SVK-2016-2-002
a) Slovakia / **b)** Constitutional Court / **c)** Plenum / **d)** 29-04-2015 / **e)** PL. ÚS 10/2014 / **f)** / **g)** *Zbierka nálezov a uznesení Ústavného súdu Slovenskej republiky* (Official Digest), 29.12.2016, 443/2015 / **h)** CODICES (Slovak).

Keywords of the Systematic Thesaurus:

03.16	General Principles - **Proportionality.**
03.18	General Principles - **General interest.**
05.03.32	Fundamental Rights - Civil and political rights - **Right to private life.**
05.03.36.02	Fundamental Rights - Civil and political rights - Inviolability of communications - **Telephonic communications.**
05.03.36.03	Fundamental Rights - Civil and political rights - Inviolability of communications - **Electronic communications.**

Keywords of the alphabetical index:

Data, retention, electronic communication / Data, personal, protection, disclosure.

Headnotes:

Obliging telecommunications and internet providers to store data concerning communications parties in case prosecuting authorities should require them, regardless of whether these communications parties' conduct may be linked to serious crime and without providing safeguards against possible misuse of these data, constitutes a violation of the right to private life for failing the second part of the proportionality test due to not being necessary for achieving the pursued objective.

Summary:

I. On 29 April 2015, the Constitutional Court decided on the non-conformity of several provisions of the Electronic Communications Act, Criminal Procedure Code and Police Force Act with the Constitution, Charter of Fundamental Rights and Freedoms and European Convention on Human Rights.

The challenged provisions of the Electronic Communications Act introduced an obligation for internet providers and mobile phone service providers to store, for a certain period of time, traffic data, location data, and data concerning communications parties if needed by state authorities. The challenged provisions of the Criminal Code and Police Force Act then regulated the access of prosecution authorities to these data.

The motion for the commencement of the proceedings on the constitutional conformity of these laws was filed by a group of 31 members of Parliament (hereinafter, the «applicants»). The applicants stressed, *inter alia*, that the introduction of the duty to store data on electronic communications constitutes a major interference with privacy, since it implies the monitoring of all inhabitants of Slovakia, regardless of their integrity and reputation. Data would be thus collected daily on every inhabitant of Slovakia, including with whom he or she makes phone calls, to whom he or she sends text messages and emails, when he or she did so and where he

or she was at the time, what type of telephone or service he or she used, how long the phone call lasted, etc. A complete personality and communications profile of an individual can be made using this information. Furthermore, it enables them to track the movements of the individual and may reveal a number of essential characteristics of his or her identity or behaviour, in other words, a substantial part of his or her private life.

II. After examining the motion, the Constitutional Court concluded that the challenged legislation requiring the storing of data for the purposes of their possible disclosure to state authorities served a legitimate aim of public interest, i.e. fight against serious crime and protection of public security.

However, this fact in itself is insufficient to conclude that the said legislation conforms to the Constitution. As indicated, it is possible to learn a great deal of information about the private lives of individuals by analysing stored communications data. This situation together with sustained, systematic and pervasive data collection might have induced a feeling in the minds of the affected individuals that their private life is subject to continuous surveillance.

Under these circumstances it was necessary to assess whether the challenged legislation is proportionate and necessary for the realisation of the pursued objectives.

The challenged provisions of the Electronic Communications Act applied to all forms of electronic communications, which is very widespread and of increasing importance in the daily life of the inhabitants. Data retention applied to all persons using electronic communications services. It was thus also applied to persons in whose case there was no reason to suppose that their conduct could be even indirectly or remotely linked to serious crime.

For that reason, the legislation on electronic communications could not be considered as proportionate and necessary for the realisation of the pursued objective. It is certainly possible to fight serious crime and ensure public security through other means which constitute a less intensive interference with right to privacy in comparison to preventive data retention. One possibility would be for example to monitor and store data only on specific, predefined communications participants and under specific conditions.

It followed then from the wording of the Criminal Procedure Code and Police Force Act provisions that, contrary to the regulation found in the Electronic Communications Act, the power of prosecuting authorities to require identification and disclosure of data on electronic communications applies not only to specific, predefined crimes, but rather to all intentional crimes (according to the challenged provision of the Criminal Procedure Code) or to any crime (according to the challenged provision of the Police Force Act). In the opinion of the Constitutional Court, these conditions for the interference with the fundamental right to protection of privacy, private life and personal data are defined too broadly and vaguely.

The power of prosecuting authorities to require identification and disclosure of data on electronic communications cannot be considered a usual and routine means of prevention and detection of crime due to the intensity of its interference with fundamental rights. This measure can be used solely in cases where there are no other means to achieve this objective, which would be less of an interference with fundamental rights.

Any adequate legal regulation should furthermore contain clear and detailed rules for securing stored data. The legislator should also consider introducing more detailed rules for the contents of the court order to identify and disclose data on communications traffic as well as of the motion of prosecution authorities seeking to have this court order issued. Given the nature of the proceedings and decision-making in these matters, where the participation of the person concerned in the proceedings is not expected, the court's task is also one of «finding a balance» in the procedural situation and it is inacceptable for the Court to be in the position of an «assistant» to the indictment, since the Court must remain impartial under all circumstances.