网络数据安全成全球热点

近几年来，大数据和网络数据风光无限，成为各国政府、企业、科研机构等竞相追逐的“明星”。而随着移动互联网、云计算、大数据、物联网为代表的新一代信息通信技术与经济社会各领域、各行业的深度融合和跨界融合，相应的网络数据安全管理问题也日益凸显。

什么是网络数据

我国“网络数据”的概念第一次出现在全国人大常委会2015年公布的《中华人民共和国网络安全法（草案）》(以下简称《草案》)中。《草案》第65条第四款规定：“网络数据是指通过网络收集、存储、传输、处理产生的各种电子数据。”

国外法律规定中并无“网络数据”的定义，各国数据保护法都只对数据以及个人数据等相关概念进行了定义。例如，英国《数据保护法》只对数据下了定义，数据是指根据发出的处理指令自行运行的设备所处理的信息，为了由上述设备加以处理而记录的信息以及作为相关存档系统的组成部分，或为了成为相关存档系统的组成部分而记录的信息。

在实践中，网络数据还经常和大数据混用。维基百科将大数据定义为一个复杂而庞大的数据集。香山科学会议(技术型定义)则认为大数据是来源多样、类型多样、大而复杂、具有潜在价值但难以在期望时间内处理和分析的数据集。从定义理解来看，大数据是由无数的网络数据组成的数据集，通常二者也很难严格区分开来。

网络数据安全成为全球热点

随着网络数据价值的不断增加，针对网络数据的安全威胁也与日俱增，给数据安全保障带来了严峻的挑战，使很多国家对网络数据使用的态度发生了转变。“棱镜”事件前，网络数据开放逐年深化，针对跨境流动等的国际合作不断推进，注重开放成为国际网络空间数据使用的主流态度；而“后棱镜”时代，各国开始明确并不断强化网络数据安全保护，加强网络数据安全管理。

2015年9月1日，俄罗斯第149-FZ号联邦法《关于信息、信息技术与信息保护》生效。该项法律规定：俄罗斯公民的个人信息数据只能存于俄境内的服务器中，以实现数据本地化。2015年10月6日，欧盟最高司法机构欧洲法院作出裁决，认定欧盟委员会2000年通过的关于认可美欧安全港框架的决定(2000/520/EC)无效，使得美欧之间最重要的跨境数据传输方式丧失合法性基础。2015年10月，澳大利亚通过《电信(监控和接入)修正(数据留存)提案》，对数据留存做出强制性法律规定，要求电信运营商对电话、互联网、电子邮件的用户数据留存两年。2015年9月5日，我国发布了《关于印发促进大数据发展行动纲要的通知》，提出要加强大数据环境下的网络安全问题研究和基于大数据的网络安全技术研究，落实信息安全等级保护、风险评估等网络安全制度，建立健全大数据安全保障体系。

各国“施法”保护网络数据安全

总体来看，为应对日益严峻的网络数据安全问题，国际社会正在从法律法规、战略政策、标准评估、管理体制等方面下手，全面开展数据安全保障实践。

在法律法规方面，各国通过修订原有立法和制定新法为网络数据安全管理提供强有力的立法保障。英国对《2000年调查权规则法案》进行修正，改为《2014年数据留存和调查权法案》，要求通信服务提供商保留用户通信数据长达12个月，并且在执法部门提出合法要求时予以披露。美国于2015年6月2日正式出台《美国自由法案》，赋予电信运营商承接情报执法机构的电话数据搜集和留存职责，必要时按照特定程序向政府机构提供。2015年12月15日，欧委会、欧洲议会、欧盟理事会三方机构在立法进程的最后阶段，就欧盟数据保护改革达成一致，核心改革成果——《欧盟数据保护总规》即将正式颁布。新规继续坚守保护公民基本权利理念，全面提升个人数据保护力度，开创性引入数据可携权、被遗忘权，并特别针对大数据背景下的数据分析、画像活动予以严格规制。

在战略政策方面，各国顶层设计与政策落实并重，先后出台国家级战略规划，在促进数据发展的同时兼顾安全保护。英国于2012年6月发布《开放数据白皮书》，推进公共服务数据的开放；2013年10月31日又发布了《把握数据带来的机遇：英国数据能力战略》，制定了提升数据分析技术、加强国家基础设施建设、推动研究与产业合作、确保数据被安全存取和共享等举措。日本2013年发布《创建最尖端IT战略》，明确阐述了开放公共数据和大数据保护的国家战略；2014年，印度国家电信安全政策指导意见草案对移动数据保护作出规定；美国白宫2015年发布白皮书《抓住机遇，守护价值》，总结大数据中的隐私保护政策，提出发展大数据的具体举措和安全保障，加强数据管理。

在管理体制方面，各国主要分为政府主导和行业自律两种模式进行网络数据管理。政府主导型监管体制是最主要的管理模式，通常有较成体系的保护机制。如德国，专门特设保护机关——联邦数据保护委员会；荷兰专门特设保护机关——数据保护局；韩国行政安全部和韩国通信委员会共同承担数据安全行政监管职能。行业自律型监管体制的典型代表为美国。美国的监管体制可细分为以下两种模式：一是建议性的行业指引，由行业组织或商业实体制定行为指引或隐私标准，为行业内的隐私保护提供示范；二是网络隐私认证计划，要求具有隐私认证标志的网站必须遵守在线隐私资料收集的行为规则。

此外，各国还在标准体系、技术手段、安全评估等方面采取了相关措施。

安全与发展并重

在我国的“互联网+”时代，互联网与传统产业的深度融合使得操作系统更加复杂，各种数据海量增长，新情况、新问题层出不穷，网络数据安全和用户信息安全问题将更加突出。要坚持安全与发展并重的思路，重视互联网发展带来的数据安全风险。

一是要建设完善的网络数据安全监测评估、监督管理、标准认证和创新能力体系，加强针对信息系统设施、新型领域的安全监测评估和责任管理，推进安全标准的研究制定和实施。初步建立适应于发展需求的网络数据安全监管制度和标准体系，提升“互联网+”的安全保障能力。

二是充分重视互联网与政务、医疗、金融等各领域融合带来的数据安全风险，完善网络数据保护体系，加强安全管理和技术措施，包括建立数据分级、分类安全管理制度，加强跨境数据流动评估认证制度，明确相关主体数据安全保护责任。

（邮电）