论我国网络安全立法的双重定位及体系构成

于雯雯

[摘 要] 我国网络安全立法具有鲜明的中国特色，在总体国家安全观的指导下，既有国际背景下捍卫网络空间主权与维护国家安全的迫切需要，也有为国家开展网络空间治理提供基本法律依据的现实需求。基于“国家网络空间安全捍卫法”与“国家网络空间治理基本法”的双重定位，我国网络安全立法体系构成可以从三个维度观察，其一是网络安全法与国家安全其他领域中涉及网络安全的法律规范；其二是网络安全法与数据安全法的关系；其三是其他法律部门或领域中的相关法律规范。基于网络法制体系的发展健全，未来我国网络安全法将通过更加具有差异化和精细化的设计来凸显“国家网络空间安全捍卫法”定位，同时通过提供相应的原则性规范及法律适用链接来实现“国家网络空间治理基本法”定位。

[关键词] 网络安全国家安全；网络空间治理；双重定位体系构成
[中图分类号] D63 [文献标识码] A [文章编号] 1674-7453（2023）07-0066-10

当今，网络安全已成为重要的世界性议题。美、欧等世界主要国家和地区均通过强化国家战略和专门立法来加强网络安全保障。我国于2016年先后制定出台了《国家网络空间安全战略》和《中华人民共和国网络安全法》（以下简称网络安全法），加强网络安全的战略保障和法律保障。对于我国网络安全法的体系定位问题，目前理论界已有所论及。而随着数据安全法、个人信息保护法等涉网立法的相继出台，该问题愈加凸显。如何理解网络安全法与数据安全法、个人信息保护法等相关法律的关系，涉及我国网络安全立法的定位及其体系构成问题，需要引起学界的重视与探讨。本文尝试在既有理论研究成果的基础上，基于网络安全与国家安全的关系，以及网络安全

[作者简介] 于雯雯，北京市社会科学院法治研究所副研究员。

对网络空间治理的基础性作用，来分析我国网络安全立法的双重定位及基于此形成的三个维度的体系构成，并在此基础上尝试判析我国网络安全立法的未来发展走向。

一、国家网络空间安全捍卫法

（一）网络安全与国家安全的关系

国家安全是安邦定国的头等大事和重要基石，属于法治运行系统强规制的核心领域。①传统安全观把主权、领土、政治安全作为国家安全的重中之重，维护国家安全主要依靠军事力量和手段。随着人类社会不断发展和世界形势的不断变化，以网络安全为代表的非传统领域安全日益凸显，成为威胁国家安全的重要因素。面对国内外安全形势的复杂变化，我国提出了总体国家安全观，强调统筹外部安全和内部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全。[1]

在各种非传统安全领域中，网络安全愈加受到重视，并对国家安全具有重要意义。近年来，多国不断调整完善国家安全战略，确立安全战略目标，并规定优先关注事项，在国家安全和军事安全的全局战略高度突出网络安全的重要性，并以立法形式保障和促进网络安全的实现。如美国是世界上首个制定网络安全战略并将之纳入国家安全战略的国家，同时制定了《联邦信息安全管理法案》《网络安全增强法案》《网络安全信息共享法案》等来保障网络安全；欧盟一方面制定了《欧盟网络安全战略：一个开放、安全、可靠的网络空间》，另一方面先后制定了《网络与信息系统安全指令》《网络安全法案》等。我国亦在2016年先后制定发布了《国家网络空间安全战略》和网络安全法，加强网络安全的战略保障和法律保障。网络安全法第1条明确将“维护网络空间主权和国家安全”作为立法目的；第4条规定“国家制定并不断完善网络安全战略”。国家安全法第25条规定了维护网络与信息安全作为维护国家安全的任务要求。因此，我国网络安全立法首先应定位为国家网络空间安全的捍卫法，也是国家安全法治体系的重要组成部分。

（二）网络安全法将维护国家安全作为立法目的之一

尽管网络安全整体上与国家安全紧密相关，但单一网络安全事件并不必然引发国家安全风险。基于此，我国网络安全法的立法目的并未局限于“国家安全”，而是包括了国家安全、社会公共利益以及公民、法人和其他组织的合法权益在内的更加广泛的立法目的。②并细分关涉

①2013年11月9日，习近平总书记在关于《中共中央关于全面深化改革若干重大问题的决定》的说明中指出，国家安全和社会稳定是改革发展的前提。2014年4月15日，习近平总书记在中央国家安全委员会第一次会议上指出，国家安全是我们党巩固执政地位、坚持和发展中国特色社会主义的“头等大事”。2017年10月18日，党的十九大报告，进一步将“安全”作为新时代我国社会主要矛盾中人民美好生活日益增长的与民主、法治、公平、正义、环境等并列的六大需要之一，强调“国家安全是安邦定国的重要基石”。这些重要论述，明确了国家安全在新时代中国特色社会主义发展过程中具有“头等大事”和“重要基石”地位，不仅极其重要，而且是基础、是根基。《高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的讲话》（2022年10月16日）进一步指出：“国家安全是民族复兴的根基。”

②网络安全法第1条规定：“为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。”

国家安全与不关涉国家安全等不同情况分设不同的义务—责任水平。[①]并且在制度设计上体现了对国家安全的重点保护与强保护，主要体现在：

其一是网络安全等级保护制度。1994 年国务院颁布了《计算机信息系统安全保护条例》，明确提出："计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法由公安部会同有关部门制定。"2007 年公安部、国家保密局、国家密码管理局、国务院信息工作办公室联合发布了信息安全等级保护管理办法，规定信息系统的安全保护等级根据信息系统在国家安全、经济建设、社会生活中的重要程度，以及遭到破坏后对国家安全、社会秩序、公共利益及公民、法人和其他组织的合法权益的危害程度等因素确定，分为五级，从第一级到第五级的保护要求渐次提升。在此基础上，网络安全法以法律形式确立了网络运行安全基础制度，其中第 21 条和第 59 条确立了网络安全等级保护制度及网络运营者的基本义务。[②]

根据《信息安全技术 网络安全等级保护定级指南》（GB/T 22240–2020），在网络安全等级保护定级中，将受侵害的客体分为"公民、法人和其他组织的合法权益""社会秩序、公共利益""国家安全"三类。其中：（1）"公民、法人和其他组织的合法权益"定级分为一级（一般侵害）、二级（严重侵害或者特别严重侵害）；（2）"社会秩序、公共利益"定级分为二级（一般侵害）、三级（严重侵害）、四级（特别严重侵害）；（3）"国家安全"定级分为三级（一般侵害）、四级（严重侵害）和五级（特别严重侵害）。定级越高，对网络安全保护的要求也越高。由此可见，我国网络安全法的保护对象具有广泛性，不限于"国家安全"。[③]同时，网络安全法对三者的保护程度又存在区分，对"国家安全"实行高定级和强保护。

其二是关键信息基础设施保护制度。这是网络安全法新规定的重要制度之一。2021 年 7 月 30 日，国务院颁布了《关键信息基础设施安全保护条例》，将关键信息基础设施定位于"重要网络设施和信息系统"，并以列举方式明确了其行业属性和影响属性两大界定标准。[2] 将"国防科技工业"列为重要行业和领域，凸显了国家安全的影响属性；明确对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯罪活动；关键信息基础设施的运营者采购网络产品和服务可能影响国家安全的，应当依法通过国家安全审查。

其三是网络安全审查制度。网络安全审查是网络安全领域的重要法律制度，也是国家安全审查制度的重要组成部分。为了确保关键信息基础设施供应链安全，维护国家安全，我国于 2020 年出台了《网络安全审查办法》。数据安全法出台后，为了落实相关法律要求，保障数据安全，国家互联网信息办公室联合相关部门对《网络安全审查办法》进行了修订。根据该办法，关键信息基础设施运营者采购网络产品和服务，网络平台运营者开展数据处理活动，

①笔者认为，这种立法思路也与其第二重定位密切相关。详见本文第二部分内容。

②主要包括：（1）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（2）采取防范计算机病毒和网络攻击、网络侵入等危害国家安全行为的技术措施；（3）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（4）采取数据分类、重要数据备份和加密等措施，体现了对重要网络数据的重点安全保护要求。

③参见网络安全法第1条的立法目的。

影响或者可能影响国家安全的，都应当依法进行网络安全审查。[①]网络安全审查重点评估相关对象或者情形的国家安全风险因素。[②]

（三）网络安全法与国家安全领域其他立法中的相关规范

基于此，网络安全立法体系化的第一个观察维度应包括两部分内容：网络安全法与国家安全领域其他立法中关于网络安全的法律规范。其中，网络安全法不仅包括网络安全法，而且包括网络安全法的配套法规和规章，如网络安全审查办法、关键信息基础设施保护条例、网络产品安全漏洞管理规定等。而国家安全领域其他立法中相关规范，如国家安全法第25条规定："国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。"反恐怖主义法第18条规定："电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密等技术支持和协助。"第19条规定："电信业务经营者、互联网服务提供者应当依照法律、行政法规规定，落实网络安全、信息内容监督制度和安全技术防范措施，防止含有恐怖主义、极端主义内容的信息传播；发现含有恐怖主义、极端主义内容的信息的，应当立即停止传输，保存相关记录，删除相关信息，并向公安机关或者有关部门报告。网信、电信、公安、国家安全等主管部门对含有恐怖主义、极端主义内容的信息，应当按照职责分工，及时责令有关单位停止传输、删除相关信息，或者关闭相关网站、关停相关服务。有关单位应当立即执行，并保存相关记录，协助进行调查。对互联网上跨境传输的含有恐怖主义、极端主义内容的信息，电信主管部门应当采取技术措施，阻断传播"等。

（四）网络安全法与数据安全法的关系

随着数据对国家安全的愈加重要，网络数据安全问题凸显。根据国家安全法第25条及网络安全法第76条，网络安全包括"保障网络数据的完整性、保密性、可用性的能力"。对网络数据安全的保护散见于其制度设计之中。[③]网络安全法无论是在基本概念界定、总体要求还是具体制度设计方面都将网络数据安全纳入了考量，并予以规范。另外，网络安全法对"网络数据安全"的碎片化规范设计，又难以满足数据渐成"国家战略资源、企业关键资产与个人人格表征"[3]的体系化规范需求。在此背景下，我国加快了数据领域的立法进程。数据安全法已于2021年6月10日正式通过，2021年9月1日起施行。

从网络安全法与数据安全法的关系来看：首先，二者均是由全国人大常委会制定的一般法律，属于同一层级并行的法律，并非上下位法的关系；其次，二者同属安全法系列，采取以"风险"为基础的社会控制模式，[4]在对网络或数据进行分类基础上建立风险防范、评估和危机应对等安全制度。再次，二者均承载着贯彻总体国家安全观、维护国家安全的重任，对关涉国家安全的网络设施和信息系统、重要数据和国家核心数据实行重点保护和强保护。最后，在调整对象方面，二者在网络数据安全规范方面存在交叉。数据安全法所调整的数据

①网络安全审查办法第2条。

②网络安全审查办法第10条。

③网络安全法第10条、第21条、第27条、第34条、第37条。

是指任何以电子或者其他方式对信息的记录。其不仅包括电子形式的数据，还包括其他形式的数据；既包括通过网络处理的数据，也包括通过其他媒介处理的数据。

今后宜将数据安全法作为关于数据安全的基本的、主要的法律规范依据。首先，从立法初衷和定性来看，基于数据的重要性、复杂性和特殊性考虑,将“数据安全”作为独立于“网络安全”的特定领域进行单独立法调整规范。将数据安全法作为“数据安全领域的基础性法律”。[5]其次，某种程度上数据安全法亦是为了弥补网络安全法在网络数据安全方面的规范供给不足而制定。[6]作为后来立法，数据安全法需要解决网络安全法实施以来在数据安全方面的短板和不足，在吸收网络安全法的规范经验基础上发展完善。而且，作为“数据安全领域的基础性法律”，数据安全法不应该在“网络数据”这一重要规范对象方面出现空白或者借助于其他法律来规范。因此，整体上宜由数据安全法吸纳网络安全法的规范设计，未来网络安全法在网络数据安全方面或可提供法律适用链接。

从数据安全法的内容来看，亦体现了对关涉国家安全的重要数据及核心数据的重点保护和强保护。一是数据安全法将“维护国家主权、安全和发展利益”作为重要立法目的之一。①二是明确规定维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。②三是国家建立数据分类分级保护制度，加强对重要数据的保护。关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。③四是国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。④五是国家对于维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。⑤

二、国家网络空间治理的基本法

（一）加快网络法治建设的时代背景

我国网络安全立法起步较早，自1994年全功能接入国际互联网后，我国相继制定了《计算机信息系统安全保护条例》（1994）和《计算机信息网络国际互联网管理暂行规定》（1996）等来加强网络安全维护和管理。2000年以后，随着互联网的媒体属性、商业属性和社会属性的不断增强，电信条例、互联网信息服务管理办法等相继颁布，各部门开始重视和积极参与网络信息治理。[7]2000年全国人大常委会制定并发布了《关于维护互联网安全的决定》，进一步强化对互联网运行安全和信息安全的保障，特别是刑法保障。随着互联网应用场景的愈加丰富和逐渐普及，网络与现实社会的结合愈加紧密，成为现实社会不可或缺的组成部分，开启了我国网络全面社会化阶段。[8]网络法治建设也随之加快发展。特别是党的十八大以来，党中央高度重视网络空间治理及网络法治建设,《中共中央关于全面深化改革若干重大问题的决定》明确指出，“坚持积极利用、科学发展、依法管理、确保安全的方针，加大依法管理网络力度，加快完善互联网管理领导体制，确保国家网络和信息安全。”2014年2月27日，中央网络安全与信息化领导小组成立，通过设立更强有力、更有权威性的机构，来统筹指导网络安全与信息化工作，加强

①数据安全法第1条。
②数据安全法第4条。
③数据安全法第21条。
④数据安全法第24条。
⑤数据安全法第25条。

网络空间治理力度。2014 年 10 月党的十八届四中全会通过了《中共中央关于全面推进依法治国若干重大问题的决定》，绘就了依法治国的新路线。网络空间治理法治化是依法治国的应有之义。[9] 该决定明确指出要加强互联网领域立法，完善网络信息服务、网络安全保护、网络社会管理等方面的法律法规，依法规范网络行为。我国专门出台了《国家信息网络专项立法规划 2014—2020》，网络立法进入了快速发展阶段。

在加快网络法治建设的历史时期，网络安全法承载着规制网络空间乱象，为网络空间治理提供基本法律依据，维护网络空间安全和秩序的重任，具有网络法制体系基础性、综合性的初衷定位。首先，从立法必要性来看，《关于＜中华人民共和国网络安全法＞（草案）的说明》指出，网络和信息技术迅猛发展，在促进技术创新、经济发展、文化繁荣、社会进步的同时，网络安全问题也日益凸显，如网络入侵攻击；侵害公民个人信息、侮辱诽谤他人、侵犯知识产权等违法犯罪活动；传播扩散违法信息等。其次，从立法目的来看，网络安全法不仅旨在“维护网络空间主权和国家安全”，而且旨在“维护社会公共利益”，以及“保护公民、法人和其他组织的合法权益”。从国家维护网络安全的主要任务来看，不仅包括“采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏”，而且包括“依法惩治网络违法犯罪活动”，不仅包括“维护网络空间安全”，而且包括“维护网络空间秩序”。再次，理论界的研究评价亦指出，“网络安全法是中国互联网治理经验的总结，是中国治理互联网的理念展示，也吸收了其他国家和地区互联网治理的成功做法。其生效实施，不仅将开启中国互联网治理、互联网立法的新时代，也将对全球互联网治理产生重要影响。”[10]“中国通过网络安全法的出台，拥有了依法治网的‘总开关’，完备了依法治网的总括性。”[11]“网络安全法包括确定网络国家主权、确定国家监管机关、确定网络运营服务商的网络安全维护义务和权利、确立网民的基本权利和义务，因而这是一部网络空间治理的基本法。”[12] 综合以上，我国网络安全立法同时也是网络空间治理基本法，这是网络安全立法的第二重定位。其意义主要体现在两个方面：其一是体现了“安全”作为网络空间的基础性价值。安全的网络环境是开展网络市场交易、网络社会交往、网络文化传播的基础和前提。从我国网络法治进程来看，无论是将互联网作为技术工具的早期，还是之后网络的商业化、社会化阶段，网络安全都始终是网络立法中的基础和重要内容，并在不同时期得到立法的调整和加强。其二是体现了以人民为中心的发展思想。网络安全法集中体现了人民群众对个人信息安全、未成年人保护、违法不良信息规制等方面突出的立法关切和诉求。在相关法律制度尚未建立和完善的情况下可以为法律适用提供一般性法律依据。

（二）网络安全法的规范支撑

网络安全法的基本法定位来源于其对网络空间秩序价值的维护，彰显于网络信息内容的识别和多法域链接，以及对其合法性和正当性的评价。从制度设计来看，主要体现于“一般性网络运行安全义务”的相关规范，主要规定于“网络运行安全”章的“一般规定”中，适用于所有的网络运营者、网络产品及服务的提供者，无论是否关涉“国家安全”都需要依法履行。一般性网络运行安全义务是网络运行环境安全性的基本保障，同时也是网络空间治理在安全领域的基本要求。此外，总则及“信息安全”章也为网络空间治理提供了法律层面的

规范依据。

其一是对网络违法犯罪活动的概括性规制。总则第5条规定了“依法惩治网络违法犯罪活动”、第7条规定了“国家积极开展打击网络违法犯罪的国际交流与合作”、第10条规定了“防范网络违法犯罪活动”。其中所违之“法”并不限于网络安全法或者刑法上的违反网络安全保护义务相关犯罪，而是包括了所有对网络媒介下的行为具有规范意义的法律规则。

其二是未成年人的特别保护。总则第13条规定：“国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。”

其三是个人信息安全制度。网络安全法在《关于加强网络信息保护的决定》基础上，完善了个人信息安全制度，主要包括：建立用户信息保护制度（第40条），个人信息收集使用规则（第41条），网络运营者的个人信息保护义务（第42条），个人信息的删除权和更正权（第43条），禁止非法获取、买卖、提供个人信息（第44条），监督管理部门的保密义务（第45条）以及法律责任（第64条）。

其四是网络信息内容规制。网络安全法从法律层面为网络信息内容治理提供了法律规范依据，主要包括推动传播社会主义核心价值观的倡导性规范（第6条）、规定内容底线的禁止性规范（第12条）、网络运营者对用户发布信息的管理义务（第47条）、网络运营者未尽管理义务的法律责任（第68条）四个条文。如学者所言，这是我国首次以法律位阶规定的传媒内容底线，而以往传媒禁载、禁播条款都只是由行政法规、部门规章加以规定。[13]而网络安全法规定网络信息内容规制亦具有立法上的传承性。①

（三）多部门/领域法发展的规范支撑

网络安全法是我国较早完成的一部网络专门立法，此后我国还先后制定出台了数据安全法、个人信息保护法等专门性法律，而且在既有传统部门法的制定或者修订过程中，也会增加专门规范信息网络的内容，如民法典、刑法、未成年人保护法等，这些立法规范内容共同构成了我国网络空间治理的规范依据，规范网络空间主权范围的人际行为或关系的法律秩序。因此，我国网络安全立法的第二重定位将在法律适用中得到多部门/领域法发展的规范支撑。如网络违法犯罪将得到社会治安处罚法、刑法的规范支撑；未成年人网络保护将得到未成年人保护法的规范支撑等。

对于个人信息保护问题。2021年8月20日，十三届全国人大常委会第三十次会议审议通过了个人信息保护法，其是我国首部个人信息保护方面的专门性法律。一方面，个人信息保护法是综合性法律，它既不是作为民法典特别法的民事单行法，也不是单纯的行政管理法，而是针对个人信息保护的特点，综合运用强制性规范、禁止性规范以及行政责任、民事责任等多种法律责任对个人信息处理活动进行规范的法律；另一方面，个人信息保护法是个人信息保护领域的基本法律，它是全面系统地保护个人信息权益与调整规范个人信息处理活动的法律。[14]可见，将个人信息保护作为独立于网络安全的领域进行专门立法规范的思路十分清晰。从规范层面来看，个人信息保护法吸收了

①主要体现在：1994年《中华人民共和国计算机信息系统安全保护条例》第14条、1996年《中华人民共和国计算机信息网络国际联网管理暂行规定》第13条、1998年《中华人民共和国计算机信息网络国际联网管理暂行规定实施办法》第20条、2000年《全国人民代表大会常务委员会关于维护互联网安全的决定》第7条。

网络安全法的相关规范，并进行了细化、修正和完善。[①]因此，无论是从立法意义还是从规范层面来看，个人信息保护都是独立于网络安全的立法调整领域，个人信息保护法是该领域的基础性、专门性法律。从个人信息保护法与网络安全法的关系来看，个人信息保护法并非网络安全法的下位法或者配套法，它们是彼此独立的两部法律。对于个人信息的安全问题，个人信息保护法亦已提供了基础性规范依据，该法第 9 条规定了个人信息处理的“安全原则”，第 51 条、第 57 条提供了相应的制度支撑，防止未经授权的访问以及个人信息泄露、篡改、丢失。网络安全法修订中可调整为仅提供法律适用链接。

对于网络信息内容治理问题。网络信息内容治理不仅涉及维护网络文化安全的国家安全内容，还涉及宪法上的公民权利，具有相当的复杂性与敏感性。应该说，网络信息内容治理的范围较之网络安全法“信息安全”的内容更加广泛，对于网络信息内容治理的法律依据，宜从宪法的高度以及传媒法治建设方面进行完善。网络安全法的立法思路和规范依据当属权宜之计。由于我国传媒规制的传统以及传媒法治的发展情况，违法有害信息规制内容可能仍将存在于网络安全法中，为相关领域的执法活动提供法律层面的规范支撑，但是从长远发展来看，这部分内容由专门的传媒立法来调整会更加妥当。因为传媒规制不仅关涉安全，而且关涉知情权、表达自由和舆论监督，这三者构成了传媒规制的三大基石，也是实现民主与法治社会的权利基础，[15] 因此立法调整需要更具平衡性。

由上可知，随着我国网络法治体系的不断发展完善，在网络安全立法以外的其他法律部门或者法律领域立法与网络安全立法之间存在一定交叉，也会涉及网络安全规范，这部分内容也应该作为我国网络安全立法体系的组成部分，但是就多法律部门或法律领域本身而言，可能涉及多维法律价值的考量与平衡，因此整体这些法律部门或者领域应独立于网络安全立法体系。

结 论

我国网络安全立法具有“国家网络空间安全捍卫法”与“国家网络空间治理基本法”的双重定位。从体系构成来看，我国网络安全立法体系可以从三个维度来观察：其一是网络安全法与国家安全其他领域中涉及网络安全的法律规范；其二是网络安全法与数据安全法的关系；其三是其他法律部门或领域中的相关法律规范。同时，从义务—责任视角来看，网络运营者均需承担一定的网络安全义务，但是因为所运营网络所属领域与国家安全、社会公共利益、人民合法权益的关系及其程度不同，其网络安全保护义务的水平和内容存在差异。违反网络安全义务可能导致行政责任、民事责任及刑事责任多种责任，而且责任的程度也存在差异。[②]另外，从监管方—被监管方视角来看，有限的国家监管力量需要在泛在的网络安全保护的基础上有所侧重。而被监管人则需要更加明确的网络安全义务标准以及合理的成本投入。

---

①如网络安全法第74条、第59条。

②具体包括：网络安全法第40条对应于个人信息保护法第11、58条；网络安全法第41条对应于个人信息保护法第5、6、7、13条；网络安全法第42条对应于个人信息保护法第9、51、57条；网络安全法第43条对应于个人信息保护法第46、47条；网络安全法第44、45条对应于个人信息保护法第10条；网络安全法第64条对应于个人信息保护法第66条。

基于网络法制体系的发展健全，未来我国网络安全法将通过更加具有差异化和精细化的设计来凸显第一重定位，同时基于第二重定位提供相应的原则性规范及法律适用链接，进一步强化和完善网络安全风险识别与预警、监测与评估、处置与应急、安全认证等关键环节规则设计。重点包括：一是细化分类。核心关切在于明确关键信息基础设施及国家核心数据的范围，从国家战略、安全保护义务、强制性标准、监管资源分配等方面给予重点和强保护。考虑一般企业特别是中小企业在网络安全管理方面的成本和能力，从义务水平、标准推荐、资金投入等方面给予相应的鼓励与支持。形成多层次、差异化、标准化的网络安全保护义务体系。二是信息共享。尽管网络安全法第39、25、51条涉及“信息共享”“信息报告”和“信息通报”，① 但规定过于原则，在主体、行为性质、程序、责任等方面存在差异和空白，有必要在借鉴其他国家和地区经验的基础上予以整合细化，建立健全及时有效的一体化信息共享制度。[16][17] 三是国际合作。各国尽管在风险认知、管理制度、监管措施等方面会存在差异，但基于网络安全风险的合理界定，这些认知分歧将更容易获得缓解并达成共识。在网络安全信息共享与全球应对方面更易于取得切实的合作效果。四是人才培养与技术创新。一方面，进一步完善网络安全人才教育培养、职业保障、网络安全技术研发等方面的配套制度。另一方面，进一步强化和完善网络安全技术准则支撑。基于网络安全的技术性特征，网络安全的保障和能力提升离不开网络安全的技术标准化。将行业最优实践定期转化为相关标准，并根据网络安全等级定级及是否为关键信息基础设施而采取强制性标准或者推荐性标准，将成为未来网络安全领域规则供给的又一重要来源。

[参考文献]

[1]习近平.高举中国特色社会主义伟大旗帜 为全面建设社会主义现代化国家而团结奋斗——在中国共产党第二十次全国代表大会上的讲话[EB/OL].中国政府网，https://www.gov.cn/xinwen/2022-10/25/content_5721685.htm，2023-07-11.

[2]中国信息安全测评中心.以关键信息基础设施安全防护筑牢网络安全之基[J].中国信息安全,2021(9).

[3]许可.《数据安全法》：数字时代的基本法[N].经济参考报,2021-06-22.

[4]翟志勇.网络安全法的体系定位[J].苏州大学学报（哲学社会科学版）,2021(1).

[5]关于《中华人民共和国数据安全法（草案）》的说明——2020年6月28日在第十三届全国人民代表大会常务委员会第二十次会议上[EB/OL].中国人大网，http://www.npc.gov.cn/npc/c30834/202106/2ecfc806d9f1419ebb03921ae72f217a.shtml，2021-11-16.

[6]黄道丽,胡文华.中国数据安全立法形势、困境与对策——兼评《数据安全法（草案）》[J].北京航空航天大学学报（社会科学版）,2020(11).

[7][8]李欲晓等.论我国网络安全法律体系的完善[J].中国工程科学,2016(6).

[9]于雯雯.网络治理法治化是依法治国的应有之义[N].学习时报,2017-07-10.

[10]王四新.《网络安全法》：互联网治理的总动员令[J].人民论坛,2016(12).

[11]赵宏瑞等.中国《网络安全法》的立法特色与国际影响[J].中国信息安全,2018（7）.

①网络安全法第39条规定“促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享”；第25条规定网络运营者应“按照规定向有关主管部门报告”网络安全事件；第51条规定“国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。”

[12]程琳主编.中美网络安全比较研究[M].北京：中国人民公安大学出版社,2017:97.
[13]魏永征.基于《网络安全法》的传媒法治建设探究[J].社会治理,2020(3).
[14]程啸.个人信息保护法理解与适用[M].北京：中国法制出版社,2021：7.
[15]王军.传媒法规与伦理（第二版）[M].北京：中国传媒大学出版社,2021:32.
[16]李建伟.美国网络安全监控战略与法制变迁及其启示[J].北京航空航天大学学报(社会科学版),2020(5).
[17]刘金瑞.欧盟网络安全立法近期进展及对中国的启示[J].社会科学文摘,2017(6).

责任编辑：林珊珊

On the Dual Positioning and System Composition of China's Cybersecurity Legislation

Yu Wenwen

[**Abstract**] China's cybersecurity legislation has distinctive Chinese characteristics. With the holistic view of national security, it has the urgent need to defend cyber sovereignty and national security in the international context. It also has the practical need to provide basic legal basis for the country to carry out cyberspace governance. Based on the dual positioning of "national cybersecurity defense law" and "national basic law on cyberspace governance ", the constitution of China's cybersecurity legislation system can be observed from three dimensions. The first one is from the perspective of the relations between cybersecurity law and the legal norms related to cybersecurity in other areas of national security. The second one is from the perspective of the relations between the cybersecurity law and the data security law. The third one is from the perspective of the relevant legal norms in other legal departments or fields. Based on the development of network legal system, China's cybersecurity legislation will highlight the positioning of the "national cybersecurity defense law" through more differentiated and precise design in the future. At the same time, it will realize the positioning of "national basic law on cyberspace governance" by providing principle norms and legal applications.

[**Key Words**] Cybersecurity;National Security;Cyberspace Governance;Dual Positioning System Composition