Provisions of the North Rhine-Westphalia Constitution Protection Act regarding remote searches and Internet surveillance measures are declared void

Press Release No. 22/2008 of 27 February 2008

Order of 27 February 2008
1 BvR 370/07, 1 BvR 595/07

The constitutional complaints of a journalist, of a member of the North Rhine-Westphalia regional branch of the party *DIE LINKE* and of three lawyers challenging provisions of the North Rhine-Westphalia Constitution Protection Act (cf. Press Release No. 82/2007 of 27 July 2007) are, insofar as they are admissible, for the most part well-founded. In its judgment of 27 February 2008, the First Senate of the Federal Constitutional Court declared the provisions on remote searches of information technology systems and Internet surveillance measures to be unconstitutional and void.

§ 5(2) no. 11 first sentence, second alternative of the North Rhine-Westphalia Constitution Protection Act (*Verfassungsschutzgesetz Nordrhein-Westfalen* — VSG), which governs covert access to information technology systems ('remote searches'), violates the general right of personality in its special manifestation as a fundamental right to protection of the confidentiality and integrity of information technology systems and is void. In particular, the provision fails to satisfy the proportionality requirements. In view of the severity of interference, the covert infiltration of an information technology system for the purposes of monitoring the use of the system and extracting data stored on its storage media is only permissible under constitutional law if there are factual indications of a specific danger (*konkrete Gefahr*) to an exceptionally significant legal interest. Moreover, such interference must in principle be subject to judicial authorisation. § 5(2) no. 11 first sentence, second alternative VSG does not satisfy these requirements. There are also no adequate statutory safeguards to prevent interferences with the core of private life, which enjoys absolute protection.

The legislative authorisation to carry out covert Internet surveillance pursuant to § 5(2) no. 11 first sentence, first alternative VSG violates constitutional law and is void. Covert Internet surveillance interferes with the privacy of telecommunications if the Office for the Protection of the Constitution (*Verfassungsschutzbehörde*) monitors secure communication contents by using access keys obtained without the consent or against the will of the communicating parties. An interference with fundamental rights of such severity in principle requires a statutory basis that at least sets a qualified and substantive threshold for interference. Such a threshold is lacking in this case. The provision authorises, on a large scale, purely precautionary intelligence service action before specific dangers actually materialise, but fails to take into account the weight of the legal interests, including of third parties, that are potentially violated as a result. Moreover, the provision does not contain any safeguards protecting the core of private life. By contrast, where the state obtains knowledge of communication contents that are publicly accessible on the Internet, or participates in publicly accessible communication processes, it generally does not interfere with fundamental rights.

In essence, the decision is based on the following considerations:

§ 5(2) no. 11 first sentence, second alternative VSG ("remote searches")

I. § 5(2) no. 11 first sentence, second alternative VSG authorises interferences with the general right of personality in its special manifestation as a fundamental right to protection of the confidentiality and integrity of information technology systems.

1. The use of information technology systems is central to the personality development of many individuals, but also creates new risks to one's personality. Monitoring the use of such a system and analysing the data on the system's storage media allows for far-reaching conclusions regarding the personality of the users concerned, and may even make it possible to compile personality profiles. This gives rise to a considerable need for protection from a fundamental rights perspective. The guarantees of Art. 10 of the Basic Law (*Grundgesetz* – GG) – telecommunications privacy – and of Art.

13 GG – inviolability of the home –, like the manifestations of the general right of personality previously developed by the Federal Constitutional Court in its case-law, do not adequately take account of the need for protection arising from advances in information technology.

a) The scope of protection of telecommunications privacy also extends to Internet communication services (e.g. emails). Where a legislative authorisation only permits state measures intercepting the contents and circumstances of ongoing telecommunications in a computer network, or measures analysing this data, the interference must be measured only against Art. 10(1) GG. In this case, the scope of protection of this fundamental right is affected regardless of whether, at the technical level, the measure targets the transmission route or the device used for telecommunications. Therefore, Art. 10(1) GG serves as the sole standard of review in terms of fundamental rights protection where the authorisation to carry out 'source telecommunications surveillance' is strictly limited to data stemming from ongoing telecommunications. This must be ensured by technical and legal safeguards.

Yet the fundamental rights protection afforded by Article 10(1) GG does not extend to the contents and circumstances of telecommunications data stored within the domain controlled by a communicating party after the transmission has been completed, to the extent that they can take their own precautions against covert data access. Likewise, the protection afforded by the privacy of telecommunications does not apply if a state authority monitors the use of an information technology system as such or searches the system's storage media. In this respect, a gap in protection arises, which must be filled by the general right of personality in its manifestation as protection of the confidentiality and integrity of information technology systems. Where the technical infiltration of a complex information technology system is undertaken for the purposes of telecommunications surveillance, this infiltration is the critical step that makes it possible to spy on the system as a whole. The resulting risks for one's personality go far beyond the risks associated with the mere surveillance of ongoing telecommunications. In particular, the state can also obtain knowledge of data stored on a computer that have no link to the use of the system for telecommunications purposes.

b) The guarantee of the inviolability of the home, too, gives rise to gaps in protection with regard to access to information technology systems. Art. 13(1) GG does not generally protect individuals against infiltration of their information technology system regardless of how the access is gained, not even if the system is located within a private home. The interference at issue can occur regardless of one's location; therefore, a location-specific protection would not counter the specific risks to the information technology system. To the extent that infiltration measures make use of a network connection between the targeted computer and another computer, they do not affect the sphere of private space within one's home.

c) The manifestations of the general right of personality that have so far been recognised in the Federal Constitutional Court's case-law, in particular the guarantees protecting the private sphere and the right to informational self-determination, also do not sufficiently meet the special need for protection of users of information technology systems. The need for protection on the part of users of information technology systems is not limited solely to data attributable to their private sphere. Nor does the right to informational self-determination fully reflect the risks to one's personality resulting from the infiltration of information technology systems. Third parties accessing the system can potentially obtain extremely large quantities of data with significant informative value without having to resort to further data collection and processing measures. The weight of such data access for the personality of affected persons goes far beyond that of isolated data collection measures against which the right to informational self-determination affords protection.

2. The general right of personality applies by virtue of its function to fill gaps in protection; it meets the aforementioned need for protection, which goes beyond the other manifestations of this right recognised so far, by guaranteeing the integrity and confidentiality of information technology systems. The fundamental right to protection of the integrity and confidentiality of information technology systems is applicable where the statutory basis authorising interferences covers systems that may contain, by themselves or due to network connections, personal data of users in such large quantities and of such variety that access to the system facilitates insights into essential aspects of one's personal life or even allows for the creation of a comprehensive personality profile.

II. Interferences with this right may be justified both for preventing dangers to public security and for law enforcement purposes. However, they must have a statutory basis that is in line with constitutional law. § 5(2) no. 11 first sentence, second alternative VSG does not satisfy this requirement.

1. In particular, the provision fails to satisfy the principle of proportionality.

a) § 5(2) no. 11 second sentence VSG authorises particularly intrusive interferences with fundamental rights. Where a state authority collects data from complex information technology systems, this authority gains access to data records which, in terms of their volume and variety, may by far exceed traditional sources of information. In view of the severity of interference, the covert infiltration of an information technology system for the purposes of monitoring the use of the system and extracting data stored on its storage media is only permissible under constitutional law if there are factual indications of a specific danger to an exceptionally significant legal interest. Exceptionally significant legal interests are the life, limb or liberty of the person or public interests that are of such significance that a threat to them would affect the

foundations or existence of the state, or the foundations of human existence. However, the measure may be justified even if it cannot yet be established with sufficient probability that the danger will materialise in the near future, provided that there are specific facts indicating an impending danger (*drohende Gefahr)* to an exceptionally significant legal interest in the individual case.

Furthermore, statutory provisions authorising covert access to information technology systems must provide for suitable procedural safeguards protecting the interests of affected persons. In particular, such access must generally be subject to judicial authorisation.

b) § 5(2) no. 11 first sentence, second alternative VSG does not satisfy these requirements. According to the provision, the use of intelligence service methods by the Office for the Protection of the Constitution is only subject to the condition that there be factual indications suggesting that these methods allow the gathering of information on anti-constitutional activities. This does not subject the exercise of these powers to a sufficient substantive threshold, neither regarding the factual prerequisites for carrying out the interference, nor regarding the weight of the legal interests the measure aims to protect. Also, the provision fails to ensure prior review by an independent authority. These shortcomings are not remedied through the statutory reference to the requirements for surveillance measures under the Article 10 Act – which only applies to certain cases. In relation to measures taken pursuant to § 5(2) no. 11 first sentence, second alternative VSG, the grounds for interference set out in the Article 10 Act do not satisfy the constitutional requirements, neither with regard to the threshold for exercising the relevant powers nor with regard to procedural safeguards.

2. Moreover, there are no adequate statutory safeguards to prevent interferences with the core of private life, which enjoys absolute protection. Compared to other surveillance measures, an investigative measure that accesses an information technology system, which can be used to collect comprehensive data from the target system, gives rise to an increased risk of highly personal data being collected. The constitutionally required protection of the core of private life can be guaranteed by a two-tier concept of protection. The statutory provision must be designed to ensure that the collection of data relating to the core is avoided from the outset as far as this is possible in terms of information technology and investigative technique. In particular, available information technology safeguards must be used. If it is virtually unavoidable that information will be obtained before its link to the core can be determined – as is the case with covert access to information technology systems –, sufficient protection must later be ensured at the analysis stage. In particular, where data relating to the core is found and collected, it must be deleted without undue delay and any further use must be ruled out. § 5(2) no. 11 first sentence, second alternative VSG does not satisfy these requirements either.

3. Moreover, the provision violates the requirements of legal clarity and specificity.

§ 5(2) no. 11 first sentence, first alternative VSG ("covert surveillance of the Internet")

I. In certain cases, measures authorised pursuant to § 5(2) no. 11 first sentence, first alternative VSG may constitute interferences with the privacy of telecommunications (Art. 10(1) GG) that are not justified under constitutional law.

Where the state obtains knowledge of the contents of Internet communication by using the normal technical means provided for this purpose, an interference with Article 10(1) GG arises only if the relevant state authority was not given permission by one of the communicating parties. This is the case if the Office for the Protection of the Constitution monitors secure communication contents by using access keys obtained without the consent or against the will of the communicating parties. By contrast, it does not amount to an interference with Art. 10(1) GG if investigation measures by the state do not involve unauthorised access to telecommunications, but merely fail to fulfil users' expectations regarding the identity and authenticity of their communication partners. Therefore, there is no interference with the privacy of telecommunications if, for instance, a participant in a private chatroom has voluntarily provided a person acting on behalf of the Office for the Protection of the Constitution with their access information, which the authority then uses. An interference with telecommunications privacy can certainly be ruled out where the authority collects generally accessible contents, for instance by viewing open discussion forums or websites that are not password protected.

The interferences with Art. 10(1) GG arising under § 5(2) no. 11 first sentence, first alternative VSG are not justified under constitutional law. They are not compatible with proportionality requirements. The provision authorises, on a large scale, purely precautionary intelligence service action before specific dangers actually materialise, but fails to take into account the weight of the legal interests, including of third parties, that are potentially violated as a result. Moreover, the provision does not contain any safeguards protecting the core of private life.

II. Nevertheless, the Office for the Protection of the Constitution may continue to use Internet surveillance measures to the extent that these do not amount to interferences with fundamental rights. As a rule, Internet surveillance as such will generally not amount to an interference with fundamental rights. The confidentiality and integrity of information technology systems guaranteed by the general right of personality is not affected by Internet surveillance measures where these measures are limited to collecting data intended by the relevant system's owner for Internet communication purposes using the normal technical means provided in this regard. This also applies if a state authority assumes a cover identity to build up communication relationships with affected persons. Where the identity and authenticity of one's communication partners cannot be verified, the communication relationships facilitated by Internet communication

services do not merit legitimate expectations in this regard. Nor does it amount to an interference with the right to informational self-determination if a state authority collects communication contents that are available on the Internet and addressed to the general public or to a group of persons that is not further defined.

§ 5a(1) VSG (monitoring of bank accounts)

The collection of data on bank accounts and transactions provided for in § 5a(1) VSG is compatible with the Basic Law. In particular, it does not violate the right to informational self-determination. The provision makes such data collection contingent on threats that are qualified both with regard to the affected legal interests and with regard to the factual grounds for interference; it thus satisfies proportionality requirements. Moreover, the provision sets out adequate procedural safeguards taking into account the weight of interference.