THE UNAUTHORIZED USE OF A COMPUTER : A CRIMINAL OFFENCE

By
Panagiota Koutsogiannis*
LEGER ROBIC RICHARD, Lawyers
ROBIC, Patent & Trademark Agents
Centre CDP Capital
1001 Square-Victoria - Bloc E – 8th Floor
Montreal, Quebec, Canada H2Z 2B7
Tel.: (514) 987 6242 - Fax: (514) 845 7874
www.robic.ca - info@robic.com

The Canadian Criminal Code creates an indictable offence in cases where the unauthorized use of a computer has been established (s. 342.1). In fact, four separate offences emerge from this same section and can be identified as follows: (1) the obtaining offence, (2) the interception offence, (3) the user offence, and finally (4) the enabling offence. In order to trigger the application of this section, the unauthorized acts must have been committed fraudulently and without colour of right. It is important to note that these two elements are cumulative and therefore must both be present in order for a court to find the accused guilty of any of the four offences mentioned above.

In a recent decision, *R. c. Paré* JE-97-1179, the Court of Quebec was compelled to analyze the parameters of the obtaining offence and determine whether a police officer had acted fraudulently in obtaining computer services without colour of right. The accused admitted to his absence of right in obtaining the services however he denied acting fraudulently. The Court was of the opinion that an act is not qualified as fraudulent simply because it is not authorized. The Defendant s conduct must also have been dishonest and morally wrong. The Defendant tried to minimize the gravity of his actions by conceding that his superiors knew and tolerated the situation. However the Court found his conduct to be equivalent to wilful blindness and disregard and his attempt to justify his use did not remove his fraudulent intentions.

The first of the four offences mentioned above is the obtaining offence and arises when any person fraudulently obtains a computer service either directly or indirectly. For the purposes of this section, a computer service includes the processing of data as well as the storage or retrieval of data. Obtaining a computer service is far from being a criminal offence, however coupled with the two elements of fraud and absence of right, the Court would have sufficient

evidence to convict if it was convinced of the evidence against the Defendant beyond a reasonable doubt. Today with the evergrowing presence of the Internet worldwide, a more accurate and complete definition of a computer service should perhaps include the external transmission or reception of information as a means of telecommunication.

The second offence created by s. 342.1 of the Canadian Criminal Code is the interception offence and will be set off by any person who intercepts or causes to be intercepted, directlly or indirectly, any function of a computer system. The list of devices capable of causing the interception is not exhaustive and may include any contrivance which may be used to intercept any function of a computer system. However, a hearing aid used to correct subnormal hearing of the user to not better than normal hearing is specifically excluded from the various possible methods of interception provided for by this section of the Criminal Code. A computer system as used in this section can be defined as a device or a group of interconnected or related devices that (1) contain computer programs or other data or (2) perform logic and control, and may perform any other function pursuant to computer programs.

The user offence is committed when someone uses or causes to be used, directly or indirectly, a computer system with the intent to commit an offence such as the obtaining or interception offences, as described above, or mischief in relation to data or a computer system (s. 430). The burden of proof lies with the plaintiff to show that all the elements required for the commission of the prohibited act were present. The Plaintiff must first prove the physical act of using a computer system, whether directly or indirectly. Furthermore, the Plaintiff must also show that the act was committed fraudulently and without colour of right. Evidence of these elements is still insufficient to impose criminal liability on the accused. For this offence, an additional mental element must also be proven; the Plaintiff must prove the Defendant s intent to commit either the obtaining or interception offence or mischief in relation to data or a computer system.

The offence of mischief in relation to data, although not one of the four offences dealt with in the present article, is directlly linked to the provision on the unauthorized use of a computer. For the purposes of both sections 342.1 and 430 (1.1) of the Criminal Code, data is defined as a representation of information or of concepts that are being or have been prepared in a form suitable for use in a computer system. When a person wilfully destroys, alters, renders ineffective or interferes with the lawful use of data, he is committing the offence of mischief, however, when a computer is used fraudulently with the intent of committing these mischievous acts, the user offence is also said to have been committed.

The fourth and final offence created by s. 342.1 is the enabling offence. This offence will have been committed if a person used, possessed, trafficked in or

permitted another person to have access to a computer password that would enable a person to commit one of the three offences described above. A computer password allows a computer system or service to be obtained or used by keying in certain data.

Although the Courts have had to deal very little with the offences foreseen in section 342.1, it might be warranted to assume that with the rapidity at which the Internet has been expanding in every part of the world, in businesses as well as in homes, it will create more possibilities for wrongdoing with respect to computers and will perhaps broaden the scope of situations to which this section can be applied.

ROBIC + LAW + BUSINESS + SCIENCE + ART

ROBIC + DROIT + AFFAIRES + SCIENCES + ARTS