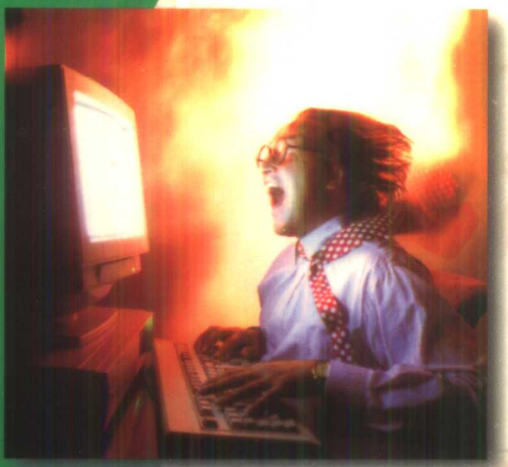
法律英语读物

English Readings in Legal Studies

计算机犯罪及其法律防范

Computer Crime and Legal Prevention

〔澳〕张立中/编



出版社

PUBLISHING HOUSE OF LAW

Computer Crime and Legal Prevention

[澳] 张立中/编著

法律出版社
PUBLISHING HOUSE OF LAW

图书在版编目(CIP)数据

计算机犯罪及其法律防范：英文注释本 /(澳大利亚)张立中编著. -北京：法律出版社，1999.1
(法律英语读物)
ISBN 7-5036-1900-7

Ⅰ. 计… Ⅱ. 张… Ⅲ. 计算机犯罪-对策-英语-语言读物 Ⅳ. H319.4:D

中国版本图书馆 CIP 数据核字(1999)第 00406 号

出版·发行/法律出版社
经销/新华书店
印刷/外文印刷厂印刷
开本/787×1092 毫米 1/32 **印张**/5.75 **字数**/152 千

版本/1999 年 1 月第 1 版 1999 年 1 月第 1 次印刷
印数/0,001—5,000

社址/北京市广外六里桥北里甲 1 号八一厂干休所内(100073)
电话/63266794 63266796

书号：ISBN7-5036-1900-7/D·1486
定价：12.00 元
(如有缺页或倒装，本社负责退换)

出版者的话

1755年，在英语——作为一种文字的发展史上，是具有里程碑意义的。这一年，英国的第一部《英语大辞典》问世。她的作者便是英国著名的作家和词典编纂学家撒缪尔·约翰逊（Samuel Johnson）。他在这部大辞典的序言里写下了这样一句话：The great pest of speech is frequency of translation. … this is the most mischievous and comprehensive innovation（语言最大的祸害就是频繁的翻译，这是一种最有害且最综合意义上的"再炮制"。）

"炮制"常常会差强人意，甚至于以讹传讹，而法学译作更在一定意义上是件"不可为而为之"的作品。英美法的一些概念、术语实难在汉语中有完美的匹配。于是我们推崇读原文。

原文闪烁着作品本身质朴而灵动的光芒，而地道的语言传送着的是英语中"法言法语"独特的个性化色彩。

少有机会读到英美法学原篇的中国学子们，将会从这套丛书中看到真正的英文法学篇章是个什么样子。这里既有严谨、典型的英美法学学术篇章，也有法庭上唇枪舌剑的审判实录，更有闻名于世的英美法"案例学习"。

这套辑录自90年代以来的"原法原味"的法学英语读物，我们相信她带给您的会是这样的阅读体验——语言一百分，思想不打折。

1998年12月

导　言

电子计算机是20世纪发展最快、对人类社会影响最大的科学技术。自从1946年世界上第一台通用电子计算机在美国宾夕法尼亚大学问世，仅仅经过半个世纪的发展，电子计算机技术已经渗透到人类社会的各个领域，在现代化建设中充当主力军角色，使生产自动化和全球网络化成为现实。

在强有力地促动着社会进步的同时，电子计算机技术也给人类生活带来了新型的社会问题。一些不法之徒利用计算机技术从事形形色色的犯罪活动，经济诈骗，文件伪造，情报盗用，数据破坏，网络侵入，软件盗版等等，不一而足。近10年来，伴随着计算机系统网络化和智能化程度迅速提高，以及金融业的高度发达，白领犯罪屡见不鲜。他们运用高科技即所谓非传统的手段从事传统的犯罪活动，挟巨额资金高效率地贩卖毒品，聚众赌博，兜售色情，拐骗资金和洗钱，从而牟取暴利，几乎把社会上流行的所有犯罪活动都发展到网络世界，使犯罪后果更快地蔓延，因而更具威胁性，构成了计算机犯罪的高度隐蔽性、高智能化、案值巨大和跨国犯罪频发的特点。

另一方面，计算机系统和网络的安全性已经成为当今社会最为关注的问题之一。现代化工作和生活的各个方面都依赖于计算机系统，从航空、铁路、公路等交通系统，到医疗服务、国家安全防卫等专项设施，到处都用到计算机技术。这些计算机系统一旦发生故障，就会给社会生活乃至人身安全带来威胁和危险。由于大型计算机网络跨国度发展，许多计算机信息网络，如现已流行的因特网，都与发达的通讯业融为一体，这样就大大增强了计算机系统的脆弱性，同时也就增加了不法分子滥用计算机或攻击计算机系统本身的犯罪机会。这类新型犯罪活动不但会严重扰乱社会秩序，也会直接造成不可估量的经济损失。

因此，通过法律手段来防范和制裁计算机犯罪成为世界各国所面临的一项迫切而艰巨的任务。早在70年代，一些发达国家就开始了有关计算机犯罪的立法工作。对于计算机侵害行为，起初主要以非刑事的"滥用"和"电信欺诈"等方式惩处，其制裁办法主要是经济和行政的性质。面对计算机犯罪发案率的逐年提高，将计算机犯罪纳入刑法调整范围的呼声日盛。第一部计算机犯罪法于1978年由美国佛罗里达州通过。目前，世界上大多数国家都相继制定了有关计算机犯罪的刑事、民事和行政法律法规，计算机犯罪学已发展成为高等政法院校的专业课程。

值得强调的是，由于当代计算机技术的发展日新月异，计算机犯罪的新现象和新形式层出不穷，总是使相对稳定和滞后的立法工作防不胜防，审判体系往往也难以适应这种发展的需要。例如，计算机犯罪的国际化现象就需要世界各国政府不断商讨和协调，采取统一的法律防范和制裁措施。对于这类问题，联合国组织了关于犯罪防范和罪犯待遇的专题会议，每5年召开一届。在近10年来联合国召开的三届会议中(1985年第7届，1990年第8届，1995年第9届)，计算机犯罪都列入了主要议事日程。会上，联合国成员国通过了一系列决议，对防范计算机犯罪的国际协作制定了有关方案和措施。根据这些方案和措施，联合国还组织编写了《联合国关于计算机犯罪防范和控制手册》，于1994年正式出版。

为使中国读者尽快了解计算机犯罪的国际研究成果，提高法律英语水平，本书内容节选了《联合国关于计算机犯罪防范和控制手册》和联合国有关决议、文件，以及国际上关于因特网上犯罪、黑客与计算机犯罪、计算机伦理学与计算机犯罪立法等最新资料。笔者在本书的编写和注释过程中参考了大量文献专著，在此一并致谢。

张立中

1999年1月于澳大利亚 La Trobe 大学

责任编辑/郭晋平
装帧设计/聂靖和

法律英语读物从书

1. 《O·J·辛普森案诉讼文书选》许卫原/编
   The Court Records of O.J.Simpson Trial
2. 《关贸总协定与世界贸易组织》王毅/编
   GATT & WTO—Law and Rules for Wor ld Trade
3. 《贸易与环境》高凤 毛毛/编
   Trade and the Environment
4. 《英美律师业介绍》冯秀梅/编
   An introduction to the Legal Profession of England and the United States
5. 《英国公司法经典案例》张明澍/编
   Leading Cases in English Company Law
6. 《欧美刑事司法制度》何家弘/编
   Criminal Justice Systems in Europe and North America
7. 《欧美民事诉讼程序》王景琦/编
   Civil Procedure in Europe and North America
8. 《国际司法协助》皓明/编
   International Legal Assistance
9. 《美国监狱和矫治》陈忠诚/编著
   U. S. Prisons and Corrections
10. 《西方银行法》陈庆柏/编
    Western Banking Law
11. 《计算机犯罪及其法律防范》〔澳〕张立中/编
    Computer Crime and Legal Prevention

ISBN 7-5036-1900-7

9 787503 619007 >

ISBN7-5036-1900-7/D·1
定价：12.00元

目　录

1. Definition of Computer Crime
计算机犯罪的定义

It is difficult to determine when the first crime involving a computer actually occurred. The computer has been around in some form since the abacus[1], which is known to have existed in 3500 B.C. in China, Japan and India. In 1801 profit motives encouraged Joseph Jacquard, a textile manufacturer in France[2], to design the forerunner of the computer card[3]. This device allowed the repetition of a series of steps in the weaving of special fabrics[4]. So concerned were Jacquard's employees with the threat to their traditional employment and livelihood that acts of sabotage[5] were committed to discourage Mr. Jacquard from further use of the new technology. A computer crime had been committed.

There has been a great deal of debate among experts on just what constitutes a computer crime or a computer-related crime[6]. Even after several years, there is no internationally recognized definition of those terms. Indeed, throughout this article the terms computer crime and computer-related crime will be used interchangeably[7]. There is no doubt among the authors and experts who have attempted to arrive at definitions of computer crime that the phenomenon[8] exists. However, the definitions that have been produced tend to relate to the study for which they were written[9]. The intent of authors to be precise about the scope and use of particular definitions means, however, that using these definitions out of their intended context often creates inaccura-

cies. A global definition of computer crime[10] has not been achieved; rather, functional definitions[11] have been the norm.

Computer crime can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief[12], all of which are generally subject everywhere to criminal sanctions[13]. The computer has also created a host of potentially new misuses or abuses that may, or should, be criminal as well.

In 1989, expanding on work that had been undertaken by OECD[14], the European Committee on Crime Problems of the Council of Europe produced a set of guidelines for national legislators[15] that enumerated activities that should be subject to criminal sanction. By discussing the functional characteristics of target activities, the Committee did not attempt a formal definition of computer crime but left individual countries to adapt the functional classification to their particular legal systems and historical traditions.

The terms "computer misuse" and "computer abuse" are also used frequently, but they have significantly different implications. Criminal law[16] recognizes the concepts of unlawful or fraudulent intent and of claim of right; thus, any criminal laws that relate to computer crime would need to distinguish between accidental misuse of a computer system[17], negligent misuse of a computer system and intended, unauthorized access[18] to or misuse of a computer system, amounting to computer abuse. Annoying behavior must be distinguished from criminal behavior in law.

In relation to the issue of intent, the principle of claim of right also informs the determination of criminal behavior. For example, an employee who has received a password from an employer, without direc-

tion as to whether a particular database[19] can be accessed, is unlikely to be considered guilty of a crime if he or she accesses that database. However, the principle of claim of right would not apply to the same employee who steals a password from a colleague to access that same database, knowing his or her access is unauthorized; this employee would be behaving in a criminal manner.

A distinction must be made between what is unethical[20] and what is illegal; the legal response to the problem must be proportional to the activity that is alleged[21]. It is only when the behavior is determined to be truly criminal that criminal prohibition and prosecution should be sought. The criminal law, therefore, should be employed and implemented with restraint[22].

Throughout the evolution of criminology, its students have concentrated their efforts and studies in the areas known as "traditional crimes." These are usually associated with the more serious common law crimes[23], such as rape, burglary, larceny, and murder[24]. As a result, a legal structure has evolved that addresses essentially only these types of offenses. However, with the rise of modern technology, nontraditional crimes have increased in currency and attention[25]. The electronic revolution has given the criminal a new tool. With the aid of modern technology, an individual can steal millions of dollars. Computer crime is the product of this new era. It not only merits our study, but tests our society's ability to adapt its underlying legal philosophy to the challenges of a changing technology.

There is no widely accepted definition of computer crime. Some authorities define it as making use of the computer to steal large sums of money. Others include theft of services within this definition, as well as invasions of privacy[26]. Some take an open approach to the problem,

viewing it as the use of a computer to perpetrate any scheme to defraud others of funds, services, and property.

However, a more sophisticated and encompassing definition[27] must be developed to take into consideration the advances in the economic sector. Computers can easily be employed to create false assets, to manipulate the price of stock, to provide "insiders" with material information on a company, thus enabling them to make millions of dollars. The computer can provide a small group of terrorists with the ability to manipulate the arsenals of large armies; it can make possible a $2 billion fraud. The computer is a giant calculator that enables individuals to obtain large amounts of data at the press of a button. It also enables felons to hide their crime as though it were a "needle in the haystack." [28] By simply destroying a computer's program felons erase their tracks.

An adequate definition of computer crime should encompass the use of a computer to perpetrate acts of deceit, concealment, and guile that have as their objective the obtaining of property, money, services, and political and business advantages. Computer crime may also take the form of threats or force directed against the computer itself. These crimes are usually "sabotage" or "ransom" cases[29]. Computer crime cases have one commonality: the computer is either the tool or the target of the felon.

Notes

1. abacus: 算盘。

2. Joseph Jacquard, a textile manufacturer in France: 约瑟·雅克德，一个法国纺织厂主。

3. forerunner of the computer card: 计算机卡的先驱。

4. weaving of special fabrics: 特定织物的编织。

5. acts of sabotage: (对财产等的)故意毁坏;破坏活动。

6. computer-related crime: 与计算机有关的犯罪。

7. be used interchangeably: 相互交替地使用。

8. phenomenon: 现象。

9. the definitions that have been produced tend to relate to the study for which they were written: 为某一相关研究所下的定义。

10. a global definition of computer crime: 计算机犯罪的通用定义。

11. functional definitions: 功能性定义。

12. theft, fraud, forgery and mischief: 盗窃，欺骗，伪造和损害。

13. criminal sanctions: 刑事制裁。

14. OECD: 经济合作与发展组织,Organization for Economic Cooperation and Development 的缩写。

15. legislators: 立法者。

16. criminal law: 刑法。

17. accidental misuse of a computer system: 计算机系统的滥用。

18. unauthorized access: 非授权访问。

19. a particular database: 特定的数据库。

20. unethical: 非伦理的。

21. alleged: 被指称的,被说成的。

22. employed and implemented with restraint: 抑制性使用和实施。

23. common law crimes: 普通法犯罪。

24. rape, burglary, larceny, and murder: 强奸、夜盗、偷窃和谋杀。

25. increased in currency and attention: 在传播和关注方面有所增强。

26. invasions of privacy: 侵犯隐私权。

27. more sophisticated and encompassing definition: 更为精致和全面的定义。

28. enables felons to hide their crime as though it were a needle in the haystack: 使重罪犯能隐藏他们的犯罪，就象“在草堆里藏着一根针”一样。

29: ransom cases: 绑票案件。

2. The Extent of Computer Crime and Losses
计算机犯罪和损失的程度

Only a small portion of crimes come to the attention of the law enforcement authorities[1]. In his book Computer Security[2], J. Carroll states that "computer crime may be the subject of the biggest cover-up since Watergate". [3] While it is possible to give an accurate description of the various types of computer offences committed, it has proved difficult to give an accurate, reliable overview of the extent of losses and the actual number of criminal offences[4]. At its Colloquium on Computer Crimes and Other Crimes against Information Technology[5], held in Germany, from 5 to 8 October 1992, the Conference Organizing Committee[6] released a report on computer crime based on reports of its member countries[7] that estimated that only 5 per cent of computer crime was reported to law enforcement authorities.

The number of verifiable computer crimes is not, therefore, very high. This fact notwithstanding, authorities point out that the evidence of computer crime discernible from official statistical sources, studies and surveys indicates the phenomenon should be taken seriously.

The American Bar Association[8] conducted a survey in 1987: of 300 corporations and government agencies, 72 claimed to have been the victim[9] of computer-related crime in the 12-month period prior to the

survey, sustaining losses[10] estimated to range from $ 145 million to $ 730 million. In 1991, a survey of security incidents involving computer-related crime was conducted at 3,000 Virtual Address Extension (VAX)[11] sites in Canada, Europe and the United States of America. Seventy-two per cent of the respondents said that a security incident had occurred within the previous 12-month period; 43 per cent indicated that the security incident they had sustained had been a criminal offence. A further 8 per cent were uncertain whether they had sustained a security incident. Similar surveys conducted around the world report significant and widespread abuse and loss.

Law enforcement officials indicate from their experience that recorded computer crime statistics do not represent the actual number of offences; the term "dark figure"[12], used by criminologists to refer to unreported crime, has been applied to undiscovered computer crimes. The invisibility of computer crimes is based on several factors. First, sophisticated technology[13], that is, the immense, compact storage capacity of the computer and the speed with which computers function, ensures that computer crime is very difficult to detect. In contrast to most traditional areas of crime, unknowing victims are often informed after the fact by law enforcement officials that they have sustained a computer crime. Secondly, investigating officials often do not have sufficient training to deal with problems in the complex environment of data processing. Thirdly, many victims do not have a contingency plan[14] for responding to incidents of computer crime, and they may even fail to acknowledge that a security problem exists.

An additional cause of the dark figure is the reluctance of victims to report computer offences once they have been discovered. In the business sector, this reluctance is related to two concerns. Some victims may be unwilling to divulge information about their operations for fear