高等政法院校法学教材

法律英语教程

（下册）

司法部法学教材编辑部编审

主编 宋 雷

成都科技大学出版社

高等政法院校法学教材

法律英语教程

（下册）

A Course Book of LEGAL ENGLISH

（BOOk Ⅱ）

司法部法学教材编辑部审

主　编：宋　雷

成都科技大学出版社

(川)新登字 015 号

责任编辑:李世雄　王　杨
封面设计:沈　飚

法律英语教程
主　编　宋　雷

成都科技大学出版社出版发行
西南政法大学印刷厂印刷

开本:850×1168　1/32　印张:13.25
1994年12月　第1版　　1995年5月　第1次印刷
印数:1—1000　　字数:332千字
ISBN 7－5616－2818－8/H・308

定价:19.50元(上、下册)

说　明

随着改革开放的不断深入和社会主义市场经济的迅速发展，我国对具有较高的专业外语水平的法律人才的需求量日益增长，为适应这一形势的要求，我们特请政法院校从事法律英语教学的老师编写了《法律英语教程》，以供业已达到大学英语四级或六级水平的大专院校学生继续学习英语使用。

本教程以培养学生阅读和理解法学各专业文章及书籍能力为目的，同时要求学生能掌握一定的法律英语翻译技巧，对中等难度的文章的翻译速度达到每小时 1000 单词左右，准确率不低于 70%。

本书选材新颖，题材广泛。该书在编写过程中注意语言的实用性，且注重增加词汇输入量，提高复现率，加强语感的培养。

整个教材分为上、下两册，由浅入深，难度逐渐增大。上册选文多为法学基础理论简介，下册则着重介绍有关民、商法及司法文书等实用性较强的内容。

鉴于编者水平有限，加之时间仓促，书中疏漏之处在所难免，欢迎广大读者批评指正。

《法律英语教程》主编为李荣甫（上册）、宋雷（下册），该书经多方讨论，由主编统稿定稿。并由宋雷为上册审稿，李荣甫为下册审稿。本书编者为：李荣甫、刘镭生、宋雷、沙丽金、吴月祥、范晓玲、顾海根、秦浩、龚兵、樊林波（以姓氏笔划排列）。

主　编：宋　雷　副教授　西南政法大学外语系主任

副主编：刘镃生　副教授　中南政法学院外语系主任

顾海根　讲　师　华东政法学院外语教研室

撰稿人：（以姓氏笔划）

刘镃生　宋　雷　吴月祥

顾海根　秦　洁　龚　兵

试读结束：需要全本请在线购买：　www.ertongboo

CONTENTS

Lesson One

Computer Crime

The computer has become a ubiquitous machine in modern society and just as common is the problem of computer crime. The seriousness and pervassiveness of computer crime is well documented[1]. The difficulties in combating computer crime are numerous. Frequently, prosecution is difficult due to the sophistication of the crime. Law enforcement officers[2] normally do not receive the training necessary to investigate high-tech computer crimes. Even legislation has failed to keep pace with the advances in technology. Policing of[3] computer crime is complicated by fact that many people consider computer criminals in a different class than the common criminal. Some even regard computer criminals as a sort of folk hero in the battle of "man against machine" or the "large corporation"[4].

The data gathered by the author from a review of current industrial practices, litigation trends, literature in the professional journals, and interviews with security and departmental managers suggest that there is a need to evaluate the laws protecting personal computers, data, and networks as well as legislation regulating computer crime both internationally and in the United

States.[5] Because of the growing use of networking and the international use of computers, many of the problems that arise in the investigation of computer crime are international in scope and application.

Companies and governmental agencies historically have paid attention to the security of sensitive data.[6] Legislation has been enacted to protect proprietary datas[7] of company and property laws[8] over the years have been modified to provide for prosecution of those who would steal data and secrets as opposed to tangible assets.[9] The mainframe computer,[10] personal computer, and computer networks have introduced a new consideration into the topic of data security and integrity.

Access restriction[11] has always been a prerequisite for access control to safeguard the security and integrity of sensitive data. Prior to the common use of personal computers data was stored in file cabinets or vaults or "computer rooms"[12] which were secured by mechanical locks and security personnel. The hard disk storage technology and networking ability[13] of the personal computer has made it possible to have access to numerous data bases[14] and store very large amounts of data on a single personal computer which may have little if any mechanical security devices to protect against unauthorized access[15]. This situation probably evolved from the fact that when personal computers were first introduced there were few personal computers around and few people knew how to use them. Data security was inherent in[16] that the average person just could not figure out how to do anything harmful even if he or she did have physical access to the personal computer. This type of inherent security worked well in the past

but it is not as safe now.

At one midwest county jail[17] in 1989, for example, an inmate[18] was nearly successful at escaping from the jail by gaining access to the booking computer[19] and changing his release date. An investigation revealed that no other security measures such as password protection guarded the system from unauthorized entry because of the administration's assumption that inmates would not be "smart enough to figure out how to work the computer even if they did have access to it." Obciously this was an erroneous assumption.

The perception that inherent security measures are sufficient is not limited to criminal justice administrators. Many of the security procedures practiced by directors of Information Service (IS) departments and other personnel charged with the care and security of personal computers and data are inadequate. This inadequacy in security can be due to many reasons. Some common explanations are: (1) the lack of an explicit charge[20] by management to personnel to evaluate and provide a secure operating environment, (2) the lack of knowledge and training by the supervisor and operating personnel and (3) the absense of a central coordinating of controlling office to secure equipment and data located throughout an organization.

Basically security policies and procedures can be categorized as responding proactively or reactively to risks. Proactive policies and procedures[21] are those activities which attempt to prevent damaged, lost or compromised data prior to an actual attack. This would include such actions as establishing password protection of data to detour unauthorized access.

Reactive policies and procedures[22] are those activities which the organization undertakes in the event of a security violation, the actual occurrences of an emergency or a loss of data or equipment. Reactive policies can include procedures for investigation to determine the identity of violators and recovery of equipment, prosecution of violators, or emergency procedures to be followed in the event of fire. The value of proactive security policies and procedures is obvious in preventing loss and minimizing risk. The value of reactive measures should not be underestimated. Just the presence of procedures which provide for the identification and prosecution of violators can act as a deterrent to some people.[23] Reactive policies and procedures should provide a plan of action for what could be called a damage control guide. A damage control guide would outline specific actions to be taken by personnel and the organization in the event of a major security violation. The policies and procedures must reflect prior planning, verification, and preparation to be an effective damage control guide, to minimize losses, and to avert total disaster. For example, an organization cannot restore lost data if no back up procedure has been instituted and faithfully followed.

The greater risk, however, is not lax security procedures but the lack of perception by management and personnel that an organization is at serious risk. In addressing the problem of software security, for example, William E. Perry, executive director of the Quality Assurance Institute Orlando, Florida stated, "My perception is that most IS (Information Service) directors feel that they are doing well now—and they're not. I always liken it to Alcoholics Anonymous; you don't go until you know you're an

试读结束：需要全本请在线购买： www.ertongboo

alcoholic. You have to say, "I have a problem."

Many managers and organizations will not admit to a problem in personal computer security because they think that "security on a personal computer is too troublesome, too comfusing, and too expensive". Likewise law enforcement officials and public prosecutors frequently deny that there is a problem in catching and prosecution of computer criminals. Like other "white collar" crimes the computer criminal receives low priority and few resources in the criminal justice system.

It must be admitted that not all loss of data is due to criminal intent. There is a certain amount of data loss and security breach that is accidental. This is because it is the humans in the environment that produce the adverse operating parameters for data security.[24] Some risk to data is due to ignorance, compliancy,[25] or neglect on the part of the personnel. For example, many personal computers sit on desks in office environments that have water sprinkler systems. In the event of an accidental release of water in many office environments thousands of dollars worth of needless damage would result to personal computers and data disks because of the lack of awareness of the personnel to take protective action to minimize water damage. Even employees who were aware of the need to take protective action may be thwarted by the absence of preparations of the organization if the organization has not provided ready access to plastic covers. Most personal computers have cooling fans which draw air in and circulate it over various parts of the computer's CPU[26] and power supply to cool them. When people smoke or use hair spray[27] anywhere near a personal computer, the air containing the smoke or hair spray

can be pulled into the personal computer's CPU where damage may be done. Hair spray which falls onto the magnetic surface of a floppy disk[28] can destroy the disk and the data on the disk when the disk is inserted into the computer.

Managers who supervise personnel who use personal computers need to be educated regarding the various environmental risks and inturn educate their employees. Some threats to data security are the results of common behaviors which are normally harmless but which need to be modified in a computer environment. For example, magnets which may be used to hold notes to metal desks can destroy data on floppy disk drives.[29] A strong permanent magnet that is within some six to eight inches of a floppy disk can cause irreparable loss of data. Employees who transport data on floppy disks can destroy the data if the disk is left on an automobile's dashboard[30] or in the glove box[31] where the temperature may exceed 150 degrees. Coffee or drinks spilled on a computer keyboard[32], a personal computer, or floppy disks can cause hundreds, perhaps thousands of dollars worth of damage. Such problems as those described above are best dealt with by the individual company rather than by legislation or law enforcement. In correcting such behaviors, managers must remember human psychology. Because these are common behaviors, it is frequently necessary for the manager to actively shape the behavior of his or her employees until the desired level of compliance with the rules prohibiting such behaviors is achieved.

Proper Names

1. Information Service Departments 信息服务部

2. the Quality Assurance Institute, Orland, Florida 佛罗里达州奥兰多市质量保险所

3. Alcoholics Anonymous 酒精中毒救济会(成立于 1934 年),美国

Notes

1. The seriouseness and pervasiveness of computer crime is well documented. 有关计算机犯罪的严重性及普遍性的记载极多。

2. Law enforcement officers 执法人员

3. policing of,这里 police 为动词,意为侦破,等同于 track down and clear up a case

4. the battle of "Man against machine" or the "large corporation""人机"大战或"与大公司"之战

5. The data gathered by…in the United States.

笔者对目前工业实践,诉讼动向和律师杂志论著等的研究所获得的资料,以及在与(计算机)保安部门负责人员的会谈中所获的信息表明,大有必要对国内外私人计算机,资料及其网络系统的保护法规和规定计算机犯罪的立法进行一番评估。

6. sensitive data 高度机密资料

7. proprietary data 专有资料

8. property laws 产权法

9. as opposed to tangible assets 与有形资产相对的(指无形资产)

10. mainframe computer 电脑主机

11. Access restriction 接触使用限制规定

12. file cabinets or vaults or"computer rooms"档案室、库或"计算机房"

13. networking ability 联网能力

14. data bases 数据库

15. unauthorized access 未经准许接触使用

16. Data security was inherent in…资料的防护有赖于……

17. one midwest county jail 美国中西部一县监狱

18. inmate 罪犯

19. booking computer 注册登记电脑

20. explicit charge 明确指示

21. Proactive policies and procedures 积极措施和办法

22. Reactive policies and procedures 消极措施和办法

23. Just the presence of procedures…to some people 正是有了认证和指控罪犯的办法,才使得一些人受到摄威。

24. This is because it is humans in the environment…for data security. 这是因为人们总难免在环境中制造一些不利于资料安全的参数.

25. Compliancy=without compliancy with the rules

26. CPU:Central Processing Unit 中央处理机

27. hair spray 发胶

28. floppy disk 软盘

29. floppy disk drives 软磁盘驱动器

30. automobile's dashboard 汽车仪表板

31. glove box=glove compartment 汽车仪表板上的小贮藏

柜

32. keyboard 键盘

Exercises

I. Reading comprehension:

Read the following passages carefully and choose the best answer to each of the questions.

(1)

A frequent and potentially costly risk is associated with actions which have criminal intent. It is diffincult to measure with precision the losses due to some reasons but a survey of 1,000 organizations reported that "the verifiable losses attributed to computer crime in 1985 were estimated between $145 million to $750 million". The rate of increase of computer crime is rising significantly. One measure of this is the 1986 survey sponsored by the National Instiute of Justice. It reported that 75 percent of the police chiefs surveyed and 63 percent of the sheriffs said computer crime investigations were likely to have a significant impact on their workloads in the future. In jurisdictions having populations of 500,000 or more, the proportion was even higher, 84 percent of police chiefs and 75 percent of sheriffs.

The profile of the computer criminal revealed in a study indicated that while offenders ranged in age from 20 to 50, the median age was thirty. Seventy-five percent had some college and had been employed for an average of five years with the comany before committing their crimes.

Questions:

1. Actions which have criminal intent _____.

a. often damage costly computers

b. may frequently result in heavy losses.

c. may often cause lots of dangers to people.

d. will risk people's fortune and health frequently

2. "The verifiable losses" are _____.

a. those that can verify because of computer crime

b. what can be verified by computers

c. losses that can be proved to be true or accurate

d. evidences or proofs that show the losses

3. Computer crime in the U. S. A. _____.

a. is increasing greatly

b. has a significant impact on the police's workloads

c. was surveyed by police chiefs and sheriffs in 1986

d. is decreasing in a considerable way

4. Which of the following is not true?

a. Most of the computer criminals are well-educated

b. People are easy to commit computer crime in the age of their twenties.

c. Most offenders used to be company employees.

d. Most of the police officers believe that computer crime is rising significantly.

5. The psssage implies _____.

a. the police chiefs and sheriffs will work hard in the future

b. computer crime is of sophistication

c. where the population is large, there is higher proportion of offenders

试读结束：需要全本请在线购买： www.ertongboo