Stiftung Neue Verantwortung

The Human Rights, Big Data and Technology Project

Caught in the Act?
An analysis of Germany's new SIGINT reform

Research Report

by

Kilian Vieth-Ditlmann and Thorsten Wetzling

25 November 2021

UKRI Economic and Social Research Council

Human Rights Centre | University of Essex

Report Authors

Kilian Vieth-Ditlmann researches surveillance and democratic governance at the think tank Stiftung Neue Verantwortung (SNV). He is a member of the GUARD//INT research consortium, as well as project manager for the European Intelligence Oversight Network (EION) and part-time editor at aboutintel.eu. His work examines the potentials and limits of overseeing surveillance and reform approaches for human rights-based and more efficient intelligence and surveillance policy in Germany and Europe.

Dr. Thorsten Wetzling heads the SNV's research unit on basic rights, surveillance and democracy. He currently directs the European Intelligence Oversight Network (EION), a collaborative research project to support and challenge intelligence oversight bodies across Europe. He is also a Principal Investigator for the international research consortium GUARD//INT which aims to build empirical and conceptual tools to better understand the limits and potential of intelligence oversight mechanisms. Thorsten is also founder and editor-in-chief of aboutintel.eu – a European discussion forum on surveillance, technology and democracy.

About the Stiftung Neue Verantwortung. The Stiftung Neue Verantwortung (SNV) is an independent, non-profit think tank working at the intersection of technology and society. SNV's core method is collaborative policy development, involving experts from government, tech companies, civil society and academia to test and develop analyses with the aim of generating ideas on how governments can positively shape the technological transformation. To guarantee the independence of its work, the organization has adopted a concept of mixed funding sources that include foundations, public funds and corporate donation.

Table of Contents

Executive Summary

When the German parliament amended the legal framework for Germany's foreign intelligence service in March 2021, it had a unique chance to set the pace among liberal democracies for better legal standards on proportionate government access to data and the protection of fundamental rights. Recent European jurisprudence such as the *Schrems II* ruling by the Court of Justice of the European Union and the *Big Brother Watch* and *Centrum för Rättvisa* decisions by the European Court of Human Rights brought additional momentum to the international quest for better standards in legislation and oversight practice.

Unfortunately, the Bundestag did not seize the moment. Despite laudable progress in some areas, there is a pressing need for future legislative work to align the German legal framework on foreign intelligence collection with international standards and to better meet the German Constitutional Court's minimal requirements. This report thus calls for a comprehensive intelligence reform to improve the quality of the legal framework and to guarantee more robust fundamental rights protections and to overcome the undue fragmentation of oversight and authorization processes.

Regarding the **quality of the legal framework,** lawmakers should

- establish a clear and consolidated legal framework for investigatory powers across the German intelligence and security sector. This should include a single judicial authorization mechanism that eliminates inefficient duplications.
- regulate bulk data access more transparently, including provisions on commercial data purchases, suitability tests, and interception of machine-to-machine communications.

Regarding **fundamental rights protection,** lawmakers should

- create an effective judicial remedy mechanism for ex post facto review of foreign surveillance, as required by European jurisprudence.
- apply the same standards and safeguards that pertain to the collection of personal content data also to the collection of metadata. This is in line with the recent ECtHR Grand Chamber judgement which deemed both data types as equally worthy of protection.

Regarding the **oversight and authorization process,** lawmakers should

- expand the independent approval powers to cover bulk data analysis (examination warrants), suitability tests (testing and training warrants), and commercial data buying (data acquisition warrants).
- include systematic points of friction in the judicial authorization process by allowing for adversarial counsel in the assessment of bulk warrants, as well as by providing direct access for the oversight body to bearers of communications in order to verify

adherence to warrant criteria, as is common practice in the Swedish foreign intelligence framework.
- define a concrete ex post control mandate that enables data-driven oversight of the BND's data handling, including the independent analysis of the selectors used.
- introduce binding enforcement powers for the independent oversight body, including the power to prohibit certain data collection and to require data destruction.
- codify comprehensive public reporting obligations for the oversight body.

1. Introduction[1]

After a far-reaching judgement by the German Constitutional Court in May 2020, Angela Merkel's governing coalition of conservatives and social democrats found themselves, yet again, in the position to pass a foreign intelligence reform through the Bundestag.[2] This had become necessary after the Court settled the basic question whether the territorial reach of the right to private communication and press freedom as guaranteed under Article 10 and Article 5 of the German constitution extends beyond the German territory and protects not just German nationals and residents. Unlike the government, the Constitutional Court unequivocally affirmed that these fundamental rights are human rights and not citizen rights, and that they can therefore apply extraterritorially, when state authorities collect data of individuals abroad.[3] In turn, this required a wholesale amendment of both the legal framework for foreign intelligence and its judicial oversight.

The BND Act, as amended in March 2021, now substantially changes and expands the surveillance powers of Germany's foreign intelligence agency, the *Bundesnachrichtendienst* (BND).[4] It also establishes a wide range of new safeguards and oversight structures.[5] This report introduces the new regulatory framework and offers an assessment of its merits and shortcomings. It does this in recognition of other recent legal and political developments at the international level. More specifically, Germany's foreign intelligence reform came at a time when the practice and legal bases for bulk collection and other forms of (automated) government access to personal data received renewed attention across Europe. Among these recent developments were

- The *Schrems II*[6] ruling by the Court of Justice of the European Union (CJEU) which saw inadequate safeguards against government access to personal data as the main reason to terminate the Privacy Shield agreement for data transfers from the EU to the US.

[1] This research was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation - Project Number 396819157) and by the UK Economic and Social Research Council project 'Human Rights, Big data and Technology' [ES/M010236/1].
[2] For an analysis of the 2016 reform of the BND's legal framework for foreign intelligence collection see: Wetzling, Thorsten, "New Rules for SIGINT Collection in Germany: A Look at the Recent Reform," 23.07.2017, Lawfare, https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform
[3] BND Act judgement and original media summary of the Federal Constitutional Court available at: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2020/bvg20-037.html
[4] With a reported budget of € 1.079 billion in 2021 and roughly 6.500 official employees, the BND is a sizable foreign intelligence service, wielding significant technical resources to conduct bulk collection and computer network operations among other methods such as human intelligence collection.
[5] The Bundestag passed the reform on 25.03.2021, it will enter into force on 1.01.2022, but a range of transitional provisions and transitional periods apply (§ 69 BND Act).
[6] References to all the cases cited can be found in the annex.

- The CJEU's ruling on the *Quadrature du Net* and the *Privacy International* cases which pronounced on some EU member states' laws on mandatory data retention in the private sector, and which prohibited general and indiscriminate data retention and established conditions for effective oversight of government access to this data.

- The European Court of Human Rights (ECtHR) recently observed that "seven Contracting States (being Finland, France, Germany, the Netherlands, Sweden, Switzerland and the United Kingdom) officially operate bulk interception regimes over cables and/or the airways,"[7] and called for a more robust legal framework and restrictions to ensure data protection standards, effective oversight, and remedies in *Centrum för Rättvisa v Sweden* judgement, and requiring more in-depth and rigorous oversight in *Big Brother Watch and others v UK*.

- The Council of Europe promotes its modernised Convention 108 as the only legally binding international agreement on data processing and data protection that extends to the realm of national security and defence (Council of Europe 2018) but key representatives acknowledge publicly: "While Convention 108+ provides a robust international legal framework for the protection of personal data, it does not fully and explicitly address some of the challenges posed in our digital era by unprecedented surveillance capacities."[8]

- The Organisation for Economic Co-operation and Development (OECD) has initiated work towards adopting a high-level principles document to establish basic common standards for government access to personal data held by the private sector.[9]

Much like Germany's second attempt to reform the legal bases and oversight framework for the BND's foreign intelligence collection, many of these developments are tied to pressing political and legal questions regarding the de jure and de facto conditions, guarantees, and safeguards for bulk collection and oversight. Together, this might create a new momentum for a collective search for appropriate safeguards and effective oversight and redress mechanisms which the Snowden revelations had initially ignited.

---

[7] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 19.06.2018, recital 131, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=40. The Court also observed that "if Norway's draft law is enacted, it will also authorise bulk interception" (recital 132).
[8] Pierucci, Alessandra and Jean-Philippe Walter. (2020). Better protecting individuals in the context of international data flows: the need for democratic and effective oversight of intelligence services, Joint Statement by the Council of Europe's Chair of Convention 108 and the Council of Europe's Data Protection Commissioner. Available at: https://rm.coe.int/statement-schrems-ii-final-002-/16809f79cb
[9] OECD Committee on Digital Economy Policy. 2020. Statement: Government Access to Personal Data Held by the Private Sector. See: https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm.

Hence, this report's deep dive into how Germany has just redesigned its legal framework for strategic bulk collection and computer network exploitation, it is hoped, might be of interest to non-German readers, too.[10]

[10]At the outset, it should be noted that other intelligence disciplines, such as human intelligence gathered by agents abroad, are not part of the report's focus. Neither does this paper provide an analysis of other intelligence reforms that the Bundestag adopted in 2021. On the reform of the law governing domestic intelligence agency (*Bundesverfassungsschutzgesetz*) and the law on domestic surveillance measures (*Article 10 Act*) see, for example: Vieth, Kilian and Dietrich, Charlotte, "New hacking powers for German intelligence agencies", https://aboutintel.eu/germany-hacking-reform/.

2. Reformed bulk surveillance powers

This section discusses the main changes of the BND Act after the comprehensive reform of 2021 in order to make them intelligible for non-German readers. Beginning with an overview of the central foreign surveillance powers exercised by the BND (2.1), the section then dissects three key bulk powers, namely strategic bulk interception (2.2), computer network exploitation (2.3) and transnational data sharing (2.4) based on detailed reference to the underlying reformed provisions. By comparing the new legal framework to the criteria provided by the German Constitutional Court ruling, the section provides context for the intricate regulations. Section 3 then deals with the new oversight structures. A subjective assessment of the reform's advantages and deficits as well as the remaining gaps in relation to international standards and case law follows in section 4.

2.1 Overview of key surveillance powers

Before digging deeper into the individual data collection authorities and their respective requirements, a short general overview of key surveillance powers shall help readers to get a better grasp of Germany's foreign intelligence law. By way of introduction, figure 1 provides an overview of the BND's key legal authorities to access data under the new BND Act.

First, the BND wields a general mandate to collect communications for foreign intelligence purposes. It may compel actors from the private sector to provide communications data, such as data streams flowing through backbone fiber optic cables which are administered by telecommunications providers. *Compelled access* is typically directed at domestic communications providers which are subject to German jurisdiction. Due to Germany's geographical location in the heart of Europe, routing of foreign communications makes up a relevant fraction of overall telecommunication traffic, even in domestic communications networks.[11]

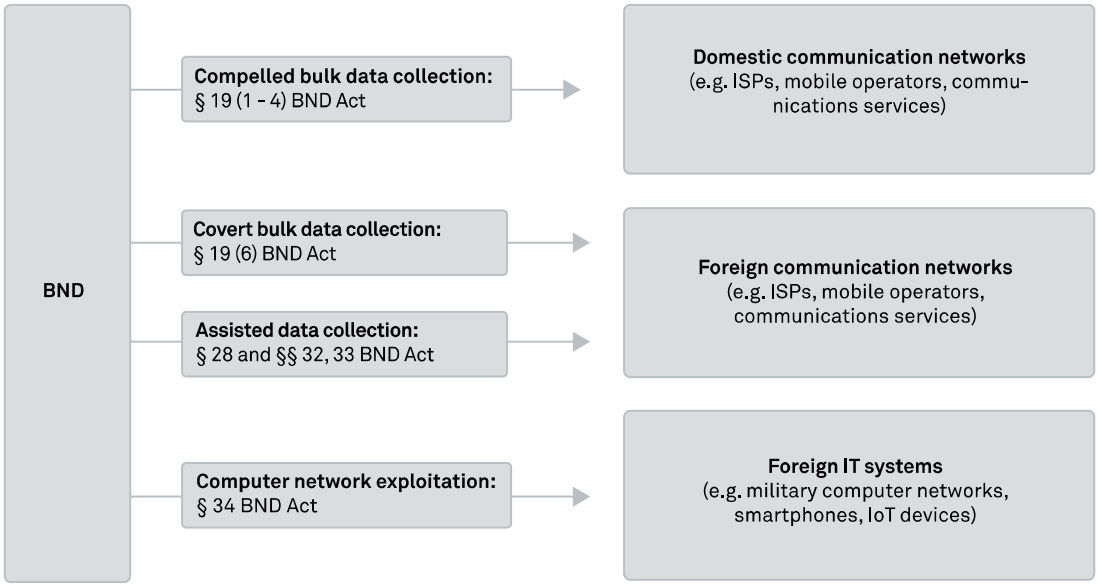
Second, foreign communications networks, such as internet service providers (ISPs) or mobile phone network operators can also be directly targeted by the BND. On the one hand, it may infiltrate foreign providers covertly, interfering with the IT systems to enable data access (*covert bulk data collection*). On the other hand, the BND can request the assistance of foreign intelligence agencies to access data. *Assisted data collection* entails sending relevant search terms to a foreign public body, which then sends relevant hits, for example for certain IP or MAC addresses, back to the BND. These two forms of data access are used if the company that holds or routes the data cannot be legally compelled by the BND.

[11] For example, the internet exchange point DE CIX in Frankfurt is one of the largest in the world, with an average overall traffic of more than 6.5 terabits per second at this hub. For more detailed traffic statistics see: https://de-cix.net/en/locations/frankfurt/statistics

Importantly, there is also a general authority to conduct *bulk collection suitability tests*. The BND can tap into foreign and domestic communications networks in order to assess the usability of a specific provider or networks for strategic surveillance purposes and to check the relevance of search terms.

Third, a legal authority to interfere with and exploit foreign computer systems has been enshrined in the new BND Act. This *hacking authority* may target IT systems abroad that the BND expects to yield relevant foreign intelligence data.

Figure 1: BND's SIGINT data access authorities under the 2021 BND Act



Fourth, albeit not included in the illustration, the report will discuss transnational data-sharing as a separate important authority. The amended BND Act features new standards for international SIGINT data transfers and cooperation. The BND can share data with foreign agencies ad hoc and in bulk, even automated transmissions are possible. The agency can also transfer large amounts of data to the German military and other domestic actors.

2.2 Strategic foreign communications collection (bulk interception)

2.2.1 Legal basis and scope

The central norm that regulates the BND's mandate to collect foreign communications in bulk is paragraph 19 of the BND Act (see the annex for an unofficial translation). It lists the aims which the government must pursue when seeking the authorization for strategic foreign telecommunications collection (*Strategische Ausland-Fernmeldeaufklärung*). [12] Whereas paragraph 19 applies to foreign communications only,[13] it does not mean that the collection of foreign communications under this provision is limited to non-German territory. Rather, if the communications of foreign entities or individuals are processed by providers within Germany, the BND can compel them to provide access to this data (§ 25 BND Act).

Moreover, the BND Act now also includes an explicit regulation for the covert intrusion of communications systems if it is necessary for the implementation of bulk interception measures (§ 19 (6) BND Act). Accordingly, the BND may use technical means to secretly infiltrate the IT systems of a communications service provider abroad. Authorizing an intelligence agency to break into the computer systems of a foreign entity in a foreign country will, most likely, come into conflict with the law there. The Federal Constitutional Court acknowledged this tension in its May 2020 judgement and noted that this may still be afforded: "In the interest of the Federal Republic of Germany's security and capacity to act, the intelligence that can be obtained must also include information that is deliberately withheld from Germany – possibly with negative intentions – and is kept secret within the other jurisdiction. Under the law of the state targeted by surveillance measures, such measures may also be illegal, or at least unwanted."[14] In response to this, the 2021 reform of the BND Act took this controversial practice of covert bulk interception out of the legal grey zone and established a specific legal basis for it.

The general scope of paragraph 19 of the BND Act is limited to the collection of personal content data (*personenbezogene Inhaltsdaten*) in the context of strategic foreign communications collection. Consequently, a range of other data collection practices in the

[12] Note: In this paper, we use the terms "bulk interception" and "bulk collection" to refer to this statutory power, because these concepts are more frequently used in the English language.
[13] A separate law, the Article 10 Act, regulates the interception of domestic communications. The Article 10 Act, however, also goes beyond "interception of domestic communications" in that foreign-domestic traffic, i.e., communication that involves both foreign and domestic participants, is regulated in § 5 of the Article 10 Act. For more information on the Article 10 Act and recent reform attempts, see e.g. Wetzling, Thorsten, 2016, https://www.stiftung-nv.de/sites/default/files/snv_g10.pdf; Vieth, Kilian and Dietrich, Charlotte, 2020, https://aboutintel.eu/germany-hacking-reform/
[14] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 159, https://data.guardint.org/en/entity/neb3eo8hl9h?page=43

pursuit of, for example, human intelligence, the commercial acquisition of data, open source intelligence and social media intelligence are not covered by the comprehensive regulation and oversight regime that the 2021 reform of the BND Act established.[15] These forms of foreign intelligence gathering were not part of the 2021 reform legislation and are subject to other, often less stringent, legal requirements.

The BND Act distinguishes between different data categories: content data, metadata, traffic data and inventory data (see table 1). One key distinction is the one between content data and metadata. Whereas paragraph 19 applies only to *personal content data*, the collection and processing of metadata, including traffic data, are subject to separate and far less stringent requirements (for example § 26 BND Act regarding domestic traffic data). Most importantly, the collection and processing of foreign metadata is exempt from most legal restrictions. The collection of inventory data is only explicitly referred to in the context of covert bulk interception (§ 19 (6) BND Act).

Table 1: Data categories used in the BND Act

Category	Description	Provision(s)
Content data	The content of individual communications, e.g., body of emails or text messages, audio of online calls, etc.	§ 19 (1) and (5) § 27
Metadata	All data that is not content data. Examples provided:[16] - all technical and operational information generated by telecommunications systems, e.g., related to routing, - data about the structure and use of other data - data about data, such as data type, technical classifications, etc.	Not specified in the BND Act.[17]
Traffic data	A subset of metadata which is produced, processed or used during the operation of communications services.	§ 26 § 33
Inventory data	A provider's stored information about users, e.g., name, address, etc.	§ 19 (6)

[15] For some forms of intelligence collection, the government will continue to refer to the very broadly formulated general authority to collect information provided in paragraph 2 of the BND Act, directly available (in German) at: https://data.guardint.org/en/entity/dwo3l04euwc?page=5
[16] Explanatory Statement of the draft BND Act, 25.11.2020, p. 57
[17] There is a lack of legal definitions that allow to clearly distinguish between metadata and "traffic data" as well as "personal traffic data" (§ 26 BND Act), see: Federal Data Protection Commissioner, Official Statement on the draft BND Act, 18.12.2020, p. 6f, https://www.bundestag.de/resource/blob/822374/aab1552370d14e223a56bf66ef23f041/A-Drs-19-4-682-data.pdf

Suitability tests (Cold-starting capability)

Beyond the general authority to conduct bulk interception discussed above, the BND Act allows also for another form of bulk collection – albeit with far fewer safeguards and control requirements. As an exception to the general rule that content data may only be collected in bulk on the basis of search terms (§ 19 (5) BND Act), the BND may perform so-called suitability tests (*Eignungsprüfungen;* § 24 BND Act) in order to either test the suitability of specific telecommunication networks for bulk collection purposes (purpose 1) or to generate new search terms or to assess the relevance of existing search terms (purpose 2). On the face of it, suitability testing is intended to ensure that bulk collection is targeted at the most relevant carriers, using the most appropriate search terms. Suitability tests in pursuit of purpose 1 (relevant networks) require a written order by the president of the BND or his or her designated deputy and may only be performed if factual indications exist that the selected telecommunications networks bear appropriate data for the purposes of strategic foreign surveillance as regulated in the BND Act. Suitability tests in pursuit of purpose 2 (relevant search terms), however, do not require such safeguards. What is more, there is no requirement, as is the case in some other democracies,[18] for the ex ante authorization involving independent oversight bodies nor is the duration and the volume of the data collection in pursuit of suitability tests subject to (effective) limitations.[19]

In general, data that has been collected in pursuit of the suitability test must be processed only for either purpose (listed above). This rule does not apply, however, when factual indications point to a grave threat to individuals or the security of either the Federal Republic of Germany or institutions of either the European Union and its Member States, EFTA and NATO (§ 24 (7) sentence 1 BND Act). Another exception to this rule is the force protection of the German military and that of EU, NATO and EFTA Member States: If factual indications exist that data from suitability tests points to threats to either of them, it may also be processed. Finally, and importantly, the BND may also transmit data from suitability tests automatically (i.e., without further data minimization) to the German Armed Forces (§ 24 (7) sentence 3 BND Act) where the requirements govern the processing, transfers and deletion of such data are far less stringent and transparent. Moreover, it should be borne in mind that the new judicial and administrative oversight mechanisms created as part of the 2021 reform of the BND Act (see section 3.2) have no mandate to review the use of such data by the German Armed Forces.

[18] According to "Part 4 Authorisations - Subpart 3 - Practice Warrants - Section 91 - Application for issue of Practice Warrant" New Zealand's Intelligence and Security Act 2017 establishes a detailed authorization procedure for testing and training warrants that involves the Chief Commissioner of Intelligence Warrants und des Inspector General. See: https://www.legislation.govt.nz/act/public/2017/0010/latest/whole.html#DLM7118938

[19] While there is no limitation rewarding the volume of traffic that may be collected by means of so-called suitability tests for either purpose, only the suitability test according to purpose 1 is subject to a six months time limit, which may also be renewed for an unspecified number of times for further six months (§ 24 (2) sentence 2 and 3 BND Act).

2.2.2 Requirements

Lawful aims

The basic authority to conduct strategic foreign intelligence collection requires a prior written application that ought to state which lawful aim is being pursued. According to paragraph 19 this can only be one of the following two general cases: gathering information for the Federal Government of Germany (aim 1) and to detect threats of international relevance (aim 2).

In general, the BND may conduct strategic surveillance based on orders of the Federal Chancellery in order to provide information for foreign and security political decision-making (§ 19 (3) BND Act). This general authority may not be used for economic espionage, which is defined as gaining competitive economic advantages (§ 19 (9) BND Act).

Applications for strategic foreign communications collection to gather information for the Federal Government of Germany (aim 1) can only be issued if they serve the purpose to obtain information about foreign countries, are relevant for German foreign and security policy, and were ordered by the Federal Chancellery. By contrast, applications for strategic foreign communications collection to detect threats of international relevance (aim 2) ought to satisfy the same criteria required for aim 1, and in addition they must meet the requirement that factual indications exist at the time of the application that such measure might produce insights into eight general threat areas such as crises abroad, national defense, and threats to critical infrastructure, or if they yield insights that allow to protect five legal interests, for example the security of the German state or of institutions of the European Union.

Table 2: Overview of lawful aims

Aim 1: Providing information to the Federal Government (§ 19 (3) BND Act)	**Aim 2: Early detection of threats of international importance** (§ 19 (4) BND Act)
Strategic surveillance measures for aim 1 are only permitted, if they - serve the purpose of obtaining information about foreign countries, - are relevant for German foreign and security policy, and - were ordered by the Federal Chancellery	Strategic surveillance measures for aim 2 are only permitted, if they - serve the purpose of obtaining information about foreign countries, - are relevant for German foreign and security policy, and - were ordered by the Federal Chancellery and if there are factual indications that these strategic surveillance measures can: 1. produce insights into the following eight threat areas:

	- national defense as well as protection of (allied) armed forces abroad - crises abroad and their effects - terrorism and (violent) extremism, or its support - criminal, terrorist or state-sponsored attacks on information technology systems by means of malware, or support for such attacks - organized crime - international proliferation of weapons of war, as well as unauthorized foreign trade with goods and technical support services in cases of significant importance - threats to critical infrastructures - hybrid threats or if they 2. produce insights that help to protect the following five legal interests: - life or freedom of a person - existence or security of the Federal Government or a state (Land) - existence or security of institutions of the European Union, the European Free Trade Association or NATO or a member state of these organisations - the Federal Republic of Germany's ability to act in foreign policy - important legal interests of the general public.

The list of permissible aims demonstrates the BND's dual role as a foreign intelligence and a military intelligence agency. While being formally supervised by the Federal Chancellery, different parts of the government and their subordinated agencies, including the foreign ministry, the interior ministry and the domestic intelligence services as well as the defense ministry and the armed forces receive information from the BND's SIGINT operations and contribute to its national intelligence priority framework (*Aufgabenprofil BND*).

Volume limitation

Besides requesting new and more detailed legal authorities for main operational aims discussed above, the Federal Constitutional Court's judgement also demanded that bulk

interception of communications must not be unlimited and "sweeping,"[20] which prompted lawmakers to include a new data volume limitation. It limits the amount of data that the BND may collect to a maximum of 30 percent of the transmission capacity of all globally existing telecommunications networks (§ 19 (8) BND Act).[21] We will discuss the relevance of this legal boundary for bulk data collection in the analysis section below. It should be noted, also, that this volume limitation does not pertain to bulk collection in pursuit of the suitability tests.

Specific protections and exceptions

The BND Act also comprises a number of specific provisions that ought to protect the fundamental rights to privacy of correspondence, posts and telecommunications (Art. 10 of the Basic Law), press freedom (Art. 5 of the Basic Law), and the right to informational self-determination as well as confidentiality and integrity of IT systems (derived from Art. 2 (1) in connection with Art. 1 (1) of the Basic Law). Following the landmark decision by the Constitutional Court, the BND Act now includes additional rules that seek to better protect these rights in specific SIGINT governance contexts. By way of introduction and illustration, these protections are tied to the distinction into different data protection categories summarized below.

Table 3: Overview of data protection categories

Data category	Scope
Foreign data	Personal data related to communications of foreigners abroad.
Domestic data	Personal data related to communications of - German citizens and residents - Companies and organizations in Germany
Protected professional communications	Personal data related to professional communications of clerics, lawyers and journalists abroad.
Data related to the core of private life	Content that relates to the essence of an individual's privacy. It must not be subject to surveillance of any kind under German constitutional law.
EU data	Personal data related to citizens of the European Union citizens, EU institutions, and public bodies in EU member states.

[20] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 168, https://data.guardint.org/en/entity/neb3eo8hl9h?page=46

[21] Whether this volume limitation of 30 percent applies to suitability tests that the BND can conduct according to paragraph 24 of the BND Act is not specified.

Most of the protections of data categories listed in table 3 are constructed according to the same logic: the provision first prohibits the collection of certain communications in principle, and then lists exceptions from that basic rule.

The discrimination of foreign and domestic data is the most basic distinction throughout the BND Act. While the collection of foreign data is the BND's mission, it must not, in principle, collect domestic data. Paragraph 19 section 7 prohibits the collection of data of any German citizen, even if they are located abroad, as well as any person located on German territory. It also bans the BND from intercepting the communications of companies and other legal bodies within Germany, because their communications are also protected by the right to private correspondence. That said, incidental collection of domestic data is inevitable if an intelligence agency collects bulk data in telecommunication networks. How the BND approaches the challenge to filter out domestic data is discussed below in the subsection on data processing.

Put differently, unless one's communication data is protected by virtue of its professional characterization (see below) or by virtue of one's identity as a German citizen, German company or resident in Germany or the European Union, the new SIGINT framework in Germany offers little explicit protection, let alone redress options. The BND ought to afford everyone the right to privacy under Art. 10 of the German Constitution, irrespective of citizenship or current geographical location. This basic legal premise, however, does not amount to equal treatment in practice. Rather, when it comes to the authorization procedure, non-EU communications are subject to far less stringent requirements and data subjects have virtually no options available to obtain effective remedy for misuse of their personal data. According to the Constitutional Court, a strengthened judicial and administrative oversight over the BND's treatment of non-national communications data was necessary in order to compensate "for the virtual absence of safeguards commonly guaranteed (to non-nationals) under the rule of law."[22] More specifically, it found that an amended BND Act "must compensate for the gap in legal protection that follows from the weak possibilities for individual legal protection in practice. Given that very limited information and notification requirements apply to the surveillance of foreign telecommunications in light of its need for secrecy, effective legal protection can hardly be obtained."[23]

Protected professional communications

Following the Constitutional Court's demand that the surveillance of communication of professional groups such as journalists, lawyers or priests must be further restricted, the BND Act now offers increased protections to communications of certain professional groups (§ 21 BND Act).[24]

[22] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 273, https://data.guardint.org/en/entity/neb3eo8hl9h?page=71
[23] Ibid.
[24] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 194, https://data.guardint.org/en/entity/neb3eo8hl9h?page=52

The legal norm states that targeted collection of personal content data with search terms is illegal, if it relates to the communications of clerics, lawyers and journalists. The protection is limited to these three professional groups, because they have a right to confidential communications and a privilege to refuse to give evidence.[25] The professions listed in the German code of criminal procedure that enjoy similar confidentiality safeguards would also include members of parliament, social workers, tax consultants, physicians, psychologists, pharmacists, midwives and others,[26] but they are not included in the wording of paragraph 21 of the BND Act.[27]

The second section of § 21 specifies the exceptions to the general protection of journalists, lawyers and clerical professions. When facts justify the assumption that a person from one of these three groups is the perpetrator or participant in certain criminal offenses,[28] so-called 'targeted' data collection (i.e., the use of search terms related to that person) is allowed. The same is the case if the data collection is necessary to prevent serious threats to life, limb or freedom of a person and a number of other legal interests listed in section 2 of paragraph 21. The legal norm, thus, makes two basic weighting decisions necessary. First, the BND needs to assess whether a person belongs to one of the protected professional groups. Second, it must decide if there are facts that allow exceptional data collection.

Regarding the first decision on classifying someone as a journalist, attorney or pastor, the policy makers acknowledge that such assessments require more detailed criteria, especially in the case of journalists, because this profession is not legally defined and not necessarily linked to an employer or organization. More detailed requirements regarding who counts as a journalist will, according to the explanatory statement, be subject to a secret executive decree (*Dienstvorschrift*).[29]

Data related to the core of private life

German law recognizes the "core of private life" (*Kernbereich privater Lebensgestaltung*) as another basic principle aimed at protecting the individual from government surveillance. It was

[25] § 53 (1) German code of criminal procedure (*Strafprozessordnung*)
[26] § 53 (1) sentence 1, number 3, 3a, 3b, 4 of the German code of criminal procedure
[27] The Federal Association of Tax Consultants, for example, submitted a statement in the legislative process which requested that tax counselling should be protected under § 21 BND Act, too. Tax advisors process sensitive personal data on a long-term basis, they argued, which permits comprehensive insights into the economic and personal circumstances of their clients. Similar arguments could probably be made for other professions that work under increased confidentiality requirements. Full statement in German: Bundessteuerberaterkammer, 3.12.2020, https://www.bundesregierung.de/resource/blob/976020/1826352/4f5c9136681ee130b65e4906141072d0/2020-12-09-bnd-gesetzentwurf-stellungnahme-bundessteuerberaterkammer-1--data.pdf?download=1
[28] § 29 (3) BND Act refers to the relevant criminal offenses listed in § 100b (2) of the German code of criminal procedure, https://www.gesetze-im-internet.de/stpo/__100b.html as well as to the foreign trade act, §§ 17 and 18, https://www.gesetze-im-internet.de/awg_2013/__17.html
[29] Explanatory Statement of the draft BND Act, 25.11.2020, p. 68

developed in case law and insulates the core of private life, for example communications of highly personal character such as soliloquy, expression of feelings, unconscious experience or sexuality from state surveillance. In so doing, the essence of privacy and intimacy shall be off-limits, and this applies also in the context of strategic foreign communications surveillance (§ 22 BND Act). Even interests of paramount importance cannot justify an intrusion in the core of private life.[30]

Given that technical parameters and search terms are insufficient means to determine whether the core sphere of private life is affected, the BND is required to conduct manual assessments and must delete pertinent data immediately. In unclear cases, the Independent Control Council (see section 3) must scrutinize whether the data may be processed further (§ 22 (3) BND Act).

Data processing

When pressed, the BND stated in the constitutional court proceedings that it collects about 270.000 human communications such as phone calls or chat messages per day of which "an average of 260 data transmissions are identified and forwarded to the relevant departments every day."[31] The processing of data – from the collection point to the final intelligence output – is consequently an important element in a legal framework for strategic surveillance operations.[32] The BND Act addresses the role of data filters in paragraph 19 section 7 and the handling of domestic metadata in paragraph 26.

Filtering (data minimization)
According to paragraph 19, section 7, sentence 1 of the BND Act domestic content data that was collected in foreign SIGINT operations must be automatically filtered out and immediately deleted. Yet, the technical infrastructure of the internet makes incidental collection of domestic data inevitable. Despite the general prohibition, the legal framework includes an exception that allows processing incidentally collected domestic content data if the BND has reason to believe that the further processing of the illegally collected domestic data may help to prevent dangers to life or freedom of a person, national security or the security of an EU or NATO member state (§ 19 (7) sentence 6 BND Act).

In practice, this rule might create an incentive to actually retain and process domestic data instead of immediately deleting it. The exception presupposes that domestic data has already been processed to some extent, because otherwise no actual evidence with regard to the permissible exceptions could have been retrieved.

---

[30] Explanatory Statement of the draft BND Act, 25.11.2020, p. 69
[31] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 25, https://data.guardint.org/en/entity/neb3eo8hl9h?page=19
[32] See the *International repository of legal safeguards and oversight innovation* for an analysis of good practices in governing intelligence data handling throughout the entire signals intelligence cycle: https://www.intelligence-oversight.org/; and: Wetzling, Thorsten and Vieth, Kilian 2018

The Federal Constitutional Court, in principle, accepted that the BND deploys filter systems to process as little domestic content data as possible in foreign intelligence collection. Regarding the accuracy and sophistication of the filter technology, the judgement required that the "legislator must impose an obligation on the intelligence service to continually develop filtering methods and to keep them up to date with developments in science and technology."[33] The governing coalition, however, decided to introduce a less ambitious legal requirement that demands that the filter methods shall be continuously developed and must be kept up to date with the current state of the art (§ 19 (7) sentence 4 BND Act). This limits the development of the filter methods to minimization techniques that are already available and does not comply with the standard formulated by the Federal Constitutional Court.

Search terms

Under the authority of a bulk interception warrant, the BND may collect and process content data only with the help of search terms (also called selectors). The processing of metadata does not require the use of search terms and is not covered by the requirements of paragraph 19 of the BND Act.[34]

The BND Act states that it is not necessary to list individual search terms in the bulk interception warrants (§ 23 (6) sentence 2 BND Act), which in practice exempts most search terms from ex ante approval of lawfulness. Only specific categories of search terms that target, for example, EU citizens or journalists, are subject to ex ante approval of the judicial control body (§ 42 BND Act). Other selectors that do not target one of the specifically protected categories such as confidential professional communications (see above), cannot be checked prior to their use.

Search terms that are not approved on the basis of a warrant, can, however, be reviewed at random by the administrative control body.[35] During the Constitutional Court proceedings the BND revealed that it uses a "six digits" number of search terms in its SIGINT operations.[36] If between 100.000 and 999.000 selectors are used simultaneously to collect content data, manual random inspections appear largely ineffective. The BND Act, though, does not include requirements for more structured or automated oversight of the use of search terms. Only the

[33] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 173, https://data.guardint.org/en/entity/neb3eo8hl9h?page=47

[34] Search terms can be connection IDs, geographical areas, but also the identifiers of an entire telecommunications network of a closed user group. Search terms may also be actual words or phrases, as well as search patterns. In practice, though, the search terms are more often formal communication identifiers such as IP address ranges or email addresses. Content-related search terms, for example names of specific chemical compounds used for the weapon production, are used less frequently. See: Explanatory Statement of the draft BND Act, 25.11.2020, p. 64

[35] Explanatory Statement of the draft BND Act, 25.11.2020, p. 71

[36] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 24, https://data.guardint.org/en/entity/neb3eo8hl9h?page=37

transfer of search terms to foreign intelligence services must be subjected to automated checks.

Assisted data collection

The BND may also ask a foreign intelligence service for permission to feed certain selectors into their operational systems. Prior to a foreign public body using BND search terms, the government ought to make sure that these terms meet the same requirements as those governing the BND's own use of search terms (§ 28 (3) BND Act): They must not lead to the processing of telecommunications traffic from German nationals, domestic legal entities or persons residing in Germany. Equally off limits are search terms to engage in industrial espionage. The surveillance of EU institutions, of public bodies of its member states or of EU citizens requires the same independent approval. In addition, search terms must respect the protection of confidentiality relationships, as well as the safeguards related to highly private content data.[37]

Domestic metadata

Compared to the more detailed provisions on personal content data, the federal legislators shied away from writing specific requirements and safeguards into the law as regards metadata. Thus, most of the data protection categories specified in paragraphs 19 to 23 (see table 3 above) concern personal content data, despite the fact that most of the data collected and processed in SIGINT is metadata (including traffic data).[38] While paragraph 26 declares the processing of personal domestic traffic data, i.e. data related to German citizens, German legal bodies and all persons located on German territory, as illegal in principle, it also introduces two broad exceptions to this basic prohibition:

First, the BND may collect metadata in the context of machine-to-machine communications. This is defined as automated technical data transmissions without the intervention of the user (§ 26 (3) sentence 2 number 1 BND Act). Examples for such automated communications could be back ups and other synchronizations with servers, automated online payments, log in exchanges between mobile phones and cell towers, or automatically logged location data. The legislators presume that such data flows should not be regarded as related to personal communications and should fall outside the scope of the constitutionally protected confidentiality of telecommunication (Article 10 of the Basic Law).[39]

Second, it permits the processing of domestic traffic data without restriction if it is automatically made unreadable immediately after their collection (§ 26 (3) sentence 2 number 2 BND Act).

---

[37] §§ 19 (5), 20, 21, 22, 23 (5) of the BND Act
[38] See table 1 for definitions
[39] For example, the Federal Constitutional Court decided in a different ruling that the collection of metadata produced by mobile phones with the help of IMSI catchers (sometimes called stingrays) does not violate the right to confidential communications in Article 10. Federal Constitutional Court, Mobile Phone Tracking Judgement, 22.08.2006, press release in German available at: https://www.bundesverfassungsgericht.de/pressemitteilungen/bvg06-093.html

This masking of personal domestic traffic data shall be implemented by using hash functions that would allow a re-identification of the original data "only with disproportionate effort."[40] All traffic data that does not allow to identify participants in domestic communications, such as time stamps and other technical parameters, need not be hashed. The metadata of the foreign participants of the communication must also not be made unreadable with the hash function. This raises the question whether the hashing achieves the intended goal of anonymization of domestic data. If only one side of a communication is hashed, there could remain a possibility to re-identify the domestic persons based on correlations.[41] If the BND's operational systems fail to anonymize domestic data, the law requires that the respective data be hashed belatedly as soon as possible or deleted immediately. But this requirement is also subject to the exception that the BND may process the domestic traffic data if facts indicate that it might help to prevent significant dangers.[42]

Data retention

Table 4 below sums up the different retention limits for personal data collected under the authorities for suitability tests and bulk interception. Notice, there is no definite retention limit for content in bulk interception. The previous BND Act included a maximum retention limit for content of ten years, which was replaced by a mandatory evaluation of whether data is still needed in intervals of seven years. Traffic data may be retained for up to six months, but longer storage is possible if the BND regards the data as necessary.

Personal data collected in search term suitability tests can be stored for up to two weeks, network suitability tests can be retained for up to four weeks (§ 24 (6) BND Act). An exception applies to encrypted data, which can be retained for up to ten years.

Table 4: Retention rules for bulk interception

Authority	Data category	Retention rule	Legal provision
Suitability tests	Personal data collected in suitability tests for search terms	Retention for up to two weeks	**§ 24 (6) sentence 1**

[40] Explanatory Statement of the draft BND Act, 25.11.2020, p. 78
[41] eco, Official Statement on the draft BND Act, 18.02.2021, p. 4, https://www.bundestag.de/resource/blob/823354/a8060be2f61786ee68a7baec7be153e9/A-Drs-19-4-731-E-data.pdf
[42] Amnesty International Germany criticized these exceptions, arguing that it does not comply with the prohibition to process domestic metadata. Even if one regards hashing traffic data as a form of immediate deletion, there is a risk to re-identify individuals in combination with other data. See: Amnesty International Germany, Official Statement on the draft BND Act, 17.02.2021, p. 7, https://www.bundestag.de/resource/blob/823300/941d473299f4e353f088a4f7bf6eb1c1/A-Drs-19-4-735-data.pdf

	Personal data collected in suitability tests for telecommunication networks	Retention for up to four weeks	**§ 24 (6) sentence 1**
	Encrypted (unreadable) personal data collected within any suitability tests that is required for research purposes	Retention for up to ten years	**§ 24 (6) sentence 3**
Bulk interception	Data collected under a preliminarily approved and then revoked warrant	Immediate deletion	**§ 23 (4) sentence 6; § 23 (7) sentence 6**
	Domestic traffic data that was not or cannot be anonymized	Immediate deletion, with exceptions for emergency cases of serious dangers	**§ 26 (4)**
	Traffic data	Retention up to six months, with exceptions permitted	**§ 26 (5)**
	Personal content data	Mandatory evaluation of relevance in intervals of seven years; immediate deletion if data is deemed irrelevant	**§ 27**

Authorization and Oversight

The strategic foreign communications collection pursuant to paragraph 19 of the BND Act requires written bulk warrants (*Anordnungen*) which must be signed off by either the president of the BND or his or her deputy (§ 23 BND Act). These bulk warrants must include information on the purpose of the data collection, the relevant topic within the lawful aims of paragraph 19 sections 3 or 4, the geographical focus, the duration, and a justification. The law does not provide a period of validity for the warrants. The warrant's lawfulness must then be approved by the judicial control body of the Independent Control Council before its implementation (§ 23 (4) BND Act, see section 3.2 of this report). If the warrant is declared unlawful, the warrant expires. In cases of imminent danger, a preliminary approval can be obtained by one single member of the judicial control body (for details on oversight structures and ex ante approval powers, see section 4 of this report).

Once the warrant has been approved by the judicial oversight body, the BND sends an order to each implicated communications provider, which must include the name of the compelled company, the duration of the measure, and the affected communications (§ 25 (2) BND Act).

2.3 Computer network exploitation

2.3.1 Legal basis and scope

The amended BND Act now includes a (bulk) equipment interference authority (§ 34 BND Act). The provision allows the BND to compromise IT systems used by foreigners abroad and to collect communications as well as stored data on these systems.[43]

The main reasons to hack into foreign IT systems are that a global expansion of encryption undermines the effectiveness of (bulk) interception and that the BND has no jurisdiction to order compelled access to data held by private parties abroad. This constraint has also been addressed under the general authority for strategic foreign communications surveillance. It states that if the BND cannot establish "cooperative access" (*kooperativer Zugang*), then it may use secret means to collect data and infiltrate the information systems of telecommunications providers to overcome security measures (§ 19 (6) BND Act, see above). The typical targets of the BND's computer network exploitation (CNE) are not individual smartphones, but rather computer systems used for business purposes or to operate IT infrastructure such as computer networks of military facilities or telecommunications providers.[44] Paragraph 34 and following, nonetheless, allow interfering with the personal devices of individuals abroad, too. It also permits collecting both stored data as well as ongoing communications.

The use of computer network exploitation is now also explicitly permissible if it "inevitably" affects data of other individuals or systems (§ 34 (6) BND Act). According to the official explanatory statement that accompanies the new BND Act this would, for example, include a scenario in which the BND first needs to compromise the computer of a network administrator and intercept her password in order to, then, infiltrate the actual target system of the operation.[45]

[43] While the use of hacking operations has been common practice before, the legislators now established a legal norm that explicitly permits the hacking of foreign IT systems by the BND. The creation of a legal basis for the BND's hacking operations is acknowledged as an attempt to establish legal clarity for this intrusive surveillance power. See: Explanatory Statement of the draft BND Act, 25.11.2020, p. 94.
[44] Explanatory Statement of the draft BND Act, 25.11.2020, p. 94
[45] Explanatory Statement of the draft BND Act, 25.11.2020, p. 96

2.3.2 Requirements

Lawful aims

The BND may deploy means of equipment interference for the same lawful aims that apply to the use of bulk interception (see section 2.2). These are either the (political) information of the German Federal Government (aim 1), or the early detection of imminent dangers of international significance (aim 2).[46] The only difference is that CNE requires "facts" rather than "factual indications" that the hacking operation conducted in pursuit of aim 2 will allow detecting threats of international importance (§ 34 (3) BND Act). This represents a higher legal threshold if CNE is used for threat detection instead of information gathering.

Specific protections and exceptions

Only computers used by foreigners abroad may be targeted under this authority (§ 34 (1) BND Act). Thus, the BND is, pursuant to the BND Act, not allowed to hack into the devices of German citizens, domestic organizations and persons located on German territory.[47]

In addition, the BND Act provides the same protections for confidential professional communications of lawyers, clerics and journalists that are also protected under the rules for strategic foreign communications surveillance (cf. discussion of § 21 in section 2.2 above). No hacking operations may thus be directed at members of said professions, if they communicated in confidential professional relationships. The same exceptions to this rule, however, also apply.[48] The legal norm requires the same case-by-case weighting decisions, in which the BND agents need to determine if the computer system in question belongs to one of the protected professional groups, secondly, whether there are legal exceptions that permit hacking the device.

Equally, any data collection related to the core of private life, i.e. content that relates to the essence of an individual's privacy or intimacy, is off limits in the context of hacking operations. Paragraph 36 (parallel to § 22, see section 2.2.2 above) provides the same general prohibition and subsequent balancing considerations. The processing of highly private information is

[46] Cf. § 34 (1) number 2 BND Act, in connection with § 19 (4)) BND Act
[47] However, under the amended Article 10 Act of 5.07.2021, the BND, as well as all other German intelligence agencies are allowed to use means of CNE against domestic communications. There are constitutional complaints pending against this domestic hacking mandate (see Vieth and Dietrich 2020 for an English commentary on the draft law).
[48] For example, the collection of protected professional communications of an individual, such as the communication of a foreign journalist with a source, is allowed if the journalist might be participating in certain criminal offenses or if the infiltration of her device is necessary, for instance, to prevent serious threats to vital goods of the general public (§ 35 (2) number 2, littera b) BND Act); see also discussion in section 3.1.2 above.

illegal, and if the BND is uncertain as to whether specific material touches this core sphere of private life, the independent oversight council needs to authorize further processing.

On a technical level, the Act requires that the BND must ensure that modifications made to the targeted IT systems are necessary for data collection and that they are revoked automatically once the operation ends (§ 34 (4) number 1 BND Act). The software and hardware used to break into foreign computers and exfiltrate data must be protected against unauthorized use in accordance with up-to-date technical standards (§ 34 (4) number 2 BND Act).

Data processing

The data processing rules included in the framework for CNE only relate to data retention (see table 5), and do not touch upon data minimization rules or metadata processing, as is the case in bulk interception.

Table 5: Retention rules for CNE

Authority	Data category	Retention rule	Legal provision
Computer network exploitation	Data collected in hacking operations	Data collected in hacking operations shall be evaluated immediately, if possible, but no later than three years after collection. Revaluation in intervals of five years whether the data is (still) relevant. Irrelevant data must be deleted immediately.	**§ 34 (7)**
	Data collected under a preliminarily approved and then revoked warrant	Immediate deletion	**§ 37 (4)**

The BND must immediately check whether personal data gathered in hacking operations is necessary for one of the permissible aims. The wording in § 34 (7) BND Act suggests that the data could also be deemed necessary for a different operational purpose than the one that was included in the initially signed CNE warrant.[49] If an immediate assessment of the data is

[49] Cf. § 34 (7) sentence 1 BND Act: "The Federal Intelligence Service [BND] shall immediately check whether the personal data collected as part of an CNE measure in accordance with section 1 are required alone or together with data already available for the purposes pursuant to section 1" (own translation).

not possible, for example if the data is encrypted, the data can be retained for up to three years. The Independent Control Council may approve longer retention periods than three years for encrypted devices or their images, such as copies of storage medium (§ 34 (9) BND Act).

Authorization and Oversight

Parallel to bulk interception warrants, all CNE measures pursuant to paragraph 34 BND Act must first be signed off by either the president of the BND or his or her deputy and then approved in advance by the Independent Control Council, based on written warrants. The CNE warrant must include the following information:

1. purpose of the hacking operation
2. corresponding subject matter of the measure
3. goal of the measure
4. type, scope and duration of the hacking operation
5. justification
6. if applicable the extended data analysis period.[50]

The warrants are limited to 12 months, with an (unlimited) renewal option for another 12 months at a time, if the necessary conditions are still met (§ 37 (3) BND Act). The warrants neither have to include specifications of the targeted system or person nor information about the tools used to infiltrate the system. This means that the oversight body will not be able to verify whether the technical means used in CNE measures complies with basic human rights standards.[51]

The BND Act also remains silent as regards the management of vulnerabilities and exploits that the BND uses to conduct hacking operations. Retaining and exploiting the vulnerabilities for intelligence hacking operations – instead of patching them – may affect large numbers of users. Whether and how known and unknown vulnerabilities may be exploited and how the BND approaches the trade-offs of IT security and intelligence gathering, remain unregulated by the BND Act and are not subject to independent oversight.[52]

---

[50] Listed in § 37 (2) BND Act

[51] Most recently, the public debates about the proliferation and abuse of hacking tools such as "Pegasus" by the NSO Group have triggered renewed calls to regulate the trade in such spy weapons, see e.g. "Joint open letter by civil society organizations and independent experts calling on states to implement an immediate moratorium on the sale, transfer and use of surveillance technology" https://www.apc.org/en/pubs/joint-open-letter-civil-society-organisations-and-independent-experts-calling-states-implement; "German Chancellor Angela Merkel Calls For More Restrictions On Spyware" https://www.ndtv.com/world-news/german-chancellor-angela-merkel-calls-for-more-restrictions-on-spyware-2492352

[52] For a vulnerabilities assessment and management model see: Herpig, Sven, "Governmental Vulnerability Assessment and Management: Weighing Temporary Retention versus Immediate Disclosure of 0-Day Vulnerabilities," August 2018, https://www.stiftung-nv.de/sites/default/files/vulnerability_management.pdf

2.4 Transnational data transfer and cooperation

2.4.1 Legal basis and scope

As Germany's core signals intelligence agency, the BND maintains close connections with foreign intelligence services around the globe and shares data in large quantities with other agencies. It cooperates with about 450 intelligence services in over 160 countries,[53] and maintains close ties to institutions of the European Union and NATO. Between 50 and 60 percent of search terms used by the BND stem from intelligence services of allied states, such as the Five Eyes.[54]

The role of the BND's transnational cooperation with so-called partner services was scrutinized closely by the Constitutional Court, in part because it had previously been subject of political contestation within the parliamentary inquiry committee.[55] The NSA inquiry committee in the Bundestag showed that previous intelligence legislation and oversight regimes were insufficient to prevent abuse and malfeasance in the context of international SIGINT cooperation. In the Constitutional Court proceedings, the judges frequently expressed their discontent with the previous oversight structure characterized (in part) by inadequate access, impenetrable secrecy and lack of resources and control instruments.

While the court acknowledged the basic need to cooperate with foreign services as a means to fulfil the BND's mandate, it also held that "German state authority is responsible for the sharing of data and is bound by the fundamental rights when sharing data."[56] Under German constitutional law, the judges argued, sharing data with other bodies constitutes a separate interference with fundamental rights and consequently requires independent statutory protections that must be necessary and proportionate. And this, the Court argued, was not sufficiently guaranteed in the 2016 reform, even though one of the main drivers for that reform had been to rein-in on intelligence cooperation malpractice.

Notably, the CJEU argued in the same vein in its *Schrems II* decision, where it found "that the communication of personal data to a third party, such as a public authority, constitutes an interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, whatever

---

[53] See BND website on cooperation (in German): https://www.bnd.bund.de/DE/Die_Arbeit/Kooperationen/kooperationen_node.html
[54] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 27, https://data.guardint.org/en/entity/neb3eo8hl9h?file=15978344731474zg14a5ky0w.pdf&page=38
[55] NSA Inquiry Committee Report, 28.06.2017, p. 516 ff, https://data.guardint.org/en/entity/xaoryados7?page=516; for an overview of all reports related to the NSA Inquiry Committee (in German), such as the special report on the use of selectors and the special votes of the parliamentary opposition, see: https://data.guardint.org/en/entity/jpspzqpia5
[56] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 233, https://data.guardint.org/en/entity/neb3eo8hl9h?page=61

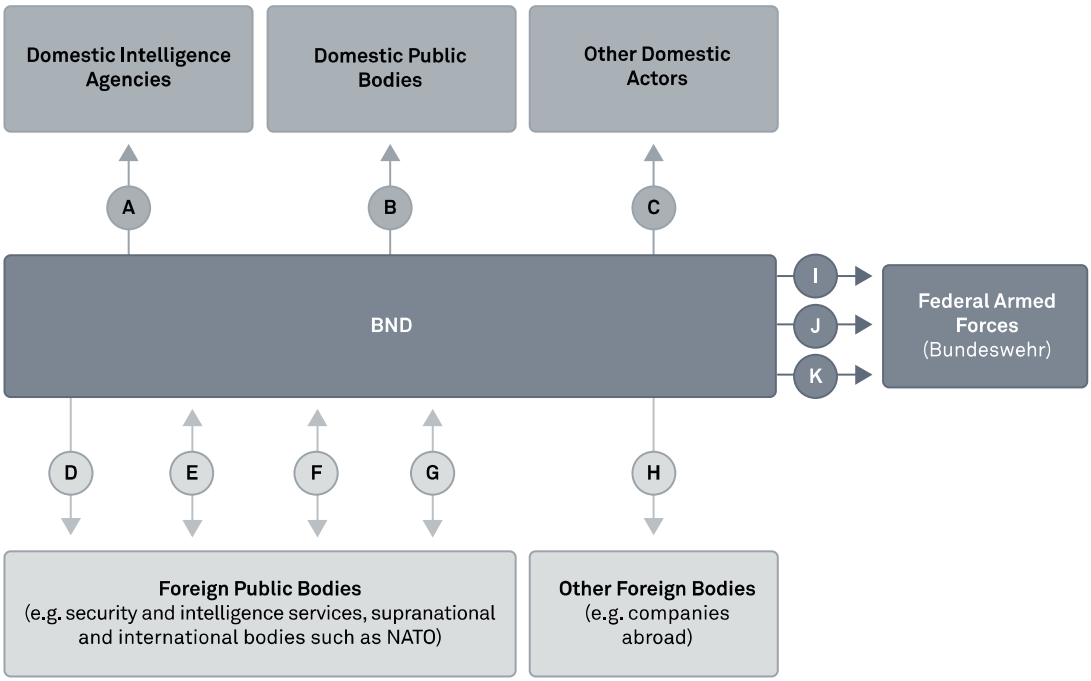
the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities, irrespective of whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference."[57]

The BND Act distinguishes between ad hoc transnational data transfer and data sharing and exchanges that are administered under written cooperation agreements, so-called Memorandums of Understanding (MoU). The transfer of personal SIGINT data to foreign and transnational bodies in the absence of a cooperation agreement is now governed by paragraph 30, which enables the BND to exchange data with foreign intelligence services and other foreign public bodies. If the data-sharing happens within a cooperation, for example with agencies from EU member states or NATO, the formation of this cooperation falls under the rules of paragraph 31 BND Act.

It is important to note that the requirements discussed below only apply in the context of SIGINT and do not replace the general regulations on data transfers and joint databases included in paragraphs 11 to 18 of the BND Act.

[57] Court of Justice of the European Union, Schrems II Judgement, 26.07.2020, recital 171, https://data.guardint.org/en/entity/k4ae1290jz?page=38

Figure 2: BND's SIGINT data-sharing authorities



A **Data transfer:** § 29 (1) and § 38 (1) BND Act

B **Data transfer:** § 29 (2) and § 38 (2) BND Act

C **Data transfer:** § 29 (6) BND Act

D **Data transfer:** § 30 (1, 2, 5) and § 39 (1, 2) BND Act

E **Shared automated databases:** § 16 (2) BND Act

F **Automated bulk data transfer:** §§ 31, 32, 33 BND Act

G **Assisted data collection:** § 28 BND Act

H **Data transfer:** § 30 (4, 5) BND Act

I **Shared databases:** § 12 BND Act

J **Automated data transfer:** § 29 (5) and § 38 (5) BND Act

K **Automated transfer of data from suitability tests:** § 24 (7) BND Act

Moreover, the BND Act includes a wide range of provisions governing the transfer of SIGINT data with domestic bodies, including other domestic intelligence agencies at the federal and state level and other public bodies of the German security sector, as well as private actors. These domestic data sharing processes, in the context of SIGINT, are for the most part regulated in paragraph 29 of the BND Act. In this section, the discussion focuses on the transnational dimension of intelligence sharing, discussing the requirements for cross-border data transfers, international SIGINT cooperation, and the enhanced data sharing between the BND and the German Federal Armed Forces, the *Bundeswehr*.

2.4.2 Requirements

Lawful aims

SIGINT data transfer

Personal data collected under the legal authorities for bulk interception or computer network exploitation may be transferred to foreign agencies and transnational bodies if this is necessary to fulfil the BND's mandate *in the context of international political cooperation* (§ 30 (1) and § 39 (1) BND Act). Beyond that, data may, for example, also be shared for law enforcement purposes (§ 30 (2) and § 39 (2) BND Act) and other aims such as prevention of significant dangers (§ 30 (3) and § 39 (3) BND Act). Data gathered for information purposes can exceptionally be shared outside of the context of international political cooperation, too, with the aim to prevent imminent dangers (§ 30 (5) BND Act). It is basically the BND's responsibility that the data transfer is lawful. It must inform the recipients about the applicable purpose restrictions and can inquire whether the data has been processed by them for permissible purposes only. The recipient must agree to a binding assurance to comply with the request to delete data. Transfers can no longer take place if factual indications exist that such a binding assurance is not being honoured by the recipient (§ 30 (8) BND Act).

The legal norm further specifies cases in which data may not be transferred to foreign agencies: "A transmission does not take place if the BND recognizes that, by taking into account the type of personal data and its collection, the legitimate interests of the data subject exceed the general public interest in the transfer of data."[58]

The interests of an individual under surveillance that are "worthy of protection" (*schutzwürdig*) may prevail, if there are factual indications that the use of the shared data in the recipient country could lead to significant human rights violations or the violation of basic principles of the rule of law. This would be the case if the data is used for "political persecution or inhuman or degrading punishment or abuse" (§ 30 (6) sentence 2 BND Act, own translation). The law, thus, imposes a weighting of interests in borderline cases before the BND shares personal data in the SIGINT context. In cases of doubt, the BND has to take into account whether the recipient provides a *binding assurance of adequate protection* for the shared data, and whether there is evidence that such assurances will not be complied with. When the BND makes this assessment, it needs to factor in the type of information as well as the previous handling of shared data by the recipient (§ 30 (6) sentence 3 BND Act).

This "generalised assessment of the factual and legal situation in the receiving states"[59] was a requirement of the Federal Constitutional Court which requested that all data transfers must be balanced and justifiable according to minimum safeguards

[58] Own translation of § 30 (6) sentence 1 BND Act.
[59] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 239, https://data.guardint.org/en/entity/neb3eo8hl9h?page=62

(*Rechtsstaatlichkeitsvergewisserungpflicht*). It leaves a significant scope of consideration to the BND and does not require proactive investigations to corroborate the rule of law assessment. It suffices that the BND "recognizes"[60] that the protection of the individual outweighs the interest in the data transfer.

SIGINT cooperation agreements

Bulk data sharing that goes beyond ad hoc transfers of information requires written agreements, so-called memorandums of understanding (*Absichtserklärung*), that specify the purposes of bulk data exchanges. Paragraph 31 section 3 outlines the three operational purposes for transnational cooperation with other intelligence services, which include the early detection of severe threats (number 1) and the protection of foreign and security interests of the Federal Republic of Germany (number 2). It also allows cooperation if the operations of the BND would otherwise be made very difficult or impossible (number 3).

In practice, this means that the legislator mandates the BND to negotiate agreements with foreign services about the exchange of search terms for bulk interception, as well as automated transfer of unevaluated bulk data. For data collection based on search terms, the BND can receive and use search terms determined by foreign intelligence services to scan data traffic and to forward the relevant hits automatically to the foreign services. Conversely, the BND may also transmit its own search terms to foreign agencies, who then feed them in their operational data collection systems (assisted data collection pursuant § 28 BND Act).

The MoUs with partner services from EU or NATO member states must be approved by the Federal Chancellery (§ 31 (7) BND Act). All other cooperation agreements must be approved by the head of the Federal Chancellery and the parliamentary oversight committee must be informed about the conclusion of new MoUs. If the MoU entails sharing unevaluated bulk data automatically, it requires the head of the BND to sign off (§ 33 (3) BND Act).

[60] It must be recognizable (*erkennbar*), which does not indicate a proactive obligation of verification.

Table 6: Requirements for transnational cooperation agreements

Lawful aims of cooperations (§ 31 (5) BND Act)	**Necessary binding assurances** (§ 31 (4) BND Act)
Cooperation is permissible to collect information on: 1. Early detection of dangers related to terrorism and extremism 2. Early detection of illegal proliferation of weapons of mass destruction 3. Protection of the armed forces 4. Critical developments abroad 5. Threats to individuals 6. Political, economic or military activities abroad that are relevant for foreign and security policy 7. foreign intelligence activities targeted at Germany 8. international organized crime 9. establishing and maintaining essential capabilities of the BND or partner services 10. international malware attacks on the confidentiality, integrity or availability of IT systems 11. comparable cases.	The foreign intelligence service must assure that: a. Purpose limitations are adhered to and data is only shared with third parties if the BND agrees b. German domestic data must not be collected or processed c. Data from protected professions must be deleted if detected d. Data pertaining to the core area of private life must be deleted if detected e. Data use is compatible with fundamental principles of the rule of law and, in particular, that data may not be used for political persecution or for inhuman or degrading punishment or treatment or for the suppression of the political opposition or certain ethnic groups f. The BND may receive, upon its request, information about the data processing g. Data will be deleted upon request of the BND h. Traffic data is only retained for up to six months.

The eight binding assurances that the BND needs to negotiate with its partner services mostly include the same rules that the BND needs to comply with in its own bulk interception activities. For example, the foreign service needs to agree to delete data related to German citizens and organizations, protected groups and the core of private life (see table 6). Next to the binding assurances listed in paragraph 31, section 4 of the BND Act, the law names eleven permissible cooperation purposes, which range from gathering information on early detection of threats, protection of armed forces, and organized crime, to "comparable cases" (§ 31 (5) number 11 BND Act). The permissible purposes are worded in broad terms, which leaves a significant scope of action for the BND.

Expanded data sharing with the armed forces

The BND, and especially its SIGINT branch, serves also as a provider of military intelligence to the Federal Armed Forces (*Bundeswehr*). While the German military manages its own

strategic surveillance capabilities,[61] the BND Act provides for designated data sharing arrangements. Next to jointly administered databases between the BND and the armed forces (§ 12 BND Act), the BND may also transfer bulk data to agencies under the auspices of the defense ministry. Bulk data gathered as part of the SIGINT suitability tests can be shared in an automated way (§ 24 (7) BND Act). Such bulk collection measures for testing purposes serve to determine relevant search terms and relevant communications networks for future bulk interception measures. They are exempt from any ex ante oversight, and it is unclear which legal provisions regulate the data handling by the armed forces (see section 4 for details).

Data collected for threat detection purposes based on search terms can also be transferred automatically to the German military under certain conditions. This applies to data collected in CNE operations, as well as bulk collection based on search terms.[62] The Federal Government included the provisions that allow automated data sharing with the Armed Forces, although the constitutional judgement did not include substantial considerations regarding (automated) sharing of data between the BND and the military.

Data processing

SIGINT data transfer

The legal rules on transnational data sharing include that recipients may only process the shared data for a previously defined purpose. The BND must inform all recipients that such purpose limitations apply and that it may request information from them about how they have processed the shared data. To put this into practice, the BND is required to arrange corresponding access to information rights (*Auskunftsrechte*) with the body that receives the data. The recipient must also give a binding assurance to comply with a request for deletion by the BND. If there are factual indications that such an assurance by the recipient will not be complied with, no data collected in the context of strategic surveillance may be shared (§ 30 (8) BND Act).

In addition, the foreign recipient must check whether the shared personal data is actually needed and delete the shared data if it is not necessary. It must not be deleted, though, if the data that was evaluated as non-essential is linked to other information and the separation of the data would create undue costs.[63] If the personal data that is supposed to be shared is linked or grouped together with additional personal data, for example of other individuals, then the data can still be shared as long as the legitimate interests of the third person do not "clearly

[61] For example, the Military Intelligence Command of the Armed Forces (*Kommando Strategische Aufklärung*), that also includes several battalions for electronic warfare and reconnaissance, see: https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir/kommando-strategische-aufklaerung

[62] The legal basis for bulk interception is § 29 (5) BND Act, for automated data sharing of hacking data § 38 (5) BND Act applies.

[63] § 29 (13) BND Act in connection with § 30 (9) BND Act

prevail" (§ 29 (14) BND Act). Furthermore, if shared personal data is incomplete or incorrect, the BND must notify the recipient, unless the mistakes are inconsequential (§ 29 (15) BND Act).

Selector-based bulk data

The search terms that foreign intelligence services feed into the BND's data collection systems are subject to the same filter requirements that apply to the use of the BND's own selectors.[64] The law requires an automated scan to check whether the search terms determined by foreign partners are compliant with the written cooperation agreement.

Automated filters shall verify whether the data includes information on the core area of private life, domestic personal data (e.g., on German residents) or specially protected confidential relationships (e.g. journalists). It must also be checked in an automated way whether the transmission of the data collected would conflict with the national interests of the German state (§ 32 (3) and (4) BND Act). Regarding protected professional communications, the BND must maintain block lists of identifiers of journalists, lawyers and clerics whose communications are afforded special confidentiality protection in order to gradually improve the filter accuracy (§ 32 (5) BND Act). Creating such block lists for protected groups was an explicit requirement put forward by the Constitutional Court judgement.[65] Subsequent to these automated scans, the selector-based data is transferred automatically to the partner service.

The accuracy and veracity of the automated checks and filtering of search terms must be subject to random checks by internal BND staff. According to the BND, about 300 search terms are checked manually per month.[66] Despite frequent calls to the contrary, the current law does not foresee an active involvement of the Independent Control Council in the filter verification. The Chancellery must be informed every six months about the BND's manual random inspections of automated data sharing (§ 32 (7) BND Act). The BND is explicitly allowed to retain the search terms submitted by cooperation partners for two weeks in order to enable random checks. The shared search terms from partner services may also be probed by the BND to generate additional search terms for its own purposes (§ 32 (8)). After two weeks, the selectors are deleted automatically.

[64] See discussion in section 2.2.2 above on filtering of domestic data and other safeguards.
[65] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 258, https://data.guardint.org/en/entity/neb3eo8hl9h?page=68
[66] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 27, https://data.guardint.org/en/entity/neb3eo8hl9h?file=15978344731474zg14a5ky0w.pdf&page=38

Table 7: Retention rules in the context of data sharing

Authority	Data category	Retention rule	Legal provision
Data sharing	Data transfer to domestic authorities based on a preliminarily approved and then revoked warrant	Receiver shall be requested to delete the data immediately	**§ 29 (8) sentence 6**
	Shared personal data	Transferred data must be evaluated by the recipient, if deemed irrelevant, it must be deleted immediately, with some exceptions	**§ 29 (13); § 30 (9); § 38 (8)**
	Transferred bulk data in cooperations	Unevaluated retention up to six months	**§ 31 (4) number 3, littera h)**
	Erroneously transferred data in cooperations	The foreign public body must assure immediate deletion of wrongly transferred data as a prerequisite for the cooperation	**§ 31 (4) number 3, littera b) - d) and g)**
	Search terms from foreign intelligence services	Retention for two weeks	**§ 32 (8)**

Unevaluated bulk data

Beyond the collection and transfer of selector-based communications data, the BND now also has the legal mandate to process unevaluated data in the context of SIGINT cooperations (§ 33 BND Act). This includes the transfer of metadata and content in bulk to a foreign intelligence service. The constitutional court had explicitly demanded a separate statutory basis for this kind of exchange, because the BND ceases any control over how the partner service processes content.[67]

The same rules that apply to automated transfer of selector-based data summarized above, apply here, too. Additionally, the law requires to determine a so-called "qualified intelligence

[67] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 263, https://data.guardint.org/en/entity/neb3eo8hl9h?&page=68

need" (*qualifizierter Aufklärungsbedarf*) that justifies the sharing of bulk data. It lists the following six threats as lawful purposes (§ 33 (2) BND Act):

1. The preparation of an armed attack on Germany or EU and NATO member states, or the cooperating state
2. Preparing for terrorist attacks,
3. Proliferation of weapons of war on a specific route or with a specific destination
4. International criminal, terrorist or state attacks using malware on the confidentiality, integrity or availability of IT systems,
5. Investigation of disinformation campaigns targeted at Germany
6. Preparation of attacks that threaten Germany's security.

The "qualified intelligence need" must be declared in writing and assigned to a strategic bulk interception warrant for threat detection purposes.[68] The Independent Control Council must check the lawfulness of the declared intelligence need as a basis for the cooperation before the data is transferred. If the oversight body does not confirm the lawfulness of the proposal, the data must not be transferred (§ 33 (3) BND Act).

Authorization and Oversight

SIGINT data transfer

The Federal Government shied away from introducing a general independent approval power for transnational data sharing. It established, based on the guidelines of the Constitutional Court,[69] an ex ante approval power limited to data sharing related to communications of protected professions.[70]

The BND may share personal data from communications of protected professions, for example by journalists, if the judicial control body approves the transfer: It must weigh the foreigners' interests in protected confidential communications against the legitimate operational aims of the BND in its lawfulness test before data is transferred. Such a transfer of a lawyer's personal data would be allowed if evidence justifies the suspicion that the person in question may be the perpetrator or participant of a crime or if the transfer is necessary to prevent dangers to certain legal interests.[71] In case of imminent danger, a preliminary approval by one member of the oversight body suffices to permit the data transfer. If the decision is

[68] Cf. § 19 section 1 number 2 BND Act; section 2.2.2 of this report
[69] The court noted: "To the extent that the shared data includes data of journalists, lawyers or other professions meriting confidentiality protection, [...] it must generally be subject to ex ante oversight resembling judicial review," see: Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 240, https://data.guardint.org/en/entity/neb3eo8hl9h?page=63; cf. United Nations Office of the High Commissioner for Human Rights, Letter of the Special Rapporteurs of 29 August 2016, OL DEU 2/2016, p. 7, https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_DEU_2.2016.pdf
[70] §§ 29 (8) and 30 (9) BND Act in connection with § 42 (1) number 5 BND Act
[71] § 29 (8) in connection with § 30 (9) BND Act

later revoked, the BND shall request the deletion of the shared data (§ 29 (8) sentence 5 BND Act).

The Independent Control Council must also review, ex post, the repurposing of data. This can be the case if data that was first collected for information purposes is then transferred for threat prevention purposes.[72] Future case law will tell whether this rule on purpose changes satisfies the courts requirements for data sharing, including that lawmakers must create safeguards to ensure that undue purpose changes are excluded in principle.[73]

[72] § 30 (5) BND Act in connection with § 42 (2) number 2 BND Act
[73] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 177, https://data.guardint.org/en/entity/neb3eo8hl9h?page=48

3. New oversight framework

Building on the description of the three codified bulk powers of the BND, this section elaborates on the new oversight structure that the BND Act also established. Section 3.1 provides an overview of the institutional set-up and the specific focus and features of the new oversight mechanisms; followed by an analysis of the overseers' respective new control mandates (3.2).

3.1 Institutional set-up

3.1.1 Legal basis and scope

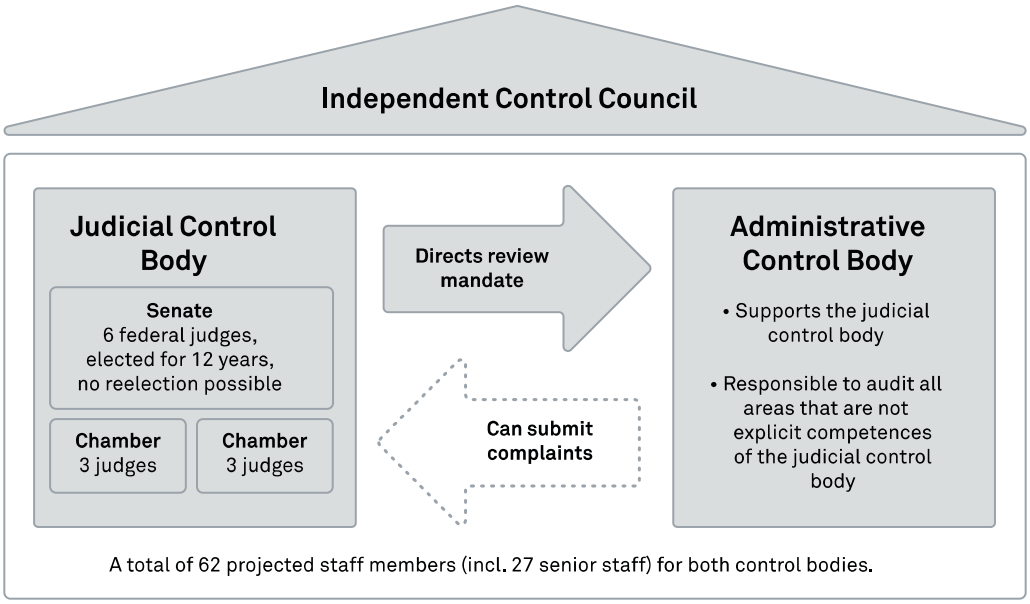
The constitutional court demanded that the amended legal framework must provide for two distinct types of oversight for the BND's SIGINT activities: judicial and administrative control.[74] It did not prescribe, however, whether these separate oversight functions should be performed by one or several bodies. The lawmakers decided to combine both tasks within just one new oversight institution, the Independent Control Council (*Unabhängiger Kontrollrat*), visualized in figure 3.[75] The Federal Government and the majority in parliament saw a unitary oversight body for the BND's SIGINT department as a precondition for continued international cooperation. They warned that, if too many oversight or review agencies would be involved, say a separate court for judicial review and a separate administrative control body, which might have involved the Federal Commissioner for Data Protection, foreign intelligence agencies might shy away from sharing information because of a fear that their data might not remain confidential.[76]

Foreign-domestic bulk interception measures, that is to say selector-based collection of communications that involve German citizens, residents or organizations, continue to be governed by a different legal framework and remain exempt from the mandate of the new ICC.[77] Despite this split legal framework and oversight regime for domestic and foreign collection of communications, according to the Federal Government, the new oversight

[74] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 274f, https://data.guardint.org/en/entity/neb3eo8hl9h?page=72
[75] The composition and mandate of this new oversight body are codified in paragraphs 40 to 58 of the BND Act.
[76] Explanatory Statement of the draft BND Act, 25.11.2020, p. 101
[77] The central legal norm is § 5 of the Article 10 Act on strategic foreign-domestic communications surveillance. These bulk interception measures continue to be subject to the, by now far less rigorous, quasi-judicial control of the G10-Commission.

framework guarantees a comprehensive control of signals intelligence (*technische Aufklärung*).[78]

Figure 3: The two bodies of the Independent Control Council



The judicial control body of the ICC consists of six federal judges, of which one serves as president and one as vice president of the Independent Control Council as a whole.[79] The second branch, called the administrative control body, must be headed by a fully qualified lawyer and is subject to the directions of the president of the ICC (§ 50 BND Act).

The new ICC replaces the previous oversight body for foreign intelligence collection created by the 2016 intelligence reform, a part-time body called the Independent Committee (*Unabhängiges Gremium*). The level of available personnel and resources for the new

[78] See answer to question 21 provided by the Federal Chancellery to a parliamentary inquiry: "Befugnisse und Kontrolle des Bundesnachrichtendienstes nach dem Urteil des Bundesverfassungsgerichts zur Auslands-Auslands-Fernmeldeaufklärung," 26.01.2021, no. 19/26120, https://dserver.bundestag.de/btd/19/261/1926120.pdf

[79] The first president of the ICC is Josef Hoch, who had already presided over the precursor oversight body, the Independent Committee. Vice president is Till Oliver Rothfuß, a former federal administrative judge. The other four elected members are: Johanna Schmidt-Räntsch, Elisabeth Steiner, Christian Tombrink und Dietlind Weinland. See: Deutscher Bundestag, press statement, 23.06.2021, https://www.bundestag.de/dokumente/textarchiv/2021/kw25-pa-pkgr-849378; Federal Government, press statement, 8.06.2021, https://www.bundesregierung.de/breg-de/aktuelles/bundesrichter-josef-hoch-zum-praesidenten-des-unabhaengigen-kontrollrates-ernannt-1925366

oversight council will increase significantly compared to the previous committee which consisted of only three persons.[80]

Table 8: Selected budget figures

Published BND budget[81]	Expected ICC budget[82]	Expected one-time costs
2013: € 531 million 2015: € 616 million 2017: € 833 million 2019: € 966 million 2021: € 1.079 billion	Annually: ~ € 11.6 million (Estimate included in explanatory statement)	BND: ~ € 450 million ICC: ~ € 5.0 million (Estimates included in explanatory statement)

The budget estimates show that the BND's budget will most likely continue to increase significantly in the coming years. In 2021, it surpassed the mark of one billion euros for the first time, after considerable annual budget increases over the past couple of years (doubling its budget since the Snowden revelations, see table 8). The Federal Government estimates that the implementation of the BND Act will produce one-time costs of about 450 million euro, and consecutively, also increased annual operational costs. Notice, though, that these figures are estimates published in the context of a legislative process and that the actual costs for implementing the new law and the concrete allocation of funds will be part of the budgeting process for 2022.

3.1.2 Requirements

Independence

Much like the European Court of Human Rights in its recent *Big Brother Wat*ch and *Centrum för Rättvisa* decisions, the German Constitutional Court also placed significant emphasis on the independence of the new oversight body from the BND and the Federal Government. According to the amended BND Act, the ICC is not bound by instructions from the Federal Government (§ 41 (3) BND Act), and it can define its own internal rules and procedures as well as its own oversight priorities and resources. The judges that form the judicial control body are elected for a term of 12 years and no reelection is permitted (§ 45 BND Act). The candidates for the six seats that form the senate of the judicial control body must be experienced federal judges that are proposed by the Federal Court of Justice

[80] The explanatory statement of the law outlines the projected costs for setting up and running the new oversight structure. It projects costs for 62 staff positions, including 27 senior staff members (*höherer Dienst*) for the Independent Control Council as a whole. With this, the amended law aims to address the stipulation in § 57 of the BND Act that the ICC should be endowed with adequate human resources and equipment.

[81] Figures retrieved from public federal budget: https://www.bundeshaushalt.de/#/2021/soll/ausgaben/einzelplan/0414.html

[82] Expected one-time and annual costs are only projections included in the draft law; see: Explanatory Statement of the draft BND Act, 25.11.2020, p. 4

(*Bundesgerichtshof*) and the Federal Administrative Court (*Bundesverwaltungsgericht*) and are elected by the parliamentary control committee of the Bundestag (§ 43 BND Act). The same rules that apply to ensure the independence of judges in Germany also apply to members of the judicial control body.[83] In addition, the six members of the judicial control body make their decisions in chambers of three judges. The composition of the two chambers must be changed every two years (§ 49 (2) BND Act). The administrative oversight body, as the second branch of the ICC, works under the direction of the judicial oversight body and is led by a legally trained civil servant.

Access to information

The oversight body will be based in Berlin and Pullach (Bavaria). There, the ICC enjoys comprehensive access to all BND premises and to all its IT systems as long as they are under the sole direction of the BND (§ 56 (3) BND Act). If the ICC requests access to data that is not under the BND's sole direction, the BND shall "take appropriate measures" to facilitate access (§ 56 (3) number 2 sentence 2 BND Act).

However, the law does neither include specifications of what such "appropriate measures" shall be and nor does it entail a duty to proactively inform the ICC about all operational systems and jointly administered databases with foreign services.[84] Moreover, the BND is not obliged to provide a comprehensive overview over the complex systems used to collect and process foreign intelligence.

It was a firm requirement by the Constitutional Court that the so-called "Third Party Rule" (also known as the originator control principle), the basic principle that intelligence services must not share any information they receive from foreign agencies with other – third – parties, may not undermine the effective and comprehensive oversight by the ICC. The judges pronounced that "the legislator must ensure that the Federal Intelligence Service cannot prevent oversight by invoking the third party rule."[85]

Hence, there continues to be a risk that there will be "unknown unknowns" for the independent oversight body as regards operational systems and data processing: The mandatory logging for audit purposes is required for a few selected cases of data deletion and purpose changes (see table 8), but the law does not foresee the mandatory recording of comprehensive audit trails. Plus, the limited audit logs that are required – for example if the confidential communications of a journalist that were unlawfully collected in a hacking operation are deleted (§ 35 (3) BND Act) – appear to be only accessible for review by the internal data

[83] For the rules concerning judicial independence, see the German Judges Act (Richtergesetz) paragraphs 25 and following: https://www.gesetze-im-internet.de/drig/BJNR016650961.html#BJNR016650961BJNG000500666

[84] Furthermore, the Federal Commissioner for Data Protection must be consulted before the BND creates new shared databases with foreign public bodies. See: §15 (1) sentence 4 and 5 BND Act.

[85] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 292, https://data.guardint.org/en/entity/neb3eo8hl9h?page=75

protection and compliance unit of the BND. The same is the case, for instance, if unevaluated bulk data is shared with a foreign intelligence service. The automated transfer must be logged, but only internal BND inspections may access these audit logs (§ 32 (6) and (7) BND Act).

Table 9: Overview of SIGINT audit log requirements

SIGINT activity	Audit log requirement
Deletion of data related to protected professional communications collected in bulk interception and hacking operations	**§ 21 (3) and § 35 (3)** Logging of the deletion and retention of the logs until the end of the second calendar year following the logging. **§ 21 (4) and § 35 (4)** Obligation to document decisions on whether a person is assigned to a protected professional group or not.
Encrypted data collected in suitability test	**§ 24 (6)** Logging of the deletion of encrypted personal data collected in suitability tests and retention of the logs until the end of the second calendar year following the logging.
Deletion of personal content data collected in bulk interception and hacking operations	**§ 27 (1) and § 34 (7)** Logging of the deletion and retention of the logs until the end of the second calendar year following the logging.
Deletion of data related to the core of private life collected in bulk interception and hacking operations	**§ 22 (2) - (3) and § 36 (2) - (3)** Logging of the deletion and retention of the logs until the end of the second calendar year following the logging.
Domestic and transnational sharing of personal data	**§ 29 (16) and § 30 (9)** The recipients, the legal basis for the data transfer and the date of the transfer must be recorded. The logs must be retained until the end of the second calendar year following the logging.
Transnational sharing of bulk data in cooperations	**§ 32 (6)** Logging of data transfers and retention of the logs until the end of the second calendar year following the logging.

Reporting
The work of the ICC ought to remain strictly confidential (§ 54 BND Act) and the BND Act does not impose a public reporting obligation upon the ICC.[86] Instead, it must report to the parliamentary oversight committee every six months (§ 55 (1) BND Act), but the content of these reports is not specified in the law. While the ICC is, at least formally, exempt from the Third Party Rule, the Federal Government continues to regard the parliamentary oversight committee as a third party in the context of information sharing. This has consequences for the ICC's reporting to the parliamentary committee: Only information that is under the exclusive control of the BND may be included. The ICC must consult the Federal Chancellery before reporting to the parliamentary committee, to ensure that the report does not comprise third party information (§ 55 (2) BND Act).

Oversight cooperation
The ICC may exchange views and compare notes with other domestic oversight bodies, namely the Federal Commissioner for Data Protection, the G10 Commission and the parliamentary oversight committee about oversight-related matters. In doing so, it must comply with the respective obligations to protect secrecy. There is no analogue reference to international oversight cooperation, for example in the context of the European intelligence oversight working group.[87]

3.2 Control competences

3.2.1 Judicial control body

The new control council is only competent to review the *lawfulness* of foreign SIGINT activities. In German administrative law, this involves an assessment of the formal and substantial legality of a given action. The evaluation of the utility of the BND's surveillance measures remains a prerogative of the executive. In order to encircle the independent control mandate, the BND Act includes a very specific catalogue of control competences for the judicial control body (§ 42 BND Act). The lawmakers distinguished between ex ante approval and ex post review competences that the judges may exercise (see table 9).

The list of oversight competencies includes the approval of bulk interception and computer network exploitation based on the warrants submitted by the BND. As outlined above, the bulk warrants are authorized by the president of the BND and the lawfulness of this authorization

[86] The Swedish intelligence oversight body, for example, has a duty to issue public reports that include review activities related to SIGINT. See, e.g. European Court of Human Rights, Centrum för Rättvisa v. Sweden, 25.05.2021, recital 352, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=79
[87] "Carter of the Intelligence Oversight Working Group" https://english.ctivd.nl/documents/publications/2019/12/12/index;
"Strengthening oversight of international data exchange between intelligence and security services" https://www.comiteri.be/images/pdf/publicaties/Common_Statement_EN.pdf

is then assessed by one of the chambers of three members of the judicial control body. The warrants have to state explicitly if the respective SIGINT measures, such as selector-based bulk interception or hacking operations, target certain groups such as EU citizens, journalists, lawyers or clerics. In addition, the judges need to validate the justification for automated bulk data transfers and the sharing of personal data related to protected professional communications in advance. They also make weighting decisions about the processing of data related to the core of private life, if the BND is unsure whether the processing is proportionate.

Table 10: Competences of the judicial control body

Ex ante approval of lawfulness of	**Ex post review of lawfulness of**

- SIGINT warrants (§ 23 (1))
- CNE warrants (§ 37 (1))
- Targeted data collection of
  - Data about EU citizens, EU institutions, and public bodies in EU member states (§ 20 (1))
  - Individuals to prevent threats or for transfer to law enforcement (§ 20 (2))
  - Members of protected professional groups (§ 21 (2))
- Automated transfer of bulk personal data (§ 33 (2))
- Processing of data related to the core of private life (§ 22 (3))
- Domestic and transnational transfer of data related to protected professional groups (§ 29 (8) and 30 (9) and 38 (8))
	- Processing of data related to protected professional groups (§ 21 (3) and 35 (3))
	- Domestic and transnational transfer of data collected for information purposes (i.e., change of purpose) (§ 29 (7) and § 30 (5) and 38 (7))
	- Internal regulations of the BND, e.g., regarding technical implementation of data processing (§ 62)
	- Formal complaints made by the administrative control department (§ 52)

The ICC's ex ante approval powers neither include the collection of foreign metadata nor the lawfulness of suitability tests. If the lawfulness of a bulk warrant is rejected by the judges of the judicial oversight body, the warrant expires (§ 23 (4) sentence 2 BND Act). Beyond that, the law does not prescribe concrete powers to deter unlawful warrants or to sanction non-compliance with legal safeguards. Also, if bulk warrants repeatedly feature the same boilerplate text or if BND staff do not cooperate adequately with the overseers, the judicial control body has no specified legal enforcement tools at its disposal which undermines their practice of effective review.

In addition, the judicial control body is, ex post, responsible for reviewing the lawfulness of the processing of data related to protected professional communications, the repurposing of data

that was initially only collected for information purposes, the BND's non-public internal regulations for data processing, as well es the complaints submitted by the administrative control body.

The legal norms do not specify what the control of lawfulness (*Rechtmäßigkeit*) must include in concrete judicial oversight practice. Consider the balancing of interests between the protections for journalists and the BND's general aim to gather foreign intelligence information: What determines its assessment and does the oversight body have the adequate information to arrive at a well-founded decision? An informed balancing of legitimate aims and safeguards requires substantial context information. The law remains unclear as to whether the warrants will contain sufficient material to assess the form and content of a proposed collection measure and how oversight staff are trained to fulfil their review tasks.

Warrants

The table below summarizes the different warrant types included in the BND Act. Some of the warrants are very specific in their scope of application, for example if they refer to the communications of EU citizens, EU institutions, and public bodies in EU member states (§ 42 (1) number 2 BND Act). Other bulk warrants, such as the general foreign bulk collection warrant and the CNE warrant may be broader in their scope of application and may cover a "topic" related to a "geographical focus" for an unspecified period of time. Some warrants are also generally missing, but have been included in other SIGINT frameworks, such as examination warrants[88] and testing and training warrants.[89]

[88] United Kingdom Investigatory Powers Act, section 158, regarding bulk acquisition warrants authorizes both the collection of communications data in bulk from a telecommunications operator *and* the selection for examination of the data obtained under the warrant (see: https://data.guardint.org/en/entity/jqw6xmbdk4b?page=142); more examples for warrant types and bulk warrant criteria: https://www.intelligence-oversight.org/phases/application-process/

[89] New Zealand Intelligence and Security Act 2017, Subpart 3, practice warrants, https://www.legislation.govt.nz/act/public/2017/0010/latest/whole.html#DLM7118938

Table 11: Warrant types and legal basis in the BND Act

Warrant type	Legal provision
Foreign bulk collection warrant	§ 23 (1) BND Act in connection with § 19 (1) BND Act
Special bulk collection warrants: **EU warrant:** Targeted collection of personal data of bodies of the EU, public bodies in the member states of the EU or EU citizens **Threat prevention warrant:** Target collection of personal data of individuals to prevent threats or for transfer to law enforcement **Professional secrecy warrant:** Targeted collection of personal data related to protected professional communications	§ 23 (5) BND Act in connection with § 20 (1) BND Act § 20 (2) BND Act § 21 (2) BND Act
Computer network exploitation warrant	§ 37 (1) BND Act in connection with § 34 (1) BND Act
Testing and training warrant	Not required under the BND Act
Data examination warrant	Not required under the BND Act.
Data transfer warrant	Not required under the BND Act.

Next to the warrants listed in table 10, the judicial approval of bulk data transfers is a notable novelty in the amended Act. The lawful justification of a "qualified intelligence need" for automated transfer of unevaluated bulk data to a foreign intelligence agency is now subject to independent judicial approval.[90] With this approval power, the legislator implements, again, a specific requirement put forward by the Constitutional Court. It had declared that "the sharing of an entire set of traffic data cannot be authorised continually and merely on the basis of the purpose pursued but requires a qualified need for intelligence relating to specific indications that a specific danger may emerge."[91] The judicial oversight body has to make an assessment whether the need for intelligence is lawful, otherwise the raw bulk data may not be shared (§ 33 (3) BND Act).

[90] § 33 (1) BND Act in connection with § 31 BND Act
[91] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 263, https://data.guardint.org/en/entity/neb3eo8hl9h?page=68

Search terms

It is not required to list individual search terms in the bulk interception warrants (§ 23 (6) sentence 2 BND Act), which in practice exempts most search terms from ex ante approval of legality. Only specific categories of search terms that target, for example, EU citizens or journalists, are subject to ex ante approval of the judicial control body (§ 42 BND Act). Other selectors that do not target one of the specifically protected categories such as confidential professional communications, cannot be checked prior to their use. Search terms that are not approved based on a warrant, can, however, be reviewed at random by the administrative control body (see table 11 below).

The explicit exclusion of most search terms from ex ante approval raises the question whether all the search terms used by the BND are stored and made accessible for independent oversight purposes. Some selectors might only be used for short periods of time, and the BND Act does not include a provision that requires their retention for ex post review. In this regard, the BND Act might be at odds with the jurisprudence of the European Court for Human Rights (ECtHR). In its first assessment of the Swedish bulk collection regime, the court acknowledged that applications for strategic surveillance measures "must specify not only the mission request in question and the need for the intelligence sought but also the signal carriers to which access is needed and the search terms – or at least the categories of search terms – that will be used."[92]

Weighting decisions

What qualifies as protected communications, for example of an attorney who communicates with a client? And under what conditions might the BND still be allowed to monitor these communications? The Constitutional Court requires "in any case [that] ex ante oversight resembling judicial review must in principle ensure that such relationships are protected."[93] Despite this clear demand, the BND Act does not provide for ex ante oversight of the classification decision on what is regarded as a confidentiality relationship and which individuals enjoy protection in the first place. This initial decision, which is the basic precondition, is not subject to the approval powers of the judicial control body and can only be reviewed ex-post by the administrative control body. There is, though, an ex ante approval competence for decisions on exceptions to the protections of professional groups.[94]

What is more, incidental collection of protected professional communications, for example if a journalist is communicating with the target of a surveillance operation about a topic without foreign intelligence relevance, can never be fully prevented. The BND Act addresses this problem by clarifying that insofar as the collection of data from confidentiality relationships is only noticed during data analysis, the BND must check whether collection of this data would

[92] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 19.06.2018, recital 139, https://data.guardint.org/en/entity/tivrjsdq1ei?page=43
[93] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 194, last sentence, https://data.guardint.org/en/entity/neb3eo8hl9h?searchTerm=157&page=53
[94] § 42 (1) number 2 in connection with § 23 (5) number 3 BND Act

have been materially permissible according to the requirements illustrated in the section above. That means, further processing of the incidentally collected data is allowed if it serves to prevent serious crimes and dangers (listed in § 21 (2) BND Act). This decision is then subject to ex post reviews by the judicial control body.

3.2.2 Administrative control body

Contrary to the specific control competences of the judicial control body, the BND Act bestows a vague mandate upon the administrative control body. Given that the constitutional court saw the need to establish a "continual legal oversight that allows for comprehensive access,"[95] the BND Act remains surprisingly silent on the actual remit, the process, the tools and the overall objective of the ICC's administrative control body. The Act merely states that the administrative control body shall support the work of the judicial control body and is responsible for auditing all SIGINT activities that are not explicit competences of the judicial control body (§ 51 (1) BND Act). Hierarchically, it is subordinated to the judicial branch of the ICC.

Due to its vague mandate, it also remains unclear to what extent the control competences of the Federal Commissioner for Data Protection and the administrative control body overlap. The amended law also does not foresee any independent review of the data minimization systems (filters) used by the BND. This unspecific review mandate bears the risk that the administrative control body needs to constantly justify its oversight competence and oversight priorities. It could also be an advantage, though, if a review mandate is rather broad, if it allows for unannounced inspections and independent investigations.

In the context of data sharing, the accuracy and veracity of the automated checks and filtering of search terms must be subject to random checks by internal BND staff, but not the administrative control body (§ 32 (7) BND Act). The independent overseers also do not have an explicit mandate to check the block lists that the BND needs to maintain to filter out protected professional communications before sharing data (§ 32 (5) BND Act).

[95] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 272, https://data.guardint.org/en/entity/neb3eo8hl9h?page=71

Table 12: Competences of the administrative control body

Review mandate	Power to file formal complaints
- Supports the judicial control body and is responsible for all areas that are not explicit competences of the judicial control body (§ 51 (1)) - Its specific review mandate is defined by the judicial control body (§ 51 (2)) - It can review the lawfulness of search terms, if the judicial control body is not competent to do so (§ 51 (1) sentence 2)	- If it detects an unlawful situation, it can file a formal complaint - The BND and the Chancellery must be consulted in the process - The final decision about the complaint is made by the judicial control body

Complaints

The administrative control body has the legal standing to initiate a formal complaint procedure (*Beanstandung*) if it identifies unlawful conduct, such as non-compliance with certain legal protections in data processing (§ 52 BND Act). The administrative control body must first consult with the BND before it initiates a formal complaint. If the cause for complaint is not eliminated, it may bring the complaint to the attention of the Federal Chancellery. If the Chancellery does not rectify the cause of the complaint, the judicial control body gets to finally decide how to handle the complaint, but it is not specified in the law what the legal consequences of this final decision shall be.

4. Discussion and assessment

Having primarily explained the key regulatory changes to German legislation on foreign intelligence in response to the Constitutional Court's landmark decision, the focus now turns to an assessment of those changes. For this, the text first elaborates on aspects the authors consider laudable improvements (4.1). Next, it accounts for missed opportunities and what the authors consider to be poor legislative practice (4.2). Each section features arguments that refer to the *quality of the legal framework*, the degree of *fundamental rights protection* and the *authorization and oversight process*.

As indicated, the discussion draws on the authors' subjective reading of the reform. They very much encourage direct feedback and acknowledge upfront that their account does not claim to be exhaustive. They hope to contribute, however, to more inclusive debates in like-minded democracies on the evolving authorities, safeguards and governance processes for government surveillance including standards regarding transnational data transfers.

4.1 Improvements of the status quo

4.1.1 Quality of the legal framework

More comprehensive and transparent legal framework

When compared to previous intelligence reforms but also with a view to how other democracies have codified (or not) foreign intelligence collection in their respective laws, Germany has undoubtedly come a long way with the 2021 reform of the BND Act.[96] With this reform, it cements its position among the few democracies in the world that offer comprehensive legislation and key safeguards regarding the use of bulk powers for foreign intelligence collection.[97]

Not only did bulk collection receive a far more comprehensive legal footing, (bulk) computer network exploitation is now also explicitly recognised and codified as state practice. In

[96] See, for example, the online repository of good legal provisions and oversight practice regarding bulk collection: www.intelligence-oversight.org. As regards Germany's post-Snowden intelligence reform trajectory, see, for example, Wetzling, Thorsten, 2020.

[97] For a rare public statement on the general availability of legal protections against government surveillance and oversight frameworks, see the 2018 report of the UN Special Rapporteur of the right to privacy to the UN Human Rights Council, notably page 27. "More than 80 percent of the United Nations Member States do not have any law which protects privacy by adequately and comprehensively overseeing and regulating the use of domestic surveillance […]. The situation relating to foreign intelligence is much more fluid, elastic. What actually constitutes a necessary and proportionate measure in a democratic society […] is still very much work-in-progress all across Europe […]. Even where legislation exists regarding the oversight of intelligence it is often largely silent on what happens when personal data is shared across borders and what further safeguards should be put in place in such cases" (UN Human Rights Council, 2018).

addition, the BND Act now features probably one of the world's most detailed legal frameworks regarding the dos and don'ts when it comes to (automatic) international data transfers, with separate chapters devoted to their authorization, documentation and corresponding judicial and administrative oversight, including specific obligations on the part of the BND to restrict the subsequent use of shared data by partner services.

The following two examples illustrate further why and how the legal framework for foreign intelligence collection has improved significantly.

First, the BND Act now features new and more comprehensive rules on aspects that were previously dealt with in classified executive decrees (*Dienstvorschriften*). This includes provisions on the exceptional processing of data of specially protected persons – which should have been deleted immediately but are used nevertheless – where the Constitutional Court called for a reformed set of regulations which needs to be subjected to parliamentary approval and receive proper statutory footing.[98] This gap has now been fixed. Likewise, whereas the previous quasi-judicial oversight body, the Independent Committee, did not have full access to the executive decree relating to data transfers to foreign partner services, this has now been changed and a number of the provisions from that executive decree have found their way into the BND Act.

Second, the BND Act now includes detailed provisions with respect to standing SIGINT cooperation with foreign partner services, ad hoc data transfers and jointly administered databases with foreign partner services to name just a few dimensions. Each aspect now received a more comprehensive legal footing. Consider, for example, the fact that eight (!) binding assurances (on different data use aspects) now have to be included in written MoUs that the BND signs with foreign partners (§ 31 (4) number 3, littera a-h BND Act). Furthermore, as regards standing SIGINT cooperation agreements, the BND is now under the legal obligation to verify in an automated way whether the transmission of the data collected would conflict with the national interests of the German state (§ 32 (3) and (4) BND Act). Also, as regards protected professional communications and international SIGINT cooperation, the BND must maintain block lists of identifiers of journalists, lawyers or similar persons or groups whose communications are afforded special confidentiality protection in order to gradually improve the filter accuracy (§ 32 (5) BND Act).

4.1.2 Fundamental rights protection

Extraterritorial reach of fundamental rights no longer disputed

Probably the single most important bone of contention with previous reforms of foreign intelligence legislation was the hitherto open question, whether or not the territorial reach of the right to private communication and press freedom as guaranteed under Article 10 and

[98] Federal Constitutional Court, BND Act Judgement, 19.05.2020, recital 174, https://data.guardint.org/en/entity/neb3eo8hl9h?page=48

Article 5 of the German constitution extends beyond German territory and beyond German nationals and residents. While the German government argued consistently up until May 2020 that it does not, the Constitutional Court unequivocally affirmed that these fundamental rights are human rights and not citizen rights. It held that the German state's obligation to protect these fundamental rights cannot be restricted to cover only certain groups of people or only some geographical regions. In turn, this required a wholesale amendment of both the legal framework and the remit of German intelligence oversight institutions.

In practice, however, as argued further below, this does not mean that foreign nationals now enjoy the same de facto protection from electronic surveillance by the BND or that the pathway to effective remedy for a German citizen equals that of a non-national.

Enhanced protection for journalists, lawyers and clerics
When compared to previous legislation, the amended BND Act now offers improved protections as regards the communications of foreign professionals who require greater confidentiality. Following the landmark judgement, the drafters of the reform had to accept the premise that foreign journalists, for example, have a special right to have their communication data exempt from bulk surveillance measures. By itself, this is an important step in the right direction, despite significant criticism that ought to be voiced as regards the implementation of this premise (see the discussion in section 2.2.2 on the many exceptions and their room for improvement).

4.1.3 Authorization process and oversight

Judicial oversight of foreign intelligence collection
Whereas the previous reform went the extra mile to prevent it, the 2021 reform had to finally establish a proper judicial review body – the Independent Control Council – in Germany. Unlike its predecessor, the Independent Committee, the ICC will have recourse to roughly sixty full-time staffers and a much greater budget, at least according to the projections made in the explanatory statement of the new law.[99] Its judicial branch is responsible for a wide range of legality reviews, many of them ex ante (see the catalogue in § 41) and will consist of six federal judges to be appointed for twelve years – both important preconditions for the ICC's independence.[100]

Improved oversight access and logging requirements
At least de jure, the amended BND Act also establishes a much improved access for the judicial oversight body to the IT systems and operational databases of the BND. Whether this

[99] Explanatory Statement of the draft BND Act, 25.11.2020, p. 4
[100] Structurally, the ICC fulfils all basic requirements for independence, such as rules on conflict of interest; discretion over its budget and staff and fixed terms of office. Time will tell whether operational independence in oversight practice will also be guaranteed. For more criteria on independence of oversight, see: Murray et al., 24.05.2021, p. 10.

is sufficient to allow for data-driven intelligence oversight using new supervisory technology needed for 21st century audits will be discussed further below. Fact is, however, that concerns about the Third Party Rule can no longer prevent the independent judicial oversight body from accessing such information. In addition, the various provisions that now require logging (e.g., to protect the core area of private life or the protected communications of certain professions) combined with an obligation to promptly delete such data gives further substance to the remit of the administrative branch of the ICC.

In sum, the 2021 reform of the BND Act improves the democratic legitimacy, the transparency and the legal certainty of foreign intelligence collection. Other parliaments might find it insightful, it is hoped, to consider in particular the comprehensive catalogue of data transfer requirements and the robust institutional independence of the ICC.

4.2 Missed opportunities and the need for further reform

The German government, it ought to be remembered, has tried hard to prevent many aspects of the 2021 reforms which only came into being as the result of strategic litigation. Unsurprisingly, then, it could have gone much further to rectify the many grave deficits that became apparent in the litigation process. The next section aims to show why the 2021 reform, taken together, did not establish a model legal framework for foreign intelligence collection.

4.2.1 Quality of the legal framework

Fragmented legal framework

Unlike other democracies, such as the UK or Canada, Germany sports far too many individual pieces of intelligence legislation.[101] German lawmakers tend to focus primarily on the individual security service at hand and have thus far shied away from a more functional approach that focuses instead on the general nature of investigatory powers that the state may use to obtain access to different types of data – irrespective of which agency then deploys them. Given that more and more powers and software converge across the security sector, the Bundestag's approach to intelligence reform has done very little to improve legal clarity. Instead, new reforms add to the sheer complexity of the subject matter by inserting various new cross-references to similar yet still different provisions in other laws.

It is also increasingly questionable whether this approach – which requires the establishment of (too many) separate oversight mandates for (too many) oversight bodies – is compatible with important international obligations. As observed recently by the Dutch intelligence oversight bodies CTIVD and TIB in their memo on the Council of Europe's modernised

[101] Interested readers are invited to contact the German Parliament to obtain a copy of the (by now outdated) "Gesetzessammlung: Rechtsgrundlagen für die Tätigkeit und die Kontrolle der Nachrichtendienste des Bundes (September 2018)." It features 31 separate pieces of legislation.

Convention 108, "when appointing the oversight body/supervisory authority (i.e. Article 11.3, 15, and 16(2) of the Convention), it must be clear that the entire national security domain falls under the responsibility of the oversight body or bodies to be appointed."[102] This is certainly not the case in Germany where very different oversight entities work with very different resources, tools and mandates to ensure different types of government accountability for the military, intelligence and police forces' use of investigatory powers. More specifically, not only is the pursuit of bulk collection and computer network exploitation by the German armed forces subject to different oversight bodies (and control densities), even the BND's own bulk collection is still overseen by two separate judicial bodies. More specifically, the G10-Commission's remit under the Article 10 Act covers foreign-domestic bulk collection whereas the ICC's mandate under the BND Act is to review the legality of the bulk collection of foreign-foreign traffic. While the Federal Government sees no problem with this at present,[103] consider how the new Canadian oversight body NSIRA reports on its "additional and novel mandate to review any activity in the federal government that relates to national security or intelligence. […] This allows NSIRA to break down the *previously compartmentalized* approach to review and accountability, and replace it with horizontal, in-depth interagency review."[104]

Against this backdrop and knowing that the Constitutional Court's judgement pointed only to minimal standards that had to be implemented in order for Germany to have a constitutional framework for foreign intelligence, the reform could and should have aimed for more. Arguably, the drafters of this reform did not seize the unique and timely chance to pursue a more ambitious reform consolidated and clear legal framework on Germany's investigatory powers. Instead, it added to the complexity of German intelligence law which leaves it to the 20th Bundestag, for example, to extend the mandate of the ICC to other investigatory powers and – at the very least – to codify the BND's bulk collection powers in one single piece of legislation and to work against undue duplications both in the authorization and oversight process.

Disconnect with recent European jurisprudence

Those who amended the BND Act in March 2021 should have paid more attention to the October 2020 jurisprudence of the European Court of Justice (CJEU) on security and intelligence legislation in the United Kingdom and France. What is more, relevant insights on opportunities for future reforms can now also be gleaned from the European Court of Human Rights (ECtHR) Grand Chamber judgements on surveillance legislation in the United Kingdom and Sweden that were delivered in May 2021.

---

[102] Source: TIB and CTIVD memo on Convention 108, https://english.ctivd.nl/documents/publications/2021/02/17/memo-en. For a more detailed discussion on the relevance of Article 11 of this modernised Convention for democratic intelligence in Europe, see: Wetzling, Thorsten and Dietrich, Charlotte, 2021, "Report on the need for a guidance note on Article 11 of the modernised Convention," https://rm.coe.int/t-pd-2021-6-draft-guidance-note-on-exceptions-under-article-11-of-the-/1680a2d512

[103] Answer of the Federal Government to the minor interpellation 19/2583, p.5 https://dserver.bundestag.de/btd/19/261/1926120.pdf

[104] National Security and Intelligence Review Agency, 2020, p. 16, our emphasis.

First, the discussion draws on pertinent insights from the CJEU's *Privacy International v. Secretary of State*[105] and *La Quadrature du Net and Others v. Premier Ministre and Others* case.[106] Next, the focus turns to important insights from the ECtHR's judgement in the *Centrum för Rättvisa v. Sweden* case.[107] Both discussions reveal incompatibilities of the amended BND Act with the criteria and requirements put forward by the Luxembourg and Strasbourg Courts.

With regard to the CJEU's *Privacy International v. Secretary of State* case, the Court did not pronounce on foreign intelligence legislation specifically but it did clarify that "a legislative measure [...] on the basis of which the competent national authority may require providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission [...] exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society."[108]

This ruling, then, casts severe doubt on the compatibility of § 24 (4) of the BND Act which – as part of the rule set on so-called "suitability tests" (see the discussion in section 2.2.1) – embodies such a "legislative measure" that allows for "general and indiscriminate transmission" of data. Suitability tests are an exception to the general rule that content data may only be collected in bulk on the basis of search terms (§ 19 (5) BND Act). If the BND wants to perform suitability tests in order to generate new search terms or to assess the relevance of existing search terms, there seems to be no requirement for a written order by the president of the BND nor does the requirement that these tests may only be performed if factual indications exist that the selected telecommunications networks bear appropriate data for the purposes of strategic foreign surveillance seem to apply. What is more, there is no requirement, as is the case in some other democracies,[109] for the ex ante authorization involving independent oversight bodies nor is the duration and the volume of the data collection in pursuit of suitability tests subject to clear limitations or ex post reviews.[110]

---

[105] Court of Justice of the European Union, Privacy International v Secretary of State, 06.10.2020, https://data.guardint.org/en/entity/35ernv51jnp

[106] Court of Justice of the European Union, La Quadrature du Net and Others v Premier Ministre and Others, 06.10.2020, https://data.guardint.org/en/entity/20gb4kvky39j

[107] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 25.05.2021, https://data.guardint.org/en/entity/wdwrxl9tv6f

[108] Court of Justice of the European Union, Privacy International v Secretary of State, 06.10.2020, recitals 78-81, https://data.guardint.org/en/entity/35ernv51jnp

[109] According to "Part 4 Authorisations - Subpart 3 - Practice Warrants - Section 91 - Application for issue of Practice Warrant" New Zealand's Intelligence and Security Act 2017 establishes a detailed authorization procedure for testing and training warrants that involves the Chief Commissioner of Intelligence Warrants und des Inspector General. Available at: https://www.legislation.govt.nz/act/public/2017/0010/latest/whole.html#DLM7118938

[110] While there is no limitation rewarding the volume of traffic that may be collected by means of so-called suitability tests for either purpose, only the suitability test according to purpose 1 is subject to a

Against this backdrop, it is highly questionable whether the obligation under § 24 (4) BND Act which compels service providers to assist in suitability tests when their assistance is deemed necessary, can be considered within the limits of what is strictly necessary and thus justified, within a democratic society. Rather, the authors see therein an unduly broad obligation on the part of service providers to transmit "data to the security and intelligence agencies by means of general and indiscriminate transmission."[111] Taking into account the fact that the BND may transmit data from suitability tests automatically in bulk to the German Armed Forces and given that data collected in pursuit of a suitability test may, under certain exceptions, also be processed for purposes other than testing, for instance if factual indications suggest a grave threat, casts further doubt on the compatibility with EU case law.

Furthermore, consider the CJEU's finding that "since general access to all retained data, regardless of whether there is any link, at least indirect, with the aim pursued, cannot be regarded as being limited to what is strictly necessary, national legislation governing access to traffic data and location data must rely on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data at issue." With this in mind, and recalling the CJEU's logical conclusion that "those requirements [then] apply, a fortiori, to a legislative measure [...] on the basis of which the competent national authority may require providers of electronic communications services to disclose traffic data and location data to the security and intelligence agencies by means of general and indiscriminate transmission," the question arises whether the requirements that the CJEU formulated with respect to data retention in the QDN case, should equally apply to all legislative measures that compel service providers to transmit data in bulk to the security and intelligence services. If the same reasoning were to be applied to the provisions in the BND Act by which service providers can be compelled to cooperate with the BND, they would very likely be viewed as obligations to transmit personal data in a general and indiscriminate manner not limited to what is strictly necessary in a democracy.

Moreover, in the LQDN case, the CJEU stipulated that the following categories of decisions by security and intelligence services ought to be subject to an independent court's or administrative body's jurisdiction:

- a decision giving an instruction to providers of electronic communication services to carry out general and indiscriminate retention of data (paragraph 139);

six months time limit, which may also be renewed for an unspecified number of times for further six months (§ 24 (2) sentence 2 and 3 BND Act).

[111] Even more so, since, more generally, the new rules on the remit of the new judicial oversight body do not specify whether it has jurisdiction over decisions by the Federal Government to issue technical capability notices (as they are called in the Investigatory Powers Act) to service providers in accordance with § 25 BND Act.

- decisions on national security grounds requiring providers of electronic communication services to retain general and indiscriminate traffic and location data (paragraph 168)
- decisions authorising automated analysis (paragraph 179);
- the sharing of real time traffic and location data (paragraph 189);
- national rules which authorise automated analysis (paragraph 192).

And, as argued by the Court in the PI case, safeguards governing the interaction between service providers and security and intelligence service that apply to data retention should, *a fortiori*, also apply to the interaction between intelligence agencies when it comes to data transfers between them.[112] By analogy this would require that orders according to § 25 BND Act would also have to be added to the explicit competence catalogue of the judicial oversight body. At present, it seems that such decisions "giving an instruction to providers of electronic communications services to carry out such [transmissions are not] subject to effective review, [n]either by a court [n]or by an independent administrative body."[113]

Whether or not some of the other enumerated decisions are sufficiently subject to the jurisdiction of the ICC and whether the CJEU requirements should at all apply to the BND Act is a matter that requires further consultation.[114] At present, the ICC does not seem to have jurisdiction over decisions by the Federal Government that compel service providers to retain data. The BND Act provides evaluation intervals for the general retention of the personal data the BND stores, however (see e.g. table 4, mandatory evaluation after seven years for bulk interception, § 27 BND Act). As argued above, the BND Act also allows for the automated transfer of data from suitability tests to the German Armed Forces without granting the ICC an explicit review mandate in this regard.

Gaps in comparison to ECtHR standards

While the ECtHR has in principle accepted the compatibility of the Swedish foreign intelligence framework with the European Convention on Human Rights, it nonetheless alluded to a range of relevant criteria in its *Centrum för Rättvisa* decision which the BND Act might also be tested on in the future. For instance, the judgement noted that "relevant safeguards against arbitrariness" should be included in the independent ex ante authorization procedure. To achieve this, the Swedish bulk interception law "provides for the mandatory presence of a privacy protection representative at that court's sessions, except in urgent cases. The representative, who is a judge, a former judge or an attorney, acts independently and in the

[112] Court of Justice of the European Union, Privacy International v Secretary of State, 06.10.2020, recital 79, https://data.guardint.org/en/entity/35ernv51jnp?page=19
[113] Court of Justice of the European Union, La Quadrature du Net and Others v Premier Ministre and Others, 06.10.2020, https://data.guardint.org/en/entity/20gb4kvky39j?page=40
[114] See, for example, the discussion in German by Müller and Schwabenbauer (2021).

public interest but not in the interest of any affected private individual. He or she has access to all the case documents and may make statements."[115]

The BND Act does not foresee a similar "safeguard against arbitrariness"[116] when it comes to the approval processes of the ICC. That is, it does not include systematic "points of friction"[117] – such as a privacy protection representative, some kind of adversarial council, advisory body or similar outside perspectives that serve to harden the authorization mechanism against regulatory capture. Thus far, the judicial control body only hears the perspective of the BND when reviewing the lawfulness of bulk warrants. But a judicial review procedure is meant to weigh contrasting interests before coming to a conclusion. In order to establish a more "court-like" (*gerichtsähnlich*) review when deciding on surveillance operations in practice, the perspective of those affected by surveillance needs to be strengthened procedurally. In light of the special protections for certain professional groups, for example, it might be a profitable approach to involve adversarial representatives that argue in the interests of affected groups, such as protected professions or other vulnerable demographics.[118]

In addition, the ECtHR also emphasized that any independent authorization process "implies necessity and proportionality analysis"[119] and goes on to underscore that it might be difficult for the judicial approval body "to appreciate the proportionality aspect where only categories of selectors are specified"[120] in applications for bulk interception. Against this backdrop, the fact that no individual search terms or descriptions of categories of selectors must be listed in the bulk warrants (§ 23 (6) sentence 2 BND Act), calls into question whether the ECtHR would be satisfied with the judicial approval process pursuant to the new BND Act. In practice, the several hundred thousand search terms used by the BND are exempt from ex ante approval of legality, which substantially weakens the required assessment of necessity and proportionality.

Moreover, the ECtHR's *Rättvisa* judgement also examined whether the Swedish ex post oversight body, the Foreign Intelligence Inspectorate (SIUN),[121] is adequately equipped to assess aspects of the proportionality of the interference with the rights of individuals in SIGINT activities. It considers that SIUN conducts "numerous detailed examinations of, in particular, the selectors used" and that "it is tasked with granting the FRA access to communications

[115] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 25.05.2021, recital 297, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=79
[116] Ibid.
[117] Murray et al., 24.05.2021, p. 12
[118] Also consider this statement on the merit of adversarial voices: "to avoid being a rubber stamp, the process needed an adversary [...] to challenge and take the other side of anything that is presented to the FISA Court [...] anybody who has been a judge will tell you that a judge needs to hear both sides of a case before deciding" (Bradford Franklin, Sharon, 29.05.2020).
[119] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 25.05.2021, recital 299, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=79
[120] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 25.05.2021, recital 301, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=80
[121] Statens inspektion för försvarsunderrättelseverksamheten (SIUN), http://www.siun.se/index.html

bearers after verifying that the requested access corresponds to the permit issued by the Foreign Intelligence Court."[122] The BND Act does not provide for direct access to bearers of communications for the ICC, nor does it foresee a similar double verification of approved warrants. The ability to unblock particular bearers and to grant access to specific cables or facilities after checking a warrant is a powerful control competence that would significantly shift the power dynamic between the BND and the ICC compared to what is currently foreseen in the law.

If it identifies undue SIGINT conduct, the Swedish Foreign Intelligence Inspectorate can also decide – with binding effect – "that the collection must cease or that recordings or notes of collected data must be destroyed."[123] By contrast, whether and to what extent the complaint mechanism available to the administrative control body of the ICC (§ 52 BND Act) may have binding consequences for the BND is not specified in the BND Act. In addition, the Swedish oversight body itself is subject to audits by the Swedish National Audit Office that evaluates whether the oversight activities made a difference and how it could be improved.[124] The evaluation of the effectiveness of the ICC's oversight, in turn, is conducted mostly inward-looking by the ICC itself (§ 61 BND Act). Overall, neither the judicial, nor the administrative control body of the ICC seem to fully match the oversight competences and level of access to data that the Swedish SIGINT law provides and that the ECtHR deemed relevant to allow for an effective independent assessment.

Data purchases remain insufficiently regulated

While the BND Act covers foreign intelligence collection mainly, there certainly can be instances where it receives larger datasets from individuals, such as informants or company owners who have voluntarily handed this to them. What is more, the BND may purchase datasets on the open market or in less open corners of the web. The rules that should govern the access and subsequent use of data resulting from these kinds of purchases or gifts, and whether and how to involve independent oversight in the process, are not yet settled in the legal framework. Put differently, the current BND Act does not seem to include a provision on the governance and oversight of the service's purchase of commercially available data. By contrast, the UK's intelligence oversight body IPCO seems to be following this lead more attentively, when it states that it has conducted "an extensive review of bulk datasets held by third parties to which UK intel community had access", so as "to provide assurance that BPD (bulk personal dataset) warrants were being obtained where applicable."[125] Germany has not established bulk personal dataset warrants. As with bulk interception of foreign-foreign telecommunications, where the Federal Government has long tried to argue that no specific

[122] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 25.05.2021, recital 347-348, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=89
[123] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 25.05.2021, recital 350, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=90
[124] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 25.05.2021, recital 54, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=16
[125] IPCO/OCDA, 2020, para 2.29, p. 13, https://data.guardint.org/en/entity/v6vk5dcc88?page=14

provisions were necessary because of the BND's general mandate (§ 1 (2) BND Act), it can be said that unspecified regulation for such bulk data purchases exist. Yet, even the general provision in paragraph 1 section 2 of the BND Act covers only the collection and analysis of information, and one should argue that purchases cannot be sufficiently subsumed under this norm in the absence of further, more detailed provisions on the process, safeguards and oversight.

Ineffective data volume limitation

Other intelligence laws, such as the Article 10 Act include volume limitation based on transmission capacities within individual telecommunication networks. For the BND Act, lawmakers decided to adopt a more abstract limit based on entire telecommunication networks. They argued that the BND might want to collect all data from a specific telecommunications network in its entirety, in some cases. For example, if a foreign state uses its own network for communication between public bodies.[126]

The amended BND Act limits the amount of data that the service may collect to no more than 30 percent of the transmission capacity of all globally existing telecommunications networks (§ 19 (8) BND Act). Whether this rule implies an actual limit to bulk interception has been subject to debate during the policy making process. Eco, a business association of internet service providers, argued that 30 percent of all global telecommunications networks does not constitute a verifiable limit in their official commentary on the draft law. They explained that about 70.000 communications networks participate in international data traffic, which would mean that targeting roughly 20.000 networks would be permissible under the BND Act. In Germany alone about 1.250 carriers are linked to the internet. The legal volume limitation would consequently permit data collection up to a volume of 16 times the entire data traffic in Germany. Since a small number of larger telecommunication networks have a dominant share in overall data traffic, the ten largest providers typically carry about 95 percent of all data transmissions, the 25 largest networks transmit roughly 99 percent.[127] Thus, whether the volume limitation rule pursuant to paragraph 19 section 8 qualifies as a sufficient limit of bulk interception is questionable. Taking into account that the BND's technical and financial capacities will hardly suffice to get close to such an abstract data collection cap, the defined legal maximum will most likely remain a rather hypothetical construct with little practical value.

4.2.2 Fundamental rights protection

No redress mechanism for foreigners

It is a fundamental deficiency of the German foreign intelligence framework that the BND Act excludes effective ex post redress mechanisms against foreign surveillance by the BND.

[126] Explanatory Statement of the draft BND Act, 25.11.2020, p. 66
[127] eco, Official Statement on the draft BND Act, 18.02.2021, p. 3, https://www.bundestag.de/resource/blob/823354/a8060be2f61786ee68a7baec7be153e9/A-Drs-19-4-731-E-data.pdf

International case law has repeatedly emphasized the significance of individual remedies: Both the British and the Swedish bulk interception regimes, which were recently assessed by the ECtHR, feature concrete, codified mechanisms for "ex post facto review" of bulk interception.[128] The CJEU has demanded more effective remedy options for EU citizens regarding data processing by US intelligence agencies in its Schrems II ruling,[129] while – on the European side of the Atlantic – the BND Act does not provide effective redress options for foreigners against its bulk collection programs, either.

There is no legally defined path for foreign individuals, such as journalists abroad, who want to find out if their communications have been collected in SIGINT operations and, if so, to verify whether the collection and processing of their data was lawful. What is more, the legislators opted to explicitly waive notification rights for foreigners regarding the bulk collection of their personal data (§ 59 (1) BND Act). While an obligation to notify foreign individuals about past SIGINT activities was not required by the German constitutional judgement, German citizens, organizations and residents, however, in principle enjoy a right to be informed if the BND has collected their communications. While the collection of domestic communications is prohibited in principle under the BND Act, the BND may nonetheless retain domestic data to prevent considerable dangers. In such cases, the G10-Commission must be informed and needs to decide whether the affected domestic person or organization shall be notified, or whether the notification shall be deferred.[130]

That the BND Act denies foreigners the right of notification, naturally, raises the question how they may seek redress and complaint against alleged surveillance of their communications. In the Rättvisa judgement, the ECtHR's Grand Chamber pronounced that "the absence of a functioning notification mechanism should be counterbalanced by the effectiveness of the remedies that must be available to individuals who suspect that their communications may have been intercepted and analysed."[131] Similarly, the Straßbourg court highlighted in its Big Brother Watch case that the British Investigatory Powers Tribunal (IPT), which has comprehensive jurisdiction over British intelligence activities, can examine any complaints about illegal interceptions regardless of notifications to the data subject.[132] It uses, for

[128] European Court of Human Rights, Big Brother Watch v. UK, 25.05.2021, recital 413ff, https://data.guardint.org/en/entity/8bxe5z9q3ar?page=125 ; Centrum för Rättvisa v. Sweden, 25.05.2021, recital 354ff, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=91
[129] Court of Justice of the European Union, Schrems II Judgement, 26.07.2020, recital 191, https://data.guardint.org/en/entity/k4ae1290jz?page=40
[130] If the BND processes domestic personal data collected in hacking operations, the BND Act also requires a notification of the affected German individuals or organizations (§ 34 (6) in connection with § 59 (2) BND Act).
[131] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 25.05.2021, recital 355, also 272, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=91; information about the complaint mechanism provided by the Swedish oversight body SIUN available at: http://www.siun.se/begaran.html
[132] European Court of Human Rights, Big Brother Watch v. UK, 25.05.2021, recital 414, https://data.guardint.org/en/entity/8bxe5z9q3ar?page=126; information about the complaint mechanism provided by the British IPT available at: https://www.ipt-uk.com/content.asp?id=27

example, specific methods to handle cases that involve classified material, such as closed procedures, considerations of assumed facts and a duty to inquire about additional material from the services in order to substantiate a complaint. Such a remedy – which is independent of any notification requirement and the authorization and oversight process – might even allow for more effective redress if a proper procedure is in place.

Neither the legal framework regarding the Independent Control Council, nor that for the G-10 Commission feature provisions regulating how non-nationals can turn to them similar to the remedy processes available in the UK and Sweden. Plus, internet service providers and other carriers that the BND can compel to provide data have no complaint options either, for example to request a re-evaluation of the lawfulness of a bulk warrant.

Legal protections are restricted to personal data

Another critical gap in the new BND Act is the exclusion of metadata from most safeguards. The collection and processing of metadata, such as *traffic data* or *related communications data*, is, due to the large volumes of data processed, the cornerstone of SIGINT. Digital communications produce much more metadata than content, because every piece of content is embedded in a variety of related pieces of metadata. In its Rättvisa decision, the ECtHR has also underscored and explained the tremendous significance of metadata:

> "While the content might be encrypted and, in any event, may not reveal anything of note about the sender or recipient, the related communications data could reveal a great deal of personal information, such as the identities and geographic location of the sender and recipient and the equipment through which the communication was transmitted. Furthermore, any intrusion occasioned by the acquisition of related communications data will be magnified when they are obtained in bulk, since they are now capable of being analysed and interrogated so as to paint an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with."[133]

The court was clearly unconvinced that the collection of metadata is in any way less intrusive than the collection of content data. Consequently, it required that the same standards and safeguards should apply for metadata and content and used the eight step test that it developed to assess the Swedish SIGINT law consistently for both types of data.[134] Given that the BND Act excludes foreign traffic data and other foreign metadata from its requirements for bulk interception (§ 19) and CNE (§ 34), it is hard to imagine how it could successfully substantiate its compatibility with the standards of the European convention of Human Rights.

---

[133] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 25.05.2021, recital 256, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=68

[134] European Court of Human Rights, Centrum för Rättvisa v. Sweden, 25.05.2021, recital 277, https://data.guardint.org/en/entity/wdwrxl9tv6f?page=74

Instead of abandoning the metadata vs. content distinction – as did the Netherlands and Sweden – the Federal Government of Germany reinforced the data differentiations in the BND Act. Consider the protection of confidential communications of journalists and lawyers abroad, as another example, which is strictly limited to personal data relating to an identified or identifiable individual or organization. Again, it is hard to conceive hypothetical cases in which the collection of traffic data of an attorney who communicates with a number of clients or a journalist who corresponds with a source would be less worthy of protection than the content. The BND Act, though, allows for the unrestricted collection of supposedly "non-personal" traffic data, which undermines trust in the confidentiality and integrity of communication channels and thus may have chilling effects on the exercise of fundamental freedoms, such as press freedom, around the globe.[135]

4.2.3 Authorization process and oversight

Laws can only go so far. Professional intelligence oversight requires much more than a solid legal basis and given that the ICC will only begin its important work in 2022, it may seem premature to point to weaknesses or poor practice at the outset. A few important things, however, can already be observed, which point to a continued need for further optimization.

Obfuscation by fragmentation

This section already alluded to the different legal bases for very similar investigatory powers in Germany. Consider bulk collection: Depending on whether the BND intercepts domestic-foreign traffic or foreign-foreign traffic, a BND analyst has to abide by two separate laws (the Article 10 Act and the BND Act, respectively) and two separate oversight bodies provide (quasi-) judicial oversight (the G10-Commission and the ICC, respectively). Service providers currently receive separate technical capability notices for very similar requests and the level of granularity in warrants and oversight obligations depending on whether a measure is based on the BND Act or the Article 10 Act are also notably different. Add to this the various different reporting obligations for different oversight bodies, and the call for a more consolidated investigatory powers framework and a less crowded oversight landscape becomes even more persuasive. At a minimum, future reforms should extend the remit of the ICC to other intelligence activities of the BND and abandon the underwhelming idea to provide professional quasi-judicial oversight through honorary members of an understaffed G10-Commission.

Yet, frankly, the task for future legislators is far more daunting than this. Like in many other democracies, it becomes increasingly more difficult to defend the notion that the same investigatory powers and modes of government access and data processing can be governed and overseen radically differently across the security sector. More specifically, the bulk collection practices by the various departments of the Federal Armed Forces embody the same risks to the enjoyment of the fundamental rights of Art. 10 and Art. 5 of the German Constitution. Yet, oversight over their access and use of such data is nowhere near as

[135] Dittmer, Lisa, 15.12.2020, p. 6f

comprehensive and resourceful. As indicated previously, given the privileged partnership between the BND and the German Armed Forces, a comprehensive legal framework would go a long way to mitigate the inherent risk of collusive delegation or, to put it more mildly, creative non-compliance.[136] In addition, a more comprehensive framework with reduced but strengthened oversight bodies would limit the risk to oversight effectiveness that stems from duplication. For example, next to the oversight bodies of the Armed Forces that may look into bulk data processing, one also has the G10-Commission, the ICC and the Federal Data Protection Commissioner looking into this – each from different vantage points but in sum, it may amount to an inefficient investment of control resources, not just burdensome to the BND but also not in keeping with the objective of end-to-end oversight.

Not enough value for compliance and transparency

Given the amount of resources that the Federal Government projected for the redesign of intelligence oversight in Germany and recalling the importance of trust in Germany's role as arbiter of privacy rights,[137] oversight needs to be effective and its processes – despite the necessary secrecy requirements – ought to be documented in a way that allows the public to (re-)build trust. They need to be confident that the oversight bodies are not merely consultants – or worse: mushrooms that like to live in the dark growing on manure[138] – but an independent force for positive change.

The following discussion puts two question marks behind Germany's ability to meet this objective. The first one is tied to the aspect of oversight effectiveness, the other one to public trust. As regards the former, it is good that the BND Act now includes a more elaborate catalogue of purpose restrictions and data use limitations for both manual and automated contexts. For example, the BND is obliged to log data sharing: The recipients, the legal basis for the data transfer and the date of the transfer must be recorded.[139] This is good because complete and meaningful audit trails are necessary for internal controls and executive oversight by the Federal Chancellery. Yet, they are also a basic prerequisite for effective data-driven intelligence oversight. As increasingly practiced in many European democracies, independent controls of data processing require, in particular, comprehensive, direct access to the log data that accumulates along the various stages of the intelligence cycle, for example, automated, standardized logs of filter errors, logs of purpose changes, data transfers and

[136] At the moment, the Federal Government may have an undue incentive to delegate more tasks to intelligence units of the Armed Forces due to the fact that processing of data from bulk collection is less rigidly overseen there. Of course, this is unlikely to be a sole criteria for such decisions but good legislative practice ought to be more mindful of such factors, too.
[137] At the international level, the credibility of Germany's efforts to table a new resolution for better privacy protections at the UN level in the wake of the Snowden revelations was challenged in light of the various spying practices and oversight deficits that emerged from the Bundestag's NSA inquiry committee.
[138] A metaphor used by the former senior member of the U.S. House of Representatives Intelligence Committee Norman Mineta, quoted in: Glennon, Michael, 2016.
[139] Audit trail obligation for data sharing pursuant to § 29 (16) in connection with § 30 (9) BND Act

timely data destruction. These records must be available to judicial and administrative control in a machine-readable form in order to enable efficient data-driven oversight.[140]

The audit logs that are currently required by the BND Act, however, are insufficient in this regard (see table 8): Many of the logging requirements are narrow and cover only very specific operations, such as the deletion of personal data (e.g., § 27 (1) BND Act). Most importantly, the law does not clarify whether, and if so, how the ICC may access and use the logs. The respective provisions state that logs are exclusively available for carrying out controls of data processing, including data protection controls, which applies, according to our reading, solely to internal reviews conducted by BND staff. If this is the case, then the unfettered oversight access to all relevant data in paragraph 56 of the BND Act would be severely undermined. Not only the BND but also the administrative control body would benefit enormously from the automated provision of logs.

Already before the reform, it was most likely common practice for the BND to record and use log files for its internal purposes. Making the logs available to the administrative control body would allow for data-driven audits and boost oversight effectiveness. The Swedish oversight body SIUN, for example, runs statistical pattern analyses based on deletion audit trails.[141] This could be enabled, too, by a legal audit trail obligation that requires that comprehensive logs must be kept and maintained by the BND in such a way that it meets the needs of the ICC. While the BND is currently spending large sums of taxpayers' money on redesigning its operational systems to make them compliant with the amended BND Act (see table 7), the needs of the independent overseers within the judicial and administrative branch of the ICC should equally be taken into account.

As regards public trust and confidence in the lawfulness and legitimacy of foreign intelligence collection, the reporting obligation of the ICC to the standing parliamentary intelligence oversight body (*Parlamentarisches Kontrollgremium*, PKGr, § 55 BND Act) appears to be insufficient. At present, it has to file a secret report about its activities to the PKGr at least every six months and it may report openly to the PKGr about complaints (see section 3.2.2) allowing the PKGr to then inform the Bundestag – and by extension the public. Yet, the public needs to know more about the processes and decisions of the ICC. And here, the secret activity reports to the PKGr and the limitation on complaints when it comes to public information keeps too much information away from the public eye. Granted, the government needs a core area of exclusive executive responsibility and its commitment to the Third Party Rule must be credible in the eyes of its international intelligence partners. Thus, it is understandable that according to paragraph 55, section 2 of the BND Act the secret activity reports of the ICC to the PKGr are limited to areas where the BND has executive control rights (*Verfügungsberechtigung*). Yet, in addition to complaints, the ICC could report on its general decisions and its experiences with audits, for example. It may seek inspiration here from the

[140] Vieth, Kilian and Wetzling, Thorsten. 2019, p. 22ff
[141] SIUN, 22 February 2018, Section 4.1, http://www.siun.se/dokument/Arsredovisning_2017.pdf

Dutch oversight body TIB. Not only does this body which is responsible for authorizations regularly publish reports not just in Dutch but also in English. It also provides insightful statistics on the thematic nature and totality of its authorization decisions, including the reasons for dismissals and rejections.[142]

What is more, the ICC should be encouraged through legislation but also through its interaction with other oversight bodies, to embrace public reporting as part of its mission so as to help cement public trust in its work – and by extension in the work of the BND. This is all the more important as the BND's mandate to interfere with fundamental rights through its collection and processing of personal data by means of bulk collection and computer network exploitation is now firmly established in German intelligence legislation. Having more substantive reports from the PKGr and ICC would help to assess the value added of certain intelligence powers over time and to trace how oversight instruments need to adjust in order to keep pace with the ongoing evolution of modern surveillance technology.

What follows from this discussion, is that the current catalogue of the ICC's control competences, especially with regard to its administrative oversight body, and its general reporting obligations should be strengthened and enlarged. A future mandate for the ICC should also comprise the authority to:

- examine the lawfulness of the entire practice of the suitability tests (incl. those meant to generate search terms)
- examine and report on the recording and maintenance of log files (to which it must have full access)
- examine the processing of metadata, also including technical data that is not personal data in a narrow sense (*Sachdaten ohne Personenbezug*)
- engage in closer and more structured forms of cooperation with its domestic and international oversight partners[143]
- sanction malfeasance and abuse of investigatory powers by the BND or its political masters in the Federal Chancellery.

[142] For instance, the TIB reports that it examined and decided upon 2.159 orders for surveillance measures between May 2018 and April 2019. It also accounts for the number of rejections and the types of reasons for it (TIB, 2019).
[143] For an elaboration of new forms of cooperation between different intelligence oversight bodies, see Wetzling, Thorsten and Vieth, Kilian, 2020.

5. Conclusion

In March 2021, the German Bundestag amended yet again the legal framework for one of Europe's most powerful intelligence agencies, the *Bundesnachrichtendienst*. This report highlighted key legislative changes regarding the provisions on strategic bulk interception, computer network exploitation and transnational data sharing. It also reviewed the institutional set-up and competences of Germany's new judicial and administrative oversight institution, the Independent Control Council.

Analysing the quality of the legal framework, the degree of fundamental rights protection and the authorization and oversight process, the authors draw a sober conclusion: Despite noticeable improvements, the reform fails to address a number of known deficits and creates new accountability gaps.

By international comparison, the BND Act now features an important high water mark: It no longer restricts the German Constitution's guarantee of the privacy of telecommunications and the right to press freedom to citizens and residents of Germany. Instead, these fundamental rights against state interference "also protect foreigners in other countries."[144] At least *de jure*. In practice, however, non-nationals might not benefit much from their rights when confronted with surveillance by German intelligence. This is because the BND Act also does not incorporate the standard for effective remedy that the European Court of Justice recently found missing in U.S. intelligence legislation.

At long last, the reform established genuine independent judicial oversight for some of the BND's key collection and processing practices. Still, the legal framework remains replete with too many ambiguities and omissions. The report highlighted the ICC's vague mandate for administrative oversight and the law's ineffective data volume limitation. It also deplored broad exemptions from the warrant requirement and cautioned against accountability gaps tied to suitability testing and data transfers between the BND and the German Armed Forces.

Addressing and overcoming these legislative deficits will require more than quick fixes and gestural compliance. The new Bundestag should seize the opportunity to establish a comprehensive legal framework for investigatory powers across the intelligence and security sector. In so doing, it must also extend the remit of the ICC to other forms of intelligence collection and allow for more enhanced transparency reporting.

[144] German Federal Constitutional Court, BND Act Judgement, 19.05.2020, Headnote 1, https://data.guardint.org/en/entity/neb3eo8hl9h?page=1.

6. Annex

6.1 References

Amnesty International Germany. 2021. *Official Statement on the draft BND Act*. https://www.bundestag.de/resource/blob/823300/941d473299f4e353f088a4f7bf6eb1c1/A-Drs-19-4-735-data.pdf.

Bradford Franklin, Sharon. 2020. “A Key Part of Surveillance Reform Is Now in Jeopardy.” *Slate Magazine*. May 29, 2020. https://slate.com/technology/2020/05/usa-freedom-reauthorization-act-fisa-reform-surveillance-amicus-curiae.html.

Brown, Ian, and Douwe Korff. 2021. “Exchanges of Personal Data After the Schrems II Judgment.” Study requested by the LIBE committee. European Union: European Parliament. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/694678/IPOL_STU(2021)694678_EN.pdf.

Council of Europe. 2018. *Convention 108+*. https://data.guardint.org/en/entity/o2r9zbeii5n.

Court of Justice of the European Union. 2020a. “La Quadrature Du Net and Others Judgement.” C-511/18; C-512/18 and C-520/18. https://data.guardint.org/en/entity/20gb4kvky39j.

———. 2020b. “Privacy International Judgement.” C-623/17. https://data.guardint.org/en/entity/35ernv51jnp.

———. 2020c. “Schrems II Judgement.” Case C-311/18. https://data.guardint.org/en/entity/k4ae1290jz.

Dittmer, Lisa. 2020. “The Unwanted Reader: BND Draft Bill Would Continue the Surveillance of Journalists and Their Sources.” *About:Intel*. December 15, 2020. https://aboutintel.eu/bnd-failure-journalistic-safeguards/.

eco. 2021. *Official Statement on the draft BND Act*. https://www.bundestag.de/resource/blob/823354/a8060be2f61786ee68a7baec7be153e9/A-Drs-19-4-731-E-data.pdf.

EOS Committee. 2019. “Annual Report 2018.” https://eos-utvalget.no/wp-content/uploads/2019/05/eos_annual_report_2018.pdf.

European Court of Human Rights. 2021a. “Big Brother Watch and Others v. the United Kingdom.” Applications nos. 58170/13, 62322/14 and 24960/15. https://data.guardint.org/en/entity/8bxe5z9q3ar.

———. 2021b. “Centrum För Rättvisa v. Sweden.” Application no. 35252/08. https://data.guardint.org/en/entity/wdwrxl9tv6f.

Federal Constitutional Court, 1. Senat. 2020. “BND Act Judgement.” https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html.

Federal Government. 2020. *Explanatory Statement of the BND Act*. https://dserver.bundestag.de/btd/19/261/1926103.pdf.

Glennon, Michael J. 2016. *National Security and Double Government*. Reprint Edition. London: Oxford University Press.

IPCO/OCDA. 2020. "Annual Report of the Investigatory Powers Commissioner 2019." London. https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/IPC-Annual-Report-2019_Web-Accessible-version_final.pdf.

Miller, Russell. 2020. "The German Constitutional Court Nixes Foreign Surveillance." *Lawfare*. May 27, 2020. https://www.lawfareblog.com/german-constitutional-court-nixes-foreign-surveillance.

Müller, Michael, and Thomas Schwabenbauer. 2021. "Unionsgrundrechte und Datenverarbeitung durch nationale Sicherheitsbehörden." *NJW* 29: 2065–2144.

Murray, Daragh, Pete Fussey, Lorna McGregor, and Maurice Sunkin. 2021. "Effective Oversight of Large-Scale Surveillance Activities: A Human Rights Perspective." *Journal of National Security Law and Policy* 11 (3). https://jnslp.com/2021/05/24/effective-oversight-of-large-scale-surveillance-activities-a-human-rights-perspective/.

National Security and Intelligence Review Agency. 2020. "NSIRA Annual Report 2019." https://www.nsira-ossnr.gc.ca/wp-content/uploads/2020/12/AR-NSIRA-Eng-Final.pdf.

Rojszczak, Marcin. 2021. "Extraterritorial Bulk Surveillance after the German BND Act Judgment." *European Constitutional Law Review* 17 (1): 53–77. https://doi.org/10.1017/S1574019621000055.

TIB. 2019. "Annual Report 2018/2019." https://www.tib-ivd.nl/binaries/tib/documenten/jaarverslagen/2019/04/25/annual-report-2018-2019/TIB+Annual+Report+2018-2019.pdf.

UN Human Rights Council. 2018. "Report of the Special Rapporteur on the Right to Privacy." A/HRC/37/62. https://undocs.org/A/HRC/37/62.

Vieth, Kilian, and Charlotte Dietrich. 2020. "New Hacking Powers for German Intelligence Agencies." *About:Intel*. October 27, 2020. https://aboutintel.eu/germany-hacking-reform/.

Vieth, Kilian, and Thorsten Wetzling. 2019. "Data-Driven Intelligence Oversight. Recommendations for a System Update." Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/data_driven_oversight.pdf.

Wetzling, Thorsten. 2017. "New Rules for SIGINT Collection in Germany: A Look at the Recent Reform." *Lawfare*. June 23, 2017. https://www.lawfareblog.com/new-rules-sigint-collection-germany-look-recent-reform.

———. 2020. "Germany's Troubled Trajectory with Mass Surveillance and the European Search for Adequate Safeguards." German - Israeli Tech Policy Dialog. IPPI and Heinrich Böll Foundation. https://doi.org/10.13140/RG.2.2.29938.32965.

Wetzling, Thorsten, and Charlotte Dietrich. 2021. "Report on the Need for a Guidance Note on Article 11 of the Modernised Convention." Council of Europe.

https://rm.coe.int/t-pd-2021-6-draft-guidance-note-on-exceptions-under-article-11-of-the-/1680a2d512.

Wetzling, Thorsten, and Kilian Vieth. 2018. *Upping the Ante on Bulk Surveillance. An International Compendium of Good Legal Safeguards and Oversight Innovations*. Schriften Zur Demokratie 50. Berlin: Heinrich-Böll-Stiftung. https://www.stiftung-nv.de/en/publication/upping-ante-bulk-surveillance-international-compendium-good-legal-safeguards-and.

———. 2020. “Stellungnahme im Rahmen der Verbändebeteiligung zum Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts und des Bundesverwaltungsgerichts.” Berlin, Germany: Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/stellungnahme_refe_bndg_wetzling_vieth.pdf.

6.2 List of tables and figures

6.3 Overview of SIGINT data retention rules

Authority	Data category	Retention rule	Legal provision
Suitability tests	Personal data collected in suitability tests for search terms	Retention for up to two weeks	**§ 24 (6) sentence 1**
	Personal data collected in suitability tests for telecommunication networks	Retention for up to four weeks	**§ 24 (6) sentence 1**
	Encrypted (unreadable) personal data collected within any suitability tests that is required for research purposes	Retention for up to ten years	**§ 24 (6) sentence 3**
Bulk interception	Data collected under a preliminarily approved and then revoked warrant	Immediate deletion	**§ 23 (4) sentence 6; § 23 (7) sentence 6**
	Domestic traffic data that was not or cannot be anonymized	Immediate deletion, with exceptions for emergency cases of serious dangers	**§ 26 (4)**
	Traffic data	Retention up to six months, with exceptions permitted	**§ 26 (5)**
	Personal content data	Mandatory evaluation of relevance in intervals of seven years; immediate deletion if data is deemed irrelevant	**§ 27**

Data sharing	Data transfer to domestic authorities based on a preliminarily approved and then revoked warrant	Receiver shall be requested to delete the data immediately	**§ 29 (8) sentence 6**
	Shared personal data	Transferred data must be evaluated by the recipient, if deemed irrelevant, it must be deleted immediately, with some exceptions	**§ 29 (13); § 30 (9); § 38 (8)**
	Transferred bulk data in cooperations	Unevaluated retention up to six months	**§ 31 (4) number 3, littera h)**
	Erroneously transferred data in cooperations	The foreign public body has to assure the immediate deletion of wrongly transferred data as a prerequisite for the cooperation	**§ 31 (4) number 3, littera b) - d) and g)**
	Search terms from foreign intelligence services	Retention for two weeks	**§ 32 (8)**
Computer network exploitation	Data collected in hacking operations	Data collected in hacking operations shall be evaluated immediately, if possible, but no later than three years after collection. Revaluation in intervals of five years if the data is (still) relevant. Irrelevant data must be deleted immediately.	**§ 34 (7)**
	Data collected under a preliminarily approved and then revoked warrant	Immediate deletion	**§ 37 (4)**

6.4 Unofficial translation of § 19 BND Act

§ 19 Strategic Foreign Telecommunications Collection

(1) In order to fulfil its tasks, the Federal Intelligence Service may use technical means to process personal content data of foreigners abroad on the basis of previously ordered strategic collection measures (strategic foreign telecommunications collection), insofar as this is necessary for the purposes of

1. political information of the Federal Government or
2. the early detection of threats of international significance emanating from abroad.

(2) A strategic collection measure shall limit the respective objective of the strategic foreign telecommunications surveillance by providing information on

1. collection purpose,
2. collection theme/priority,
3. geographical focus and
4. duration.

(3) Strategic collection measures pursuant to subsection 1, number 1, shall only be permissible if they serve to obtain information on foreign countries which is of foreign and security policy significance for the Federal Republic of Germany and for the surveillance of which the Federal Chancellery has commissioned the Federal Intelligence Service.

(4) Strategic collection measures pursuant to subsection 1, number 2, shall only be permissible if they serve to obtain information on foreign countries which is of foreign and security policy significance for the Federal Republic of Germany and which the Federal Chancellery has commissioned the Federal Intelligence Service to investigate, and if there are factual indications that knowledge may be gained through them

1. with reference to the following areas of danger:
    a) national or allied defence as well as missions of the Federal Armed Forces or of allied armed forces abroad,
    b) crisis developments abroad and their effects,
    c) on terrorism or extremism which is prepared to use violence or which is aimed at the planned covert implementation of political, religious or ideological views, or the support thereof,
    d) international criminal, terrorist or state-sponsored attacks by malicious software malware on the confidentiality, integrity or availability of information technology systems,
    e) to organised crime,

f) on the international proliferation of weapons of war within the meaning of the Act on the Control of Weapons of War as well as illicit foreign trade in goods and technical support services in cases of major significance,
g) threats to critical infrastructures; or
h) hybrid threats

2. for the protection of the following legal interests:
a) Life, limb or freedom of a person,
b) the existence or security of the Federation or of a Land,
c) the existence or security of institutions of the European Union, the European Free Trade Association or the North Atlantic Treaty or the existence or security of a member state of the European Union, the European Free Trade Association or the North Atlantic Treaty,
d) the Federal Republic of Germany's ability to act in foreign policy matters,
e) important legal interests of the general public, the foundations of which affect the existence of human beings.

(5) The Federal Intelligence Service may only collect personal content data within the framework of strategic foreign telecommunications collection on the basis of search terms. These must be intended, suitable and necessary for the strategic collection measures in accordance with paragraph 1 and their use must be consistent with the foreign and security policy interests of the Federal Republic of Germany.

(6) Insofar as this is necessary to carry out strategic collection measures in accordance with paragraph 1, the Federal Intelligence Service may use technical means to gain access to the information technology systems of a foreign telecommunications or telemedia service provider abroad, even without the latter's knowledge, and collect personal data from the ongoing communication which the provider processes in the course of providing its service. In doing so, the Federal Intelligence Service may also collect personal data which the foreign telecommunications or telemedia service provider stores in its information technology systems during the processing of ongoing communications, provided that this data is collected within the time frame of the strategic reconnaissance measure in accordance with paragraph 1 and is not older than 48 hours before it is collected by the Federal Intelligence Service. If the Federal Intelligence Service gains access to an information technology system of a foreign telecommunications or telemedia service provider abroad in accordance with sentence 1, it may also process inventory data of the foreign telecommunications or telemedia service provider which the latter processes on the occasion of the provision of its service, insofar as these are collected on the basis of search terms or relate to the counterpart of the data collected on the basis of the search term.

(7) The collection of personal data of the following persons from telecommunication traffic is not permitted:
1. German nationals,

2. domestic legal persons as well as
3. persons residing in the territory of the Federal Republic of Germany.

As far as technically possible, the use of automated filters shall ensure that such data are filtered out. The filtered data shall be deleted automatically without delay. The filtering methods shall be continuously developed and shall be kept up to date with the current state of the art. If, despite this filtering, data is collected contrary to sentence 1, this data shall be deleted immediately. This shall not apply if there are factual indications that the further processing of the data may avert a significant danger to the life, limb or freedom of a person, the security of the Federation or of a country or the security of other Member States of the European Union, the European Free Trade Association or the North Atlantic Treaty.

(8) Unrestricted strategic foreign telecommunications collection is not permitted. The volume of strategic foreign telecommunications collection shall be limited to no more than 30 per cent of the existing telecommunications networks.

(9) Strategic foreign telecommunications collection for the purpose of gaining competitive advantages (industrial espionage) is inadmissible.

(10) Personal data shall be identified immediately after data collection as follows:

1. Indication of the purpose of the data collection pursuant to paragraph 1; and
2. indication of the means of data collection.

The tagging shall be omitted in the case of data transfers.

6.5 Overview of basic concepts and translations

English term	Original German term	Related terms
Secret executive decree	Dienstvorschrift	Internal regulation
German code of criminal procedure	Strafprozessordnung	
Personal content data	Personenbezogene Inhaltsdaten	Content data relating to an identifiable individual
Signals Intelligence (SIGINT)	Strategische Fernmeldeaufklärung	Bulk interception, communications intelligence
Traffic Data	Verkehrsdaten	Related communications data
Data transfer	Datenübermittlung	
Independent Control Council (ICC)	Unabhängiger Kontrollrat	Oversight body
Strategic foreign telecommunications collection	Strategische Ausland-Fernmeldeaufklärung	Bulk interception
Factual indications	tatsächliche Anhaltspunkte	evidence that justifies an assumption
German Federal Armed Forces	Bundeswehr	
Memorandum of Understanding	Absichtserklärung	Agreement
National Intelligence Priority Framework	Aufgabenprofil BND	
Core of private life	Kernbereich privater Lebensgestaltung	
Warrant	Anordnung	Order, notice

Stiftung
Neue
Verantwortung

The Human Rights, Big Data and Technology Project

Human Rights Centre,
University of Essex,
Colchester CO4 3SQ
+44 (0)1206 872877

@HRBDTNews
www.hrbdt.ac.uk