AUT-2023-3-004

a) Austria **b)** Constitutional Court **c)** **d)** 14/12/2023 **e**) G 352/2021 **f)**
g) ECLI:AT:VFGH:2023:G352.2021 **h)** Codices (German)

Keywords of the Systematic Thesaurus

5.3.32 · Fundamental Rights - Civil and political rights - Right to private life
5.3.32.1 · Fundamental Rights - Civil and political rights - Right to private life - Protection of personal data

Keywords of the alphabetical index

Data, Personal, Collecting, Processing / Privacy, Rights and interests, Balance

Headnotes

Data stored on IT devices, e.g., on a mobile phone, may provide a comprehensive picture of the previous and current life of the owner. The seizure of such devices for evidentiary reasons therefore constitutes a serious interference with the owner's right to respect for his private and family life as well as with his right to data protection.

In view of the necessary prevention of abuse, effective protection of these fundamental rights requires that seizure of data carriers be subjected to prior approval of an independent court.

In addition, the legislator must take adequate precautions to ensure that the prosecution authorities adhere to the principle that data may only be evaluated to an extent that is absolutely necessary for the purpose of the investigation, and that these authorities proceed in a manner that is both understandable and verifiable.

Summary

I. Under Article 110.1 of the Code of Criminal Procedure of 1975 (*Strafprozeßordnung* 1975, hereinafter, "StPO") as amended in 2004, items may be seized if this appears necessary for evidentiary reasons in criminal investigations. This provision applies to any movable physical property, including laptops, PCs, mobile phones and other IT devices.

In addition to access to physical data carriers, Article 110 StPO also allows access to the data stored on the data carrier without the storage medium being (physically) taken into custody by prosecution authorities.

One of the main differences between the seizure of data storage media and the seizure of other items is the possibility of evaluating the data stored on a data storage medium and thus drawing conclusions about the person concerned. The data stored on a secured data carrier is potentially extremely extensive and can, among other things, be linked and stored

with otherwise available data (not only from prosecution authorities). This data can (even when linked to other data) provide a comprehensive picture of the previous and current life of the person concerned, which is usually not the case when evaluating other items. The prosecution authorities are not only allowed to access the locally stored data, but may also retrieve externally stored data, i.e., data stored on a network or in a cloud.

The law does not regulate how the data stored (locally or externally) is evaluated, neither in terms of content nor procedurally; it is therefore entirely up to the prosecution authorities how they proceed with the evaluation of the data.

If the content stored (locally or externally) is encrypted or protected against access, the prosecution authorities are allowed to decrypt the data and overcome the access block.

For the seizure measure (and for the evaluation of the seized item) no urgent suspicion is required in the investigation procedure, but an initial suspicion is sufficient. This occurs when, based on certain evidence, it can be assumed that a crime has been committed.

The law does not provide for any specific severity or other qualification of the crime as a requirement to seize and evaluate items; it is sufficient that, on the basis of certain evidence, it can be assumed that some crime has been committed.

The seizure does not require judicial approval, but only an order from the public prosecutor's office, which the criminal police must carry out. Under certain conditions, the criminal police may seize items on their own initiative.

Not only items that the accused is in possession of can be seized, but also items that are in the possession of (non-suspect) third parties, provided that there is initial suspicion against another person and the item appears to be necessary evidence.

The applicant is suspected of infidelity. On 21 July 2021, the public prosecutor ordered the applicant’s mobile phone and his Outlook calendar to be seized.

The applicant objected to this on the grounds that the measure was disproportionate. The criminal court dismissed the objection; it argued that securing the cell phone and the calendar were necessary for evidentiary reasons and were the most lenient means to clarify the suspicion.

The applicant filed a constitutional complaint with the Constitutional Court, claiming that the legal provisions allowing seizure of cell phones violate the right to respect for his private and family life (Article 8 ECHR) and the right to data protection under Article 1.1 of the Data Protection Law (*Datenschutzgesetz* – hereinafter, "DSG”).

II. The fundamental right to data protection guarantees every person the right to confidentiality of personal data concerning him or her, provided that there is an interest worthy of protection, in particular to protect private life. This right to confidentiality of personal data worthy of protection not only protects against the disclosure of collected data, but also prohibits the person concerned from being unduly obliged to disclose it. This

protection applies even if the obligation to disclose is not imposed on the data subject himself, but on a third party who has protected data relating to the data subject.

Article 1.2 DSG contains a material legal reservation in this regard, which sets the limits for interference with fundamental rights more narrowly than is the case with regard to Article 8.2 ECHR: Apart from the use of personal data with consent or for vital purposes in the interests of the person concerned, the right to secrecy may therefore be only limited to protect the overriding legitimate interests of another, and, in the case of interventions by a state authority, only on the basis of laws that are necessary and sufficient for the reasons stated in Article 8.2 ECHR.

The Constitutional Court noted that the aim pursued by these provisions of prosecuting criminal offences by securing (accessing and evaluating) evidence, which also includes data storage media, is a legitimate aim. The corresponding powers of the prosecution authorities are also suitable for achieving this (legitimate) goal. A further prerequisite for proportionality and thus for the admissibility of the interference with the fundamental right to data protection and respect for private and family life is that the severity of the specific interference does not exceed the weight and significance of the objectives pursued by the interference. With regard to data that is particularly worthy of protection, Article 1.2 DSG provides a further barrier to intervention that the use of such data may only be intended to protect important public interests and that the respective law must establish appropriate guarantees for the protection of the confidentiality interests of those affected. The Constitutional Court found that the contested provisions failed to meet these requirements.

In view of the extensive and intrusive powers of the prosecution authorities and the necessary prevention of abuse, effective protection of fundamental rights can only be guaranteed through the control of an independent court.

In particular, a court should determine which categories of data and which data content may be evaluated over a period of time and for which purposes if it approves seizure.

The provisions of the StPO allowing the public prosecutor and the criminal police to seize mobile devices without the approval of a court therefore violated Article 1.2 DSG in conjunction with Article 8.2 ECHR.

The Constitutional Court added that the requirement for judicial authorization to seize a data storage medium would not in itself guarantee adequate protection of fundamental rights.

Rather, the legislator must weigh and balance the public interest in the prosecution and investigation of crimes against the constitutionally protected interests of those affected, in particular the protection of confidentiality interests and the protection of privacy and family life.

The constitutional requirements for this balancing task vary depending on the intensity of the intervention caused by the specific legal design. In this proportionality test, the legislator must consider several aspects:

First, it can make a difference whether data carriers are to be seized for all crimes or only for certain crimes, e.g. only for serious crimes or cybercrime.

The constitutional admissibility of seizing data carriers may also depend on whether the legislator has taken precautions to ensure that the evaluation of the seized data carriers is limited to the necessary extent and that the evaluation procedure is comprehensible and verifiable.

The legislator shall also ensure that those affected by the seizure of a data medium and the evaluation of the data stored on it (locally or externally) can receive the information in an appropriate manner that is necessary to protect their rights in the preliminary investigation and in the main proceedings.

Finally, it must also be taken into account whether the legislator provides for effective measures of independent supervision, which checks whether the prosecution authorities have observed the legal precautions and court approval when evaluating the data and whether the rights of those affected have been respected in a proportionate manner.

Cross-references

Constitutional Court:
- G 47/2012, 27.06.2014, AUT-2014-2-003;
- G 72-74/2019, 11.12.2019, AUT-2019-3-003.

European Court of Human Rights:
- *Klass v. Germany*, 5029/71, 06.09.1978, ECH-1978-S-004;
- *Leander v. Sweden*, 9248/81, 26.03.1987, ECH-1987-S-002;
- *S. and Marper v. United Kingdom* (GC), no. 30562/04, 04.12.2008, ECH-2009-1-003;
- *Zakharov v. Russian Federation* (GC), no. 47143/06, 04.12.2015;
- *Szabó and Vissy v. Hungary*, no. 37138/14, 12.01.2016.