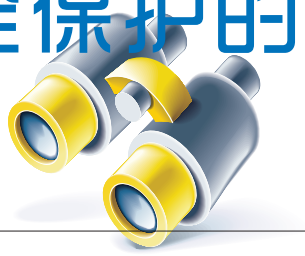
俄罗斯联邦信息安全保护的法律规制（上）



● 刘洪岩

中国社会科学院法学所

在当今时代，现代信息技术的发展和运用使人们的生存方式和生活习惯发生了根本性的改变。信息资源的获取和保护已成为公民个人、社会和国家发展的决定性因素之一。信息资源在实现公民的宪政权利和自由、保障公民个人自我价值实现、社会精神重建、国家政治和社会稳定、保障国家职能高效率实现等方面发挥着积极的关键性作用。信息技术的发展正越来越成为世界发达国家之间经济发展、综合国际竞争强有力的决定性因素之一。伴随着信息化融入到国家、社会及公民个人生活并触及到相关群体切身利益，信息安全亦成为了国家安全及国家、社会及公民和谐发展的重要有机组成部分。

一、俄罗斯实施信息安全保护法律规制的背景

近年来，由于国际信息技术的突破性发展，俄罗斯在信息安全领域面临来自诸多方面的现实威胁。早在1996年犯罪分子就曾试图在莫斯科银行的计算机系统中使用假报表。而根据俄罗斯联邦安全委员会的数据，1999年计算机犯罪给俄罗斯造成的损失相当于俄罗斯的国防预算。据官方消息，2004年在俄罗斯联邦总统选举时，俄罗斯中央选举委员会原网站遭到了1 800次黑客攻击，其中20%来自境外。据俄罗斯最新公布的数据显示，在过去2年里，黑客对联邦安全局所保护的国家权力机关信息系统进行了两百多万次的攻击；同时，俄罗斯总统网站遭受了三十多万次攻击。据阿什莫诺夫及伙伴公司统计，俄罗斯企业每年由于接收和删除垃圾邮件的人员怠工所导致的经济损失达三千万美元。据科尔比纳杰列科姆公司估计，俄罗斯邮电部门因非法接入和不支付电话通话费用每年损失约1.5~2亿美元。由于密码失窃恢复被计算机病毒破坏的程序，个人计算机家庭用户每年要花费大约1500~2000万美元。据估计，俄罗斯IT基础设施用户的损失每年以30%的速度增长，全世界IT基础设施用户的损失也是如此。

正是基于上述原因，近年来俄罗斯越来越重视在信息安全方面的法制建设。以1995年颁布的《俄罗斯联邦信息、信息化和信息保护法》为发端，俄罗斯于1997年又出台了《俄罗斯国家安全构想》，其中明确提出：“保障国家安全应把保障经济安全放在第一位”，而“信息安全又是经济安全的重中之重”；2000年9月，普京总统批准了《俄罗斯联邦信息安全学说》。该文件中首次明确了俄罗斯在信息领域的利益、所面临的内在和外在威胁以及为确保信息安全应采取的措施，成为俄罗斯官方保障国家信息安全的目的、任务、原则和主要内容的观点总和，是制定和起草俄罗斯联邦有关信息安全保障的国家政策、法律、提案和专门计划的基础；2001年1月俄罗斯又出台了《2002~2010年俄罗斯信息化发展目标纲要》；同年又颁布了《俄联邦信息和信息化领域立法发展构想》，明确了5~10年的立法内容；2003年启动了《保障俄联邦主体信息安全的联邦政策框架》等。

二、俄罗斯实施信息安全保护的基本政策及架构

2004年，俄罗斯联邦明确了信息安全保障体系的优先发展方向，确立了俄罗斯联邦信息安全

保护的总体政策及架构。具体包括：

（1）发展信息安全保障体系，研究信息理论和实践；

（2）改进并研制新的信息安全保障方法和手段；

（3）改进并建立新的信息保护法律标准；

（4）改进信息安全机制；

（5）建立信息安全分析模型和方法，评估信息保护等级和信息安全的完整性；

（6）发展信息质量管理系统，改进监控方法和手段。

在保障信息安全的基本策略及措施方面，第一，俄罗斯非常重视信息安全领域新技术及新设备的研发。俄罗斯注重对重要信息系统保护的同时，大力发展信息保护高端技术设备的研制，其中包括信息压缩积聚设备、信息形式掩蔽设备、灾难恢复与备份设备、信息分析诊断设备和技术侦察跟踪设备等。俄罗斯在发展信息安全技术上强调自主创新、坚持自成体系，积极推广采用俄罗斯自己研制的电子数字签名及其他保护设备，如在财政金融系统，注重芯片自主研发，联邦办公自动化系统强制使用俄罗斯智能卡；在加密领域，密码学院从事着加密技术研究工作，着力加强光纤通信加密和量子加密方面的研究。

第二，俄罗斯十分注重信息安全领域的技术理论创新及对信息技术及设备监管。俄罗斯在加密领域制定了监控光纤通信的原则及技术方法，在光通道传输信息、量子通道的基础上从事量子加密方面的研究，制定电信—信息系统信息保护的系统方案。在信息安全技术市场上实行国家干预和调控，保证优先发展特种信息保护设备和保护国家秘密的手段，对特种信息保护设备流通领域实行严格的专营管理和准入制度。俄罗斯将信息传输中数据完整性要求放在首位，经常进行不同地点的数据备份；规定公司的信息安全应成为经常审查的项目之一；在全联邦大力普及、推广和应用最新的应对灾难恢复的软件产品。同时，建成了高效安全的数据传输模式，确保了俄罗斯联邦各主体行政中心之间文件的网络传输；在最高国家机关安装了保障加密数据交换的技术设备，解决了该系统与国内其他通信网协同的技术问题。

第三，俄罗斯致力于开展信息安全领域的国家服务。俄罗斯积极开展技术侦察，评估和预测使用全球计算机网络的信息安全风险，及时发现有害信息攻击。建立全球计算机网络预谋犯罪者行为的相应概念模式；对全球计算机网络的违法行为进行详细的结构化和程序算法描述；对病毒软件的性能和信息攻击的方向进行业务分析，分析评估全球计算机网络用户信息安全的威胁程度。目前，俄罗斯大部分企业和组织都在使用反病毒软件作为安全措施，其中40%的企业使用IDS评估全球计算机网络信息安全威胁程度，及时发现有害影响。

第四，俄罗斯建立网络使用及信息监察制度。俄罗斯对涉密计算机只允许使用单向导入系统连接互联网，将互联网中的信息导入到涉密网内。对涉密网实行与国际互联网物理隔离，同时比较注重网络连接方面的保密技术管理措施。同时，俄罗斯允许对经由因特网传播的信息进行监督检查，通过建立联邦经济信息保护中心负责政府网络及其他的专门网络、网络信息配套保护、国家政权机关信息技术保障等。

此外，俄罗斯以信息安全人才培养体系为基础，加强信息安全人才的培养。目前，俄罗斯已经拥有了信息安全专业的高等学校、信息安全地区教学中心、各部委信息安全管理机构和科研机构，并以此为基础建立起信息安全人才培养体系，专门培养和培训信息安全方面的专业人才。该培养体系根据国家教学标准，涵盖了计算机安全、信息对象的综合保护、密码学、信息保护制度与技术、通信系统的信息安全和反侦察信息技术、自动化系统的信息安全综合保障等多个信息安全专业。

三、俄罗斯信息安全保护的法律规制

俄罗斯在确立信息安全保护的政策和基本架

构的同时，在立法实践中也逐步建立了较为完善的信息保护法律体系，颁布了一系列涉及信息安全保护的法律，其中包括《俄罗斯联邦信息、信息技术和信息护法》《俄罗斯联邦安全法》《俄罗斯联邦国家秘密法》《俄罗斯联邦出入境法》《俄罗斯联邦产品服务认证法》《俄罗斯消费者权益法》等法律。其中《俄罗斯联邦安全法》是一部有关保障国家安全和保护国家信息安全方面的基本法，其他涉及信息保护法律的制定与施行都必须以该法为基础。此外，俄罗斯还以《俄罗斯联邦宪法》《俄罗斯联邦安全法》为基础，制定了一系列保障信息安全的法规及其他涉及调整与保护信息安全的相关法律文件。俄罗斯颁布的大量涉及信息安全领域的规范性法律文件为俄罗斯国家信息安全战略的实施、国家秘密的保护及限制涉密信息的传播提供了可靠的制度保障，具体体现在以下几个方面。

（一）确立信息保护的法律标准

2006年7月27日颁布的《俄罗斯联邦信息、信息技术和信息保护法》（第149号令）规定，根据接触权限将信息划分为两大类，即大众化信息和受联邦法限制接触的信息。接触权限受限的信息是指设有专门保存和使用制度的信息。在俄罗斯联邦通常使用“秘密”这个术语来表示受立法保护的信息。在司法实践中，《俄罗斯联邦国家秘密信息定秘规则》规定了确定国家秘密的执行标准；而《俄罗斯联邦国家秘密信息清单拟定规则》则规定了拟定秘密清单的标准。现行《俄罗斯联邦国家机密法》（2004年颁布）在第二章第五条中规定了国家秘密信息文件资料清单，在第三章确立了国家秘密信息文件资料的划定标准，国家依据不同的秘密等级对涉密信息实行不同的保护措施。2006年2月11日俄罗斯联邦总统第90号令又对被划定为国家秘密的信息文件资料清单进行了修订，为信息保护明确了等级和方向。

同时，俄罗斯确立了《计算机系统安全评估标准》《产品安全评估软件》等一系列完善的系统安全评估指标，相关职能部门依据此标准进行执法评估。2005年颁布的《俄罗斯联邦有关国防产品（工程、服务）、国家秘密信息或者受限制接触信息（依照俄罗斯联邦立法）产品（工程、服务）以及国家秘密产品（工程、服务）的保护标准化条例》对信息保护产品的若干标准作出了明确规定，其中包括：国家间军事标准、国家军事标准、战事状态期间国家军事标准补充、国家战时状态标准、限制扩散国家标准、行业标准等内容。

在人才培养方面，《俄罗斯联邦关于培养国家秘密信息保护专家及关于无需国家认定即可向相关企业、机关和组织推荐信息保护专门人才的教学机构名单》《俄罗斯联邦国家秘密信息保护专家培养教学大纲》以及俄罗斯联邦教育部学科（信息学）示范大纲（信息安全和国家秘密保护部分）为信息保护人才的培养在教育机构、教学计划及内容方面确立了国家标准。

（二）建立了健全的保障信息安全的法律监控方法和手段

1. 对接触涉密信息特定主体的管理

（1）对接触涉密信息公民的出入境限制。根据《俄罗斯联邦出入境法》规定：公民被许可接触绝密或者机密信息，而依照《俄罗斯联邦国家秘密法》这些信息属于国家秘密，应在其签订的劳动合同中约定暂时限制其出境的条款，但限制期限不超过5年；公民接触过的绝密或者机密信息，在公民递交出国申请时，相应的国家秘密审查机构还保留有该信息相应的密级，那么劳动合同中应约定对劳动者出境权利限制期限可以由国家秘密跨部门管理委员会作出延长限制出境年限的规定，对出境权的限制合计不应当超过10年（该法第十五条）；限制俄罗斯联邦公民出境权时，该公民护照在临时限制期满前必须交给发放护照的国家机构保管（该法第十八条）；俄罗斯联邦武装力量中的军人以及联邦执行权力机关

中规定有兵役的军人（不包括应征入伍服兵役人员），在按照俄罗斯联邦政府规定程序办理了出差许可情况下可以出境（该法第十九条）。此外，在《俄罗斯联邦政府关于俄罗斯联邦武装力量军人，以及规定有兵役的联邦执行权力机关军人办理出国许可手续程序的决议》、《俄罗斯联邦公民出入境手续办理和护照发放规则》等法律文件中还对军人、公民出入境时的涉密问题作出了专门规定。

（2）对接触涉密信息主体使用信息的法律规制。依据《俄罗斯联邦有关双重国籍、无国籍，以及外国公民、侨民接触国家秘密许可程序规则》规定：获得双重国籍的人员，根据对俄罗斯联邦公民公开原则的规定应允许接触国家秘密。只有在联邦安全局机构采取了审查措施后上述人员才有权接触带有“秘密”印章标注的国家秘密信息（该法第三条）；无国籍人员依照俄罗斯联邦政府决议可以获得接触国家秘密信息的许可。通常不允许无国籍人员接触绝密信息和机密信息（该法第四条）；外国公民获得接触国家秘密的许可依据国际公约中有关外国国家保护其得到国家秘密信息的义务性规定。外国公民还可以被准许接触通过履行向其他国家转交国家秘密信息准备条款规定程序而获得的信息（该法第六条）；被允许接触国家秘密的人员，根据俄罗斯联邦立法规定承担泄露所接触国家秘密的责任（该法第十条）。

《俄罗斯联邦权力执行机关关于限制传播公务信息的程序规则》中也包含相应的对使用限制信息的规定，如将注有“公务用”的文件和卷宗从一位工作人员向另一位转交，应当得到相关负责人许可；当负责登记“公务用”文件的责任人交接班时，应形成文件接收和转交记录，该记录由相关负责人签字确认；如果必须将标注“公务用”文件邮寄到几个地址时，要编制一份分发记录，按地址填上所邮寄文件的编号，由起草文件的部门执行人和负责人在分发目录上签字等。

依据《俄罗斯联邦技术与出口监督条例》，联邦技术与出口监督局有权对联邦国家权力机关、俄罗斯联邦主体国家权力机关、联邦执行权力机关、俄罗斯联邦主体执行权力机关、地方自治机关和单位，在保障信息基础设施关键系统的信息安全、技术侦察防范和信息技术保护领域的活动实施监督；对俄罗斯联邦对外经济活动参与者遵守出口监督方面的俄罗斯联邦法律和其他规范性法律文件情况实施监督检查等。

《俄罗斯联邦国家机密法》第二十一至二十六条规定了对涉密人员的管理，如被准许或曾被准许接触国家机密的公职人员或公民的权利可以暂时受到限制，所涉权利包括：在办理准许公民接触国家秘密手续时签订的劳动合同（契约）中所约定期限内的出境权；传播扩散国家秘密信息文件资料的权利和使用包含有这些信息文件资料的发现与发明的权利；在办理准许接触国家秘密手续期间进行检查时私人生活不受侵犯的权利。同时，个人在接触和使用国家秘密信息时都应遵守一定的特别程序，并应当对本人的泄密行为承担相应的责任。该法第十六、十七、二十七条对企业、机构和组织的涉密问题作出了规定，如企业、机构和组织从事涉及使用国家机密信息文件数据的工作应当获得许可；在按法律规定程序签订的进行共同工作和其他工作的合同中，要规定出双方不论在工作进行过程中还是在结束后保障国家秘密信息文件资料完好性的相互责任等。

此外，俄罗斯明令禁止涉密办公室内的计算机连接互联网，禁止在涉密场所、部位的计算机上安装视频、音频输入设备；涉密计算机的软驱、打印口、USB等端口只允许开放输入功能，关闭输出功能，需要使用时必须通过保密管理人员授权；严格涉密场所和涉密电子设备的电磁发射保密管理，涉密场所定期进行电磁环境检测，涉密电子设备必须进行检测后才可使用，并强制采取屏蔽室、低泄射和干扰器等相应的防护措施。经过检测的涉密电子设备不许擅自改动，甚至不允许更换位置；在举行重要的涉密会议和活动时均使用手机信号干扰器，采用了智能干扰技术。重点涉密人员可使用保密专用手机，并对公众使用手机实行 “实名制” 。 （未完待续，见下期）