

“互联网+”时代中国的暗网犯罪及其刑法规制

王德政

(四川师范大学 法学院, 四川 成都 610068)

摘要:暗网犯罪近年来在我国不断发生。暗网具备重大法益侵害性和犯罪工具性两大性质,已达到我国社会无法容忍的地步。为了保护我国公民个人法益和社会公共法益不受暗网犯罪的侵害,可借鉴德国刑法学中“敌人刑法”理论,对暗网采取彻底取缔的态度。但我国《刑法》中的既定规制方式却无法有效地规制暗网,可通过运用刑法基本原理而提出相应的修法原则,据此增设规制暗网行为的5个新罪名,并以具体的法条表述明确清晰地划定应受规制的暗网核心行为,排除不应被规制的暗网边缘行为,许可国家机关依法使用暗网,以此从根源上防范暗网犯罪在我国继续发生,有效保障我国公民个人利益、社会公共利益和网络的安全。

关键词:“互联网+”时代;暗网犯罪;刑法规制;网络安全

中图分类号:D924.3

文献标识码:A

文章编号:1673-2359(2020)02-0101-08

当前,随着互联网在我国各个行业、领域的普及,我国已全面进入“互联网+”时代。互联网给我国公众的生活带来各种便利的同时,也带来了一定的负面效应,比如网络犯罪的发生。与网络犯罪逐渐紧密相连的,是一种叫暗网的新兴事物。2015年,轰动全国的“章莹颖失踪案”发生后,美国警方抓捕了犯罪嫌疑人克里斯滕森,发现其曾访问暗网中一个名为“绑架101”的网站,从此,随着媒体的大量报道,暗网走进了我国公众的视野。如果说“章莹颖失踪案”由于发生在美国,其给我国带来的影响具备一定程度的间接性,那么,直接在我国本土发生的暗网犯罪案件,较为知名的是于2013年3月我国警方查处的一起利用暗网传播未成年人淫秽信息的案件。而新近发生的两起暗网犯罪案件均涉及侵犯公民个人信息罪,其案情分别为:2018年8

月,非法侵入浙江省学籍管理系统的王某等人通过暗网发布交易信息,将浙江省1000万条学籍数据以0.02比特币(约153.55美元)的价格出售,后被浙江警方查获;^[1]2019年2月,湖北警方在四川省抓获犯罪嫌疑人吴某,其利用黑客手段非法获取武汉某公司300余万条公民个人信息,并在暗网上以1个比特币的价格销售。^[2]由此可见,暗网这一原本为我国公众所不太熟知的新兴事物,逐渐从国外走入国内,“知名度”随之不断提高,并且从在我国媒体上曝光伊始,就与网络犯罪紧紧勾连。

对我国公民或者发生在我国本土的暗网犯罪既然已经发生并且呈现不断发生的趋势,为了使我国公民免受暗网犯罪的侵害,从而维护我国公民的生命、身体、财产等合法权益,有必要从逻辑、事实和规范的角度厘清以下问题:第一,就我国

收稿日期:2019-11-10

作者简介:王德政(1985-),男,四川通江人,四川师范大学法学院讲师,博士。

基金项目:教育部人文社会科学研究青年项目“刑法目的解释研究”(18YJC820057)

《刑法》分则而言,全球包括我国已发生的暗网犯罪所涉及的罪名主要包括哪些种类?第二,暗网与犯罪之间究竟存在何种关联?具体而言,常见的暗网犯罪是指使用暗网的行为(下文简称为暗网行为)本身构成犯罪,还是通过使用暗网构成其他的犯罪?第三,我国《刑法》是否针对暗网设定了针对性的规制方式,如果没有设定或者既定规制方式存在缺陷,如何从刑事立法的角度对暗网提出有针对性的规制方案。因此,笔者拟先考察暗网相对于普通网络所表现出的特点和暗网犯罪涉及的罪名种类,据此总结出其性质,继而具体分析我国刑事立法中针对暗网的规制方式呈现出的不足,再运用刑法学基本原理,从立法角度对暗网规制提出具体的改进建议,以期从源头治理的角度,运用刑事法治的利器,将暗网犯罪扼杀于萌芽之中,借以保护我国公民的合法权益不受暗网犯罪的非法侵害。

一、暗网的特点、性质和罪名种类

暗网是指只能用特殊软件、特定授权或对电脑作特殊设置才能连上的网络。^[3]根据搜索引擎的轻易搜索性作为划分标准,可将互联网分为“明网”(Surface Web)和“深网”(Deep Web)两个部分,那么,在深网中,有一个子集只能为特殊软件或加密动态网络技术才能访问,该子集是一种网络集合,称为暗网(Dark Web)^[4],占据了整个网络数据的96%^[5]。

暗网始于1995年,美国海军为了确保体系内的网络通信不被人追踪,研制出一种名为“Tor”的工具。随后,随着Tor被其他组织推广,暗网随之蔓延开来。当前,类似Tor并且较为知名的暗网工具还有Tor2web、Freenet、I2P^[6]、Zeronet等,但Tor属于访问暗网的中坚力量。根据美国乔治城大学和美国海军研究实验室的估测,在Tor的用户中,德国、中国、美国的数量最大。^[7]当前,随着暗网知名度的提升,我国越来越多的网民开始关注甚至染指暗网,暗网在我国尤其受到年轻人、网络知识丰富者或具备犯罪倾向者的青睐。比如,有网民在“百度贴吧”中创建有关暗网的贴吧,散播关于暗网的信息。而在我国香港行政区、我国台湾地区,暗网也逐渐参与到社会活动中来,类似于Tor的工具“FireChat”成了“占中”运动和“太阳花”学运

中的有力联络工具。

暗网与普通网络相比,具备以下特点:第一,隐蔽性。这是指常规搜索引擎无法直接访问暗网。^[8]因此,暗网形成一种相对封闭的系统,不为外界所能轻易侵入,也由此形成一种“特殊”和“神秘”的色彩,容易使我国普通公众产生好奇心,以及使社会上的不稳定分子产生蠢蠢欲动的心理。第二,匿名性。这是指,访问暗网的用户身份、IP地址等信息均显得极其隐秘,无法直接获取其具体信息。如果说网络对访问者的个人信息“自带”某种程度的匿名性,那么,暗网则加强了这种匿名性并将其推向极致。第三,支付方式的特殊性。针对暗网上的交易所进行的支付不同于人们日常生活中所使用的货币,甚至也不同于网络交易通常使用的电子银行、支付宝、微信等支付方式,而是采取一种与暗网的匿名性相匹配的匿名支付方式——数字货币,如比特币。比特币属于一种P2P形式的数字货币,不同于国家发行的货币,其使用过程具有隐秘性。^[9]这种支付方式为那些意图寻求隐秘交易的人打开了方便之门。第四,违法犯罪信息的普遍性。充斥于暗网上的信息并非常规、合法信息,而往往是违法犯罪信息或者将导致违法犯罪发生的信息,前者比如淫秽色情视频,后者比如寻求买凶杀人信息,这一点使得暗网与我国相关法律法规造成重大冲突,也使得暗网在我国公众心目中往往留下可怕、阴暗、邪恶的印象从而对之具备戒备心和恐惧心。第五,无法追踪性。这是指,暗网访问者的相关信息及其在暗网上进行的交易结算,在事后均无法被具体确定、查明,尤其是交易信息在交易完成后即被清除^[10],导致了暗网访问者和暗网犯罪者“来无影,去无踪”,无人知晓其究竟在暗网上发布和取得了何种信息、进行了何种交易。第六,监管困难性。暗网一般游离于各国有关机关的监管之外,至少以普通的监管工具和技术手段,无法或很难对暗网上的动态进行有效、全面的监管。有学者认为访问便捷性^[11]、跨越地域范围较大性也是暗网的特点^[12],但既然暗网是从普通网络中所分离出来的子集,其特点的归纳必须体现其不同于普通网络的特殊之处,访问便捷性和跨越地域范围较大性属于普通网络的特征而非暗网的独特之处,所以不宜被视为暗网的特点。

就现实而言,暗网犯罪早已在全球蔓延开来并渗透入我国。如果从放眼世界而立足我国的角度,以实证的方法全面考察既定学术文献和新闻报道中关于暗网犯罪的各种信息,会发现就我国《刑法》而言,暗网犯罪主要涉及(经常涉及但不限于)以下罪名:第一,危害公共安全罪,主要包括非法买卖枪支、弹药、爆炸物罪,恐怖犯罪;第二,破坏社会主义市场经济秩序罪,主要包括出售、购买假币罪,走私罪,洗钱罪;第三,侵犯公民人身权利、民主权利罪,主要包括故意杀人罪(包括教唆犯),故意伤害罪,非法拘禁罪,拐卖妇女、儿童罪,侵犯公民个人信息罪,组织出卖人体器官罪;第四,妨害社会管理秩序罪,主要包括伪造、变造、买卖国家机关公文、证件、印章罪,伪造、变造、买卖身份证件罪,贩卖、传播、淫秽物品罪,侮辱尸体罪,贩卖毒品罪。其中,尤其值得我国重视的是暗网恐怖主义犯罪。最近,恐怖主义犯罪呈现日趋网络化的新动向,并且,恐怖分子为确保恐怖活动的策划和实施更为安全顺利,以及使内部成员的相互联系更加方便,已将暗网作为有力工具^[13],恐怖组织的网络化由此逐渐演变为危害性更大的暗网化^[14]。在当前我国与东突恐怖主义作斗争的过程中,恐怖犯罪暗网化的趋势值得我国高度警惕并应采取相关应对措施,以确保国家安全。

从所涉及罪名的种类来看,暗网犯罪主要集中在我国《刑法》分则中的侵犯公民人身权利罪和妨害社会管理秩序罪。刑法的任务是保护法益,而犯罪侵害了法益,前述两类犯罪说明了暗网犯罪的危害主要体现于其对公民人身法益和公共法益的侵害,这意味着,暗网犯罪已对我国社会最重要的利益——公民人身权、社会公共利益造成了严重的威胁。本文开始连续列举了3个涉及我国公民或在我国本土发生的暗网犯罪案件,第1个案件中受到侵害的是公民人身权,后两个案件中受到侵害的是社会公共利益。这并非偶然,说明了无论是在国外还是国内,暗网犯罪都与这两类法益紧密相关,可以据此预测,如果我国将来再次发生暗网犯罪案件,这两类法益也极有可能首当其冲地受到侵害。这是暗网的性质之一——重大法益的危害性。

从暗网犯罪所涉及的上述罪名种类还可以看出,这些罪名的实行行为并非暗网行为本身,而是

在日常生活时常可见的罪名,其问题的本质在于,暗网仅仅被作为一种有力的工具而促发了这些犯罪的发生。正是因为暗网所具备的特点使得暗网成为犯罪信息自由传播、外界又基本无法介入的工具,从而导致暗网犯罪的发生。这是暗网的性质之二——犯罪工具性。

根据以上论述可知,暗网的特点和暗网犯罪的种类决定了其具备两大性质——重大法益的危害性和犯罪工具性,从价值观的角度来看,为了保护我国公民中最重要的人身法益和社会公共法益,必须对暗网本身予以严厉制裁;从方法论的角度来看,应彻底取缔暗网这种平台,如此一来,暗网犯罪自然会失去发生的基础和可能性,可从根本上解决暗网犯罪的问题。

二、既定规制方式的问题和原因

暗网的上述特点和性质导致其被不少人加以利用而造成暗网犯罪大行其道,不少国家如美国、英国、德国、法国等国和国际刑警组织都已采取相关行动,还有一些国家如俄罗斯、韩国、越南已完善了针对暗网的立法。就我国具体情况而言,无论对暗网采取何种规制方式,在法治社会的现实语境中,这种规制方式都必须于法有据,才符合法治的原则,因而必须全面考察我国《刑法》中针对暗网的既定规制方式是否存在问题,才能具体地提出完善或改革既定规制方式的建议。然而,对我国《刑法》进行深入考察的研究范式迄今未引起我国学术界充分的注意,这表现为,以暗网的法律规制为主题的论文,在我国已发表的学术文献中只占极小的比例,以暗网的刑法规制为主题的论文则基本上呈现空白状态。大多数学者都试图从社会综合治理的角度对暗网提出规制方式,诸如加强暗网治理技术手段的研发、强化行政管理、推动政企合作、开展网络安全治理国际合作等。^[15]虽然以上手段具有较为全面周详的效果,但不可否认的是,相比其他规制方式,从刑事立法的角度考察和完善对暗网的规制方式,不仅能为暗网的规制获得法治上的正当性,还能运用刑罚的特殊和一般预防功能对既定或潜在的暗网犯罪分子形成强大的震慑,此外,还能以一种最强力、最长效的制度保障去防止今后任何形式的暗网工具死灰复燃,

从而一劳永逸地解决暗网犯罪问题。

宏观上,就我国立法现状而言,有学者一针见血地提出:“我国网络监管相关立法发展至今,已颁布了 60 余部法律法规和部门规章,但缺乏对暗网相关行为在法律上的具体规定。”^[16]因此,“应完善暗网行为在法律中的具体规定”^[17]。诚然,我国虽然迄今为止没有针对暗网的具体法律规定,亦即对暗网欠缺直接具体的法律规制方式,但有必要考察我国《刑法》中关于网络犯罪的规定是否可以适用于暗网,从而厘清我国刑事立法中的既定规制方式是否存在问题。

我国《刑法》原本没有网络犯罪的规定,但 2015 年我国《刑法修正案(九)》修改了我国《刑法》中第 285 条至第 287 条,增设了关于网络犯罪的 3 个新罪名,分别为:拒不履行信息网络安全管理义务罪、非法利用信息网络罪、帮助信息网络犯罪活动罪,但这些罪名面对暗网存在问题:

第一,没有一个直接针对暗网的罪名,无助于直接、全面、具体地规制暗网,只能从不同的侧面间接、部分、笼统地规制暗网,效果已大打折扣。

第二,拒不履行信息网络安全管理义务罪无助于彻底取缔暗网,效果由此大为减损。该罪属于纯正不作为犯,是将纯正的不作为规定为独立的犯罪类型^{[19]18},属于行为犯而非结果犯,其法条表述是:网络服务提供者不履行信息网络安全管理义务,经监管部门责令采取改正措施而拒不改正,情节严重。这意味着,该罪对暗网的规制存在以下漏洞:(1)仅将网络服务提供者作为行为主体,对其他网络参与者如暗网访问者、暗网信息发布者、暗网工具制作者等造成遗漏,以至于后者实施的诸多暗网行为都无法得到规制。(2)仅规制网络服务提供者实施的不作为而未规制其实施的作为,造成了重大的处罚漏洞。行为人的实行行为可分为作为和不作为。^{[19]26}网络服务提供者实施的暗网行为也可以是作为,比如直接在暗网上发布犯罪信息等,这类行为不属于不作为而无法受到本罪规制。(3)“拒不改正”的构成要件要素纵容了暗网服务提供者的不作为,暗网既然危害极大而应被彻底取缔,就不能以“拒不改正”这种带有行政法意义的要素作为入罪的门槛,否则将导致暗网犯罪的蔓延。

第三,非法利用信息网络罪对暗网行为的规

制也不全面。该罪的法条表述是:行为人利用信息网络设立用于实施违法犯罪活动的网站、通讯群组,或者发布违法犯罪信息,或者为实施违法犯罪活动发布信息,情节严重。可见,该罪虽然属于行为犯,可将网络服务提供者实施的、前罪无法规制的部分作为(如发布犯罪消息)纳入,但存在以下问题:(1)“设立用于实施违法犯罪活动”的构成要件要素容易给暗网参与者提供逃脱处罚的借口,因为暗网参与者建立暗网网站或通讯群组后可能提出:“我建立的暗网的目的并非为了实施违法犯罪活动,其他人是否以之用于实施上述活动,我并不知情。”如果没有充分证据证明暗网参与者具备此目的,其上述行为难以被认为构成此罪,造成暗网的建立无法受到该罪规制。除非取消该罪构成要件要素中的目的要素——用于实施违法犯罪活动,才能全面规制暗网行为。(2)“情节严重”这种客观处罚条件会导致对暗网犯罪的规制时点过于滞后。这是因为,暗网不同于普通网络,其具备的匿名性、无法追踪性、监管困难性等特点决定了一旦犯罪信息被发布于其中,其造成的危险就难以得到有效的控制,直至这种危险转化为实害,已为时晚矣。此外,“情节严重”的定位在我国刑法学界有争议,如果有学者将之定位于构成要件要素^[20],那么,根据故意的成立要求——行为人应对客观构成要件要素有认识和意欲才能成立故意^{[21]44},暗网参与者如果未认识到其行为可能导致“情节严重”,其行为就不构成该罪,非法利用信息网络罪是我国《刑法修正案九》设立的新罪名,面对暗网犯罪的规制,该罪的特殊性在于,似乎“非法利用信息网络”可以直接涵摄暗网参与者的行为,那么该罪就可以直接规制暗网行为,但这只是感觉和表象而非本质和真相。从罪刑法定原则的明确性要求和犯罪论体系的构造来看,必须详细分析该罪的构成要件要素。如前所述,一旦细察该罪的构成要件要素,会发现该罪的目的要素“用于实施违法犯罪活动”和“情节严重”这一客观处罚条件对暗网参与者的行为而言,实际上起到的不是入罪而是出罪效果,这意味着该罪对于暗网行为的规制作用极其有限,反过来证明了以该罪来规制暗网行为并不切合实际。

第四,帮助信息网络犯罪活动罪对暗网参与

者的行为基本没有规制效果。该罪的法条表述是：行为人明知他人利用信息网络实施犯罪，为其犯罪提供帮助，情节严重。暗网参与者一般直接在暗网上发布犯罪信息，比如出售公民个人信息等，直接支配了实行行为的实施，根据刑法学上的犯罪支配说，其行为属于直接正犯而非任何形式的共犯。该罪规制的是对暗网参与者实施暗网行为的帮助，即暗网行为的帮助犯，从而对暗网参与者实施的直接正犯不当地形成了规制漏洞。

综上，我国《刑法》中关于网络犯罪的所有规定，不仅在宏观上欠缺专门规制暗网的罪名，其既定罪名都对暗网行为存在各种处罚漏洞并且规制时点较为滞后，即使通过刑法解释也无法解决问题。^[23]因此，既定规制方式对暗网的效力受到极大的减损，无法从源头上彻底解决暗网犯罪问题。

之所以出现以上弊端，归根究底是因为暗网对我国而言毕竟属于新兴事物，刑事立法的针对性回应显得不够及时。此外，立法者、学术界和实务界可能误认为我国《刑法》中关于网络犯罪的3个既定罪名可以充分规制暗网和防范暗网犯罪，无须修改立法。然而，诚如笔者在上文中论证，既定罪名根本无力全面、有效地规制暗网。因此，我国的刑事立法应当立即正视并重视当前我国网络犯罪的新趋势，以新眼光、新思维去提出新举措，以有针对性地规制暗网，而不能固守“立法无须修改”的传统思维而导致暗网犯罪将来可能在我国失控。

三、新规制方式的提出

（一）理论借鉴和修法原则

由于暗网具备重大法益侵害性和犯罪工具性这两大性质已达到让我国社会无法容忍的地步，并且由于我国《刑法》对暗网的既定规制方式存在上述问题，对既定罪名采取“小修小补”的修改方式，无法起到釜底抽薪的规制效果。因此，我们有必要增设新的、直接规制暗网行为的罪名，才能彻底取缔暗网平台，从而彻底杜绝暗网犯罪。之所以应以新设罪名的方式来彻底取缔暗网，其理论根据还可借鉴德国的敌人刑法理论。德国学者京特·雅科布斯曾提出在刑法学界较为知名的敌人刑法理论：“传统的遵守比例原则的刑法为‘公民刑法’，其仅适用于愿意订立并遵守社会契约的公

民。但破坏社会契约的人属于公民的‘敌人’，无权适用‘公民刑法’，而应适用减损法治国原则的‘敌人刑法’。”^[23]^[1704]暗网既然已成为网络中难以追踪、控制的“毒瘤”，危害了我国社会和个人最重要的法益，并与新型恐怖主义犯罪紧紧勾连，应被视为我国社会的“敌人”而予以彻底摧毁，不能在刑事立法上对其留有任何余地。类似情形如同我国《刑法》分则对恐怖主义、黑社会、毒品等犯罪等设立的相关罪名，立法者对相关行为方式采取了极其严密的规制方式，以及对相关行为人处以重罚，是因为恐怖主义等相关行为给我国社会带来的极大危害性使得相关行为人类似于反社会的“敌人”，对相关行为方式进行的彻底禁绝和对相关行为人采取的重罚，恰好反映了刑事立法对我国社会的强大保护。因此，将暗网视为“敌人”而通过立法彻底取缔，在当前我国具备极强的现实意义。

然而，必须考虑到，我国的国家机关在行使行政、监察、审判、检察、军事权力时，完全可能实施某些暗网行为，这是保证国家权力的正常行使所必须的，应予正当化，从违法性层面将其行为排除在犯罪成立之外。因此，以新设罪名的方式彻底取缔暗网，不能机械地理解为任何主体在任何情况下都不能实施暗网行为，其本质上是对暗网民用化的彻底禁止。

此外，在新罪名的设计之前，修法原则的先行确定极为重要，因为这可以从宏观上为新罪名的具体设计提供一条正确的思路，使之在大方向上不出偏差。可根据刑法理论，将修法原则确定如下：

第一，将暗网行为的帮助行为正犯化。一般而言，帮助行为属于共犯而非正犯，其不法内涵和处罚均低于正犯，所以有学者认为网络犯罪的帮助行为不宜正犯化^[24]，但暗网既然具备不同于普通网络的特殊性，如果不将暗网的帮助行为正犯化，就无法实现与其危害性相匹配的定罪和量刑，因此，以立法推定的方式进行这种正犯化是必要的。

第二，将“情节严重”这种客观处罚条件从罪名的法条表述中删除。以此方式，不仅可以避免在学界发生“情节严重”属于构成要件要素还是客观处罚条件的争议，从而导致发生相关认识错误如何解决的难题，还可以最大限度地规制暗网行为，由此实现“一箭双雕”的效果。

第三,增加抽象危险犯的适用。犯罪可划分为行为犯和结果犯^{[25][286]},行为犯中又包括抽象危险犯。抽象危险犯的实质是将结果和危险从某种犯罪的客观构成要件要素中排除出去,并且实行行为无须侵害法益时才能既遂,当实行行为的某个“行为点”在不同的个案中有侵害法益的危险或没有该危险时,或者说,不回到个案中去具体判断而是抽象地判断,发现这个“行为点”有侵害法益的危险时,该“行为点”则为既遂时点。因此,抽象危险犯的既遂时点亦即处罚时点在所有的犯罪类型中最为提前,可由此充分保护法益不受到任何被侵害的危险。以抽象危险犯的设定来规制暗网犯罪,正好与暗网的性质相匹配。

第四,增加纯正不作为犯的适用。犯罪还可划分为作为犯和不作为犯,不作为犯可进一步划分为纯正不作为犯和不纯正不作为犯。由于纯正不作为犯的构成要件要素不包括结果的发生及其与实行行为之间的因果关系^{[26][657]},这意味着其以特殊的构成要件所蕴含的较大涵括性,起到了对法益强大的保护效果,可由此用于规制不关闭暗网、不取消暗网工具等不作为。

第五,暗网的罪名设计无须考虑适用中立帮助行为理论。有学者提出:“传统理论和司法解释一贯认为,只要行为客观上促进了他人实施犯罪,行为人在主观上也对此明知,就应作为帮助犯受到处罚。这种不加区别的做法极可能导致过于限制公民日常生活中的交易、交往自由。”^[27]必须明确的是,暗网具备违法犯罪信息的普遍性,该特点决定了在暗网发生的交易中,相当一部分都属于违法犯罪交易,如果对暗网上的交易自由应予无条件的保护,付出代价的将是我国社会和个人最重要的法益。此外,正当、合法的交易完全可以通过普通网络来进行,没有必要通过暗网来进行,暗网中发生的交易由此欠缺保护必要性。因此,在暗网的罪名设计上,必须遵循刑法通说,不能以中立的帮助行为理论为暗网的帮助行为除罪化。

(二) 规制范围

以增设新罪名的方式规制暗网,需要明确其规制范围,亦即这些罪名的构成要件效力范围。从事实和逻辑的角度,可将暗网的规制范围分为两大板块:暗网及其工具的核心行为和暗网访问的

核心行为。首先应明确的是,如果国家机关根据法定程序实施了上述被规制的行为,应一律正当化,将其排除在犯罪成立之外。具体而言,被规制的行为如下:

1. 有关暗网及其工具的核心行为

这些行为包括:(1)建立暗网和不关闭暗网。暗网包括网站(以及独立网页)、通讯群组、交易平台等。行为人建立暗网的行为是暗网规制的核心内容,理应首先被禁止实施。不关闭暗网是指行为人建立暗网后不履行关闭义务的不作为。建立交易平台的行为由于与暗网犯罪的关联最为直接和紧密,应从重处罚。(2)制作暗网工具和不取消暗网工具。暗网的工具包括访问工具(如 Tor 等)、数字货币(如比特币、莱特币等)。行为人制作访问工具的行为应被禁止,对于已制作的访问工具应承担取消义务,如通过技术手段予以删除、最大限度降低其使用可能性或使用效果。行为人制作数字货币的行为也应被禁止,对于已制作的数字货币应负取消义务。对暗网及其工具进行任何形式的加工,也应视为建立、制作行为。关于如何判断网站、通讯群组、访问工具、数字货币是否属于“暗网及其工具”,可由我国网监机关进行审查和作出判断。

如果行为人没有制作暗网工具,而是实施了其他边缘行为,包括下载、使用、传输、持有访问工具及其类似行为,以及对数字货币进行购买、出卖、提现、持有及其类似行为,这些行为因危害性有限,由此受到刑法最后手段原则^{[28][22]}的限制而不应被规制。

2. 有关暗网访问的核心行为

这些行为包括在暗网上传信息、下载信息、传输信息。上传信息包括发布信息、共享信息、回复信息、相互联络等,下载信息包括复制信息等。这些属于有关暗网访问的核心行为,与有关暗网及其工具的核心行为相互呼应,可以说,没有前者行为,后者行为也会失去意义、难以为继。因此,后者行为对暗网犯罪的促发性及由此而来的危害性,仅次于前者行为,两者共同致力、直接参与了暗网状态的改变,应同样受到规制。

如果行为人未在暗网上传、下载、传输信息,而是单纯地进入、浏览暗网,以及注册通讯群组,由此未对暗网造成任何状态上的实质改变,这些

边缘行为同样因危害有限和受到刑法最后手段原则的限制而不应被规制。

通过确立以上规制范围,可为新罪名的构成要件划定一个精确的效力范围,通过罪与非罪的细致区分来实现罪刑法定原则的明确性要求^{[29][42]},同时最大限度地起到彻底取缔暗网的效果,并顾及了国家机关的权力行使和公民的行为自由。

(三)新罪名的内容和解释

根据上文提出的修法原则和规制范围,可在我国《刑法》分则中增设5个关于暗网的罪名,分别列举如下:(1)非法建立暗网或制作暗网工具罪。该罪的法条表述是:行为人未经国家机关授权,建立的网站、通讯群组、交易平台等被网监机关鉴定为暗网,或者制作的访问工具、数字货币等程序被网监机关鉴定为暗网工具。已建立的平台无论是否含有违法犯罪交易的信息,都应从重处罚建立者。(2)非法帮助建立暗网或制作暗网工具罪。该罪的法条表述是:行为人帮助他人未经国家机关授权建立暗网或者制作暗网工具。该罪是非法建立暗网或制作暗网工具罪的帮助犯,可分为作为的帮助和不作为的帮助两类。作为的帮助,是指行为人实施的某种行为对他人未经国家机关授权建立暗网或制作暗网工具起到直接的促进作用,具体而言,使得后者行为更容易被实施。不作为的帮助,是指具备暗网监管义务的行为人未履行其监管义务,不阻止或不处理他人未经国家机关授权建立暗网或制作暗网工具。(3)不关闭暗网、取消暗网工具罪。该罪的法条表述是:行为人未经国家机关授权建立暗网或制造暗网工具后,在30天内或经网监机关警告后不采取任何手段关闭该暗网或取消暗网工具。(4)非法在暗网上传、下载信息罪。该罪的法条表述是:行为人未经国家机关授权,在暗网上传信息(发布信息、共享信息、回复信息、相互联络等)或者下载信息(复制信息等)。(5)非法帮助他人在暗网上传、下载信息罪。该罪的法条表述是:行为人帮助他人未经国家机关授权在暗网上传信息或者下载信息。该罪亦可分为作为的帮助和不作为的帮助。作为的帮助,是指行为人实施的某种行为对他人未经国家机关授权在暗网上传、下载信息起到直接的促进作用。不作为的帮助,是指具备暗网监管义务的行为

人未履行其监管义务,不阻止或不处理他人未经国家机关授权在暗网上传、下载信息。

针对上述5个暗网罪名,需要说明的是:第一,通过法条表述的具体内容,将应受处罚的暗网行为“一网打尽”,排除了诸如下载暗网访问工具在内的所有边缘行为,并将国家机关依照法定程序实施的暗网行为排除在外,由此在法益保护、公权行使、公民自由之中找到了一个最大的平衡点。第二,在罪名设计的宏观原则上,充分运用了刑法学基本原理:不仅将“情节严重”这种客观处罚条件排除在犯罪论体系之外,还确立了2个抽象危险犯(罪名1、罪名4)、2个帮助犯(罪名2、罪名5)、1个纯正不作为犯(罪名3),以此方式最大限度地规制了暗网行为。当然,在个案中,如果行为人的犯罪情节较为轻微,法官可以对行为人从宽处罚,以实现罪刑相当原则。第三,该罪的保护法益为复合法益,包括公民个人利益的安全、社会公共利益的安全、网络的安全三个具体法益。其中,暗网的特点和性质、暗网犯罪所涉罪名的种类联合决定了新罪名的实行行为与公民个人利益、社会公共利益的安全紧密相关,正基于此,新罪名的保护法益首先是上述两个具体法益,其次才是网络的安全。

四、结语

“互联网+”时代中,暗网犯罪在全球的猖獗及其近年来在我国的不断发生值得全社会、学术界和立法者的警惕。暗网具备的不同于普通网络的特点及其在现实中所涉犯罪的种类,决定了暗网具备重大法益侵害性和犯罪工具性两大性质,为了保护我国公民个人法益和社会公共法益不受暗网犯罪的侵害,在确保国家机关为了公益依法使用暗网应受保护的前提下,应对暗网采取彻底取缔的态度,但我国《刑法》中的既定规制方式无法充分、有效地规制暗网,因此,可增设规制暗网行为的5个新罪名,并以具体的法条表述明确清晰地划定应受规制的暗网核心行为,排除不应被规制的暗网边缘行为,在规制暗网的同时保护公民的行动自由。通过以上方式,可从根源上防范暗网犯罪在我国继续发生,充分、有效地保障我国公民个人利益、社会公共利益和网络的安全,彻底终结网络中的“暗黑”。

参考文献:

- [1] 张黎明.我市警方通报侵犯公民个人信息犯罪典型案例[N].金华日报,2018-09-20.
- [2] 龚轩.我省开展“2019 净网专项行动”已抓获嫌犯 312 人,破获全省首起涉“暗网”案[N].湖北日报,2019-03-12.
- [3] 李新文,崔再华.“暗网”,多少罪恶假汝而行[J].网信军民融合,2018(1).
- [4] 陈莹,赵子竣,狄珂,等.从暗网谈隐蔽信道对网络执法的威胁[J].法制博览,2018(6).
- [5] 梁晓轩.揭开暗网的神秘面纱[J].检察风云,2017(23).
- [6] 范江波.暗网法律治理问题研究[J].信息安全研究,2018(1).
- [7] 赵志云,张旭,罗铮,等.“暗网”应用情况及监管方法研究[J].知识管理论坛,2016(2).
- [8] 王佳宁.暗网对国家安全的危害[J].网络安全技术与应用,2016(9).
- [9] 秦玉海,杨嵩,陈杰.针对“暗网”的监管机制研究[J].辽宁警察学院学报,2017(5).
- [10] 胡立.解密暗网 6 大领域趋势[J].计算机与网络,2018(20).
- [11] 杨亚强.暗网恐怖主义应对路径探析[J].江西警察学院学报,2017(4).
- [12] 黄紫斐,刘洪梅,张舒.基于暗网环境的网络恐怖主义及其治理[J].信息安全与通信保密,2018(12).
- [13] 张伟伟,王万.暗网恐怖主义犯罪研究[J].中国人民公安大学学报(社会科学版),2016(4).
- [14] 赵航,曾帝.论恐怖组织暗网化趋势[J].唐山师范学院学报,2019(1).
- [15] 倪俊.从社会治理角度认知暗网的威胁与应对[J].信息安全与通信保密,2017(11).
- [16] 焦康武.总体国家安全观视域下我国暗网犯罪应对研究[J].犯罪研究,2017(6).
- [17] 罗军舟,杨明,凌振,等.匿名通信与暗网研究综述[J].计算机研究与发展,2018(12).
- [18] Hans-Heinrich Jescheck. Lehrbuch des strafrechts allgemeiner teil[M].Berlin: Duncker & Humblot,1996.
- [19] Frank Zieschang. Strafrecht allgemeiner teil[M]. Berlin: Richard Boorberg Verlag,2017.
- [20] 余双彪.论犯罪构成要件要素的“情节严重”[J].中国刑事法杂志,2013(8).
- [21] Claus Roxin. Strafrecht allgemeiner teil band I grundlagen·der aufbau der verbrechenslehre[M]. Berlin: Verlag C. H. Beck,2006.
- [22] 张明楷.网络时代的刑事立法[J].法律科学,2017(3).
- [23] Dirk Sauer. Das strafrecht und die feinde der offenen gesellschaft[J]. Berlin: Neue Juristische Wochenschrift, 2005(58).
- [24] 刘艳红.网络犯罪帮助行为正犯化之批判[J].法商研究,2016(3).
- [25] Reinhart Maurach. Strafrecht allgemeiner teil 1 erschcheinungsformen des verbrechens und rechtsfolgen der tat[M]. Berlin: C. F. Müller,1992.
- [26] Eberhard Schmidhäuser. Strafrecht allgemeiner teil lehrbuch[M].Berlin: J. C. B. MOHR(Paul Siebeck) Tübingen,1970.
- [27] 陈洪兵.论中立帮助行为的处罚边界[J].中国法学,2017(1).
- [28] Friedrich-Christian Schroeder. Festschrift für reinz maurach zum 70. geburtstag[M].Berlin: C. F. Müller,1972.
- [29] Urs Kindhäuser. Strafrecht allgemeiner teil[M].Berlin: Nomos,2015.

责任编辑 顾理辉

Crimes about the Dark Web of China and Their Criminal Regulation in the Times of “Internet+”

WANG De-zheng

(School of Law, Sichuan Normal University, Chengdu 610068, China)

Abstract: In recent years, dark web crimes are constantly identified in China. The dark web has two properties, namely harming the important legal interests and the criminal instrument, which are intolerable in our society. In order to protect the personal legal interests of the Chinese citizens and the social public legal interests from the harm of the dark web, the theory of “criminal law towards enemy” in German criminal law is used for reference and the dark web should be completely forbidden. However, the present Criminal Law in China cannot be applied to regulate and punish the dark web effectively. Some relevant principles of revising are proposed by using the basic theory of the criminal law, five new crimes should be added to regulate the dark web conducts, and specific descriptions should be used to define the core conducts about the dark web which are deserved to be regulated and punished, and the board-line conducts about the dark web which are not deserved to be regulated should be excluded. The government should be entitled to use the dark web legally. In this way, the crimes related to the dark web can be fundamentally prevented and the personal legal interests of the Chinese citizens, the social public legal interests as well as the web safety can be protected effectively.

Key words: times of “Internet+”; dark web crimes; criminal regulation; Internet safety