

# 试论电子数据的刑事证据立法问题<sup>①</sup>

林安民

(闽江学院 法律系,福建 福州 350108)

**摘要:** 电子数据作为刑事证据存在着立法的不完善甚至缺失,已经成为打击网络犯罪的一大问题。为此,各国纷纷加强立法对策,通过国际公约对数据、电子记录等电子证据作了界定,并规定了收集、保全电子证据的方法与手段。我国并没有针对网络犯罪的专门证据立法,使得理论与实务界对电子数据的刑事证据无法统一认定,因此,有必要借鉴外国的相关立法及国际公约,建立我国的电子证据法规。

**关键词:** 网络犯罪;电子数据;刑事证据;立法

中图分类号:D915.13

文献标识码:A

文章编号:1674-117X(2011)01-0030-04

## Analysis of Electronic Data for Criminal Evidence Legislation

LIN Anmin

(School of Law, Minjiang University, Fuzhou, 350108)

**Abstract:** Electronic data as criminal evidence was not provided in detail in the laws, which have become a problem to strike cyber crime. In view of the definition of data and electronic records of international convention, more and more countries paid attention on the legislation, as well as collected and stored electronic methods and ways. However, we did not legislate the evidence law to deal the cyber crime. Therefore, it is necessary to establish our country's electronic evidence laws and learn from foreign country's relevant legislation and international conventions.

**Key words:** cyber crime; electronic data; criminal evidence; legislation

近年来随着网络技术的发达,网络犯罪可实施的范围也越来越广泛。据相关资料显示,近年来我国通过计算机违法犯罪案件呈迅猛上升的趋势,全国公安机关在1998年立案侦查各类计算机信息网络违法犯罪的案件只有100多起,而到了2000年就达到2700余起,到了2002年则高达6633起了。<sup>[1]</sup>而2008年,公安机关单单是侦办的网络盗窃案件就高达3600多件。<sup>[2]</sup>而国外网络犯罪的发展也是急剧膨胀,据报道,美国的硅谷,网络犯罪以每年400%的速度急剧增长;英国的计算机犯罪,每年也以213%的速度增长。

通过网络实施的犯罪,主要通过电子数据的方

式存留于计算机系统或网络服务器中。这些以其储存的文字、数据、图像、声音、程序等电子化信息资料来证明案件真实情况的电子物品或电子纪录,就是我们所说的电子证据。但是由于电子证据的形式与传统证据差异较大,因此无论是对于电子证据的法律属性还是收集、保全手段以及证据规则等方面,都与传统证据有所差异,现行的法律难以完全适应电子证据呈现出的新问题。因此网络犯罪案件的破案率普遍较低。据称,即使在美国等发达国家,网络犯罪的破案率也不足10%,而定案率则不到3%。

因此,当前打击网络犯罪突出的一个问题是

<sup>①</sup> 收稿日期:2010-08-25

作者简介:林安民(1977-),男,福建连江人,闽江学院副教授,法学博士,主要从事刑法研究。

对刑事电子证据尚没有明确的规定。虽然国外已经开始立法,并且发达国家也迫切希望通过国际公约来预防与打击网络犯罪,但总体上看,立法还有待进一步完善,而我国的刑事电子证据存在更多问题。

### 一 国际社会针对网络犯罪的电子证据立法

随着网络犯罪的普遍化与严重化,各国纷纷加强立法以应对网络犯罪的兴起。美国作为网络的发源地以及网络最为发达国家,最先通过积极的立法预防和打击网络犯罪《网上禁赌法令》《儿童在线保护法》《通讯端正法》《计算机安全法》等法案,对预防网络犯罪起了积极作用;而佛罗里达州1976年通过的《计算机犯罪法》更是世界上第一部专门针对网络犯罪的法律,对预防和打击网络犯罪起了示范作用。其他发达国家也相继通过一些法律来惩治网络犯罪,如英国2000年通过了《调查权力规制法》,日本2002年颁布了《禁止非法侵入计算机系统法律》,我国在2000年12月也通过了《全国人大常委会关于维护互联网安全的决定》。由此,各国在国内法中都构建起了反网络犯罪的法律。

虽然网络犯罪在犯罪构成要件方面与传统犯罪一样,可以通过一般的实体法予以追究;但由于其犯罪手段的特殊性,也使法律难以在证据上予以证明其犯罪的客观事实,因此迫切需要通过专门的法律予以规制。针对网络犯罪主要通过互联网实施,其主要证据通常以电子数据方式保留,因此各国纷纷开始重视对电子证据的立法。比如,加拿大在20世纪中期就开始就电子证据进行专门的立法,并且于1999年12月经加拿大国会通过了《1998年统一电子证据法》。该证据法虽然只有9个条文,但对“数据”、“电子记录”、“电子记录系统”等电子证据的概念、适用以及相关认证规则等问题作出详细规定,根据电子证据的相关特性指明其对其他证据法相关规定的协调与变更,使得电子证据法成为普通证据法的补充。<sup>[3]</sup>该电子证据法虽然不是专门针对网络犯罪,但针对电子证据的差异性作出特别规定,使之成为电子证据的专门立法。这一法律也成为世界上第一部单独为电子证据制定的专门法律。它根据电子证据的特性,以“数据”、“电子记录”和“电子记录系统”来界定证据,突破了传统最佳证据规则对“原件”的要求,通过电子记录系统的

完整性、安全性、可靠性和准确性来解决一般证据规定对传统证据的相关要求,突破了英美法系中对证据的约束性规定,<sup>[4]</sup>对打击网络犯罪起到了切实有效的作用。美国、英国等其他国家虽然没有通过专门的电子证据法,但也通过对相关法令的修正以及通过判例确认了电子证据的效力,并对其适用了特殊的证据规则。<sup>[5]</sup>

此后,一些发达国家考虑到网络犯罪的跨国性,需要各国通力合作才能有效防治网络犯罪,因此主张在立法上加强打击网络犯罪的国际合作。在此背景下,美国、日本以及欧盟等网络发达的国家率先发起,在欧盟理事会主持下,国际间展开了多年的网络犯罪公约协商。在历经20多次修改后,2001年达成了全球第一个国际性的《网络犯罪公约》,为在国际范围内打击网络犯罪扫除了法律障碍。该公约虽然是实体法与程序法合一的综合性专门法律,但其更为重要的意义在于对电子证据的统一规定。该公约不仅对“计算机系统”、“计算机数据”等网络犯罪的相关概念作出界定,而且还对与网络犯罪电子证据相关的问题作出详细规定。具体包括如下几个方面:

1. 现存计算机数据的快速保护 (Expedited preservation of stored data)。即要求计算机数据管理人或其他人保存已经以静态形式存在的计算机数据,防止由于外部原因而改变或灭失,维护现存计算机数据的安全和完整性;同时要求保护这些数据的时间必须充足,以使权力机关能搜查案件的事实;并且,如果这样不能保证数据的安全,权力机关有权采取搜查、扣押、披露或相似的法律措施。在这一过程中,保护计算机数据的管理人或其他人在依法向权力机关提供以上协助期间,必须保守秘密,以免惊动犯罪嫌疑人。

计算机系统内的往来数据,记录了该通信的发出地、目标地、路径、时间、日期、长度、持续时间或底层服务类型等,因此该数据对于确定过去通信的发起地、目的地和发现犯罪人起关键作用。但这些数据在服务提供者的计算机系统中往往只保存很短时间,因此对其实施快速保护尤为重要。此时,可以要求所有参与了通信传输的服务商,都必须能对往来数据进行迅速保护,司法机关才可以追踪到通信的发起地、目的地,进而发现犯罪人。

2. 提供令 (Production order)。即可以要求个人在其控制范围内提交其持有或控制的特定计算机

数据。该数据储存在计算机系统或某计算机数据存储媒体中,可以要求提供服务的服务商在其持有或控制范围内提供与这些服务有关的用户信息。这里所指的计算机数据仅指现存的计算机数据,而不包括尚未发生的通信中的相关数据。用户信息则指包含在计算机数据形式或任何其他形式中,由服务提供商持有的任何信息,而且这一信息与该服务的用户相关而非业务数据或内容性资料。通过这一信息,可以获悉所使用的通讯服务的类型、采取的技术规则、服务期限;还有根据服务条款或协议可以获得用户的身份、邮政编码、地址、电话或其他号码、账单或支付信息以及安装通讯设备的地点等信息。这些规定对于获取相关电子证据以及相关证据提供了有效途径,可以为侦查犯罪事实提供有利条件。

3. 搜查、扣押现存的计算机数据(Search and seizure of stored computer data)。首先,权力机关可以搜查或访问计算机系统存储的数据以及存储媒介。其次,当权力机关搜查或类似地访问前述计算机系统时,如果有理由相信要搜查的数据存储在一计算机系统中,而且这些数据对初始系统是公开的或可以合法访问的,则权力机关可以快速地扩大搜查或类似地访问该系统。再次,权力机关可以采取必须措施以扣押或类似地获取前述的计算机数据,包括直接扣押计算机系统、计算机数据存储媒介,制作或保留这些计算机数据的副本,维护所存储的相关计算机数据的完整性,以及在访问计算机时使得该计算机数据不可访问或不可移动。最后,权力机关可以要求具备熟悉计算机系统功能以及可采取合理措施保护计算机数据的专家,提供合理、必要的信息,以确保前述相关搜查、扣押等措施的实施。通过这些规定,可以对相关电子证据进行必要的固定,以证实犯罪。

4. 计算机数据的实时收集(Real-time collection of computer data)。这种实时收集包括对往来数据的实时收集,可以由权力机关自己用技术手段收集、记录通过计算机系统传输特定通信的实时往来数据;也可以通过强令服务商在其技术范围内应用相关技术收集或记录,或与权力机关合作或协助其收集、记录上述数据。这里也包括对内容数据的实时拦截,具体措施与前述的往来数据实时收集一样,但这种数据必须与严重犯罪有关。另外,对计算机数据进行实时收集时,要确保服务商对相关采

集证据行为及信息保守秘密。

与《加拿大电子证据法》相比,该公约不是专门针对电子证据的立法,而是针对网络犯罪所规定集实体法与程序法于一体的专门性国际公约,其针对性更强。其中在程序法方面,就是专门针对网络犯罪的电子证据的保护、收集、搜查、扣押以及复制等问题的。这些立法体现了国际社会对网络犯罪之电子证据的重视,也为我们制定网络犯罪电子证据法律提供了借鉴。

## 二 我国电子数据刑事立法存在的问题及对策

目前我国对刑事证据的规定主要集中在刑事诉讼法以及相关司法解释中。《刑事诉讼法》经过1996年的修订以及多年的司法解释不断更新,有关证据的法律体系已较为完善。无论是对证据调查的主体,还是对相关人员的协助义务以及有关证据的搜查、扣押等都有了较详细的规定,使得我国的刑事证据法律形成了体系,这也是我国网络犯罪的电子证据法律依据。但这些规定对电子证据都没有任何明确的规定,而我国也没有其它专门针对网络犯罪的电子证据立法,因此我国理论界和实务界对电子证据的理解还存在较大分歧,对于电子证据的法律属性以及刑事强制措施等主要套用一般的证据法律规定。目前涉及到电子证据的内容则是零星散见于公安部颁布的《公安机关电子数据鉴定规则》、国务院颁布的《互联网信息服务管理办法》、《计算机信息网络国际联网管理暂行规定实施办法》,以及信息产业部、公安部、文化部、国家工商行政管理局联合颁布的《互联网上网服务营业场所管理办法》、信息产业部颁布的《互联网电子公告服务管理规定》、最高人民法院等五个部门联合颁布的《关于办理死刑案件审查判断证据若干问题的规定》等,这些法规一来法律位阶较低,二来只是对电子证据的保存、搜集等做了简要、概括的规定,无法适应现实社会的需求。因此,目前我国电子证据立法急待细化与进一步完善。

由于目前我国并没有将电子证据单列为一种特殊证据,因此司法实践只能往往将其涵盖于七种法定刑事证据中,对这一特殊证据的侦查措施只能套用一般证据的手段,由此使得面对网络犯罪往往难以获取充分的证据。因此,完善我国电子证据立法,必须以国家基本法形式对电子证据作出明确、统一的规定。

考虑到国外电子证据立法的完善以及我国目前的状况,可以通过借鉴国外发达国家的电子证据立法以及前述《网络犯罪公约》的立法经验,来进行我国的电子证据立法。我国目前所要进行的电子证据法律体系立法,可以有以下三种立法模式:一是制定单行的刑事电子证据法;二是在正在起草的证据法中将电子证据列为独立的证据形式;三是通过相关的电子商务法来规定电子证据。我们认为这三种立法模式各有优劣,但第一种模式不太现实,毕竟单行的证据法在我国还未制定,一步到位制定电子证据法在我国时机还不成熟;第三种方式虽然考虑到电子证据与电子商务法的共性,但将实体法与程序法合在一起则不符合立法趋势,也使得电子商务法自身体系的不科学;而第二种立法模式则较为合理,既符合我国的现实,又可以起到解决我国电子证据存在的问题的效果。

在对电子证据的具体法律规定上,我们认为,应当注意以下几点:(1)设立专门的“电子证据”一章,明确界定电子证据的属性,以及电子证据的法律效力;(2)在电子证据的界定上,应当包括电子数据、电子记录及记录的系统,即采纳广义的“电子证据”,扩大其包容性,以防止因为科技的瞬息万变而带来的法律的不稳定性;(3)对电子证据的收集、保全、展示规则上,法律应当尽量具体化、细化,并要根据电子证据的特殊性制定相应的规则;(4)电子证据的质证规则中,应当要求与电子数据相关的录入人员、管理人员、监控人员作证,或通过鉴定方式确认电子证据的可采性;(5)在电子证据的审查、判断规则上,应当注重电子证据与其它相关证据的印证;(6)在证据法中还应该注意电子证据的规定与现有其它相关法律法规的规定相衔接。通过《证据法》中专门一章电子证据的规定,我国的电子证据法律体系主体将得以构成,而相关的电子签名法等将与其构筑起我国完善的电子证据法律体系。

法律是由物质生活条件决定的,并且应当根据物质生活条件的变化而变化。有关电子数据的刑事证据就属于这一情形,当电子数据和网络已经成为社会生活重要一部分内容时,刑事证据不能再局限于书证、物证等传统证据媒介,而应当适时全面系统地对电子数据的刑事证据作出规定。

随着整个社会国际化趋势的加强,法律国际化的趋势也愈加明显。网络、手机等通讯方式的普及,使得犯罪跨越国境成为一种常态,由此各国共同打击犯罪也成为一种趋势。在这一情形下,有关电子数据证据的刑事立法有必要趋向国际化。另一方面,我国在电子数据方面还暂时落后于一些发达国家与地区,这是不争的事实,因此我国的电子数据刑事证据立法暂时落后于这些国家与地区也可以理解。但是,我们必须勇于借鉴这些国家与地区的先进立法,从而完善我国的电子数据刑事立法。

#### 参考文献:

- [1] 王刚. 计算机网络犯罪及其取证初探[J]. 四川警官高等专科学校学报, 2005(2): 52-58.
- [2] 车振宁. 打击网络犯罪的窘境与出路[J]. 人民公安, 2009(6): 12-14.
- [3] 王立民. 加拿大法律发达史[M]. 北京: 法律出版社, 2004: 407-409.
- [4] 刘颖, 李静. 加拿大电子证据法对英美传统证据规则的突破[J]. 河北法学, 2006(1): 125-128.
- [5] 廖明. 电子证据对传统传闻规则的冲击及传闻规则对电子证据的回应——以刑事诉讼为视角[EB/OL]. (2006-08-09)[2010-02-26]. <http://www.criminallawbnu.cn/criminal/Info/showpage.asp?showhead=&ProgramID=150&p>.

责任编辑:黄声波