重庆大学学报(社会科学版) 2023年第29卷第2期
JOURNAL OF CHONGQING UNIVERSITY(Social Science Edition) Vol. 29 No. 2 2023

Doi:10.11835/j.issn.1008-5831.fx.2020.06.001

欢迎按以下格式引用:熊波.我国人工智能刑法的行政前置性立法探析[J].重庆大学学报(社会科学版),2023(2):232-245. Doi:10.11835/j.issn.1008-5831.fx.2020.06.001.

Citation Format: XIONG Bo. An analysis of the administrative pre-legislation of China's AI criminal law[J]. Journal of Chongqing University (Social Science Edition),2023(2):232-245. Doi:10.11835/ j.issn.1008-5831.fx.2020. 06.001.

我国人工智能刑法的行政前置性立法探析

熊 波

(华东政法大学 刑事法学院,上海 200042)

摘要:人工智能法学研究应当谨防"学术泡沫",人工智能刑事法治建设应当立足我国本土实践的真问题,重点关注真正能够对我国刑法产生挑战的人工智能危害行为。新型人工智能犯罪属于典型的行政犯,在人工智能技术发展的初期,人工智能刑法应当塑造行政前置性立法方法,具体包括"前置行政不法"和"前置行政程序"两类立法模式。其中,"行政性"是指人工智能行为等构成要件在静态规范层面中的不法行政评价和动态行政程序执行中的过程性、经历性行政评价,而"前置性"是指行政性评价前置于人工智能犯罪行为的刑事责任认定。相较于信息网络犯罪和计算机系统犯罪的立法而言,人工智能技术危害的实践特质在于人工智能的深度学习性和算法技术对人类活动时空的延伸性。因而,行政前置性立法特质要在人工智能刑法体系中得以体现,就需要立法者尤为注重全面性和双重性规则。行政前置性立法有助于保障刑事归责的专业性,重点聚焦人工智能的技术特质挑战,实现不同算法技术危害行为的等级评价。在具体设计行政前置性立法规则时,立法者需要将规则特质运用在人工智能技术的研发以及人工智能产品的测试、生产、销售和使用等阶段。具体而言,第一,对于行政不法前置性立法,刑法应当重点评价人工智能产品的销售和使用阶段,对销售不符合行政标准的人工智能产品行为设置抽象危险犯,并对人工智能产品使用阶段的制造安全事故、危险驾驶、非法侵入、破坏系统的危害行为,增设涵盖行政不法规范的新罪名或相关条款。第二,对于行政程序前置性立法,刑法应当重点评价人工智能技术的研发阶段,以及人工智能产品的测试、生产、销售和使用阶段。行政程序前置性立法发挥着行政行为公共服务监管的本质机能,行政许可、登记、责令等程序能够确保人工智能技术研发和产品测试、生产、销售和使用等各阶段,符合人类的道德伦理性和技术安全性。行政程序前置性立法要求刑法

基金项目:2022年国家社会科学基金青年项目"数据安全的刑法区分性保护研究"(22CFX015);司法部2021年度法治建设与法学理论研究科研项目"数据犯罪治理的'民行刑'衔接路径研究"(21SFB3009);互联网法治研究院(杭州)2021年度重点研究课题;上海市教育委员会和上海市教育发展基金会"晨光计划"资助项目;四川省犯罪防控研究中心项目"法秩序统一视阈下数据犯罪治理研究"(FZFKK22-10)

作者简介:熊波,华东政法大学刑事法学院副教授,Email:xiongbolawyer@163.com。

应当单独设置相关罪名，将行政许可、登记、责令等程序作为人工智能技术发展初期的刑法规制缓冲和风险预防手段。

关键词：人工智能；信息网络；行政不法；行政程序；行政犯

中图分类号：D924；TP18　　**文献标志码**：A　　**文章编号**：1008-5831(2023)02-0232-14

人工智能立法是我国新时代法治建设的重大现实课题[1]，法定犯时代，人工智能犯罪属于典型的行政犯。刑法作为后盾法，因此，相应地，这一影响应当具体体现在刑法和行政法的相互沟通、衔接的维度之上，而并非刑法闭塞体系内的立法方法探讨。当前，我国人工智能刑法立法研究因侧重于人工智能主体性地位研究，并未体现法学研究的务实性和现实性关切，而被诸多学者认为是在创造“学术泡沫”。国内外的理论与实践多数不承认人工智能的主体地位[2]，纵使是人工智能刑事主体地位得到部分学者的承认，国内外的顶层政策设计也明确表示反对[3]398-450。因此，人工智能刑事法治建设应当立足我国本土性的实践真问题，并非所有的问题均属于人工智能刑法面临的真正挑战。人工智能刑法立法应当做好与行政性法规范的衔接工作，这便要求塑造行政前置性立法的思维和规则。

一、人工智能刑法的行政前置性立法的理念塑造

当前，行政前置性立法规则探讨存在缺失，学界较为忽视人工智能刑法的行政前置性立法的概念、特质和价值等本体问题。

（一）何为行政前置性立法

行政前置性立法的概念问题，主要是从刑法规范层面进行研讨，因为“行政法与刑法衔接的问题主要体现在法律条文的规定上”[4]。由于人工智能技术属于互联网技术运用的高阶部分，在人工智能刑法立法并未形成的现实情况下，人工智能刑法立法的行政前置性方法的概念理解，可以结合现行刑法规制的信息网络犯罪和计算机信息系统犯罪进行。

以计算机信息系统犯罪为例，计算机信息系统作为人工智能基础设施的主要表现形式之一，亦是新型人工智能犯罪重点关注的领域。《中华人民共和国刑法》（以下简称《刑法》）第285至286条的非法侵入计算机信息系统罪，非法获取计算机信息系统数据，非法控制计算机信息系统罪，提供侵入、非法控制计算机信息系统程序、工具罪，破坏计算机信息系统罪等罪名，在罪状表达时采取了“违反国家规定”的立法技术。《刑法》第96条对“违反国家规定”的含义进行了解释：“本法所称违反国家规定，是指违反全国人民代表大会及其常务委员会制定的法律和决定，国务院制定的行政法规、规定的行政措施、发布的决定和命令。”而由于全国人大及其常委会制定的法律中明确包含了行政性规范要求的程序和义务，因此，计算机信息系统犯罪中的“违反国家规定”便属于一种行政不法前置性立法。诸如此类的还有刑法规范中的“违反国家规定”“违反国家有关规定”“违反……法规”“违反……管理规定”，其属于一种静态层面的行为评价，违反行政法律规范就构成了“行政不法”[5]。

但不同于行政不法前置性立法，刑法规范中还存在着部分行政程序前置性立法，其本身属于对行政程序的动态规范运行的认定和评价[6]。罪刑法定原则要求我们应当将刑法规范作为一切刑法活动的“帝王条款”。既然，刑法规范明文将行政程序作为罪名规范表述的一部分，这就表明刑法单

独对其进行强调,需要重点关注。而在运用“行政不法前置性”立法方法设置的空白罪状中,则不存在行政程序的约束,其只要行政规范的静态层面的符合即可,而并不需要行政机关开启行政程序进行先行判断。

以包含“行政程序前置性”立法的拒不履行信息网络安全管理义务罪为例,纵使是网络服务提供者在不履行法律、行政法规规定的信息网络安全管理义务的情况下,造成了违法信息大量传播、用户信息泄露、刑事案件证据灭失等严重情形,但只要网络服务提供者在相关行政监管部门责令采取改正措施时积极配合改正的,便不构成犯罪。其与前述“行政不法前置性”的立法方法不同的是,行政程序前置性立法为行为人设置了行政程序的积极配合义务,以行政程序的先行处理来实现犯罪圈的限缩目的。

值得强调的是,行政程序前置性立法中的“行政程序”并不包括行政诉讼程序。按照行政法学界的通说观点,“所谓行政程序,是指行政主体作出行政行为的过程中所遵循的步骤、顺序、方法、方式以及时限的总和”[7]315。由此可知,行政程序的“行政性”特点在于程序性事项作出的主体是“行政机关”,而依据《中华人民共和国行政诉讼法》第1条的立法目的,行政诉讼程序是一种司法程序,该种程序的主体性特点在于程序性事项作出的主体是“人民法院”。

综上所述,人工智能刑法立法的行政前置性是刑法应对人工智能时代技术发展所应当运用的主要立法方法。其中,“行政性”是指人工智能行为等构成要件在静态刑法规范层面中的不法行政评价和动态行政程序执行中的过程性、经历性行政评价,而“前置性”是指前者前置于人工智能犯罪行为的刑事责任评价。

(二)人工智能刑法行政前置性的立法特质

如前所述,除了人工智能领域外,前置性立法方法在计算机信息系统犯罪和信息网络犯罪领域中也有所体现。那么,人工智能刑法立法的行政前置性特质在哪?其能否被其他犯罪的行政前置不法规范所涵盖?

从《刑法》第285至286条的计算机信息系统犯罪的罪状设置来看,“违反国家规定”是对网络技术危害行为对封闭计算机信息系统空间的控制性、攻击性和破坏性的前置行政规范评价;而从《刑法》第253条之一、286条之一的信息网络犯罪的罪状设置来看,“行政性法律、法规规定的信息网络安全管理义务”“违反国家有关规定”是对信息网络技术危害行为本身的传播性、无物理边界性和传播瞬时性的前置行政规范评价[8]。虽然《刑法》第287条是利用网络技术实施的传统犯罪,但是其并非纯粹强调前两者网络技术性犯罪的特质,而是指向利用互联网实施的传统犯罪[9],在这种情况下,前置行政不法规范的涵盖范围就局限于上述信息网络犯罪的技术特殊性。

但是,就人工智能技术利用的特性来看,人工智能产业的高速发展并不仅仅局限于上述两类网络犯罪的特性。考察人工智能技术的危害特质,我们可以从“人工智能”的基本概念入手。国家标准化管理委员会和中国电子技术标准化研究院共同编制的《人工智能标准化白皮书(2018版)》对人工智能的概念进行了精准的界定:“人工智能是利用数字计算机控制模拟、延伸和扩张人的智能,感知环境、获取知识并使用知识获得最佳结果的理论、方法、技术及应用系统。”[10]5 因此,人工智能最大的特性便在于:人工智能技术延伸、扩展、模拟的对象是人类。虽然在刑法规定的计算机信息系统犯罪和信息网络犯罪中,同样存在这种情况。但是“网络犯罪是在网络空间实施的犯罪,这是网络犯罪的基本特征”[11]。这就表明人工智能与上述两类网络犯罪的最大差异在于算法技术延

伸、扩展、模拟的对象不仅是人类的思想，还有人类行为的时空上的移动，而这在纯粹的网络空间中是无法实现的。因此，人工智能产品才能具有感知环境、与人交互、与人互补、连续扩展的特性，这是人工智能深度学习的必然效应[12]。诸如，2018 年 3 月在美国发生的 Uber 无人驾驶测试车撞死行人事故以及 2015 年 7 月德国大众汽车厂发生机器人杀人案，均属于人工智能技术自由扩展人类思维和现实活动所导致的技术危害。

由此可见，人工智能技术危害的实践特质是在人工智能的深度学习性和对人类活动时空的延伸性的技术差异中衍生而来的。在上述特质下，人工智能产品可以无限扩展人类的思维和活动空间。基于此，计算机信息系统犯罪的“违反国家规定”和信息网络犯罪的“行政性法律、法规规定的信息网络安全管理义务”“违反国家有关规定”等前置行政规范评价并不能涵盖人工智能的技术危害。因而，计算机信息系统刑法和信息网络刑法的行政前置性立法方法并不能完全契合人工智能刑法的行政前置性立法。诸如，《人工智能标准化白皮书（2018 版）》中的人工智能标准的明细表，详细统计了我国已发布、在研以及拟研制的人工智能相关标准共计 200 项，其中已发布的就有 80 项，占据 40%[10]61-70。而这些便是出于人工智能技术危害的特质性而单独制定的一种行政标准规范。

因此，在前述所言的信息网络犯罪和计算机信息系统犯罪的行政前置性立法的现状下，人工智能刑法的行政前置性立法方法并非是毫无根据或者脱离刑法体系的立法方法。但信息网络犯罪和计算机信息系统犯罪的行政前置性立法，由于信息网络犯罪、计算机犯罪与人工智能犯罪存在技术特质的差异性，因而，人工智能刑法的行政前置性立法并不能直接照搬信息网络犯罪和计算机信息系统犯罪的立法模式。立法者应当将人工智能技术危害的实践特质明确表述在行政前置性立法方法当中，以突显人工智能刑法立法的独立性。这种独立性体现在两个方面。

其一，人工智能刑法的行政前置性立法注重全面性。“全面性”指人工智能刑法立法的全面化行政前置性立法。在信息网络和计算机刑法立法中，虽然行政前置性立法方法也为立法者运用，但是立法者考虑到当前我国网络技术和计算机技术的相对成熟性，司法者并不需要援引行政性法规范当中的术语定义、技术标准等，就可以直接依据危害结果进行入罪。因而，立法者并未全面地采取行政前置性立法方法，而仅是在前述部分罪名之中采取了行政前置性立法。

但是，正如前述，人工智能技术特质在于人工智能的深度学习性和对人类活动时空的延伸性，其是不断变化的。因而，司法者仅凭非人工智能技术专业性的刑法规范认定每个变化过程中人工智能技术危害，完全是“天方夜谭”。而行政程序和行政不法规范因不同的行政管理领域，就可以直接关涉到人工智能技术的专业性规范。此时，人工智能刑法行政前置性立法注重全面性，就可以使司法者在具体运用刑法过程中，避免人工智能技术壁垒导致刑法适用的罪刑失衡。但是，在信息网络和计算机信息系统的刑法立法中，行政前置性的全面立法完全没有必要，其反而会导致信息网络和计算机刑法立法的繁杂、冗余，不利于立法的简洁性。

其二，人工智能刑法行政前置性立法注重双重性。“双重性”指“行政不法+行政程序”的双重规则。在人工智能技术研发和产品运用的前期阶段，人工智能技术相对于信息网络或者计算机信息系统的技术研发和产品制造而言，不太成熟。并且，人工智能技术危害具有深度学习性和对人类活动时空的延伸性，因而，如果刑事立法者不借助行政程序防控不太成熟的人工智能技术前期阶段潜在的风险，一旦人工智能技术的抽象危险转为现实危害，那么其就具有全球性、不可估量性与蔓

延性。所以,在国内外人工智能技术相关的法律法规之中,行政程序对于确保人工智能技术的研发以及人工智能产品的测试、生产、销售和使用的安全性,发挥着举足轻重的作用[3]398-450。诸如,人工智能技术研发的行政许可或者审批程序、人工智能产品测试的行政监管程序。

立法者考虑到当前我国网络技术和计算机技术的相对成熟性,在现行刑法立法过程中,计算机刑法没有采用行政程序前置性立法,信息网络刑法中也仅有《刑法》第286条之一的拒不履行信息网络安全管理义务罪采取了行政程序前置性立法。并且该种行政程序并非是出于网络技术的特性考量,仅是为了行政机关责令网络平台及时履行管理义务而设置。因此,出于防范潜在且抽象的人工智能技术危害,人工智能刑法行政前置性立法在援引术语定义、技术标准等行政不法规范之外,还需要尤其注重行政程序性立法。相较于信息网络和计算机信息系统的现存的行政前置性立法,人工智能刑法行政前置性立法需要注重"行政不法+行政程序"的双重规则。

综上所述,人工智能技术危害的实践特质是在人工智能的深度学习性和算法对人类活动时空的延伸性的技术差异中衍生而来的。基于这一实践特质,行政前置性立法特质体现在,相较于信息网络和计算机刑法而言,人工智能刑法的行政前置性立法更需要注重全面性和双重性规则。

(三)人工智能刑法行政前置性的立法意义

毋庸置疑,人工智能刑法的行政前置性立法旨在强化刑法与行政法对人工智能法益侵害行为规制的互动衔接关系。那么人工智能刑法立法行政前置性规则的构建,是否有其必要?这需要细致剖析人工智能刑法行政前置性的立法意义。

1.行政前置性立法有助于发挥行政不法和程序的先行评价机制,防止单独的刑罚处罚阻碍人工智能的技术创新

刑法在人工智能技术产业推动社会转型的过程中,发挥的作用应始终保障并服务于人工智能技术竞争和社会发展。尤其是当前人工智能作为一种新型技术发展,在我国乃至国际上仍属于智能产业初期的发展阶段,塑造行政前置性立法规则,强调行政不法和程序的先行评价机制,有助于推动人工智能的技术创新。其一,行政前置的先行机制有助于契合刑法的第二次保障机制,防止刑法独立扩充人工智能犯罪的行为概念和类型。其二,行政前置的先行机制为不被允许的人工智能刑事风险的认定,提供了具体评价标准[13]。只有在行政前置的先行评价机制明确回应了技术发展的最合理的形式和类型之后,我们才能确定超过合理技术的具体样态和行政标准的人工智能危害行为是否属于值得刑法评价的犯罪行为。

2.行政前置性立法契合人工智能危害行为的抽象性和分散性,有利于保障人工智能刑事归责的专业性

人工智能作为互联网技术产业的新生事物,其危害行为由于存在场域的虚拟性,而具有不同于传统犯罪行为的不可直观性、纯粹技术性的抽象属性。在行政前置性法规范的立法规则下,刑事司法者不应当承担诸如"人工智能""信息网络"等纯粹的专业技术性概念解释的任务,而只需对"情节严重"等定罪量刑的具体标准进行界定。而由于前置不法规范的本质属性在于抽象行政行为,其代表的是行政性规范文件对不特定人或事项的约束力。再加上,行政法规范的目的在于实现广泛性、复杂性公共事务的管理[14]。因此,前置行政不法规范包括的行为概念和类型可以是具体的、多样的。如此一来,在人工智能刑法中加入行政前置性立法方法,刑事司法者无疑可以将定罪量刑以外的纯粹专业技术性概念的解释性工作,交于前置行政法规范予以解决,其仅专注于人工智能犯罪

中的专业化和精确化的定罪量刑工作即可。

3. 行政前置性立法能够防止人工智能刑法的重复性立法，有利于立法者重点聚焦人工智能的特质性对刑法立法的挑战

当下，人工智能刑法学研究乃至法学研究并未如同人工智能社会转型一样，实现质的突破，因而被部分学者认为人工智能法学研究只是在徒增“学术泡沫”[15]。人工智能法学研究中的“学术泡沫”除了过于关注人工智能的主体性地位之外，还存在将本不属于人工智能技术特质的行为类型作为立法建议的依据，导致人工智能刑法立法的效率低下、重复性现象大量出现[16]。而此类现象出现的根本原因在于：缺乏前置行政不法规范对人工智能刑法立法的约束性思维。但笔者认为上述观点评价的人工智能犯罪现象，如同《刑法》第 287 条一样，属于利用人工智能技术实施的传统犯罪，是一种传统犯罪网络异化的表现，并未突显人工智能刑法立法的行政前置性法规范所涵盖的行为特质，上述立法方案属于一种重复性、情绪性或者间断性立法的表现。因此，充分利用好行政前置性立法，梳理并排除人工智能与信息网络犯罪和计算机信息系统犯罪的同质性在立法中的影响，有利于立法者重点聚焦并回应人工智能的特质性对刑法立法的挑战，防止人工智能刑法的重复性立法。

4. 行政前置性立法相较于单一化的刑法立法方法，有利于实现人工智能技术的不同危害行为的等级评价

在人工智能技术的深度学习性和对人类活动时空的延伸性的特质下，人工智能犯罪所致的危害行为的程度应当是不同的。诸如，人工智能医疗器械在销售阶段的风险，一般存在三种类型：第一，人工智能医疗器械在销售时，被不法分子植入干扰算法系统深度学习的病毒。第二，被植入上述病毒的人工智能医疗器械，销售者未经过行政登记或者故障排除就直接售卖给医院。第三，被植入上述病毒的人工智能医疗器械，在未经销售者的行政登记或者故障排除后，被医院直接运用于手术治疗中，造成多人重伤、死亡。

上述情形中，如果是第一种或者第二种类型，在未发生任何医疗事故时，刑法考虑到不法分子属于初犯、偶犯，可以直接交由公安机关进行一般的行政处罚；销售者也可以仅予以一般的行政处罚。但是，在第一、第二种类型下，如果不法分子为惯犯，且植入病毒的危害性较大，同样销售者并非仅销售一台医疗器械；或者是在第三种类型下进行销售的。那么，可以肯定的是，单独的行政处罚并不足以发挥法律体系对严重危害行为的完全评价机能。此时，对于销售者而言，吊销营业执照的行政处罚和单位犯罪的刑罚处罚则可以并科。因为，在第一、第二种类型下，不法分子的植入行为和销售者的未经过行政登记或者故障排除的行为，仅处于人工智能医疗器械系统的静态的深度学习过程，而并不牵涉第三类行为的“医生治疗行为的时空延伸性”风险。

由此可见，人工智能风险是否需要单独由行政处罚进行规制，是由深度学习性和时空延伸性特质所致的不同危害行为所决定的。人工智能刑法在缺乏行政前置性立法时，单一化的刑法立法很有可能突破刑法的谦抑性原则，对人工智能的技术危害“大包大揽”。因而，行政前置性立法能够满足现实中不同程度的人工智能危害行为的分级评价需求。

二、立法规则Ⅰ：人工智能刑法的行政不法前置化

既然“行政前置性”对于人工智能刑法立法而言，发挥着举足轻重的作用。那么，如何具体设计

人工智能刑法立法的行政前置性规则,便是本部分需要重点解答的问题。其中,人工智能刑法的“行政不法前置化”立法是首要方法。

(一)前置行政不法对于人工智能犯罪行为基本类型的选择

行为是犯罪概念的基础事实或基本要素,不仅如此,其在阶层论和构成要件论的犯罪认定方法中,也是各要素评价的主要对象[17]。同样,这在行政法规范中亦是如此[7]336。因此,笔者拟首先从人工智能危害行为的行政前置化规则构建着手进行探讨。而人工智能危害行为的类型化可以依据人工智能的技术、产品的发展特点,划分为人工智能技术的研发阶段,人工智能产品的生产、销售、测试和使用阶段。

第一,人工智能犯罪属于典型的行政犯,在法定犯时代,自然犯中的利用人工智能手段杀人、放火、抢劫、盗窃、诈骗等行为类型,就不属于行政不法前置性立法规则所需要考虑的行为范围。因为,此类犯罪行为仅是犯罪手段或者工具的更新,其在行为要件的本质属性和法益类型评价上,与传统犯罪并不存在任何差异。

第二,纵使是在人工智能行政犯的类型中,也并非是所有的人工智能犯罪行为类型,均是行政不法前置性立法规则涵盖的范围。因为,在现行刑法的其他罪名涵盖的行为类型中,利用人工智能犯罪的行为并未突破原有罪名的构成要件涵摄的范围和保护法益的具体类型[18]。诸如,汽车制造商、车载操作软件提供商如果提供瑕疵的人工智能传感器,导致交通事故的,其本身就属于《刑法》第146条生产、销售不符合安全标准的产品的行为,刑法无需单独设置人工智能交通肇事罪。

第三,在排除上述两种情形后,能够对行政不法前置性立法规则产生影响的行为类型是较为有限的。按照行为类型的突破点不同,笔者将其分为两类:(1)对行为构成要件的本质属性的突破。具体类型有自动驾驶汽车的危险驾驶行为,非法侵入、破坏人工智能系统的行为。(2)对法益类型评价的突破。具体类型有造成人工智能产品安全事故的行为、不符合行政标准的人工智能产品的销售行为。第一种是对行为要件的本质属性的突破,表明刑法无需再脱离原有的行政不法前置性立法规则单独设置一个新罪名。其仅需要在相关罪名的构成要件中,添加相应的人工智能危害行为要件即可。第二种是对法益类型评价的突破,表明原有的前置行政不法规范本身保护的法益类型,已经无法评价人工智能危害行为所侵犯的法益,刑法需要单独设置一个新罪名,以体现刑法对新类型人工智能法益的单独保护。

综上,结合刑法立法原理,真正能够对刑法产生挑战的人工智能危害行为类型仅有四类:销售不符合行政标准的人工智能产品的行为,使用阶段造成人工智能产品安全事故的行为,自动驾驶汽车的危险驾驶行为,非法侵入、破坏人工智能系统的行为。

(二)人工智能刑法前置行政不法性规则的具体建构

在确立真正能够对刑法立法产生挑战的人工智能危害行为类型之后,我们就需要具体构建人工智能刑法的行政不法前置性立法规则。

1. 立法者需要对销售不符合行政标准的人工智能产品行为设置抽象危险犯

人工智能产品的技术危害与传统犯罪领域中的产品安全危害不同,虽然,本质上两者均涉及日常生活和工作用品,且服务于经济、校园、生活等各行各业;但是,人工智能的深度学习性和对人类活动时空的延伸性,决定了智慧经济、智慧校园、智慧生活、智慧医疗等人工智能产品的运用,能够较传统产品的领域更为迅速、更为普惠。而且,人工智能产品并不需要人类的持续性操控和随时性

监管,其自身能够通过外在环境的数据传输和感应,实现人类时空脱离的自主操作。因此,在人工智能产品及其相关测试平台的销售和使用阶段,基础设施系统的安全性、算法数据的正义性和全面性就显得格外重要。

但是,现行刑法在规制产品销售导致的严重法益侵害时,是基于传统产品、商品能够在人类的持续性操控和随时性监管下的使用情况而设置的,其对法益的状态评价更侧重于销售阶段产品的现实危害和销售金额。人工智能产品不同于人类操控指令支配下的技术服务和输出的传统产品,销售不符合行政标准的传统产品并不存在严重危及公共安全的潜在隐患,单个瑕疵传统产品的法益侵害仅具有个体性、固定性,且法益侵害风险较易被发现和排除。但人工智能产品使用的危害特性恰好完全与之相反。

基于此,人工智能产品并不能简单依附于《刑法》第 140、145、146 条的行政前置不法规范的评价,前文所述的《人工智能标准化白皮书(2018 版)》中的 200 项不同的人工智能相关标准,就已经表明了两者不可等同视之。在后续的人工智能刑法立法中,立法者应当明确依据人工智能相关产品(包括测试平台)的国家标准和行业标准,对搁置许久的人工智能相关产品,在最后出售前未经内部环节的评测、检验,就随意出售给使用者的行为,设置抽象危险犯。

2. 立法者需要对人工智能产品使用阶段的制造安全事故、危险驾驶、非法侵入、破坏系统等三类危害行为增设涵盖行政不法规范的新罪名或条款

人工智能行业发展的主要动力来源于“深度学习算法”“海量计算资源”“大数据资源”。“深度学习算法”是对系统功能本身的要求,“海量计算资源”“大数据资源”是对外在数据的质量和数量的要求[19]。可见,在人工智能产品的使用阶段,可以预想的是,行政先行评价机制中,产品的使用者除了要履行确保人工智能基础设施平台安全的行政义务之外,还需要履行排除输入的数据的数量和质量安全隐患的行政义务。

其一,刑法立法通过“人工智能产品使用安全的行政性法规范”评价人工智能产品安全事故的行为。人工智能产品在使用过程中,通常是用于公共服务行业。诸如,公共服务机器人、酒店服务机器人、银行服务机器人、场馆服务机器人、餐饮服务机器人在公共场所的使用。人工智能机器人作为自动化技术的重大成就,机器人和人类社会的生产、生活密不可分。有数据统计显示:2016 年全球机器人数量接近 30 万,2019 年增至 41.4 万。当前全球机器人数量年均增长率约为 15%,中国是推动机器人市场繁荣发展的最大“发动机”[20]。智能机器人完全展现了人工智能的特质性,其既可以按照人类预先编程好的算法结构运行,又可根据深度学习系统感知环境变化进行自主操作。而由于商业机密的保护需要,人工智能算法系统的数据输入到模型输出的学习过程均存在着不透明性[21]。因此,在这一“算法黑箱”下,一旦行为人不熟悉算法运行结构,疏忽大意或者过于自信地违反了人工智能基础设施平台安全和输入的数据的数量和质量安全的国家有关规定,导致了重大伤亡事故或者其他严重后果的情形,刑法应当设置人工智能活动事故罪对其予以评价。而在现行刑法规定的事故类犯罪的罪名之中,《刑法》第 134 至 139 条之一均是属于对特定生产、工作行业事故的规制,因而,上述罪名规定的前置行政不法规范均无法独立涵盖“违反人工智能产品使用安全的法律、法规”的行为。因此,立法者有必要比照事故类犯罪的立法模式,单独设置“人工智能安全事故罪”。

其二,刑法立法通过“自动驾驶的相关国家规定”防范自动驾驶汽车的危险驾驶行为风险。自

动驾驶汽车可以说是人工智能产品使用阶段中最受欢迎的智能工具,2018年4月3日,工业和信息化部、公安部、交通运输部联合印发了《智能网联汽车道路测试管理规范(试行)》,其中,第9条规定了测试主体需要确保智能网联机动车的安全技术和自动驾驶等功能检验合格的行政义务要求。除此之外,根据美国高速公路安全管理局推出的《自动驾驶汽车的分级标准》(NHTSA),该标准按照智能化、自动化的程度将智能网联汽车分为4个等级,其中L1-L3属于驾驶支援和部分、有条件的自动化驾驶[3]78-79。这就表明,在不同程度和等级的自动化技术情况下,危险驾驶的认定方式也有所不同。我国《刑法》第133条之一危险驾驶罪的规定,采取的是四类封闭式的行为方式列举:"追逐竞驶、醉酒驾驶、超载超速行驶以及运输危险化学品驾驶",但其均无法包括人类驾驶员或者测试主体未确保智能传感、摄像、雷达感知等设备的安全性能或者未履行半自动化驾驶的监控职责等危险驾驶行为。按照《中华人民共和国网络安全法》(以下简称《网络安全法》)第31条的规定,交通属于国家在网络安全等级保护制度的基础上,重要保护的网络基础设施安全的行业和领域,保护的具体范围和具体办法由国务院制定。因此,《刑法》第133条之一的危险驾驶罪有必要将智能网联汽车的危险驾驶行为纳入该条之中,增设第5项"(五)违反自动驾驶的国家规定,危及公共安全的"智能网联汽车危险驾驶罪。

其三,刑法立法通过"人工智能系统管理安全的行政性法规范"规制侵入、破坏或干扰行为。在人工智能算法编程的不透明性、不公开性的情况下,除编制基础设施及其运行数据的研发者以及输入的功能算法数据的使用者,能够熟知相应阶段的算法数据外,不熟悉算法运行结构的行为人,侵入甚至破坏人工智能算法系统,或者破坏人工智能基础设施系统存储、处理、传输的算法数据的,将极易诱发智能数据运行乱码的潜在危险。以阿里云ET城市大脑为例,"2017年底,ET城市大脑被列为首批四大新一代国家人工智能开放创新平台之一,被认为是人工智能的'登月计划',将成为接下来10年机器智能最重要的研究平台"[22]。阿里云基础设施平台通过汇集企业数据、公安数据、政府数据、运营商等多方的城市数据,借助ET大脑的深度算法学习,全局、实时地发现城市的问题并给出相应的优化处理方案,同时联动城市内各项资源调度,以整体提升城市运行效率。由于ET城市大脑服务着多个城市群,并能及时提供问题的优化方案,一旦行为人侵入甚至干扰、破坏此类企业的人工智能系统及其运行的数据的,将极有可能致使城市之间的资源调动和问题化解系统出现崩溃。虽然,按照《刑法》第285条、第286条的非法侵入计算机信息系统罪和破坏计算机信息系统罪的相关规定,对于干扰国家事务、国防建设、尖端科学技术领域的人工智能系统,以及人工智能系统功能数据本身的行为,刑法的相关规定足以应对上述危害,但是却存在如下问题:第一,虽然人工智能系统过于专业化和技术化,但是其仍需要专业的人工智能技术和产品的研发公司予以维护和操作。而此类人工智能系统也如同《刑法》第285条特定的计算机信息系统一样,承担着辅助公共服务的决策功能。上述的阿里云ET城市大脑和部分城市采用的企业安防系统便属于此类情况。而囿于第285条对计算机信息系统的封闭式列举,导致该条的"违反国家规定"的前置行政不法规范,无法将侵入阿里云ET大脑等人工智能系统的危害行为纳入该条立法之中。第二,在算法数据本身不存在任何质量和数量瑕疵的情况下,行为人也有可能干扰人工智能系统中存储、运行、处理的数据,致使系统产生运行偏差,而该偏差并非属于人工智能系统无法正常运行的情形。此时,《刑法》第286条第1、2款的"违反国家规定"的行为类型就无法将其予以涵盖。依据《网络安全法》第33条的规定,对于人工智能系统的基础设施建设,相关主体应当确保其具有支持业务稳定、持续运

行的性能。这就表明一般行为人还应当承担不干扰智能系统的业务稳定性能的行政义务,而并不应当仅局限于人工智能系统的正常运行。

基于此,笔者认为,刑法立法应当将《刑法》第285条中的“违反国家规定”的涵盖范围扩充至人工智能系统;在《刑法》第286条第1、2款的“违反国家规定”的涵盖范围中,加入干扰人工智能系统功能的数据,致使系统偏离指令运行,以及干扰存储、处理或者传输的算法数据,致使人工智能无法正常运行或者偏离指令运行等行为。

综上所述,行政不法前置性立法具体体现在人工智能产品的销售和使用阶段。具体而言:(1)立法者需要对销售不符合行政标准的人工智能产品行为设置抽象危险犯;(2)立法者需要对人工智能产品使用阶段的制造安全事故、危险驾驶、非法侵入、破坏系统的危害行为增设涵盖行政不法规范的新罪名或相关条款。

三、立法规则Ⅱ:人工智能刑法的行政程序前置化

根据现行刑法中已有的前置行政程序规范,人工智能刑事风险规制的前置行政程序的具体表现形式包括行政责令、下达改正通知、行政机构提出相关要求、行政处罚、行政许可等程序类型。根据人工智能犯罪行为在不同阶段的法益侵害特性,行政程序前置性立法方法具体体现的阶段有人工智能技术的研发阶段,人工智能产品的测试、生产、销售和使用阶段。

1. 立法者需要设置行政许可等程序来确保人工智能技术的研发以及人工智能产品的测试阶段的安全性或符合人类的道德伦理性

基于人工智能技术创新的要求,行政程序前置化方法主要是考虑人工智能刑法义务承担的缓冲性,其能够体现人工智能网络技术行政监管失灵后的刑法最后手段原则。最后手段原则表明,人工智能的技术创新需要在行政程序的监管下进行。换言之,人工智能技术的研发必须以制造、生产符合人类的道德伦理和技术安全的产品为最终目标,而人工智能的产品测试能够检测出人工智能技术的研发是否符合上述目标。为了体现行政程序在人工智能技术研发和人工智能的产品测试阶段的监管作用,确保人工智能创新能够按照国家政策方针和产业战略、规划的既定目标进行,我们有必要将行政程序融入技术研发和产品测试的阶段之中。

在行政法学界,行政程序本质上是一种具体行政行为。行政行为具有公务性,是出于全体国民的公共利益而进行的行为[23]。基于技术创新的最终目标要求和刑法介入的最后性原则,无论如何,我们可达成的共识是,在人工智能技术研发、产品测试环节之前,相关行政部门必须先对深度学习的人工智能系统提出相应的限制要求[24],以使其符合人类的基本伦理或道德。

其一,通过行政许可、登记程序来确保人工智能技术研发阶段符合人类的道德伦理性和技术安全性。首先,通过行政许可程序确保技术研发的伦理性和安全性。行政机关需要先对人工智能技术研发的主要方向和使用目的进行审查,以确保人工智能技术合规。如果人工智能技术并未通过行政机关委托的独立第三方专业机构的技术评估,那么据此研发出来的人工智能技术的可靠性便无从确保。而通过行政许可、登记程序,可以确保后续制造、生产阶段依据的人工智能产品的技术来源,以明确人工智能产品使用阶段法益侵害结果的责任承担。其次,行政监管部门通过人工智能研发技术的分类管理,便于为后续开展不同程度的刑事归责提供相应依据。由于人工智能产业涉及面广、自动化技术运用的程序不一,而自动化程度和涉及的产业面与人工智能技术的法益侵害性

程度形成正比。因此,《网络安全法》第21、31条以及工业和信息化部等10部门在2019年7月26日联合发布的《加强工业互联网安全工作的指导意见》均提出:要对互联网技术实施分类施策,分级管理,根据行业重要性、企业规模、安全风险程度等因素予以不同程度的规范保障。当前,人工智能技术研发阶段的刑法规制仍呈现空白,而未经行政审批、许可或者技术登记,就直接进行技术研发而违背人类伦理等类似缺陷,在"基因编辑婴儿"事件中就已经表现得淋漓尽致。可预料到的是,人工智能研发技术的滥用危害在智能时代将会更加突出。因此,笔者认为刑法有必要对未经行政审批、许可而开展人工智能技术的研发行为进行规制。

其二,通过行政责令、登记程序来确保人工智能产品的测试阶段的技术安全。当前,人工智能技术的产业发展还处于萌芽期,在未来一段时间内,人工智能产品的测试将愈发普遍。为了体现人工智能产品测试的环境真实性和相关产品基础设施面临突发危险的灵敏度,测试场域一般是在现实生活当中,而并非虚拟的空间环境。但是,现实场域中人工智能产品测试并不同于普遍推广或者日常生活使用的人工智能产品的成熟性能,在现实场域的测试环境中,算法的深度学习随时可能面临不可预料的突发情况。而行政监管部门对人工智能产品测试环节提出的具体要求,可以降低此类风险。以智能网联汽车的测试为例,上海市、北京市、重庆市、深圳等地的《智能网联汽车道路测试管理办法(试行)》均要求测试主体应当在公安交通管理部门指定的区域、时段进行测试。因此,对于相关测试主体不提交测试的范围和路线直接测试,脱离行政部门监管的,或者虽然提交了测试的范围和路线,并经行政主管部门许可,但违反行政许可、登记所指定的测试区域和时段要求,造成严重法益侵害后果的行为,刑法应当单独进行规制。

2. 立法者需要设置行政许可等程序来确保人工智能产品的生产、销售和使用阶段的安全性,以防范人工智能刑事风险

通过了行政管理部门对人工智能研发技术和测试产品安全性检验的,并不意味着人工智能产品的生产、交易流通环节就可以脱离行政部门的监管。人工智能产品的深度学习性不同于传统互联网产品单纯的指令操控性,人工智能技术的研发、人工智能产品的测试阶段的行政监管程序,只是对人工智能基础设施平台和算法系统功能的安全性监督,并不代表人工智能产品的生产、销售、使用阶段的数据模块的改造和人类输入指令数据质量的安全性。人工智能系统一旦独立运作,其自身便会依据产品所处的客观环境对算法数据进行编制。因此,每个环节的注册登记,可以确保行政监管部门能够通过联网系统随时知悉人工智能产品的生产、销售和使用阶段的基础数据的算法运作状态[25]。

在生产、销售和使用阶段,如果生产者、销售者、使用者,在生产、销售、购买人工智能机器人之后、交易使用之前,未及时登记造册,网上填写企业和个人电话、身份证号、住址等相关信息,导致网络监管部门在人工智能系统瘫痪时,无法及时联系相关责任主体,无法责令具体个人和企业消除隐患而造成严重后果的行为,刑法应当发挥后盾法的作用。

此外,由于人工智能系统运作的技术专业性和抽象性,刑法规范中的行政责令还可以使一般使用者和销售者更好地排除人工智能系统的算法偏失。以"微软的人工智能聊天机器人Tay事件"为例,假设机器人Tay与有偏激言论的人互动后,被引导出仇视女性和种族歧视之类的偏激算法数据之时,相关行政监管部门通过智能联网系统及时发现,并发出责令微软企业关闭使用账号并下架机器人的程序,便可防止事态的进一步恶化。

“系统地看,人工智能犯罪产生侵害结果是一个行为流程链条”[26],人工智能产品的销售阶段是人工智能产品流向各行各业的最后环节。因此,在人工智能产业发展初期,人工智能产品的销售行为应当实施行政许可。违反人工智能产品管理法律、法规的非法销售的行为,应当属于非法经营的行为。而按照《刑法》第225条非法经营罪的规定,人工智能产品不同于盐业、烟草业等行业的特许产品;也不同于需要进出口的产品;更不同于需要国家有关主管部门批准的非法经营的证券、期货、保险、资金支付结算业务。但为防止人工智能产品随意销售的普遍而导致产品质量低劣、脱离行政部门监管的现象发生,笔者认为,《刑法》第225条应当单独增设第4项“(四)未经许可经营的人工智能相关产品的”条款,以规制不经行政许可,扰乱市场秩序,随意销售人工智能产品的行为。

综上所述,人工智能刑法的行政程序前置性立法具体体现在人工智能技术的研发阶段,人工智能产品的测试、生产、销售和使用阶段。行政程序前置性立法发挥着行政行为公共服务监管的本质机能,行政许可、登记、责令等程序能够确保人工智能技术研发和产品测试、生产、销售和使用等各阶段,符合人类的道德伦理性和技术安全性。行政程序前置性立法要求刑法应当单独设置相关罪名,将行政许可、登记、责令等程序作为人工智能技术发展初期的刑法规制缓冲手段和风险预防手段。

结合人工智能刑法的“前置行政不法+前置行政程序”这两类立法规则,我们发现,在立法者具体设计人工智能刑法的行政前置性立法规则时,前置行政不法和前置行政程序的刑法立法始终贯穿人工智能技术的研发阶段,以及人工智能产品的测试、生产、销售和使用的各个阶段。这也契合前文所述的全面性和双重性的立法规则特性。其中,将人工智能技术危害的实践特性明确涵盖于“违反相关人工智能的法律、法规”之中,是行政不法前置性立法的典型表现;运用行政许可、登记、责令等程序,实现潜在性和不特定性人工智能技术危害的风险预防和缓冲,是行政程序前置性立法的典型表现。

四、结语

人工智能刑事法治建设应当立足我国本土实践的真问题。人工智能犯罪作为典型的行政犯,人工智能刑法立法规则的探究,应当体现法学研究的务实性和现实性关切,契合法定犯时代人工智能刑法的行政前置性立法特质。在“定性+定量”的刑法规范设置和分散性、多样性的行政法规范下,我国人工智能刑法的行政前置性立法具有鲜明的中国特色。因此,在我国人工智能技术产业发展的初期,行政前置性立法势必有利于我国人工智能刑法引领世界潮流,助力人工智能技术的国际竞争。人工智能刑法立法在法定犯时代永远与行政法保持着密切的沟通和衔接关系,结合现行刑法的立法现状,行政前置性立法包括“前置行政不法+前置行政程序”立法规则。而在人工智能的深度学习性和对人类活动时空的延伸性这一实践特质的引导下,行政前置性方法便独立于传统犯罪、计算机信息系统犯罪和信息网络犯罪领域。在具体设计人工智能刑法行政前置性立法规则时,立法者应当在人工智能技术的研发阶段,以及人工智能产品的测试、生产、销售和使用阶段注重全面性和双重性的规则特性。

参考文献:

[1]杨维汉.全国人大常委会委员长会议组成人员进行专题学习 栗战书主持并讲话[N].人民日报,2018-11-25(01).

[2]刘洪华. 论人工智能的法律地位[J]. 政治与法律,2019(1):11-21.
[3]腾讯研究院,中国通信院互联网法律研究中心. 人工智能:国家人工智能战略行动抓手[M]. 北京:中国人民大学出版社,2017.
[4]程凡卿. 行政刑法立法研究[M]. 北京:法律出版社,2014:3.
[5]熊波. 行政犯的类型与违法性判断的区分[J]. 政治与法律,2020(5):40-55.
[6]熊波. 网络服务提供者刑事责任"行政程序前置化"的消极性及其克服[J]. 政治与法律,2019(5):50-65.
[7]罗豪才,湛中乐. 行政法学[M]. 北京:北京大学出版社,2016.
[8]全国人大常委会法制工作委员会. 中华人民共和国刑法释义[M]. 北京:法律出版社,2015:495-496.
[9]于志刚. 虚拟空间中的刑法理论[M]. 北京:社会科学文献出版社,2018:20.
[10]中国电子技术标准化研究院. 人工智能标准化白皮书(2018 版)[EB/OL]. (2018-01-24)[2019-09-03]. http://www. cesi. ac. cn/images/editor/20180124/20180124135528742. pdf.
[11]陈兴良. 网络犯罪立法问题思考[J]. 公安学刊(浙江警察学院学报),2016(6):8-12.
[12]大数据战略重点实验室. 块数据:4. 0——人工智能时代的激活数据学[M]. 北京:中信出版社,2018:244.
[13]熊波. 人工智能刑事风险的样态评价与规制理念[J]. 探索与争鸣,2019(5):134-142,176.
[14]章剑生. 现代行政法总论[M]. 北京:法律出版社,2019:22.
[15]刘艳红. 人工智能法学研究的反智化批判[J]. 东方法学,2019(5):119-126.
[16]熊波. 论人工智能刑事风险的体系定位与立法属性[J]. 重庆大学学报(社会科学版),2020(3):142-154.
[17]余振华. 刑法总论[M]. 台湾:三民书局,2017:120.
[18]张明楷. 网络时代的刑事立法[J]. 法律科学,2017(3):69-82.
[19]谷建阳. AI 人工智能:发展简史+技术案例+商业应用[M]. 北京:清华大学出版社,2018:52-53.
[20]周亮. 全球机器人数量到底有多少[EB/OL]. (2018-07-06)[2019-09-03]. http://www. elecfans. com/jiqiren/614969. html.
[21]陶盈. 机器学习的法律审视[J]. 法学杂志,2018(9):55-63.
[22]阿里云研究中心. 阿里 ET 城市大脑白皮书[EB/OL]. (2018-07-05)[2019-09-08]. http://www. qianjia. com/html/2018-07/05_297143. html.
[23]姜明安. 行政法[M]. 北京:北京大学出版社,2017:236.
[24]埃里克·希尔根多夫,黄笑岩. 自动系统、人工智能和机器人:一个刑法角度的定位[J]. 法治现代化研究,2019(1):85-94.
[25]熊波. 数据状态安全法益的证立与刑法调适[J]. 当代法学,2023(1):70-82.
[26]郭旨龙. 中国刑法何以预防人工智能犯罪[J]. 当代法学,2020(2):44-55.

An analysis of the administrative pre-legislation of China's AI criminal law

XIONG Bo

(*School of Criminal Law, East China University of Political Science and Law, Shanghai 200042, P. R. China*)

Abstract: Artificial intelligence law research should guard against the "academic foam", and the construction of artificial intelligence criminal rule of law should be based on the real problems of China's local practice, focusing on the harmful behaviors of artificial intelligence that can really challenge China's criminal law. The new AI crime belongs to typical administrative crime. In the early stage of the development of AI

technology, the AI criminal law should shape the administrative pre-legislative method, specifically including two legislative models: "pre-administrative illegality" and "pre-administrative procedure". Among them, "administrative" refers to the illegal administrative evaluation in the static normative level and the procedural and experiential administrative evaluation in the implementation of dynamic administrative procedures of the constituent elements such as AI behavior, while "prepositive" refers to administrative evaluation precedes criminal responsibility determination of the AI criminal behavior. Compared with the legislation of information network crime and computer system crime, the practical characteristics of the harm of AI technology lie in the deep learning of AI and the extension of algorithm technology to human activities in time and space. Therefore, in order to embody the characteristics of administrative pre-legislation in AI criminal law system, legislators need to pay special attention to comprehensive and dual rules. Administrative pre-legislation helps to ensure the professionalism of criminal liability, focusing on the technical characteristics of AI challenges, and achieving the level evaluation of different algorithmic technology hazards. When designing specific administrative pre-legislation rules, legislators need to apply the characteristics of the rules to the development of AI technology and the testing, production, sales and use of AI products. To be specific, first, for the legislation of administrative illegality, criminal law should focus on the evaluation of the sales and use stages of AI products, set up abstract dangerous crimes for the sales of AI products that do not meet administrative standards, and add new charges or relevant provisions covering administrative illegality norms for the dangerous acts of manufacturing safety accidents, dangerous driving, illegal invasion, and system destruction during the use stage of AI products. Second, for the legislation of administrative procedure, criminal law should focus on the evaluation of the research and development stage of AI technology, as well as the testing, production, sales and use stage of AI products. The pre-legislation of administrative procedures plays an essential role in the supervision of public services of administrative acts. Administrative licensing, registration, ordering and other procedures can ensure the development of AI technology and the testing, production, sales and use of products, in line with human ethics and technical safety. The pre-legislation of administrative procedures requires that criminal law should set up relevant charges separately, and take administrative licensing, registration, order and other procedures as the criminal law regulation buffer and risk prevention means in the early stage of the development of AI technology.

Key words: artificial intelligence; information network; administrative illegality; administrative procedure; administrative criminal

(责任编辑　胡志平)