2002-11987

PEOPLE'S REPUBLIC OF CHINA：

COMPUTER SECURITY AND PROTECTION OF COMPUTER INFORMATION

China has adopted a number of regulations and administrative measures in recent years to prohibit attacks on computer systems, improper use of computers, and the use of the Internet to commit actions classed as crimes. The Criminal Code itself contains provisions punishing breaches in computer security. In addition, provisions have been adopted on computer viruses, internet service providers, and privacy issues. Since 1991, computer software has also been subject to intellectual property protection under detailed rules, which have been updated to include protection of the rights for transmission via a digital network. Recent changes in legislation have been introduced to meet WTO requirements.

With the growth of foreign trade and the development of a sophisticated, computer using public, the issue of legal protection for automated systems has gained more attention in China in recent years. A range of regulations and administrative measures have been adopted; the discussion that follows covers some of the major pieces of legislation. The provisions in some cases overlap, with one legal norm re-enforcing another.

The laws cover a number of different aspects, including attacks on computer systems themselves and improper use of computers and the Internet to commit actions classed as crimes. Some of the restrictions are similar in nature to what any nation would impose, such as rules against spreading destructive viruses. Others are particular to the policy agenda of government of China, including such caveats as the ban on spreading feudal superstition and the prohibition of inciting hatred between ethnic groups.

Regulations on Safeguarding Computer Information Systems

In 1994, the People's Republic adopted Regulations on Safeguarding Computer Information Systems (hereafter Computer Systems Regulations).[1] This regulation covers computers and related equipment, such as networks. It does not cover individual microcomputers not connected to networks. The regulation places the Ministry of Public Security (the national police agency) in charge of safeguarding automated information systems, but work on security is to be carried out also by the Ministry of State Security (created in 1983 to handle espionage and counter-intelligence), the State Secrecy Bureau, and relevant departments under the State Council.

The regulation states that no organization or individual may use computer information systems to engage in activities that endanger national or collective interests, as well at the legitimate interests of citizens. Furthermore, they are not allowed to jeopardize computer systems. Computer information systems in public agencies are to be protected on the basis of security grades. These grades are to be drawn up by the Ministry of Public Security, together with protective measures to be implemented based on the grades. Offices that use computers connected to international networks must register their systems with provincial-level public security offices. Any incidents related to the security of systems must be reported to local pub

[1] Feb. 28, 1994. Effective the same day. English translation available in Foreign Broadcast Information Service, DAILY REPORT: CHINA [Hereafter FBIS], Mar. 24, 1994, at 34-36.

lic security offices within 24 hours.

The public security organs are to issue warnings or shut down systems for screening in the event any actions have been taken that endanger systems. These include but are not limited to:

· contraventions of computer security systems;

· violations of the registration system for internationally networked systems;

· failure to report incidents promptly; and

· failure to take remedial action after being notified by public security organs of needed improvements in s ecurity.

In addition to warnings, public security organs may impost fines of up to 5,000 *yuan* (about US$605) for an individual or 15,000 *yuan* (about US$1,814) for a work unit, if computer viruses or other data harmful to co mputer systems are deliberately inputted or if special safety products for computer systems, whether hard ware or software, are sold without permission. Any illegal proceeds are subject to confiscation; the fine sh all be 100-300% more than the total proceeds.

The regulation also specifies that if violations of computer security constitute crimes, they may be i nvestigated and perpetrators held responsible under the Criminal Code.[2] When violations constitute infrac tions of public security, they may be punished under the provisions of the Regulations on Security Adminis tration and Punishment.[3] These regulations allow police to impose punishments directly, without trial, con sisting of warnings, fines or detention of up to 15 days; they are generally applied in cases not considered serious enough for prosecution under the Criminal Code.

Criminal Sanctions

The Criminal Code itself provides for punishment of a number of types of breaches of computer se curity. Article 285 punishes improper intrusions of those computer systems containing information on stat e affairs, the construction of defense facilities, and sophisticated science and technical data; the sentence is up to three years in prison or criminal detention.[4] Anyone who deletes, alters, adds, or interferes with th e information in a computer system, causing abnormal operations of the system and serious consequence s, will be sentenced to up to five years of imprisonment or detention; in especially serious cases, the sente nce is five years or more in prison (art. 286). The same punishments may be given to those who delete, al ter, add, or interfere with application programs installed in or processed and transmitted by computer syste ms. The provisions of the article are also extended to those who intentionally create or spread destructive programs such as computer viruses.

In addition to establishing these crimes against computer systems, the Code also discusses the u se of computers to commit other crimes, including financial fraud, theft, embezzlement, misappropriation o f public funds, and theft of state secrets. Punishments are to be applied in accordance with the other articl

---

[2] As revised Mar. 14, 1997, in force from Oct. 1, 1997; English translation available in 9 THE LAWS OF THE PEOPLE'S REPUBLIC OF CHINA 21 -149 (1998). Amended Dec. 25, 1999, Chinese text in 2000 *Zhonghua Renmin Gongheguo Guowuyuan Gongbao* [State Council Gazette] 14-15 (J an. 20, 2000); amended again Dec. 29, 2001, to stiffen penalties for terrorist activities, http://www.isinolaw.com.

[3] Adopted Sept. 3, 1986, as last amended May 12, 1994. English translation available in FBIS, May 16, 1994, at 15-21.

[4] *Supra* note 2. Criminal detention is defined in article in articles 42-44; it lasts from one to six months, the subject is held by the public security organ locally, and he or she is permitted to return home for one to two days each month.

es of the Code that cover those crimes (art. 287).

Computer Information Network and Internet Security Protection and Management Regulations[5]

In 1997, China enacted further regulations on computer security (hereafter called the Network Sec urity Regulations). These regulations were explicitly written on the basis of the 1994 Regulations (art. 1) a nd cover the security, protection, and management of all computer information networks inside the People' s Republic (art. 2).

Like the 1994 Computer Systems Regulations, the Network Security Regulations establish that th e Ministry of Public Security is the body responsible for the security, protection and management of compu ter information networks and the Internet. The Computer Management and Supervision organ of the Minis try is specifically entrusted with protecting the security of networks, as well as the legal rights of service pr oviders and individuals and the public interest (art. 3).

Besides stating that no one may use the Internet to harm national security, disclose state secrets, or injure in the interests of the state, society, groups, or the legal rights of individual citizens or to commit c rimes (art. 4), which echos provisions in the 1994 Computer Systems Regulations, the 1997 document list s information that may not be created, replicated, retrieved, or transmitted via the Internet. This includes i nformation that would:

· incite someone to resist or break the Constitution, laws, or administrative regulations; to overthrow the go vernment or the socialist system; to divide the country; or to increase hatred or discrimination among natio nalities;

· distort the truth and spread rumors, destroying social order;

· promote feudal superstitions or involve sexually suggestive material, gambling, violence, or murder;

· promote terrorism or insult or slander others; or

· injure the reputation of state organs (art. 5).

In addition, the following activities that directly harm the security of computer networks are banned:

· using networks or network resources without proper approval;

· changing network functions or adding or deleting information, either basic to the network itself or being st ored, processed, or transmitted through the network, without permission;

· intentionally creating and transmitting viruses; and

· other activities that harm the network (art. 6).

The Network Security Regulations specify that infringement of the rules outlined in articles 5 and 6

[5] Promulgated by the Ministry of Public Security, Dec. 30, 1997, effective on the same date. English translation at http://www.qis.net/chinalaw/prclaw54.htm.

may result in a warning and, if profits resulted, confiscation of illegal earnings. In addition, a fine of up to 5000 *yuan* for an individual or 15,000 *yuan* for a work unit may be imposed; these fines parallel those imposed under the 1994 Computer Systems Regulations. In serious cases, network access can be cut off for up to six months or the business operating license and network registration of the work unit can be cancelled. Criminal activities will be prosecuted as specified in the Criminal Code (art. 20).

Laxity in observance of computer security can in some instances be punished. Failure to establish a management system for network security and protection, not implementing security techniques, not providing security training for network users, furnishing false or incomplete information or electronic documentation related to security, not having a system to register staff and public users and manage electronic bulletin boards, not removing web addresses or closing servers where relevant state regulations require, and lending or transferring accounts may be punished with an order to remedy the situation and a warning. Any illegal income may be confiscated, and if remedial action is not taken within a specified time, a fine of up to 5000 *yuan* may be imposed on management personnel and other responsible individuals; a work unit may be fined up to 15,000 *yuan*. Especially serious cases may result in networks being closed for up to six months and the loss of business licenses and network registration (art. 21).

Internet Secrecy Provisions

In January 1999, the State Secrecy Bureau issued Provisions on Secrecy Management of Computer Information Systems on the Internet that became effective January 1, 2000.[6] Out of concern for the security of information involving state secrets, computer systems with that information are not to be linked directly or indirectly with the Internet (art. 6). In addition the provisions specify that those who set up electronic bulletin boards, chat rooms, and news groups must be aware of the duty to preserve state secrets and establish management systems to do so (art.10). When using email to exchange information, users must follow relevant secrecy provisions (art. 11), and secrecy education is to be considered a part of Internet technology training (art. 12). Those officials and departments charged generally with maintaining state secrets have the responsibility to handle infractions related to the Internet as well.

Computer Virus Measures

In March 2000, the Ministry of Public Security adopted Measures for Administration of Prevention and Control of Computer Viruses.[7] The Measures define computer viruses and outline administrative responsibilities connected to preventing them from causing harm. All those working on computer virus prevention and control must submit samples of the viruses to a designated unit of the Ministry of Public Security. Any products designed to prevent computer virus damage must be licensed and when sold will have "licensed sales" symbols on them. Work units that use computer information systems must establish systems to prevent the spread of computer viruses, including technical methods and staff training. They must also test for and remove any viruses they find in a timely manner, using licensed virus prevention and control products, and must report major malfunctions caused by viruses. Public security organs may impose various penalties in connection with virus security, including fines of up to 5,000 *yuan* for individuals or 10,000 *yuan* for a work unit. When there are illegal proceeds involved, the fine may be three times the amount gained, up to 30,000 *yuan.*

[6] Transmitted by Xinhua, Jan. 25, 1999; English translation in English translation in Foreign Broadcast Information Service [FBIS], Jan. 28, 2000.

[7] Mar. 30, 2000, effective Apr. 26, 2000. Described in China Legal China, http://www.chinalegalchange.com.

Standing Committee Decision

A number of the provisions in the Network Security Regulations were reinforced by the Decision of the Standing Committee of the National People's Congress (NPC) Concerning Maintaining Internet Security.[8] This Decision stresses that criminal liability will be investigated and dealt with according to the Criminal Code for infiltrating computer information systems, deliberately spreading destructive programs such as computer viruses and attacking computer systems, or arbitrarily suspending computer or telecommunications services in violation of state rules. It also states that the crimes of using the Internet to undermine national security, social stability, and the socialist market economy will be prosecuted under the Criminal Code, including such actions as using the Internet to create rumors, disseminating harmful information, and inciting subversion, as well as infringing intellectual property, disrupting securities trading, and other criminal acts.

Since all of these actions are already outlawed in the regulations or the Criminal Code itself, the purpose of the December 2000 NPC Decision is to underline the importance of the restrictions and guide the development of Internet use.

Internet Service Provider rules

A key component of computer security in China is requirements placed on Internet service providers. The Ministry of Information and Technology issued new rules in January 2002, outlining their responsibilities. One area of concern is protection of their systems; the service providers must protect users' accounts and passwords and prepare for possible system crashes with backup hardware and software.

[8] Dec. 28, 2000. Chinese text in 2001:1 Zhonghua Renmin Gongheguo Quanguo Renmin Daibiao Dahui Changwu Weiyuanhui Gongbao [Gazette of the Standing Committee of the National People's Congress of the People's Republic of China] 18-19 (Jan. 15, 2001).

While the Network Security Regulations specify that the legal rights of citizens are to be protected, that is not the same as allowing unrestricted access to Internet use. A second area of responsibility for service providers is to track people's actions by keeping detailed records of the users' online activities. Those providers that offer services involving "sensitive and strategic sectors," which includes news and bulletin board services and online forums, must compile records of account numbers, addresses, telephone numbers, and the times the service is used. Software must be installed to screen and copy email messages with sensitive material and to stop messages that are considered obscene or subversive from being sent. Reports on illegal activities by users must be provided to the Ministry of Information and Technology, the Ministry of Public Security, and the Bureau for the Protection of States Secrets. News sites must carry news only from Chinese media sources.[9]

Privacy Issues

The Computer Systems Regulations touch on the issue of privacy only indirectly, stating in article 7 that information systems are not to be used to endanger the "legitimate interests of citizens." The regulation does not contain any standards or definitions to determine what a citizen's "legitimate interest" might be. The Network Security Regulations also contain only one article on the issue; article 7 states that the freedom and privacy of network use is protected by law. In addition, the December 2000 NPC Decision states that criminal liability will be attached for such actions as illegally intercepting or tampering with someone's email or infringing on the freedom and privacy of citizens' communications.[10] China does have regulations on state secrets[11] and confidentiality in publishing and the media,[12] but these are designed to protect the secrecy of state documents, rather than to protect the interests of individuals in maintaining privacy.

The Chinese constitution does specify that the freedom and privacy of correspondence of citizens is to be protected, except in cases where "to meet the needs of state security or of criminal investigation" public security personnel may review mail. If this provision were interpreted to apply to electronic mail, it could be the basis for legal protection of privacy in that area.[13]

---

[9] *South China Morning Post*, Jan. 18, 2002.

[10] *Supra* note 6.

[11] State Secrets Law, Sept. 5, 1988. English translation in FBIS, Sept. 9, 1988, at 35-37.

[12] Regulations on Confidentiality in Publishing and the Media, Aug. 3, 1992. English translation available in CHINA LAWS FOR FOREIGN BUSINESS [Hereafter CLFB] ¶19-578 (Sydney, CCH Australia, 1982-).

[13] Art. 40. Constitution of the People's Republic of China, Dec. 4, 1982, as last amended Mar. 15, 1999. English translation of available in 1 CLFB ¶4-500.

Intellectual Property

The intellectual property represented in computer systems was first protected in detail under the 1991 Computer Software Protection Rules.[14] The Rules were developed in accordance with the existing copyright law, which included computer software as one of the types of works it covered.[15] Since that time both laws have been updated. The revised Copyright Law, adopted in 2001,[16] further outlines the protection provided for online materials and brings other provisions of the Law into the digital age. For example, article 10 defines the rights related to copyright; item 7 of that article now states the right to rent the use of the copyrighted item for compensation, and that right explicitly applies to computer programs. Item 12 is the right to transmit information via a digital network. Article 37, on performers' rights, includes the right to authorize others to transmit a performance via digital networks.

Protection under the original Computer Software Protection Rules was granted to works created by Chinese citizens, whether or not the software had been published. For foreigners, protection was granted if the software was first published in China, if a copyright protection agreement had been concluded between the foreigner's country and China, or if both countries participated in an international copyright protection convention.

The Rules established a system of registration for software; once the designated government organ approved registration, it issued a registration certificate and made a public announcement.[17] In addition to the Rules, China issued Measures for Computer Software Copyright Registration.[18] These Measures described in detail the procedures to be followed for application for registration of software and for examination and approval of such applications.

Following the adoption of the new Copyright Law, new Regulations on Protection of Computer Software and Measures on Software Copyright Registration were issued.[19] Changes were put in place to meet WTO requirements, including the key provision that software can be accorded copyright protection even if not registered in China, although registration is still encouraged. Software developers now can own the right to publish, revise, copy, lease, broadcast, and translate the software. The copyright is effective for life plus 50 years after the death of the developer. The rules also state that violations of copyrights for software will be punished with cessation orders and fines. In serious cases, the government can confiscate equipment and materials and prison sentences may be imposed.[20]

---

[14] May 24, 1991, effective from Oct. 1, 1991. English translation available in CLFB, ¶11-704.

[15] Art. 3. Law adopted, Sept. 7, 1990, in force from June 1, 1991. English translation available in CLFB ¶11-700.

[16] Oct. 27, 2001; translation available from the International Intellectual Property Alliance.

[17] Art. 23, *id.*

[18] Apr. 6, 1992. English translation in CLFB ¶11-706.

[19] Regulations, issued Dec. 20, 2001, effective Jan. 1, 2002, http://www.isinolaw.com; Measures effective Jan. 1, 2002, "China Revises Software Copyright Registration Measures." Xinhua, Mar. 5, 2002.

[20] "State Council Releases New Statute on Copyright Protection of Computer Software Products," CHINA IT & TELECOM REPORT, Jan. 4, 2002, via LEXIS/NEXIS, Asiapc library.

Prepared by Tao-tai Hsia, Chief, Eastern Law Division,
and Constance A. Johnson, Senior Legal Research Analyst
Legal Research Directorate
Law Library of Congress
March 2002