Statement

on the Federal Chancellery's Draft Bill to Amend the Federal Intelligence Service Act (BND-Gesetz)

Recommendations for revising the Federal Intelligence Service Act to ensure that it is in conformity with fundamental rights and safeguards press freedom

Berlin, December 2020

With this position paper, Reporters Without Borders (RSF) Germany presents proposals for a revised version of the statutory basis that governs the strategic surveillance of foreign telecommunications by the Federal Intelligence Service (*Bundesnachrichtendienst*, BND).

In view of the German Federal Constitutional Court's ruling in favour of the constitutional complaint brought by RSF as well as seven media workers and other persons working in professions that enjoy special confidentiality protection, we examine to what extent the draft bill meets the requirement to strengthen protective rights for journalists (*journalistische Schutzrechte*), i.e. their right to special protection against surveillance and to confidentiality of communications. To this end, we focus in particular on the provisions concerning the protection of confidential relationships of trust (*Vertraulichkeitsbeziehungen*), such as relationships between journalists and their sources, or lawyers and their clients, the new statutory provisions concerning unauthorised intrusions into IT systems, the handling of traffic data (metadata), and cooperation with other intelligence services, as well as amendments to the oversight of intelligence services that are relevant to protective rights for journalists.

Contents

1 Summary

The aim of the constitutional complaint against the amended Federal Intelligence Service Act (*Gesetz über den Bundesnachrichtendienst*—BNDG) which came into force in 2017 was to ensure that the statutory basis for the surveillance activities of the intelligence services and the oversight thereof are designed in conformity with fundamental and human rights. The May 2020 judgment of the Federal Constitutional Court confirmed the need for a revision of the statutory basis for the strategic surveillance of foreign telecommunications (where all communicating parties are located outside Germany, *Ausland-Ausland-Fernmeldeaufklärung*) by the BND. The court ruled that the German state authority is also bound by the fundamental rights of the German Constitution, the Basic Law, when conducting surveillance of non-Germans in other countries, and must respect their press freedom rights and privacy of telecommunications.

The draft bill's fundamental recognition of the need to protect confidential communications between foreign journalists and other persons working in professions that enjoy special confidentiality protection and third parties is an important step in the right direction. In the digital age, freedom of the press requires that special confidentiality rights for journalists be strengthened in line with the expanding technical capabilities of intelligence services and other state surveillance. By formalising the protection of the confidential relationships of trust of non-German persons outside Germany, the draft sends a signal that transcends the scope of German legislation regarding future developments in the areas of protection from surveillance and the handling of internationally processed data. In a best-case scenario, this could even serve to enhance respect for the rights of German citizens and persons in professions that enjoy special confidentiality protection, whose data is inevitably analysed by non-German intelligence services.

However, if we look at the draft law as a whole, a sobering picture emerges: the focus is not on placing democratic limitations on the mass surveillance of digital communication, but rather on legalising the continuation of this practice to the greatest possible extent. The draft law formally recognises protective rights, only to undermine these very same rights through far-reaching restrictions, discretionary powers of authorities subject to little or no oversight, and the legitimisation of far-reaching and highly intrusive powers. In particular, the retention of the BND's powers to collect traffic data, for example the connection data for communications between journalists or between journalists and their sources, sends a disastrous message. The resulting continued relativization and even erosion of special confidentiality rights for journalists compromises the relationship of trust between journalists and their sources all over the world and damages other efforts to strengthen press freedom.

RSF Germany therefore urgently recommends that the protection of confidential communications be given higher priority in the draft bill, and that encroachments on the special confidentiality rights of journalists be subject to more clearly defined restrictions. In addition to clear provisions regarding the situations in which exceptions to the general ban on the surveillance of confidential relationships may apply, oversight mechanisms can ensure that surveillance practices comply with constitutional law. Consequently, effective oversight mechanisms must be created for all procedures related to such surveillance, from the classification of confidential relationships of trust to decisions regarding the surveillance of media workers and the lawful handling of collected data.

2 RSF’s recommendations for revising the draft bill

1. The protection of confidential relationships of trust must extend to **all information and data, including traffic data** and must not be limited to a ban on the targeted collection of "personal data".

2. The **dangers** set out in Section 21(2) that justify encroachments on the special protective rights of journalists in specific situations must be **clearly defined** and **limited** to situations that pose a genuine threat to the state.

3. The BND's classification **of confidential relationships of trust** must be subject to **documentation requirements** as well as ex-ante review by an **independent oversight body**.

4. **Balancing decisions** in which security interests are weighed against the protection of confidential relationships must be subject to effective **end-to-end oversight**. If the Oversight Council is to make an informed judgment about the legality of surveillance operations, it must have access to all the relevant data, in particular the search terms that guide the data collection process.

5. The **far-reaching powers** envisaged in the draft bill especially regarding covert intrusion into IT systems and the gathering, processing, and sharing of traffic data, contradict the necessary strengthening of protective confidentiality rights for journalists. Observing these rights in operational practice requires at the very least general **bans on use of the intelligence**, appropriate **filtering procedures**, and **strengthened administrative oversight mechanisms** to ensure protection of sources.

6. An **adversarial procedure** should be introduced to ensure impartial balancing decisions by the independent Oversight Council. At the very least, however, the Oversight Council should be expanded to include relevant **expertise concerning the rule of law and freedom of the press**.

7. Rather than being restricted to an "observer role" as the draft bill currently foresees, a strengthened administrative oversight body should be given comprehensive and continual access to data as well as appropriate rights of objection so that it can meet the challenge of providing effective oversight of modern, data-based telecommunications surveillance.

3 Introduction

Seven years after the Snowden revelations and the start of an intense public debate on global mass surveillance by the NSA and its international partners, the imbalance between the intelligence services' powers of surveillance and the protection of fundamental and human rights persists. At the international level, RSF, as an organisation that campaigns for press freedom and human rights, observes a structural weakening of the rights of media workers as a result of state surveillance powers which are constantly expanding in scope due to the digitalisation of all areas of life. These measures have particularly serious consequences in countries where surveillance is used with the specific goal of restricting personal freedoms and work-related activities and silencing critical voices. However, democratic states also continue to undermine the human right to freedom of the press by failing to place adequate restrictions on the surveillance of global Internet traffic and the confidential communications of media workers.

In Germany, the NSA revelations led to a serious examination of the role of the country's intelligence services. From the point of view of press freedom, the political outcome of this examination, the amended Federal Intelligence Service Act (BNDG) which came into force in 2017, was disappointing.[1] Criticism voiced by civil society groups as well as three UN Special Rapporteurs to the effect that the law allowed virtually unrestricted surveillance of foreign persons working in professions that enjoy special confidentiality protection, such as journalists and lawyers, went unheard. Doubts regarding the constitutionality of the law were likewise ignored. In 2018, the international organisation Reporters sans frontières (RSF) together with seven journalists and lawyers and with the support of other civil society organisations therefore filed a constitutional complaint against the BNDG.

In May 2020, the Federal Constitutional Court declared the provisions for the strategic surveillance of foreign telecommunications unconstitutional in their current form and instructed the federal government to create clearly defined standards for the protection of confidential relationships of trust. The court stressed the need for freedom of the press and telecommunications privacy to be respected as fundamental rights that apply irrespective of state borders and nationalities in the context of actions by German authorities, as well as in their dimension as human rights, which the judgment acknowledges in several references to the criticism and recommendations put forward by David Kaye, former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.[2] The draft bill now on the table fails to meet this requirement. Although it formalises certain protective rights with regard to the communications of journalists and other persons working in professions that enjoy special confidentiality protection with third parties, it simultaneously once again undermines these rights through far-reaching restrictions,

[1] Reporter ohne Grenzen 2016. Stellungnahme: Wahrung der Meinungs- und Pressefreiheit durch eine grundrechtskonforme Fassung des BND-Gesetzes. https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Downloads/Berichte/2016/160804_ROG_Stellungnahme_zum_BND-Gesetzentwurf.pdf

[2] United Nations Office of the High Commissioner for Human Rights, letter sent by the Special Rapporteurs from 29 August 2016, OL DEU 2/2016.
https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=3316

unmonitored discretionary powers (section 4.2), and provisions granting new powers to hack foreign IT systems (section 4.5). If this draft bill were to form the basis for the future activities of the BND, media workers would remain exposed to an unacceptable risk of being targeted for state surveillance merely because of their investigative activities. The protection of sources would be seriously compromised and the oversight function of the media would be weakened.

Reporters Without Borders therefore urgently calls for a revision of the draft bill. It is possible to formulate the BNDG in such a way that freedom of the press is safeguarded without disproportionately limiting the intelligence service's capacity to act. It is the task of the federal government to create clear standards that reconcile security interests with fundamental and human rights. Reporters Without Borders aims to contribute to this process with constructive proposals.

4 Position on individual provisions

4.1 On the protection of “confidential relationships of trust” (Section 21)

The draft bill currently under consideration recognises the fundamental need for special limitations on surveillance of the confidential relationships between journalists, lawyers, members of the clergy and third parties, in line with Section 53 of the German Code of Criminal Procedure, yet at the same time it creates considerable scope for the continuation of current practices.

First of all, improvements are needed concerning the protection of all data subject to editorial confidentiality and source protection. While Section 2 (1) continues to provide for the processing of "necessary information including personal data," the draft bill is clearly based on the assumption that, particularly as regards technical surveillance, "due to a lack of relevance to fundamental rights" (see the explanatory comment on Article 1 Section 19 (1), p. 57) there is no need for further provisions regarding non-personal data (i.e. data that contains no references to individual persons). Consequently, the provisions for the protection of confidential relationships (Section 21 (1) of the draft bill) only apply to personal data. This is apparently based on the idea that only personal data is relevant to fundamental rights. Specifically, this probably refers to the right to protection of personality enshrined in Article 2 (1) in conjunction with Article 1 of the Basic Law in its dimension as a right to informational self-determination. However, this ignores the fact that Article 5 (1) of the Basic Law provides for comprehensive protection of all journalistic activities "from the procurement of information to its dissemination"[3], and thus protects not only the personality rights of media workers, but also the "institution of the free press" in general. Consequently, "purely technical data" (*Sachdaten*; for example traffic data or anonymous data) enjoys the same protection under Article 5 (1) of the German Basic Law as data that refers to a specific person. This is particularly important because digital anonymisation tools (anonymous mailboxes, the Tor network) play a central role in international journalistic work, especially in the context of collaborative investigative projects conducted by media networks. Anonymisation and the

[3] BVerfGE 20, 162 [176] "Spiegel"

expanding role of automation in journalism and other areas of life must not provide a gateway for press freedom to be undermined. Above all, encroachments on the rights stipulated in Article 5 (1) of the Basic Law cannot be remedied by the BND processing confidential information or passing it on to other agencies in anonymised form only. The Federal Constitutional Court also foresees comprehensive protection in its ruling of 19 May 2020.

Limiting the protection to personal data would also be problematic because there is no way to ensure that data that at first glance appears to be "purely technical" could nevertheless be traced back to a specific individual if combined with other findings of the BND or other authorities, which would de facto seriously undermine the protection of sources. However, the Federal Constitutional Court rightly assumes that media are dependent on their sources, and that the latter will only approach the media if they can continue to rely on editorial confidentiality and source protection. The confidential relationship of trust between media workers and their sources is therefore also protected by the freedom of the press.

The wording of the first sentence of the section on confidential relationships of trust, which states that the "*targeted* collection of personal data for the purpose of acquiring information exchanged within a confidential relationship of trust" is "fundamentally impermissible" also appears to aim to extend the scope for potential intrusions into confidential relationships. It is not the intention behind the intrusion that is decisive, but the recognition of the need for all confidential relationships to be protected. Consequently, if the use of a specific search term leads to the collection of data exchanged within a confidential relationship of trust to a significant degree, its use must be prohibited. The collection of data exchanged within confidential relationships must also be prevented when it occurs as unintentional "by-catch" of surveillance measures aimed at other targets. This underscores the urgent need for the Oversight Council to be informed of the search terms on which surveillance measures are based, yet Section 23 of the draft bill does not provide for such a procedure.

Furthermore, Section 21 (2) of the draft bill relativizes the protection of journalists' confidential relationships to a substantial degree and must therefore be more specific and more precise. The same applies for the parallel standards, such as Section 29 (8) or Section 35 (2). According to Section 21 (2), the protection ceases to apply and data collection is permissible as soon as there are "factual indications" that an individual is perpetrating or participating in certain criminal acts. The draft bill therefore apparently adopts the terminology used in the German Code of Criminal Procedure (StPO) in regard to initial suspicion pursuant to Section 152 (2) of the StPO. In its ruling on the case of the German online magazine Cicero, the Federal Constitutional Court stated with regard to the police raid of the magazine's editorial offices and the materials confiscated during the raid that the provisions of the Code of Criminal Procedure regarding the press were to be interpreted with a pro-fundamental rights bias, and that "specific [!] factual indications" were required with regard to the degree of suspicion. [4] Consequently, it cannot be acceptable that media representatives lose the protection of confidentiality simply because they are in contact with persons who are suspected of a crime, for example. Such contacts occur on a regular basis, especially among investigative journalists, yet this should not give rise to the suspicion that the journalists are involved in a crime. Journalists may even be bound by due diligence to

[4] BVerfGE 117, 244 [266] „Cicero“

make such contacts in the context of reporting on suspicious activities. In addition, undercover research methods may at times be necessary, especially when media workers are investigating criminal offences pursuant to Section 100b (2) of the Code of Criminal Procedure, and are also protected by Article 5 (1) of the German Constitution. When we also take into account that Section 59 (1) of the draft bill fails to stipulate that foreign journalists must subsequently be informed of their surveillance—contrary to the provisions that apply for online surveillance (cf. Section 101 StPO)—and that as a result it also effectively excludes subsequent examination of the legality of the measure by the person affected, it becomes clear that this legal concept is too vague and opens the gateway to considerable encroachments on journalists' investigative freedom. The weaker the procedural safeguards for the rights of those affected, the higher the requirements must be for clear provisions regarding encroachments on these rights. The Federal Constitutional Court made explicit reference to this in its decision of 19 May 19 2020. [5]

The fact that Section 21 (2) no. 1 in conjunction with Section 29 (3) of the draft bill provides for greater legal clarity by reducing the list of criminal offences for which confidentiality restrictions may be waived is to be welcomed. On the other hand, it is incomprehensible that Section 29 (3) of the draft bill merely refers to the catalogue of offences enumerated in Section 100b (2) of the Code of Criminal Procedure, but not to the other requirements specified in Section 100b (1) of the Criminal Code. It is also not clear why according to the Criminal Code, online surveillance of a media worker is not permitted—and rightly so—if the suspected offence is not serious in nature or if the facts of the case can be determined through other means, but it is permitted under the draft bill. Both requirements are concrete expressions of the principle of proportionality, which must be applied equally in all intelligence investigations.

Similarly worrying in view of the Federal Constitutional Court's call for clearer provisions and specificity, are the terms "goods of vital public interests" and "threats to the existence or security of the Federal Republic or one of its states, or to the security of a member state of the European Union, or of the European Free Trade Association or of the North Atlantic Treaty" in Section 21 (2) no. 2 of the draft bill. Although the reduction in the number of dangerous situations that are considered to justify intrusions into confidential relationships is an improvement on the first draft and therefore to be welcomed, the aforementioned terminology still fails to create a clear basis for differentiation. It is therefore all the more crucial to ensure that the Oversight Council can make an informed judgment also when weighing the confidentiality rights of the persons affected by surveillance against the expected added value of gaining intelligence regarding the interests mentioned above. This necessarily includes knowledge of the search terms that guide and enable the targeted collection of data.

4.2 On further restrictions on confidential relationships of trust

The draft bill does not provide clear answers to the key question of who is to be considered a journalist and can therefore claim protective rights against surveillance. According to the draft bill in its current version, the decision concerning which communication is considered to be

[5] BVerfG, Judgment of the First Senate of 19 May 2020 - 1 BvR 2835/17 -, margin number 137. http://www.bverfg.de/e/rs20200519_1bvr283517.html

part of a confidential relationship of trust rests solely with BND staff. In accordance with Section 42, the newly established Oversight Council is merely to evaluate to what extent the BND may lawfully intrude into confidential relationships of trust in the interest of the early detection of dangers. This is based on the premise that affected confidential relationships are identified in advance according to criteria stipulated in a non-public service regulation and then classified as such. In its current form, the draft does not even foresee the obligation for the BND to document this classification. As a result, the very practice of key provisions and powers being regulated in secret which the Federal Constitutional Court explicitly criticised in its ruling is continued. [6] Nor can "randomised" administrative oversight of the practical application of all standards guarantee the protective rights of media workers.

A specific statement regarding who is to be explicitly denied the protection of the confidential relationship can be found in the explanatory comments to the draft bill: in line with the Federal Constitutional Court judgment, which allows for the special protection to be limited to persons whose activities are "characterised by freedom and independence"[7], one of the explanatory comments states that "representatives of foreign intelligence services disguised as journalists or persons who engage in media propaganda for journalistic and extremist groups" (p. 73) are not entitled to protection. [*Editor's note: The aforementioned quote was removed from the final draft bill passed by the Federal Cabinet on 16 December 2020; all other comments remain relevant.*]

This wording is an improvement on the first draft bill, which referred to the politicised, highly contentious and vague term "fake news". However, the fundamental problem remains: the BND is entrusted with exercising sole decision-making power over the political legitimacy and intention of journalistic reports, removed from any independent oversight commensurate to the consequences of the decision. Such a practice would be unconstitutional. State authorities are not permitted to apply criteria based on content in their interpretation of the term "journalist". A key tenet of the media freedom enshrined in Article 5 of the Basic Law is that the state is subject to the principle of content neutrality in all its measures, and that any differentiation based on the content of a publication is impermissible. Only if a journalist violates the provisions of a general law does this cease to apply. Explicit reference to the list of offences contained in Section 100 b of the Code of Criminal Procedure already ensures that any media worker who engages in activities that are relevant under criminal law is excluded from this protection.

Contrary to the definitions that apply for members of the clergy and lawyers, the term "journalist" is not contingent on institutional affiliation or possession of a state licence. The digital transformation and new forms of publishing beyond institutional media have increased media diversity, but at the same they have made it difficult to delimit the term "journalist" and thus determine who qualifies as such. In many states where the BND operates, it is above all individuals to whom autocratic governments seek to deny the opportunity to practice journalism who guarantee a minimum of independent coverage. These individuals are often exposed to great risks in their home country and are essentially dependent on the protection

[6] BVerfG, Judgment of the First Senate of 19 May 2020 - 1 BvR 2835/17 -, margin numbers 137-139. http://www.bverfg.de/e/rs20200519_1bvr283517.html

[7] BVerfG, Judgment of the First Senate of 19 May 2020 - 1 BvR 2835/17 -, margin number 196. http://www.bverfg.de/e/rs20200519_1bvr283517.html

of their anonymity and that of their contacts. The members of the citizen journalist group *Raqqa is Being Slaughtered Silently*, who secretly documented the horrors of IS rule in Syria, are a prominent example of this. Failure to respect such individuals' protective rights because of an overly narrow interpretation of the term "journalist" would have potentially catastrophic consequences for their personal safety. This is equally true for persons outside war and crisis zones, including the renowned Azerbaijani journalist Khadija Ismayilova, who was also a plaintiff in the constitutional complaint against the BND law and has repeatedly been subjected to punitive state measures such as travel bans and been barred from exercising her profession due to her research on topics such as corruption. In Belarus, Alexander Lukashenko's government is withdrawing accreditations en masse in the face of ongoing protests, and *Tut.by*, the news site with the widest reach in the country, has been denied media status.[8] Under no circumstances should this politically motivated withdrawal of the rights of media workers in their own countries lead to further weakening or suspension of their rights by foreign authorities.

Against this background, Reporters without Borders strongly advocates a definition of the term "journalist" that is based on the social function of journalism and the *process by which trustworthy journalistic content is produced*, rather than on the content itself.[9] It is not the evaluation of a person's journalistic output or their connection to a media outlet that should form the basis for granting them protective rights. Instead, compliance with journalistic standards such as those drawn up in a CEN Workshop Agreement by the "Journalism Trust Initiative" (JTI)[10], an EU-funded pilot project, under the supervision of the European Committee for Standardization should be the key criterion in deciding who is granted protective rights. The JTI document sets out objective criteria for trustworthy journalistic work processes, which can be applied to both major media outlets and the work of individuals. Originally developed with the goal of providing criteria for differentiating between reliable journalistic sources and the growing amount of disinformation on online platforms, the standard also provides concrete reference points for the BND, which faces the challenge of identifying journalists and their communications at the operational level and protecting them from surveillance. In the medium term, the broad application of a machine-readable standard like this one could also serve to support and improve the automated filtering of data exchanged within confidential relationships.

In the interest of transparency and legal clarity, the revised BND Act must clearly stipulate that all confidential relationships based on trustworthy journalistic *work processes* are to be protected. Precisely because of the potential difficulties involved in decisions about who qualifies as a journalist and can claim the related rights, the law must provide for documentation of the BND's assessment of potential confidential relationships, on the basis

[8] Reporter ohne Grenzen 2020. Kritik an Lukaschenkos Medienpolitik. https://www.reporter-ohne-grenzen.de/belarus/alle-meldungen/meldung/kritik-an-lukaschenkos-medienpolitik

[9] Reporter ohne Grenzen 2020. Nach dem Urteil des Bundesverfassungsgerichts: Empfehlungen für ein grundrechtskonformes BND-Gesetz. https://reporter-ohne-grenzen.de/fileadmin/Redaktion/News/Downloads/RSF_Empfehlungen_Neufassung_BND-Gesetz_Juli2020.pdf

[10] Reporter ohne Grenzen 2019. Journalism Trust Initiative: Standard für Journalismus vorgelegt. https://www.reporter-ohne-grenzen.de/pressemitteilungen/meldung/standard-fuer-journalismus-vorgelegt/

of which the Oversight Council can independently review the BND's classification in advance of any measures that potentially encroach on a confidential relationship.

4.3 Lack of protection concerning the collection of traffic data under Section 26

The draft bill lacks appropriate safeguards concerning the collection and processing of traffic data (*Verkehrsdaten*). Section 26 of the draft bill makes no reference to restrictions on data collection to protect confidential relationships in accordance with the provisions of Section 21. Especially in the case of journalists, extensive knowledge can be gained about their confidential relationships with sources simply by analysing contact addresses, numbers and other traffic data which is subject to the same protection of telecommunications privacy that applies to the contents of a communication. However, from a technical point of view, email subject lines, which allow even deeper insights into the contents of a communication and are thus a core element of confidential relationships, are also part of the metadata of an email and cannot be encrypted. Effective digital source protection thus requires a ban on the analysis of traffic data relating to persons who are entitled to confidentiality protection.

As far as possible, traffic data that is attributable to media workers (including those identified as such by the BND in the course of previous surveillance measures (cf. Section 32, (5) of the draft bill) must be automatically filtered out and deleted. At the very least, however, data exchanged within confidential relationships should be subject to the same de-identification process ("hashing") that the draft bill foresees for German nationals, domestic legal entities and foreign nationals. However, to ensure the constitutionally required protection of sources, it is not sufficient to "hash" the traffic data of the protected person, but not that of their interlocutor (cf. the explanatory comment on Section 26 (3) of the draft law, p. 85), because the potential feedback of the connection data of a media worker's contacts into targeted data collection measures through the use of search terms would result in a gap in protection that would invalidate the provisions of Section 21. Any categorisation of hashed data must also be ruled out. Compliance with the corresponding provisions and the functionality of the filtering procedures must be subject to regular review by the administrative oversight body.

4. 4 Lack of protection when unfiltered traffic data is processed in the context of cooperation under Section 35

“The automated sharing of unfiltered personal traffic data” in the context of cooperation with other foreign intelligence services provided for in Section 35 links up with the problems mentioned above. The draft bill provides for extremely far-reaching powers to use and share unfiltered and personal traffic data gathered en masse insofar as it serves to “gather intelligence on state-directed disinformation campaigns designed to destabilise”, among other things. Why imprecise terms such as “fake news” (used in the first draft, now replaced by "media propaganda") can cause enormous damage to freedom of the press has already been explained above. In many states, such terms all too often provide a gateway for limiting freedom of expression and freedom of the press under the pretext of protecting public opinion from harmful influence. Against this background, namely the serious impact of

discretionary decisions of this kind, the role of intelligence service oversight must be to closely monitor such decisions.

The power to share unfiltered traffic data appears highly questionable in the context of this field of activity of the BND and elsewhere. This data forms a basis for extensive intelligence concerning an individual's contacts, movement profiles, and the content-related focus of their online activities. If this data is shared unfiltered with other intelligence services, it cannot be ruled out that they will prepare such profiles about media workers and their sources even if they have no connection to the matter requiring intelligence. Ensuring that other intelligence services handle such data in accordance with the law is beyond the democratic control of German authorities, so that the subsequent use by other intelligence services of data collected by the BND to investigate confidential relationships must be ruled out in advance. Concerning this point, general assurances that the rule of law will be observed cannot preclude erosion of the protection of sources.

4.5 On the legalisation of previously unregulated powers to hack under Sections 34 and 35

The situation is further exacerbated by the fact that the draft bill is intended to codify the BND's previously unregulated hacking methods. The intelligence service has reportedly had the capability to penetrate foreign IT systems and servers, intercept digital communication, and capture stored data for a number of years. [11] The law is intended to legitimise this intrusive practice and does not exclude media professionals from "individual surveillance measures" of this kind, insofar as the data contributes to the early detection of dangers in accordance with the previously discussed, vaguely formulated provisions analogous to Section 21 (2).

It has already become clear in the context of the amendment of the Federal Protection of the Constitution Act that the practice of state hacking is highly controversial. Here, we refer the reader to RSF's position paper on the amendment of the Federal Protection of the Constitution Act.[12]

One reason for this is the serious nature of covert intrusion into third parties' systems, another is the lack of practical differentiation between targeted intrusion to obtain information for a specific purpose and accessing irrelevant data that merits protection. It can hardly be ruled out that the confidential communications or files of media workers will be gathered as bycatch when third parties' servers are infiltrated. The weak administrative oversight of data collection and processing provided for to date would not counter this risk. For this reason,

[11] Netzpolitik.org 2020. Eine neue Lizenz zum Hacken. https://netzpolitik.org/2020/bnd-gesetz-eine-neue-lizenz-zum-hacken/

[12] Reporter ohne Grenzen 2020. Stellungnahme zum Referentenentwurf eines Gesetzes zur Anpassung des Verfassungsschutzrechts. https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/user_upload/Stellungnahme_BVerfSchG-RefE_Reporter_ohne_Grenzen__RSF__2020.pdf

ensuring the observance of journalists' protective rights would at the very least necessitate continual, full access for the oversight body to data gathered through this method.

4.6 On oversight of intelligence services (Sections 23, 40-58 (sub-section 5))

Overall, the envisaged reform of the oversight of intelligence services with a view to independently ensuring the protection of confidential relationships of trust does not go far enough. A comparison of various oversight systems in European countries shows how intelligence service oversight could be designed in a way that is more effective and more appropriate to the highly enhanced technical possibilities of telecommunications surveillance without placing excessive restrictions on the BND's ability to act. Both civil society actors and the Federal Commissioner for Data Protection and Freedom of Information proposed alternatives[13,14] for dealing with this issue, yet this draft bill does not sufficiently take them into account. The tight time frame for the reform must not lead to important opportunities to revise and update the oversight system being missed.

An "Independent Oversight Council" consisting of six lawyers and an expanded staff is to make decisions regarding the BND's surveillance measures. This body is supposed to review the legality of the warrants, but must work under conditions that fail to meet the requirements of data-driven telecommunications surveillance. For example, there is no obligation for the warrants to include information about the individual search terms ("selectors") that guide the data collection and subsequent analysis (Section 23 (6)). This would mean that decisive information is withheld from the oversight body. Under these conditions, the Oversight Council would not be able to assess the extent to which specific search terms potentially affect confidential relationships. Moreover, the classification of confidential relationships is neither subject to documentation requirements nor to the Oversight Council's supervision and decision-making power. In addition, Section 56 limits the Oversight Council's access to offices and IT systems to those which are solely under the control of the BND and are not used in cooperation with other intelligence services. In view of the BND's far-reaching cooperation with other agencies, this represents a considerable restriction of democratic oversight.

The abovementioned administrative oversight body is to review the legality of the implemented collection, processing and sharing of data with partner intelligence services, however only on the basis of "random" checks; thus, the relevant provisions are far too weak to ensure that the safeguards are observed in practice. These provisions hardly allow for the "comprehensive oversight" described in the explanatory comments to the draft bill. Although the envisaged exchange between the Oversight Council and the administrative oversight body is to be welcomed, the restriction of oversight to random checks and an "observer role"

[13] Wetzling, Thorsten und Moßbrucker, Daniel, Stiftung Neue Verantwortung 2020. BND-Reform, die Zweite: Vorschläge zur Neustrukturierung der Nachrichtendienst-Kontrolle. https://www.stiftung-nv.de/sites/default/files/bnd_reform_die_zweite_vorschlaege_zur_neustrukturierung.pdf

[14] Netzpolitik.org 2020. Erste Positionierung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) zum BND-Gesetz. https://netzpolitik.org/2020/bnd-gesetz-datenschutzbeauftragter-kritisiert-staatstrojaner-fuer-geheimdienste/#2020-10-12_BfDI_BND-Gesetz_Erste-Positionierung

with only limited rights of objection undermines the effectiveness of the oversight system as a whole.

By contrast, the role of the parliamentary oversight body has not been enhanced. Its only new responsibility is to select the members of the Oversight Council, but the fact that they are preselected by the President of the Federal Court of Justice and the Federal Public Prosecutor General (Section 43) further limits this role. The draft bill retains the division of oversight of the intelligence service among various bodies whose competencies are in some far too restricted, and combines this with the questionable differentiation between surveillance of international communications (where one communicating party is in Germany and the other is outside Germany; *Inland-Ausland-Fernmeldeaufklärung*) and surveillance of exclusively foreign communications (where all communicating parties are located outside Germany, *Ausland-Ausland-Fernmeldeaufklärung*), rather than seizing the opportunity for a comprehensive reform of intelligence service oversight.

Another fundamental shortcoming is the lack of an independent and critical voice representing groups affected by surveillance and in particular persons who from professional groups that require special protection such as media workers and lawyers. If an adversarial procedure were introduced to the decision-making process, it could function as an urgently needed counterweight to the argumentation of the intelligence service, which is focused exclusively on obtaining as much intelligence as possible.

As a minimum measure, expanding the advisory board could provide the necessary expertise and plurality of voices to ensure effective, independent oversight. While legal and technical expertise are essential for effective oversight of digital surveillance activities, it is equally essential that questions concerning the rule of law, freedom of the press, and other societal developments be answered by a well-informed oversight body equipped with the necessary expertise in these areas. The corresponding models in other European countries can serve as an example.

Berlin, December 2020

Contact

Lisa Dittmer
Advocacy Officer for Internet Freedom, Reporters Without Borders Germany

Email: ld@reporter-ohne-grenzen.de