

# 俄罗斯联邦信息安全保护的 法律规制（下）

● 刘洪岩

中国社会科学院法学所

【编者按】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，因而俄罗斯越来越重视在信息安全方面的法制建设。本文在8月刊集中探讨了俄罗斯实施信息安全保护法律规制的背景和俄罗斯实施信息安全保护的基本政策及架构两个问题，并从确立信息保护的 legal 标准、建立健全的保障信息安全的法律监控方法和手段两个方面介绍了俄罗斯信息安全保护的 legal 规制，本期继续从建立涉及信息安全的许可认证制度、明确信息保护相应的执行机构和建立对长期保护信息人员的社会保障制度3个方面介绍俄罗斯信息安全保护的 legal 规制。

## （2）规定了受保护信息载体的法律监管措施

《前苏联政府档案文件解密和保密期限延长程序条例》明确了俄罗斯联邦档案机关内保存的前苏联政府文件解密或者延长保密期的规则和程序。该条例规定了由国家秘密保护跨部门管理委员会作出有关前苏联政府文件是否解密及解密内容的决定。涉及包含公民私生活情况以及个人资料的前苏联政府文件的解密，要遵照《俄罗斯联邦宪法》《俄罗斯联邦侦查活动法》，以及有关俄罗斯联邦档案资源和档案资料解密的立法原则以及其他特定的程序和方法来实施。

《俄罗斯联邦国家秘密信息转交其他国家的程序条例》规定了俄罗斯联邦执行权力机关和俄罗斯联邦各主体执行权力机关向其他国家转交涉及国家秘密信息的条件和规则，以及准备并向俄罗斯联邦政府呈报材料的程序。其中规定：（1）应与接收方签定国际协议，协议中明确接收方在保护被转交

信息方面的责任；（2）与信息转交有关的联邦执行权力机关、俄罗斯联邦各主体执行权力机关、企业、机关和组织向全权负责信息管理的国家权力机关领导人提交包含涉密信息转交理由的申请，其中应说明：信息转交的目的；被计划转交信息的清单、信息的密级，信息保密的决定人及保密理由（列入国家秘密保护名录）；信息转交接收方的全权职能机关清单；信息转交必要性和适宜性的依据，评估信息转交对保障俄罗斯联邦政治和经济利益的影响；在接收方未履行其承担义务情况下损失赔偿的计划程序；（3）应当对要转交的国家秘密信息进行鉴定。

在2004年颁布的《俄罗斯联邦关于在国际信息交流中保障俄罗斯联邦信息安全的措施》总统令中，规定了在借助信息系统、网络和通信系统（包括互联网国际协会）手段开展国际信息交流时应保障俄罗斯联邦信息安全的措施及要求。其中规定了在俄罗斯联邦，对处理国家秘密信息、限制传播公务信息，以及对许可接触秘密信息载体所应遵

循的特别原则。涉密的信息系统、通信系统和个人电脑，在国际信息交流中，相关负责人不能将其接入到国际信息交流设备，其中包括互联网国际协会。只有在使用了保障信息完整性和安全性的信息保护认证设备（其中包括确认信息可靠性的密码设备）之后，国家信息资源的监控者才可以将其接入国际信息交流设施；上述资源的所有者和使用者应将国际信息交流时所使用的公开信息系统、网络和通信系统，包括互联网中的技术设备放置在涉及国家信息安全问题的秘密谈判场所之外。

《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》规定了联邦权力机关及其下属企业、机关和组织（以下简称组织）内处理包含限制传播公务信息文件和信息其他材料载体（注：此条例涉及处理其他限制传播公务信息材料载体〈照片、电影、视频和音频等〉的程序）的总体程序。其中规定了：不列入限制传播的公务信息种类；处理包含限制传播公务信息文件的程序规则，如在包含限制传播公务信息的文件上（必要时在文件草案上）应作出“公务用”标注、对公务信息文件的复制须得到相关领导人书面许可、向部门工作人员转交公务信息文件以收条为依据、公务信息文件应保存在保险箱和贮柜内等等。

《俄罗斯联邦国家秘密法》的第二条、十一条、十二条、十九条对涉密信息的载体管理作出了明确规定，如：如果载体是由不同密级的信息文件资料组成的，其每部分都应盖有相应的密级印章（密别印），则整个载体要加盖与组成部分中最高密级相同的密级印章（密别印）；载体和（或）随同文件中除了本条款所列的要项外，还可注明规定哪些负责人具有了解该载体中信息文件资料的补充标记；当不可能证明所获取（制定）的信息文件资料与现有清单中所包含的信息文件资料相符时，国家权力机关、

企业、机构和组织中的负责人应当按照拟定密级对其预先进行保密；拥有国家秘密信息文件资料的国家权力机关、企业、机构和组织，当其职能和所有制形式发生改变时，以及当被清算或被终止从事使用国家秘密信息文件资料的工作时，应当采取措施保护这些信息文件资料及其载体。同时，国家秘密信息文件资料的载体应当按规定程序予以销毁、上交存档或移交给法定的相应机构等。

### 3 建立了涉及信息安全的许可认证制度

（1）保护信息的产品认证。根据《俄罗斯联邦消费者权益保护法》《俄罗斯联邦产品服务认证法》和《俄罗斯联邦国家秘密法》的规定，信息保护设备实行强制认证，并成立专门的认证机构和实验室；安全等级分为A、B、C、D、E五个等级。俄罗斯生产的信息保护设备和产品只有在获得认证后，才能在市场上销售并准许使用。认证工作由联邦技术出口监督局、联邦安全局、对外情报局和国防部分别负责。

《俄罗斯联邦国家秘密信息安全保护设备认证体系条例》规定了国家秘密信息安全保护设备系统的基本原则、组织结构，秘密信息安全保护设备的认证程序、认证设备注册程序，以及对认证设备实施检查的程序。

对信息加密保护（密码）产品实行认证制度。2002年9月2日，俄罗斯政府签署691号决议，通过《密码设备销售活动许可条例》《密码设备技术服务活动许可条例》《密码领域服务许可条例》和《密码设备及相关信息、远程通信系统研制与生产许可条例》等一系列文件，对密码设备领域的活动许可事宜进行具体规定。

（2）保护信息的技术许可。2006年俄罗斯政府通过504号决议，批准了新的《秘密信息技术保护条例》。新文件增加了许可

要求与条件,以及违反规定的处罚内容,从而大大增强了条例的针对性。《俄罗斯联邦秘密信息技术保护的许可证制度条例》(2006)规定了法人和个体企业主获取经营秘密信息技术保护业务许可证的程序,许可机关依据法定条件对申请人的执行业务申请进行审批。

(3) 涉及信息保护的许可证。依据《俄罗斯联邦企业、机关和组织从事涉及国家秘密信息使用、信息保护设备制造以及实施使用国家秘密信息保护设备方面的保护措施和(或者)提供服务相关工作业务许可证制度条例》(2007)规定:对各种所有制形式企业、机关和组织(以下称企业)从事涉及国家秘密信息使用、信息保护设备制造以及实施使用国家秘密信息保护设备方面的保护措施和(或者)提供服务相关工作实行业务许可证制度。许可证是一种依据特定条件允许在规定期限内开展某种具体业务的正式文件,它在俄罗斯联邦境内有效,在境外的俄罗斯联邦机关内也同样有效;许可证应根据业务种类确定许可证的有效期限,但一般不能少于3年和超过5年;依据申请人的特别要求,也可以签发少于3年期限的许可证。

## 4 明确了信息保护相应的执行机构

在国家秘密信息保护方面,俄罗斯联邦安全部门负有主要责任。依据《俄罗斯联邦安全部门法》(2005)规定:联邦安全局负责:参与制定和实施保护国家秘密信息的措施,对国家秘密信息的完好性进行监督,在国家机关、军事武装、企业、机构和各种所有制形式的组织中按规定程序实施与公民许可接触国家秘密信息相关的措施;依照俄罗斯联邦立法参与处理涉及俄罗斯联邦公民进入俄罗斯联邦境内和出境的问题。

关于拥有定密执行权的公职人员。2006年颁布的《俄罗斯联邦有权确定国家秘密全权的国家权力机关公职人员名单》明确了有权确定国家秘密的公职人员,此项法令有利于提高工作效率和进行责任追究。

关于外国公民接触国家秘密的许可。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》第七条规定:由以下机构领导人作出外国公民接触国家秘密的许可决定,即俄罗斯联邦国家权力机关、俄罗斯联邦各主体国家权力机关、俄罗斯联邦政府赋予全权从事向其他国家转交国家秘密信息全权的企业、机关和组织。上述决定要得到俄罗斯联邦安全局的同意。

关于信息保护相关业务许可。依据《俄罗斯联邦企业、机关和组织从事涉及国家秘密信息使用、信息保护设备制造以及实施使用国家秘密信息保护设备方面的保护措施和(或者)提供服务相关工作业务许可证制度条例》(2007)规定,负责许可证业务的全权机关包括:

- 颁发企业从事涉及使用国家秘密信息工作的许可证业务由俄罗斯联邦安全局及其地区机关(在俄罗斯联邦境内)、俄罗斯联邦对外情报局(境外)负责;

- 对从事制造信息保护设备工作实施许可,由联邦技术和出口监督局及其地区机关、俄罗斯联邦对外情报局、俄罗斯联邦国防部、俄罗斯联邦安全局(在其职权范围内)负责(俄罗斯联邦政府2004年12月17日807号决议版本);

- 对实施使用国家秘密信息保护设备方面保护措施和(或者)提供相关服务进行许可,由俄罗斯联邦安全局及其地区机关,联邦技术和出口监督局及其地区机关,俄罗斯联邦对外情报局(在其职权范围内)负责(俄罗斯联邦政府2004年12月17日807号决议版本)。



对于许可俄罗斯联邦安全局、俄罗斯联邦国防部、俄罗斯联邦边防局、俄罗斯联邦对外情报局、俄罗斯联邦技术和出口监督局所属企业从事涉及使用国家秘密信息工作方面业务的许可证颁发，由上述企业所隶属的俄罗斯联邦各部和主管机关领导人员作出决定（俄罗斯联邦政府2004年12月17日807号决议）。

关于使用保护信息的许可鉴定。依据《俄罗斯联邦对许可企业、机关和组织开展涉及使用国家秘密信息业务问题实施专门鉴定的程序规则》的规定：由俄罗斯联邦安全局和区域安全机关，俄罗斯联邦总统直属国家技术委员会，俄罗斯联邦总统直属联邦政府通信和信息机关及其各地区机关，俄罗斯联邦其他部和主管机关（这些部门的领导人员对其所管辖企业在涉及使用国家秘密信息问题方面拥有全权）组织和实施对企业、机关和组织在俄罗斯联邦境内开展涉及使用国家秘密信息的专门鉴定。

关于与信息保护有关的技术及出口监督。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是全权负责技术侦察防范和信息技术保护的联邦执行权力机关，同时也是负责出口监督的特命全权机构。其职能是：（1）保障对信息领域国家安全有重要影响的信息与远程通信基础设施系统中的信息安全；（2）在俄罗斯联邦境内防范外国技术侦察；（3）保障俄罗斯联邦境内的国家秘密信息、其他有访问权限制的信息得到保护（运用非加密手段），防止这类信息通过技术渠道泄露，防止未经批准访问此类信息，防止发生出于获取、销毁、篡改和封锁访问此类信息的目的而恶意破坏信息（信息载体）的行为；（4）在研制、生产、使用和销毁非信息辐射装置、系统和设备时实施信息保护；（5）实施出口监督。

信息保护的跨部门协调。依据《俄罗斯联邦国家秘密跨部门保护委员会规则》

（2004）规定，国家秘密跨部门保护委员会负责协调联邦国家权力机关、俄罗斯联邦主体国家权力机关保护国家机密方面的活动。它有权：审查与国家秘密保护有关的法律文件；编制被赋予划定国家秘密信息文件资料范围全权的国家权力机关公职人员名单和被判定为国家秘密信息的文件资料清单；决定国家秘密文件的解密；审查国家秘密文件的对外移交等。

## 5 建立了对长期保护信息人员的社会保障制度

2006年通过的《俄罗斯联邦关于向允许长期接触国家秘密公民和国家秘密保护机构工作人员按月支付职务工资津贴的规则》规定：国家向长期接触国家秘密的公民每月支付职务工资津贴，津贴的支付以公民合法接触秘密信息的保密级别来确定。在规定每月的津贴数额时，要考虑到准许上述公民接触信息的信息量，以及这些信息保密级别的实际持续时间。这一法令的施行从社会保障领域进一步完善了国家信息安全保护的法制机制。

综上所述，俄罗斯无论是在宏观的政策引导还是在微观的法律规制领域都已经构建了比较完备的信息安全保护规则和制度。其中俄罗斯有关信息安全保护的许多有益的经验对我国的信息安全保护的立法具有很强的借鉴意义，特别是其中的涉密机构职能划分、涉密人员的管理及培养以及涉密机构协调机制对我国进一步完善信息安全保护法律体系建设大有裨益。在不断深化的国家法治化进程中，俄罗斯信息安全保护的法制化发展必将得到强化和完善，这是俄罗斯在融入国际社会进程中应对不断严峻的国际安全形势的必然选择，也是俄罗斯实施国家安全战略的重要组成部分和实现路径。BMS