

List of issues for the consideration of Germany's periodic report under the International Covenant on Civil and Political Rights (ICCPR)

- Contribution by Reporters Without Borders (RSF)



1. Short description of the submitting organization

Founded in 1985, **Reporters Without Borders**, also known internationally under its French name Reporters sans frontières (RSF), strives for a world in which all people are able to access reliable information enabling them to fully understand current global challenges and to form their own opinion. RSF promotes freedom, pluralism and independence of journalism, in particular by supporting and defending those who embody these ideals.

Its worldwide presence through its vast international network (an international secretariat based in Paris, eleven sections and regional offices as well as correspondents in more than 130 countries) gives RSF the ability to mobilize support, challenge governments and wield influence both on the ground and in the ministries and precincts where media and Internet standards and legislation are drafted.

RSF benefits from a consultative status with the United Nations, UNESCO, the Council of Europe, the International Organization of La Francophonie (OIF) and the African Commission on Human and Peoples' Rights (ACHPR). At the intersection of journalism, human rights and development, RSF's efficiency and audacity, coupled with a sometimes combative tone makes it an original international NGO.

2. Reference to ICCPR articles being discussed

- □ Article 17
- □ Article 19

3. Summary of the human rights issue discussed

This overview covers the period from early January 2019 to late March 2020.

- Hostilities, threats and violence against journalists
- □ Hate crimes and the media draft laws and reactions
- D Pre-emptive legal strategies hindering investigative reporting



- Outlook: Declining diversity in the daily newspaper industry; AfD gaining influence in the public broadcasting system
- □ Corona crisis presents media with a whole new set of challenges

3.1 Hostilities, threats and violence against journalists

In 2019, the **number of physical attacks on journalists dropped to 13 compared with 22 in the previous year, but this is no reason for complacency**. Almost half of the cases recorded in 2018 occurred on the fringes of protests by right-wing populist groups in Chemnitz between late August and early September. Far-right demonstrations and events also took place in 2019, but on a smaller scale than in 2018. Nearly half of the 13 attacks verified by RSF were against the homes or cars of media professionals, a slight increase on the previous year.

RSF also registered many **alarming examples of verbal abuse and attempted intimidation** of journalists. These are not included in the figures although they are internally documented. Of particular concern here are the online hate campaigns in which victims are often left to deal with the situation on their own and legal prosecution tends to lead nowhere.

The situation is similar as regards the "**lists of enemies**" circulating in the far-right milieu that disclose the full names and addresses of numerous journalists. Legal proceedings against the lists proved largely ineffective (<u>https://ogy.de/a9as</u>). Hasnain Kazim, an author and freelance journalist for the German weekly *Die Zeit*, has been on the receiving end of death threats for many years, but in early 2020 he was getting several a day. Even though his name is on death lists and he has reported the threats to the police, this has failed to produce results (<u>https://ogy.de/cnxm</u>).

2019 also saw **numerous cases of police obstructing media coverage,** in particular in the context of demonstrations and events staged by far-right groups and parties as well as counter-demonstrations. RSF welcomes the fact that in 2019 the police in Saxony and other federal states undertook a transparent analysis of their mistakes and stepped up efforts to address the issue of media rights and freedom of the press in both basic and advanced police training programmes. The measure comes in response to a longstanding demand by RSF that a special focus be placed on media rights and interactions with media professionals and that measures be taken to ensure that police officers put what they learn into practice.

The German Press Council, the self-monitoring organ of the press run jointly by journalist unions and publishers' associations, has also announced that it will revise the **"Code of**



Conduct for the Press/Broadcasters and Police", which was drawn up in 1993 with the aim of preventing the obstruction of police work and media coverage. The Press Council explained that a revision was warranted because the codes of conduct were formulated in response to the Gladbeck hostage crisis and the school shooting in Winnenden, but were never updated. The problems are different today, for example as a result of social media, the Press Council said.

3.2 Hate crimes and the media

A high volume of online intimidation and abuse continued throughout 2019. In November 2019, the fact-checking editorial team of the research platform *CORRECTIV* reported that it had been bombarded with intimidation attempts and threats from the far-right. (<u>https://ogy.de/7eiu</u>).

Mass campaigns of threats, abuse and intimidation, primarily on social media, are nothing new. But journalists affected are increasingly voicing criticism of their employers. This has been particularly noticeable among public broadcasters.

In that context, RSF welcomes in principle the federal government's plans to amend the Network Enforcement Act (NetzDG) to make it easier to investigate online hate crimes (see also Chapter 4). At the same time RSF warns that obligations to notify law enforcement agencies and the intelligence services in particular should not be carried too far, in particular as regards the obligation of social media providers and platform operators to hand over passwords.

3.3 Freedom of Information Act (IFG)

The Freedom of Information Act, which came into force on January 1, 2006, has brought significant progress compared to the old legal situation and is therefore to be welcomed. In principle, all documents of public bodies should now be accessible without personal affections or even without provide a reason for the application. In practice, however, the IFG inquiries do not promise quick information. The IFG only affects federal authorities. Authorities often exceed their legally prescribed response period of one month, demand information fees of up to 500 euros or block access to documents. This is not only due to the authorities, but also to the law: If documents contain business and trade secrets, for example, the authorities are not allowed to disclose anything. The German states of Bavaria, Saxony and Lower Saxony do not even have an IFG and can therefore fend off all such requests. (https://ogy.de/8ar5)

So far, thirteen federal states have each passed their own freedom of information laws for their area of responsibility. (<u>https://ogy.de/4uyr</u>) Special laws such as the Environmental and Consumer Information Act (UIG and VIG) also oblige federal states without an IFG to publish information on environmental and consumer issues.

Only oral and simple written information (including a few copies) is free of charge. Otherwise, fees for the workload of the authority and material expenses (e.g. for copies 0.10 Euro per DIN A4 page) can be charged. Depending on the duration of the inspection of files at the Office and the amount of preparation work required by the authority, the fee may range from 15 to 500 Euro. **Details of the fee schedule has turned out to be deterrent and not very citizen-friendly.**

In November 2019, the research platform *Correctiv* won a landmark ruling before the Gelsenkirchen Administrative Court on the prohibition of excessive fees for information provided by authorities under the Freedom of Information Act (IFG). Correctiv had filed a complaint in North Rhine-Westphalia (NRW) after both the NRW Health Ministry and the district government of Munster presented it with a bill of 500 euros for documents provided in connection with the platform's research into adulterated cancer medications (<u>https://ogy.de/pmg6)</u>. The court said in its decision that the fees were so high that they could deter citizens and journalists from seeking information from the authorities. This contradicts a 2017 court decision that was also handed down in a case brought by *Correctiv* (<u>https://ogy.de/0s3s</u>).

3.4 Pre-emptive legal strategies hindering investigative reporting

The trend towards the use of pre-emptive strategies devised by law firms and aimed at fending off unwanted investigative research and intimidating journalists continued in 2019. For the first time companies are also trying to sue media outlets for substantial damages. Of particular concern here is that freelance journalists who do not have the clear "backing" of a client or employer may be exposed to considerable risks, above all in the initial phase of their research when their work has not yet been commissioned by a specific media outlet. It is hard to determine how many stories go unreported or are abandoned due to this trend. In view of the increasingly difficult financial situation in the newspaper sector and above all in the local and regional newspaper segment, the latter in particular are reportedly less and less willing to support potentially controversial investigative reporting that could incur high legal costs.

Companies and state authorities such as ministries hardly ever provide transparency on their use of external law firms for public relations and for consulting on legal matters related to the press. Two rulings handed down last year now offer hope, at least as regards state institutions. The Administrative Court of Cologne ruled in July 2019 that the Federal Office for the Protection of the Constitution (BfV) must disclose all legal costs incurred in connection with press-related legal consultations from 2014 to 2018 (<u>https://ogy.de/5v20)</u>.

In October 2019, it emerged that federal ministries were paying big law firms fees of between 250 and 380 euros per hour to fend off questions and research by the media. According to the

results of a small inquiry ("Kleine Anfrage") submitted by the parliamentary group of The Left party, the Federal Office for the Protection of the Constitution was at the top of the list, having paid 74,147.91 euros in legal fees for such services from 2013 to 2018, followed by the Institute for Federal Real Estate with 48,990.34 euros. The Federal Ministry of Transport and Digital Infrastructure came third. It spent 34,931 euros on these services in that period (<u>https://ogy.de/dsgo).</u>

According to a study published by the *Society for Civil Rights (GFF)* and the trade union-run Otto Brenner Foundation in the summer of 2019 on "Pre-emptive legal strategies against media" (<u>https://ogy.de/r4up</u>), the ministries have not had much success in this endeavour, at least not against media that engage in investigative reporting on a regular basis. However, the study called attention to the fact that also in the area of public broadcasting **by no means all broadcasters are willing to assume the liability risks of external authors and producers** when they commission documentaries and reports. It also said that media outlets were more willing than in the past to submit to cease-and-desist declarations.

3.5 Gradual loss of diversity among newspapers and attacks on public broadcasters

The press

As in previous years, media diversity continues to decline, especially at the regional and local level. The closure at the end of March 2019 of the German edition of *Huffington Post*, which was launched in a collaboration with publisher *BurdaForward* in 2013, illustrates the fact that even new digital enterprises cannot guarantee sustainable improvement (<u>https://ogy.de/arik)</u>.

The **Cologne-based** *DuMont* **media group**, one of Germany's oldest and largest publishers, **announced its withdrawal from the newspaper industry** in 2019 and put all its titles (including the *Kölner Stadt-Anzeiger* and the *Berliner Zeitung*) up for sale. With the exception of the Cologne-based newspapers all have now been sold on to new owners (Current as of April 2020). A silver lining is that so far none of the papers have been closed down.

The number of takeovers and closures in the German newspaper industry has gone down in comparison to previous years, even though individual publishers like the *Funke* media group implemented major cost-cutting rounds (<u>https://ogy.de/9ehd)</u>.

Public broadcasting

The debate about the legitimacy of Germany's public broadcasters in the digital world and their future structure and financing continued in 2019. An agreement reached by the Ministerial Conference of the Federal States in March 2020 according to which broadcasting licence fees will increase to 18.36 euros per month as of 2021 has at least provided some security on the

last point. The nominal increase has yet to be approved by all 16 German state parliaments (<u>https://ogy.de/faaj)</u>.

Because the federal states have not yet been able to agree on the structural reform of the public broadcasting system, which was originally scheduled for 2017, there is also considerable uncertainty in this respect. Moreover, the three public broadcasters *ARD*, *ZDF* and *Deutschlandradio* have so far failed to score many points in the rather sluggish public debate about their continued relevance in the digital world. According to **media policy experts the broadcasters' restructuring efforts remain inadequate** (<u>https://ogy.de/mt1y)</u>.

In addition, the public broadcasters are the main target of the AfD's destabilisation campaign against what it calls the "system media". Most of Germany's public broadcasting institutions have failed to come up with convincing answers, either in their response to the AfD and its representatives in their programmes or within their own internal structures. **Two-thirds of the public broadcasting institutions now have representatives of the AfD** on their supervisory boards. This number will increase in 2020 and the subsequent years. This could provide the AfD with far more effective means to undermine the system from within, or at least limit its self-administrative capacity and cause long-term damage through complicated inquiries and obstructive tactics.

3.6 The corona crisis and its already visible impact

The coronavirus crisis has put many media, including Germany's, in a paradoxical situation. User statistics are soaring, with established media brands benefiting most from this trend. But at the same time journalism at all levels is facing unprecedented challenges. The authorities have not (as of September 2020) imposed official restrictions on the work of representatives of the media, but the massive restrictions on basic rights in Germany impact the work of journalists. Bans on social contact and de facto curfews hamper interviews, research, and filming on location. Most press conferences are held online. Demands for the use of mobile phone location data are fuelling concerns about new forms of data gathering and surveillance that could endanger the confidentiality of journalists' sources (<u>https://ogy.de/co1n</u>). In particular, the disparities in the regulations of Germany's 16 federal states – which are responsible for both the regulations aimed at fighting the virus and those that apply for the media – are proving problematic (https://ogy.de/rg2n). As "key workers", the staff of newspapers, radio and television broadcasters and other media enjoy special rights such as being exempt from curfews or travel restrictions. At the same time, all media companies are implementing safety measures for their employees. Many media products and services are being produced by staff working from home while editorial, technical or printing tasks that require the physical presence of staff are carried out by teams that are kept separate from each other in order to minimise the risk of infection.



But at the same time the advertising revenues of commercial media are plunging. Private TV channels are being watched by record numbers of younger viewers, but they have warned via their association, VAUNET, that in some cases they are facing losses of revenues that "pose an existential threat" (<u>https://ogy.de/t4vr).</u>

Newspapers are also grappling with cancelled advertising and lost revenues for both print and online editions. Some companies have already announced short-time work for employees. Freelance journalists are the worst hit at present. Some have literally been left with nothing.

In the area of data protection and privacy protection, the **lacking transparency of video conferencing apps** such as "Zoom", which have become hugely popular as a result of social distancing measures, and plans to introduce **smartphone-based coronavirus tracking apps are a cause for concern**. There have been reports that Zoom does not provide adequate protection against cyberattacks. This prompted New York Attorney General Letitia James to launch an investigation into Zoom's privacy practices in March 2020 (<u>https://ogy.de/pey0)</u>.

From the perspective of press freedom, the plans for coronavirus tracking apps raise the **question of whether such apps can guarantee the anonymity and protection of journalists' sources.** RSF has formulated a **list of minimum requirements** to address this issue (<u>https://ogy.de/98vp</u>). After initially criticizing proposals by the Minister of Health, such as the collection of location data, the German app project has regained trust through a transparent development process and the choice of a decentralized approach. The long public debate about the conditions of using such a technology seems to have paid off. Nevertheless, even shortly before the launch of the app, security questions still arose: Due to a lack of technical equipment, many laboratories will not be able to transmit and confirm test results within the app. Instead, users will have to confirm their test results via a hotline to inform their contacts about their illness via the app. The integration of "external service providers" creates an additional target for abuse and the possible de-anonymization of callers. The permanent activation of the Bluetooth function also increases the risk of digital attacks. In recent years, security gaps in connection with the technology have repeatedly had to be closed. (<u>https://ogy.de/vgst</u>)

4. Description of the legal framework and practices by State authorities

In 2019, numerous draft laws were set in motion, which, if signed into law, could enforce mass surveillance and criminalize commonly used encryption and anonymization tools. These draft laws are not specifically directed against the work of the media yet their implementation would undermine the protection of journalistic sources.

The potential criminalization of Tor anonymization technology would also have a severe impact on the work of independent media and journalists in countries and regions without press freedom. Plans to tighten the corresponding articles in Germany's Criminal Code have been put on hold for the time being due to resistance from the Social Democratic Party (SPD).

4.1 Law against right-wing extremism and hate crimes

Despite widespread criticism, in February 2020 the Federal Cabinet presented **a draft law extending the obligation of Internet companies to pass on user data and report criminal content to the Federal Criminal Police Office (BKA)** (<u>https://ogy.de/0w80</u>). This extension of the Network Enforcement Act (NetzDG), which has been in force since 2017, also foresees changes to Germany's Telemedia Act (TMG), Penal Code (StGB) and Criminal Procedure Code (StPO), as well as the BKA Act and the Federal Registration Act.

A particularly controversial provision of the proposed legislation obliges social media providers and platform operators to hand over passwords and other sensitive user data to law enforcement agencies under certain circumstances. In the latest version of the draft law, the criteria for enforcing this provision are considerably more restrictive than in earlier versions. Telecommunications providers must store and pass on the passwords in encrypted form. In addition, the obligation to hand over passwords is limited to investigations into particularly serious crimes and cases in which public security or public order is at stake (<u>https://ogy.de/x684)</u>. Concerns regarding the appropriate protection of users' data do however remain.

According to the draft law, network operators must report any posts that draw complaints from users for containing illegal threats of violence, neo-Nazi propaganda, hate speech or similar content to the Federal Criminal Police Office (BKA). The current legislation only requires that such content should be blocked for users in Germany. The proposed law would also require companies to pass on the IP addresses and port numbers of the authors to the BKA. Proposals for an alternative "quick freeze" procedure, e.g. from the Federal Commissioner for Data Protection and Freedom of Information, which would add safeguards against unnecessary and unfounded data collection by police authorities, were disregarded (<u>https://ogy.de/mx3b</u>).

To what extent these measures will prove helpful in combating the type of online threats and hate speech described above remains to be seen. The lack of means to enforce justified demands poses a major problem, given that Germany's judicial system already suffers from a shortage of specialized prosecutors and judges, a challenge that is likely to be worsened by the amendment, if it is not accompanied by substantial additional resources. The tightened provisions would not apply to normal insults, slander or libel. In such cases, it will continue to be left to those affected to report such incidents.

In a special session held on 27 March 2020, the Bundesrat (the upper house of Germany's parliament which represents Germany's 16 federal states) called for amendments to be made to the draft law. The federal states fear excessive costs for the justice system and have also voiced concerns regarding data protection (<u>https://ogy.de/gid8)</u>.

4.2 BND constitutional complaint

In mid-January 2020, the Federal Constitutional Court held oral hearings in respect of a constitutional complaint brought by RSF Germany, the Society for Civil Rights and four other media organisations regarding the online surveillance measures of the BND (Bundesnachrichtendienst), Germany's foreign intelligence agency. In the context of its communications intelligence activities, the BND scans data streams in networks outside Germany – without judicial supervision and without concrete suspicion. It uses "selectors", or defined search parameters, to constantly and automatically monitor the internet on the basis of search terms. The BND also passes on the results to foreign partner services upon request.

The case dealt with the **question of whether the 2016 Act on the Federal Intelligence Service and the global mass surveillance of online data traffic by the BND, which the law allows for are compatible with Germany's constitution** (<u>https://ogy.de/f34s)</u>. The question of whether German authorities are obliged to respect the basic rights enshrined in the German constitution also when dealing with non-German media representatives working outside Germany is of key importance to the case.

In May, the court ruled that the BND law disregards both the freedom of the press guaranteed in article 5 and the freedom of telecommunications guaranteed in Article 10 of the Basic Law as it does not recognise that foreign surveillance must be conducted in conformity with the Basic Law. When revising the BND law, the legislature will have to take into account that foreign surveillance without cause is only possible under specific and limited circumstances. Vulnerable groups of persons such as journalists must be granted special protection. Tighter criteria must also apply to the targeted surveillance of individuals. Furthermore, international surveillance must be controlled much more effectively by independent bodies with their own budgetary sovereignty. The ruling thus sets new standards in international human rights protection and for freedom of the press.

The Constitutional Court in its ruling (<u>https://ogy.de/qipw</u>) referred several times to the Letter of the Special Rapporteurs (United Nations Office of the High Commissioner for Human Rights, 29 August 2016, OL DEU 2/2016, <u>https://ogy.de/8kio</u>):

- Paragraph 240: Where the [data] transfer relates to data of journalists, lawyers or other professional groups recognized as subject to confidentiality protection, an independent weighing of interests is required, which differs from the weighing of interests relating solely to the domestic use of such data. The transfer must be subject to a court-like prior check. (referring to OL DEU 2/2016, p.7)
- Paragraph 305: Surveillance under Section 6 of the Federal Intelligence Service Act is not limited to weighty, differentiated purposes. The broadly and openly formulated purposes, which are not intended to restrict the range of tasks in any way, even after the explanatory memorandum to the draft law, clearly fail to meet this requirement. (referring to OL DEU 2/2016, p.5)
- Paragraph 325: The provisions are also incompatible with the Constitution as far as they authorize surveillance measures against journalists and thus constitute interference with Article 5 (1) sentence 2 of the Basic Law, since they do not take adequate account of the specific protection needs of independent foreign journalists. (OL DEU 2/2016, p.5f)

4.3 Act on Harmonising the Protection of the Constitution

In May 2019, RSF Germany warned about legislation drawn up by the Ministry of the Interior, which would allow German intelligence services to spy digitally on media inside and outside Germany. A ministerial draft bill foresees an "Act on Harmonising the Protection of the Constitution" (Gesetz zur Harmonisierung des Verfassungsschutzrechts) that would give Germany's domestic and foreign intelligence agencies powers to hack into the servers, computers and smartphones of publishers and broadcasters as well as the accounts of freelance journalists. The agencies would be permitted to use state-sponsored intrusion software, known as "Staatstrojaner", to intercept ongoing communications. So-called source telecommunication surveillance (Quellen-TKÜ) would enable the secret services to monitor ongoing communication, including encrypted communication, insofar as the state's interest in information is given priority over interference with freedom of the press in the context of a proportionality test.

Faced with widespread criticism, the German Minister of the Interior Horst Seehofer (of the Christian Social Union - CSU) insisted that the bill was not directed against the media and that journalists would continue to enjoy "special" protection under the proposed intelligence service

legislation (<u>https://ogy.de/h0qg</u>). As the Social Democratic Party (SPD) has voiced major doubts about the measures the draft law has been put on hold for the time being (<u>https://ogy.de/4pc3</u>).

Recently, **criticism has also come from the ranks of the telecommunications providers**, who according to the draft law are to be obliged to redirect data streams in order to enable the intelligence services to install surveillance software, for example via fake software updates. In any case, government hacking requires that the authorities deliberately keep security gaps open. This would undermine the trust of all people in the integrity of the technology, according to statements by associations and members of parliament from the network policy community. The consequence of this policy would be a general loss of IT security.

4.4 IT Security Act

In spring 2019, Interior Minister Horst Seehofer was planning to introduce legislation that would oblige messenger services such as WhatsApp and Telegram to store the communications of their customers and pass them on to authorities in readable form, i.e. unencrypted, when presented with a court order to this effect (<u>https://ogy.de/vla8)</u>.

Moreover, both the federal states and the Ministry of the Interior plan to comply with the intelligence services' demands for measures to prevent the phenomenon of "going dark", i.e. the transfer of communications and data exchange to encrypted services on the deep web. To this end, new provisions are to be introduced to Germany's criminal law. Under a bill presented by the Bundesrat in spring 2019, a new section 126a of the Criminal Code is to facilitate the investigation of crimes on the deep web (<u>https://ogy.de/0af8</u>). This planned crackdown on crime on the deep web would in practice criminalize all anonymization. According to the draft, even running a Tor node could be classified as a potentially criminal offence because the anonymization procedures could also be used by criminals (<u>https://ogy.de/22qq</u>).

The criminalisation of Tor servers could spell the end of anonymization services, which are often used by exile media outlets and journalists to obtain sensitive information from crisis areas and war zones. The legislation could also be used against whistleblowing platforms like *Wikileaks*. These were the conclusions of an interdisciplinary analysis of the so-called "Darknet paragraph" by legal experts, IT specialists and human rights activists (<u>https://ogy.de/m8t2</u>).

In May 2020, Minister of the Interior Seehofer had submitted a new draft to the departmental vote. The **IT Security Act 2.0 is to massively upgrade the Federal Office for Information Security**: more competencies, more money, more personnel. **Some problematic points have been deleted in the new draft law,** including criminalization of the dark net and an obligation to disclose passwords. The SPD-led Ministry of Justice did not want to support these changes for formal reasons and has pushed through their deletion. However, this might only be temporary;



all of these demands are still on the table and are likely to come back when the criminal law is next amended. (<u>https://ogy.de/5di1</u>)

5. Recommendations

- RSF supports the goal of the Federal Government to more effectively pursue hate crime on the Internet and to better protect those affected. Threats of violence and intimidation of journalists online pose a considerable threat to press freedom both in Germany and internationally. Yet, we take a critical view of the fact that the Government now wants to introduce additional regulatory measures with two new draft laws without having conclusively examined the effect of the Network Implementation Act (NetzDG), which came into force in 2017. Although we welcome certain improvements, including the introduction of rights of objection and expanded requirements for transparency reports by information intermediaries, RSF sees a clear need for improvement of the draft bill to combat right-wing extremism and hate crime, with regard to the protection of sensitive data of media workers and their sources.
 - Existing legal possibilities for prosecution in the area of hate crime should be exhausted.
 - Data protection should be taken seriously, especially regarding persons subject to professional confidentiality such as journalists. We therefore support the proposal of the Federal Commissioner for Data Protection and Freedom of Information for a multi-stage reporting procedure, which provides for a preliminary examination of anonymized reported content and only in the second step the request for a "QuickFreeze" procedure for secure data worthy of protection.
 - We emphasize the necessity of explicitly **recognizing journalists as a professional group worthy of protection**. Consequently, journalists would not need to individually prove current threat situations and should be able to obtain a ban on their information in accordance with Section 51 of the Federal Registration Act.
 - Even if regulatory measures of the German government have a certain objective, their international impact is a side effect that must be considered in the legislative process. We therefore reiterate our recommendation that **national standards should be linked to international human rights requirements** and that



international standards for human rights-compliant regulation of information intermediaries be drawn up.

- RSF calls on the Federal Government to enshrine the comprehensive protection of confidential communications of journalists from intelligence surveillance in the new BND law.
 - The court decision leaves room for maneuver in terms of redefining the concept of journalism, since there is no internationally valid definition. In view of the wide range of forms of journalistic work and in view of the often politically motivated restrictions on access to the journalistic profession, RSF pleads for an understanding that is oriented towards criteria of independent journalistic work and not towards membership of an established medium. Specifically, the paper proposes an orientation towards the European norm standard of the **Journalism Trust Initiative** co-initiated by RSF, which aims to certify trustworthy media and their easier identification through algorithms.
- Effective control over intelligence services is becoming increasingly important. The federal government now has no way around the expansion of "independent objective-legal" control demanded by the ruling on the BND law. Beyond the legal scrutiny behind closed doors, measures such as increased spot checks, the possible involvement of experts from the journalistic field, possibilities for disclosing grievances and stronger parliamentary control are needed to regain lost public trust.
- With the **draft bill to amend the "Act on Harmonising the Protection of the Constitution"**, the federal government is massively damaging the confidence of informants in the confidentiality of their communications with the media. Intelligence services will be granted ever new powers to spy on media professionals solely on the basis of their access to information of interest to the security authorities.
 - RSF calls on the federal government to put journalists on an equal footing with other professional secrecy groups and to exempt them from the same authority as lawyers.
 - The federal government must adapt intelligence control to the digital possibilities and resources of the services.
 - RSF also calls for improvements in the information and transparency obligations of the services and the correction of incorrect entries on media workers in the databases are not forthcoming. For example, an investigation into the

background to withdrawn accreditations at the G7 summit in Hamburg had shown that these were partly due to gross mistakes by the authorities.

- Even though the introduction of the **Freedom of Information Act** in 2006 was revisionist, a series of weaknesses in the law and discouraging legal practice have so far prevented promises of state transparency from being fulfilled.
 - Effective Freedom of Information Acts or transparency laws should be introduced in all federal states.
 - A consistent implementation of the idea of freedom of information would mean an abolition of fees. Internationally an exception anyway, charging fees for IFG inquiries not only means additional effort for the administration, but also keeps people from making inquiries at all.
 - Exceptions for secret services, chambers of industry and commerce, federal and state audit offices, courts and universities are anchored in many information laws, but they contradict the idea of freedom of information. They should be revised.
- It is crucial for the protection of the freedom of the press that **police staff have up-to-date knowledge of journalists' rights**.
 - RSF welcomes the fact that in 2019 the police in Saxony and other federal states undertook a transparent analysis of their mistakes and stepped up efforts to address the issue of media rights and freedom of the press in both basic and advanced police training programmes.
 - A systematic educational process on media law and related topics is essential and therefore should be mandatory for the police forces in all federal states.

6. NGO should specify in case they would like their contribution to be confidential and not be made public by the Committee

RSF wishes this contribution to be made public.