部门法专论

美俄商用密码法律监管制度比较

陈欣新

摘　要: 商用密码是电子商务的关键技术, 也是保护敏感信息的重要手段。目前, 世界各国都在积极调整其商用密码政策和法律规范, 力争在信息社会取得优势地位。我们在借鉴国际社会的密码法制经验时, 也需要探索密码监管法律背后的国家政治、经济、军事、文化和技术基础。美国和俄罗斯在密码技术方面的领先优势以及对国家利益的考量是其商用密码监管法律制度的重要基础, 而维护国家安全、商业利益和用户权利之间的动态平衡则是设计商用密码监管法律制度的核心。

关键词: 商用密码; 法律监管; 比较法

中图分类号: DF07　　文献标识码: A　　文章编号: 1673- 8330(2011) 01- 0044- 08

美国和俄罗斯是全球范围内密码技术最为发达的强国, 也是商用密码法律监管制度较为完备的国家, 在国家安全和全球高技术市场占有程度方面的国家定位与我国有较强的相似性, 因此, 笔者试图通过对美俄两国的商用密码法律监管制度的比较, 探索可资借鉴之处, 以利我国完善商用密码法律监管制度。

一、美国商用密码监管制度

(一)“9• 11”之前对密码技术的规制

在美国, 对加密技术的法律规制建立了这样一种平衡: 限制加密技术在国外应用以保护国家安全, 同时也承认海外对加密技术的合法需求。美国法律规定, 密钥长度在一定位数以下的加密技术可以出口。需要较强加密技术保证其信息安全的公司要向政府提交一份审查报告, 取得许可后方可出口。出口限制使得美国生产加密软件的公司无法与不受美国法律严格限制的外国公司竞争。可见, 技术的进步是解决对加密技术放松规制的前提。

1. 出口管制中的加密规制

1996年之前, 美国通过《武器出口控制法》、《出口管理条例》(EAR) 和《武器国际贸易条例》(ITAR)。EAR 允许出口拥有一般许可的产品; 政府将加密软件视为一种军需品, 根据 ITAR 的规定, 出口军需品需要单独一项许可, 申请许可需要获得国防部和国家安全局的批准。

在 20世纪 80年代早期至中期, Phil Zimmerman 开发一种软件程序来实施公钥加密术, 使得世界对加密术的理解有了革命性的商业企业。这一软件程序被命名为“Pretty Good Privacy (英文缩写为‘PGP’)”, 在 20世纪 90年代早期, 这一程序扩大了加密术的应用范围, 不但政府和军事上使用密码, 密

[作者简介]陈欣新, 中国社会科学院法学研究所研究员, 法学博士。

码也应用到了普通的商务往来和个人信息传递过程。[①]

尽管 PGP给很多商业公司和个人带来了好处,但它同时也是保证国家安全的一个重要因素。很多国家的政府将加密软件视为一种军需品,将该软件列入了《武器出口控制法》(Arms Export Control Act)的禁止出口名单,与机枪、炸弹和导弹一样在没有许可的情况下不得出口。意识到这一点之后,Zimmerman将这一软件放到了互联网上免费下载。但美国政府认定在互联网上提供 PGP是一种出口行为,这一认定使美国政府对 Zimmerman在互联网上提供 PGP的行为是否触犯《武器出口控制法》展开了为时三年的调查。尽管美国政府进行了很长时间的调查,但并未对 Zimmerman提起诉讼。

1996年 11月 15日,克林顿签发一项执行令,将对"双重用途"加密技术的管理权从国务院转给了商务部。这一命令使得商务部拥有了对任何非军用加密技术出口的控制权。这一权力移转,从国防部转到商务部,对使用加密软件的产品出口很有利。大大缩短了出口商等待许可证和产品的装船时间。在 2000年 1月 12日,克林顿政府宣布,实质上所有含有加密技术的产品均可不受任何限制地出口,这意味着克林顿政府彻底根除了对出口的限制。2000年 7月,美国政府声明,任何美国公司无需申请许可均可向指定的国家出口含有加密技术的产品,这意味着美国解除了对加密技术出口的最后限制。

2 对国内使用加密技术进行规制的尝试

1993年,克林顿政府提出了"Clipper Chip"动案,其目的在于与恐怖主义、毒枭、间谍等使用加密技术来规避法律的人作斗争。政府打算以强制加密技术满足由"第三者保存密钥"的计划来完成这一大胆的目标。[②]与之相关的密钥保存计划要求解码的密钥由一名"可信的第三方(Trusted Third Party 'TTP')"来保存一份副本。"Clipper Chip"计划的动机是允许商务领域使用更强的加密技术,同时要保证在需要的时候为保证法律的执行使密钥可获得。

尽管政府做出相关的努力,但这一计划最终失败了。许多人认为由第三方保存密码的制度会降低产品的安全性,因为如果这样做了之后就达不到通过加密的方法保护商业秘密的目的。[③]软件工业和商事团体认为如果法律强制规定加密软件由第三方保存密码,则就等于给第三方留了一个"后门(back door)",第三方通过这一"后门"就可以获取加密的信息。国内与海外的商务团体害怕政府滥用获取"后门"的权力——以保障法律执行和保护国家安全的名义,从而获取保密信息。克林顿政府无法对上述疑虑作出指引,也不能满足计算机工业和商办工业对上述问题提出的要求,最终放弃了这一动案。[④]

3 对加密技术进行规制的疑问:规制能阻止恐怖主义或会对经济发展造成损害吗

在 9· 11之后,许多人都在反思如果美国政府对加密技术加以规制,会发生 9· 11吗? 实际上 9· 11的第二天就有国会议员提出了这一问题,[⑤]在参议院,参议员 Judd Gregg对"Clipper Chip"动案进行了更新,再次提出了对密码产品进行规制的动议。[⑥]只有少数几个同僚对其作出了回应,那些保持沉默的议员可能是因为美国没有对加密技术进行规制的历史而对其议案不予回应,很多人认为规制对商业的损害和对个人隐私的危害可能要比阻止恐怖主义进攻所形成的利益更大。

4 恐怖组织对加密技术的应用

恐怖组织使用的是加密电子邮件,alQaeda network使用的是"top- notch software engineers",[⑦]这种新技术使得情报部门收集情报的工作更加困难,现在本· 拉登使用的加密设备通过商务的渠道很容易就能获得。

---

① Interview by Russell D. Hoffman with Phil Zimmerman, *Author of PGP*, WALE Radio (Feb 2, 1996), available at http //animated software com /hightech/philspgp htm.

② Saunders, *supra note* 22, at 951.

③ See Black, *supra note* 25, at 301.

④ 前引②。

⑤ Declan McCullagh, *Congress Mulls Stiff Crypto Laws*, Wired News, Sept 13, 2001, available at http //www. wired com /news/politics/0 1283, 46816, 00, html

⑥ 前引⑤ Gregg参议员是来自新罕布什尔的共和党参议员。

⑦ Kirby, *supra note* 70.

尽管中央情报局并没有证实加密技术在恐怖袭击中的作用,但有确切的证据证明恐怖组织使用了加密的电话通讯和电子邮件。一份被广泛引用的报纸报导说,本·拉登的追随者曾将加密信息藏在色情图片中进行通讯。

但是,恐怖主义并不总是使用加密技术来传递信息,有时他们也会将其信息隐藏在图片、音乐和MP3等文件中,放在网站上,在任何时候都可以访问该信息,这是一种很巧妙的方法,这种方法使得情报部门无法用解码的方法来破解信息的内容。

5. 情报部门调查权与加解密技术的法律规制

中情局开发了一种代码为"Magic Lantern"的软件,它可以锁定嫌疑人的键盘,记录所有输入信息,以此方式获得解码的密码。起初,键盘锁定软件是为父母控制孩子上网而开发的,后来,许多公司用此技术来监控雇员使用计算机的习惯。最近,键盘锁定软件已经升级了,开始时中情局发现嫌疑人后,通过进入嫌疑人的家或办公室并将植入键盘锁定程序的芯片放进嫌疑人的键盘才能达到目的。最近,中情局将这一技术与其他技术相结合使之功能更全更有效。中情局将之与一个木马病毒合起来使用,通过向嫌疑人发送电子邮件,伪装成垃圾邮件或亲属的邮件,当嫌疑人打开邮件,木马病毒就会种在嫌疑人的计算机上,进而锁定嫌疑人的键盘。第二种方法是利用操作系统的漏洞进入嫌疑人的计算机安装程序,以此达到目的。只要嫌疑人在线,就可以将信息传回,有时也可能以电子邮件的方式传送。

联邦政府曾经使用这一技术成功地破获了一个明显的团伙犯罪。当锁定嫌疑人后,中情局向联邦地方法官申请法庭的命令,将"Magic Lantern"软件安装在嫌疑人办公室的计算机上。中情局进入New Jersey犯罪团伙成员 Nicodemo Scarfo的办公室,将键盘锁定软件安装在办公室所有计算机上,通过记录Scarfo的键盘输入,FBI发现了解码的密码,进而为控诉提供了诈骗贷款和敲诈勒索的证据。

规制 FBI使用这一技术的法律规定主要在 Patriot Act条款中。[⑧]根据现行法律,法律执行机构要想将木马病毒植入嫌疑人的计算机必须获得法庭的命令。但根据《爱国者法》,当法庭同意的命令可以随后作出的情况下,只有州或美国总检察官可以批准启动程序的措施。

"Magic Lantern"看起来能够承担防止多数规避法律执行的行为。首先,也是最主要的就是"Magic Lantern"与其他手段相比更容易获得批准。其次,与 FBI的 Carnivore制度(容易引出违反美国联邦宪法第四修正案[⑨]的问题)相比,"Magic Lantern"针对特定的计算机和特定的 EMAIL账户。这些因素加上司法监督的一种形式,将为法律实施提供一种工具,他们需要调查嫌疑人时同时保证嫌疑人的宪法权利。

(二)2001年以后美国规制加密技术政策的变迁

2000年 1月 12日,美国商务部出口管制局[U. S. Department of Commerce Bureau of Export Regulation ("BXA")]发布了一项新的出口规则,取消了此前美国对加密技术出口的大多数限制措施,这就意味着克林顿政府在严格限制技术出口方面倒退了一步。白宫放松管制可能是因为此前三年国会不断有新的立法提案提出所形成的压力。

在新规定出台时,由于人们对新规定的狂热必然导致人们忽略了克林顿政府在 1999年 9月前后颁布的 Cyberspace Electronic Security Act of 1999 ("CESA"),该法案早就开始了放松管制。CESA所确立的是限制政府使用或泄漏通过法庭程序获得的解码密钥,并为存放在第三人——"recovery agents"处的解码密钥提供特别保护,批准为 Federal Bureau of Investigations ("FBI") Technical Support Center拨款,为联邦、州和地方法律执行提供支持。支持保护网络隐私的人对 CESA却给以严厉批评,他们认为该法允许政府绕过第四修正案,可以轻而易举地获取加密的电子邮件、商务文件和私人档案。在国会 CESA做出行动前,克林顿就离任了。

美国在加密技术政策上的主要变化,尤其是放松管制和让第三人保存密钥的倡议,均是政府和社会对信息时代将朝着什么方向发展的认知造成的。在诸多互联网的扩张行动中,CESA是一种信号,是政府对加密技术进行规制的另一种尝试。有一个黑客截取了 CD Universe的客户资料,由于 CD Universe

⑧ Vamosi, *supra note* 155.

⑨ 关于公民不受非法逮捕和搜查的权利。

未能满足其要求,于是这个黑客就将截获的几千个信用卡号码出版了,这一事件突显了网络安全的脆弱性。公众对网络易攻击性的认识为强加密技术提供了很大的市场。虽然新时代的加密技术只是简单地用技术的方法代替了早期的加密法,其理论基础是一样的,但已经变得越来越复杂。

现代的加密和解密过程都要进行复杂的数学运算。密钥的强度取决于第三方解码的难度,取决于密钥的长度(以比特来衡量)及算法的复杂程度。例如,一个 40比特长的密钥就可能有一万亿以上的可能组合,一个 56比特长的密钥就可能有 72 quadrillion以上的可能组合,一个 128比特长的密钥就可能存在 3. 4 x 10(su‘ 34’)个可能组合。

最普通的、应用最广的算法是 Digital Encryption Standard (“DES”),其密钥长度为 56bits,是联邦政府在 20世纪 70年代开发的。人们曾一度认为 56位的密码技术是安全的,但最近由一个加密技术厂商赞助的破解 DES竞赛的成果证明,DES并不安全。当 1999年 6月有人承认能够满足新型网络应用的加密标准的最短的密码长度应该是 128bits时,56bits长的密码的缺陷也就显而易见了。在 1997年,当人们刚刚认识到这一问题的存在时,商务部的一个部门,名为 National Institute of Science and Technology (“NIST”),就开始寻找一种更强有力的算法,名为高级编码标准 (Advanced Encryption Standard “AES”)。 2000年 10月,NIST宣布选用 Rijndael为新的高级编码标准,假设其余的开发计划如期进行,则 AES应于 2001年夏天完成。在过渡期间,使用 triple- DES,要求使用三个 DES密钥,已经成为美国政府及其他组织使用的标准。

二、前苏联与俄罗斯商用密码监管制度

(一)前苏联与俄罗斯联邦的密码监管思路及制度沿革

在前苏联时期,科学技术尤其是信息技术被视为苏联共产党及其领导人手中的意识形态武器。在美国于 20世纪 40年代发明小型计算机后,斯大林将开发与美国水平相当的信息处理技术作为首要工作之一。 20世纪 50年代一个名为 MESM(俄文对“小型电子计算机”首字母的缩写)的小型计算机在基辅诞生。这是欧洲大陆的第一台小型计算机,MESM 在前苏联属于高度军事机密,只有少数高层的人知道这一计划。利用信息技术来达到意识形态领域的目标,在 1961年苏共提出的官方科学与技术政策中被反复强调。苏共鼓励致力于“新机器、遥控机械系统的设计理论和原理”的研究,尤其是无线电电子学、计算基础理论、控制系统与信息技术方面的机器,以及对上述机器的改进研究。这一思路在密码监管领域也得到充分体现。前苏联对含有密码技术的产品的进出口、密码产品的使用均采取极为严格的管制,密码技术的研制、开发和生产都是由国家设立的专门机构进行的,实行严格的保密措施。

此时是冷战最为激烈的时期,前苏联总是力图在科学技术方面和军事上能够超越美国及其盟国。在对含有密码技术产品的进出口、密码产品的使用进行严格规制,并对密码技术的研制、开发和生产实行国家专控的同时,前苏联力图通过情报系统获取西方的先进技术来达到其工业发展、技术发展、军事发展和现代化的目的。 1966年前苏联公开了其发展网络的最初基础——多系统的“Minsk- 222”, “Siren”则是前苏联第一个实质意义上的计算机网络。但是,在前苏联解体之前其信息和通讯技术落后于美国及其大多数西方盟国。

(二)改革与公开化(Perestroika and Glasnost)的影响

1985年,戈尔巴乔夫任苏共中央总书记,他开始了一场名为 perestroika的激进式改革和重组运动,这一政策包括公众的政治批评和公开化。公开化(Glasnost)一词的含义主要是指对公众对政府的空前的批评和自由获取信息。

1991年 8月,针对戈尔巴乔夫的政变是前苏联历史上的转折点。这也揭示了一直不为外人所知的俄罗斯计算机网络——Relcom /Demos的存在。由于前苏联根本就没有建立全国统一的计算机网络,程序员的工作是研究和教学,一些军事机构创建了 Relcom /Demos——是一个运行于前苏联主机的 Unix操作系统的非官方网络。这一非官方网络的任务是解决与 Unix相关的问题,并很快应用于苏联全境。Relcom /Demos有电子邮件、新闻组, 1990年时完成了与国际互联网的非官方连接。

在政变期间,程序员使用这一非官方网络在前苏联传递信息, Relcom /Demos允许叶利钦从其避难

所 ——俄罗斯国会就政变向苏联全境以电子邮件传送信息。而克格勃利用传统的信息渠道推动政变的做法却没能成功。从某种意义上讲, Relcom/Demos导致了前苏联的解体,并增加了俄联邦通信的全球化色彩。

在这一时期,前苏联对商用密码的监管开始出现松动。

(三)俄罗斯对互联网的规制

俄罗斯法律规定所有的互联网服务提供者(ISP)都必须在俄罗斯通信与信息部(Russian Ministry of Communications and Informatics)登记注册,也必须从政府获得许可证。此外,所有的电讯业务都必须登记注册,包括网络咖啡屋、电子邮件服务、电话中心等类似的业务。根据俄联邦大众传媒法(Law of the Russian Federation Concerning the Mass Media), teletex,视频文件和其他电信网络都被视为一种大众传播媒介。根据法律规定,俄罗斯境内的所有网站域名(.ru)都必须在 Ministry of Press, Television, Radio Broadcasting及大众传媒中心注册(付费)[By law, all Web sites in the .ru (Russian) domain have to be registered (for a fee) with the Ministry of Press, Television, Radio Broadcasting, and the Means of Mass Communication]。

1995年,俄罗斯联邦安全局(Federal Security Bureau, FSB)——克格勃在内务上的继承者,得到法律授权,其表面是为了法律实施的目的,要求俄罗斯所有的通信服务提供者在其系统上安装 SORM (System for Investigations and Field Operations),以从软件和硬件上保证国家安全局能够通过其设备对网络交通进行追踪。1998年,一个更为先进的可以对通讯及互联网进行监督的名为 SORM-2的系统投入使用。实际上,法律赋予了国家安全局权力和技术,可以为监控的目的不向法院申请执行令,就能利用其设备对所有通讯和网络交通进行追踪。一些西方国家和人权团体据此认为,俄罗斯仍然是个警察社会。

垄断性的、国有的国家或地方电话公司控制着互联网的入口,是市场供应的垄断者。私营的 ISP别无选择,只能从政府所有的电话公司购买本地交换机,这些电话公司本身就是 ISP。

(四)俄联邦对电子商务的规制

电子商务在俄罗斯的发展很困难,其商业模式与其他国家具有同类名称的商业完全不同。俄罗斯的电子商务受制于许多方面,比如俄罗斯消费者的购买力弱、信用卡不普及、信用卡诈骗犯罪率高、邮件与包裹投递系统不完善,最主要的是俄罗斯的金融部门缺乏诚信,尤其是银行。

尽管如此,俄罗斯同其他工业化国家一样,也建立了一套对电子商务进行规制的体制。1993年,俄罗斯国会修改了宪法,将个人隐私纳入到宪法保护的权利范围内,名义上为存储在计算机上的个人数据提供法律保护。1994年,民法典承认商业交易的文件包括电子文件。第二年,俄罗斯国家杜马(国会)通过了一个范围更为广泛的联邦法律——信息、信息化与信息保护法(简称信息法),针对信息的收集者、分析者和信息利用者来说,加强了对俄罗斯公民个人隐私的保护。而且,与买卖、统计研究和数据传送有关的非政府组织和个人都必须取得强制性许可。俄罗斯的域名以古斯拉夫字母.ru为代表。

(五)俄联邦对密码技术的规制

根据俄罗斯法律的规定,加密设备的制造、分销、销售和使用都受制于许可。经贸发展部为加密产品的进出口发放许可证。加密产品的大众市场销售不受豁免。

关于包含加密模块的产品和加密软件的出口,联邦安全部门具有技术咨询的资质。产品是否包含加密,由联邦安全部门(FSS)做技术鉴定,联邦安全部门的技术鉴定向国防部报告。该部门在 30日内向经贸发展部报告结论,经贸发展部根据联邦安全部门的技术鉴定为加密产品的进口或出口发放许可证。一旦进口被接受,一个许可证可用于每个单独的船载货物,联邦安全部门会对每个稍有不同的设备进行检查。

基于加密手段的数据保护的销售和使用(包括技术维护、支持和升级)如果没有被豁免,则受制于经贸发展部的许可命令。在俄罗斯国内使用的加密产品,符合下列条件之一的,可以豁免许可:

1. 可以通过邮政订单、电子订单、电话订单的程序操作系统进行零售的加密设备元件,其加密性能不能被用户更改。那些可由用户自行安装、无需供应商更多支持的设备,以及为审查可公开获得的技术性文件(加密算法的调整,交互协议,界面说明等)。

2 个人信用卡的微机安装, 其加密性质不能被用户更改。

3 批量生产的移动电话 (为商业用途和无线通讯目的的无线电话)。

4 为商业用途的广播设备、商业电视或其他设备, 和没有数字加密信号的广播, 其加密法被限定在视频和音频频道的管理。

5 专为银行和金融机构设计的作为终端组件的加密设备 (ATM 机), 其加密性质不能被用户更改。

6 专门为作为财政设备保护手段的现金机械装置设计的设备组件。

7 彼此独立, 可识别相似的加密算法的加密装置, 拥有最长不超过 40二进制数位的密钥。同样能识别不相似的加密算法, 那些算法基于整个数值的分割, 受限集合或离散对数集合中的乘数集合离散对数的计算, 不同于被指定的拥有最长 128二进制数位的一类密钥。

作为一般规则, 俄罗斯的许可制度对几种加密型产品是不适用的, 只要这些产品的操作系统组件可无偿向公众提供且满足下列条件之一:

1 它们的加密功能 (调整)不能被用户更改;

2 被研发的加密产品可由用户自行安装, 无需来自供应商更多的资料支持;

3 专门性文件 (密码转换算法的描述, 交互协议, 界面描述等)可自由获得 (包括为测试目的)。

虽然法律本身没有规定大众市场的豁免, 但在现实中, 如果产品是在上文提到的用于国内使用的豁免范围内, 那么也不需要进出口许可。不过这取决于产品的性质、种类和用途。特定的产品 (数据, 软件)是否被视为受制于许可的加密产品, 争议是见仁见智的。依据加密技术怎样起作用, 产品为什么而设计等因素, 这些产品可以被豁免许可。对于许可争议, 联邦安全部门事先以书面意见做正式澄清, 这个过程会产生潜在的时间耽搁和管理成本支出。

根据法律或相关办法, 制定国内进口和许可规则的权力由俄联邦当局行使 (包括制定一些内部指令的权力), 如果联邦安全部门为自己的需要, 对货物进口作出许可, 即无需部门许可证书。为了能够进口, 海关当局也接受联邦安全部门的许可决定 (而俄罗斯的法规没有对此予以直接规定)。

出口许可要求通常用于加密产品的“有形”出口, 如果数据不是“有形”出口, 而是以线路、电子或其他方式传输, 就不会受制于出口限制, 海关当局不会对产品在俄境外的无形传输进行限制。

事实上, 在加密数据和技术无形转换的背景中寻求出口许可是不寻常的, 然而这种电子转换受制于经贸发展部要求的出口许可。

三、美俄在 UNCITRAL原则框架下对密码技术法律规制的比较分析

联合国电子签名示范法 (The UNCITRAL Model Law on Electronic Signatures)所确立的几个重要原则是建立在保障畅通的、全球化的电子商务基础上的。联合国电子签名示范法的三个重要原则是: (1)技术中立; (2)在国内的电子签名及认证证书和外国的电子签名及认证证书之间不歧视; (3)国际化 (international outbok)。

(一)技术与媒体中立

法律不限制或不要求电子签名必须使用某种编码技术。电子签名示范法第 3条阐述了这一原则, 该条规定是“任何创造或产生电子签名的技术或方法都不应被看轻 (no technology or method of creating or gaining access to e- signatures should be discounted)”。同时这一原则也体现在该法对“电子签名”的定义中, “electronic signature means data in electronic form, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.”这一定义向所有可靠的电子技术开放, 无论是现在已知的技术还是将来发明的技术都可以用作电子签名。

1 美国的情况

美国从概念上反映了电子签名示范法所确立的技术中立原则, E- Sign Act如此定义电子签名: “An electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.”美国在立法上具有技术和媒体中立

的传统,无所不包的定义涵盖了现有的和未来的所有技术。法律列举了可供选择的使用或接受电子签名必要的程序或要求,这种对电子档案或电子签名的创立、储存、产生、接收、通讯或认证的选择性并没有赋予任何一种选择具有高于另一种选择的法律地位或法律效果。该法为所有应用于计算机和数据安全的美国技术提供了一个竞技场。

2 俄罗斯的情况

俄罗斯的情况与美国完全不同。1994年,俄罗斯首先承认电子签名的效力,2002年,通过《俄联邦数字电子签名法》来规制计算机、网络和数据库安全。该法约束的是一种特定的数字技术,名为 GOST,一种公钥数字签名算法,法律对电子签名的定义为:“A sequence of symbols that results from cryptographic transformation of basic information with the use of a secret (private) key that allows the holder of the (open) public key to establish the integrity of the information as well as the signatory or holder of the private key.”该法设立了一个国家特许的数字签名证书中心,为监视和控制的目的,政府直接参与网络商务之中。

在电子通讯中,法律承认电子签名与物理手写的签名具有相同的功能。该法排除了生物统计技术在电子签名中的应用,如眼球扫描、手写签名的类似物及手写签名的电子叙述等技术。此外,该法包括一条确认条款,根据这些认证条款的规定,政府查证中心具有查证、证实和确认电子签名是否属于某个个人或法人的职责及为数字签名签发证书的职责。数字认证中心是承担确认数字签名真实性和为数字签名签发证书,以及撤销或延缓数字电子签名的编码的人或特殊的政府部门。

(二)对国内电子证书和签名及国外电子证书和签名不歧视

电子签名示范法规定,当确定电子签名在法律上是否有效时,电子签名的创设或电子证书签发的地理位置不应成为考虑因素。电子签名示范法建议各国制定电子签名法时应明确规定,只要电子签名具有实质的可靠性,无论产生于国内和国外的电子签名均在全国范围内作为一种签名形式具有同样的法律效力。此外,电子签名示范法还规定各国可以通过双边协议或多边协议就电子签名的问题达成一致。

1. 美国的情况

作为电子商务全球化和普及电子签名的领军人物和主要受益者,美国从克林顿政府时期开始就号召各国对网络采取不干涉的政策。尽管克林顿政府倡导各国在构建网络规制结构时在全球使用 key recovery encryption,但其标志性的特征仍然是对来自各国的技术采取不歧视的政策,这一情况随着时间和技术的进步发生了变化。电子签名法规定,“对来自其他法域的电子签名和认证方法采取不歧视的政策”。但该法未涉及禁止向俄罗斯、中国等国家出口加密技术的问题。从现状来看,美国的公司是全球认可电子签名和证书的主要受益人。很难想象,一个美国的重要银行,甚至联邦储备委员会会将来自布基纳法索或缅甸的电子签名与基于美国安全公司技术的电子签名同等对待。

2 俄罗斯的情况

俄罗斯电子签名法并没有延用电子签名示范法所规定的不歧视原则,其对外国的公钥框架电子证书只有通过“交叉认证原则”才会被俄罗斯的法律所接受。这就是说,想要俄罗斯的认证机构承认其公钥证书的国家必须与俄联邦签订双边或多边协议,并向认证中心提供俄国法律所规定的与 Russian Public Key Infrastructure相称的数据并证明其通讯的安全性。

此外,1995年的一项总统令,禁止在俄联邦境内使用未经国家安全机构——政府通讯与信息管理局(Agency for Government Communications and Information)认证的加密算法或设备。未经许可出口或进口加密软件或硬件在俄罗斯都是违法的。由于公钥框架并不是在所有的司法领域都通行的规则,因此,俄罗斯的法律明显带有歧视性。

(三)国际化(Internationalist Outlook)

实际上,联合国鼓励各国采用彼此不同的电子签名政策或技术,但应与其他国家的电子签名政策或技术具有某种公认的、公开的、具有国际性的、商业化的、由市场驱动的标准。这一“公认的国际标准”原则包括国际化的技术及商业标准和规范,体现为政府或政府间的要求、建议、行为准则、声明等。

1. 美国的情况

将网络作为全球化的电子商务的一个公开平台,美国冲在了各国的最前线。克林顿政府所设计的

全球化电子商务和《电子签名法》是建立在自由、公开的国际电子商务体制的前提下的。为了促进各州之间及美国与外国之间的商务交往,《电子签名法》赋予了商务部长“在国际范围内”推动人们“接受、使用”电子签名的任务。

从全球化的角度来看,美国所推行的自由主义电子商务存在一个例外——国家安全。但事实上,美国已经放松了可用于电子商务的强加密产品的出口和再出口,除了俄罗斯、中国等国家由于国家安全的原因仍然面临进口或再出口美国强加密产品的重要限制。从法律的角度来看,实质上从美国出口或再出口含有强加密技术的产品都构成实施“信息安全问题”(获取抵抗美国的信息、间谍、从事与军需品的买卖),应获得许可或得到商务部或财政部的特别批准。将此类技术提供给美国公司在国外的工厂也要经过政府批准。这就导致了美国信息工业从业者与美国政府对电子商务中可以形成电子签名的加密技术的出口问题产生分歧。美国信息工业从业者尤其感到不满的是,这些限制使得美国人退出了 56位以上的数据强加密技术这一开放的国际市场。从这个角度来说,俄罗斯倾向于选择使用国产的加密技术的原因并不难理解,即安全和访问的因素。

对电子商务起着促进作用的美国加密技术出口或再出口的限制同样证明,在电子商务全球化的环境下,美国的国家安全利益要优先于其他国际电子商务参加者的利益。具有讽刺意味的是,UNCITRAL示范法对强加密技术或其他加密技术出口或再出口的限制问题保持了沉默。

2 俄罗斯的情况

与美国的电子签名法相比,俄罗斯法律表面上的国际性并没有美国强,尽管俄罗斯的法律承认基于双边协议或多边协议的电子签名的法律效力,但法律在适用范围上并没有国际性。俄罗斯立法的初衷是对俄联邦境内的电子商务和金融交易进行监控,而不是为了促进电子商务的全球化。未经许可,俄罗斯的 GOST公钥框架禁止出口。

值得注意的是,加密信息尽管可以免受爱打听人的偷看、偷听、拦截或窃取,但它同样也妨碍法律的实施,情报部门针对有组织的犯罪、工业间谍、恐怖主义和敌对国家所进行的监听、搭线等行为也会受到限制。于是,法律执行部门和情报机构开始要求使用关键恢复系统的生产厂商在所有权人不知晓的情况下,为暗中的第三方(政府)获取加密数据和通讯内容提供方便。关键恢复加密系统实际上意味着,“保证第三方(政府调取)获取加密的电子签名和电子数据的任何系统”。在这方面,美国与俄罗斯的情况没有差别,并且这种做法与通行的民主和法治原则存在相悖之处,在极端情况下,个人的隐私和自由可能不复存在,这就是国际社会存在着强大的避免开发此类技术系统的呼声的最根本理由。

On Comparison of Legal Regulations on the Commercial Encryption in the USA and Russia

CHEN Xin-xin

Abstract: The commercial encryption is the core technology of electronic commerce, as well as an important measure to protect sensitive information. Nowadays, most countries are adjusting their policies and laws on the commercial encryption so as to gain comparative advantages in the information society. It is suggested to explore the political, economic, military, cultural and technical foundation behind the legal regulation system of the commercial encryption when taking experiences from other countries for reference. Both U. S and Russia have advantages on the commercial encryption, and state interest also plays an important role in the process of constructing regulation on the commercial encryption. However, the core of such regulation system lies in the dynamic balance among national security, commercial interest and users' rights.

Key words: commercial encryption; legal regulation; comparative law