An Analysis of Chinese Laws Against Computer Crimes

Hakman A. Wan
Lingnan College, Hong Kong

Ming-te Lu
Lingnan College, Hong Kong

An overview of the computer crime and related legislation in the People’s Republic of China is given. Relevant laws and their interpretation by Chinese legal scholars with respect to negligence, trade secrets, copyright and piracy, data protection and privacy are presented. The unique aspects of the Chinese legal system are accentuated. Due to the differences in the cultural, political, and legal environments, the PRC courts may treat some computer crimes more severely and may hand out penalties accordingly.

Widespread computer use in the People’s Republic of China (PRC) is a recent phenomenon. Business computer use in the PRC before 1980 was almost non-existent (Lu, Qiu, and Guimaraes, 1988). Today, the use of ATMs in the streets and networked PCs in the offices of business enterprises are common scenes. By the same token, computer-related crimes have also emerged and are increasing at an astonishing rate. For example there were only nine computer-related criminal cases in 1986 and 87 (Dong, Zhang, & Zhan, 1995), but the number of cases increased to a little over a hundred in 1989, and to twelve-hundred in 1993. Also, the number of cases handled by the Intellectual Property (IP) Courts in special economic zones in southern China has experienced a drastic increase, from 28 cases in 1990 to 120 in 1993 (Cheetham, 1995).

This article provides an overview of computer crime related legislation in the PRC. An understanding of the legislation will also help millions of IS professionals in the PRC to become more alert to the boundaries between legal and illegal activities and will enable them to become better IS professionals. For the increasing number of business travelers to the PRC and to a large number of expatriates working there, an understanding of different legal concepts and practices with respect to computer crimes in the PRC may prevent them from engaging in seemingly innocent activities (from the Western perspective) which may very well be deemed serious crimes in the PRC and subject to severe punishment.

Currently, computer crime legislation in China includes the Regulations on the Protection of Computer Software of 1991, the Regulations on Safeguarding Computer Information Systems of 1994, and the 1995 Customs Regulations on Protection of Intellectual Property Rights. In addition, many computer crime cases also fall into the domain of the Copyright Law of 1990, the Patent Law 1984, Trademark Law 1982, and Anti-Unfair Competition Law of 1993. This article describes these laws and discusses their applicability to various computer crimes. Viewpoints expressed by Chinese legal scholars on computer crime and related legislation are also summarized to provide readers with insights into the implications of these laws within the particular cultural, political, and legal environment of the PRC. Distinctive aspects of the PRC’s judicial system will be highlighted to provide a background to the study.

After the Introduction section, a brief introduction of the special nature of the judicial system with its implications in prosecution and sentencing is given. The concept of “negligence” and its related legislation are presented in section three. A definition of business (trade) secrets and its implications are
addressed in section four. The issues of copyright and piracy are discussed in section five. In section six, different concepts of data protection and privacy, and lack of their legislation in the PRC regarding this protection and privacy, are explained. A discussion of other computer crimes follows in section seven. A comparison of PRC laws and U.S. laws on computer related crimes is made in section eight, followed by the Conclusion Section.

The Judicial System in the PRC

The judicial system in the PRC is a four-tiered system, the second instance being the final instance. The operational system is chief-judge centered within each court including the highest court, the Supreme People’s Court (Yu, 1997).

In China, the burden of proof rests on the prosecution party as in the West; however, oftentimes, there is a greater burden on the accused to prove their innocence than in a Western court. The penalty for a crime is proportional to the damage caused by the crime to the community, and the court has much leeway in handing out penalties. The judges may consult statutes in the relevant laws when giving out sentences; however, there are other overriding considerations, such as, “Have the secrets been disclosed to foreign organizations or individuals?” or “Is it a counter-revolutionary crime?” The State Secrets Law and State Security Law grant the authorities the power to ascertain what state secrets are and what activities endanger state security. Thus, information which is easily accessible in the West may be regarded as “state secrets” and the person who gains knowledge of such information may be accused of committing a serious crime, especially when information is leaked to foreign organizations or individuals. Furthermore, punishment for computer crimes (and other crimes too) in the PRC may seem quite severe by Western standards; in fact, in some cases, convicted criminals have been executed by firing squads (Cheetham, 1995).

To try computer-related crimes cases, a special court, the Intellectual Property (IP) Court, was first established in June, 1993 in the Beijing Intermediate People’s Court (Chang, 1995). IP courts have since been established by many other provincial and local courts. In addition, in 1994, the Supreme People’s Court announced the Notice on Further Enforcement of Judicial Protection of Intellectual Property Rights whose voice was later amplified by the US and Chinese agreement on an Action Plan in March, 1995. According to the Action Plan (Freeman, 1995), Working Conferences were created at various levels to coordinate and implement IP Rights legislation. Thus, investigation on IP infringement cases lay in the hands of the newly created Task Force Groups and the IP Courts.

Negligence

In the West, issues such as who should be responsible for the fidelity and accuracy of information, who should be held accountable for erroneous and inaccurate information, and the employees’ commitment to assigned duties are largely the domain of ethics (Mason, 1986; Spiro, 1989); exceptions are special cases, such as when the source of information is publicly reliable and regarded as an authoritative basis on which people make decisions. In the PRC, however, when a wrong decision is made as a result of inaccurate information provided by an information system, responsible IS professionals may be liable for prosecution (Hou, and Miao, 1993).

Under the Chinese law, some cases of negligence are regarded as a criminal offense as stated in A few Opinions on the Correct Identification and Handling of Negligence Offenses (Provisional), the Supreme People’s Procuratorate. The seriousness of the offense is in direction proportion to the damage or loss attributed to the act. When the damage or loss is intangible or difficult to ascertain, the prosecution often has much leeway to set the amount of damage. In the Western nations, on the other hand, the prosecution would have to provide the necessary supporting evidence for the claim; thus, an exaggerated claim is less likely to be sustained. In addition, in China, when a person is accused of negligence through which an intangible loss incurred, it may be difficult for the person to prove that negligence is not a causal factor in the event nor to argue the exact value of the damage or loss.

Negligence is often associated with irresponsibility under the Chinese law. Irresponsibility may be supported by evidence like abuse of power or breaching of rules (Liu & Liu, 1993). However, these two types of evidence are more or less related to the mental state of the accused at the time of the alleged commission of the crime. Thus, it leaves much ground for differences between the prosecutors and prosecuted.

Since computer bugs and glitches occur quite often in a computer-based information system and may bring a business operation to a standstill, thus incurring huge losses to a business, IS professionals in the PRC are potentially liable for charges of negligence and irresponsibility under these circumstances. Also, if they are not remorseful after the incident, they could be severely punished (Hou, & Miao, 1993).

Business (Trade) Secrets

Information about a business enterprise’s customers, products, R & D activities, and other sensitive issues are oftentimes the intangible assets of the enterprise. Revealing such information to outsiders may result in material losses to the enterprise; thus, business (trade) secrets legislation is often enacted to deter unauthorized access of business information or secrets. Since IS professionals deal with various aspects of computer-based information systems which collect, store, and process business information on a regular basis, it is important for them to have a good understanding of this legislation in order to differentiate the lawful and unlawful activities. In the PRC, the situation is complicated by the fact that both the charges and the penalties for unlawful access of business secrets can be much more serious than they are in the West.

Although the term “business secrets” appears in the 66th and 120th(2) Articles of the New Civil Procedure Law of 1982, the term was not defined until the Anti-Unfair Compe-
4 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the product's webpage:

[link to purchase]

This title is available in InfoSci-Journals, InfoSci-Journal Disciplines Business, Administration, and Management. Recommend this product to your librarian:

[link to recommend]

Related Content

The Impact of National Culture on Information Systems Planning Autonomy
[link to article]

Digital Government in Remote Locations
[link to article]

Key Issues in Information Systems Management: An Empirical Investigation from a Developing Country's Perspective
[link to article]

Balancing Local Knowledge Within Global Organisations Through Computer-Based Systems: An Activity Theory Approach
[link to article]