Doi:10. 11835/j. issn. 1008-5831. fx. 2020. 04. 002

欢迎按以下格式引用:庞云霞,张有林. 大数据时代网络犯罪的刑法应对——兼论人工智能犯罪的规制[J]. 重庆大学学报(社会科学版),2022(4):230-238. Doi:10. 11835/j. issn. 1008-5831. fx. 2020. 04. 002.

Citation Format: PANG Yunxia, ZHANG Youlin. Criminal law response to cybercrime and the regulation of artificial intelligence crime in the big data era[J]. Journal of Chongqing University (Social Science Edition), 2022(4):230-238. Doi:10. 11835/ j. issn. 1008-5831. fx. 2020. 04. 002.

大数据时代网络犯罪的刑法应对
——兼论人工智能犯罪的规制

庞云霞[1],张有林[1,2]

(1. 山西大同大学 法学院,山西 大同 037009;2. 陕西师范大学 哲学与政府管理学院,陕西 西安 710119)

摘要:网络技术发展促成了网络代际更迭。在大数据为核心的Internet 3.0阶段,网络在犯罪中的作用和地位发生变化,网络的刑法属性由传统的犯罪对象、工具演变为网络犯罪的场域空间和存在方式。网络犯罪的表现形式也随之演化,在传统犯罪网络化趋势加强的同时,出现了人工智能犯罪等新的犯罪形态。在对比网络犯罪与传统犯罪的危害性评价差异的基础上,可以将网络犯罪区分为三种类型:危害性评价等价于传统犯罪的网络犯罪类型、线上线下危害性评价背离的网络犯罪类型、以网络大数据为核心的新型网络犯罪,后者尤以人工智能犯罪为代表。人工智能的法律问题冲击着以人为核心的法律制度体系,也给刑法提出了新的命题。

大数据、云计算以及人工智能技术的发展,意味着新的风险时代的到来。刑法对以网络为工具和对象的犯罪进行了有效立法应对,但对大数据时代的网络犯罪规制不力,对以"网络为空间"的犯罪应对不力,对以" 网络为存在本质"的犯罪尚未作出实质回应。刑法缺乏应对新型网络犯罪的风险机制,一是对大数据系统安全、算法安全和数据与信息安全为内容的新型网络安全风险应对不足,二是对滥用人工智能技术、人工智能技术瑕疵带来的刑事风险缺乏应对。同时,在立法规制网络犯罪的过程中,刑法对计算机信息系统予以了必要重视,但失衡于网络安全法益的保护,尤其对网络公共安全和数据信息安全未予以必要重视。刑法应当进行立法调整,建立风险刑法理念,对大数据时代的网络安全风险和技术风险进行刑事预防,明确对网络公共安全法益的立法保护,其内涵为包括网络空间的数据和以信息为内容的网络秩序的安宁性;建立网络安全法益的保护体系,并增设新罪名对新型网络犯罪行为予以规制;明确人工智能在网络犯罪中的工具属性和非主体性,确立对利用可控型人工智能犯罪的过错责任、对自控型人工智能犯罪的监督过失责任;通过选择适当的路径和立法技术实现刑法对网络犯罪的应对。

关键词:刑法网络空间效力;网络犯罪;人工智能犯罪;立法回应

中图分类号:D924. 3 **文献标志码**:A **文章编号**:1008-5831(2022)04-0230-09

基金项目:山西省哲学社会科学规划课题"晋北乡村精准扶贫中微腐败问题治理研究"(2019B284)

作者简介:庞云霞,山西大同大学法学院,Email:617840805@ qq. com;张有林,山西大同大学法学院,陕西师范大学哲学与政府管理学院。

随着网络技术的发展,传统犯罪呈网络化的趋势,新型网络犯罪不断出现。大数据、云计算以及人工智能技术的发展,意味着新的风险时代的到来。人工智能的法律问题冲击着以人为核心的法律制度体系,也给刑法提出了新的命题。如何在全球化的互联网中实现刑法对网络犯罪的规制,是网络时代刑法转型需要直面的问题。

一、网络变迁背景下的网络犯罪

网络技术决定着网络的更新换代,也是网络犯罪演变的决定因素。随着大数据、物联网、区块链技术的互融发展,网络犯罪的表现形式也相应演变,在传统犯罪网络化趋势加强的同时,出现了人工智能犯罪等新的犯罪形态。

(一)网络之于网络犯罪的刑法属性变迁:“犯罪对象”“犯罪工具”到“犯罪空间”“犯罪本质”

1.“犯罪对象”和“犯罪工具”

Internet 1.0 阶段,计算机信息系统安全是网络安全的核心。网络犯罪多表现为以计算机系统安全作为目标的技术行为,植入、传播病毒是主要的行为方式。网络犯罪的外延同“计算机犯罪”重合,网络主要作为犯罪对象出现。Internet 2.0 阶段,网络社交成为网络活动主流,信息是网络活动的核心。在传统的以攻击计算机系统为主的犯罪不断减少的同时,以网络活动形式实施的犯罪迅速增长,网络的犯罪工具属性凸显。因网络行为的虚拟性、瞬时性、无界性,犯罪得以规避在物理世界中时间、场所、物证等方面的不利境地,传统犯罪借助网络技术实现了网络化。

2.“犯罪空间”与“犯罪本质”

Internet 3.0 阶段以大数据为核心,网络呈现三网资源共享的融合趋势,网络活动摆脱了以网址为基础的“点对点”的活动方式。网络与现实社会实现了融合,原本在现实世界进行的工作、安全认证、货币支付等事宜均得以甚至必须借助网络进行。大部分犯罪行为都可以在网络空间和现实社会两个层面实现危害效果。网络的刑法地位,在“犯罪对象”与“犯罪工具” 的基础上演化为犯罪存在的场域,成为“犯罪空间”[1]。

随着人工智能被广泛运用于交通、医疗、法律等领域,人工智能的法律问题已突破民事主体资格、作品的知识产权归属等领域,向刑事领域拓展和延伸。人工智能犯罪时有发生,依托大数据、算法而生的新型犯罪现象出现。人工智能犯罪的表象是其在自主意识下完成的行为,本质是以网络数据运算为内核的违法、犯罪活动。对于利用大数据与算法进行的网络犯罪而言,网络是其根本所在,网络可以是犯罪存在的空间与场域,也可以是犯罪的本质与存在方式。

(二)网络犯罪的嬗变:等价、背离、异化

网络犯罪与传统犯罪的差异性对比,可依危害性评价作为切入点。对网络犯罪的类型演变进行梳理,可将网络犯罪归纳为如下类型。

1.等价于传统犯罪的网络犯罪

“等价型”指犯罪行为变身为网络行为后,社会危害性未发生量变,行为性质也未发生质变的情形。网络仍旧是犯罪的对象或工具,网络犯罪没有发生本质变化,是传统犯罪场所切换后的表现形式。利用网络、计算机实施的犯罪,是对传统犯罪的形式改造,只是增加了网络或计算机信息系统这一介入因素。所以,这种类型的网络犯罪,“传统的定罪量刑标准等规则体系基本上没有发生变化,网络只是犯罪的手段,网络犯罪针对的仍然是现实社会的法益”[2]。

2. 网络与现实空间的危害性评价背离的网络犯罪

“背离型”指同一犯罪行为在虚拟社会和现实社会中呈现完全不同危害后果,因此产生截然不同的法律评价。其一,危害性聚变的网络犯罪。网络空间的信息活动具有瞬时性、无界性的特点,因此,网络是以数据信息为对象的犯罪活动的温床。较之于传统犯罪,网络信息犯罪因打破空间和时间的限制,危害性激增。信息散布型网络犯罪即是范例。其二,危害性弥散的“网络犯罪”,指传统犯罪进入虚拟网络后,被法律评价为不具有危害性,不构成犯罪的情形。该类型的犯罪产生具有时空上的阶段性[3]。刑法本身的滞后性使然,必然会出现“漏网之罪”,随着立法的调整又可能会重新进入刑法的规制范畴。诸如“刷单”营销、违法P2P借贷、组织网络传销等,刑法对这些行为在线上和线下的定性不同,这种评价差异在行业的网络行为模式形成初期尤为明显。

3. 异化的网络犯罪与人工智能犯罪

大数据、算法、算力等技术手段是当下网络产业发展的有力支撑,大数据时代的网络行为是以网络数据信息为核心进行的。滥用大数据和算法随之成为犯罪方式之一。人工智能是大数据运算技术发展的阶段性成果。“从法律属性上可以将智能机器人定位为经程序设计和编制而成的、可以通过深度学习产生自主意识和意志的、不具有生命体的人工人”[4]。不拘泥于外形和物理存在形态,人工智能以自主程度为标准,包括弱人工智能、强人工智能、超人工智能三类。其中,超人工智能是超越人类的高级智能,当前停留在科学设想阶段,本文暂不涉及。弱人工智能的智能是表面的、非实质性的,其运行决策取决于人类的设计编程,不具备独立的判断与决定能力,是比较低级的人工智能,即只是在特定领域、特定用途的智能化,本质上是工具的一种。强人工智能是能进行推理和解决问题的智能机器,有知觉和意识能力,能自主进行数据运算、决策产生和行为控制,具备取代人工决策的能力。

所有的技术都有被利用作为犯罪工具的可能,人工智能亦如此。此外,人工智能系统无法避免“算法黑箱”“算法歧视”等带来的运算结果瑕疵,不可避免会出现风险。根据自主程度对人工智能犯罪可进行如下分类:其一,自主意识和控制能力较低,被利用作为犯罪工具的被控型人工智能犯罪;其二,脱离其制造者和控制者,意识和控制能力自主的自控型人工智能。被控型人工智能犯罪可以在现有的犯罪理论和规则体系的语境下进行解析,自控型人工智能犯罪的主体资格认定、归责机制等则需要进行论证和探讨[5]。在人工智能的语境下,法律主体资格的认定及意识能力的判定成为一个伦理问题,人工智能犯罪的主观构成、主体资格、归责原理亦是新的命题。

二、刑法网络空间效力实现的新命题——刑法的回应与障碍

网络代际更新背景下,为应对不断变化的网络犯罪态势,刑法立法调整是必然之举。我国刑法的沿革进程呈现阶段性特征,采用法律解释和刑法修正案两种方式对刑法典进行完善,拓宽了刑法对网络犯罪行为的管辖视域和规制范畴。

(一)刑法的应对与立法沿革

对于Internet 1.0到2.0阶段的网络犯罪,刑法的立法回应体现了网络的“对象”属性和“工具”属性。网络1.0阶段,刑法中设置了非法侵入计算机信息系统罪、破坏计算机信息系统罪,并对以计算机信息系统为对象的侵入、破坏行为进行规制;对以计算机技术为工具实施的传统犯罪进行了提示性规定。网络2.0阶段,传统的罪名原则上可继续适用,通过扩张解释可以实现刑法对大部分网

络犯罪的规制。如《刑法修正案(七)》严密了网络犯罪的罪名体系,扩大了对危害网络信息系统安全行为的打击面。增设非法获取计算机信息系统数据等罪名,法益由特殊领域计算机信息系统安全扩大为所有计算机系统安全和"数据过程"安全,危害行为类型扩大为四类:侵入、破坏、获取、控制。对于提供技术性程序、工具的帮助行为进行规制,强化了对以网络技术为工具的犯罪制裁。

Internet 3.0 阶段,刑法对网络犯罪行为的规制范围进一步扩大。传统犯罪论对于网络犯罪中"技术中立"的帮助行为、预备行为危害性评价无力,与其实际危害程度不符。《刑法修正案(九)》增设四个"纯正网络犯罪",这一举措是犯罪构成理论在应对网络犯罪水土不服时的有效转型。拒不履行信息网络安全管理义务罪强化网络服务提供者的网络安全管理义务,是对"不作为型实行行为的认定"[6]。非法利用信息网络罪将为实施违法犯罪活动设立网站、群组,发布违法信息的犯罪预备行为规定为独立的犯罪,即"预备行为实行化"[6]。帮助信息网络犯罪活动将明知他人网络犯罪,而为其提供技术工具、或广告、支付结算等帮助行为规定为独立的犯罪,即"帮助行为正犯化"[6]。

(二)立法回应的审视与命题提出

检视上述立法进程,不难发现,由于无法避免立法活动与生俱来的滞后性,刑法应对网络新型犯罪力有不逮,存在先天缺陷和后天不足。表现为:立法时机的被动性和前瞻性匮乏;立法观念未成型和立法格局缺失;立法内容碎片化;立法定量的可操作性差[7]。网络犯罪带来的风险可能性是现代刑法必然应对的挑战,遏制信息网络犯罪黑数较大的局面是新的命题[8]。当下刑法对网络犯罪的效力发挥存在诸多掣肘因素,如何化解阻力寻求刑法效力发挥的有效路径,是大数据时代网络刑法的重要使命。

1. 网络犯罪的风险应对机制匮缺

网络大数据时代,刑法对于以网络为"工具""对象"的犯罪已然进行有效应对,然而对于以"网络为空间"的犯罪回应不力,对于以" 网络为本质"的犯罪尚未作出实质回应。

从网络构成的层面分析,以系统和数据两个核心网络安全要素为视角,大数据时代的网络安全风险主要有系统安全、算法安全和数据与信息安全。(1)系统安全。由于智能硬件的系统漏洞、技术风险以及生产链条可能存在的产品瑕疵,系统安全的技术风险易被犯罪人利用。(2)算法安全。以大数据为基础的算法、算力等技术无法杜绝"算法黑箱""算法歧视"等对运算与决策的影响,运算后果具有失真的可能,亦有为人不当利用实施犯罪的可能。(3)数据与信息的安全。"大数据"" 云计算"背景下的海量数据分析,不可能在取得分析对象授权的情况下进行,传统的个人信息权益保护机制难以发挥作用[9]。如"监控国家"的数据监控常态化证明了"智能"运算可以在立场偏向的情况下运行,传统隐私保护制度在大数据时代有失效的风险[10]。

人工智能技术风险是风险社会的新内容。人工智能时代的刑事风险表现为:其一,人工智能在脱离控制、独立意识的情况下完成的犯罪;其二,部分传统犯罪的危害性因人工智能的技术性而扩大;其三,人工智能被滥用的风险。一种可能是人工智能产生伊始便与大数据滥用结合;另一种可能是人工智能运行中被不当利用。因此人工智能存在被直接用于犯罪的可能,也可因产品瑕疵或病毒等原因而实施犯罪行为[11]。

2. 网络安全法益的保护失衡

纵观网络 1.0 到 2.0 阶段的立法沿革,我国刑法通过对技术安全的防护,重点突出了对计算机

信息系统的保护,却失衡于对网络安全和数据信息安全的保护。“大数据”背景下,技术法益的主导地位被取代,而刑法对信息与数据法益反应迟缓[12]。围绕大数据的立法空白,立法重点应从技术安全、系统安全视角转向网络安全,网络空间的公共安全和数据信息安全必须成为重点保护对象,实现“从系统思维转向网络思维”[13]。

当下,传统法益与网络结合实现了内涵转型,网络安全法益作为体系性的概念进入法律视野,并逐步实现对传统刑法法益的改造和替换,网络安全成为关系国家安全、公共安全和公共秩序的重大法益[12]。在整体滞后的背景下,刑法未体现对网络安全法益的整体构建和重要性评价,既有的网络安全法益在刑法中呈现碎片化和失衡的样态。刑法将网络犯罪置于扰乱公共秩序罪之中,按传统犯罪处理以网络为工具的网络犯罪,只是犯罪形式与犯罪工具的变异,未将网络秩序和网络空间安全作为法益予以系统保护,同时不能应对以大数据为本质的人工智能犯罪。

三、刑法网络空间效力的实现——命题解析与立法构想

刑法应当寻求合理的立法路径以破解上述障碍因素:确立风险刑法理念和监督过失责任;将网络安全法益概念化,对新型网络犯罪行为予以规制。

(一)风险刑法理念的确立

面对网络犯罪所带来的风险,传统刑法的归责原则已无法适应,有必要适用风险刑法理论。风险刑法理论是刑法为对抗工业文明可能产生的刑事风险,一改其谦抑性特点而逐渐扩大干预面的犯罪预防理论。刑法作为社会风险控制机制的一部分,主要使命不再集中于对既有的犯罪及其危害后果施加报应刑,而是为遏制社会风险进行预防和威慑,威慑成为适用刑罚措施的核心逻辑依据。这为刑法应对人工智能时代的风险提供了有益借鉴,风险刑法是应对风险社会网络犯罪局面的必然之举[11]。从网络的演进可以看到,风险社会在未来演进中的主要表现形式就是网络空间社会。在网络社会,防控网络技术风险,保护网络空间安全已成为刑法的首要目标。“传统的罪责刑理念已经陷入失灵状态,安全刑法观作为回应风险社会的理论产物,成为网络刑法学的重要理论成分与外部形态表征”[12]。在风险刑法的理念指引下,应当通过变事后法为预防刑法,实现刑法对网络犯罪治理模式的转型;并设计前瞻性的罪名体系,以应对网络犯罪的变化形式。

(二)网络安全法益的保护

在网络语境下,对于已存在于罪名体系中的传统法益,因网络犯罪侵犯的法益与传统法益内涵重合,故可依据现行立法进行规制或通过修正、解释的方法延伸刑法规定的适用。对侵犯新法益的“犯罪行为”,现行法律存在评价不周延或法律真空的情况,最典型的是网络安全法益的碎片化和内容缺失。网络安全法益关乎国家安全、公共安全和公共秩序,网络安全法益的保护对象应当包括“网络的安全运行”“网络数据的完整性、保密性、可靠性”[12]。网络公共安全是公共安全应有之义,网络公共秩序是公共秩序的组成[14]。网络公共安全的内涵应包括网络空间的数据和以信息为内容的网络秩序的安宁性,以系统安全、数据与信息安全为对象的网络技术行为是重点规制的内容。张明楷教授认为网络虚拟财产、电脑空间的不可侵入性等新法益应当进入刑法视野。此外依传统法益在网络时代的新内容对传统法益进行调整:伪造、变造电子文书、电子署名的行为、妨害网络经营行为都是对网络化的传统法益的侵害[15]。

为应对以网络为“空间”与“本质”的犯罪,彰显网络安全法益的重要性和保护的必要性,刑法的

罪名体系应进行调整:对现有罪名进行扩大解释,对于危害网络安全的犯罪、人工智能犯罪等新型犯罪增加新罪名。(1)将伪造、变造电子文书、伪造电子署名、妨害网络经营等行为归入相应的罪名[15]。将以虚拟财产为对象的犯罪纳入侵犯财产犯罪。(2)增设危害网络安全罪,规制“实施破坏网络、网络空间安全的危害行为,利用网络空间实施危害行为,对网络空间实施危害行为的情形”[12]。(3)增设滥用人工智能罪,应对被控型人工智能犯罪。将滥用人工智能的行为纳入刑法规制的范围。(4)增设人工智能事故罪,应对自主型人工智能犯罪。在刑法中确立人工智能研制者和使用者的严格责任,完善人工智能产品研制和使用过程中的义务体系,明确研制者和使用者的数据保护义务[11]。

(三)人工智能犯罪的刑法应对

1. 人工智能的刑法定位——工具性和非主体性

鉴于人工智能技术风险的不确定性、复杂性和后果的灾难性,对人工智能技术进行规范和风险防控,使人工智能处在有效的政治管制下是必然趋势。预防原则应放在以法律手段应对人工智能风险的中心位置[10]。在法律意义上,明确人工智能在网络犯罪中的工具属性,否定其犯罪主体地位,是刑法预防人工智能犯罪的应然之举。

(1)人工智能的工具性[16]。在超人工智能出现之前,人工智能仍然属于“工具”的范畴。对人工智能的定义有诸如程序工程、行动理性、机器人、计算机技术等多种,“但无论如何定义,智能机器人都没有脱离工具化的主体范畴”[17]。人工智能的界定是“一种基于算法设计通过数据自主学习以优化数据处理的计算机制,本质在于算法和数据”[18]。“进入人工智能时代,自由与秩序关系有何调整?法律应作出何种回应?我们对上述问题的思考会限定在工具型人工智能时代”[5]。明确“人工智能的工具价值”是应对人工智能犯罪风险的首要原则。

(2)人工智能不具有刑法主体属性。人工智能是否具有法律主体地位是理论界热议的问题。支持论认为人工智能具有自主意识和行为能力,应具有法律主体地位。如 2016 年 11 月 25 日沙特政府赋予了机器人“索菲亚”公民权。然而,自主意识和自主行为并不能决定法律主体的产生。一个反例是具有生命、智商的动物并不具备法律主体资格,刑法中将实施危害行为的动物视作犯罪工具。在传统意义上,法律体系和刑法逻辑体系都是建立在以“人”为核心的概念基础之上,以“行为能力”作为归责的基础,从而划定刑法效力范围。而人工智能不具有生命这一特质,因此不属于人的概念范畴,无法系统适用法律逻辑体系。在“工具”逻辑语境下讨论人工智能并不具有刑法主体性质。人工智能不具备自然生命属性,其“意志”源于预设的程序和指令,犯罪认定的前提与依据不存在,刑罚处罚也无法落实。“在主体层面,如果要使人工智能成为独立的责任主体,需要人工智能的高度发展与完整责任主体的转型发展,在现阶段条件尚不够成熟”[19]。人工智能的“行为”是在人预设的模式和数理逻辑下进行的,人工智能并不能作为适格主体进入刑法视野[20]。

2. 人工智能犯罪的归责——风险刑法的责任体系

前述提到,根据人工智能的自主程度,可以将人工智能犯罪分为被控型人工智能犯罪和自控型人工智犯罪。在工具属性的命题下,刑法可构建不同的归责体系追究研制者、控制者的刑事责任。

(1)利用可控型人工智能犯罪的过错责任。研制者或控制者存在故意的过错,利用人工智能实施犯罪时,研制者或控制者在设计和编程范围内对人工智能实施的犯罪行为承担刑事责任。可控型人工智能无法决定行为目的、行为方式,辨认能力和控制能力亦受研发者的控制。即使人工智能

已经具备自主学习能力并独立进行运算、决策、行为,也是设计和程序的控制使然。“智能机器人在人类设计和编制的程序范围内的行为体现的是人类的意志”,智能机器人实施的犯罪行为,从本质上体现研发者、控制者的犯罪意志,智能机器人仅充当犯罪工具[4]。因此,对犯罪后果需要承担刑事责任的是该智能机器人的研制者或控制者。

(2)对自控型人工智犯罪的监督过失责任。研制者或控制者与人工智能产品之间的关系是监督与被监督的关系,研制者或控制者有预见其技术产品发生危害结果的可能性,则因其负有预见义务成立过失犯罪。根据《网络安全法》规定,承担网络安全义务的责任主体包括:网络服务和关键信息基础设施运营者及其直接负责的主管人员和其他直接责任人员、网络产品或者服务的提供者等。人工智能供应链条结构复杂,由核心厂商和主要供应链厂商承担责任和网络安全保障义务是便利监管的高效方式[9]。研制者或控制者在制造、使用人工智能的过程中因未尽到注意义务,导致危害结果发生的,成立过失责任。基于人工智能领域刑事风险产生途径的不确定性,一旦无法确认该研制者、控制者是否具有罪过时,应当由其承担刑事举证责任[21]。法律不强人所难,存在技术上无法避免人工智能安全风险可能性的情形,属于意外事件而无需担责。

监督过失责任是强化监督者义务的一种问责机制,在危险结果出现的前提下适用严格责任原则推定其担责,唯有举证证明监督义务主体已经履行义务时,得排除其刑事责任承担。广义的监督过失还包括管理过失,强调对于管理制度或危险物品疏忽的行为。监督过失责任采取法定主义,当前我国刑法对人工智能研制者、控制者无监督义务规定,由此,“人工智能产品的研发者和使用者在我国现行刑法语境下似乎不存在过失责任问题,但这可能是刑法在人工智能刑事风险防控方面存在的一种缺陷”[11]。

四、余论——网络刑法完善路径与法律技术运用

为回应网络时代立法需求,并实现刑法在网络空间的规制效力,学界对于网络刑法的完善进行了探讨。立法技术的选择是刑法完善路径设计的关键。无论是采用对刑法典进行扩大解释或立法修正的模式、颁布单行刑法或二者并举的模式,都是建立在规制网络犯罪的必要性需求与法律发展的可行性空间基础上的权衡与选择。

观点一:扩大解释为主要方式。中国刑法分则应对网络犯罪的调整方式不应当是立法,而应是对刑法条文进行解释。有学者认为解释的形式包括:司法解释、立法解释和单行刑法[14]。这种方式实质上仍然是立法和扩大解释并举的做法。有学者认为,针对新型法益的保护需要和新型网络犯罪规制,除增设、完善罪名体系,加强传统罪名的刑法解释也是延伸刑法适用空间的有效模式[13]。观点二:颁布单行刑法。扩张解释和刑法修正案的方式,存在滞后性和破坏法典统一的弊端,因此单行网络刑法更具合理性[22]。即通过对网络犯罪颁布单行刑法的方式,实现刑法典与单行网络刑法并存,建立以“单行刑法为主、刑法典为辅”的理想结构[22]。观点三:必要性与效率的均衡。张明楷教授认为法律解释方式是首选,但不是唯一路径。以遵守罪刑法定原则为前提,通过解释路径即可以应对新类型的网络犯罪时,无需采取立法路径。如解释违反罪刑法定原则,则有必要采取立法路径以规制网络犯罪;此外,没有必要在刑法典之外制定网络刑法[15]。

刑法网络空间效力的实现路径,是在立法前瞻性与刑法稳定性统一基础上的几种立法技术考量。网络犯罪立法的前瞻性应为下位立法和司法解释预留必要的空间,立法层面要注意刑法的稳

定性,司法解释层面要注重适用性,以应对规制网络犯罪发展新局面的需要。

参考文献:

[1]于志刚. 网络"空间化"的时代演变与刑法对策[J]. 法学评论,2015(2):113-121.

[2]于志刚. 网络、网络犯罪的演变与司法解释的关注方向[J]. 法律适用,2013(11):19-24

[3]刘宪权. 网络犯罪的刑法应对新理念[J]. 政治与法律,2016(9):2-12.

[4]刘宪权,胡荷佳. 论人工智能时代智能机器人的刑事责任能力[J]. 法学,2018(1):40-47.

[5]齐延平. 论人工智能时代法律场景的变迁[J]. 法律科学,2018(4):37-46.

[6]梁根林. 传统犯罪网络化:归责障碍、刑法应对与教义缩限[J]. 法学,2017(2):3-13.

[7]王燕玲. 中国网络犯罪立法检讨与发展前瞻[J]. 华南师范大学学报(社会科学版),2018(4):128-136.

[8]王肃之. 人工智能犯罪的理论与立法问题初探[J]. 大连理工大学学报(社会科学版),2018(4):53-63.

[9]吴沈括,罗瑾裕. 人工智能安全的法律治理:围绕系统安全的检视[J]. 新疆师范大学学报(哲学社会科学版),2018(4):109-117.

[10]马长山. 人工智能的社会风险及其法律规制[J]. 法律科学,2018(6):47-55.

[11]刘宪权. 人工智能时代的刑事风险与刑法应对[J]. 法商研究,2018(1):3-11.

[12]孙道萃. 网络刑法知识转型与立法回应[J]. 现代法学,2017(1):117-131.

[13]于冲. 网络犯罪罪名体系的立法完善与发展思路:从97年刑法到《刑法修正案(九)草案》[J]. 中国政法大学学报,2015(4):39-54,159.

[14]于志刚. 网络犯罪的发展轨迹与刑法分则的转型路径[J]. 法商研究,2014(4):44-53.

[15]张明楷. 网络时代的刑事立法[J]. 法律科学,2017(3):69-82.

[16]房慧颖. 人工智能犯罪刑事责任归属与认定的教义学展开[J]. 山东社会科学,2022(4):142-148.

[17]许中缘. 论智能机器人的工具性人格[J]. 法学评论,2018(5):153-164.

[18]李晟. 略论人工智能语境下的法律转型[J]. 法学评论,2018(1):98-107.

[19]陶盈. 机器学习的法律审视[J]. 法学杂志,2018(9):55-63.

[20]白海娟. 人工智能"犯罪"之否定[J]. 兰州学刊. 2020(8):80-89.

[21]李兴臣. 人工智能机器人刑事责任的追究与刑罚的执行[J]. 中共青岛市委党校青岛行政学院学报,2018(4):112-116.

[22]张阳. 空间失序与犯罪异化:论虚拟空间的犯罪应对[J]. 河南社会科学,2018(5):66-71.

Criminal law response to cybercrime and the regulation of artificial intelligence crime in the big data era

PANG Yunxia[1], ZHANG Youlin[1,2]

(*1. School of Law, Shanxi Datong University, Datong 037009, P. R. China*;

2. School of Philosophy and Government, Shaanxi Normal University, Xi'an 710119, P. R. China)

Abstract: The development of network technology has contributed to the intergenerational change of the network. In the Internet 3.0 stage with big data as the core, the role and status of the network in crime has changed, and the criminal law attribute of the network has evolved from the traditional object and tool of crime to the field space and way of existence of cybercrime. The manifestations of cybercrime have also evolved accordingly. While the trend of traditional crime being networked has been strengthened, new forms of crime such as artificial intelligence crime have emerged. On the basis of comparing the difference between the harmfulness evaluation of cybercrime and traditional crime, cybercrime can be divided into three types:

cybercrime types whose harmfulness evaluation is equivalent to traditional crime, cybercrime types whose online and offline harmfulness evaluation deviates, and a new type of cybercrime centered on network big data, the latter being especially represented by artificial intelligence crimes. The legal issues of artificial intelligence impact the human-centered legal system, and put forward new propositions for criminal law.

The development of big data, cloud computing and artificial intelligence technology means the arrival of a new era of risk. Thecriminal law has made effective legislative responses to crimes that use the internet as a tool or an object, but it is not effective in regulating cybercrimes in the era of big data, responding poorly to crimes that use the internet as a space, and has not yet responded to crimes that use the internet as the essence of existence. The criminal law lacks a risk mechanism for dealing with new types of cybercrimes. First, it is insufficient to deal with new cybersecurity risks with the content of big data system security, algorithm security, and data and information security. At the same time, in the process of legislation and regulation of cybercrime, the criminal law has paid necessary attention to the computer information system, but it is out of balance with the protection of legal interests of network security, especially that network public security and data information security have not been given necessary attention. The criminal law should make legislative adjustments, establish the concept of risk criminal law, and carry out criminal prevention of network security risks and technical risks in the era of big data. The legislative protection of legal interests in network public security should be clarified, and its connotation includes cyberspace data and information-based content. A network security legal interests protection system should be established, and new charges to regulate new types of cybercrimes should be added. The tool attribute and non-subjectivity of artificial intelligence in cybercrime should be clarified, and the fault liability for the use of controllable artificial intelligence for crime and the supervision fault liability of self-controlling artificial intelligence crimes should be established. By choosing appropriate paths and legislative techniques, the criminal law can respond to cybercrimes.

Key words: the effectiveness of criminal law in cyberspace; cybercrime; AI-crimes (artificial intelligence crimes); legislative response

(责任编辑 胡志平)