SAFE AND FREE:
NATIONAL SECURITY SURVEILLANCE AND THE RULE OF LAW ACROSS DEMOCRATIC STATES

The University of Texas at Austin
Strauss CENTER
for International Security and Law

NATIONAL SECURITY SURVEILLANCE IN GERMANY

Thorsten Wetzling

ABOUT THE AUTHOR

Dr. Thorsten Wetzling heads the research unit on digital rights, surveillance and democracy of the Stiftung Neue Verantwortung (SNV), a non-profit think tank in Berlin. His current work focuses on the practice, the legal basis and effective independent oversight with respect to different modes of access and subsequent processing of personal data by security and intelligence agencies. More specifically, the European Network Intelligence Governance (EION) regularly explores new ideas and challenges for democratic intelligence governance in collaborative workshops with oversight practitioners from across the continent. Thorsten is also the founder of aboutintel.eu – a European discussion forum on surveillance, technology, and democracy.

From 2021 to 2022, Thorsten assisted the Organisation for Economic Co-Operation and Development (OECD) in finding common standards for law enforcement and national security service access to personal data in the private sector. Thorsten was also appointed in 2021 by the Council of Europe as a scientific expert to examine the scope of exemptions in the modernized Convention for the Protection of Individuals with regard to the Processing of Personal Data.

Thorsten Wetzling received his PhD from the Graduate Institute of International and Development Studies in Geneva with a comparative study of the performance and reform of intelligence control in Europe.

ACKNOWLEDGEMENTS

This project was supported by funds from the Robert Strauss Endowment at the University of Texas at Austin and by a charitable gift from Microsoft. Each paper in the Safe and Free series reflects the views of its author. Editorial direction for the series was provided by Adam Klein, Director of the Robert Strauss Center for International Security and Law at the University of Texas at Austin. We are grateful to Strauss Center staff members Ali Prince and Brittany Horton, and to associate editors Zachary Badore, Seth Greenwald, and Taylor Helmcamp, for their help in shepherding the Safe and Free series to publication.

CONTENTS

NOVEMBER 2023

I. INTRODUCTION

This paper focuses on German surveillance norms and standards. After introducing a few important caveats, the text depicts key institutions that conduct electronic surveillance for the purpose of national security at the federal level. Next, the paper describes the entities that pre-approve and oversee such activities. It then explores Germany's operational capabilities and priorities along with the relevant processes, laws and transparency standards. Finally, it considers recent and pending surveillance reforms and what the author considers to be Germany's comparative strengths when it comes to the democratic governance of surveillance.

Definitions, Scope, and Caveats

Much of the ensuing discussion is contingent on how *national security* and *electronic surveillance* are being defined in the national context. As argued below, one could consider a much broader spectrum of electronic surveillance for the purpose of national security than this chapter does. It is therefore important to unpack key notions at the outset and to caveat their application with a view to the selected context. The chapter's scope of analysis is determined by two editorial decisions: First, an exclusive focus on agencies and institutions at the federal level.[1] Second, the exclusion of electronic surveillance by federal law enforcement and defense agencies. Consequently, much of the analysis will focus on Germany's three federal intelligence services, namely the *Bundesnachrichtendienst* (BND), the *Bundesamt für Verfassungsschutz* (BfV); and the *Bundesamt für den Militärischen Abschirmdienst* (BAMAD).

The distinction between national security, law enforcement and defense is not always very sharp in Germany. Unlike in other democracies, national security is less commonly used as a term to refer to intelligence and federal security and intelligence legislation rarely uses the term *national security* (*nationale Sicherheit*).

In fact, several federal institutions conduct electronic surveillance for purposes closely tied to national security without being national intelligence agencies. For example, this includes different units within the German Armed Forces (*Bundeswehr*) and the Federal Criminal Police Office (*Bundeskriminalamt* – BKA). As regards the Bundeswehr, certain elements perform electronic surveillance that is difficult to distinguish from that

conducted by Germany's foreign intelligence service, BND.[2] The remit of these Bundeswehr units goes beyond what may commonly be understood as defense. Moreover, they lack a comprehensive legal framework and, to date, their processing of data is far less rigorously overseen when compared to the density of provisions that apply to the federal intelligence services.[3] As regards the BKA, the demarcation line between its intelligence-led policing (*Vorfeldermittlungen*) and the electronic surveillance conducted by the BfV is also difficult to draw.

With regard to the scope of *electronic surveillance*, this chapter focuses on bulk and targeted surveillance of personal data through direct or compelled access of fiber-optic cables and modern telecommunications infrastructures by means of signals intelligence (SIGINT). It also considers the use of malware to infiltrate individual devices or infrastructures (Computer Network exploitation (CNE), also known as hacking).

The practice and legal mandate of the German intelligence services is not limited to these forms of intelligence collection, however: Modern government access to personal data entails a plethora of other forms of electronic surveillance – often used in conjunction with data obtained through SIGINT or CNE collection. Recently, the German Federal Constitutional Court (*Bundesverfassungsgericht*, hereafter BVerfG) cautioned against "additive rights infringements"[4] precisely for this reason. Even seemingly innocuous methods of data collection, such as the automated collection of publicly available information, can enable far more granular profiling when aggregated in so-called cross-system information analysis platforms.

The practice and legal mandate of the German intelligence services is not limited to these forms of intelligence collection, however: Modern government access to personal data entails a plethora of other forms of electronic surveillance – often used in conjunction with data obtained through SIGINT or CNE collection.

With regard to the various different data types that the German intelligence services can access, consider the following non-exhaustive list:

- Telecommunications inventory data
- Telecommunications traffic data
- Telecommunications content data
- Encrypted telecommunications content data
- Internally/externally stored computer data
- Data related to the use of telemedia services
- Systematic monitoring and retention of financial transactions data
- Information related to bank accounts
- Mobility data
- Machine-to-machine communications data
- Publicly available information
- Commercially available information

II. INSTITUTIONS

This section briefly describes the institutions that conduct, authorize, or oversee electronic surveillance for the purposes of national security in Germany. Where necessary, the text includes a few historical facts deemed helpful to understand the genesis and subsequent trajectory of these entities.

Operational Entities

Germany has one foreign intelligence service (BND) and two services that perform domestic civilian and intra-military intelligence functions (BfV and BAMAD, respectively). Unlike some other democracies, Germany does not have a singular military or technical intelligence service. All three German intelligence agencies at the federal level conduct electronic surveillance for the purpose of national security.

Starting with the BND, its main mandate is to provide the federal government with insights that are relevant to its foreign or security policy decisions. Yet it also performs electronic surveillance for force protection and other military intelligence purposes. Due to this, Germany's largest intelligence service is often referred to as a "3-in-1 intelligence service,"[5] which combines the functions typically associated with a foreign intelligence service, a military intelligence service and a technical intelligence service. The Federal Chancellery coordinates its steering and the national intelligence priorities process and conducts executive oversight.

The origins of the BND date back to a Third Reich intelligence unit with eyes and ears on the USSR, which, after WWII, became *Organisation Gehlen*. It received direct funding and instructions from the U.S. – first from the U.S. Army and then from the newly established CIA. Once Germany regained its sovereignty in 1952, it took until 1955 for the country to formally establish a federal service for foreign intelligence collection. Interestingly, not just the president of the former Organisation Gehlen but a range of other key operatives made the transition to the BND. This historical fact is of interest because it illustrates the close ties and (initial) dependence of the German foreign intelligence establishment to its counterparts in the United States and its direct ties to the Third Reich. Today, the BND has a workforce of roughly 6,500 people.

Germany's oldest intelligence service is the BfV, however. Since its foundation in 1950, it has been tasked by the Federal Ministry of the Interior (BMI) to collect information on a growing list of (domestic) threats to the country's constitutional order. The BfV, with a current workforce of around 4,300 employees, is also tasked with counter-intelligence and helping German businesses protect their trade secrets from industrial espionage. It also coordinates the interaction of all domestic intelligence agencies – at the state and federal levels. Interestingly, since its inception, the BfV has also housed so-called coordination offices to liaise with the intelligence services of the United Kingdom and those of the United States. Arguably, the demarcation between domestic and foreign intelligence was never too rigid from the start.

Germany's oldest intelligence service is the BfV, however. Since its foundation in 1950, it has been tasked by the Federal Ministry of the Interior (BMI) to collect information on a growing list of (domestic) threats to the country's constitutional order.

Finally, the smallest of the three federal services, BAMAD, has traditionally been entrusted with a more inward-looking mandate to protect military security secrets so as to guarantee the operational capability of the German Armed Forces and its contributions to the NATO alliance. It is tasked and executively overseen by the German Ministry of Defense. Since 2004, the mandate of the agency includes the protection of German military employees abroad from various threats, including extremism (from within), terrorism, espionage and counter-sabotage.

All three agencies have their own statutory footing: the BfV since 1950, and the BND and BAMAD since 1990. All services are constitutionally required to adhere to the principle of separation (*Trennungsgebot*), which in practice means that law enforcement and intelligence services in Germany are organizationally strictly separated in the interest of fundamental rights protection because "someone who may know (almost)

everything, should not be able do (almost) everything; whereas someone who may do (almost) everything, should not be able to know (almost) everything."[6] Consequently, the German intelligence services do not have operational powers of the sort that would allow them to capture individuals or to use lethal force other than for self-protection.

Authorizing Entities

Electronic surveillance interferes with fundamental rights and freedoms. In the German context, this often concerns the constitutional guarantee of human dignity (and its extension to a protected core area of private life), the fundamental rights to the privacy of telecommunications and to informational self-determination as well as to the confidentiality and integrity of information technology systems. In addition, electronic surveillance can also interfere with the fundamental right to freedom of the press as well as the general principle of equal treatment.[7] These are not absolute rights, however.

To be justified, an interference must comply with a growing number of conditions. One of them is the availability of a comprehensive legal framework. Any surveillance measure that interferes with fundamental rights and freedoms of the German Constitution (*Grundgesetz* – Basic Law) requires a legal footing in primary legislation. Such laws must explicitly state which fundamental right is affected by the surveillance measures that the law permits. In addition, such measures must be subject to a rigorous authorization and oversight process.

A failure of the lawmaker or the government to respect these guardrails has caused federal courts to admonish the other branches of government for infringements or violation of said rights in either intelligence practice or legislation. In turn, this usually means substantial legal and political reforms. Most recently, in April 2021, the Bundestag passed a reformed BND Act which included new approval and oversight mechanisms and institutions for the BND's bulk collection and CNE measures.[8] The following account draws on this and other legislation (see section V in this chapter). This said, due to more recent court decisions and a change in government, the Bundestag is set to introduce substantial changes to intelligence legislation and oversight processes towards the end of 2023 (see section VII in this chapter).

At present, German intelligence law sports two entities for prior approval of electronic surveillance for national security purposes at the federal level: The G10 Commission for the pre-approval of measures under the Article 10 Act and the Independent Control Council (*Unabhängiger Kontrollrat*, hereafter UKR) for foreign intelligence collection under the BND Act. Both institutions perform very similar functions. However, their setup, budget as well as the scope of their remit and their reporting obligations differ significantly. Next to the pre-approval of both individual and classes of cases, these institutions are also mandated by law to conduct post hoc oversight of such measures.

The G10 Commission consists of a chairman, who must be qualified to hold judicial office, and four assessors as well as five deputy members, who may attend the meetings with the right to speak and ask questions. The members of the Commission hold an honorary public office. They are appointed by the German Parliament's (*Bundestag*) standing intelligence oversight body (*Parlamentarisches Kontrollgremium*, hereafter PKGr) for the duration of one legislative period of the Bundestag. They are obliged by law to meet at least once per month.

The Commission decides on the admissibility and necessity of government applications for surveillance measures under the Article 10 Act, or on the basis of complaints. As regards the former, the Article 10 Act

stipulates that the responsible Federal Ministry (i.e., the Federal Chancellery for measures concerning the BND, the MoI for measures concerning the BfV and the MoD for measures concerning the BAMAD) shall obtain the approval of the G10 Commission for the surveillance ordered. Importantly, except in cases requiring special urgency,[9] the order may not be executed until the G10 Commission has reviewed its admissibility and necessity and has, in turn, decided to approve it.[10] If the G10 Commission does not approve the ordered surveillance, the competent Federal Ministry shall cancel the warrant without delay.[11]

The law also stipulates that the Commission members ought to be independent in the performance of their duties, thus their decisions to either reject, approve (with or without conditions), supplement and extend measures are not subject to any instructions. This said, the Commission members operate, as specified by the BVerfG, within the "functional area of the executive," i.e., in the "operational" area when deciding on the admissibility and necessity of government applications for surveillance measures,[12] albeit without being "incorporated into it."[13] In essence, the BVerfG characterizes the G10 Commission as a "control body of its own kind outside the judicial power, which serves as a substitute precisely for the lack of judicial remedy."[14] The fact that individuals affected by government surveillance measures generally cannot participate in the judicial decision whether or not an application is deemed admissible and necessary is, in the words of the Court, compensated by the "representation of their interests" in the "ongoing and comprehensive legal control" process.[15] As will be further discussed in section VII, unlike Sweden, Germany has not yet opted for a direct representation of the interests of affected groups in the authorization process. Instead, the members of the G10 Commission solely hear the arguments of the German government prior to their decision-making on the admissibility and necessity of individual or groups of cases.[16]

Next to the G10 Commission, the newly created UKR started its work in January 2022 to provide judicial control over a variety of electronic surveillance measures codified in subsection 4 of the BND Act. More specifically, it is tasked to review the *lawfulness* of SIGINT and CNE authorizations and subsequent data collection and processing activities under the BND Act. According to German administrative law, this requires an assessment of the formal and substantial legality of a given action. Unlike in Belgium, for example, the evaluation of the *effectiveness* of the BND's surveillance measures remains a prerogative of the executive. Unlike the G10 Commission, the UKR is a supreme federal authority on par with the federal ministries that perform executive oversight over the federal intelligence agencies. Notably, the UKR thus has a higher organizational status than the federal intelligence agencies do.

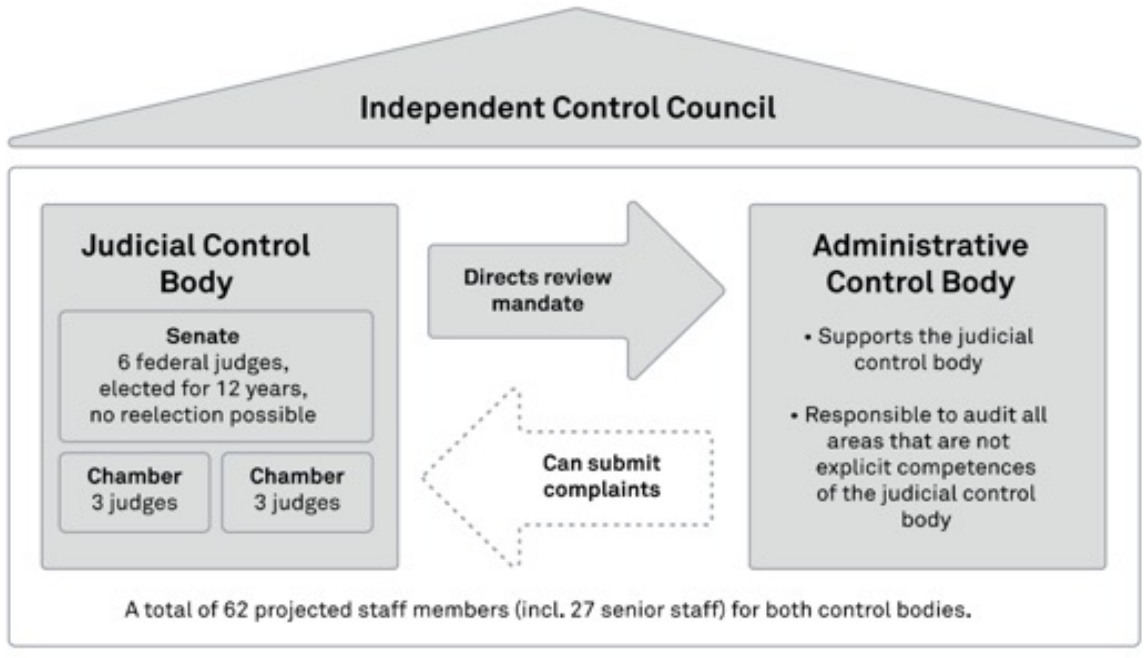

Figure 1: The two bodies within the UKR

The judicial control body of the UKR consists of six federal judges. According to the amended BND Act, it is not bound by instructions from the Federal Government (BND Act § 41(3)), 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 (BND Act § 45). 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 (*Bundesgerichtshof*, hereafter BGH) and the Federal Administrative Court (*Bundesverwaltungsgericht*, hereafter BVerfG) and are elected by the parliamentary control committee of the Bundestag (BND Act § 43).

The same rules that apply to ensure the independence of judges in Germany also apply to members of the judicial control body. 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 (BND Act § 49(2)).

The BND Act includes a specific catalog of competences for the UKR (BND Act § 42) regarding bulk interception and computer network exploitation measures that the UKR needs to approve. For this, and for the administrative oversight of data processing that the other body of the UKR is tasked with, the UKR 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 (BND Act § 56(3)). If the UKR requests access to data that is not under the BND's sole direction, the BND shall take appropriate measures to facilitate access (BND Act § 56(3), nr. 2, sentence 2).[17] This was a firm requirement by the BVerfG's decision in 2020 that the so-called *third-party rule* must no longer undermine the effective and comprehensive oversight by the UKR.[18] The BVerfG held that "the legislator must ensure that the Federal Intelligence Service cannot prevent (judicial) oversight by invoking the third-party rule."[19]

The work of the UKR is strictly confidential (BND Act § 54) and the BND Act does not impose a public reporting obligation upon it. Instead, it must report to the parliamentary oversight committee every six months (BND Act § 55(1)), but the content of these reports is not specified further within the law.[20]

Oversight Entities

Next to the requirement of independent prior approval, German intelligence law also prescribes independent oversight of the implementation of surveillance measures so that, amongst other things, it can be independently verified that the processing of data from warranted surveillance measures adheres to the legal requirements. This type of administrative control involves not just the G10 Commission and the UKR but also the German Federal Data Protection Authority (*Bundesbeauftragter für den Datenschutz und die Informationssicherheit*).

In addition, there is parliamentary oversight by the standing intelligence oversight committee and the so-called "trust committee" (*Vertrauensgremium*), which reviews the budget of the federal intelligence services. The spending of public money is then also monitored by the Federal Audit Office (*Bundesrechnungshof*).

The law also provides for oversight of how data is processed. Section 15(5) of the G10 Act stipulates that the control competence of the G10 Commission extends to all processing of personal data obtained pursuant to this Act by federal intelligence agencies, including the decision to notify affected persons. It also states that the Commission and its staff shall be granted access to all documents, in particular to the stored data and data processing programs, which are related to the warrant-related surveillance measure. It specifically adds that this includes being able to retrieve data from automated files during an inspection at the Federal Intelligence Service itself.

By virtue of its exemption from the third-party rule, the administrative body of the UKR enjoys even more comprehensive access rights (BND Act § 56). It is tasked to oversee the "adherence of all formal and substantive authorization requirements, including, among other things, the provisions for the selection of selectors, the suitability test, the observance of deletion regulations and of transmission and cooperation regulations as well as the handling of notification obligations."[21] In addition, the judicial body of the UKR is tasked to review *ex post* the lawfulness of "processing of data related to protected professional groups" (BND Act §§ 21(3),

35(3)); domestic and transnational transfer of data collected for the government's information purposes (BND Act §§ 29(7), 30(5), 38(7)) as well as the BND internal regulations, e.g., regarding technical implementation of data processing (BND Act § 62) and formal complaints made by the administrative control department (BND Act § 52).

In addition, the Federal Data Protection Authority also has an important, albeit sometimes overlapping, role to play in the ex *post* oversight of electronic surveillance for the purpose of national security. The German legal framework requires so-called "file orders" (database establishing orders) for each automated database that the services wish to operationalize. Such orders ought to contain very specific information: the name of the database, its purpose, the requirements regarding retention, transfer, use (including information on the group of persons to be affected and the type of data used), origins of the data, access restrictions, dates for required reviews and protocol requirements (BfV Act § 14). By law, this information is to be made available not just to the government for its executive controls, but also to the Federal Data Protection Authority. It needs to be consulted prior to the operationalization of each new database, no matter the origin of the data therein. The Federal Data Protection Authority can put this information to good use as the totality of file orders (database-establishing orders) can give independent supervision bodies substantial knowledge on the variety of different intelligence databases and the data types therein. Its positive effect could be strengthened further through more intense and systematic oversight cooperation.[22]

The German legal framework requires so-called "file orders" (database establishing orders) for each automated database that the services wish to operationalize. Such orders ought to contain very specific information: the name of the database, its purpose, the requirements regarding retention, transfer, use (including information on the group of persons to be affected and the type of data used), origins of the data, access restrictions, dates for required reviews and protocol requirements.

III. OPERATIONAL CAPABILITIES AND PRIORITIES

Much of the BND's electronic surveillance involves the monitoring of worldwide telephone, Internet and satellite communications in bulk. This has traditionally been considered the flagship competence of the service. While other surveillance powers, such as targeted CNE or automated OSINT, may now challenge SIGINT's long-term undisputed prominence as the most valuable method, it is important to remember that older methods can still produce immense insights. For example, consider how the BND recently intercepted many Russian military radio messages using an outdated method that other services have abandoned. In doing so, the BND provided very useful information to the Ukrainian intelligence services.[23]

To date, SIGINT also remains the central tenet of the BND's cooperation with over 450 intelligence services worldwide. Almost half of the daily BND reports to the Federal Chancellery are reported to originate from its foreign intelligence collection via SIGINT. Arguably, it is down to its competence and Germany's hosting of the world's largest internet exchange point DE-Cix (which gives Germany something unique to offer in its cooperation with foreign partners) that the BND manages to maintain profound liaisons with the NSA and GCHQ despite its trajectory of regular parliamentary inquiries, constant changes to its legal framework and the recent narrowing of the third-party rule in Germany.

More generally, it was reported in 2020 that the BND copies 1.2 trillion IP connections per day at DE-Cix alone.[24] According to its own testimony during the proceedings before the Constitutional Court in January 2020, the BND deploys between 100,000 and 999,000 search terms simultaneously to collect personal content data, such as text messages or phone calls. Between 50 and 60 percent of search terms used by the BND stem from intelligence services of allied states.

Naturally, this enormous collection ability requires responsible tasking. Similar to the U.S. National Intelligence Priorities Framework, the German government regularly establishes the so-called *Aufgabenprofil* BND. It is a classified document that sets priorities for the BND. It can involve information priorities regarding specific countries but also general information on cross-cutting themes such as terrorism, cybercrime, the proliferation of weapons or migration trends. Different ministries such as Foreign Affairs, MoI, MoDs and the Federal Ministry for Economic Affairs and Climate Action as well as the Federal Ministry for Economic Cooperation and Development can submit information requests and tasks under the overall coordination of the German Chancellery. Despite criticism from the PKGr,[25] the BND's priority framework remains exempt from the remit of parliamentary oversight.

IV. PROCESS FOR APPROVING SURVEILLANCE

Before conducting electronic surveillance for the purpose of national security, the three federal intelligence services need to submit a written request for specific types of surveillance to the respective ministry tasked with executive oversight over them. The ministry then reviews the legality and necessity of such a request and, if approved internally, submits a surveillance warrant to the competent quasi-judicial review bodies for prior authorization.

As regards the *substantive standard* and the conditions that the independent prior approval process needs to meet, important differences exist depending on the envisaged surveillance method. Not only do different surveillance measures affect different fundamental rights and freedoms differently, but one must also distinguish between measures that take aim at a particular individual or known group of individuals (targeted surveillance) and bulk collection and bulk hacking (untargeted surveillance). As regards the latter, only the BND is authorized among the three federal intelligence agencies to conduct bulk surveillance.

The German legislative framework adds complexity to this by distinguishing between bulk surveillance of *international* telecommunications (where one end of the communication involves a domestic connection) and bulk collection of *foreign* telecommunication data (without a domestic connection involved). The former is regulated in §§ 5 and 8 of the G10 Act whereas the latter is codified in Part 4 of the amended BND Act of 2021.

Even worse: Not only are these two similar processes codified in separate laws with different substantive standards, but they also involve different entities for prior approval (the G10 Commission and the UKR, respectively). These differences exist despite the fact that the very collection might well be administered without knowing whether a foreign selector will yield international telecommunications, foreign telecommunications or both.[26]

Notably, both modes of bulk collection under the G10 Act and the BND Act are conducted mostly from within Germany. However, the BND also conducts bulk collection outside of Germany with the help of "mobile equipment."[27]

As regards the process for approving *targeted domestic collection against domestic targets*,[28] there first needs to be a written and justified application for a targeted surveillance against a domestic target by the head of either the BfV or the MAD. This needs to be followed by a written, reasoned and temporary order issued by the MoI.

This order is then subject to judicial review by the G10 Commission, which can reject or accept the order with or without additional conditions. As its operationalization often requires compelled access, the telecommunication providers also need to be notified. The implementation of the measure must also be performed in the presence of an employee of the services who is qualified to be a judge. Once the targeted surveillance measure against a domestic target is terminated, it is upon the agency that submitted the original application to notify the persons affected by the measure to facilitate their right to effective remedies (redress).[29]

As regards the *substantive standards* required for targeted surveillance against domestic targets, the G10 Commission has to verify the existence of factual indications of an imminent danger rather than mere suspicion or assumed risk thereof. More specifically, the G10 Act provides an exhaustive catalog of serious crimes for which actual indications need to exist that the targeted person is planning, is performing or has performed such activities which also need to pose an existential threat to public order. Furthermore, the Commission needs to verify that the investigation of the facts by means of less right-infringing measures would otherwise be futile or substantially impeded. The Commission further needs to verify the absence of factual indications that a measure would solely collect information from the core area of private life, and it has to rule out or significantly reduce the surveillance

of individuals' professional secrets. Neither the substantive standard nor the application process for domestic surveillance against domestic targets make any qualifications that this applies only to German nationals.

As regards the substantive standard and process for approving *domestic collection against overseas targets*, the focus now turns away from targeted surveillance against individuals to bulk collection or bulk hacking by the BND. Interestingly, the G10 Act stipulates that selectors used for bulk collection of international communications data must not contain identifiers that would allow a targeted collection of individuals or collection from any persons' core area of private life. This said, the G10 Act also clarifies that these qualifiers do not apply for collection abroad as long as it can be ruled out that telecommunication connections owned or regularly used by German citizens are specifically targeted.[30] By comparison, the regime for collecting foreign telecommunications data under the BND Act (described further below) is stricter in the sense that it explicitly prohibits the collection of personal data of German citizens as part of the BND's bulk collection of foreign telecommunication data.[31]

Regarding the *approval process* for collection of international telecommunications data under the G10 Act, it starts with a determination by the MoI of the types of telecommunication data it wishes to collect, naming in rather abstract terms the geographical focus and the types of connections and carriers to be affected. This abstract determination does require the approval of the parliamentary intelligence oversight committee before a written and reasoned application by the President of the BND (or his or her deputy) can be sent to MoI that must name clearly defined and suitable search terms (G10 Act § 10(1)) to be used in the process. Following internal reviews this can then lead to MoI issuing a warrant (G10 Act § 10(1)) for collection which, initially, is only valid for three months with the possibility of another extension of no more than three additional months is possible (G10 Act § 10(5)). The transmission paths to be monitored (cable connections, bearers, telecommunications satellites) must be precisely determined in advance as part of the warrant (G10 Act § 10(4)). Prior to the implementation of the warrant, MoI needs to inform the G10 Commission, which will review the legality of the warrant. If it decides against the envisaged measure, MoI must immediately retract the warrant. Only if the G10 Commission attests the legality of the warrant can the measure be performed. Once the collection is terminated, MoI is obliged to notify persons affected unless their data were not immediately deleted.
The G10 Act also lists specific measures to ensure independent data processing reviews by the BFDI and (quasi-)judicial review by the G10 Commission. This includes a review every 6 months of whether data is still needed (G10 Act § 6, Abs. 1, S1), and of documentation and tagging obligations.

> ***The approval process for bulk collection of foreign communications under the BND Act requires a written request from the president of the BND (or designated deputy), which must contain detailed information on the parameters of the collection: purpose, theme, geographical focus and duration, along with a specific justification.***

The approval process for bulk collection of foreign communications under the BND Act requires a written request from the president of the BND (or designated deputy), which must contain detailed information on the parameters of the collection: purpose, theme, geographical focus and duration, along with a specific justification.[32] Next, the judicial review body of the UKR examines the legality of the application prior to its implementation (BND Act §§ 23(4), 42(1)). Afterwards, the Federal Chancellery sends a security letter to telecommunication service providers, who may be compelled to assist in the collection process (BND Act § 25).

In 2021, a landmark judgment by the German Constitutional Court found key tenets of Germany's BND Act unconstitutional.[33] In response, the Bundestag introduced an important additional guardrail to the process of collecting foreign communications via signals intelligence: The amended BND Act now distinguishes between foreign communication collection for the purpose of "politically informing the government" (BND Act § 19(1), nr. 1) and collection for the "early detection of foreign threats to the Federal Republic that are of international significance" (BND Act § 19(1), nr. 2). As regards the former purpose, the law stipulates that such collection is only permissible if:

- the collected foreign communication serves the purpose of gathering information that is relevant to German foreign and security policy, and
- where the Federal Chancellery has ordered the BND to collect such information (BND Act § 19(3)).

By contrast, according to § 19(4) of the BND Act, bulk foreign communications collection for the purpose of early detection of threats to the Federal Republic of international significance are only permissible if the two aforementioned conditions are met and when:

- factual indications (*tatsächliche Anhaltspunkte*) exist that the ordered collection of foreign communications data can:
  - produce insights into the following *eight* threat areas:
    1. national defense as well as protection of (allied) armed forces abroad,
    2. crises abroad and their effects,
    3. terrorism and (violent) extremism, or its support,
    4. criminal, terrorist or state-sponsored attacks on information technology systems by means of malware, or support for such attacks,
    5. organized crime,
    6. international proliferation of weapons of war, as well as unauthorized foreign trade with goods and technical support services in cases of significant importance,
    7. threats to critical infrastructures, and
    8. hybrid threats; or
  - produce insights that help to protect the following *five* legal interests:
    1. life or freedom of a person,
    2. existence or security of the Federal Government or a state (*Land*),
    3. existence or security of institutions of the European Union, the European Free Trade Association or NATO or a member state of these organizations,
    4. the Federal Republic of Germany's ability to act in foreign policy, and
    5. important legal interests of the general public.

During the prior-approval process, the judges of the UKR validate the justifications provided in the written applications for these surveillance measures. They also decide on the legality of the processing of data related to the core of private life. The appendix provides further information on the different warrant types, their codification in the respective legal frameworks and the corresponding review competences of the UKR. Notably, the UKR's *ex ante* approval powers neither extend to the BND's collection of metadata nor do they cover its so-called suitability tests (BND Act § 24).[34] Unlike New Zealand, for example, Germany does not require a warrant for the latter. Unlike the United Kingdom, for example, German lawmakers also did not introduce mandatory data examination warrants.

Interestingly, a current member of the UKR recently criticized the legal design of the authorization process for bulk collection in the BND Act.[35] According to Elisabeth Steiner, the "breadth of possible application scenarios and the high level of abstraction inherent in the list of permissible collection objectives render the de facto implementation of the required limitations difficult. Furthermore, the perspective of those whose fundamental rights and freedoms are directly affected by bulk collection is represented only in a very abstract manner."[36] She thus concludes that the "depth of investigation" (*Prüfungstiefe*) which was envisaged by the BVerfG at the *ex ante* phase is therefore "not attained in actual practice."[37]

Comparing the standards and process for bulk collection under the G10 Act and the BND Act, several differences emerge. The G10 Act contains less-granular descriptions of legitimate purposes. It lacks a comparable protection scheme regarding the protection of the

core of private life. And its protections concerning the communication of certain protected professions are less rigorous than those in the BND Act.

What both authorization processes have in common, however, is that they lack systematic points of friction: Currently, the members of the G10 Commission and the UKR only hear from the government side prior to their decision-making on the lawfulness of surveillance applications. Unlike in Sweden or the U.S., there is no privacy representative, amicus or some other form of adversarial counsel included in the German authorization process to help harden the mechanism against the genuine risk of being captured by the executive.[38]

Much of the BND's collection of both international and foreign telecommunication data occurs from within Germany. That does not mean, however, that the service does not also operate devices for the collection of data from outside of Germany. What is more, and very interesting by international comparison, the very question of whether the collection takes place within or outside Germany became less relevant following the BVerfG's landmark judgment of May 2020. Since then, it is undisputed that Germany's Basic Law, especially its positive obligations regarding the protection of fundamental rights, binds the BND in its activities outside of Germany's jurisdiction just as much as they do within Germany. The fundamental rights under the German Constitution are universal human rights and not just rights for nationals. According to the BVerfG, "German state authority is bound by fundamental rights even in relation to actions taken vis-à-vis foreigners in other countries."[39]

This said, the BVerfG did qualify the right to effective remedy as applied to foreign nationals which, presumably, greatly affects collection practice. For non-Germans, the Court held:

> [T]he legislator may, in principle, refrain from imposing notification requirements for strategic surveillance measures . . . Compared to notification provided to persons living in Germany, notification provided to persons living abroad can neither provide a basis for legal protection that is attainable in practice . . . nor can it achieve the aim of creating public trust or of generating democratic discourse on such measures . . . Instead, notifying affected persons in another legal order may even be dangerous, as it may expose those persons to the attention and mistrust of the authorities in their state and, as the case may be, third parties. Thus, the requirements for transparency of state action are significantly less strict and there are fewer possibilities for obtaining individual legal protection in practice. Recourse to the courts . . . remains formally unaffected, yet affected persons will only be able to obtain legal protection through this avenue in exceptional cases, given that they are not aware of the surveillance measures. In this respect, too, comprehensive independent oversight is required as compensation and in order to uphold the principle of proportionality.[40]

V. RELEVANT LAW

This section describes key constitutional provisions and related case law that are central to the German legal framework for intelligence. This includes the right to private communication under Basic Law Article 10, the guarantee of human dignity in its manifestation as protection of the core area of private life (Basic Law Art. 1(1)), the right to informational self-determination and the fundamental right to guarantee the confidentiality and integrity of information technology systems (Basic Law Arts. 2(1), 1).

In addition, there are a number of key legal principles that the lawmaker ought to adhere to when adopting surveillance legislation. These include:

- the principle of legal certainty (*Bestimmtheitsgebot*), which requires that rules must be clear and definite, especially when statutes limit basic rights: "the indefiniteness of a statute that limits basic rights represents an additional (factual) encroachment on basic rights. Therefore, if a statute does not fulfill the attainable degree of definiteness, this must be justified by the specific need for statutory flexibility in the respective legislative field";[41]
- the doctrine of essential matters (*Wesentlichkeitstheorie*), which requires that all questions of constitutional significance ought to be regulated within the law itself (and not in executive decrees);
- the citation rule (*Zitiergebot*), which stipulates that if a statute is intended to permit an interference with constitutionally protected rights, Article 19 of the Basic Law requires the statute to explicitly mention the rights from which derogation is permitted;
- prohibition of excessive measures (*Übermaßverbot*), which states that the more severely an individual freedom is restricted, the more significant the pursued interests of the common good must be (BVerfG 1; BvR 781/21); and
- the principle concerning the innermost sphere of private life (*Kernbereich persönlicher Lebensgestaltung*), which protects the development of one's personality. Basically, it states that a person can reasonably expect that an innermost sphere of private life will not be surveilled. "This includes the possibility of expressing one's internal processes, sensations, feelings, thoughts, opinions, and experiences of a most personal character, in particular through non-public communications with trusted person" (BVerfG 1; BvR 1619/17, 276; author's translation).

Key statutory regimes for electronic surveillance for the purpose of national security at the federal level include: the BND Act, the BfV Act, the MAD Act, the Article 10 Act, the Parliamentary Oversight Panel Act (PKGrG) as well as additional laws tied to vetting and state secrets, federal databases used by law enforcement and police to counter right-wing extremism and for counter-terrorism purposes.

As regards executive decrees, the BVerfG's landmark decision in May 2020 called upon the Bundestag to ensure that a number of aspects which were previously governed without a direct involvement of the Parliament ought to be (partially) turned into legal provisions adopted by Parliament. This concerns, for example, aspects of executive decrees (*Dienstvorschrift*, hereafter DV) regarding international cooperation on SIGINT, the processing of personal data from protected professions and the core area of private life.

As regards executive decrees, the BVerfG's landmark decision in May 2020 called upon the Bundestag to ensure that a number of aspects which were previously governed without a direct involvement of the Parliament ought to be (partially) turned into legal provisions adopted by Parliament.

The decision made it more difficult to embody important constraints on intelligence powers in agency manuals rather than laws passed by the Bundestag. While the Court accepted that the intelligence services can continue to write more granular rules on the implementation of specific objectives and processes into intelligence service manuals that may not involve Parliament (but which do need to be subject to independent oversight), it held, for example, that the basic framework to be determined by the legislator includes "the applicability of the principle of proportionality to the selection of search terms . . . provisions governing the use of intrusive methods of data analysis, in particular complex forms of data cross-checking . . . and adherence to prohibitions of discrimination under the Basic Law . .

. The legislator may also have to lay down how algorithms may be used, in particular to ensure that their use can generally be reviewed by the independent oversight regime."[42]

Consequently, 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 aspects covered in foreseeable legal provisions.[43] Other important aspects, however, such as the tasking of the BND through the government by means of the National Intelligence Priorities Framework (*Aufgabenprofil* BND), continue to be documented by means of executive decree and without parliamentary oversight bodies able to access this dynamic document.[44]

Furthermore, while the Standing Parliamentary Intelligence Oversight Panel (PKGr) has published its bylaw (*Geschäftsordnung*), which, among other interesting aspects, provides a public record for its priorities per legislative period, no such publicly available bylaw exists yet for the UKR.

On a different note, European Union law, such as the GDPR, and the case law of the European Court of Justice, has started to become a factor that needs to be increasingly considered. For example, it has been argued that the GDPR might apply in instances where national intelligence collection cannot be tied solely to purposes of national security but to broader purposes such as informing the government about topics relevant to security and foreign policy.[45] More significant, perhaps, is the decision of the Court of Justice of the European Union in the 2020 *Privacy International* case, in which the Court found that European Union law applies to national intelligence practices that compel private sector entities to assist in bulk collection.[46] The potential ratification of the modernized Convention 108 by the Council of Europe may further expand the corpus of relevant European law.[47]

The BverfG has also interpreted Germany's constitution to impose certain overarching limits on all surveillance activities. The Basic Law, it held,

"does not allow for global and sweeping surveillance, not even for the purpose of gathering foreign intelligence . . . Therefore, the legislator must restrict the volume of data to be taken from the respective transmission channels . . . and the geographical area covered by surveillance. Since the technical possibilities for processing data are changing quickly, merely referring to actual capacity limits in this respect is insufficient . . . Yet above all, the legislator must circumscribe the powers in accordance with the rule of law so as to structure and partially restrict data collection and processing. In particular, this includes rules on the use of filtering techniques . . . the purposes of surveillance . . . the design of the surveillance process . . . the focused use of search terms . . . the limits of traffic data retention . . . the methods of data analysis . . . the protection of relationships of trust . . . and the protection of the core of private life . . . as well as the imposition of obligations to delete data . . . In addition, the legislator must adhere to requirements regarding transparency, individual legal protection and, above all, comprehensive independent oversight".[48]

This, taken together, is what the European Court of Human Rights later called "end-to-end" safeguards, meaning that guardrails have to be in place at every instant of the intelligence lifecycle. Obviously, this also includes a trimming of the objectives for which electronic surveillance may be allowed. More specifically, in the context of electronic surveillance of international communications data by means of bulk collection, the Bundestag responded to the BVerfG's long list of required changes by including several restrictions. Accordingly, it is, in principle, unlawful to:

- subject German citizens (but also residents in Germany and domestic legal persons) to this type of surveillance (BND Act § 19(7));
- use it to obtain a competitive advantage in economic terms (BND Act § 19(9));
- use it to target the communications of those whose communications are particularly protected, such as attorneys, journalists, and clergy (BND Act § 21(1)); and
- obtain information on the core area of private life (BND Act § 22(1)).

Notice, however, that the legal framework includes exceptions to these general prohibitions. For example, the law requires automated filtering processes to prevent the incidental collection of content (and metadata, see BND Act § 26(3)) of German citizens, residents or domestic legal persons and requires that such incidentally collected data be instantly deleted by means of automated processes (BND Act § 19(7), sentences 2, 3). Yet, the legal framework allows for the subsequent use of such incidentally collected information if the BND has factual indications that lead it to believe that the further processing of such 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 (BND Act § 19(7), sentence 6). Similar exceptions apply to the other restrictions mentioned above.

With regard to "procedural protections," in 2020 the BVerfG required an overhaul of the entire foreign intelligence legislation, a redesign of oversight and various new structures and processes within government.

Consequently, as mentioned earlier, German foreign intelligence law now distinguishes between two different types of permissible objectives for bulk collection: namely to politically inform the government (BND Act § 19(1), nr. 1) and also to engage in the early protection of threats of international relevance (BND Act § 19(1), nr. 2). Different handling rules apply to data collected for each purpose. For example, the original purpose of the data collection must be reflected in the tagging of such data and different procedural requirements and thresholds apply to the further processing and transfer of such data.

These are important restrictions in the German system. In addition, one could point to explicit quantitative restrictions on the volume of data[49] and data minimization requirements.[50] Germany also has elaborate, albeit very complex, protection schemes when it comes to *data transfers* between German intelligences services and their international partners. Furthermore, as illustrated with the help of the tables in the Annex, the German legal framework on bulk collection also includes specific rules for international intelligence cooperation in this context.

VI. TRANSPARENCY

The reform of German foreign intelligence law in 2021 also required additional investments in transparency. As noted, many aspects of surveillance that were previously governed by executive decrees were transposed into statute, rendering them accessible to the public. The reform also included new oversight institutions which were placed under new reporting requirements.

At present, the UKR must file a secret report about its activities to the PKGr at least every six months (BND Act § 55). In theory, it may decide to report openly to the PKGr about potential malfeasance detected as part of its inspections. In turn, this would then enable the PKGr to inform the Bundestag and, by extension, the public. This has not yet happened in practice, however. In part, this may be due to the fact that this presupposes a series of complex and formal proceedings.[51]

By and large, the public needs to know more about the important weighing processes and decisions of the UKR—a public body with a current annual budget of €16 million.[52] And here, the secret activity reports to the PKGr and the high hurdles it needs to overcome prior to informing the PKGr openly about malfeasance keep, in the author's view, too much information away from the public. 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, the secret activity reports of the UKR to the PKGr are limited to areas where the BND has executive control rights (*Verfügungsberechtigung*, BND Act § 55(2)).

Still, in addition to formal complaints about malfeasance, the UKR should be empowered to report openly, at least with regard to its general decisions and its experiences with audits, for example. In so doing, it may seek inspiration here from the Dutch oversight body TIB. The TIB, which is responsible for authorizations, regularly publishes 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.

By contrast, the UKR submits such information only in secret to the PKGr. Interestingly, in a recent report by German media,[53] it was revealed that the first activity report of the UKR to the PKGr covered about 121 surveillance measures, including computer network exploitations, out of which it apparently authorized 120 measures.

Still, in addition to formal complaints about malfeasance, the UKR should be empowered to report openly, at least with regard to its general decisions and its experiences with audits, for example.

Of course, in the absence of further information, which the UKR is prohibited to provide, the interested observer wonders why the oversight body seemingly authorized all but one application. Does this mean that the new oversight body is either teethless or too credulous? Not necessarily; the new regime may have also prevented the government from submitting untenable applications in the first place, for example. Still, future legislation should allow for more transparency and allow for more systematic interaction among the various other oversight bodies. Public reporting requirements could be extended so as to promote further public trust in oversight—and, by extension, the work of the intelligence agencies.

VII. REFORMS

Germany has come a long way over the course of the last two decades in its reform of intelligence legislation. Every legislative period over the last twenty years has featured a parliamentary inquiry committee focused on intelligence and surveillance matters.

Most famous was the Bundestag's inquiry into NSA-BND SIGINT cooperation following the revelations of Edward Snowden. Yet, apart from the Bundestag, the Federal Constitutional Court played a key role in the recent refinement of Germany's legal framework and oversight practice thanks to a plethora of important cases it had to adjudicate.

While the reforms to foreign and domestic intelligence legislation in recent years have brought significant changes, further reforms are pending. This is due, in part, because of the more recent jurisprudence by the BVerfG.[54] It found key provisions regulating data transfers between domestic agencies of the security sector unconstitutional and has requested legislative change by the end of 2023. In addition, it found key parts of the Bavarian domestic intelligence law unconstitutional. Given that some of these provisions exist also at the federal level, government officials and parliamentarians are also preparing legislative fixes at the federal level. This includes further ex ante review competences for additional modes of data collection not mentioned in this chapter.

In addition, the coalition agreement of the Scholz administration includes a number of suggested reforms and evaluations of the security and intelligence laws. These include a comprehensive account of all provisions in German law that allow surveillance as well as an estimate of how these measures, in part and in aggregation, may interfere with fundamental rights and freedoms (*Überwachungsgesamtrechnung*).

At the time of writing, however, the self-proclaimed "progress coalition" has yet to deliver on these good plans and pre-legislative scrutiny proceedings on required intelligence reforms have not yet begun.

VIII. OTHER IMPORTANT FACTORS

The German public is rather sensitive to government surveillance. At least in part, this is due to Germany's history. It is replete with human rights abuses by the Third Reich and the German Democratic Republic (the former East Germany).

Due to this sensitivity, the public seems to have also grasped that privacy and sovereignty are public goods that cannot be taken for granted. Rather, the rapid technological evolutions and growing datafication of our lives require careful attention to the potential advantages and disadvantages. Given that technological change can profoundly affect its freedoms—both positively and negatively—the German public seems to understand, too, that technology policy serving the public good requires further arbiters than just government and business.

Germany's recent reforms to its intelligence laws provide some interesting milestones for other democracies to reflect and, ideally, improve upon. The Bundestag, for example, has created a proper legislative footing for all its bulk surveillance measures, whereas other democracies still cover important segments in executive decrees, or worse, seem to have no legal framework, let alone oversight in place.[55] While an executive order may very well be part and parcel of a national legal framework, it is still a qualitative difference if a surveillance practice is codified in statute because the parliamentary process of adopting laws provides democratic legitimacy. As such, German legislation on bulk collection was subject to pre-legislative scrutiny, several readings in parliament, a public hearing and a vote in parliament. This bears significantly more democratic legitimacy than an executive decree or order.

More specifically, Germany now provides judicial review of foreign-foreign intelligence collection, grants oversight agencies direct access to IT-databases and operational systems and, in all likelihood, contains the world's most detailed legal provisions regarding the dos and don'ts when it comes to (automatic) international data transfers, with separate articles devoted to their authorization, documentation and corresponding judicial and administrative oversight. This includes specific obligations on the part of the BND to restrict the subsequent use of shared data by partner services.

IX. CONCLUSION

Despite the important constitutional differences that exist across rule-of-law systems, many democracies face similar threats to their internal and external security. They also experience similar challenges when it comes to the democratic governance of their responses to these threats. Generally speaking, the systematic review of democracy's attempts to align key objectives of security and freedom promises great potential for good practice exchanges and mutual learning. This seems particularly important at a time when the rapid evolution of technology and the ubiquity of data profoundly affect the very practice and the governance of intelligence collection.

This chapter has shed light on German surveillance norms and standards. It has argued that Germany has substantially professionalized the governance of its electronic surveillance in recent years. This said, the author also highlighted significant challenges and pointed to the Bundestag's unfinished homework going forward.

While the unique trajectory of each democracy may resist direct comparative assessments or rankings, this new repository of surveillance standards and norms across liberal democracies will hopefully show how much they have in common and where opportunities for further refinements exist. It is this constant work in progress and genuine efforts at intelligence accountability that allow our democracies to credibly repudiate unconstrained electronic surveillance by authoritarian regimes.

X. BIBLIOGRAPHY

Bäcker, Matthias. (2022). Verfassungsbeschwerde gegen einzelne Paragraphen des BND-Gesetzes. Available at https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/BNDGII_Beschwerdeschrift_anonymisiert.pdf.

Bewarder, Manuel und Flade, Florian. (2023). Lauschangriff? Erlaubt!. Abrufbar unter: https://www.tagesschau.de/investigativ/ndr-wdr/bnd-unabhaengiger-kontrollrat-101.html.

Bradford Franklin, Sharon. (2020). "A Key Part of Surveillance Reform Is Now in Jeopardy." Slate Magazine. Available at: https://slate.com/technology/2020/05/usa-freedom-reauthorization-act-fisa-reform-surveillance-amicus-curiae.html.

Biselli, Anna. (2020). Bundesverfassungsgericht verhandelt zwei Tage lang über das BND-Gesetz. Liveblog. Available at netzpolitik.org.

Brissa, Enrico. (2011). Militärischer Auslandsgeheimdienst der Bundeswehr? Die öffentliche Verwaltung, pp. 391–398.

CTIVD/TIB. (2021). Joint Memo on Convention 108+. Available at: https://www.ctivd.nl/documenten/publicaties/2021/02/17/memo-en.

Deutscher Bundestag. (2016). Unterrichtung durch das Parlamentarische Kontrollgremium. Drucksache 18/9142. Available at: https://dserver.bundestag.de/btd/18/091/1809142.pdf.

Deutscher Bundestag. (2022). Unterrichtung durch das Parlamentarische Kontrollgremium. Drucksache 20/4976. Available at: https://dserver.bundestag.de/btd/20/049/2004976.pdf.

EU Fundamental Rights Agency (FRA). 2023. Surveillance by intelligence services: Fundamental rights safeguards and remedies in the EU - 2023 update. Available online at: https://fra.europa.eu/en/publication/2023/surveillance-update.

Gebauer, Matthias et al. (2023). Enttarnter Spion beim BND: Der Verräter. Available at: https://www.spiegel.de/politik/deutschland/bnd-warum-ein-mutmasslicher-spion-zugang-zu-brisanten-informationen-hatte-a-59133840-4d22-4db7-9ab2-ccc9e46b6557.

Gusy, Christoph. (2011). Grundrechte und Verfassungsschutzrecht. (VS Verlag für Sozialwissenschaften: Wiesbaden.

Hochl, Josef, Schmidt-Räntsch, Johanna. and Philipp Brunst. (2023). Ein Jahr Rechtskontrolle der technischen Auslandsaufklärung des Bundesnachrichtendienstes. In: NVwZ (10), 712-717.

Hoppenstedt, Max, and Wiedmann-Schmidt, Wolf. (2020). So überwacht der BND das Internet. Available at: https://www.spiegel.de/netzwelt/netzpolitik/.

Löffelmann, Markus and Mark Zöller. (2022). Nachrichtendienstrecht (Nomos: Baden-Baden).

Meister, Andre. (2023). ZITiS Gesetz: Bundesregierung will Hacker-Behörde ausbauen. Available at: https://netzpolitik.org/2023/zitis-gesetz-bundesregierung-will-hacker-behoerde-ausbauen/.

Papier, Hans-Jürgen and Johannes Möller. (1997). Das Bestimmtheitsgebot und seine Durchsetzung. In: Archiv des öffentlichen Rechts, Vol. 122, No. 2, pp. 177–211.

Poscher, Ralf and Kilchling, Michael and Landerer, Lukas. (2022). Überwachungsbarometer für Deutschland: Ein Modellkonzept. Available at: www.freiheit.org.

Sosna, Sabine. (2022). An oversight body operating below the radar of public perception? (English translation of the orginal article published in Zeitschrift für das Gesamte Sicherheitsrecht (GSZ Issue Nr. 6: 245-251).

Steiner, Elisabeth. (2023). Zur Leistungsfähigkeit der gerichtlichen Vorabkontrolle der technischen Auslandsaufklärung des Bundesnachrichtendienstes. In: Zeitschrift für das Gesamte Sicherheitsrecht, Issue Nr. 3, 124-130.

Vieth-Ditlmann, Kilian and Thorsten Wetzling. (2021) Caught in the act? An analysis of Germany's new SIGINT reform. (Stiftung Neue Verantwortung: Berlin).

Wetzling, Thorsten (2021). Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts und des Bundesverwaltungsgerichts. Available at: bundestag.de.

Wetzling, Thorsten and Charlotte Dietrich. (2022). Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform? (Stiftung Neue Verantwortung: Berlin). Available at: https://www.stiftung-nv.de/sites/default/files/snv_commercially_available_data.pdf.pdf.

Wetzling, Thorsten and Kilian Vieth-Ditlmann. (2023). Mehr Rechtskontrolle wagen: Warum das Mandat des Unabhängigen Kontrollrats erweitert werden sollte. (Stiftung Neue Verantwortung: Berlin). Available at: https://www.stiftung-nv.de/sites/default/files/snv_impuls_mehr_rechtskontrolle_wagen.pdf.

XI. APPENDIX

1. As mentioned in Section 4, the following tables provide further information on the different warrant types, their codification in the respective legal framework and the corresponding review competences of the UKR.

Warrant types and their legal basis in the BND Act:

Warrant Type	Corresponding legal provision(s)
General warrant to collect foreign communications data in bulk	§ 23(1) in connection with § 19(1)
Special collection warrants: **"EU warrant"**: Collection of personal data of bodies of the EU, public bodies in the member states of the EU or EU citizens. **"Threat prevention warrant"**: Collection of personal data of individuals to prevent threats or for transfer to law enforcement. **"Professional secrecy warrant"**: Collection of personal data related to protected professional communications.	§ 23(5) in connection with: § 20(1) § 20(2) § 21(2)
Computer network exploitation warrant.	§ 37(1) in connection with § 34(1)

Approval and review mandate of the UKR:

***Ex ante* approval of the lawfulness of:**	***Ex post* review of the 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), 30 (9), 38(8)).
	- Processing of data related to protected professional groups (§§ 21(3), 35(3)).
	- Domestic and transnational transfer of data collected for information purposes (i.e., change of purpose) (§§ 29(7), 30(5), 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).

2. As mentioned in section V, above, the table below provides further information on the legal requirements with regard to international cooperation in the field of signals intelligence.

Lawful aims of cooperations (BND Act § 31(5))	**Necessary binding assurances** (BND Act § 31(4))
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; and 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; and h. traffic data is only retained for up to six months.

ENDNOTES

1. Each state of the German federation has its own domestic intelligence service. They are overseen by separate parliamentary and quasi-judicial oversight institutions at the state level. Each of these institutions has their own statutory footing. For example, consider the Bavarian legal framework for state-level domestic intelligence. It consists inter alia of the law on the Bavarian intelligence service (BayVerfschG) and the law regarding the pre-approval and ex post oversight entities (*Ausführungsgesetz* Art. 10-Gesetz and BayPKGG, respectively). Bayern Recht, *Inhaltsverzeichnis*, Bayerische Staatskanzlei (Nov. 8, 2010), https://www.gesetzce-bayern.de/Content/Document/BayPKGG. One finds similar information for each of the 16 states within the German Federal Republic. While notable differences regarding the individual surveillance powers of state-level intelligence services and their quasi-judicial and parliamentary control exist, most states have more or less mirrored the structures in place at the federal level for domestic intelligence.
2. Enrico Brissa argued in 2011 that "the Bundeswehr's military intelligence system does not have a sufficiently clear legislative basis. Parliamentary control of this area is also much less pronounced than in the case of the intelligence services." *See* Enrico Brissa, MILITÄRISCHER AUSLANDSGEHEIMDIENST DER BUNDESWEHR? DIE ÖFFTENLICHE VERWALTUNG (2011), 391 (author's translation).
3. In turn, this invites creative non-compliance or collusive delegation whereby competences with regard to data processing are being delegated to elements that are less rigorously overseen than others. For more on this, *see* Thorsten Wetzling, *Stellungnahme zum Entwurf eines Gesetzes zur Änderung des BND-Gesetzes zur Umsetzung der Vorgaben des Bundesverfassungsgerichts und des Bundesverwaltungsgerichts*, bundestag.de (Feb. 21, 2021), 16–17, https://www.bundestag.de/resource/blob/823556/760abb7961fa7df144e1bc834702d44f/A-Drs-19-4-731-F-data.pdf; Matthias Bäcker, *Verfassungsbeschwerde gegen einzelne Paragraphen des BND-Gesetzes*, freiheitsrechte.org (Dec. 29, 2022), https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/BNDGII_Beschwerdeschrift_anonymisiert.pdf. More generally, unlike Canada or the United Kingdom, Germany does not adhere to a functional logic when it comes to its design of pre-approval and oversight institutions. Whereas the remit of oversight bodies such as IPCO (UK) and NSIRA (Canada) extend beyond individual intelligence services to any government agency's use of investigatory powers for the purpose of national security, the mandate of relevant German pre-approval or oversight entities is restricted to cover only specific intelligence services.
4. BVerfGE 123, 186 <266>.
5. See Anna Biselli, Bundesverfassungsgericht verhandelt zwei Tage lang über das BND-Gesetz, Liveblog (Jan. 14, 2020), https://netzpolitik.org/2020/bundesverfassungsgericht-verhandelt-ueber-das-bnd-gesetz/.
6. *See* Christoph Gusy, GRUNDRECHTE UND VERFASSUNGSSCHUTZRECHT (2011), 3 (author's translation).
7. These rights and freedoms have been recognised (and developed) by the Federal Constitutional Court of Germany and have their statutory basis in the following norms, respectively: Arts. 1(1), 10(1) and 2(1) in conjunction with Arts. 1, 5(1) and Art 3(1) of Germany's Basic Law (*Grundgesetz*).
8. For a comprehensive analysis of the many changes to the German legal framework for foreign intelligence collection, see Kilian Virth-Ditlmann & Thorsten Wetzling, *Caught in the act? An analysis of Germany's new SIGINT reform*, Research Report, Stiftung Neue Verantwortung (Nov. 25, 2021), https://www.stiftung-nv.de/sites/default/files/caught-in-the-act_analysis-of-germanys-new-sigint-reform_0.pdf.
9. See the exception for so-called *Eilanordnungen* (urgency applications) in § 15a of the G10 Act.
10. Notice, however, that the law also includes provisions on how to proceed in special urgency or emergency situations, allowing the government in such exceptional cases to implement a surveillance measure prior to a decision by the G10 Commission. *See* G10 Act § 15a.
11. G10 Act Art. 15(6).
12. *See* the BVerfG decision from 2016 at 2 BvE 5/15, recital 54.
13. *Id.* at recital 41.
14. *See* 1 BvR 1016/93.
15. *See* 2 BvE 5/15, recital 54.
16. As argued convincingly by Sharon Bradford Franklin, current Chair of the U.S. oversight body PCLOB, with regard to this aspect in the FISA Court: "[T]o 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." Sharon Franklin, *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 (internal quotations omitted).
17. The law does not include further specifications of such "appropriate measures," however.
18. This rule, also known as the Originator Control Principle, requires that intelligence services must not share information they received from foreign agencies with other—third—parties without an explicit authorization to do so.

See 1 BvR 2835/17, recital 292.

19. *See* 1 BvR 2835/17, recital 292.

20. Notice that while the UKR is exempt from the third-party rule, this does not apply to the Bundestag's oversight bodies, which are *de facto* considered as a third party in the context of information sharing. This has consequences for the UKR's reporting to the parliamentary committee: Only information that is under the exclusive control of the BND may be included. The UKR must consult the Federal Chancellery before reporting to the parliamentary committee to ensure that the report does not comprise third party information. BND Act § 55(2).

21. *See* Markus Löffelmann & Mark Zöller, Nachrichtendienstrecht (2022), 263 (author's translation). For a synopsis of the meaning and relevance of so-called suitability tests, see n. 34, below.

22. *See* Sabine Sosna, An oversight body operating below the radar of public perception?, GSZ Issue No. 6 (2022) (English translation of the original article published in Zeitschrift für das Gesamte Sicherheitsrecht); Thorsten Wetzline & Kilian Vieth-Ditlmann, *Mehr Rechtskontrolle wagen: Warum das Mandat des Unabhängigen Kontrollrats erweitert werden sollte*, Stiftung Neue Verantwortung (May 2023), https://www.stiftung-nv.de/sites/default/files/snv_impuls_mehr_rechtskontrolle_wagen.pdf.

23. *See* Matthias Gebauer et al., *Enttarnter Spion beim BND: Der Verräter*, Der Spiegel (Jan. 2023), https://www.spiegel.de/politik/deutschland/bnd-warum-ein-mutmasslicher-spion-zugang-zu-brisanten-informationen-hatte-a-59133840-4d22-4db7-9ab2-ccc9e46b6557.

24. *See* Max Hoppenstedt & Wolf Wiedmann-Schmidt, *So überwacht der BND das Internet*, Der Spiegel (May 19, 2020), https://www.spiegel.de/netzwelt/netzpolitik/bundesnachrichtendienst-so-ueberwacht-der-bnd-das-internet-a-216ebe9a-6f22-4883-b1c9-ac5d1442497a.

25. *See* Deutscher Bundestag, Unterrichtung durch das Parlamentarische Kontrollgremium, Drucksache 18/9142 (July 7, 2016), https://dserver.bundestag.de/btd/18/091/1809142.pdf.

26. There are, of course, provisions in the legal framework on automated data minimization as well as restrictions on data handling. Still, the labyrinth of different procedural requirements and oversight bodies assigned to similar practices will hopefully be trimmed and streamlined in future reforms. See also discussion in section VII, below.

27. *See* Markus Löffelmann & Mark Zöller, NACHRICHTENDIENSTRECHT (2022), 173.

28. Bulk collection against domestic targets is not permissible. There can, however, be systematic and automated Open-Source Intelligence collection and other forms of non-compulsory government access to commercially and publicly available data. See Thorsten Wetzling & Charlotte Dietrich, *Disproportionate use of commercially and publicly available data: Europe's next frontier for intelligence reform?*, Stiftung Neue Verantwortung (Nov. 2022), https://www.stiftung-nv.de/sites/default/files/snv_commercially_available_data.pdf.pdf.

29. *See* Markus Löffelmann & Mark Zöller, NACHRICHTENDIENSTRECHT (2022), 141.

30. *See* G10 Act § 5(2).

31. According to BND Act § 19(7), bulk collection of personal data from foreign telecommunication traffic is not permitted when the data relates to German nationals, domestic legal entities and persons residing in the Federal Republic of Germany.

32. Depending on the bulk collection measure envisaged, additional parameters might be necessary in the written application. For example, special restraints apply when the measure interferes with the rights of persons whose professional communication is subject to special protection, or when the measure affects the communication of public offices of the EU or its member states. See BND Act § 23(5)–(6) in relation to §§ 20, 21(2).

33. *See* 1 BvR 2835/17. The Constitutional Court provides an English translation of this judgment here: https://www.bundesverfassungsgericht.de/SharedDocs/Downloads/EN/2020/05/rs20200519_1bvr283517en.pdf?__blob=publicationFile&v=1#page=1.

34. Beyond the general authority to conduct bulk surveillance, the BND Act allows also for another form of bulk collection, albeit with 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 (BND Act § 19(5)), the BND may perform so-called suitability tests (*Eignungsprüfungen*; BND Act § 24) 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). According to the government, such suitability testing is necessary 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 such as New Zealand, 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. For further details, see Kilian Vieth-Ditlmann & Thorsten Wetzling, CAUGHT IN THE ACT? AN ANALYSIS OF GERMANY'S NEW SIGINT REFORM (2021).

35. *See* Elisabeth Steiner, Zur Leistungsfähigkeit der gerichtlichen Vorabkontrolle der technischen Auslandsaufklärung des Bundesnachrichtendienstes, Zeitschrift für das Gesamte Sicherheitsrecht no. 3, 124 (2023).

36. *Id*. at 130 (author's translation).

37. *Id.* at 130 (author's translation).

38. For an argument in support of an adversarial process to prevent secret courts from becoming a "rubber stamp" for government surveillance requests, s*ee* n. 16, above.

39. 1 BvR 2835/17, recital 93. The Court also held that "the binding effect of German fundamental rights entails accountability and

responsibility solely on the part of German state organs. It only applies to autonomous political decisions made by the Federal Republic of Germany and solely limits Germany's own latitude. Accordingly, in other countries German fundamental rights – in their dimension as rights against state interference – are only applicable vis-à-vis German state authority and are thus in line with the restrictions arising from the principle of non-intervention under international law. Thus, the binding effect of fundamental rights does not amount to a violation of the principle of non-intervention or to a restriction of other states' executive or legislative powers. It neither imposes German law on other states, nor does it supplant the fundamental rights of other states. In particular, the binding effect of fundamental rights does not extend German state powers abroad but limits potential courses of action of German state authority." *Id.* at recital 101 (author's translation).

40. *Id.* at recitals 269–70 (author's translation).

41. Hans-Jürgen Papier & Johannes Möller, *Das Bestimmtheitsgebot und seine Durchsetzung*, 122 Archiv des öffentlichen Rechts 177, 177 (1997), accessible at https://www.jstor.org/stable/44316314 (author's translation).

42. 1 BvR 2835/17, recital 192.

43. Consider, also, for example, the provision which now stipulates that eight (!) binding assurances (on different data use aspects) have to be included in written memoranda of understanding that the BND signs with foreign partners (BND Act § 31(4), nr. 3, littera a–h). Furthermore, as regards protected professional communications and international SIGINT cooperation, the BND is now legally required under the BND Act to 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 (BND Act § 32(5)).

44. *See* Markus Löffelmann & Mark Zöller, NACHRICHTENDIENSTRECHT (2022), 253.

45. *See* Matthias Bäcker, Verfassungsbeschwerde gegen einzelne Paragraphen des BND-Gesetzes, freiheitsrechte.org, 65 (Dec. 29, 2022), https://freiheitsrechte.org/uploads/documents/Freiheit-im-digitalen-Zeitalter/BNDGII_Beschwerdeschrift_anonymisiert.pdf.

46 *See Privacy International v. Secretary of State for Foreign and Commonwealth Affairs* (Oct. 6, 2020), Case C-623/17, EU:C:2020:790, Secretary of State for the Home Department, Government Communications Headquarters, Security Service, Secret Intelligence Service, Judgement of the Court of Justice (Grand Chamber).

47. This goes beyond the scope of this article but interested readers are invited to consult this brief memo jointly produced by two Dutch intelligence oversight bodies on this Convention of the Council of Europe and its importance for future intelligence governance. *See Council of Europe Convention 108+ and oversight on national security*, Review Committee on the Intelligence and Security Services (CTIVD) & Investigatory Powers Commission (TIB), Memo (Feb. 2021), https://www.ctivd.nl/documenten/publicaties/2021/02/17/memo-en.

48. 1 BvR 2835/17, recitals 168–69 (author's translation).

49. See G10 Act § 10(4); BND Act §§ 19, Abs. 8.

50. The use of specific search terms must be determined and be deemed appropriate prior to their use on the raw data stream (G10 Act §§ 5(2), sentence 1, 10(4)). The legal framework governing bulk collection of international communications requires that the BND collect and process content data only with the help of search terms. The BND Act states also that it is not necessary to list individual search terms in the bulk interception warrants (BND Act § 23(6)), 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 (BND Act § 42). 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. The processing of metadata also does not require the use of search terms and is not covered by the requirements of § 19 of the BND Act.

51. The administrative control body has 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 (BND Act § 52). 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.

52. For an insightful commentary on the initial performance of the UKR by members of this body, see Elisabeth Steiner, Zur Leistungsfähigkeit der gerichtlichen Vorabkontrolle der technischen Auslandsaufklärung des Bundesnachrichtendienstes, Zeitschrift für das Gesamte Sicherheitsrecht no. 3, 124 (2023); Josef Hochl, Johanna Schmidt-Räntsch & Philipp Brunst, *Ein Jahr Rechtskontrolle der technischen Auslandsaufklärung des Bundesnachrichtendienstes*, 10 NVwZ 712 (2023). For a discussion on possible future extensions of the UKR mandate, see Thorsten Wetzling & Kilian Vieth-Ditlmann, Mehr Rechtskontrolle wagen: *Warum das Mandat des Unabhängigen Kontrollrats erweitert werden sollte*, Stiftung Neue Verantwortung (May 2023), https://www.stiftung-nv.de/sites/default/files/snv_impuls_mehr_rechtskontrolle_wagen.pdf.

53. Manuel Bewarder & Florian Flade, *Lauschangriff? Erlaubt!*, tagesschau (April 21, 2023), https://www.tagesschau.de/investigativ/ndr-wdr/bnd-unabhaengiger-kontrollrat-101.html.

54. See 1 BvR 2354/13 and 1 BvR 1619/17.

55. See, for example, the recent update of the EU's Fundamental Rights Agency reporting on intelligence legislation. Among other interesting observations, one learns therein that "five of 27 EU Member States have detailed provisions on general surveillance of communications (bulk surveillance). Out of these 5 Member States, only 3 Member States provide for binding involvement of an independent body in the authorization of measures" (FRA 2023: 9).