Constitutional complaints against investigatory powers of the Federal Criminal Police Office in the domain of counter-terrorism partially successful

Press Release No. 19/2016 of 20 April 2016

Order of 20 April 2016
1 BvR 966/09, 1 BvR 1140/09

In its judgment pronounced today, the First Senate of the Federal Constitutional Court decided that the statutory authorisation of the Federal Criminal Police Office (*Bundeskriminalamt*) to carry out covert surveillance measures in order to avert dangers posed by international terrorism is, in principle, compatible with fundamental rights. In some respects, however, the current design of the investigatory powers does not satisfy the principle of proportionality. The Federal Constitutional Court therefore held that certain individual provisions within the overall statutory framework were unconstitutional. Consolidating a long line of case-law, the decision addresses the prerequisites for carrying out of such covert surveillance measures and the permissibility of sharing data with other authorities for other purposes. For the first time, the Court also addresses the requirements subject to which data may be shared with authorities in other states.

With regard to the statutory prerequisites for carrying out covert surveillance measures, the provisions introduced in 2009 are in part too vague and too broad. Some also lack supplementary rule-of-law safeguards, particularly safeguards protecting the core of private life or ensuring transparency, and sufficient guarantees of individual legal protection and administrative oversight. Several parts of the provisions concerning data sharing are not sufficiently limited in scope, with respect to both authorities in Germany and in other states. Since the reasons for the unconstitutionality of the challenged provisions do not concern the actual substance of the statutory powers, the challenged provisions continue to apply, subject to certain conditions, until 30 June 2018.

In parts, the decision was not unanimous. Justices Eichberger and Schluckebier delivered dissenting opinions.

Facts of the case:

The constitutional complaints challenge investigatory powers that were introduced into the Federal Criminal Police Office Act (*Bundeskriminalamtgesetz* – BKAG) in 2009. The federal legislator extended the existing mandate of the Federal Criminal Police Office in the domain of law enforcement by assigning it new tasks in the domain of averting dangers to public security posed by international terrorism, a responsibility that had until then been within the exclusive competence of the *Länder* (federal states). The constitutional complaints also challenge a provision in the Federal Criminal Police Office Act that predates the amendment at issue and concerns the sharing of data with foreign authorities, the scope of which has been extended by the newly assigned tasks.

Further information on the background of the case can be found in Press Release No. 43/2015 of 16 June 2015 [in German].

Key considerations of the Senate:

1. The challenged powers authorise the Federal Criminal Police Office to covertly collect personal data for the purposes of averting dangers to public security and of preventing crime. Depending on the power in question, the measures result in interferences with the fundamental rights relating to the inviolability of the home, the privacy of telecommunications and informational self-determination, as well as the fundamental right to protection of the confidentiality and integrity of information technology systems. It is incumbent upon the legislator to balance the severity of these interferences against the duty of the state to protect the general public. The legislator must take into account, on the one hand, that the challenged powers for the most part authorise far-reaching interferences with the private sphere, and can, in individual cases, even intrude upon private refuges, the protection of which is of particular significance for safeguarding human dignity. On the other hand, the legislator must take into account that effective means of gathering information are of

great importance for averting terrorist dangers to the free democratic order and for the protection of fundamental rights. In this respect, the security of the state, as a constituted power of peace and order, as well as the security of the citizens it is bound to protect – while respecting the dignity and the intrinsic value of the individual – rank equally with other constitutional values that are accorded high standing.

2. The decision rendered by the Court fundamentally consolidates the existing case-law on the constitutional requirements that are relevant for achieving this balance. The powers assigned to the Federal Criminal Police Office are, in principle, not objectionable. However, where these powers constitute deep intrusions into the private sphere, which is the case for most of the powers at issue here, they are subject to certain general requirements resulting from the principle of proportionality. In particular, the powers must be limited to the protection of sufficiently weighty legal interests and are constitutional only if there is a sufficiently specific and foreseeable danger to these legal interests. Particularly strict standards apply when the investigatory powers affect persons who belong to the target person's contacts but are not themselves legally responsible for the danger. With regard to powers which typically lead to intrusions upon the strictly protected core of private life, specific safeguards are required. Moreover, privileged information from persons bound by professional confidentiality must be sufficiently protected. The investigatory powers at issue must also satisfy constitutional requirements regarding transparency, individual legal protection and administrative oversight. These include notification requirements vis-à-vis affected persons after the measures have been carried out, judicial review powers, regular administrative oversight as well as reporting obligations vis-à-vis Parliament and the public. Finally, the investigatory powers must be supplemented by statutory requirements regarding the deletion of collected data.

3. In various respects, the challenged provisions do not meet these constitutional requirements.

a) The provisions on the use of special means of surveillance outside of private homes, such as observation, recording of speech and images, the installation of tracking devices or the use of police informants, are not sufficiently limited in scope (§ 20g(1) to (3) BKAG).

aa) The legislator authorises such measures not only for the purpose of averting specific dangers (*konkrete Gefahren*), but also for preventing crime (§ 20g (1) no. 2 BKAG). While such a legislative approach is in principle permissible, it is subject to limits to which the provision does not adhere. The provision neither requires that it must at least be possible to determine the type of incident that might occur, and that it will occur within a foreseeable timeframe, nor, alternatively, that the individual conduct of a person establishes the specific probability that they will commit terrorist acts in the not so distant future. Thus, § 20g BKAG does not set sufficiently specific criteria for the authorities and the courts to work with and could give rise to disproportionately broad measures.

bb) Some of the measures authorised in § 20g BKAG may typically result in the monitoring of confidential situations that are beyond the reach of the state. Thus, in order to safeguard the core of private life both with respect to data collection and to data analysis, the legislator must provide for safeguards. These, however, are lacking here.

cc) Furthermore, to the extent that it relates to long-term monitoring or non-public conversations, the requirement of prior judicial authorisation (*Richtervorbehalt*) in § 20g(3) BKAG is inadequate, given that some of the measures are not contingent upon obtaining a judicial warrant at all, while others do not require a judicial warrant for the first month.

b) The provision on the surveillance of private homes (§ 20h BKAG), which allows data collection in the form of visual and acoustic surveillance, only partially satisfies the proportionality requirements.

aa) The authorisation to carry out surveillance of private homes directed at a target person's contacts or associates (§ 20h(1) no. 1(c) BKAG) is incompatible with Art. 13(1) and (4) of the Basic Law (*Grundgesetz* – GG). The surveillance of private homes constitutes a particularly serious interference with the private sphere. Therefore, such a surveillance measure is only appropriate if it only targets conversations of the person responsible for the danger in question. Unlike for other measures, directly targeting third parties with this type of surveillance is impermissible. At the same time, constitutional law does not give rise to an absolute prohibition of measures that could indirectly affect third parties.

bb) The rules on the protection of the core of private life in § 20h(5) BKAG are inadequate under constitutional law. Since the surveillance of private homes can constitute a deep intrusion into the private sphere, the requirements for protecting the core of private life are particularly strict. After such a measure has been carried out – unless there is danger requiring immediate action (*Gefahr im Verzug*) – all data must first be screened by an independent body to check whether it contains highly private information before it can be used by the Federal Criminal Police Office. The provision, however, does not ensure that this is the case.

c) Sufficient protection of the core of private life is lacking with regard to remote searches of information technology systems (§ 20k BKAG). The body tasked with screening the collected data is not sufficiently independent. It is necessary that such screening be carried out by external bodies not charged with security tasks. While involving staff from the Federal Criminal Police Office to obtain investigation-specific or technical expertise is not ruled out, the actual execution and decision-making responsibility must lie in the hands of persons independent from the Federal Criminal Police Office. By assigning the task of data screening mainly to staff from the Federal Criminal Police Office, § 20k(7) third and fourth sentence BKAG falls short of these requirements.

d) The provision on the surveillance of ongoing telecommunications (§ 20l BKAG) is only partially compatible with the Constitution. In particular, the provision extending the scope of telecommunications surveillance to the prevention of crime is too vague and disproportionately broad. This shortcoming is also found in the provision on the collection of telecommunications traffic data (§ 20m(1) and (3) BKAG).

e) All of the challenged investigatory and surveillance powers lack further provisions to ensure respect for the principle of proportionality.

aa) The protection of persons bound by professional confidentiality is inadequate insofar as a distinction is made between defence lawyers and other lawyers. Since the surveillance measures in question do not serve law enforcement purposes but public security purposes, such a distinction is unsuitable for protecting lawyers.

bb) The provisions aiming to guarantee transparency, legal protection and administrative oversight do not satisfy the constitutional requirements in all respects either. They lack adequate rules on regular mandatory audits, comprehensive documentation requirements which allow the full and effective review of the surveillance measures in question, and reporting obligations vis-à-vis Parliament and the public.

cc) The obligations to delete the collected data also only satisfy the constitutional requirements in part. It is unconstitutional that there is a general possibility of avoiding the deletion of collected data, once the data has served its purpose, on the grounds that the data is needed for law enforcement or for the prevention of crime or as a precaution for the future prosecution of considerable criminal acts (§ 20v(6) fifth sentence BKAG). This possibility permits the storage of data for new purposes that are only defined in general terms; the Act does not and, in view of its broadness, in fact cannot provide any legal basis for such use. The very brief period for keeping the deletion logs created by the Federal Criminal Police Office is also inadequate, as it does not sufficiently ensure the possibility of subsequent review.

4. On the basis of existing case-law, the Court's decision in the present proceedings develops new distinctions for requirements regarding data use that goes beyond the specific investigation [that prompted the data collection]. Such further data use is governed by the principles of purpose limitation and change in purpose. A distinction must be made between further use of data for the purpose for which it was originally collected, which is generally permissible, and a change in purpose, which is only permissible within certain limits.

a) The legislator may allow the use of data beyond the specific investigation that prompted the data collection where this further use serves the same purpose as the original data collection (further use), provided that the authority that is authorised to collect data uses this data while acting within the same remit for the protection of the same legal interests and the prosecution or prevention of the same criminal acts as specified in the statutory provision authorising the data collection. Allowing the authority in question to consider the data as mere evidentiary traces used for further investigations does not run counter to the principle of purpose limitation. However, the same does not apply for data stemming from the surveillance of private homes or from remote searches of information technology systems. Due to the severity of the interferences resulting from these measures, any further use of such data must additionally satisfy the prerequisites for establishing sufficient indications of danger that were applicable to the original data collection .

b) Moreover, the legislator may also allow further data use for purposes other than those for which the data was originally collected (change in purpose). The proportionality requirements applicable to such a change in purpose derive from the principle of a hypothetical recollection of data (*hypothetische Datenneuerhebung*). According to this principle, the new use of the data must serve to protect legal interests or to detect criminal acts of such weight that would, by constitutional standards, justify a new collection of the data with comparably weighty means. However, there is generally no need to establish, for a second time, the existence of an identifiable danger (*konkretisierte Gefahrenlage*), as required for the original data collection; it is necessary but generally also sufficient to require that there be a specific basis for further investigations. By contrast, with regard to surveillance of private homes and remote searches of information technology systems, which result in particularly serious interferences, a change in purpose is subject to the same requirements regarding the danger categories as the data collection itself. By specifying these standards, the Court's decision consolidates a long line of case-law and carefully delimits it.

5. The provisions on data use and sharing with domestic authorities only partially satisfy these principles.

a) It is not objectionable that the Federal Criminal Police Office may use the data obtained, in principle without requiring the existence of a specific danger, to carry out its tasks of averting dangers posed by international terrorism (§ 20v(4) second sentence no. 1 BKAG). However, this power is disproportionate with regard to data obtained through the surveillance of private homes and remote searches. In view of the particular severity of interference resulting from such measures, further use of the data thus obtained may only be permitted in cases where there is an impending danger (*drohende Gefahr*) or a sufficiently identifiable danger in the specific case.

The unlimited power of the Federal Criminal Police Office to use the data for the protection of witnesses or other persons (§ 20v(4) second sentence no. 2 BKAG) is too vague and does not satisfy the constitutional requirements.

b) The powers to share data with other domestic authorities (§ 20v(5) BKAG) are unconstitutional.

Data sharing for public security purposes is unconstitutional insofar as data may be shared for the purpose of general prevention of terrorist acts, without requiring a specific basis for further investigations. The provision governing data sharing for law enforcement purposes is not compatible with the Constitution. The referenced provisions of the Code of Criminal Procedure (§ 161(1) and (2) of the Code of Criminal Procedure, *Strafprozessordnung* – StPO) neither sufficiently ensure the constitutionally required restrictions of data sharing, nor do they ensure that the sharing of data obtained through the surveillance of private homes or remote searches is limited to the purpose of prosecuting sufficiently serious criminal acts; the provision also does not rule out the sharing of data obtained through the visual surveillance of private homes with law enforcement authorities, although Art. 13(3) and (4) GG only authorise such visual surveillance for public security purposes, but not for law enforcement purposes. The powers for sharing data with offices for the protection of the Constitution (domestic intelligence services), the Military Counter-Intelligence Service and the Federal Intelligence Service are disproportionately broad (§ 20v(5) third sentence no. 1, fourth sentence BKAG).

Furthermore, with regard to all data sharing powers, the relevant prerequisites for effective oversight by the Federal Data Protection Officer are not sufficiently guaranteed.

6. The decision contains general statements on the requirements for the sharing of data with foreign security authorities. It is the first time that the Federal Constitutional Court has been called upon to decide on this matter. The Court's' decision, however, does not pertain to the sharing of data with Member States of the European Union (§ 14a BKAG).

After data has been shared with other states, the guarantees of the Basic Law can no longer be applied directly and the standards prevailing in the respective receiving state apply instead. Yet this does not generally prevent data sharing with other states. The Basic Law commits Germany to international cooperation. This includes respect for foreign legal orders and values. When deciding whether to share personal data with other states, German state authority remains bound by the fundamental rights. Data sharing is thus subject to the general constitutional principles of change in purpose and purpose limitation. When assessing new uses of data, however, the autonomy of the foreign state's legal order must be respected. Foreign state authorities are only bound by their own legal obligations.

Firstly, data protection guarantees impose limits on data sharing. The limits set by the Basic Law for the domestic collection and processing of data must not be undermined, in terms of their substance, by data sharing between security authorities. The legislator must thus ensure that this fundamental rights protection is not eroded neither by the sharing of data collected by German authorities with other states and international organisations nor by the receipt and use of data from foreign authorities that was obtained in violation of human rights. This is not to say that the other state's legal order must guarantee institutional and procedural safeguards corresponding to Germany's system. Yet it must be ensured that there is an appropriate level of substantive data protection for the handling of the shared data in the receiving state.

Secondly, limits to data sharing arise with regard to the use of the data by the receiving state if there are concerns about human rights violations. The sharing of data with other states is ruled out if there is reason to fear that its use could lead to violations of fundamental principles of the rule of law. Under no circumstances may the state be complicit in violations of human dignity.

The sharing of data with other states must be restricted to sufficiently weighty purposes for which the data may be shared and used; moreover, it must be ascertained that the data will be handled in accordance with human rights and data protection standards in the receiving state. In addition, effective oversight must be ensured.

7. In part, the challenged powers to share data with public authorities in other countries do not satisfy these constitutional requirements.

a) The purposes for which data may be shared are too broad (§ 14(1) BKAG). The general authorisation to share data for the performance of the tasks incumbent upon the Federal Criminal Police Office (§ 14(1) first sentence no. 1 BKAG) is not sufficiently limited and thus disproportionate. The provision fails to ensure that data from particularly intrusive surveillance measures may only be shared for the purpose of protecting legal interests or investigating criminal acts of such weight that would, by constitutional standards, justify a new collection of the data with comparably weighty means. The power to share data to avert a significant danger to public security in the individual case (§ 14(1) first sentence no. 3 BKAG) is generally not objectionable. However, it is insufficiently limited with regard to data stemming from the surveillance of private homes. Also, insofar as data sharing is allowed because there are indications that considerable criminal acts will be committed (§ 14(1) second sentence BKAG), data sharing is not sufficiently restricted in accordance with the criterion of a hypothetical recollection of data.

b) By contrast, the challenged provisions satisfy the requirements for ascertaining that the data will be handled in accordance with data protection standards and human rights guarantees in the receiving state. When interpreted in conformity with the Constitution, § 14(7) BKAG sufficiently ensures adherence to such standards.

c) With regard to domestic data sharing, constitutional law requires regular administrative oversight as well as reporting obligations. Such safeguards are lacking here.

8. For the most part, the Court refrained from declaring the challenged provisions void, opting to declare them merely incompatible with the Constitution instead. Given that the constitutional shortcomings do not concern the granting of the powers as such, but essentially pertain solely to the specific design of these powers, the provisions continue to apply – subject to the conditions determined by the Court – until 30 June 2018.

Dissenting opinion of Justice Eichberger:

I cannot concur with this judgment, as I disagree in several respects with the conclusions regarding the challenged provisions, and with parts of the reasoning.

It is true that the judgment draws on lines of case-law developed by the Court over the past twelve years regarding the permissibility of interferences with fundamental freedoms in view of the state's duty to ensure security. However, the standards set out by the Senate majority in this judgment, like in the past, almost exclusively rely on an assessment of proportionality, that is a balancing of the burdens imposed on persons affected by very intrusive measures interfering with fundamental rights, on the one hand, and the state's duties of protection with regard to averting terrorist dangers, on the other. Yet in this case, too, the legislator has a prerogative of assessment when appraising the factual basis of dangers and making a prognosis on how such dangers may develop. In light of this, the Senate should not have set such detailed requirements. In weighing the latent risk posed by covert surveillance and investigation measures, it must be kept in mind that, for the most part, the challenged provisions do not authorise a general collection of data indiscriminately affecting a large number of persons. If, in a specific case, investigation measures affect persons that have not themselves provided grounds for the investigation or have only marginally contributed to such grounds, they may nevertheless be asked to endure the measure as a special sacrifice, as part of their duty as citizens, that serves to maintain public security.

Not all of the requirements imposed on the legislator with regard to provisions governing procedure, transparency and oversight are actually prescribed, in this exact form, by the Constitution – even if many of these requirements may be sensible and fitting. Though commendable in its attempt to consolidate existing case-law, the present judgment generalises previous findings in a manner that ultimately results in a problematic affirmation of excessive constitutional requirements in the domain at issue here.

I think the judgment goes too far in deriving from the principle of proportionality the requirements that persons affected by very intrusive surveillance measures be afforded effective sanctioning mechanisms; that the oversight of data collection and use be carried out in regular intervals not exceeding approximately two years; and that reporting obligations vis-à-vis Parliament and the public to ensure transparency and oversight be provided for. It would have been sufficient to simply specify the level of protection that must be ensured by the legislator.

Insofar as the Senate majority considers the authorisation to carry out certain investigation and data collection measures for the purposes of crime prevention to lack specificity and to be disproportionate, it needlessly foregoes the possibility of interpreting the relevant provisions in conformity with the Constitution. The Senate majority objects to the legislator's approach of not subjecting most of the initial surveillance measures in § 20g(2) BKAG toprior judicial authorisation, as the law only requires such judicial authorisation for an extension of the measures at issue, yetI consider this approach to be tenable under constitutional law. Furthermore, I cannot concur with the Senate majority's view that § 20g BKAG is unconstitutional for not sufficiently ensuring protection of the core of private life.

With regard to the use of data obtained through surveillance measures, the judgment refines and consolidates the idea of a "hypothetical recollection" of data as the notional base for determining the conditions for a change in purpose. I cannot support the exception called for by this concept, whereby any further use and change in purpose of data stemming from the surveillance of private homes or remote searches must be justified by an acute or an identifiable danger in the specific case, just as for the original data collection. In the context of the surveillance of private homes, too, the real and severe intrusion into the private sphere takes place when the authorities carry out the actual surveillance measure in the protected domain. While any further use, including for changed purposes, does indeed perpetuate this interference, it does not reach the level of severity of the initial interference, not even where the data was obtained through the surveillance of private homes (or remote searches of information technology systems for that matter). The further use, including a change in purpose, of information obtained through surveillance measures should only be measured against the general rules applicable in this regard. The Senate majority has missed the opportunity to correct its case-law accordingly.

Dissenting opinion of Justice Schluckebier:

To the extent that the judgment objects to the challenged provisions on constitutional law grounds, I agree neither with large parts of its outcome nor with its reasoning. The Senate majority conducts a proportionality assessment that I believe to be misguided, from a constitutional perspective, in several respects, and sets out excessive specificity requirements in relation to individual provisions. Ultimately, by laying down numerous requirements relating to

technical legislative details, the Senate majority puts its own notion of how the statutory framework should be designed before that of the democratically elected legislator. In my opinion, this goes too far. Contrary to what the Senate majority assumed, some of the challenged provisions could in fact have been interpreted in conformity with the Constitution.

Before going into detail, it should be noted that the legislator, in designing the statutory framework, has essentially found an appropriate and tenable balance in the complex conflict between the fundamental rights of persons affected by the police measures, and the underlying statutory bases, on the one hand, and the legislator's duty to protect the fundamental rights of individuals and the constitutionally protected interests of the public on the other hand. The legislator thus gives effect to the principle that, in a state under the rule of law, individuals must be able to rely on both effective protection *by* the state and the protection of their freedoms *against* the state.

The Senate majority held that the surveillance framework lacks an explicit statutory provision ensuring protection of the core of private life, particularly with regard to the special methods of data collection outside private homes (§ 20g(2) BKAG); in my opinion, such an express provision is not necessary. In principle, when they are not inside private homes, affected persons are "in public", rather than in specifically protected private areas. Protection of the core of private life can be ensured when the law is applied in practice.

Furthermore, I cannot support the reasoning by which the Senate majority requires the establishment of an "independent body" with external staff – staff not working on security tasks – that is responsible for actually carrying out and making decisions on the collection and use of data stemming from the surveillance of private homes and remote searches. The rather complicated solution prescribed by the Court hampers the effectiveness of the envisaged measures since the evaluation of findings is often very urgent and needed as quickly as possible in the context of the prevention of crime and of public security. This means that these powers no longer constitute appropriate means for effective protection against terrorism. The possibility afforded the legislator to provide the Federal Criminal Police Office with "the means to take action at short notice" in exceptional cases of danger requiring imminent action– which, in practice, will occur rather frequently – is in clear contrast to the Senate majority's assumption that the Federal Criminal Police Office must in general be almost completely excluded from initial screening given that the data merits special protection.

To the extent that the Senate majority considers that the powers to further use the data collected for counter-terrorism purposes and to share such data with domestic and foreign authorities are unconstitutional in several respects, I cannot fully agree with this conclusion either. This applies in particular to the extent that the Senate majority permits the use of lawfully collected data in other contexts solely for the purposes of protecting the same or equally weighty legal interests. The judgment makes the sharing and further use of the data for other purposes contingent on whether, after the change in purpose, this data continues to serve the protection of legal interests or the detection of criminal acts of such weight that this could, by constitutional standards, justify collecting the data again with comparably weighty means (criterion of a hypothetical recollection of data). This view may be tenable with regard to information obtained through particularly intrusive and very serious interferences, such as through surveillance of private homes or remote searches. However, with regard to other types of interferences, which result in so-called coincidental findings, this approach, in my opinion, would lead to hardly tolerable results since it requires the legal order, which is committed to the rule of law, to stand back and allow crimes to happen and legal interests to be violated. Provided that such coincidental findings were obtained through a lawful and thus also constitutional interference, it is unacceptable in my view that a state under the rule of law is forced to deliberately "look away" in these cases. This leaves the potentially affected individuals or the legal interests of the public unprotected while giving priority to the protection of the data of those targeted by the measures at issue; this is especially unfortunate given that this case does not concern a change in purpose of very broad mass data that was collected indiscriminately.

As for the additional statutory provisions demanded by the Senate majority with regard to the sharing of data with authorities in other states, I do not share the view that these are constitutionally required. The relevant provision (§ 14 BKAG) could have been interpreted in conformity with the Constitution. The provision explicitly states that the sharing of personal data is prohibited if there are reasons to believe that the data could be used in a manner which would run counter to the statutory purpose set forth in German law or if, in the individual case, the interests meriting protection of the persons concerned prevail. This also requires the existence of an appropriate data protection standard in the receiving state. The Act also contains prohibitions to share data and grounds for denial (§ 27 BKAG). With these, it can easily be ensured that the sharing of data does not in any way promote human rights violations in other states and that a prior ascertainment of the use of the shared data in the receiving state takes place. Once again, the insertion of additional detailed provisions into the existing legislative framework, as is now required of the legislator, will inflate the legislative text further, rendering the already excessively long statute even less legible and comprehensible – which ultimately leads to the opposite of legal clarity. At the same time, it will not even benefit affected persons, given that it will hardly lead to any measurable strengthening of protection in practice.