaging app Telegram and are targeting WhatsApp.[194](#) Complaints and lawsuits against the law and similar state laws have been filed at the Constitutional Court by data protection organizations and activists.[195](#)

In Bavaria, Germany's second-largest state by population, the governing Christian Socialist Union (CSU) introduced a bill at the beginning of 2018 that would grant the Bavarian police vastly expanded powers, including the authority to access any information technology system preventively in the event of a—broadly defined—imminent danger, without concrete evidence of a specific crime.<sup>196</sup> Critics allege that the bill would blur the line between police and intelligence services, a strict distinction that was built into the constitution as a consequence of abuses from the Nazi era.<sup>197</sup> Federal interior minister Horst Seehofer, the former minister and president of Bavaria and a member of the CSU, has stated that he intends to use the Bavarian law as a model for police laws in all German states.<sup>198</sup> Since then, similar laws granting police forces vastly expanded power to access communications have been passed in Sachsen, Nordrhein-Westfalen, Niedersachsen, Brandenburg, Hessen, Mecklenburg-Vorpommern, Rheinland-Pfalz, Sachsen-Anhalt, and Baden-Württemberg, while others are under discussion in Berlin and Schleswig-Holstein.<sup>199</sup> In some cases, these laws permit police to use Bundestrojaners.

The Bundestag approved a bill in December 2019 expanding the powers of the customs authorities to conduct communications surveillance, including through monitoring software and device searches.<sup>200</sup> The law also provides a legal basis to obtain user data from telecommunications providers without the knowledge of the persons concerned, and it permits customs authorities to use IMSI catchers, which mimic cell phone towers in order to collect data from all proximate devices.<sup>201</sup> The laws phrasing vaguely describes the circumstances justifying the application of spyware, providing only that customs authorities may use technical means to intervene in information technology systems if necessary. Federal Commissioner of Data Protection and Freedom of Information Ulrich Kelber criticized the almost unconditional and unprompted collection and enrichment of data.<sup>202</sup>

Newly arriving migrants and refugees are also targeted by measures that infringe on their privacy rights. According to 2017 amendments to the asylum law, an arriving refugee's electronic device data, including location data, may be copied and analyzed in order to determine the person's place of origin if he or she does not provide identity documents.<sup>203</sup> Although authorities originally gave assurances that these measures would be limited to exceptional cases, later statements revealed that because no such limitation is provided for in the text of the law, the Federal Office for Migration and Refugees intends to implement the measures as standard practice.<sup>204</sup>

C6 1.00-6.00 pts0-6 pts

Are service providers and other technology companies required to aid the government in monitoring the communications of their users?	4.004 6.006
--	----------------

The German government established a legal framework to protect personal data in 1990, though several laws require companies to provide user data to the authorities. German law requires the localization of some telecommunications data.<sup>205</sup>

In June 2020, after the coverage period, the Bundestag approved an amendment to NetzDG that requires companies report the personal data of users who post certain types of illegal content, including far-right nationalist and extremist content, to the Federal Criminal Office (BKA). Introduced in February 2020, the amendment requires the reporting of

personal data, including usernames, IP addresses, port numbers and—with a judicial order—passwords.<sup>206</sup> Digital rights associations have criticized that the expected masses of user data, which will flow to the BKA, can hardly be processed by the public prosecutor’s offices.<sup>207</sup>

Despite a 2014 CJEU decision that struck down the EU Data Retention Directive,<sup>208</sup> the federal parliament enacted a law on data retention in 2015.<sup>209</sup> Both the parliamentary opposition and data protection officials had fiercely objected to the legislative proposal, maintaining that it contradicted civil laws and violated the guidelines established by the CJEU. Under the new law, different sets of data have to be stored on servers located within Germany for 10 weeks, while providers have to retain the numbers, as well as the dates and times, of phone calls and text messages. ISPs are also required to retain the internet protocol (IP) addresses of all users, as well as the dates and times of connections. The location data of mobile phone connections must be saved for four weeks. The requirements exclude sites accessed, email traffic metadata, and the content of communications.

Several constitutional complaints against the data retention legislation have been filed and are pending at the Federal Constitutional Court.<sup>210</sup> In February 2017, the federal parliament’s own research service concluded that the law does not conform to the guidelines set by the CJEU in its 2014 ruling and is thus contrary to EU law.<sup>211</sup> After the internet provider Spacenet filed a lawsuit against its obligation to start storing its customers’ data, the Higher Administrative Court of Nordrhein–Westfalen, which has jurisdiction over this question, likewise decided in June 2017 that the German legislation contradicts EU law and is thus not applicable to Spacenet’s conduct.<sup>212</sup> Since then, the application of the law has de facto been suspended; ISPs never stored any data based on the retention legislation. In November 2019, the BNetzA disclosed that many providers store extensive customer data for multiple months and share them with authorities if requested.<sup>213</sup>

A December 2019 law establishes a legal basis for customs authorities to obtain user data from telecommunications providers without the knowledge of the persons concerned (see C5).<sup>214</sup> The amended Telecommunications Act of 2013 regulates “stored data inquiry” requirements.<sup>215</sup> Under this law, approximately 250 registered public agencies, among them the police and customs authorities, are authorized to request from ISPs both contractual user data and sensitive data. While the 2004 version of the law allowed the disclosure of sensitive user data only for investigations of criminal offenses, the amended act extended it to cases of misdemeanors or administrative offenses. In addition, whereas the disclosure of sensitive data and dynamic IP addresses normally requires an order from the competent court, contractual user data (such as the user’s name, address, telephone number, and date of birth) can be obtained through automated processes. Moreover, several studies have shown that judicial review does not actually take place in a majority of instances when it is required.<sup>216</sup>

C7 1.00-5.00 pts-5 pts

Are individuals subject to extralegal intimidation or physical violence by state authorities or any other actor in retribution for their online activities?	4.004 5.005
---	----------------

There were very few reported cases of direct physical intimidation or violence against online journalists or other ICT

users in retaliation for their activities during the coverage period.

In October 2019, law enforcement shut down Germany’s biggest filesharing platform Share-Online.biz and seized its website and servers. After police raided their offices and their employees’ apartments, the operators were charged with commercial unauthorized use of copyright protected works.[217](#)

In June 2018, police raided the offices of the Zwiebelfreunde, an activist association promoting online anonymity tools—an action a court later ruled to be illegal. Additionally, the homes of its board members in Augsburg, Berlin, Dresden, and Jena were searched, in order to obtain material relevant to criminal proceedings against unknown suspects accused of inciting illegal activities at a political rally in Augsburg. For communication, the suspects used the confidential email provider Riseup, for which Zwiebelfreunde collected donations.[218](#) The implicit assumption of the investigators was that Zwiebelfreunde had information on the identity of the suspects, because the group supported Riseup. Despite the group being “witnesses” in this case, police seized documents containing names, addresses, and bank details of people supporting Riseup and Zwiebelfreunde. Police allegedly made threats to people from Zwiebelfreunde present at the raid, intimating that they might become suspects.[219](#) Following criticism by press freedom and internet rights activists, the State Court in Munich ruled the searches and seizures were illegal and ordered all seized material to be returned.[220](#)

A June 2019 study on hate speech reported that immigrants, Muslim people, women and LGBT+ people are predominantly targeted by harassment online. Men reported experiencing online harassment more frequently than women, which might stem from different online behavior.[221](#) When it comes to cases of online discrimination of LGBT+ people, Germany ranks relatively low in comparison to other European Countries.[222](#)

C8 1.00-3.00 pts-3 pts

Are websites, governmental and private entities, service providers, or individual users subject to widespread hacking and other forms of cyberattack?	2.002 3.003
---	----------------

Human rights activists and NGOs are rarely victims of cyberattacks or other forms of technical violence that are aimed at stifling freedom of expression. However, government institutions and the business sector have been targeted by cyberattacks.[223](#)

The Federal Office for Information Security (BSI) reported in 2019 that ransomware, spam, and bot networks remain a constant threat and are becoming more efficient in design. Between June 2018 and May 2019, roughly 770,000 emails containing malware were intercepted in German administrative networks.[224](#) During the coverage period, information security experts repeatedly raised concerns to the government regarding the shortage of security specialists and inadequate policy and regulatory infrastructure.[225](#)

In December 2018, the personal data of parliamentarians, politicians, television personalities, activists, and YouTube artists were published online.[226](#) An individual who confessed to the leaks, a German citizen, was arrested shortly

after the case received public attention in January 2019.<sup>[227](#)</sup> The case led to public discussions about online safety, since much of the retrieved data was protected by weak passwords such as “1234.”<sup>[228](#)</sup>

Earlier, in 2015, the federal parliament had enacted an ICT security law to strengthen its response capabilities; the law obliged telecommunications companies and critical infrastructure operators to report security breaches to the BSI. However, the law has been criticized as being largely ineffective, and its mandates concerning the storage of traffic data to determine the source of possible cyberattacks have been criticized as intrusive.<sup>[229](#)</sup>