AUT-2019-3-003

a) Austria / **b)** Constitutional Court / **c)** / **d)** 11-12-2019 / **e)** G 72-74/2019-48, G 181-182/2019-18 / **f)** / **g)** ECLI:AT:VFGH:2019:G72.2019 / **h)** CODICES (German).

Keywords of the systematic thesaurus:

05.03.32	Fundamental Rights - Civil and political rights - **Right to private life.**
05.03.32.01	Fundamental Rights - Civil and political rights - Right to private life - **Protection of personal data.**
05.03.35	Fundamental Rights - Civil and political rights - **Inviolability of the home.**

Keywords of the alphabetical index:

Data, personal, collecting, processing / Privacy, rights and interests, balance / Surveillance, secret.

Headnotes:

Automatic number plate recognition as well as covert surveillance of encrypted messages may be a suitable means for fighting crime and terrorism. However, such measures are disproportionate and therefore violate the right to respect for private life if they apply to cases of (serious) property crimes. In so far as the automatic transmission of personal data gathered by automatic speed monitoring systems to security authorities was concerned, such a measure was also disproportionate and unconstitutional if it applied regardless of whether the behaviour of the persons concerned had given rise to its use.

Summary:

1. Section 54 of the Security Police Act *(Sicherheitspolizeigesetz)* allows security authorities to covertly collect and store (image) data in order to identify vehicles and vehicle drivers. Section 98a of the Road Traffic Act *(Straßenverkehrsordnung)* regulates the transmission and storage of data from automatic section-related speed monitoring ("Section Control"). Section 135a of the Code of Criminal Procedure *(Strafprozessordnung)* provides authorisation to monitor encrypted messages by installing a so-called "Federal Trojan" in a computer system. Under certain circumstances, this may include the power to intrude into and search apartments for the purpose of installing such a trojan without the knowledge of the person concerned.

2. Members of the National Council and the Federal Council filed constitutional complaints against these provisions claiming that they were disproportionate and violated several fundamental rights, above all the right to data protection (Section 1 of the Data Protection Act) and the right to respect for private life (Article 8 ECHR).

3. The Constitutional Court found these provisions to be unconstitutional:

3.1. Section 54 of the Security Police Act regulates the automatic and covert collection and storage of data, including of images. For the purposes of preventing and prosecuting criminal offences, security authorities are authorised to process, e.g. record, store, use, transmit, data relating to vehicle identification, such as number plate, type, colour, and to drivers. The authorisation to gather data constitutes, given its scope regarding type and extent of the data, operational area and conditions for their determination, a serious interference with confidentiality interests further to Section 1 of the Data Protection Act and the right to respect for private life under Article 8 ECHR of those persons affected. This interference was disproportionate given the intended purpose of the provision. In particular, it was disproportionate because the investigative measure may (also) be used for the pursuit and defence of acts that only constitute minor property delinquency.

3.2. Section 98a of the Road Traffic Act deals with the transmission and storage of personal, including image, data gathered by section-related speed monitoring systems to or by security authorities, respectively. Such monitoring systems use an image-processing technical device which measures the average driving speed of a vehicle on a specified route. This is permitted if it is necessary to secure traffic safety, to protect the population, or the environment, among other things. In respect of the new competence to process data from speed control systems, the Constitutional Court held that the provision constituted a serious interference with confidentiality interests further to Section 1 of the Data Protection Act and with the right to respect for private life (Article 8 ECHR). Transmission of data to the security authorities affects people regardless of whether their behaviour gave rise to such transmission or not. Section 98.a of the Road Traffic Act was thus disproportionate because it did not guarantee that the stored data would only be processed if it facilitated the prosecution and investigation of serious crimes. This unconstitutionality also affected Section 57 of the Security Police Act, which allowed certain personal data to be compared with other such data, and which was intrinsically linked with Section 98.a of the Road Traffic Act.

3.3. Section 135.a.1 and 135.a.2, in conjunction with Section 134.3.a of the Code of Criminal Procedure permits the surveillance of encrypted messages in specified cases and under certain conditions.

The Constitutional Court held that monitoring of use of computer systems covertly constituted a serious interference with the privacy protected by Article 8 ECHR and is only permitted within extremely narrow limits in order to protect equally important legal interests. The "Federal Trojan" is a particularly intense form of surveillance measure, particularly because an overview of the data obtained by monitoring a computer system enables conclusions to be drawn about individual users' personal preferences, tendencies, and lifestyle, among other things. Moreover, the trojan affects a large number of people, including individuals who are uninvolved with the person who is subject to the surveillance. According to the Court, Section 135.a of the Code of Criminal Procedure violated Article 8 ECHR because there was no guarantee that the surveillance measure would only take place if it was used to prosecute and solve sufficiently serious offences. Additionally, it was unconstitutional because the measure did not adequately secure the protection of the privacy of those affected by the trojan. The Constitutional Court pointed out there was no guarantee that after the *ex ante* judicial approval of the measure, the competent legal

protection officer would actually be able to effectively and independently control any on-going monitoring.

3.4 Section 135.a.3 of the Code of Criminal Procedure permits entry into an apartment or other rooms protected by domestic law, in order to search containers and to overcome specific security measures in order to install the "Federal Trojan" provided that this is unavoidable to facilitate surveillance. The Constitutional Court held that the provision violated the right to inviolability of housing i.e., private property, in so far as it included the power to search the house. According to the Court, this provision authorised the execution of house searches without the person concerned becoming aware of them. This was inconsistent with the Law on Protection of the Rights of the Home of 1862 *(Hausrechtsgesetz)*, according to which home searches that are carried out without the knowledge of the persons concerned must be reported to them within 24 hours of the search taking place.

4. The Constitutional Court concluded that:

- first, the legal provisions regarding number plate recognition constituted a disproportional interference with the right to data protection and the right to respect for private;

- secondly, the covert collection and storage of data for the identification of vehicles and drivers was disproportionate. It constituted an interference with confidentiality interests. It also violated the right to data protection and private life;

- thirdly, covert surveillance of encrypted messages by installing a "Federal Trojan" constituted a violation of Article 8 ECHR. The data obtained enabled conclusions to be drawn about the personal preferences and lifestyle of the user; the measures affects a large number of people, including those who were not involved, and the protection of the privacy of those affected was not adequately ensured; and,

- finally, authorisation to enter on premises for the purpose of installing this monitoring program without the knowledge of the person concerned violated the right to inviolability of the home i.e., of private property.

Cross-references:

Constitutional Court:

- G 47/2012, 27.06.2014, *Bulletin* 2014/2 [AUT-2014-2-003].

Federal Constitutional Court of Germany:

- 1 BvR 2074/05, 11.03.2008, *Bulletin* 2018/1 [GER-2018-1-007];

- 1 BvR 966/09, 20.04.2016, *Bulletin* 2016/1 [GER-2016-1-007];

- 2 BvR 1454/13, 06.07.2016;

- 1 BvR 370/07, 27.02.2008, *Bulletin* 2018/1 [GER-2018-1-006];

- 1 BvR 142/15, 18.12.2018, *Bulletin* 2019/1 [GER-2019-1-002].

European Court of Human Rights:

- *Buck v. Germany*, no. 41.604/98, 28.04.2005;

- *Camenzind v. Switzerland*, no. 136/1996/755/954, 16.12.1997;

- *Cremieux v. France*, no. 11471/85, 25.02.1993;

- *Iordachi et al v. Moldova*, no. 25198/02, 10.02.2009;

- *Jalloh v. Germany*, no. 54801/00, 11.07.2006;

- *Klass et al v. Germany,* no. 5029/71, 06.09.1978;

- *Kopp v. Switzerland,* no. 13/1997/797/1000, 25.03.1998;

- *Kruslin v. France,* no. 11801/85, 24.04.1990;

- *Leander v. Sweden,* no. 9248/81, 26.03.1987;

- *Malone v. United Kingdom,* no. 8691/79, 02.08.1984;

- *Niemietz v. Germany,* no. 13710/88, 16.12.1992;

- *Rotaru v.Romania,* no. 28341/95, 04.05.2000;

- *S. und Marper v. United Kingdom (GC),* no. 30.562/04, 04.12.2008;

- *Segerstedt-Wiberg et al. v. Sweden,* no. 62.332/00, 06.06.2006;

- *Szabo and Vissy v. Hungary, no. 37138/14, 12.01.2016;*

- *Uzun v. Germany,* no. 35623/05, 02.09.2010;

- *Zakharov v. Russia (GC),* no. 47143/06, 04.12.2015.

Languages:

German.