Criminal Law and Criminological Aspects of the Internet Criminality

Key words: Internet, Criminal law, Criminology

Abstract (EN):

Internet criminality is a very young phenomenon; the internet itself was presented in the recent form only about 20 years ago. Nevertheless, the relative youth of the internet does not mean that the internet crimes are less serious or less prevalent than other criminal activities. The mass, relative anonymity and progressive globalization of the internet together with bustling development of computer technology provide both the organized crime and individuals with perfect means to commit all sorts of offences.

With regard to its extant, this study is not supposed to serve as an overall and full detailed analysis of the internet criminality. The objective of this paper is a criminological description of socially dangerous phenomenons related to the internet, concretely the origin of these phenomenons in the society, the most frequent *modus operandi* of the internet crime, means of prevention and the criminal law qualification of the relevant criminal activities. The paper itself is divided into four separate parts.

The first part contains a general introduction into the problems of internet criminality. We can find there a definition of the term “internet” and “internet criminality”, its differentiation from the terms “computer criminality” and “cybernetic criminality” and its further classification. Futhermore, it provides basic characteristics of the offenders of internet criminality, reasons for the spread of this type of criminality and general criminal law issues related to the internet criminality.

The second part describes selected types of criminal activities committed directly or at the hand of internet. This part is divided into five titles; each of them contains criminological and consequently criminal law analysis of each type. The emphasis was placed on the most actual problems, i.e. criminal protection of the copyright, “hacking” and internet viruses, so called Nigerian scam letters and “phishing”, illegal internet distribution of pornography (especially the child pornography), and “abuse of the computer time” in context of the internet.

The third part consists of the critical analysis of the actual legislation (*de lege lata*) brought by the new Penal Code, effective from 1st January 2010, and suggests possibilities of future changes of the legislation (*de lege ferenda*) that may help to overcome current difficulties set by the new criminal code.

The last part of this thesis compares different criminal regulations of cybercrime of selected European countries (Slovakia, Switzerland and Germany) with Czech regulation using two points of view. The first one explores the conformity of the concerned regulation with the CoE Convention on Cybercrime as the minimal standard of criminal regulation of cybercrime. The second one analyzes the comprehensibility and certainty of the regulation for the recipients.