《网络安全法》与《刑法》衔接问题研究

周洪波 岳向阳

摘 要: 《网络安全法》有关网络安全的管理规定确定了中国网络安全管理的基本规则,对适用刑法具有重要价值,同时也存在二者适用中的衔接问题。这主要表现于四个方面:网络空间主权规定对刑事管辖权的积极影响;《网络安全法》对信息网络安全管理义务的规定对《刑法》第二百八十六条之一规定的拒不履行信息网络安全管理义务罪的影响;对公民个人信息的规定不同表述的理解;如何正确适用宽严相济的刑事政策。

关键词: 网络安全;网络安全管理义务;个人信息
中图分类号:D922.17 **文献标识码:**A **文章编号:**1004-9142(2018)06-0047-09

《中华人民共和国网络安全法》(以下简称《网络安全法》,2017 年 6 月 1 日起施行)的颁行标志着中国网络空间领域进入了新的发展阶段,也意味着中国网络现代化治理工作迈上了新的台阶。该部法律回应了新时期中国社会主义现代化建设遇到的新挑战,对社会广泛关注的涉及网络安全方面的各种问题进行了详细规定,对依法治理网络、推动互联网行业健康发展、维护国家网络安全具有重要作用。《网络安全法》与《刑法》(以下简称"两法")在适用中存在衔接问题。本文就这个问题作一探讨,以期有利于"两法"的贯彻实施。

一、关于网络空间主权与刑事管辖权问题

(一)中国互联网发展状况

在中国,互联网已经深深嵌入了社会生活、工作与交往的各个方面。中国互联网络信息中心(CNNIC)最新公布的《中国互联网络发展状况统计报告》(第 40 次)充分显示了互联网对中国社会各方

收稿日期:2018-06-11
作者简介:周洪波,男,河南淮滨人,国家检察官学院教授,法学博士;
岳向阳,男,河南登封人,国家检察官学院副教授,法学博士。(北京 102206)
基金项目:本文是教育部人文社会科学重点研究基地项目(项目批准号:11JD820014)的阶段性成果。

面的影响:截至2017年6月,中国网民规模达到7.51亿人,占全球网民总数的1/5。互联网普及率为54.3%,超过全球平均水平4.6个百分点。中国手机网民规模达7.24亿,较2016年底增加2830万人。网民中使用手机上网的比例由2016年底的95.1%提升至96.3%,手机上网比例持续提升。上半年,各类手机应用的用户规模不断上升,场景更加丰富。其中,手机外卖应用增长最为迅速,用户规模达到2.74亿人,较2016年底增长41.4%;移动支付用户规模达5.02亿人,线下场景使用特点突出,4.63亿网民在线下消费时使用手机进行支付。① 可以说,互联网已经深入社会生活的各个方面,成为人们工作、生活与学习不可或缺的重要工具或者活动场所。

适应网络发展的需要,近些年国家立法机关及有关部门在制定、修改法律法规、部门规章等文件时,都有涉及互联网的相关规定。据统计,中央网络安全和信息化领导小组自成立以来,已颁布实施了近50部互联网相关法律法规。② 作为网络安全管理的基础性"保障法",《网络安全法》明确了有关网络安全的一系列规定,如网络空间主权的原则、网络产品和服务提供者的安全义务、网络运营者的安全义务、个人信息保护规则、关键信息基础设施安全保护制度、关键信息基础设施重要数据跨境传输规则等。《网络安全法》还对建设、运营、维护和使用网络,以及网络安全的监督管理、网络空间治理、网络技术研发和标准制定、打击网络违法犯罪国际交流与合作等方面做了明确规定。这些都对固定发展成果、促进互联网在社会治理模式中继续发挥作用至关重要。《网络安全法》的颁布和施行,是中国政府积极参与网络社会治理、顺应社会发展潮流的具体体现,是对网络时代降临的肯定和推动。

互联网信息的跨境流动,使跨境实施犯罪的可能性增加。以美国为首的西方大国,利用互联网技术先发优势,利用网络针对他国实施侵害行为。"棱镜门"事件显示,美国利用技术优势对他国甚至盟国领导人进行监视、监控和监听。在商业或者私人领域,利用远程控制等网络技术实施控制、攻击他人计算机或者传播病毒等行为也屡见不鲜。西方国家利用其网络国际空间话语权,在网络犯罪国际立法、司法等方面持双重标准,造成中国涉外网络犯罪频发,打击困难,严重危害中国社会经济健康发展。

(二)网络空间主权下网络犯罪管辖权

网络空间主权是中国有效开展网络犯罪治理的理论前提和法治保障。针对网络发展现状以及网络空间治理的需要,习近平总书记在第二届世界互联网大会演讲时全面阐释了推进全球互联网治理体系变革需要坚持的尊重网络主权、维护和平安全、促进开放合作、构建良好秩序四项原则,系统提出共同构建网络空间命运共同体的五点主张。《网络安全法》以基本法律的形式,重申《国家安全法》确立的网络空间主权概念,这对司法机关行使跨境网络犯罪刑事管辖权意义重大。对网络犯罪管辖权涉及到的具体问题,中国学者在网络空间主权概念之下开展研究,关注度较高且取得成效。③ 如有学者提出,网络犯罪的管辖权应体现谦抑原则,在属人管辖之外,以犯罪行为对本国国家或公民的实际侵害或者影响关联性作为确定是否具有管辖权的标准。④ 司法实践中,确立了以犯罪地管辖为主、犯罪嫌疑人居住地管辖为辅的原则。如,2014年"两高"、公安部《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》明确规定,网络犯罪案件由犯罪地公安机关立案侦查。必要时,可以由犯罪嫌疑人居住地公安机关立案侦查。网络犯罪案件的犯罪地包括:用于实施犯罪行为的网站服务器所在地,网络接入地,网站建立者、管理者所在地,被侵害的计算机信息系统或其管理者所在地,犯罪嫌疑人、被害人使用的计算机信息系统所在地,被害人被侵害时所在地,以及被害人财产遭受损失地等。以犯罪地为主、犯罪嫌疑人居

① 中国互联网络信息中心,http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201708/t20170803_69444.htm,2017年9月8日访问。

② 张宝山:《"中国方案"推动全球互联网治理向前迈进》,《中国人大》2017年第5期。

③ 张旭、施鑫:《我国网络犯罪研究的现状与反思——基于1234的文献计量分析》,《净月学刊》2016年第6期。

④ 于志刚:《关于网络空间中刑事管辖权的思考》,《中国法学》2003年第6期。结合网络犯罪的发展趋势,作者又对早先提出的网络犯罪管辖权的观点进行了修改,认为网络犯罪的刑事管辖权应深刻分析网络行为的特点,通过解释"行为"的特点来构建全新的解释思路,补充解释"实害联系标准"。详见于志刚:《"信息化犯罪"时代与<网络安全法>的中国取舍——兼论网络犯罪刑事管辖权的理念重塑和规则重建》,《法学论坛》2013年第3期。

住地为辅的原则,有利于中国司法机关正确行使网络犯罪案件的管辖权,依法处理相关涉外案件。

近年来,在坚持“尊重各国网络主权,反对侵犯他国网络主权”的原则下,中国推动国内立法完善,参与双边合作与多边合作,推动建立国际网络新规则。以近年来中美两国之间共同打击国际网络犯罪多轮对话为例,通过双方的共同努力,在利用网络实施的犯罪案件的信息共享、案件合作,打击利用技术和通讯组织、策划和实施暴力恐怖活动等方面取得共识。如 2016 年 6 月第二次中美打击网络犯罪及相关事项高级别联合对话,明确优先以获取经济利益为目的的网络知识产权窃密案件进行合作;在打击网络传播儿童淫秽信息、不正当使用技术和通讯帮助暴力恐怖活动、电子邮箱和钓鱼网站等网络诈骗、网络贩枪等 4 个领域开展合作。2016 年 12 月中美举行第三次打击网络犯罪及相关事项高级别联合对话,在打击利用网络实施的犯罪、网络保护、打击利用技术和通讯组织、策划和实施暴力恐怖活动等方面取得共识。

二、“两法”中“信息网络安全管理义务”的理解与认定

《刑法修正案(九)》第二百八十六条之一规定了拒不履行信息网络安全管理义务罪。根据该条规定,成立本罪的前提条件,就是网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务,导致出现危害社会的结果。但是,网络服务提供者的范围以及其应该遵守何种信息网络安全管理义务,当时并没有法律作出明确规定。根据《网络安全法》的规定,承担危害网络安全的责任主体有:网络运营者,网络产品、服务的提供者,关键信息基础设施的运营者,电子信息发送服务提供者和应用软件下载服务提供者等。这些负有维护信息网络安全管理义务的主体因具体角色不同,承担的维护网络安全义务有所区别,但承担义务的本质是相同的。以网络运营者为例,《网络安全法》规定的其网络安全管理义务可以大致分为两类:一是一般性义务,即网络安全责任主体均应遵守的义务;二是特殊性义务,即与具体网络主体有关的维护网络安全的义务。

(一)一般性信息网络安全管理义务

网络运营者在开展与互联网有关的各项社会活动时,应该遵守宪法,遵重社会公德,遵守商业道德,这是公民、法人或者社会组织等进行社会活动时的基本要求。早在 20 世纪 90 年代,中国有关部门已经注意到网络运行带来的风险,并在有关的规范中对网络运营主体的守法义务做了明确规定。例如,1997 年公安部制定的《计算机信息网络国际联网安全保护管理办法》第四条明确规定,任何单位和个人不得利用国际联网危害国家安全,泄露国家秘密,不得侵害国家的、社会的、集体的利益和公民的合法权益,不得从事违法犯罪活动,并在第五条规定了禁止传播的信息范围。1997 年农业部《计算机信息网络系统安全保密管理暂行规定》第 20 条规定,联入农业部计算机信息网络的单位和个人,不得利用网络系统从事危害国家安全、泄露国家秘密等违法犯罪活动,不得编制、运行、传播危害网络安全的软件,不得制作、查阅、复制和传播妨害社会治安的信息和淫秽色情等信息。上述规范性文件对于促进互联网行业健康发展,保护网络安全起到了重要作用。

随着网络技术的发展,维护网络安全涉及的问题愈加复杂,单纯对网络相关主体的守法义务予以明确已经不能满足行业发展以及维护网络安全的需要。诸如黑客攻击、网络暴力、人肉搜索、互联网金融等除对现行法律体系形成冲击外,还危及社会公共道德与商业道德。在《网络安全法》中,除明确网络运营者的守法义务之外,还要强调尊重社会公德、遵守商业道德。例如,该法第 8 条规定,“网络运营者,开展经营服务活动,必须遵守法律行政法规,尊重社会公德,遵守商业道德,诚实信用,履行网络安全保护义务,接受政府和社会的监督,承担社会责任。”第 12 条第二款规定,“任何个人和组织使用网络应当遵守宪法法律,遵守公共秩序,尊重社会公德,不得危害网络安全,不得利用网络从事危害国家安全、荣誉和利益,煽动颠覆国家政权、推翻社会主义制度,煽动分裂国家、破坏国家统一,宣扬恐怖主义、极端主义,宣扬民族仇恨、民族歧视,传播暴力、淫秽色情信息,编造、传播虚假信息扰乱经济秩序和社会秩

序,以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。”

(二)具体信息网络安全管理义务

1. 网络运行安全管理义务

网络运行安全管理义务分为两种:一般性网络运行安全管理义务和关键信息基础设施运行安全管理义务。从针对的对象来说,前者是针对普通信息设施,后者针对国家关键信息基础设施。从义务范围分析,后者在前者应遵守的义务范围的基础上,又根据国家关键信息基础设施的特点增加了特定的义务。就一般性义务而言,主要有网络安全等级保护义务、网络实名制义务、网络事件应急预案以及及时补救报告义务、协助义务等。以网络安全等级保护义务为例,为了维护网络安全,1994 年国务院颁布的《计算机信息系统安全保护条例》第九条规定,计算机信息系统安全实行等级保护,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。1999 年公安部颁布了《计算机信息系统安全保护等级划分准则》,2007 年公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合发布的《信息安全等级保护管理办法》均明确了信息安全等级保护的具体要求。《网络安全法》第二十一条进一步重申了网络安全等级保护制度,并细化了具体义务。根据该条规定,网络运营者应当按照网络安全等级保护制度的要求,履行安全保护义务,保障网络免受干扰、破坏或者未经授权的访问,防止网络数据泄露或者被窃取、篡改。这些义务具体包括:(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、网络侵入等危害网络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;(5)法律、行政法规规定的其他义务。而对于国家关键信息基础设施而言,行为主体除遵守上述义务外,还应遵守如下义务:(1)设置专门安全管理机构和安全管理负责人,并对该负责人和关键岗位的人员进行安全背景审查;(2)定期对从业人员进行网络安全教育、技术培训和技能考核;(3)对重要系统和数据库进行容灾备份;(4)制定网络安全事件应急预案,并定期进行演练;(5)法律、行政法规规定的其他义务。

2. 网络信息安全义务

网络信息安全义务,是针对所有网络运营者,包括对国家关键信息基础设施运营者、网络产品和服务提供者(含电子信息发送服务提供者和应用程序下载服务提供者)设定的普遍性义务。这些义务主要包括:用户信息保密义务、依法收集用户信息义务、对用户发送信息的管理义务、不得设置恶意程序的义务等。以用户信息保密义务为例,《网络安全法》明确了“网络运营者应当对其收集的用户信息严格保密,并建立健全用户信息保护制度。”这项义务又可分为三个方面,即:(1)收集用户信息应坚持公开、合法、必要原则,公开收集、使用规则,明示收集、使用信息的目的、方式和范围,并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息,不得违反法律、行政法规的规定和双方的约定收集、使用个人信息,并应当依照法律、行政法规的规定和与用户的约定,处理其保存的个人信息。(2)网络运营者不得泄露、篡改、毁损其收集的个人信息;未经被收集者同意,不得向他人提供个人信息。但是,经过处理无法识别特定个人且不能复原的除外。网络运营者应当采取技术措施和其他必要措施,确保其收集的个人信息安全,防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时,应当立即采取补救措施,按照规定及时告知用户并向有关主管部门报告。(3)个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的,有权要求网络运营者删除其个人信息;发现网络运营者收集、存储的其个人信息有错误的,有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。由上述分析可知,《网络安全法》详细规定了个人信息保密义务的具体要求,可操作性较强,不仅有利于网络运营者完善保密制度、落实法律的具体规定,也有利于有关行政管理部门履行监管职责,依法维护网络信息安全。

3. 监测预警与应急处置义务

《网络安全法》关于监测预警与应急处置的规定,主要针对国家有关主管部门,如国家网信部门应

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。对于网络运营者而言，主要体现为整改义务，即发现网络存在较大安全风险或者发生安全事件时，网络运营者应当按照政府有关主管部门的要求采取措施，进行整改，消除隐患。根据刑法第二百八十六条之一规定，成立拒不履行网络安全管理义务罪的前提条件，就是要求经国家监管部门责令采取改正措施，而拒不改正，致使发生危害社会结果的情形。设置整改义务的目的主要是围绕网络安全，督促网络运营者正确履行《网络安全法》确定的网络运行安全管理义务和网络信息安全义务。

三、“两法”中“公民个人信息”各自范围的划定

2015 年施行的《刑法修正案(九)》修改了原第 253 条之一规定的侵犯公民个人信息罪，加强了对公民个人信息的保护。修改后的该条规定，违反国家有关规定，向他人出售或者提供公民个人信息情节严重的，或者将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人的，或者窃取或者以其他方法非法获取公民个人信息的，属于该罪的客观行为表现。2017 年 5 月 8 日“两高”发布的《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》对该罪的定罪量刑标准予以明确，这有利于进一步加强对公民个人信息的保护。

(一)关于公民个人信息的范围

2012 年 12 月 28 日，全国人大常委会颁布的《关于加强网络信息保护的决定》没有明确定义个人信息，仅表述为“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”。该规定虽然没有说明个人信息的范围，但大致指明了个人信息保护的对象。随着互联网逐步推广，不同行业主体在从事社会活动时都存在搜集公民个人信息的情况，有关部门也看到了其中存在的风险并逐步通过加强立法，完善部门或行业管理规定，加强对公民个人信息安全的保护。例如，2013 年 7 月 16 日工业和信息化部《电信和互联网用户个人信息保护规定》第四条使用“用户个人信息”的概念，基本明确了公民个人信息的范围。根据该条规定，用户个人信息是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证号码、住址、电话号码、账号和密码等，能够单独或者与其他信息组合识别用户的信息以及用户使用服务的时间、地点等信息。《网络安全法》明确了个人信息的范围，表述更为全面、科学。根据该法规定，个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。《网络安全法》在明确个人信息范围的同时，并没有限制个人信息的范围。这主要是因为，个人信息的范围与社会经济发展密切相关，在一定意义上取决于社会发展的程度。社会经济发展状况、科技发展程度、社会管理方式方法及技术措施等。

“两高”发布的《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》对公民个人信息的表述与《网络安全法》的规定略有不同，但并不存在实质上的差异。该解释第一条规定，刑法第 253 条之一规定的“公民个人信息”，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。

从上述分析看，除现行《网络安全法》以及刑法司法解释对公民个人信息的范围有所界定外，尚有一系列的行政法规规定了公民个人信息的范围。有论者认为，刑法上的公民个人信息虽然与民法、行政法上的公民个人信息具有同质性，但在形态上却有所不同。刑法上的公民个人信息是具有法益关联性的信息，非法获取、使用、泄露这些信息将对公民的人格权和财产权造成严重的侵害或者使其处于遭受严重侵害的危险之中。只有具有如此重要价值的信息，才可以被刑法上的公民个人信息所涵摄；否则，

则应归属于民法或行政法上的公民个人信息。[①] 事实上,对公民个人信息作行刑或者民刑意义上的区分,意义不大。从公民个人信息产生的过程看,它与公民个人工作生活密切相关。个人日常生活工作中产生的个人信息,虽然可在对个人信息重要性程度上做适度区分,但完全将部分信息排除在刑法保护范围之外并不科学。主要原因在于:网络时代背景下,个人信息被认为是现代商业乃至整个社会发展的基础资源,基于个人信息组成的大数据信息资源已成为精准营销、网络推送、个性化定制以及制定社会管理策略乃至社会发展政策等的必要条件,获取公民全方位个人信息已经成为现代商业竞争、社会发展的基本样态。借助网络科学技术的发展,不同信息的组合运用可以创造出新的商业运营模式,进而对公民生产生活产生巨大影响。即便被认为对公民个人不太重要的个人信息,对与此类信息有关的产业来说也是不可或缺。因此,对严重危及信息安全的行为都应该保留刑法处罚的可能性。对公民个人信息不作行刑或者民刑意义上的区分,并不意味着对情节较轻、危害不大的侵犯公民个人信息的行为不能进行民事、行政处罚。对达不到入罪条件不构成犯罪的侵害公民个人信息的行为,可以作民事、行政责任的追究。

(二)刑法中公民个人信息的判断

在《关于加强网络信息保护的决定》《网络安全法》以及"两高"的司法解释中,对个人信息的界定均含有"识别自然人个人身份"的特征表述。不论公民个人信息的产生,还是侵犯公民个人信息的危害后果,都与特定公民个人紧密相关。因此,以能否"识别自然人个人身份"作为判断公民个人信息的标准是不存在歧义的。这也是《网络安全法》明确规定,对"经过处理无法识别特定个人且不能复原的"信息,不经被收集者同意也可以向他人提供的原因。但是,《关于加强网络信息保护的决定》还明确了"涉及公民个人隐私的电子信息","两高"司法解释中规定了"反映特定自然人活动情况"的信息,这两项规定是否也属于判定公民个人信息的核心标准,需要作进一步研究。

首先,个人信息与隐私权存在交叉关系。中国《民法总则》规定了公民的隐私权,但没有规定公民个人信息权。《网络安全法》使用了"侵害个人信息依法得到保护的权利的"表述,也没有采用公民个人信息权的规定。隐私权的范围,法律并没有明确规定,学术界有不同的观点。如有论者认为,隐私权应以生活安宁和私人秘密作为其基本内容。生活安宁是指自然人对于自己的正常生活所享有的不受他人打扰、妨碍的权利,包括排除对私人正常生活的骚扰、禁止非法侵入私人空间、对个人自主决定的妨碍。生活秘密是个人的重要隐私,涵盖的范围很宽泛,包括了个人的生理信息、身体隐私、健康隐私、财产隐私、谈话隐私、基因隐私、个人电话号码等,也包括个人家庭中有关夫妻生活、亲属关系、婚姻状况(如离婚史等)、是否为过继、父母子女关系及夫妻关系是否和睦、个人情感生活、订婚的消息等。[②] 也有论者认为,隐私权就是个人对私人领域内的各种隐私信息享有独享权与私生活不被非法或不正当侵扰的独处权。[③] 从学者对隐私权的概念解释中可知,个人信息与个人隐私概念之间存在交叉重合,公民个人隐私常常以个人信息的形式表现出来,很难对二者做非常清楚的界限划分。

中国民法司法实践中,对个人信息的保护都是通过隐私权制度加以实现的,相关问题的研究也多在隐私权制度的框架下展开。实际上,个人信息的概念与隐私不完全等同,个人信息权在权利属性和权利内容上也不同于隐私权。与"个人信息"相比,"个人隐私"涵盖范围较窄,个人信息在内涵上强调主体对其个人信息所享有的积极控制权,也不同于作为消极防御权的个人隐私。从权利性质上看,个人信息体现着主体的人格利益和财产利益,个人隐私仅具有人权权益。因此,有论者主张个人信息权应该独立于隐私权,将其作为一种独立的人格权规定下来。[④] 也正是因为二者存在特殊关系,《关于加强网络信

① 叶良芳、应家赟:《非法获取公民个人信息罪之"公民个人信息"的教义学阐释——以 < 刑事审判参考 > 第 1009 号案例为样本》,《浙江社会科学》2016 年第 4 期。

② 王利明:《隐私权概念的再界定》,《法学家》2012 年第 1 期。

③ 范进学:《我国隐私权的立法审视与完善》,《法学杂志》2017 年第 5 期。

④ 王利明:《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》,《现代法学》2013 年第 4 期。

息保护的决定》在界定公民个人信息保护范围时将二者并列使用,以免因法律规制缺失而造成保护或者处罚的漏洞。

其次,“反映特定自然人活动情况”属于隐私权的范畴。在“两高”的司法解释中,把公民个人信息核心要素表述为“识别特定自然人身份或者反映特定自然人活动情况的”各种信息。这里的“反映特定自然人活动情况”可以归属隐私权的范畴。实践中,隐私权表现为自然人享有的私人生活安宁与私人信息秘密,是特定抽象人格权在个人载体上的自然延伸。而特定自然人的社会活动情况,正是自然人人格权的具体化,是抽象的、法律规范中的隐私权在社会生活中的具体表达。因此,“两高”解释中“反映特定自然人活动情况”没有超出隐私权的范围,是隐私权在刑事司法解释中的具体运用。

针对“两高”解释与《网络安全法》在界定个人信息范围方面的差异,有论者认为,刑法关于侵犯公民个人信息犯罪的规定早于《网络安全法》的相关规定。对侵犯公民个人信息罪所涉及的“公民个人信息”的解释不必完全受制于在此之后施行的《网络安全法》的规定。① 这种说法有一定的道理,但从立法目的方面进行分析更能说明二者规定的差异。因为,《网络安全法》的立法目的是保障网络数据安全,有必要从数据安全角度界定个人信息的范围。而《关于加强网络信息保护的决定》与“两高”司法解释侧重保护与公民个人信息有关的权利。在有关规范性文件和法学理论对个人信息与隐私权之间的界限尚没有清晰界定的情况下,从个人信息可识别性与隐私权两个方面限定个人信息的范围是必要的,以免造成处罚漏洞。在《网络安全法》中,有关公民个人信息的规定属开放性的表述,其概念外延的可延展性与立法对个人信息、隐私权范围的不确定性具备内在的一致性,完全可以将隐私权范围内的事项纳入个人信息范畴。

四、“两法”处罚的衔接与政策的把握

对于网络安全违法行为,《网络安全法》规定了行政处罚,构成犯罪的,《刑法》规定了刑罚。实践中,对一些网络安全违法犯罪行为,是进行行政处罚还是刑事处罚,除了严格按照“两法”的规定处理外,还要注意二者的衔接以及政策的把握。尤其要正确认识网络技术对社会生活的影响,认识网络犯罪的特殊性,贯彻好宽严相济的刑事政策,做到既不扩张犯罪打击面,发挥《网络安全法》的前置作用,又要发挥刑法的惩罚功能,重点惩治发案频率高、社会影响恶劣、社会危害严重、人民群众反应强烈的犯罪行为。

(一)网络技术引发的社会治理模式变化

前《网络安全法》时代,社会治理模式较为单一,基本上依赖各种人力资源进行各类社会管理活动。随着网络技术的发展,社会治理模式各要素发生了较大的变化,传统依靠人力资源进行社会治理的领域逐步被网络技术取代,人力从社会治理的第一线(第一现场)转移到幕后控制(第二现场)。以交通违章为例,传统社会中对交通违章事件的处理,以交警现场执法为主,执法机关发现违法能力较弱、执法范围有限、执法的连续性不强,无法体现社会主义法治所要求的“有法必依、违法必究”的社会治理要求。在网络化时代,交通警察的工作让渡于电子监控系统,对违法行为的发现能力大大增强,执法的范围也可以拓展到以前人力难以企及的场所,且可以达到 24 小时不间断发现违法行为。在此种情况下,交通警察的工作由现场执法转移到幕后管理操作,执法的能动性增强,执法效果大大提升。在 2016 年的《政府工作报告》中,李克强总理明确提出,要大力推行“互联网 + 政务服务”,实现部门间数据共享,让居民和企业“少跑腿、好办事、不添堵”。中国政府网刊登了 2017 年各地区各部门开展“互联网 + 政务服务”工作主要目标任务汇总表,从工作目标任务来看,31 个省份都在大力推进“线上政府”建设,助力“互联网 + 政务服务”,加快实现“利企便民”等。这表明,为适应互联网时代的社会变迁,中国政府已经主动进

① 喻海松:《侵犯公民个人信息罪司法适用探微》,《中国应用法学》2017 年第 4 期。

行社会管理模式转型。

互联网技术深深改变了人们的生产生活方式与传统的社会治理模式,同时对犯罪行为的实施方式以及犯罪组织形式等产生了较大的影响。利用各种网络技术,传统犯罪借助信息网络实现了犯罪过程与犯罪手段的升级转型,与网络技术有关的犯罪日益常态化,犯罪分子利用网络平台、网络空间和现代通讯工具实施犯罪的行为更为隐蔽、复杂,危害结果更易扩散与不可控,跨国(境)实施犯罪的可能性大大增加。以网络社群犯罪为例,作为一种借助网络技术组合而成的新型犯罪形式,表现为两种情况:一是传统犯罪团伙的网络化,即传统犯罪团伙向网络犯罪社群转型;二是完全虚拟化社群,社群成员通过自媒体平台结识、交流、沟通与合作,彼此互不相识,只掌握网络身份。① 在互联网背景下,人们对网络犯罪现象及其社会危害性的认识也在不断深化。在立法方面,互联网行为的治理规范日益完备,围绕《网络安全法》的配套立法工作正在逐步推进。司法方面,司法机关已经根据惩治网络犯罪的需要,调整相应的侦查、检察和审判方法。有关的司法机关根据网络犯罪案件情况,成立了专门机构,配备专业人员和技术设置,提升办理网络犯罪案件的能力。2016 年 9 月,“两高”、公安部联合下发《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》,进一步规范电子数据的收集提取和审查判断,确保涉网络刑事案件的办案质量。

(二)贯彻宽严相济的刑事政策

社会治理模式的转型,要求司法机关根据社会治理形式的需要,调整相应的刑事应对策略。切实贯彻宽严相济的刑事司法政策,要根据社会治安形势和犯罪分子的不同情况,实行区别对待,注重宽与严的有机统一,该严则严,当宽则宽,宽严互补,宽严有度,对严重犯罪依法从严打击,对轻微犯罪依法从宽处理,对严重犯罪中的从宽情节和轻微犯罪中的从严情节也要依法分别予以宽严体现,对犯罪的实体处理和适用诉讼程序都要体现宽严相济的精神。② 办理网络犯罪案件中贯彻宽严相济刑事政策,就是要正确区分犯罪的严重程度、客观判断犯罪是否高发多发等情况,全面研究衡量犯罪的社会危害性,达到罪责刑相适应的法律适用效果。具体而言,司法机关应在以下几个方面加强打击力度:

1. 电信网络诈骗违法犯罪

近年来,电信网络诈骗犯罪一直呈现高发多发的态势,不法分子结成团伙,设置窝点(许多窝点设置在境外),精心设计各种骗局,通过拨打网络改号电话、利用“伪基站”设备群发手机短信、网上发布诈骗信息等方式,针对不特定群众,大肆实施诈骗活动,诱使被害人上当受骗,汇转资金。从查获的案件资料看,此种违法犯罪手段不断更新,危害后果严重,社会影响较大,群众反映强烈。相关部门通过共同发布通告、出台司法解释,挂牌督办等刑事手段重拳打击电信网络诈骗犯罪。例如,最高人民检察院与公安部联合挂牌督办“徐玉玉案”等 62 起重大案件,加强境外执法司法合作;2016 年度批准逮捕电信网络诈骗犯罪嫌疑人 19345 人;北京、浙江、广东检察机关提前介入侦查,及时批捕起诉张智维等 116 人、罗兆隆等 108 人、崔培明等 129 人特大跨国电信网络诈骗案等。③ 司法机关的严厉打击,有效遏制了电信诈骗违法犯罪猖獗的势头。从现有情势看,为了逃避打击,此类犯罪作案手法、地点等更为隐蔽,仍是今后重点惩治对象。

2. 计算机信息安全违法犯罪

信息安全违法犯罪包括的范围很广,除刑法明确列明的有关个人信息的犯罪、计算机犯罪外,还涉及网络谣言以及刑法第 252、253 条侵犯通信自由和通信秘密的违法犯罪等。以网络谣言为例,不法分子利用网络便利条件,制造并散布网络谣言,社会危害性严重。2017 年澳门遭受强台风“天鸽”袭击后,解放军驻澳门部队出动 1000 名官兵协助澳门政府和市民一起进行灾后的各项援助和建设工作。在解

① 谢晓专:《网络犯罪社群行动特征与防控策略》,《中国人民公安大学学报》(社会科学版)2017 年第 2 期。
② 详见 2007 年《最高人民检察院关于在检察工作中贯彻宽严相济刑事司法政策的若干意见》。
③ 曹建明:《最高人民检察院工作报告》,2017 年 3 月 12 日。

放军赴澳门救灾过程中,有网络谣言声称解放军在澳门杀人。据调查,造谣者在美国经多个国家的伺服器,将信息发送至香港。此类谣言有意贬低及攻击解放军,造成了恶劣的社会影响。再比如,通过技术手段,对公民使用包括电子邮件通信在内的网络通信自由和通信秘密实施非法监听、拦截公民通信内容的行为,以及因使用互联网进行社交、电子商务等社会交往活动中产生的大量信息的使用管理问题等,都会成为互联网时代计算机信息保护的关键问题。可以预见,网络技术的发展使得与计算机信息安全有关的网络不法行为会不断出现,加大对此类犯罪的处罚力度有其客观必要。

3. 互联网金融违法犯罪

金融安全是现代经济的基础,借助网络技术,传统金融越来越多地表现为互联网金融的形式,如互联网支付、网络借贷、股权众筹融资、互联网基金销售、互联网保险、互联网信托和互联网消费金融等。由于中国互联网金融企业的内控治理水平较为薄弱,与行业的快速发展情况不相称,利用金融监管漏洞实施违法犯罪行为成为互联网金融犯罪的显著表现。为争夺市场资金和客户资源,向社会公众(包括单位和个人)吸收资金的过程中,部分互联网金融企业违反国家金融管理法律规定,片面宣传、夸大收益等现象较为普遍。如部分 P2P 网贷平台,虚构标的,或者通过虚构、夸大融资项目收益前景等方法误导出借人;股权众筹发布虚假标的,部分 P2P 融资平台通过设立资金池的形式偏离金融信息中介的定位,筹集资金自用,“明股实债”或变相乱集资;以“股权众筹”等名义从事股权融资业务或募集私募股权投资基金等;以投资特定项目名义进行所谓股权众筹,承诺一定期限内还本付息或给予其他方式回报等;对投资理财类产品的收益、安全性等情况进行虚假宣传,欺骗和误导消费者等。也有的行为主体借助于互联网金融交易便捷的特点,利用互联网金融企业缺乏辨识资金性质的有效手段,隐瞒交易资金真实来源和去向,为走私、贩毒、赌博等非法活动从事洗钱行为。近年来爆发的互联网金融犯罪案件,如 e 租宝等,涉案交易金额巨大,社会影响严重,严重危及社会稳定。为维护金融安全,确保国家社会经济健康发展,对互联网金融犯罪行为要加大打击力度。

How the Network Security Law Relates to the Criminal Law

ZHOU Hong-bo and YUE Xiang-yang

Abstract: The Network Security Law is about regulating network security, and to that end, establishes the basic rules of network security management in China, which is vital for the application of Criminal Law. To correctly understand how the two laws relate to each other, the following four main aspects merit serious attention: the positive influence of the network space sovereignty on criminal jurisdiction; the influence of regulations of the Network Security Law on network information security management obligation concerning crimes of refusal to perform the information network security management legal obligations stipulated in Article 286 of the Criminal Law; understanding of different expressions of personal information of a citizen; and the correct application of the criminal policy of tempering justice with mercy.

Key words: network security; network security management obligations; personal information

(责任编辑:新中)