Search and Seizure of Electronic Evidence

As information and communications technologies have entered everyday life, computer-related crime has dramatically increased. As computers or other data storage devices can provide the means of committing crime or be repository of electronic information that is evidence of a crime, the use of warrants to search for and seize such devices is given more and more importance.

The primary source of the law governing electronic evidence in criminal investigations is the Criminal Procedure Act (the “Act”). The search and seizure of electronic evidence is in most respects the same as any other search and seizure. For instance, as with any other search and seizure, the search and seizure of computers or other electronic storage media must be conducted pursuant to a warrant which is issued by a district court if there is probable cause to believe that they contain evidence of a crime. In addition to the general principles, however, the Act, as amended in 2011, has in place the following specific provisions for electronic evidence stored in computers or other data storage media.

1) In case that electronic information stored in computers or other data storage media is to be searched and seized, the information to be searched must be identified with particularity and shall be obtained in the form of printed or electronic copies. If it is unfeasible to specify the scope of information to be obtained in copies, or if the purpose of the seizure cannot be accomplished by obtaining the specified information in copies, computers or other data storage media themselves may be seized (Article 106(3) of the Act).

2) In case that the electronic information seized in the form of printed or electronic copies contains personal data, the data subject must be notified without delay (Article 106(4) of the Act).

3) In case that electronic information stored in computer or other data storage media is to be searched and seized, the warrant must describe with particularity the period during which the information was created, besides the name of the suspect, the crime, the things to be searched and seized and the place to be searched, which are generally required to be specified in any search and seizure warrant (Article 114(1) of the Act).

It has been pointed out, however, that these current rules governing electronic evidence do not fully reflect the particular characteristics of electronic information, such as mass quantities, non-visibility, non-readability or network association. In a recently released report, the National Assembly Research Service discusses potential reforms to the current rules to address issues, in particular, relating to (i) the search and seizure of remotely located servers; (ii) the search and seizure of servers where a huge array of information (including irrelevant

(Continued)
information) is stored; (ii) the search and seizure of information owned by a third party; (iii) the suspect’s or their counsel’s participation in the search process; and (iv) deleting or destroying electronic information seized.

On the other hand, under Article 13 of the Protection of Communications Secrets Act, prosecutors and law enforcement agents may also require telecommunications operators to submit telecommunications data if it is necessary in criminal investigations. This provision can serve as another path that prosecutors and law enforcement agents may turn to, in particular when they need to search for log information associated with the internet of things, or unmanned aerial or ground vehicles.

As the search and seizure of electronic evidence is given more and more importance in criminal investigations, it would be advisable to keep abreast of further developments in relevant legal and regulatory reforms.