Abstract

Computer related fraud is categorized as one of the forms of computer or cybercrime which impacts several dimensions including loss of property and harm to computer security. This computer crime is complex and varies in pattern. The amendment of Computer related crime Act B.E. 2560 reflects the importance of preventing and suppressing this crime by amending section 14 (1) as a specific offense.

However, in considering character of computer related fraud and related foreign laws, the legal issue arise whether section 14 (1) cover the complex and vary behavior of computer fraud in digital economy. This research classified computer related fraud into 4 group of behavior, i.e., computer fraud targeting automatic programming, computer fraud targeting financial transaction, “Phishing” and “Scam” and then studied the application of section 14 (1) to the 4 groups of behavior by taking a comparative analysis method of Thai and related foreign laws.

The results of this research indicated several problems and obstacles of section 14 (1) for applying to computer related fraud especially fraud which target automatic decision, e.g., the section does not cover a variety of action relating to computer fraud targeting automatic processing such as suppress, interfere, alter, delete because the action element is limited only to “input” of computer data. In addition, due to the fact that element of data was limited to “Fraud, false or distortive” computer data, this section cannot be applied to the fraud that using code to affect the automatic decision or processing of program. Consequently, the research proposed the recommendation to amend section 14 (1). In particular, the “model law” of computer fraud was suggested in order to amend Thai computer crime law in compliance with international standard.