



In their current form, the Federal Intelligence Service's powers to conduct surveillance of foreign telecommunications violate fundamental rights of the Basic Law

Press Release No. 37/2020 of 19 May 2020

Judgment of 19 May 2020

1 BvR 2835/17

(Federal Intelligence Service – foreign surveillance)

In its judgment pronounced today, the First Senate of the Federal Constitutional Court held that the Federal Intelligence Service (*Bundesnachrichtendienst* – BND) is bound by the fundamental rights of the Basic Law when conducting telecommunications surveillance of foreigners in other countries, and that the statutory bases in their current design violate the fundamental right to the privacy of telecommunications (Art. 10(1) of the Basic Law, *Grundgesetz* – GG) and freedom of the press (Art. 5(1) second sentence GG). This applies to the collection and processing of data, the sharing of data thus obtained with other bodies and the cooperation with foreign intelligence services. At the same time, the Court held that statutory bases for the surveillance of foreign telecommunications can be designed in conformity with the Constitution.

The Court held that, under Art. 1(3) GG, German state authority is bound by the fundamental rights of the Basic Law and that this binding effect is not restricted to German territory. At least Art. 10(1) and Art. 5(1) second sentence GG, which, in their dimension as rights against state interference, afford protection against telecommunications surveillance, also protect foreigners in other countries. This applies irrespective of whether surveillance is conducted from within Germany or from abroad. As the legislator assumed that fundamental rights were not applicable in this matter, the requirements arising from these fundamental rights were not satisfied, neither formally nor substantively. The legislator did not adhere to the requirement to expressly specify affected fundamental rights (*Zitiergebot*) with regard to Art. 10(1) GG, nor do the provisions satisfy the key substantive requirements arising from fundamental rights. In particular, the surveillance measures are not restricted to sufficiently specific purposes and thereby structured in a way that allows for oversight; various safeguards are lacking as well, for example with respect to the protection of journalists or lawyers. Regarding data sharing, the provisions lack a limitation to the protection of legal interests of sufficient weight and sufficient statutory thresholds for data sharing. The provisions governing cooperation with foreign intelligence services also do not contain sufficient restrictions or safeguards. The powers under review are also not subject to comprehensive independent oversight. Such oversight must be designed as continual legal oversight that allows for comprehensive access to scrutinise the surveillance process.

If the powers were designed in accordance with the principle of proportionality, however, the surveillance of foreign telecommunications would, in principle, be compatible with the fundamental rights of the Basic Law. Therefore, the challenged provisions may continue to apply until the end of 2021 in order to allow the legislator to enact new provisions taking into account the constitutional requirements.

Facts of the case:

The complainants are mostly journalists who report on human rights violations in conflict zones and in authoritarian states. With their constitutional complaint, they challenge the amended version of the Federal Intelligence Service Act (*Gesetz über den Bundesnachrichtendienst*, BNDG) of 2016 as well as the surveillance measures to which they could be subjected according to this legislation. The amendment of the Act created – for the first time – a statutory basis for the Federal Intelligence Service's practice of strategic surveillance of foreign telecommunications. It grants the Service powers to access telecommunications transmission routes and networks to collect telecommunications data in order to then identify telecommunications that are of interest to the intelligence services from the collected data by using search terms (selectors), other tools of analysis and by a subsequent manual analysis. According to the challenged provisions,

data regarding telecommunications involving German nationals or persons within Germany must be separated from the other data and deleted prior to any further analysis; such data may be collected incidentally for technical reasons, but is excluded from examination or use by the Intelligence Service.

As a form of strategic surveillance, these powers are not tied to specific grounds or suspicions; rather, in relation to communications between foreigners in other countries, they can be used generally to obtain information indicating situations of danger or general intelligence that is of interest to Germany in foreign or security policy matters. Under these powers, every single instance of telecommunication can be collected. As such, the use of these powers is not subject to objective statutory thresholds, but merely guided and restricted by the purpose pursued. Surveillance may be based on content-related search terms that do not target specific individuals as well as on formal search terms (such as telecommunications identifiers), which are most common in practice; it can thus also target specific individuals. Traffic data can be retained and analysed irrespective of search terms for six months.

The constitutional complaint is primarily directed against the novel legal provisions allowing the Federal Intelligence Service to collect, store and analyse data in the context of the surveillance of foreign telecommunications. Additionally, it challenges the previously existing provisions that authorise the Federal Intelligence Service to share with domestic and foreign bodies the information it has obtained, insofar as these provisions now also extend to the sharing of data obtained under the newly created powers. These provisions allow the Federal Intelligence Service in specific cases, subject to certain conditions, to share information it has obtained with domestic public bodies (especially the police and public prosecution office), foreign public bodies and private bodies. These powers regarding data sharing apply irrespective of the statutory basis on which the data was collected and extensively refer to provisions contained in other statutes, particularly the provisions on sharing contained in the Federal Protection of the Constitution Act (*Bundesverfassungsschutzgesetz*). The constitutional complaint is also directed against powers that allow the Federal Intelligence Service to cooperate with foreign intelligence services when conducting foreign surveillance. These include the filtering of data traffic collected by the Federal Intelligence Service on the basis of search terms determined by the foreign partners as well as the automated sharing of any matches with the cooperating partners; it also includes the automated sharing of unfiltered traffic data.

These proceedings do not concern the powers of the Federal Intelligence Service to conduct strategic surveillance of telecommunications in which German nationals or persons within Germany are involved on at least one side (§§ 5 *et seq.* of the Act Restricting The Privacy of Correspondence, Posts and Telecommunications, *Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*).

Key considerations of the Senate:

I. With its decision, the Federal Constitutional Court has clarified for the first time that the protection afforded by fundamental rights vis-à-vis German state authority is not restricted to the German territory.

1. Art. 1(3) GG provides that German state authority is comprehensively bound by the fundamental rights of the Basic Law. No restrictive requirements that make the binding effect of fundamental rights dependent on a territorial connection with Germany or on the exercise of certain sovereign powers can be inferred, neither from the provision itself nor from its legislative history or position in the systematic framework of the Basic Law. Rather, the Basic Law's aim to provide comprehensive fundamental rights protection and to place the individual at its centre suggests that fundamental rights as rights of the individual ought to provide protection whenever the German state acts and thus potentially creates a need for protection – irrespective of where, towards whom and in what manner it does so. In any event, this holds true for the fundamental rights at issue in the present case, which, in their dimension as rights against state interference, afford protection against surveillance measures.

This binding effect of fundamental rights even in relation to foreigners in other countries also reflects the participation of Germany in the international community. In Art. 1(2) GG, the Basic Law places fundamental rights in the context of international human rights guarantees that seek to provide protection beyond national borders and are afforded to individuals as human beings. Insofar as the Basic Law provides for certain fundamental rights as human rights rather than as rights that only apply to Germans, it follows that they apply accordingly to foreigners in other countries vis-à-vis German state authority. This does not amount to a violation of the principle of non-intervention under international law nor to a restriction of the executive or legislative powers of other states. Rather, it prevents a situation where fundamental rights protection can no longer keep up with the expanding scope of action of German state authority in the course of internationalisation and where it might even be undermined through the interaction and cooperation of different states.

2. The comprehensive binding effect of fundamental rights on German state authority does not alter the fact that their scope of protection can differ. The extent to which certain guarantees are applicable differs between Germany and other countries already with regard to the persons and subject matters afforded protection. Likewise, distinctions can be drawn between the different dimensions of fundamental rights – such as the effect fundamental rights have as rights against

state interference, as positive obligations of the state, as decisions on values enshrined in the Constitution, or as the basis for duties of protection. Where the state acts in a foreign environment, this must be taken into account all the more when setting requirements for the justification of interferences with fundamental rights in the context of proportionality.

3. The present case concerns the protection afforded by Art. 10(1) and Art. 5(1) second sentence GG as rights against the surveillance of foreign telecommunications conducted by the Federal Intelligence Service. Pursuant to Art. 1(3) GG, these fundamental rights are applicable in the case at hand; surveillance measures thus constitute an interference with these rights. Exempting surveillance measures by intelligence services from the binding effect of fundamental rights simply because they are directed at foreigners in other countries is alien to the Basic Law, just as exempting them from fundamental rights protection because of their political nature would be. Rather, the comprehensive binding effect of fundamental rights pursuant to Art. 1(3) GG creates the framework in which due consideration can be given to the risks to fundamental rights that arise from new technological developments and from accompanying power shifts. In particular, this applies to the increasing significance of intelligence services that results from advances in information technology, which allow intelligence services a wider reach in other countries.

4. The protection against state surveillance measures afforded by fundamental rights extends to communications of persons who act on behalf of foreign legal entities (*Funktionsträger*). This is not changed by the fact that those on whose behalf they act and communicate – for example foreign media outlets – cannot themselves invoke these fundamental rights.

II. Based on the foregoing, the Federal Constitutional Court held that the challenged powers of the Federal Intelligence Service are unconstitutional for formal reasons.

1. However, there are no objections with regard to legislative competence. The powers to conduct foreign telecommunications surveillance can be based on the Federation's legislative competence for foreign affairs pursuant to Art. 73(1) no. 1 GG. This competence does not include the investigation of all crimes involving a foreign element as such. However, on the basis of this competence, the Federation can confer upon the Federal Intelligence Service not only the task of providing political intelligence to the Federal Government. The Federal Intelligence Service can also be tasked with the separate responsibility of early detection of impending dangers originating from abroad that have an international dimension as long as this does not give rise to operational powers. These dangers must be of such nature and gravity that they can affect the position of the Federal Republic of Germany in the international community and they must be significant to foreign and security policy precisely for this reason.

2. However, the challenged provisions are formally unconstitutional, as they authorise interferences with the privacy of telecommunications under Art. 10(1) GG without adhering to the requirement to expressly specify affected fundamental rights, which is enshrined in Art. 19(1) second sentence GG. If the legislator does not consider fundamental rights to be applicable, it is not aware that it is authorising interferences with fundamental rights and is not willing to account for their consequences. Yet this is the very purpose of the requirement to expressly specify affected fundamental rights.

III. In substantive terms, too, the provisions do not satisfy key requirements deriving from fundamental rights. Firstly, this concerns the framework on telecommunications surveillance itself.

1. Strategic telecommunications surveillance as a special instrument for gathering foreign intelligence is in principle compatible with Art. 10(1) GG. However, given that it is not based on specific grounds and instead guided and restricted only by the purpose pursued, the power to conduct strategic telecommunications surveillance is an exceptional power that must be limited to the gathering of foreign intelligence conducted by an authority that itself has no operational powers; it can only be justified by the authority's particular tasks and the specific conditions under which these tasks must be performed.

a) Strategic surveillance of foreign telecommunications results in interferences of particularly great weight. The interferences are of such great weight because this instrument is used to covertly intrude into personal communications. It is true that it is typically less precisely targeted than surveillance of individual telecommunications ordered by warrant in the individual case, and does not give rise to operational consequences in the same manner as surveillance measures targeting Germans or persons within Germany, who are within closer reach of the German state. However, the exceptionally broad scope and the indiscriminate effect of strategic telecommunications surveillance is particularly aggravating. Such surveillance can be used against anyone without specific grounds; objective thresholds for the use of these powers are not required, neither with regard to the situations that can give rise to surveillance measures nor with regard to the individuals that may be affected by them. Such powers have an exceptional reach, particularly given the realities of modern information technology and its significance for communication relations. It must be taken into account that – unlike in previous decisions of the Court on telecommunications surveillance – they allow for targeted surveillance of specific individuals and open up the possibility of retention and holistic analysis of unselected traffic data. Today, this instrument allows for the analysis and collection of highly private and spontaneous communication processes reaching deep into everyday life as well as the identification of interests, desires and preferences reflected in Internet usage.

b) Despite the gravity of strategic surveillance measures, they can be justified under constitutional law as specific powers for gathering foreign intelligence. This is mainly due to the special circumstances of state action on foreign territory and the difficulties of gathering intelligence abroad; the legislator may exceptionally react to these specific difficulties by not limiting the use of surveillance powers to objective thresholds. The exceptionally significant public interest in effective foreign surveillance is also an important factor in justifying such powers. The supply of information to the Federal Government for its decision-making on matters of foreign and security policy helps it to assert itself in the realm of international power politics and can prevent erroneous decisions that could have serious consequences. This indirectly bears on safeguarding democratic self-determination and protecting the constitutional order – and thus on high-ranking constitutional interests. It is important to see that threats originating from abroad have increased significantly as part of the advances in information technology and international communication as well as the closer interconnectedness of living conditions across borders. In this context, the early detection of dangers originating from abroad takes on particular importance for public security. The expansion and internationalisation of communication possibilities and the resulting increased politicisation and ability to organise of international criminal gangs mean that domestic situations of danger frequently originate in networks of actors cooperating internationally and that they can easily have foreign and security policy dimensions. A further aspect supporting the argument that strategic telecommunications surveillance is justifiable is that the consequences of undertaking such surveillance without specific grounds are somewhat mitigated by the fact that it is conducted by an authority that, in principle, has no operational powers itself.

2. Strategic surveillance must be designed in line with the tasks of gathering foreign intelligence and on this basis be restricted in accordance with the principle of proportionality. For the most part, the challenged provisions do not satisfy this requirement.

a) The Basic Law 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.

b) The law must clearly provide that prior to a manual analysis domestic communications and, as the case may be, communications involving Germans or persons within Germany on at least one side be separated from the other data as far as scientifically and technically possible. It must be ensured that, in the event that such filtering is not successful, the respective data is immediately deleted during manual screening. There may only be very limited exceptions, which must be provided for by law.

c) The legislator must determine the purposes of surveillance with sufficient precision and legal clarity. If strategic surveillance serves to identify dangers, it must be substantially restricted to limited and specific purposes of great weight. Insofar as surveillance is only intended to help prepare governmental decisions, the law can allow it for the entire range of tasks performed by the Federal Intelligence Service. However, a change in purpose or the sharing of data with other bodies must then generally be ruled out.

d) To compensate for the lack of objective thresholds for the use of powers, surveillance measures must be broken down into formally determined and sufficiently specific categories. Procedural safeguards must ensure that surveillance measures are based on specific purposes and thus allow for oversight. The legislator itself must set out the essential framework for the analysis of collected data. This includes the requirement to analyse data without undue delay, the applicability of the principle of proportionality to the selection of search terms, provisions governing the use of intrusive methods of data analysis, and adherence to specific prohibitions of discrimination.

e) The power to store and retain traffic data in its entirety in the context of gathering foreign intelligence must be restricted with regard to the volume of data that can be collected; it may not be stored for more than six months.

f) In relation to foreigners, targeted surveillance of the communications of specific individuals, for example on the basis of an identifier, is not generally impermissible. Nonetheless, restrictions are required that take into account the affected persons' need for protection. The law must definitively set out the reasons and aspects subject to which strategic surveillance measures may target specific individuals. In this respect, the legislator must create a separate mechanism for the protection of individuals that could be of direct interest to the Intelligence Service, either because they might cause danger or because of follow-up measures to be taken against them.

g) In addition to this, special requirements apply to the protection of professional groups or groups of persons whose communications require special confidentiality protection. The targeted intrusion into such relationships of trust meriting confidentiality protection, for example involving lawyers or journalists, cannot be justified simply because the desired information might be of use to intelligence services. Rather, targeted surveillance of such groups must be tied to qualified thresholds for the use of powers. If it only becomes apparent during analysis that data concerning relationships of trust meriting special confidentiality protection has been collected, an additional balancing is required to determine whether the respective communications may be analysed and used. Which relationships merit protection is determined on the basis of the decisions on values enshrined in the fundamental rights of the Basic Law.

h) Furthermore, the legislator must take into account the core of private life. Analysis must cease as soon as it becomes apparent that surveillance is encroaching on the core of private life; even where mere doubts arise, the measure may only be continued in the form of recordings that are examined by an independent body prior to analysis. Intelligence relating to the highly personal domain may not be used and must be deleted immediately.

i) Finally, the principle of proportionality gives rise to deletion obligations. The legislator must ensure that data does not remain stored without justification by creating obligations to monitor data storage at sufficiently short intervals. The key steps of data deletion must be documented insofar as this is sensible and necessary for independent oversight.

IV. The challenged provisions on the sharing of intelligence obtained through foreign surveillance with other bodies are not sufficiently restrictive either.

1. The sharing of personal data obtained through strategic surveillance with other bodies constitutes a separate interference with fundamental rights and requires – in accordance with established case-law – its own clear and sufficiently specific statutory basis.

a) As data collection in the context of strategic surveillance does not require a threshold for the use of powers that is tied to specific grounds, it must be ensured that corresponding thresholds instead apply to the sharing of intelligence thus obtained. Accordingly, sharing is only proportionate if it were lawful to re-collect the personal data that is to be shared using comparably intrusive means (“hypothetical re-collection of data”). This requires that the aim of sharing is the protection of legal interests of particularly great weight and that the intelligence is sufficiently specific – as would be necessary for the surveillance of private homes. The sharing of data requires a separate assessment and formal decision by the Federal Intelligence Service and must be documented specifying the applicable legal basis.

b) In contrast, directly sharing personal data with the Federal Government is permissible without further requirements, insofar as it is exclusively intended to provide politically relevant intelligence and prepare government decisions. The Federal Government can only share this information with other bodies subject to the aforementioned general requirements on sharing. Insofar as the surveillance measure was justified exclusively by the aim to provide politically relevant intelligence to the Federal Government from the outset, and was not linked to any aim of early detection of dangers, sharing the data is in principle precluded; it is only permissible subject to narrowly restricted exceptional cases.

c) Insofar as data is shared with foreign bodies, the legislator must set out a requirement for ascertaining that the recipient will handle the data in accordance with the rule of law. This includes ascertaining that requirements under data protection law are satisfied in the recipient country and that fundamental human rights principles are adhered to when using the data obtained. If there is any indication that data sharing could put affected individuals in jeopardy, an assessment of possible risks in the individual case is required.

2. None of the challenged rules on data sharing in § 24 BNDG and none of the provisions of the Federal Protection of the Constitution Act referred to therein satisfy these requirements.

V. The provisions on cooperation with other intelligence services do not satisfy the constitutional requirements either.

1. As a constitutional order that is open to international law and international cooperation, the Basic Law permits cooperation with foreign intelligence services. However, it requires clear statutory provisions ensuring that the limits set by fundamental rights are not circumvented in the context of the cooperation and exchange between intelligence services. Particularly, the statutory provisions must prevent the sharing of intelligence stemming from surveillance measures of foreign intelligence services that target Germany. Such further sharing of data received from foreign partners (*Ringtausch*) is prohibited under constitutional law. Furthermore, the Federal Intelligence Service must essentially remain responsible for the data it has collected and analysed. The protection afforded by fundamental rights also entails an obligation of the German state to protect individuals under Germany’s jurisdiction against surveillance measures conducted by other states in violation of fundamental rights.

2. To collect and use data in the context of cooperation with other intelligence services, the legislator must first give effect to the requirements regarding strategic surveillance set out above.

3. Specific requirements apply where the Federal Intelligence Service is asked to use externally determined search terms to automatically share any matches with cooperating intelligence services. This requires a thorough assessment of the search terms determined by foreign services and the resulting matches. For this purpose, cooperating services must provide information on the search terms. Additionally, the Federal Intelligence Service must again ensure that groups of persons meriting special protection are protected as far as possible. Finally, automated sharing requires substantial assurances by the cooperating services, given that it places analysis of the data in their hands. Such assurances must reflect the fundamental rights protection of the individuals subjected to surveillance.

Furthermore, special requirements apply to the sharing of traffic data that has been collected in its entirety (“unselected data”). In this scenario, the Federal Intelligence Service hands over the data collected by it without the possibility to exercise any control. Therefore, such sharing of traffic data, as a continuous measure, cannot be authorised solely on the

basis of the purpose pursued. Rather, a qualified need for surveillance arising from the existence of specific indications of an identifiable danger (*konkretisierte Gefahrenlage*) is required. The cooperating services must assure the Federal Intelligence Service that the data will be deleted within six months at the latest.

VI. Finally, the challenged provisions do not satisfy the requirements for comprehensive independent oversight.

1. Rights to information of affected individuals vis-à-vis intelligence services can be restricted to the extent necessary for the effective performance of their tasks. The legislator may provide for exceptions to notification requirements that do exist in principle by balancing them against the constitutionally protected legal interests of third parties or in order to ensure the effective performance of the intelligence service's tasks. However, such exceptions must be restricted to what is absolutely necessary. In relation to individuals who are abroad, the legislator may, in principle, refrain from imposing notification requirements for strategic surveillance measures. Thus, the requirements for transparency of state action are significantly less strict and there are few possibilities for obtaining individual legal protection in practice. In order to adhere to the principle of proportionality, comprehensive independent oversight is required to compensate for this and to curtail the powers which are essentially only guided by the purpose pursued. Such oversight must be designed as continual legal oversight that allows for comprehensive access to scrutinise the surveillance process.

2. The oversight regime must serve two functions. Firstly, it must compensate for the gap in legal protection that follows from the weak possibilities for individual legal protection in practice, particularly given the exceptions to notification requirements. Secondly, to compensate for the fact that surveillance powers are essentially only guided by the purpose pursued, the oversight regime must ensure that the use of these powers adheres to the required procedural structure. On the one hand, it must be ensured that the key procedural steps of strategic surveillance – partially also *ex ante* – are subject to oversight that resembles judicial review and by a body that has the power to make final decisions. On the other hand, the measures must be subject to administrative oversight by a body that can conduct randomised oversight of the legality of the entire surveillance process on its own initiative.

3. Institutional independence of the oversight bodies must be guaranteed. This includes that the oversight bodies must have a separate budget, independent management of their personnel and procedural autonomy. They must be equipped with the personnel and resources required for the effective performance of their tasks. Substantively, they must have all powers necessary for conducting effective oversight vis-à-vis the Federal Intelligence Service. It must be ensured that oversight is not obstructed by the third party rule. Open and direct exchange between the oversight bodies must be guaranteed. There must also be a possibility to raise concerns with the head of the Federal Intelligence Service and, if necessary, the head of the Federal Chancellery (*Bundeskanzleramt*), as the authority responsible for administrative supervision of the Federal Intelligence Service. It must also be possible to take any criticism to Parliament and thus the public in an abstract manner that guarantees secrecy.

VII. Given that the powers in question are of great importance for ensuring the Federal Government's ability to act in political matters and given that they can, in principle, be designed in a way that is compatible with fundamental rights, the Federal Constitutional Court ordered that, despite their unconstitutionality, the challenged provisions continue to apply provisionally but only until 31 December 2021 at the latest.
