中国图书馆学报(双月刊)2000 年第 6 期
ZHONGGUO TUSHUGUANXUEBAO

●娄策群 范 昊 王 菲

现代信息技术环境中的信息安全问题及其对策

摘 要 现代信息技术的发展及应用使信息安全问题比以前更突出。信息安全所面临的问题包括信息污染、信息泄密、信息破坏、信息侵权、信息侵略等。保障信息安全的措施主要包括政策措施、行政管理措施、法律措施、技术措施和伦理措施。参考文献 5。

关键词 现代信息技术 信息安全 保障措施
分类号 G351.1

ABSTRACT The development of modern information technology causes some new problems of information security, including information pollution, information divulgement, information damage, information infringement, information invasion, etc. To solve these problems. there are such solutions as policy, administration, law, technology and echics. 5 refs.

KEY WORDS Modern information technology. Information security. Solution.
CLASS NUMBER G351.1

现代信息技术的应用,特别是计算机信息网络的建立与运行,虽然给信息资源的开发和利用带来了诸多方便和益处,但也使信息安全问题变得十分突出。我们必须充分认识现代信息技术,尤其是信息网络的发展对信息安全的影响,采取相应对策,合理使用信息网络,充分而有效开发和利用网络信息资源。

1 现代信息技术环境中信息安全所面临的问题

当今社会,信息安全的概念和范围不断扩大,包括信息本身、信息系统、信息网络的安全等。信息安全问题直接影响到国家政治、经济、科技、文化及其安全的程度与状况。归纳起来,现代信息技术环境中信息安全所面临的问题主要有 5 个方面。

1.1 信息污染

信息污染是指无用信息、劣质信息或有害信息渗透到信息资源中,对信息资源的收集、开发和利用造成干扰,甚至对用户和国家产生危害。现代信息技术环境中的信息污染主要表现为:

(1) 无用信息。无用信息对绝大多数用户没有任何实用价值,它除了影响信息资源开发利用的速度和效率外,一般对信息用户不会产生其他不良作用或对用户的负面影响较小。无用信息主要包括重复信息、过时信息和某些个人的自由言论等。现代信息技术的应用加快了信息的生产速度,信息网络的建立与运行使信息容易传递和获取,因此,近年来信息量急剧增长,信息的老化速度也加快,一些信息在产生后不久便过时,失去了使用价值。因此,现代信息技术环境中的过时信息量大,影响了有用信息的传递与加工速度,增加了用户获取和利用信息的难度。在以印刷型文献信息为主的时代,重复信息主要是由于大量的转抄、引用、剽窃、同一题材的图书多个出版社出版、一稿多投和一稿多发而造成的;而在现代信息技术环境中,重复信息除了上述原因外,还在于网络信息用户在网上对同一问题发表差别不大的意见、不同的数据库开发商开发和经营收录范围雷同的数据库等。现代出版技术和电子出版技术的发展使文献信息的出版变得十分便捷,一些价值不大甚至是内容毫无新意的文献能够出版发行。在信息网络中,信息提供者成分复杂,所有的上网者都可以在因特网上自由发表言论和发布信息,其中很多信息价值不大。

(2) 劣质信息。劣质信息是指具有一定的使用价值但作用不大,且质量较低的信息。劣质信息虽然也能利用,甚至带来效益,但会给信息资源的开发利用增加难度,传播与利用不当时还可能给用户造成一定的损失。劣质信息包括内容不完整不准确、文字错误较多的信息。劣质信息有的是信息生产者在收集和处理信息的过程中产生的,有的是在信息的传播过程中产生的。在信息生产过程中,收集的信息和数据不全、信息处理与研究的方法不够科学、转引别人文献中的观点和数据、校对不严等,都会导致劣质信息的出现。在信息传播过程中,由于信息传播技术出错或信息处理失当会导致信息一定程度的失真,产生劣质信息。

(3) 有害信息。有害信息是指利用后会给用户和社会带来不良影响的信息。有害信息的出现和增加不仅会增加信息处理工作量,增加信息筛选、甄别的难度,更大的危害是影

响个人的学习、生活和工作,影响社会政治、经济、科技、文化和教育事业的正常运行和发展,甚至造成极大的经济损失,导致社会不安定。有害信息包括虚假信息、色情信息、诽谤煽动信息等。造成虚假信息的原因主要有二:一是信息生产过程中,信息生产者由于知识水平的限制不能正确地认识客观世界,或出于政治、军事、经济目的有意识地歪曲客观事实,产生虚假信息;二是信息传递与加工处理过程中,由于信息人员水平的限制、粗心大意或别有用心会导致虚假信息出现。信息网络传播信息声像俱备、图文并茂的特点使其成为一些不法分子传播色情、淫秽信息的工具和场所。据美国卡内基大学对网上 917410 条信息、图片及影片的调查,其中 83.5 %的内容与色情有关。英国伦敦一所大学的哈罗德教授发现,因特网上非学术信息中 47 %与色情有关[1]。美国一个专家小组新近的一项调查表明,在美国多数家庭电脑连通的网络中,有 92 万件带有不同程度色情内容的图片、文章和电影,电子公告栏储存的数据图像有 4/5 含有淫秽内容[2]。互联网中大量的色情信息以游戏的方式直接呈现在屏幕上,其诱惑性、渗透性极强,对精神文明建设极为不利。诽谤煽动信息也为数不少。一些不法分子和别有用心的人利用信息网络来传播恶意中伤他人、贬低同行或同类产品、挑动民族对立情绪和种族歧视、蛊惑煽动策反、传授犯罪伎俩等信息。

1.2　信息泄密

信息泄密是指通过不合理或非法手段,窃取个人的隐私信息、企业的商业秘密、政府部门和军队的机密、计算机文件和软件等。网络信息泄密是网络中的信息在存储、传播、使用或获取的时候被其他人非法取得的过程。网络信息泄密的途径有很多。搭线窃听、电磁辐射引起的信息失密、密钥失密以及非法访问网络资源等都会使网络信息泄密。

个人稳私信息是指个人信息中不想让他人知道的信息,如个人的生理与心理特征、年龄、婚姻、病历、收入状况、银行存款、保险、宗教信仰、犯罪前科等方面的信息。随着社会信息化程度的提高,利用计算机网络对个人信息进行处理和存储已越来越普遍,有些不法之徒可能会利用种种手段进入个人信息文档,刺探、窃取或篡改他人隐私,某些机关、网点也可能滥用职权,非法扩大个人信息的收集与存储范围,监督公民的隐私,限制公民的自由权利。美国参议院的一项研究报告表明,美国联邦政府数据库中有 17 %的信息完全属于非法,84 %未经法令授权。

企业的商业秘密是指企业所具有不允许为外人和竞争者知晓的信息,如技术数据、工艺流程、作业蓝图、操作技巧、原材料供应商名单、客户名单、营销策略、交易金额、管理诀窍、财务信息等。出于市场竞争的目的,一些厂商和个人千方百计地闯入互联网,盗用商业秘密,损人利己。日本某杂志社发行代理公司将耗资 5 亿日元收集到的订户名单等商业绝密信息委托给太平洋计算机信息中心处理,在转手处理过程中,存储有这些信息的磁带被人转录,并以 82 万日元出手获利。《美国研究》杂志社的一项调查结果表明,窃贼攻击美国工作场所的计算机的事例次数 1989 年为 339000 起,1990 年为 423000 起,1991 年为 684000 起,攻击事件逐年上升[3]。

政府部门和军事机关的机密信息也有可能在网上被盗。一些犯罪分子通过信息网络出卖国家机密。据美国国防部统计,外人闯进国防部极端重要的计算机系统的次数不断上升。

1.3　信息破坏

信息破坏主要是指制造和传播恶意程序,破坏计算机内所存储的信息和程序,甚至破坏计算机硬件。对网络信息安全威胁较大的恶意程序主要有:(1) 计算机病毒,即一种会“传染”其他程序的程序,“传染”是通过修改其他程序而将其自身或其变种复制进去。(2) 计算机“蠕虫”,即一种通过网络的通信功能将自身从一个结点发送到另一个结点并启动的程序。(3)“特洛伊木马”,即一种执行超出程序定义之外的程序。如一个编译程序除了执行编译任务,还把用户的源程序偷偷拷贝下来,这就是一种特洛伊木马。(4)“逻辑炸弹”,即一种当运行环境满足某种特定条件时执行其他特殊功能的程序。(5)“邮件炸弹”,即网络中转站匿名发送一组由大量无用的电子邮件、威胁性言论和其他无用信息,以阻塞对方的计算机系统。

据不完全统计,美国在 1998 年里,约有 9 万台计算机被病毒感染。国外有人估计,现在计算机病毒的传染每两个月增加 1 倍。1988 年 11 月 2 日,一种病毒通过网络袭击了全美国互联网络,不到两天便有 6000 多台联网计算机被感染,6000 多台计算机关机,整个网络瘫痪 24 小时,直接经济损失达 9600 万美元[4]。自 1989 年我国发现首例计算机病毒起,目前拥有计算机的单位中,大约 80 %被病毒侵害过;科研机构及高等院校等单位,计算机病毒感染率达 100 %。

1.4　信息侵权

信息侵权是指对信息产权的侵犯。传统的信息产权主要是指知识产权,包括版权、专利权和商标权。知识产权涉及大量的科技信息、文化信息、经贸信息。现代信息技术,尤其是信息网络的发展和应用,导致了信息内容的扩展、信息载体的变化、信息传递方式的增加,它能实现信息的全球共享,也带来了传统知识产权难以解决的新问题。现代信息技术环境中,信息侵权具有以下特征:更容易发生,信息产权保护的范围更大;侵权手段隐蔽,不易查获;很多行为是否构成侵权难以区分;一些信息产品没有相应的知识产权法规加以保护。

现代信息技术环境中,还会出现计算机软件侵权、数据库产品侵权、网上信息侵权等。软件侵权主要是指为了销售目的而非法复制软件并对其重新包装的过程。计算机软件极容易复制,且复制费用很低,一般设计制作一个电脑游戏

的成本约为 50 万美元,而盗版电脑游戏软件的售价只有 10 美元。全世界 1993 年计算机软件盗版所造成的损失约 118 亿美元,其中,软件盗版最严重的是欧洲,占全球软件盗版的 38 %;其次是亚洲,占 31 %;北美占 19 %;拉丁美洲占 7 %;其他占 5 %。近年来,企业域名被抢注的侵权行为时有发生[5]。

1.5　信息侵略

信息侵略是指发达国家利用信息优势向发展中国家输出其价值观念与政治观点,破坏发展中国家的政治独立和文化独立的行为。霸权国利用其在信息领域的主宰地位,通过互联网络上的电子邮件、电子报刊等展开宣传战、心理战,实行政策、文化和心理侵略,威胁着发展中国家的政治、文化安全。信息传播受发达国家的控制,全球信息冲突加剧,国际信息秩序将出现恶化趋势。加拿大学者基蒙·瓦拉卡提出了"文化渗透"的概念,指出信息渗透是以牺牲绝大多数国家的民族文化为代价的。美国的比尔·盖茨宣称,信息高速公路将打破国界,并可能推动一种世界文化活动、文化价值观的共享。所谓的"世界文化"在很长一段时间内只能是西方文化,尤其是以美国为中心的文化。

2　保障信息安全的行政、法律措施

保障信息安全的行政、法律措施主要包括政策措施、行政管理措施和法律。

2.1　政策措施

政策作为国家宏观指导和管理社会经济活动的手段,能为社会经济发展确定发展方向,有效调节各种关系和矛盾。制定和执行信息安全政策,是保障信息安全的关键。信息安全政策是一国家或国际组织在一定时期内为处理信息自由传播与有限利用的矛盾而制订的一系列行政规范的总和。由于政策具有宏观性、指导性等特点,科学合理的信息安全政策能够指导信息安全方面的行政管理,指导信息安全立法与司法,也能促进信息安全技术措施和伦理措施的制定与实施。

1990 年,国家科委发布的中国科学技术蓝皮书第 4 号《信息技术发展政策》中明确指出,要保证国家机密的安全和防范信息犯罪,重视现代信息保密技术的开发利用,提高信息安全工作的水平。但我国目前还尚未形成完善的信息安全政策体系。完善我国的信息安全政策体系,可从 3 个方面入手。一是在有关的信息政策中加入信息安全政策的内容,这既可作为没有形成专门的信息安全政策前的一项应急措施,即使有了专门的信息安全政策,也能扩大信息安全政策的宣传范围和传播力度。二是制定专门的国家信息安全政策,对信息资源的充分开发与共享、信息网络的建设与管理、信息污染的控制、信息产权的保护、信息主权的维护、信息犯罪的打击、秘密信息的保密等做出相应的政策规定。三是在国家信息安全政策的指导下,控制信息安全政策实施细则和各方面具体的信息安全政策。信息安全政策颁布后,应采取切实可行的办法将政策落到实处,避免上有政策下有对策的现象发生。

2.2　行政管理措施

保障信息安全的行政管理措施主要是建立统一的信息安全管理机构,采用行政手段对网络及其他信息交流活动进行管理,保证信息安全。

西方国家一般都建立有信息安全管理机构。美国安全委员会下设了国家保密政策委员会和信息系统安全保密委员会,前者负责制定军事安全保密政策,后者负责军事信息网络的秘密信息和敏感信息的安全保密。英、法等国家建立了国家信息安全委员会。德国成立了国家信息安全局。我国的信息安全管理机构有两种模式:一是应尽快建立专门的信息安全管理机构,二是在现有的安全部门下设立信息安全管理分支机构。世界各国对因特网的管理通常是区域管理,即以块为主,条块结合,各个区域内任何单位的信息安全工作均由安全部门归口管理。目前,我国采用这种信息安全管理模式是切实可行的。由于网络犯罪、信息安全管理的特殊性,成立专门的网络信息活动公证、监察、执法机关和特别法庭也是十分必要的。

在信息安全管理手段与方式上,应加强制度化管理,建立和执行网络准入制度,对网络用户的身份进行审查;完善联网登记和联网电脑管理制度,加强对入网用户和入网电脑的管理;建立网络信息标准化管理制度,对上载信息实行统一规范。此外,对损害信息安全和在信息安全管理中有较大过失者,要给予相应的行政处分。

2.3　法律措施

由于法律的严密性、强制性和相对稳定性,它是社会关系强有力的调解器。完备的信息安全法律法规是有效保障信息安全的重要措施。

迄今为止,很多国家都制定了知识产权法、保密法,已有 30 多个国家先后从不同侧面制定了计算机安全和网络信息安全的法律法规。1978 年 8 月,美国佛罗里达州通过了《佛罗里达计算机犯罪法》,随后,美国 47 个州相继颁布了计算机犯罪法。1973 年瑞典颁布了数据法,涉及到了计算机犯罪问题,后来,西欧各国基本上都颁布了数据法。1985 年 12 月,日本制定了计算机安全规范,并出版了相应的指南。我国制定了专利法、商标法、著作权法、计算机软件保护法、保密法等。1987 年 10 月,我国制定了第 1 部有关计算机安全方面的法规《电子计算机安全工作规范(试行草案)》。1994 年 2 月,国务院颁发了《中华人民共和国计算机信息系统安全保护条例》,随后出台了《中华人民共和国计算机信息网络国际联网暂时规定》。

今后,我国的信息安全立法的重点应在以下几个方面:一是进一步完善知识产权法,尤其是要研究现代信息技术对知识产权的影响,对计算机软件、电子出版物、多媒体信息、数据库的知识产权保护做出更加具体而合理的法律规定;二

是制定网络法,对网络中计算机硬件与软件的保护、网上信息的保护、用户数据的保护、利用网络传播有害信息的处罚等做出相应规定,规范人们的网络行为,保证信息网络的安全运行和网络信息的充分而合理利用;三是制定一些其他的专门法律,如计算机犯罪法、反病毒法、电子贸易法等。

3　信息安全的技术措施

计算机网络中信息的安全问题日益受到各界人士的重视。人们通过各种硬件、软件技术和安全管理手段来保证网络以及网络信息的安全。

3.1　加密与伪装技术

信息加密是增强网络信息安全的有效手段,它是利用某种加密算法,将信息明文变换成密文进行发送,使截取者无法破译,从而实现信息的安全传输。常用的加密算法有两种:对称密钥加密算法和公开密钥加密算法。加密与解密使用同一个密钥(算法),或者密钥不同,但可以由一个推导出另一个,这种加密机制我们称之为对称密钥体系。这种情况下,通信双方必须交换彼此密钥。与对称密钥相对应的是非对称密钥,即公开密钥,它要求密钥成对使用,即加密和解密分别由两个密钥(算法)实现,不能由一个推导出另一个。

目前,国际上常用的对称密钥加密算法有:DES(数据加密标准,Data Encryption Standard),IDEA(国际数据加密标准,International Data Encryption Standard),RC4 加密算法,Blowfish 算法和 SAFER 算法。常用的公开密钥加密算法有:RSA 公开密钥加密算法,DSS(数字签名标准,Digital Signature Standard),ElGamal 公开密钥加密系统以及 LUC 公开密钥加密系统。

虽然密文可以防止黑客直接获取信息内容,却"提醒"了黑客们这儿正在传输重要的信息。而且绝对可靠的密码是没有的,因为密码可以通过计算机破译。即使破译失败,恼羞成怒的黑客们也可能会将信息破坏,使得合法的接收者无法解读出。1993 年以后,国际信息安全专家们开始研究给信息铺上一层日常生活的伪装以麻痹攻击者的更有效的保护方法,即信息伪装技术,利用信息的冗余空间,隐藏文字、图片,甚至是声音和影像等信息。这将成为保证网络中信息安全性的又一重要手段。

3.2　认证技术

在网络通信过程中,信息交流双方身份的认证也是至关重要的一环。计算机网络中的认证主要包括数字签名、身份认证以及数字证明。数字签名机制提供了一种鉴别方法;身份认证机制提供了判明和确认信息交流双方真实身份的方法,可作为访问控制的基础;数字证明机制则提供对密钥进行验证的方法。

数字签名也称电子签名,是公钥加密技术的一种应用。它提供了一种鉴别方法,普遍用于银行、电子贸易等领域,以解决如下问题:(1)伪造,即信息接受者伪造一文件,声称是对方发送的;(2)抵赖,即信息发送者或者接收者事后不承认自己发送或接收过文件;(3)冒充,即网上的某个用户冒充另一个用户发送或接收文件;(4)篡改,即信息接收者对收到的文件进行局部的篡改。数字签名的算法很多,应用最广泛的有 3 种:Hash 签名、DSS 签名和 RSA 签名。

身份认证包括身份识别(Identification)和身份验证(Authentication)。前者是指用户向系统出示自己的身份证明的过程;后者则是系统核查用户的身份证明的过程,即查明用户是否具有他所请求资源的存储和使用权。身份认证必须做到准确无误地将对方辨认出来,同时还应该提供双向的认证,即相互证明自己的身份。

数字证明有时也称为"公开密钥的证明"或"数字 ID"、"数字护照"。如果甲和乙通过因特网获得各自的公开密钥,他们需要对这些密钥进行认证。甲不能简单地向乙询问其公开密钥,因为在网络上可能存在第三者截获甲的请求,并发送给它自己的公开密钥,这样,第三者就可以阅读甲传给乙的所有信息。因此,就需要一个第三方的认证机构(CA),使甲即使通过不安全的渠道,也能够借助它可靠地获取乙的公开密钥。CA 将为乙的公开密钥生成一个证书(也称为数字签名),任何人都可以获取乙的公开密钥,并利用该证书作为验证公开密钥的根据。

3.3　防病毒技术

通常的防病毒技术可以分为 3 种:病毒预防技术、病毒检测技术和病毒清除技术。对于单一主机,它们可以有效地防止病毒的入侵。而网络中最主要的软硬件实体是网络操作系统、服务器和工作站。因而网络防病毒技术一般要从这 3 个方面入手。

(1)基于工作站的防病毒技术。工作站是网络的门,把好这道关非常重要。其主要方法有杀病毒软件和防病毒软件等。

(2)基于服务器的防病毒技术。目前,大都是以加载模块 NLM(Netware Loadable Module)进行程序设计,提供扫描病毒的能力。一般的 NLM 都具有实时在线扫描、服务器扫描选择、自动报告功能及病毒档案、工作端扫描以及对用户开放的病毒特征接口等功能,提高网络系统的防病毒能力。

(3)基于网络操作系统的方法。网络操作系统本身提供了四级安全保护措施:一是注册安全,由网络管理员通过用户名、入网口令来实现;二是权限安全检查,通过受托指定和访问权限制定来实现;三是属性安全检查,通过对各目录和文件的属性进行规定来实现;四是文件服务器安全,通过封锁控制台键盘等方法来实现。

3.4　防火墙技术

防火墙利用 1 个或 1 组网络技术设备(计算机、路由器、计算机子网等),在内部网和外部网之间构造保护层障碍,检测所有的内外连接,限制外部网络对内部网络的非法访问或内部网络对外部网络的非法访问,并保障系统本身不受信息

穿越的影响。它是通过在网络边界上设立的相应网络监控系统来实现其保护功能的。防火墙的安全措施有:

(1)报文过滤网关。这是最简单的防火墙,它对通过的数据包过滤,筛除不符合要求的数据包。具体做法是:检查所传输的数据包的源、目的 IP 地址和 TCP/IP 端口号等参数,并与用户预置的访问控制表进行比较,从而将符合条件的数据包转发到相应的目的地址端口,其余的数据包则被阻塞,从数据流中删除。报文过滤技术实现比较简单,效率较高。但这一功能在网络层实现,它对于更高层的信息无理解能力,因此,对来自更高层的安全威胁无防范能力。

(2)应用层网关。应用层网关通常由 1 台专用计算机来实现。它针对特别的网络应用服务协议指定数据过滤逻辑,并依据该逻辑以出入内部网络的数据包进行过滤。应用层网关技术可以对数据包的分析结果和采取的措施进行登记,供统计分析使用。其过滤机制需要为每个网络应用提供专用的控制码,因此效率较低,但更为安全。

(3)代理服务。报文过滤网关和应用层网关技术存在一个共同的缺点:当通过防火墙的数据流满足过滤条件时,防火墙内外的计算机系统将直接建立起连接,这时外部用户可以通过防火墙了解内部网络状况,从而威胁内部网络安全。代理服务技术就是针对这一问题而引入的防火墙技术。代理服务器单方面代替原来的客户程序与服务器建立连接,其功能类似一个数据转发器。其优点是把内外计算机系统隔开来,对外屏蔽起保护网络内部对构的作用,从而加强了网络安全性。目前常用的代理服务器软件有 Netscape 和 Microsoft 公司的 Proxy Server 等。

4　信息安全的伦理措施

现代信息技术环境中的信息安全只靠政策法规和技术是难以完全保证的,还必须从网络伦理入手采取相应的措施。简单地说,网络伦理就是人们通过电子信息网络进行社会交往时表现出来的道德关系。信息网络建设与使用中的社会道德问题日益引起各界人士的注意。

4.1　加强网络主体的道德修养

网络主体是指建设、管理与使用信息网络的个人和组织,包括不同层次、不同类型的网络用户、站点、网络产品制造商、政府机构和国际组织等。网络主体的道德品质、道德自觉性如何,是关系到网络社会整体道德水平、道德秩序状况的重要因素。网络道德建设的首要任务是加强网络主体的道德修养。

加强网络主体的道德修养应做到:(1)建立正确的网络主体道德意识。网络主体应充分认识到网络是人们生存和生活的基础,网络道德是人们正常生活必不可少的人际关系调节器。维护基本的道德秩序、禁止网络不道德行为符合人们的共同利益和需要。(2)网络主体要有严于律己、宽以待人、相互理解、相互支持的态度,尊敬网友,与人为善,履行网络义务,讲究网络礼仪。(3)要处理好小节与大节的关系。不能有"只要不破坏网络系统或他人文件、不偷窃欺诈,做做黑客无所谓"的思想。长期不拘小节会减弱自己的道德意识,养成某些不道德的恶习。(4)对不道德的网民要用合理合法的手段予以教育和制止,而不能以不道德的手段予以报复。

4.2　制定和恪守网络道德规范

网络道德规范就是网络主体和利用网络和网络信息时应遵循的道德标准。网络道德规范既可以制约人们利用网络传播、获取和利用信息的行为过程和方向,又可以为人们利用网络传播、获取和利用信息的行为进行判断和评价提供标准。

国外一些计算机和网络组织制定了一系列的规范,这些规范涉及到网络行为的方方面面。如美国计算机伦理协会规定了计算机用户在网络系统中应遵守的 10 条行为准则:(1)不应利用计算机去伤害他人;(2)不应干扰别人的计算机工作;(3)不应窥探别人的文件;(4)不应用计算机进行偷窃;(5)不应用计算机作伪证;(6)不应使用或拷贝你没有付钱的软件;(7)不应未经许可而使用别人的计算机资源;(8)不应盗用别人的智力成果;(9)应该考虑你所编程序的社会后果;(10)应该以深思熟虑和慎重的方式来使用计算机。美国南加州大学规定了 6 种不应该的网络行为:(1)不应该有意造成交通混乱或擅自闯入与网络相连的其他系统;(2)不应该将大学信息资源用于商业目的或带有欺骗性;(3)不应该在网上偷窃资料、设备或其他智力成果;(4)不应该未经许可查询他人文件;(5)不应该在公共场所做出引起混乱或造成破坏的行动;(6)不应该伪造电子邮件。

然而,迄今为止还没有形成一种全球性的网络道德规范。我们可以从现有不同的规范中抽取相同的、普遍的规定,上升为全球普遍适用的网络道德规范。在我国,也应结合国情制定网络道德规范,并在实践中努力遵守。

参考文献

1　郑朝晖. 网络信息安全的政策调控. 图书馆论坛,1998(3):29～31,28

2～5　严耕等. 网络伦理. 北京:北京出版社,1998:63,81～82,86～89,90～91

注　本文为国家社会科学基金资助项目"现代信息技术对信息服务业的影响与对策研究"论文之一。

娄策群　华中师范大学信息管理系教授、博士、系副主任。通讯地址:湖北省武汉市珞瑜路 100 号。邮政编码 430079。

范　昊　华中师范大学信息管理系教师。通讯地址同上。

王　菲　华中师范大学信息管理系硕士研究生。通讯地址同上。

(来稿时间:2000-01-25)