ABSTRACT, KEY WORDS

Seizing digital tracks for the purpose of a criminal proceeding

This thesis analyzes procedural institutes of law that serve to seize digital traces on the Internet to investigate cybercrime.

This document also deals with a selected procedural institute of the Convention on Cybercrime, which serves to secure digital traces. Furthermore, an assessment is made as to whether the Czech legislation meets these requirements.

Data retention analysis provided information on what traffic and location data are and describes the extent of their retention. The issue of identification of offenders based on seized IP addresses was explained and anonymization methods were explained.

The main goal of the thesis is an extensive elaboration of some relevant procedural institutes of the Code of criminal procedure no. 141/1961 Sb., through which digital traces are seized. This data may lead to the identification of the offender, and also for conviction of guilt during criminal proceedings. The thesis elaborates institutes: a record of telecommunication traffic, monitoring digital communication, data freeze, and physical provision of devices.

This work compares individual institutes with the requirements of the Convention on CyberCrime. The author of this thesis describes in detail the conditions defined by Czech legislation, under which they can be used. This thesis offers a demonstration of the practical use of legal instruments and provides statistics on the use of these instruments. The individual legal institutes are supplemented by a proposal of de lege ferenda. This document also describes problems of encryption, as well as the possibilities of law enforcement authorities to break encryption or other facts associated with the extraction of digital data or evidence.

The last chapter of the work briefly lists the various stages of criminal proceedings. In these phases it puts the possibility of using individual institutes.

At the end of the thesis, it evaluates the suitability of the Czech legislation for the effective provision of digital traces, as well as for penalizing crimes committed on the Internet.

Keywords

Cybercrime, operational and location data, digital traces