密码技术 法律护航

密码法旨在规范密码应用和管理，促进密码事业发展，保障网络与信息安全，提升密码管理科学化、规范化、法治化水平。密码保护是指采用特定变换的方法将可读的信息变成不能识别的符号序列以及通过安全认证和数字签名等方式，防止对信息进行非法访问、篡改、伪造等行为的技术。我国密码法已于2020年1月1日起施行。为加强对此内容的了解，本期“域外之音”介绍的是国外关于保护密码的相关法律制度。

立法保障

密码技术除了具有保密功能外，还能够抵抗对手的主动攻击。密码技术既可以被善意地用于信息安全保护，也可以被恶意地用于掩盖犯罪行为。各国主要通过立法对密码技术进行管制和保护。

对密码进行立法保护，首先由一些区域性组织倡导，然后在一些国家推广开来。

在国际法层面，产生于二战后的巴黎统筹委员会一直将密码技术作为军事用品来管制。直到1991年，才允许密码技术有限地进行贸易交换。1996年7月,33个国家在奥地利维也纳签署《瓦森纳协定》，更新了密码进出口规则，实现了密码从军事到民用的战略转移。

欧盟从1992年起，相继颁布《数据保护指令》《关于个人资料传输和自由流动的保护指令》《电信管理法》《关于个人资料向第三国传递的指令》《关于在信息网络上收集和传送个人资料的保护指令》，规范了密码保护制度。

亚太经合组织于2001年制定的《数字亚太经合组织战略》提议，为确保在线交易法律的实施，应推行电子认证和数字签名，并对密码监管持促进发展的态度，同时支持密码的电子商务应用。

美国与密码保护相关的法律有《出口管制法》《武器出口管制法》《国际武器贸易条例》等，美国在密码政策制定及立法方面实行内外有别的密码控制政策。

加拿大于1998年颁布《电子商务的密码策略框架》，要求所有电讯运营商在接收法院命令时，为执法部门或国家安全机构保持解密的能力；作为对运营商责任的附加，责成密码服务提供商提供强制解密协助，所有用户禁止使用无密码恢复的密码。

俄罗斯于1995年4月3日发布《非授权加密禁令》，要求中央银行应当采取措施，确保商业银行在与中央银行（包括分支机构）通信时使用认证密码，未经许可的密码研发、生产、执行、操作会被禁止。

严格监管

在监管方面，美国的制度比较完善。美国建立了密码产品的科研、应用、技术革新等一系列管理制度，从源头上保证了密码产品的有序、可控和安全。

组织监管。美国由国家安全局对密码实行统一管理。国家安全局是密码工作的法定领导机构，主要负责编制美国国家机关和国防部通信密码方案、领导制定民商界通信保密标准政策、协调管理保密设备的制造使用、主持研究密码破译和网络监控等，确保美国政府对网络信息的控制权，提升应对网络威胁的能力。

科研监管。在密码科研方面，美国国家安全局专门联合全美教育委员会成立公开密码学研究小组，限制密码学术研究。任何学术团体和个人在发表密码学相关论文之前，应主动向美国国家安全局递交该论文。美国国家安全局有权对国内密码学术研究成果在公开发表前进行审查。

应用监管。美国政府要求加密产品采用“托管加密标准”。该标准规定，必须在加密产品中加入密钥恢复机制，以保证必要时执法部门方便获取明文，否则该产品将不允许推广使用。为此,美国在中央、州和地方建立了三级技术中心,以方便执法部门获得更先进的保密通信技术条件以及解密一些可能涉及犯罪的保密通信信息。

成品监管。美国国家安全局在产品制造方面，要提供需求标准和产品认证，要求研发工作必须由美国商业公司完成。这样做的目的，在于加快美国产品的更新换代，方便用户获得更加优质的密码服务。

技术审查

密码技术审查一般以进出口规定为依据，由监管机构进行检查审视，防止不应出口的密码技术出口到国外。

多部门参与。对包含加密模块的产品和加密软件的出口，俄罗斯联邦安全部门均要审查。产品是否包含加密，由联邦安全部门进行技术鉴定，鉴定后向国防部报告。该部门还要在30日内向经贸发展部报告结论，经贸发展部据此为加密产品的进口或出口发放许可证。

逐步放宽。法国按照欧盟1996年《电信管理法》，对欧盟以外的密码进出口实行严格的技术审查。2000年后，法国多次调整有关密码进出口监管规定，通过了多项法令减轻出口控制力度。2001年的《信息社会法案》对进出口监管进行了更大规模修订，主要包括：用于鉴别的密码可以自由进出口；非加密设备的进口无需申报；非加密设备的出口无需审查；对于加密用途的设备进出口需要进行技术审查，执行进出口程序，并规定处罚规则。

审查权受法律保护。美国由商务部负责密码进出口技术审查。2000年1月，美国政府将可自由出口的大量交易密码产品的密钥长度提升到64位。限制对外国政府出口强密码产品是美国政府的一贯方针。目前有古巴、伊朗、伊拉克、利比亚、朝鲜、苏丹和叙利亚等国属于美国严禁出口密码技术和产品的国家。

在1996年的一个案例中，一位教授认为，密码技术出口控制限制了他对外国学生讲授密码技术以及他与国际同行合作的自由，侵犯了他在国外的言论自由权。但是，美国第九巡回法庭判决政府关于密码限制的政策没有违反宪法。1999年9月20日，美国政府为此案举行听证会，结论仍然是密码算法技术在出口之前提交政府进行技术审查是必要的。

许可限制

密码进出口许可制度是指对符合标准的密码技术和产品发放资质认可证明或批件的规则。通过密码进出口许可制度可达到限制贸易的最终目标。具体有两种做法：直接列举许可范围或规定豁免许可范围。

直接列举许可范围。英国于2000年11月11日修改相关规定，允许任何用于个人计算机或便携式计算机使用的密码系统出口。许可证不允许出口用于加密或解密在线语音通讯的产品。加拿大规定，对于从美国进口的，不包括在出口控制清单中但处于美国出口规则监管下的密码，如果美国不允许出口，则不能从加拿大出口。在日本，对大于50000日元交易额度的密码出口，要求出口商必须获取许可证令。在韩国，加密设备进口需要商务部门、能源部门和安全部门联发的许可证。在印度，加密设备进口需要许可证，密码软件进口则无限制。

规定豁免许可范围。在俄罗斯，使用加密产品符合下列条件之一的，可以豁免许可：为商业用途的广播设备、商业电视或其他设备；专为银行和金融机构设计的作为终端组件的加密设备；专门为财政现金保护机械装置设计的设备组件；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。

美国从1998年12月31日起执行出口许可证例外规定，列出了可以出口的对象和范围。这些范围是：可以出口至美国公司的分支机构；可以出口45个国家和地区的处于银行列表的在线交易商，限于“促进交易商和消费者安全电子交易”；允许向45个国家和地区的商业机构出口仅限于公司内部独占使用的“可恢复产品”。

调查处罚

调查制度是指执法机关对密码进出口违规行为进行调查处理及对相关责任人进行处罚追究的制度。

印度于2000年颁布《信息技术法》,规定控制认证机构可以以维护国家安全或预防犯罪的事由，命令政府机构侦听通过计算机资源传输的任何信息；负责计算机资源的人员在执法机构指派时，应当提供技术便利并协助信息解密；违者可判处最高7年的监禁。

澳大利亚2001年通过的《网络犯罪法》规定，地方法官可以要求释放密码或解密加密数据，违者可处以6个月以下监禁。

美国中央情报局曾开发了一种锁定嫌疑人键盘、记录所有输入信息，以此方式获得解码密码的软件。前提是：当锁定嫌疑人后，要向联邦地方法官申请法庭命令，同意将该软件安装在嫌疑人的计算机上。

（据人民法院报）