【信息经济与管理】

我国信息安全保护制度反思
——以领网权的维护为切入点

王志刚,陈丽娜
(重庆邮电大学 网络空间安全与信息法学院,重庆 400065)

摘 要:随着网络技术的飞速发展,网络空间与现实空间的交融不断加深,网络主权及信息安全等问题不断涌现,各国利益深受侵害。领网权是信息通讯技术覆盖下国家主权的延伸,对各国领网权的有效维护有助于推动全球信息安全保护的一体化,促进"网络命运共同体"目标的实现。如今,领网权问题越来越突出,5G通信、人工智能、工业互联网等新型信息技术的运用对全球信息安全保护提出了前所未有的挑战。深化领网权的证成研究有利于维护网络空间的稳定,加快网络基础设施建设,推动网络安全国际法律体系的构建,并对实现我国治理能力现代化和完善信息安全保护制度具有重要意义。

关键词:网络空间治理;领网权;信息数据保护;信息安全
中图分类号:D92 **文章编号**:1673-5420(2021)03-0037-10

2015年,习近平总书记在第二届世界互联网大会上首次提出"构建网络空间命运共同体"[1]。这是我国根据网络技术发展和国际政治局势走向,从全人类整体和长远福祉出发对全球网络空间治理提出的"中国方案"[2]。各主体只有为了网络安全共同努力,才可能构建全球共享的安全网络环境。但是,近年来,各国以自身安全优先,为大力提升网络能力不断地以各种方式试探他国实力底线,带来了大量安全威胁和隐患。从过去的互联互通与合作到如今所谓的"碎片化"与博弈是各国关系悄无声息的转变[3]。与传统主权领域划分的方式不同,网络空间并不存在物理性疆界,网络数据可跨国自由流动。当前,亟需构建更完善的权利保护机制以应对复杂严峻的网络安全态势,共同打造

收稿日期:2020-07-11 **本刊网址**:http://nysk.njupt.edu.cn
作者简介:王志刚,教授,博士,研究方向:网络法学、证据法学。
基金项目:国家社科基金重大项目"建立健全网络综合治理体系研究"(20ZDA062)

有序的国际网络环境。

一、领网权——主权国家网络主权的效力边界

(一)从网络主权到领网权

随着网络社会与现实社会的交互愈加频繁,世界战争的战场已逐渐延伸至网络空间。2013年,斯诺登曝光“棱镜计划”,揭秘美国秘密利用超级软件监控网络、电话或通过短信监控有关国家机构和上百万网民的邮件、即时通话及相关数据。2018年,巴基斯坦研究人员发现由俄罗斯资助的名为“Turla”的黑客组织发起新版本COMpfun恶意软件,通过HTTP状态代码来控制受感染的主机以从事间谍活动,窃取他国的秘密信息。信息技术高速发展带来便利的同时,各国国家主权的维护在网络空间遭遇了前所未有的挑战。领网主要指国家主权扩展到网络空间,《网络空间独立宣言》的起草人约翰·佩里·巴洛曾宣称,“工业世界里的各国政府们:你们在网络世界中不受欢迎,你们在这里没有主权。网络世界不在你们的国境之内”[4]。但笔者认为,网络空间并非孤立于现实社会而存在,随着网络社会与现实社会的联系愈发紧密,网络空间与现实社会逐渐呈现出某种呼应关系,作为新兴疆域的网络空间不是法外之地,同现实社会一样,必须始终坚持维护法治和国家主权。

网络空间本身具有的延展性和包容性强等特点使得网络主权的概念在使用上过于泛化,难以准确指向某一国家。如今,亟需制定一个统一的标准,以此来划定各国的网络主权,并进一步减少网络冲突的发生[5]。在网络主权之外再提领网权,是由于其所表征的权利疆界性特征可保障各国在特定疆域内行使国家主权,以解决网络空间的归属问题。“领网”这一表述具有确定疆域范围的作用,可使一国主权在网络空间得以实现,更符合国际法理。“领网权”将国家“网络主权”提升至同领土、领空、领海同等的战略高度。

(二)领网权的特点

1.权利内容的综合性。领网权是国家主权在虚拟空间的延伸,其内涵包含四个方面:其一,领网平等权。主权国家在国际社会享有平等主权,禁止以任何形式侵犯他国领网权。其二,领网管辖权。国家有权在本国领网领域内根据自身发展需求自主建设基础通信设施以及制定网络安全保护体系,不受他国干涉。其三,领网独立权。国家依法在一国领网领域内自主处理对内和对外事务,不受他国干涉。其四,领网自卫权。一国在遭受他国网络攻击和网络威胁时可采取必要措施以抵御他国的侵害。

2.权利范围的复合性。传统主权维护具有很强的地域依赖性,但是网络空间具有无

边界性,显然难以按照传统划分标准界定领网的范围。领网权是以网络空间活动及网络基础设施为管辖内容的,据此,笔者认为可按照两分法确定领网权的疆界范围:其一,按照属人主义。以个人的国别、组织的注册地为标准,国家对于享有该国国籍的用户,可监测其行为并对相关网络流通数据行使领网权。其二,按照属地主义。建立一个对主权国家进行高级网络地址分配的技术体系,高级地址的差异就是主权国家在逻辑网络域的边界[6]。

3.权利场域的特殊性。网络空间这一虚拟场域传输的是以 0,1 为代码的数据流,网络基础设施(硬件)、软件以及设施使用者是通过网络被联系在一起的,其信息数据的流通飘忽不定。而权利存在之场域虽然具有虚拟性,但并非完全独立于现实世界,它需要现实空间的技术支持和人员维护,具有现实性。网络攻击并非只对虚拟场域产生影响,其对现实社会造成的侵害也是显而易见的。可以说,网络空间是无法独立于现实社会而存在的,对虚拟空间发起的网络攻击所造成的不利影响必将蔓延至现实社会。

4.攻击来源的复杂性。国家计算机网络应急技术处理协调中心(CNCERT)最新发布的 2020 年第一季度我国 DDoS 攻击资源分析报告中主要分析的攻击资源包括:控制端资源、肉鸡资源、反射服务器资源、跨域伪造流量来源路由器。在四种攻击资源中,发起 DDoS 攻击的控制端资源、反射攻击资源中 NTP 反射服务器资源的数量境外占比大比例超过境内。前者境内外控制端占比分别为 5.6%和 94.4%,后者境内外控制端占比分别为 36.4%和 63.6%。相较而言,由于物理空间的有形属性以及人类行为模式的规律性,现实行为侵害社会秩序的行为来源、活动方式具有单一性。但网络空间疆域的虚拟性、代码组合的无限性、数据流传输的不确定性等特点导致发起攻击的网络资源形式更加多样、组合更为复杂,进而一国所遭受的来自境内外攻击的来源资源就更为复杂。

二、网络空间法律性质学说

某一特定的网络空间能否被划入一国领网范围,涉及网络空间法律性质的问题。世界各地学者从不同的角度出发,对网络空间法律性质进行了界定,逐渐发展出以下四种主流观点。

(一)否定说

否定说认为,网络空间虽然理论上可以由国家通过控制端口的形式实现信息监管,但网络标准化的协议形式使得信息流通和接收变得极为不可控,而且鉴于几乎所有国家都已经融入了以互联网为核心的全球一体化中,国家也不可能将本国网络空间从全

球互联网中割裂出来[7]。该学说主张网络空间不属于一国管辖范围而属于全球公域,代码规则是网络空间的唯一法则。在实践中,以美国为首的部分网络发达国家支持该学说,网络实际变成了这些网络强国挑战其他国家网络主权的工具。

(二)肯定说

该学说认为,网络空间治理应被视为全球治理的新领域,领网权是国家主权在网络空间中的自然延伸,网络空间不是法外之地。该学说有利于领网及领网权概念体系的构建。当前大多数国家已基本接受网络主权的概念,国际社会和世界大部分国家对于上述理念在立法中均有所体现。例如,2003年国际电联"信息社会世界峰会"通过的《日内瓦原则宣言》中关于网络主权的表述;联合国成立的"信息安全政府专家组"对网络空间国家主权等概念达成共识;中国在2017年在颁布的《网络安全法》中首次以法律形式确立了网络空间主权的概念。

(三)居中说

有学者将网络分为全球公域和主权管辖区域两个部分,针对互联网的三个逻辑分层的特点,将物理层级中支撑起整个互联网的基础设施以及规则层面视为全球公域,而将各国连接互联网的设备以及内容层面归属于国家主权的管辖对象。在此基础上,进一步依据海洋治理模式提出了相应的治理原则,即绝对的公域行动自由和相对的私域行动自由原则。他们提出,将网络公域的治理权利交给联合国[8]。全球混合场域说在认可国家独立领网权的前提下,主张存在网络公共领域,对该网络领域不由特定国家享有主权,而由国际组织联合国管控。

(四)自治说

该学说认为,网络空间能够根据ICANN(互联网名称与数字地址分配机构),IETF(互联网工程任务组)制定的规则,实现自治[9]56。例如,约翰·佩里·巴洛认为:"网络空间具有天然的虚拟属性,是独立于任何一个国家而存在的,因此不受各国政府规制,可实现空间自我管理。"[4]该学说忽略了网络的社会属性,将网络空间与现实社会彻底分离,认为网络世界完全独立于现实社会而存在。随着网络社会与现实社会的深度融合,纯粹网络空间的自我管治是不现实的。

三、新型信息技术环境下的信息安全保护

(一)5G通信技术带来网络安全维护新挑战

5G时代的到来,人工智能等新型信息技术在为我们带来便利的同时也使得信息安

全保护问题越来越复杂,并进一步导致各国网络空间安全治理受到了更多阻碍。与此同时,国家主权逐渐从传统物理领域延伸至新疆域,在此疆域(领网)所形成的领网权问题伴随而生,领网权的维护受到了新型信息技术发展的双面影响。现阶段,我国的网络空间治理主要通过“政府主导+行业配合”的二分体系来实现。其中政府主要通过制定法律法规、设置互联网行政机构,以及掌握各种网络控制技术来达到网络治理的初步效果;行业配合治理即互联网行业对于自身行为的监控与约束。网络空间依靠政府主导、行业自律的治理模式取得了不少成效,但随着新型信息技术的高速发展,网络治理问题越来越复杂,传统的治理模式已然无法满足当前新疆域的有效治理需求。

5G 通信技术具有一定的开放性,在发挥其技术优势的同时也使得网络空间治理面临更大的安全挑战:更多的终端在底层被连接,增大了泄露用户信息的概率;海量数据在悄无声息的情况下被各个终端所采集,由此引发的安全漏洞逐渐增加,更易被网络黑客所攻击。5G 通信技术对一国领网权维护的影响可从内外两方面来分析:从外部视角来观察,5G 通信技术对于数据流量的“吞吐量”是原有 4G 网络的一千倍之多,数据上传和下载更加便捷快速,可以承载的用户也更多。这意味着攻击方的攻击能力将大大加强,一国受到的来自境内外的 DDoS 等网络攻击将逐渐增多。从内部视角来观察,5G 使用异构网络易产生大量数据,更易遭受网络攻击。目前,我国对信息技术领域所遭受的威胁和攻击仍缺乏一套先进的应对体系,必须不断加强国家重要基础设施建设和突破信息领域核心技术以切实维护国家的领网权。

相较于技术和产业能力处于相对弱势的发展中国家,以美国为首的西方国家在网络空间的文化霸权主义持续存在,它们对全球互联网运行的控制对各国的网络安全形成了重大威胁。网络发展早期以技术治理为特征,网络运行的各种技术规范和标准成为网络治理的重要内容,这导致以技术见长的发达国家以各种方式排除乃至阻断发展中国家实质性介入网络空间治理。当前,在网络空间除了规范技术标准之外,更需要的是对表层用户的各种网络行为进行规制。笔者认为,应在联合国框架下出台具有普遍约束力的正式法律文本,推动网络空间治理的法治化进程。当前,对于 5G 发展具体趋势各国虽然显现出不同倾向,但均出台相关政策文件,支持本国 5G 发展。我国应充分利用“数字丝路”建设的契机,凝聚和团结技术能力相对弱小、对网络空间高度依赖却不满美国网络霸权的发展中国家,深化合作;积极参与《信息安全国际行为准则》草案的讨论;学习和借鉴发达国家与地区的网络法治化实践,加强国际合作;不断完善 5G 涉及的基础设施建设、信息安全管理、行为合规等内容的法律法规,实现有法可依。

另外,应当加强 5G 网络中的信息安全管理,对此,建议使用同一框架下的“双向认

证”以提高数据接入过程的安全性。最好使用分散管理的方式,在不同的数据接入点不要使用同一密钥,以防止集中攻击的发生。对于接入设备终端可以在设备中下载签约凭证和二次认证来保证数据安全,对于有特殊要求的数据可以定制专用的安全芯片和相关的软件来保障安全[10]。我国学者魏垚等提出:“5G网络组网灵活,根据网络特点对网络进行切片管理,每个网络切片由网络管理中心分配的ID,接入终端通过切片网络ID进行验证接入,各个网络切片独立进行接入网络数据监控,实行异常上报,逐步通过对网络的切片管理实现统一的网络安全防御体系。”[11]应明确设备供应商、运营商等的行业责任,督促其制定网络安全事件应急预案并及时处置系统漏洞、计算机病毒、网络攻击等安全风险,树立行业标杆作用,实现多部门配合的综合治理。

(二)人工智能带来数据安全新挑战

领网权的保护,究其本质是对一国特定网络空间数据所有权的保护。现如今,云计算、大数据技术相继得到广泛应用,人们以更为便利、高效的方式收集数据信息,但信息收集的渠道和手段却没有受到应有的限制。人工智能时代数据从输入端到输出端所面临的诸多问题,给一国领网权的维护带来了巨大的挑战。

从数据输入端进行分析,人工智能时代对海量信息数据的需求剧增。挪威数据保护局曾解释说:“人工智能工作的基础是大量的数据信息数据,人工智能的深度学习需要依赖大数据提供海量的个人信息。人工智能工具对信息数据的需求量是无穷尽的,越多的信息数据支撑,人工智能产品的精确度和准确率越高。”[12]人工智能的基础是数据,人工智能技术的应用质量和工作效率会因数据的不足而下降。此外,深度的分析必须尽可能地进行数据收集以形成牢固的数据基础,这是防止人工智能出现“失误”的基础性前提。而精确的分析结果需要大量的信息收集和处理,从运作原理上看,庞大的信息输入工作很难避免在有意或不经意间侵犯他国主权。

从数据输出端进行分析,目前,人工智能不同程度地在安防、金融、医疗、政务、交通等多领域得到运用。其中人脸识别等生物特征信息识别技术是人工智能的关键技术,其生物识别信息的高度敏感性引发了各国关于基本人权问题的讨论。该技术可轻易实现对个人隐私的侵犯,当个人信息被收录后,其通过信息筛选处理、精准画像分析,以及深度运算再将整合分析的信息予以输出。遗憾的是,当前对输出端的数据使用并未建立完整的规范体系,轻易地造成了对他国或地区领网权的侵犯。

由计算机算法驱动的人工智能需要庞大的数据库进行支撑,数据信息的收集、存储、利用等过程存在一系列的安全风险。人工智能侵犯信息数据,大多表现为被第三人利用实施侵权行为,侵权主体是人。对于人工智能被动实施侵权行为的情形,可从信息

数据的流向来思考维护路径:首先,数据输入端。当前,很多智能服务软件为获取用户数据,用变相的方式强制读取用户基本信息。对此,必须坚持个人信息数据的合法收集,即应基于用户的自愿而进行,否则大数据算法的特性必将导致更多的信息被泄露,造成严重后果。其次,必须建立足够安全的防火墙防止所储存的海量数据被窃取用以进行非法活动,同时建立人工监管和智能监管相结合的监管处罚机制,督促数据保管者主动保护所掌握的数据信息。最后,在数据输出阶段,必须合法且有限制地使用信息数据,并对使用的途径和方式加以规制。

信息技术是一把双刃剑,其在发展过程中所带来的问题必将由于技术的不断进步而得以缓解甚至彻底解决。但是,人工智能超越人类智慧而实施自主侵权的情形在未来是有可能发生的。此时侵权行为的实施主体并非现实的人,采取外部维护形式——建立安全保护制度,通过立法、政策以及多方面综合治理等方式来防止信息数据侵权的成效并不显著,法律无法让信息技术担责。对于此类侵权方式,最好的控制手段理应是侧重内部维护形式——交由技术解决,信息数据安全的维护必须依靠技术层面的不断进步,从技术源出发。

(三)工业互联网技术带来基础设施安全新挑战

《乌镇展望 2019》指出,“新型勒索软件、电子邮件数据泄露、信息盗窃等在全球范围内持续产生严重危害,各类网络攻击事件对全球经济社会发展造成的影响越来越大。5G、智能软件、区块链等新技术带来新的安全威胁,对关键信息基础设施实施网络攻击、智能杀伤性武器生产和应用等安全隐患触动各国神经”[13]。技术仍然是网络治理的重要手段,特别是在保护网络信息安全、打击网络犯罪方面,技术防范可以在网络治理体系中发挥常规性、基础性的作用。物联网通过无线网络将数据传输至各个终端,以实现人类对物品的远程控制。该技术给人们的生活带来了便利,但也产生了信息安全风险。

物联网对一国领网权维护提出的首要挑战在于信息收集过程中所产生的安全隐患问题。具体而言,其一,相比传统互联网,物联网的信息数据收集与传输常常会“秘密”进行,一旦进入物联网,使用者将会被贴上 RFID (一种非接触式的自动识别技术)标志,而 RFID 技术利用电磁波和读写器完成通信,这使得 RFID 标签使用者在不知情的情况下自动接受扫描、定位和追踪,导致信息被收集。其二,所有进入物联网的数据在传输过程中都无法加密,极易发生信息泄露的情况。在物联网这样公开的无线网络中,攻击数据和监听数据将会变得轻而易举,而且如果某个副本的数据遭到了破坏,那么整个副本数据的完整性和可靠性也会受到影响[14]。其三,物联网设备使用的终端多为弱终端,其自身并没有保障安全的能力。如果在进行数据交流过程中存在大量终端设备,相应

的服务器会向其发送大量的认证请求而导致服务系统陷入瘫痪。

委内瑞拉停电事件、物联网僵尸网络和勒索软件大规模攻击事件表明物联网发展所引发的信息安全问题对国家和社会安全造成了重大威胁。为应对不断发生的攻击事件,各国分别出台了专门的信息数据保护法来完善本国的网络安全治理体系,如美国采用了分散立法模式,欧盟于2009年制定了《射频识别技术(RFID)应用中隐私和数据保护原则的建议》。与这些网络强国和地区相比,我国有关物联网信息安全和领网权保护的立法尚未形成完整的体系。我国于2017年颁布了《网络安全法》,但是立法仅涉及网络数据、互联网安全、计算机病毒、信息安全等方面的内容,对相关配套领域,诸如关键信息、网络安全事件等术语均未作出必要的界定,对人工智能、云计算等新兴领域的安全问题还存在制度真空。借鉴国际上有关信息数据保护的有关经验,我国亟需建立完整的物联网信息保护体系,完善顶层机构的设置和管理机制,做好信息数据立法的整体规划,明确各部门、各行业的分工,以多举措推进信息数据安全保障工作。

技术层面,我国网络安全技术仍较为薄弱,必须形成硬件-软件防护体系才能实现物联网时代数据安全的有效保护,在这方面,国际上有关物联网信息安全保护的方案和对策值得我们借鉴。例如,美国联邦贸易委员会创新性地提出了"通知-选择"框架。针对物联网没有人机交互界面而导致"默认"的信息读取与收集问题,美国联邦贸易委员会建议可以在物联网设备上开发视频教程、粘贴二维码,以及在设备销售点、设备的设置向导、设备的隐私仪表板中告知消费者相关的隐私政策,由消费者进行选择[15]。我们可以根据物联网自身整体构架的特点,通过在设备上安装安全认证、对传输节点进行实时监控、建立认证和密钥管理相结合的机制等手段来实现物联网感知层、传输层、处理层、应用层的数据信息安全管理。

四、结 语

如今,区块链、人工智能、大数据等互联网领域的前沿技术已逐渐深入到人们社会生活的方方面面,与此同时,新技术的运用对网络空间的全球治理提出了新的要求和挑战。互联网技术的广泛运用让领网权的维护进一步复杂化,网络安全形势十分严峻,各国均有责参与其中。基于国家领土主权提出的领网权,有着充分的现代国际法基础与依据,是国家主权在网络空间的继承和延伸。互联网时代下国家主权的维护进一步复杂化,网络空间必须纳入国家主权的范畴,领网权的确立及其维护已成为新的国家战略重心,构建一种互联互通、共享共治的全球网络空间治理新秩序迫在眉睫。为此,中国

正在以实际行动提升国际竞争力,并为推进全球网络空间治理的良性变革贡献中国方案[16]。以此为基础,笔者尝试在立法与技术层面提出了建议,以期对我国领网权的构建以及信息安全保护制度的完善有所贡献。

参考文献:

[1] 习近平.在第二届世界互联网大会开幕式上的讲话[N].人民日报,2015-12-17(002).

[2] 李海敏."数字丝路"与全球网络空间治理重构[J].社会科学文摘,2020(2):42-44.

[3] 李艳.从战略高度审视网络空间治理发展态势[J].信息安全与通信保密,2020(1):5-9.

[4] BARLOW J P. A declaration of the independence of cyberspace[EB/OL].[2020-03-12].https://ieeexplore.ieee.org/document/6299679? arnumber=6299679.

[5] LEE A B, JON B. Internet governance: infrastructure and institutions[M]. New York: Oxford University Press,2009.

[6] 许开轶,俞润泽.基于多重场域原理的网络空间主权生成逻辑[J].社会科学研究,2020(2):49-56.

[7] 郭炯,洪永红.全球网络治理的法律困境与出路[J].湘潭大学学报(哲学社会科学版),2017(3):24-28.

[8] 强宇豪.基于国家主权的全球网络空间多边多元治理[J].渭南师范学院学报,2020(1):69-75.

[9] CATON J L. Beyond domains, beyond commons: context and theory of conflict in cyberspace[G]// CZOSSECK C, OTTIS R,ZIOKOWSKI K ,eds. 4th international conference on cyber conflict.Tallinn: NATO CCD COE Publication,2012.

[10] Federal Trade Commission. Internet of things: privacy & security in a connected world[EB/OL].[2020-03-12].https://www.researchgate.net/publication/296951341_Internet_of_things_Privacy_and_security_in_a_connected_world.

[11] 魏垚,谢沛荣.网络切片标准分析与发展现状[J].移动通信,2019(4):25-30.

[12] KUNER C, CATE F H, LYNSKEY O, et al.Expanding the artificial intelligence-data protection debate[J]. International Data Privacy Law,2018(4):289-292.

[13] 乌镇展望 2019[EB/OL]. [2020-04-15].https://www.sohu.com/a/348298429_181884.

[14] 邹聪.基于物联网的计算机网络安全分析[J].中国新通信,2020(13):170.

[15] 丁晓东.大数据与人工智能时代的个人信息立法:论新科技对信息隐私的挑战[J].北京航空航天大学学报(社会科学版),2020(3):8-16+71.

[16] 韩瑞霞,徐剑.网络主权视域下当前互联网治理的主要问题、成因及监管对策[J].南京邮电大学学报(社会科学版),2020(5):41-52.

(责任编辑:范艳芹)

Reflection on information security protection system in China: taking the maintenance of the right to lead the network as the entry point

WANG Zhigang, CHEN Lina

(School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, ChongQing 400065, China)

Abstract: With the rapid development of the Internet, the blending of cyberspace and real space is deepening, cyber sovereignty, information security and other issues continue to emerge, and the interests of all countries have been severely undermined. Network rights are the implication and extension of national sovereignty under the coverage of information and communication technology. The effective maintenance of network rights of various countries is conducive to promoting the "integration" of global information security protection and promoting the realization of the goal of "network community of shared future". Nowadays, the issue of network ownership is becoming more and more prominent. The application of new information technologies such as 5G communication, artificial intelligence and industrial Internet has put forward unprecedented challenges for global information security protection. Deepening the research on the proof of network ownership is conducive to maintaining the stability of cyberspace, speeding up the construction of network infrastructure and promoting the construction of international legal system for network security, which has important reference significance for realizing the modernization of China's governance capacity and improving the information security protection system.

Key words: cyberspace governance; the right to lead the network; information data protection; information security