热 点

关于网络安全法 你需要知道的几个问题

□王舒毅

2015年7月，《中华人民共和国网络安全法（草案）》（以下简称《草案》）面向社会公开征求意见，这是我国针对网络安全领域突出问题，以制度建设提高国家网络安全保障能力，掌握网络空间治理和规则制定主动权，维护国家网络空间主权、安全和发展利益的一项重要举措。《草案》的制定，标志着我国在立法层面完善国家网络安全战略部署、提高网络安全工作法治化水平迈出了重要步伐。

制定网络安全法的重大意义

一是应对当前我国网络安全严峻形势的迫切需要。一方面，中国互联网用户数量已跃居世界首位，网络和信息化的快速发展也带来了网络安全问题的严峻挑战。我国是网络攻击的主要受害国，境外针对我国关键信息基础设施的网络攻击威胁日益严重，云计算、大数据、物联网等新技术、新应用面临着复杂的网络安全环境。另一方面，网络情报窃密活动越发猖獗，各种有国家背景的针对我国的情报窃密活动大幅增加，敌对势力和境外情报机构利用网络技术优势，大肆窃取、刺探、搜集我国家秘密信息，甚至已达到无孔不入、无时不有、无处不在的程度。网络犯罪问题也日益凸显，通过网络获取、泄露甚至倒卖公民个人信息、侮辱诽谤他人、侵犯知识产权等违法活动时有发生。网络安全问题的严峻性、复杂性，迫切需要加快制定实施维护网络安全的基本法律，依法加强网络空间治理，规范网络信息传播秩序，惩治网络违法犯罪行为。

二是贯彻落实总体国家安全观的必然要求。2014年4月，习近平总书记在中央国家安全委员会会议上提出了总体国家安全观，强调“既重视传统安全，又重视非传统安全，构建集政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、信息安全、生态安全、资源安全、核安全等于一体的国家安全体系”。习近平总书记还在中央网络安全和信息化领导小组会议上作出“网络安全和信息化是一体之两翼、驱动之双轮”“没有网络安全就没有国家安全”的重要论断。网络安全是国家安全的重要组成部分，已全面渗透到国家的政治、经济、军事、文化和社会安全中，成为国家安全的“无形疆域”。通过立法加强网络安全工作，切实维护我国网络空间的主权、安全和发展利益，是全面贯彻落实总体国家安全观，实现国家长治久安的必然要求。

三是解决我国网络安全工作突出问题的重大举措。近年来，由于网络安全管理方面综合性、基础性法律缺位，有关网络安全战略统筹、体制机制、防护监管、科技研发等迫切需要通过立法予以调整、规范的方面，一直没有得到有力推进。网络安全工作中一些立法需求强烈的领域，如政务网络信息系统安全、关键信息基础设施保护、公民个人信息保护等，缺乏专门立法予以规范。与网络安全管理相关的调查取证、监督管理、舆情管控、应急处置、安全审查、国外产品市场准入等，还存在无法可依或法律依据不足等问题，给相关职能部门依法履行管理职责带来较大困难。制定出台网络安全法，有利于从根本上解决网络安全工作中的突出问题，将网络安全工作纳入法治化发展轨道。

制定出台网络安全法，有利于从根本上解决网络安全工作中的突出问题，将网络安全工作纳入法治化发展轨道。

《草案》的四大亮点

《草案》共分七章六十八条，包括总则、网络安全战略、规划与促进、网络运行安全、网络信息安全、监测预警与应急处置、法律责任和附则等部分，明确提出维护网络安全，必须坚持积极利用、科学发展、依法管理、确保安全的方针，处理好与信息化发展的关系；在网络设施设备安全、网络运行安全、网络数据安全、网络信息安全、监测预警与应急处置等方面建立和完善了相关制度；注意保护各类网络主体的合法权利，保障网络信息依法有序自由流动，促进网络技术创新和信息化持续健康发展等。通观全文，《草案》关于网络安全领域几大重点问题的政策落地和制度安排颇为引人瞩目，呈现出不少亮点。

第一，通过立法明确“国家制定网络安全战略”。面对当前网络安全的威胁与挑战，特别是世界主要国家纷纷调整安全政策和战略布局，出台网络安全国家战略，大肆抢夺网络空间规则制定权和“无形疆域”控制权的严峻形势，我国迟迟未能出台体现我国家利益诉求和重大安全关切的网络安全国家战略。《草案》设专章规范“网络安全战略、规划与促进”，明确了国家网络安全战略的基本内容，包括“明确保障网络安全的基本要求和主要目标，提出完善网络安全保障体系、提高网络安全保护能力、促进网络安全技术和产业发展、推进全社会共同参与维护网络安全的政策措施等”，并要求“国务院通信、广播电视、能源、交通、水利、金融等行业的主管部门和国务院其他有关部门应当依据国家网络安全战略，编制关系国家安全、国计民生的重点行业、重要领域的网络安全规划，并组织实施”，这为国家网络安全战略的加快制定实施铺平了道路，奠定了坚实的法律基础。

> 《草案》明确了国家网络安全战略的基本内容，将维护关键信息基础设施运行安全作为重点,并高度重视个人信息保护。

第二，将维护关键信息基础设施运行安全作为重点。在网络信息时代，关键信息基础设施运行安全直接关系国家安全和核心利益，因而各国普遍将保护国家关键信息基础设施作为网络安全立法的重点内容，列为网络安全保障各项行动措施的首要选项，给予最高优先级。从我国现实情况看，由于信息核心关键技术受制于人，以及管理方式、管理水平方面存在不足等原因，我国关键信息基础设施的网络安全风险隐患非常突出。《草案》在将基础信息网络、重要信息系统、军事网络和有关政务网络纳入国家关键信息基础设施范畴的同时，特别将“用户数量众多的网络服务提供者所有或者管理的网络和系统”纳入国家关键信息基础设施，予以重点保护，并作出对有关人员进行安全背景审查、实行容灾备份、对采购可能影响国家安全的网络产品和服务进行安全审查、重要数据国内存储以及定期检测评估、组织应急演练等一系列制度安排，必将有力推动我国关键信息基础设施网络安全保护工作。

第三，高度重视个人信息保护，维护公民合法权益。对收集、存储和使用公民个人信息的行为进行规范，依法保护公民合法权益，是各国网络安全立法的通行做法和重点内容。长期以来，我国在个人信息保护方面存在立法滞后、保护不力等问题，特别是一些网络运营者违规收集、使用甚至泄露公民个人信息、侵害公民合法权益的问题还比较严重。《草案》对加强个人信息保护、防止个人信息被非法获取、泄露或者非法使用予以重点关注，要求“网络运营者收集、使用公民个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意”，并规定了救济措施和相应的法律责任条款，反映了立法所坚持的问题导向原则，体现了我国对网络时代个人信息保护问题认识的深化。

第四，将一些实践中成熟的制度上升为法律。近年来，我国在网络安全保障方面做了大量卓有成效的工作，党和国家制定发布了一系列网络安全相关政策文件。《草案》将实践中一些行之有效、比较成熟的制度上升为法律，比如网络安全等级保护制度、网络实名制度、安全审查制度以及安全技术措施的“同步规划、同步建设、同步使用”等。通过将这些好做法作为制度固定下来，为开展相关工作提供了明确的法律依据，为维护我国网络安全提供了切实的法律保障。

有待完善的几个问题

我国网络安全领域立法尚处于起步阶段，很多制度本身的实践基础、工作基础并不充分，制定网络安全法很大程度上也是填补空白的应急之举，《草案》中的很多制度

安排还需要大量的配套法规制度予以补充完善。仅就《草案》条文本身来看，也有一些值得研究探讨和修改完善的地方。

（一）关于网络安全法的适用范围。《草案》第二条规定了网络安全法的适用范围，即“在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法”。网络空间的延展性、开放性和边界模糊的特点，使得网络安全问题具有突出的跨国性特征。因而网络安全法在适用范围方面具有区别于传统法律的特殊需求，是否仅限于“在中华人民共和国境内”的行为，建议借鉴和采用保护性管辖原则，适当扩大适用范围。2014年5月，美国司法部以“网络窃密”为由，引用美国法律起诉5名中国军官，虽然具有明显的政治目的，但也为我国网络安全立法提供了重要启示。

（二）关于网络安全职能机构的职责划分。《草案》明确了“国家网信部门负责统筹协调网络安全工作和相关监督管理工作”，但对工业和信息化、公安等职能部门仅原则性地规定了“依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作”。长期以来，我国网络安全管理职能部门众多，存在着相互职责交叉、条块隔离、难以协调联动等问题，严重制约了网络安全管理水平的提升。通过立法进一步明确相关部门在网络安全管理方面的职责定位和任务分工非常必要，可考虑设专章或者专节进行细化。从国际范围看，加强网络安全机构建设、明确相关机构职责划分，也是各国网络安全立法的一项重点内容。

（三）关于网络安全相关重要制度。《草案》在一些具体制度设计上也存在值得商榷的地方。第一，《草案》规定了关键信息基础设施运营者收集和产生的公民个人信息等重要数据境内存储制度，但对关键信息基础设施运营者并不能完全涵盖的大量国外互联网公司、网络安全公司，对其在中国提供网络服务过程中收集、产生的重要数据存储问题并未作出规范。从国际上看，2013年斯诺登曝光美国国家安全局与9大互联网公司合作、开展大规模网络监控活动以来，各国加强对重要信息跨境流转、存储的管控已成为趋势。2014年7月，俄罗斯国家杜马通过法案，规定互联网服务商必须将收集的俄罗斯公民个人信息存储在俄罗斯境内服务器，并告知存储这些个人信息服务器的具体地理位置，包括谷歌、Facebook、Twitter等在内的大型互联网公司被要求在2016年9月1日前在俄罗斯境内部署服务器，将俄罗斯公民个人信息转移至位于俄罗斯境内的服务器上，而不是存储于美国总部。第二，《草案》规定了因危害国家安全和社会公共秩序，处置重大突发社会安全事件需要，可以在部分地区对网络通信采取限制等临时措施的制度，对这样一项直接涉及公民、法人基本权利和切身利益的重大权力，是赋予国务院还是赋予全国人大及其常委会，也需要更为审慎稳妥的考量。第三，《草案》对网络安全人才培养、技术研发、人员安全背景审查、公私合作以及国际合作等国外网络安全立法普遍关注的重点问题，仅分别作了原则性规定，没有预留相应法规制度接口，难免留有遗憾。

> 我国网络安全领域立法尚处于起步阶段，《草案》中的很多制度安排还需要大量的配套法规制度予以补充完善。

（四）关于核心用语的定义。网络安全是一个新兴的管理领域，对相关概念的不同认识和理解将直接影响网络安全法的实施效果，因此《草案》在附则部分对法中使用的有关用语进行明确定义十分重要。但从目前对“网络”“网络安全”“网络运营者”“网络数据”和“公民个人信息”5个用语的定义来看，还存在着不全面、不准确、不完善的问题。比如，是对“网络”还是对“网络空间”进行定义需要认真考量。再比如，《草案》对“网络安全”的定义过于狭义，无法涵盖“信息内容安全”这一网络安全的重要方面，也没有涉及网络空间国家主权。又比如，《草案》中20余处使用的“网络安全事件”概念，多处使用的“网络攻击”“网络入侵”概念，涉及一系列重要制度设计，这些概念在日常使用中本身就存在多种理解，需要作出统一明确的界定。

此外，《草案》以“由国务院规定”“由国务院制定”以及国务院有关部门制定等方式，为网络安全相关配套法规制度预留立法接口10余处，虽然能促进网络安全法与相关法律法规相互衔接，但也反映出我国在网络安全工作的一些方面还没有成熟的制度能够直接上升到法律层面，从立法技术上看，过多的预留接口也会对法律本身的连贯性、完整性造成损害。■