·法学研究·

DOI:10.20004/j.cnki.ujn.2024.03.013

数据累积犯的刑法规制

张　勇,王　杰

(华东政法大学 刑事法学院,上海 200042)

[摘　要]累积犯是指单个行为不会侵害法益,但如果类似行为的大量实施就会对某种法益造成实际或现实威胁的犯罪行为。累积犯具有实质的法益侵害性和真实的累积效应,对传统的结果本位归责模式提出挑战。在数字经济时代,应当将数据、信息、计算机信息系统与其主体关系的稳定性作为数据安全法益。数据累积危险行为应当体现真实的累积效应。典型的数据累积犯有数据收集型、拒绝服务型以及数据分析型三种类型。数据累积犯的因果关系判断须立足于事实判断、重视规范评价,同时须防止规范评价侵袭事实判断。对于没有体现真实累积效应的行为,不应将其纳入数据累积犯的因果关系判断范围;对于可能导致数据累积犯扩大适用的情形,也应当排除其因果关系的存在。

[关键词]累积犯;数据安全;数据累积犯;累积危险行为;因果关系

[中图分类号]D924　　[文献标识码]A　　[文章编号]1671-3842(2024)03-0137-13

在当下社会生活中,与人有关的行为与状态信息时刻以数据形式被记录着①。随着我国数字经济的快速发展,数据安全风险问题越来越引起重视,也给刑事立法以及司法实践带来重大挑战。在海量数据的收集和利用过程中,普遍存在微量不法行为积量成罪的问题,由个别行为累积而成的危害结果无法直接归属到任何一个主体,从而产生数据犯罪的认定难题。如果刑法无法寻找到合适的介入路径,不能及时回应已经产生的危害结果,就不能有效发挥其惩治和预防数据犯罪的功能。无独有偶,在环境犯罪领域,为了解决微量不法行为的刑法规制问题,累积犯理论应运而生。该理论主张,针对犯罪行为的特殊性和危害结果的不可逆性,有必要将累积危险行为纳入刑法规制范围,从而有效解决该类犯罪认定难的问题。本文拟运用累积犯理论,对数据累积危险行为的内涵、归责根据和犯罪类型等问题进行探讨,在此基础上研究解决数据累积犯因果关系认定的疑难问题。

一、累积犯的内涵及归责根据

(一)累积犯的概念及其争议

累积犯这一概念来自环境刑法领域,是一个充满争议的"舶来品"。在国外,德国学者库伦最早提出累积犯概念。他认为,累积犯是指单个行为因为事实上的原因不会损害法益,但如果类似行为大量实施就会导致某种法益遭受侵害,因而有必要禁止的犯罪类型。德国刑法学者黑芬戴尔发展与完善了累积犯理论,认为要以某种环境破坏行为是否可能与他人同样的行为累积出破坏生态环

[基金项目]国家社会科学基金一般项目"数据安全刑事治理现代化转型机制研究"(项目编号:23BFX116)。

[作者简介]张勇,华东政法大学刑事法学院教授、博士生导师,邮箱:2094@ecupl.edu.cn;王杰,华东政法大学刑事法学院博士研究生。

①李林:《智能算法伦理审查进路的完善策略》,《学术交流》,2023年第4期。

境的结果为原则,推定将具有可罚性的、威胁环境法益的抽象危险行为作为入罪行为[①]。黑芬戴尔还将阈值概念引入累积犯,使之成为描述行为累积程度及其危害的重要参数。单一污染的规模通常小到可以忽视,若同类行为被大量实施,超出某种程度后就会爆发灾情,这里的"某种程度"就是累积犯的阈值。由于环境具有自净能力,并不是所有破坏生态要素的行为都破坏了环境系统的多样性、生态平衡和稳定发展。没有阈值概念,累积犯罪与非罪的界限无法区分。

危险犯的传统理论分类包括具体危险犯和抽象危险犯,在抽象危险犯中还可以区分出因未发生危险而需否定犯罪成立的准抽象危险犯[②]。累积犯概念的提出突破了危险犯上述分类的穷尽性,动摇了危险犯传统分类标准的周延性,并产生了以下值得探究的问题:其一,法益侵害理论是否会随着累积犯理论的提出而遭遇挑战甚至崩溃?抽象危险犯已经遭受法益侵害判断标准精神化的批评,而在累积犯中行为与法益侵害的联系更加松弛,如果将形式上不具有刑事违法性的行为认定为犯罪,似乎不符合"犯罪本质是法益侵害"的判断。其二,累积犯理论是否与责任主义相悖?责任(Schuld)是指在确定符合构成要件行为的违法性之后,对行为人进行刑罚非难的要件。基于责任主义立场,行为人无需对他人的犯罪行为负责。累积犯的法益侵害并不来自行为人的单一行为,而是来自他人众多(且是假设和不确定)行为的共同作用[③]。一旦不法行为发生重叠,就无法判断个别行为与环境污染结果的因果关系,从而动摇"刑事责任是以个人行为为基础"的认识根基。

(二)累积犯的归责根据

从理论上看,累积犯概念的提出并不与法益侵害、责任主义原理相悖,累积犯具有实质的法益侵害性。真实的累积效应是累积犯的归责基础,是对传统结果本位归责模式的重塑。

1. 累积犯具有实质的法益侵害性

环境犯罪具有污染的累积性、以组织性分工为主的经济犯罪属性,以及在环境利用上强烈的利己思维三个特征[④]。由于行为的危害性存在积聚的可能,行为的危害性不会因微量化而消失。集体法益的结果犯保护模式具有滞后性,无法满足生态系统维持长期健康、稳定的需求,也无法解决污染环境案件的证据固定难题。生态系统通过种群的自然调节、物质的循环再生、生物与环境的交叉作用塑造自己的结构、维持能量流动和物质循环[⑤],轻微污染损害会被环境自我修复。现代社会中的危险累积、重叠、连锁,在生态法益愈发独立、预防性刑法愈发得到重视的背景下,生态法益容易被认定为秩序法益。我国环境犯罪的刑事治理存在由事后惩罚向事前预防的理论转变[⑥],累积犯正是将刑法介入的节点从实害结果前置于抽象危险的形成阶段,甚至更加靠前。

2. 累积行为具有真实的累积效应

这是累积行为具有可罚性的事实基础,也是对累积行为归责的根据。真实的累积效应描述行为如何侵害法益。德国刑法学界的主流观点对该国刑法典中污染水体罪(未经许可污染水域或对其品质作不利的改变)构成要件的理解是:行为并不需要对保护法益造成抽象危险,只需使天然水体在物理、化学或生物意义遭到值得关注的恶化程度即可。这种理解具有扩张性。库伦指出,从人类中心主义生态法益观角度,《德国刑法典》第324条所保护的是:"公众在维护水体作为人类生活

①李川:《二元集合法益与累积犯形态研究——法定犯与自然犯混同情形下对污染环境罪"严重污染环境"的解释》,《政治与法律》,2017年第10期。

②[日]山口厚著,付立庆译:《刑法总论》(第3版),北京:中国人民大学出版社,2018年版,第46页。

③[德]克劳斯·罗克辛著,许丝捷译:《法益讨论的新发展》,《月旦法学杂志》,2012年第12期。

④古承宗:《刑法第190条之一作为"累积的具体危险犯"》,《月旦法学杂志》,2018年第6期。

⑤焦艳鹏:《刑法生态法益论》,北京:中国政法大学出版社,2012年版,第29-32页。

⑥房慧颖:《污染环境罪预防型规制模式的省察与革新》,《宁夏社会科学》,2022年第4期。

的自然基础上的长远利益”[①]。但是，即便将“长远利益”具体理解为特定水体在行为发生时发挥的实际作用，个别行为的法益侵害或威胁也不足以对《德国刑法典》第324条展开教义学阐释。真实的累积效应表现为：“如果不禁止特定行为，就会对他人实施类似的行为具有现实性影响”[②]。这种影响是不同主体普遍、反复实施污染行为的真实可能性，具有导致环境承载、恢复能力下降甚至无法有效运行的危险。行为人出于利己因素的考虑，往往心存侥幸，只要污染行为难以察觉，或者惩处代价与污染收益远不成比例，通常不会排斥污染行为的实施。污染行为真实的累积效应越是显著，环境承载能力受到的威胁越是急迫。与其说真实的累积效应是对污染损害作事实确认，不如说是对污染行为的传染危险进行规范评估和警示。

3. 累积犯对传统的结果本位归责模式提出挑战

累积犯构成要件中的预设结果包括单独行为引起的结果和他人大量类似行为具有关联的部分结果[③]。累积犯将犯罪结果限缩在行为人自己引起的行为贡献部分，其他潜在行为人的利己决定作为建构其污染行为需罚性的条件，由此导致的批评意见是行为人要对尚未出现的整体结果负责，要对难以预见的情况归责[④]。以假定的整体行为或结果对行为人归责，具有实际意义。首先，整体行为或结果包含了个别行为的因果贡献，只是这种因果贡献无法精准识别。如要肯定因果关系，需确认行为人违反结果避免义务，且实行行为的危险性现实地转化为构成要件结果[⑤]。基于条件说衍生的因果关系理论大多是在相对封闭的时空中叙述因果历程，这些理论的核心要素是行为支配力或者支配可能性。从造成型因果到引起型因果，再到义务型因果，行为支配力或支配可能性逐渐减弱[⑥]。在疫病犯罪或者环境犯罪领域，行为支配力或支配可能性进一步削弱。个别行为对结果发生的支配作用可能难以识别，但是这些行为对结果发生具有促进作用。正所谓“雪崩时没有一片雪花觉得自己有责任”。其次，应从行为提升危害结果出现概率的角度理解累积犯的归责模式。如果多个独立行为整体地引起构成要件结果，这些行为贡献都是决定责任的原因[⑦]。针对累积犯的行为人系因他人行为而使自己遭受刑事处罚的批判意见，罗克辛认为，任何具有构成要件该当性的行为都存在法益侵害，比如，污染水源就是破坏环境，公职人员受贿就是损害廉洁行政，不需要认为整体生态环境或国家行政受损害[⑧]。如果对污染行为采取相对缓和的理解，将个别污染行为融入整体行为，提升了整体结果出现的概率，此时就需要行为人答责。行为、结果之间直接、明确的因果关系在概率论上等价于“必然发生”。将刑法关注点从实害结果前移至促进结果发生的原因，就可以将特定的实害结果理解为犯罪过程中大概率会出现的后果。以气候刑法为例，气候犯罪的构成要件结果是“引起气候变化本身”（气候损害）[⑨]，雾霾、温室效应等大气污染是气候变化的附随后果。概率提升型因果关系的优势在于可以妥善处理条件说下行为与其他要素黏连不分时的归责问题，

①[德]洛塔尔·库伦著，胡敏慧译：《环境刑法——新教义学的探索》，方小敏主编：《中德法学论坛》（第16辑下卷），北京：法律出版社，2019年版，第112-113页。

②张志钢：《论累积犯的法理——以污染环境罪为中心》，《环球法律评论》，2017年第2期。

③张志钢：《论累积犯的法理——以污染环境罪为中心》，《环球法律评论》，2017年第2期。

④孙国祥：《论累积犯的正当性及其限度——兼谈累积犯对污染环境罪构成的影响》，《法学》，2023年第9期。

⑤[日]山口厚著，付立庆译：《刑法总论》（第3版），第50页。

⑥劳东燕：《事实因果与刑法中的结果归责》，《中国法学》，2015年第2期。

⑦[德]克劳斯·罗克辛著；何庆仁，蔡桂生译：《德国最高法院判例·刑法总论》，北京：中国人民大学出版社，2012年版，第252页。

⑧[德]克劳斯·罗克辛著，许丝捷译：《法益发展的新讨论》，《月旦法学杂志》，2012年第12期。

⑨[德]赫尔穆特·查致格，尼古拉·冯·马尔蒂茨著；唐志威译：《气候刑法——一个未来的法律概念》，《南大法学》，2022年第6期。

在累积犯这种无法直接证明因果关系的犯罪类型中,将归责根据确定为污染行为具有提升污染结果出现概率的可能性,也符合公众对累积危害行为积量成罪的感知。总之,累积犯不是对行为引发具体结果的谴责,而是个别行为与整体结果互动导致的归责[①]。在概率提升情况下如果发生了实害结果,不必再通过累积犯的理论解读,直接根据罪刑规范确认犯罪成立即可。

二、数据安全与累积危险行为

在环境累积犯中,累积危险行为因侵害或威胁生态环境法益而具有刑事可罚性;在数据犯罪领域,数据累积危险行为因威胁数据安全而应受处罚。认定数据累积犯的前提是界定数据安全法益,只有在数据安全法益的指导下,才能归纳出数据累积犯的特征,并比较数据累积危险行为与累积危险行为的异同点,为数据累积犯的类型化分析奠定基础。

(一)数据安全法益属性及内容

在数据安全领域,计算机设备之间、计算机信息系统与网络空间之间的数据交互与信息变换,如同自然环境中生态系统间的物质交换与物种调节。数据安全状况随数据处理行为而变化,这就为数据累积犯的存在提供了空间。数据犯罪应当从计算机犯罪以及网络犯罪中剥离,对数据法益应当进行独立性保护[②]。数据犯罪的最初形态是计算机犯罪,但是将数据限定为计算机信息系统数据,将使数据对计算机信息系统产生依附性和局限性,无法规制超出计算机信息系统运行范畴的数据犯罪行为[③]。将计算机信息系统安全作为数据安全法益也不符合数据犯罪本质属性,将造成罪名区分困难和量刑容易失衡的局面[④]。网络犯罪是以网络为犯罪对象、工具或空间的犯罪现象的总称,无法体现数据犯罪的犯罪机理。将数据犯罪限缩为以数据为犯罪对象的犯罪类型,符合《数据安全法》对数据的定义。数据蕴含的经济、社会价值也赋予数据独立地位。数据是数字经济时代新型的资源类型。数据记录的信息及其衍生产品在大数据技术加持下,蕴含着巨大的商业价值;涉及国家安全、国民经济命脉、重要民生、重大公共利益等数据更是具有重要的战略意义。探索数据产权结构性分置制度,根据数据内容实施分类分级保护,以保障数据安全、开发商业价值,已成为现实的法律需求。此外,数据是计算机信息系统及网络空间的基础性语言,承担着支持计算机信息系统有效运行、维系网络安全持续稳定以及信息传达的重要功能。

《数据安全法》明确规定了“数据安全”的概念,有关数据安全法益的理论争议集中在数据记录安全还是数据内容安全之争。有的学者认为,应当将数据的保密性、完整性和可用性作为数据安全法益。保密性是指数据免受未授权人探知、获悉或使用;完整性是指数据不被修改或损害;可用性是指权利人能及时、有效地获取、使用数据[⑤]。有学者则认为,数据犯罪法益的本质在于数据所表征的信息,并认为将数据技术性特征平移为法益内容的做法,存在数据犯罪认定概念化和碎片化、法益内容丧失教义学功能、法益侵害判断间接性和主观性、滞后性和局限性等问题[⑥]。目前刑法适用于数据犯罪的罪名主要有计算机数据犯罪、个人信息犯罪、国家秘密类数据犯罪、商业秘密类数据

①孙国祥:《论累积犯的正当性及其限度——兼谈累积犯对污染环境罪构成的影响》,《法学》,2023年第9期。

②刘宪权:《数据犯罪刑法规制完善研究》,《中国刑事法杂志》,2022年第5期。

③陆一敏:《数据安全新型法益的建构——基于数据与信息的交互》,《苏州大学学报》(哲学社会科学版),2023年第4期。

④张勇:《数据安全法益的参照系与刑法保护模式》,《河南社会科学》,2021年第5期。

⑤杨志琼:《我国数据犯罪的司法困境与出路:以数据安全法益为中心》,《环球法律评论》,2019年第6期。

⑥赵春玉:《大数据时代数据犯罪的法益保护:技术悖论、功能回归与体系建构》,《法律科学》(西北政法大学学报),2023年第1期。

犯罪和其他数据犯罪五大类。上述罪群通过间接保护、多重保护和重点保护方式保护数据权益[①]。从上述分类可知，决定数据犯罪行为性质的始终是客体被侵害的具体面向的。考虑到记录安全与信息安全的表里关系，一行为同时触犯计算机数据犯罪或者其他类型数据犯罪时，应以想象竞合犯处断。不过，上述观点并未回答数据安全为何需要具备《数据安全法》第3条规定的“持续保障安全状态的能力”。在数字经济时代，仅关注数据记录安全或者内容安全的治理模式大体属于数据静态安全观。数据价值源于分析与挖掘，依赖汇聚与流通，新型数据风险主要是数据利用过程中的不法获取、持有、泄露、滥用等问题。还有学者认为，应当将可控性（Controllability）作为数据流动、聚合、分析过程中数据安全范式革新的核心，这种可控性是指将安全风险维持在可接受水平的能力[②]。本文赞同该观点，并进一步认为数据安全法益主要是数据与主体之间的安全稳定性[③]。这种安全稳定性是数据、信息、计算机信息系统及其主体间关系的安全稳定性，不仅包括主体对数据控制、占有、利用状态的稳定性，还包括数据不被其他主体窃取、篡改、使用、破坏状态的安全性，以及数据信息始终处于合法利用的稳定状态。

《数据安全法》对数据处于有效保护和合法利用状态的要求，是对数据保密、完整和可用等静态安全的提示；对数据具备保障持续安全状态能力的要求，则是对数据动态安全的要求。这种安全稳定状态既要求数据自身状态安全，也要求数据利用行为全程合规。安全稳定的利用状态是发挥数据价值的先决条件。数据价值的发掘历经数据资源、数据资产以及数据资本三个阶段，发挥数据价值的关键在于数据流动[④]。将安全稳定性作为数据安全法益，可以兼容根据技术特征总结的数据侵害判定规则，分析数据状态安全与应然情况的偏离程度，适应数据安全风险类型的转变，提高刑法对轻微数据不法行为的容忍度。

（二）数据累积危险行为的内涵与特征

当下，新兴科技和法律的紧张互动关系为学界所关注[⑤]。通信理论对通信系统作出了“物理层-代码层-内容层”的技术分层，将计算机信息系统分为存储介质层、数据文件层和内容信息层，三者犹如纸张、符号及所记录信息[⑥]。物理层（或存储介质层）的电磁记录或者其他形式的数据经转化进入代码层，成为计算机信息系统能够处理的数据符号或者符号序列，最终输出为人类能理解的信息内容。由此，可以将数据犯罪的实施过程归纳为，行为对数据从物理层到代码层、内容层链路转换功能和存在状态的侵害，以及对内容层信息的侵害。数据累积犯是数据犯罪和累积犯的结合，数据累积危险行为应当同时符合两者的本质特征，威胁着数据安全法益。

1. 数据的刑法保护范围

并不是所有的数据都值得刑法保护，并不是所有侵害数据的行为都构成犯罪。结构化数据集和静态数据库是计算机时代数据的主要表现形式，信息时代数据的内涵远大于信息。数据处理行为侵犯何种法益，需依据产生的数据风险进行识别[⑦]。目前刑法在数据保护范围上有所取舍。在数据分类上，无法与特殊利益相关联的一般数据、虚假数据、超过时效而没有价值的一般数据以及规

①喻海松：《数据犯罪刑法规制模式的现状评析与未来展望》，《法学杂志》，2023年第5期。

②刘金瑞：《数据安全范式革新及其立法展开》，《环球法律评论》，2021年第1期。

③张勇：《数据安全法益的参照系与刑法保护模式》，《河南社会科学》，2021年第5期。

④杨志琼：《数字经济时代我国数据犯罪刑法规制的挑战与应对》，《中国法学》，2023年第1期。

⑤许可：《论新兴科技法律治理的范式迭代——以人脸识别技术为例》，《社会科学辑刊》，2023年第6期。

⑥纪海龙：《数据的私法定位与保护》，《法学研究》，2018年第6期。也有观点认为应当区分为规则层、数字符号层和信息内容层三个维度，参见刘宪权：《元宇宙空间非法获取虚拟财产行为定性的刑法分析》，《东方法学》，2023年第1期。

⑦张勇：《数据安全分类分级的刑法保护》，《法治研究》，2021年第3期。

模较小的一般数据无须刑法保护[①];作为刑法前置法的《网络安全法》《个人信息保护法》也将匿名数据排除出保护范围。刑法重点保护特殊数据的立场值得肯定,但是过于偏向了数据静态安全观,没有注意到一般数据具有转化为特殊数据的可能性。在处理环节上,刑法主要规制数据获取、存储、提供等前端行为,对分析、使用等后端行为规制不足。非法获取数据只是数据犯罪的起始,非法处理和利用数据才是犯罪的根本目的。数据分析是一般数据转化为特殊数据的典型场景,也是容易滋生数据累积危险行为的环节。

2. 数据累积危险行为的真实累积效应

数据累积危险行为构成犯罪,需要具备真实的累积效应。在数据安全法益受到威胁的情况下,如果无法准确指出累积危险行为对数据状态、计算机信息系统功能造成的影响,就无法妥善识别行为的危害性。数据累积危险行为的真实累积效应,是足以诱导他人实施相同或者类似行为的可能性。根据数据的记录面向以及信息面向,需要分别确定数据处理行为长期失控可能导致的类型化后果,分别设定阈值,以及提示行为具有威胁阈值可能性的阈值警戒线。数据的记录面向通常与计算机信息系统功能的正常运行相关,应当根据数据生命周期的不同阶段寻找出计算机信息系统功能不能正常运行的原因,并分析是否因微量数据不法行为的累积突破阈值所致。例如,"脏数据"(Dirty Data)一般是指不符合要求以及不能直接进行分析的数据,主要包括缺失值、异常值、不一致的值、重复数据以及含有特殊符号的数据。"脏读"(Dirty Read)产生的数据往往错误、不真实或者不一致,这些问题数据具有导致系统功能异常甚至严重故障的风险。计算机信息系统中的脏数据越多,系统功能正常运行的安全状态就越不稳定。数据的内容面向与信息类数据犯罪相关,也需要根据具体犯罪的特点分别判断其类型后果,并设定阈值以及阈值警戒线。向生成式人工智能学习样本投毒的行为,具有使AI深度学习后生成侵犯他人著作权生成物的风险。此时的风险评估就需要考察数据投毒时长、投放方式、投放内容、学习过程及输出成果,综合多种因素加以确定。

3. 数据累积危险行为类型的判断

需要关注是否具有前置性法规的相关规定。计算机数据犯罪多有"违反国家规定"的要求,侵犯公民个人信息罪则是要求"违反国家有关规定"。数据累积犯的规制范围既要与前置法保持一致,实现部门法之间的协调;还要与环境犯罪原理相互对照,以保持方法论上的一致。如果数据累积危险行为仅有前置法的行政处罚规定而无刑法的对应规定,虽然不能实现最大程度的行刑衔接,但不至于违背刑法谦抑性。相反,如果只有刑事处罚的规定,没有前置法的行政处罚规定,这样既挑战了罪刑法定原则,也对解释者就空白罪状以及构成要件的解释能力提出极高要求,可能会因此产生类推解释。此外,数据产业中存在大量国家规定之外的技术标准,其功能是提供合理定型的参照规定。特定事实借助技术标准重构或建构后方能以可接受的成本为法律所识别[②]。"承认技术标准作为空白罪状规范的资格,是一种既能实现刑法风险管控又能实现行业自治的双赢方案"[③]。只有解释结论既符合刑法的规范保护目的,又在刑法语义射程内,方可在前置法缺位的情况下,引入技术标准辅助刑法解释,以识别数据累积危险行为,但这样的解释方法需要谨慎使用。

三、数据累积犯的类型化分析

数据累积犯是对数据领域积量成罪现象的理论解读,应当尽量依托刑法现有规定,以解释为优先。数据累积犯的特点是,微量侵害大量累积之后突破阈值,侵害数据安全稳定性法益,可以发

①刘宪权:《数据犯罪刑法规制完善研究》,《中国刑事法杂志》,2022年第5期。

②陈伟:《作为规范的技术标准及其与法律的关系》,《法学研究》,2022年第5期。

③冷必元:《论行业技术标准对空白罪状的补充》,《河南财经政法大学学报》,2023年第5期。

生在数据处理行为、计算机信息系统运行中，也可以发生在对数据内容的利用中。

（一）数据收集型累积犯

与数据收集有关的数据累积犯是非法获取计算机信息系统数据罪、侵犯公民个人信息罪等获取型犯罪。网络爬虫是行为人获取数据的重要工具。刑法理论主要以网络爬虫（Web Crawler）作为研究对象，并根据数据安全法益内涵讨论爬虫行为罪与非罪的边界[①]。爬虫技术的技术风险之一就是影响计算机信息系统功能，但如何评价爬取行为对计算机信息系统的干扰，尚未得到重视。爬虫技术模仿人工点击对网站进行一次性大量访问，挤占甚至破坏被访问对象的网络资源，影响计算机信息系统的稳定与运营[②]。数据爬取行为对计算机信息系统的干扰具有累积犯特征。其一，数据爬取行为依赖技术、不依赖身份，任何掌握爬虫技术的主体都可以实施爬虫行为，爬虫技术对网站承载能力造成的负担是同质的。网站通过身份认证机制过滤用户，反爬虫机制则是针对爬虫的技术特征禁止特定的访问方式，并不限定用户。不同主体可以同时访问同一网站，在特定时间段内激增访问流量，致使网站无法提供正常服务。如果缺乏充足的后台访问日志，无法将网站干扰的结果进行精准的归属。数据爬取行为意在获取有价值的信息，行为人的动机通常在于获取经济利益，因此，爬取行为具有扩散性和模仿性。其二，可以将前置规范中的安全标准视为阈值开始受到威胁时的大致警戒标准。国家互联网信息办公室《数据安全管理办法（征求意见稿）》第16条[③]关于“超出网站日均流量三分之一”的标准是对行为危险的提示，而不是作为罪与非罪的区分标准，故难以据此拘束特定自然人。严重影响网站运行（或妨害网站正常运行）与造成计算机信息系统不能正常运行的行为并不等同，自动化访问收集流量超过网站日均流量三分之一的行为不足以导致计算机信息系统功能的崩溃。在最高人民检察院废止检例第34号“李某杰等破坏计算机信息系统案”以后，“计算机信息系统不能正常运行”应明确为计算机信息系统本身不能正常运行[④]。超过网站日均流量三分之一的技术红线更加不可能作为适格的犯罪结果，也无法发挥成立累积犯的阈值锚定作用，但是该标准可以提示行为开始具有威胁阈值的可能性。此种数据收集型累积犯的阈值，应在“超出网站日均流量三分之一”到计算机信息系统不能正常运行之间进行评估确定。

（二）拒绝服务型累积犯

拒绝服务型数据累积犯以拒绝服务攻击为典型。任何使服务可用性降低或者失去可用性的干涉都是拒绝服务。拒绝服务攻击是指攻击者让目标机器停止服务或资源访问、阻止正常用户访问的攻击，被利用的目标资源包括磁盘空间、内存、进程甚至网络宽带，既可以利用系统漏洞进行拒绝服务攻击，也可以利用协议漏洞进行拒绝服务攻击（SYN Flood/UDP Flood攻击/Land攻击/死Ping）[⑤]。拒绝服务攻击的特点是不修改、不删除、不增加计算机信息系统及数据，本质是暂时对受攻击的计算机系统功能进行干扰和影响[⑥]。除了拒绝服务攻击之外，还有分布式拒绝（DDoS）攻击、反射型DDoS攻击等变种[⑦]。DDoS攻击（Distributed Denial of Service，分布式拒绝服务）是指通过控制

①欧阳本祺：《论数据犯罪的双层法益》，《当代法学》，2023年第6期。

②孙杰：《数据爬取的刑法规制》，《政法论丛》，2021年第3期。

③国家互联网信息办公室关于《数据安全管理办法》（征求意见稿）第16条规定：网络运营者采取自动化手段访问收集网站数据，不得妨碍网站正常运行；此类行为严重影响网站运行，如自动化访问收集流量超过网站日均流量三分之一，网站要求停止自动化访问收集时，应当停止。

④根据《最高人民检察院关于宣告部分指导性案例失效的通知》（高检发办字[2024]35号），指导性案例“李骏杰等破坏计算机信息系统案”（检例第34号）被宣告失效。该案中，法院将“造成系统不能正常运行”作为定罪标准，与最高人民法院第145号指导案例“被告人张竣杰等非法控制计算机信息系统案”的定罪标准存在冲突。

⑤李飞等编著：《信息安全理论与技术》，西安：西安电子科技大学出版社，2016年版，第139-142页。

⑥郝义嘉，陈芳：《非法控制他人计算机进行拒绝服务攻击行为之定性》，《人民司法·案例》，2012年第4期。

⑦喻海松：《网络犯罪二十讲》（第2版），北京：法律出版社，2022年版，第22-24页。

“肉鸡”,对一个或多个目标发动攻击,致使目标服务器断网或资源用尽,最终停止服务。反射型DDoS攻击是DDoS的新型变种攻击方式,是指使用互联网的特殊服务开放的服务器,通过伪造被攻击者的IP地址,向开放的服务器发送请求数据包,服务器收到后将数倍的回答数据包发给被攻击者的IP,最终形成对目标的DDoS攻击①。在刑法中,对拒绝服务攻击行为进行规制的罪名主要是非法控制计算机信息系统罪和破坏计算机信息系统罪,前者规制控制肉鸡等资源的行为,后者规制具有累积犯特征的攻击行为。拒绝服务的行为特征在于一旦攻击停止就无法采集到证明攻击实施的证据②,由于攻击行为与干扰结果因果关系隐蔽,无法排除攻击者搭上他人攻击行为便车、最后全身而退的可能性。如果不加以禁止,极易诱使他人实施类似的攻击行为。拒绝服务攻击还具有攻击持续性的特点,只有被攻击对象的服务、资源被占据到一定程度,才能判定为计算机信息系统不能正常运行。拒绝服务攻击的社会危害性应当根据攻击效果评价。拒绝服务攻击的直接攻击效果是使特定的计算机信息系统不能正常运行,间接攻击效果是因被攻击对象无法正常运行而影响他人工作、生活的正常开展。在《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》(以下简称“《危害计算机信息系统安全解释》”)第4条第1款第4项③中,认定“后果严重”需要确认攻击行为造成100台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为1万以上用户提供服务的计算机信息系统不能正常运行累计1小时以上。拒绝服务型数据累积犯的阈值,应当是被攻击对象服务、资源被占据到不能正常运行的临界点。因此,该条中的“累计1小时以上”并不是对阈值的规定,而是对实害后果的规定。

(三)数据分析型累积犯

数据分析型累积犯主要是信息类数据犯罪,以侵犯公民个人信息罪为典型。借助算法可以从一般数据中分析出特殊数据,其非法分析行为具有纳入刑法规制范围的必要性④。《数据安全法》第32条规定,数据收集活动应当合法、正当,不得窃取或者非法获取,法律、行政法规另有规定的从其规定。数据在聚合分析后才可能成为个人信息,数据处理行为体现出累积犯特征。用户画像是典型的数据分析型累积犯场景,其他诸如破解商业秘密等需要聚合分析的数据处理活动,也可归入数据分析型累积犯。用户画像是以标签形式对自然人进行的特征展现和模型塑造⑤。随着画像精确程度提升,用户画像的法律属性在数据、信息、个人信息以及敏感个人信息间依次变换。一旦用户画像可用以识别出特定自然人身份或者特定自然人活动情况,画像绘制以及后续提供、使用等处理行为就有侵犯公民个人信息的风险。因此,需要讨论以下几个问题。

1. 界定公民个人信息应采取何种标准

公民个人信息的界定标准应当采取识别说还是关联说,相关规范性文件的判断标准存在变化。《网络安全法》、《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》(以下简称“《个人信息刑案解释》”)、《信息安全技术 个人信息安全规范》(GB/T 35273-2020)以及《个人信息保护法》等前置法律、司法解释及技术标准各自定义了个人信息,并根据类目列举了常见情形。通

①朱飚凯,李慧敏,刘三满等:《基于云环境的反射型DDoS攻击检测》,《信息安全与通信保密》,2022年第2期。

②喻海松:《网络犯罪二十讲》(第2版),第49页。

③根据《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》(法释[2011]19号)第4条第1款第4项规定,造成为100台以上计算机信息系统提供域名解析、身份认证、计费等基础服务或者为1万以上用户提供服务的计算机信息系统不能正常运行累计1小时以上的情形,属于破坏计算机信息系统罪罪状中的“后果严重”。

④刘宪权:《数据犯罪刑法规制完善研究》,《中国刑事法杂志》,2022年第5期。

⑤用户画像没有统一的定义。《深圳经济特区数据条例》第2条第8项规定:用户画像,是指为了评估自然人的某些条件而对个人数据进行自动化处理的活动,包括为了评估自然人的工作表现、经济状况、健康状况、个人偏好、兴趣、可靠性、行为方式、位置、行踪等进行的自动化处理。

过梳理文件可以发现，个人信息的识别规则由识别转向了关联，而且上述文件列举的个人信息种类不完全重合。某一项信息是否属于个人信息，不在于是否被列举，而是须依照个人信息的抽象定义进行个案考察[①]。例如，个人姓名、生日、性别在欠缺其他信息补强时，只能还原出符合条件的人群集合。《个人信息保护法》对个人信息的定义支持了关联路径，存在的问题是扩大个人信息范围，且无法解释匿名化信息的存在。匿名化信息是典型的符合个人信息关联路径，但由于不可还原而不属于个人信息的数据，因此，只能将关联路径理解为验证识别路径判定结果准确性的验证方式。

2. 如何界定用于绘制画像的行为信息的法律属性

该问题涉及如何判断行为信息向个人信息转变的转折点。行为信息是用户画像的数据基础。行为信息是否属于个人信息，学界尚未形成通说。行为信息一般表现为浏览记录、购买记录、交易方式等反映用户网络行为举止、消费习惯的信息，这类信息源自人的行为，但不能凭此单独识别出特定自然人或特定自然人活动情况。特定信息是否属于公民个人信息，需要根据信息本身的重要程度、和其他信息的结合程度以及行为人的主观目的进行具体判断[②]。在具体场景下需要更加严格地遵照识别路径判断。例如，行为信息与设备绑定，只有证明特定设备使用人在特定时段实施特定行为的关联性，而且通常欠缺诸如行踪轨迹、住宿信息等一类、二类信息具有的信息指向性和敏感程度。由于特定设备的使用者与特定自然人不必然重合，这就导致特定行为信息一般属于《个人信息刑案解释》第5条第1款第5项所规定的三类信息，法律属性应属可识别的个人信息，或者不可识别的个人信息[③]。

3. 如何界分去标识化信息、匿名化信息与个人信息

去标识化是数据脱敏的关键，是指数据经过处理，使其在不借助额外信息的情况下无法用以识别特定自然人或相关标识符的过程。匿名化是去标识化的强化，是指数据经过处理，无法识别特定自然人或者相关标识符且不能复原的过程。人格权益与财产权益的区分是数据展现经济价值的前提[④]。去标识化与匿名化都能够减少数据中的人格权益，实现财产利益的先决条件是不得侵犯数据产品或数据服务中的人格权益。数据生产者通过生产行为获得数据权益，该行为是事实行为且是原始取得[⑤]。个人私密、敏感的信息在去标识化后，人格属性减弱、财产属性和交易价值增加，社会公共属性得以体现、凸显，此时的数据属于单纯的个人数据[⑥]。但是，来自自然人的原始数据即便在“脱敏+不可逆”的技术处理后仍然具备可识别性[⑦]，重新加工汇集的数据产品可能使这部分数据去匿名化[⑧]，这是数据处理中必须保持的安全稳定性。

---

①韩旭至：《个人信息列举式规范之审视》，《河南财经政法大学学报》，2018年第4期。

②喻海松编著：《最高人民法院、最高人民检察院侵犯公民个人信息罪司法解释理解与适用》，北京：中国法制出版社，2018年版，第23-24页。

③已识别个人的信息是指已经确定能从人群中识别出某个人的信息；可识别个人的信息是指可能根据这些信息或结合其他信息而识别某个人的信息；不可识别的信息则是不可能识别到某个人的信息。参见丁晓东：《用户画像、个性化推荐与个人信息保护》，《环球法律评论》，2019年第5期。

④例如《深圳经济特区数据条例》第4条规定：自然人、法人和非法人组织对其合法处理数据形成的数据产品和服务享有法律、行政法规及本条例规定的财产权益。但是，不得危害国家安全和公共利益，不得损害他人的合法权益。

⑤方瑾业：《论数据财产权司法属性与归属——以数据生产与流通为视角》，《上海政法学院学报》（法治论丛），2023年第6期。

⑥张勇：《APP个人信息的刑法保护：以知情同意为视角》，《法学》，2020年第8期。

⑦苏成慧：《多元场景视域下数据流通的法律规制》，《学术交流》，2023年第12期。

⑧张敏：《数据交易中的伦理问题及其法律规制》，《上海政法学院学报》（法治论丛），2023年第6期。

4. 如何把握用户画像的使用尺度

该问题涉及去标识化信息重标识攻击成功的临界点。行为数据、去标识化或者匿名化数据是否属于个人信息,取决于数据自身属性。用户画像包括用户属性、用户特征、用户标签三要素,其中,用户属性包括用户基本信息等相对稳定的静态属性以及用户行为信息等动态属性;用户特征是从用户属性中提取的特性或共性;用户标签是根据用户特征进一步提炼的标签化文本①。用户属性中体现人格权益的静态属性部分必须进行脱敏处理。用户画像的基本元素是标签,设备(及其使用人)是用户画像所要绘制与分析的对象。从采集设备上的行为信息提炼标签,再利用标签绘制用户画像,每一步都在向真实的用户靠近。需要注意的是,用户画像默认设备使用人和设备所有人是同一主体,一旦使用人出借设备供他人使用,设备上的行为信息就会受到他人行为的污染。这也解释了用户画像中为何有群体画像的存在,以及重标识攻击只要还原到一定数量的自然人就算攻击成功。直接使用特定自然人个人信息形成的特征模型是直接用户画像②,该直接用户画像精准"狙击"了特定自然人。在用户画像场景中,将行为信息脱敏为去标识化信息,将去标识化信息提炼为用户特征、标签,将用户特征、标签分析出用户画像,三处场景中行为对象均发生了质的变化,都需要引入阈值指明量变与质变的界限。根据尊重人格权益的本质,数据服务提供方需告知信息主体数据服务提供方及其合作方的数据处理措施以及数据使用场景,使用户充分"知情同意"其身份或活动情况的后续走向。对个性化推荐或者画像使用进行提示,以及为用户提供随时撤销授权的选项就具有必要性。

5. 需持续地监控去标识化效果

此外,还需要慎重选择去标识化技术和模型、评估各个环节的数据清洗以及去标识化(甚至匿名化)处理的合规程度,妥善制定不同环节、不同去标识化技术及其模型对应的阈值,并对不同环节的数据分析、信息利用实施分类分级管理。阈值具有提示隐私政策、数据分析技术以及安全措施已经无法实现降低信息区分度的警示作用,并且提示数据分析、画像行为已经制造出不被允许的风险。去标识化技术、重标识技术以及重标识攻击都在迅速变化,必须持续性地监控去标识化效果,定时或者不定时通过重标识攻击风险评估,检测先前去标识化处理的数据是否保持稳定的安全状态。"环境风险是针对数据集发起一次或多次重标识攻击的概率。任何去标识化的数据集中都存在重标识风险,然而依据数据发布类型模型的不同,攻击者可实施攻击类型是不同的。"③例如,在公开共享数据发布模型中,数据集可供任何人使用,攻击者对数据集重标识攻击的概率为1;而在受控共享数据发布模型中,需要区分内部故意攻击、来自熟悉的数据集中的个体无意识识别以及数据泄露,按照《信息安全技术 个人信息去标识化指南》(GB/T 37964-2019)的要求,根据不同的攻击方式特点衡量出不同的攻击概率。对于突破个人信息安全阈值的行为,可以推定行为具有实质违法性,只是是否应当以犯罪论处,需要根据侵犯公民个人信息罪的犯罪构成进一步判断。

四、数据累积犯的因果关系认定

因果关系是证成数据累积犯的重要环节,也是司法认定的难题。由于数据累积犯所要规制的

①宋美琦,陈烨,张瑞:《用户画像研究述评》,《情报科学》,2019年第4期。

②参见国家市场监督管理总局、国家标准化管理委员会《信息安全技术 个人信息保护规范》(GB/T 35273-2020)第3.8条注。

③参见国家市场监督管理总局、中国标准化管理委员会《信息安全技术 个人信息去标识化指南》(GB/T 37964-2019),附录B(资料性附录)常用去标识化模型B.1.4.2环境风险度量。

对象是微量数据不法行为，无法借助传统因果关系理论描述行为与结果的关系。在数据累积犯因果关系认定过程中，应当注重以下两个方面。

（一）数据累积犯因果关系判断

1. 需引入规范评价

在数据累积犯的因果关系判断上，应当立足事实判断，重视规范评价。事实判断是从自然意义角度理解因果关系；规范评价则是根据经验法则、刑法规范以及法理，对行为与结果的联系进行价值评判。在行为单一的简单案件中，事实判断与规范评价同步完成；在主体众多、行为多样的复杂案件中，纯粹的事实判断不足以实现结果归责。规范评价倾向于以价值判断方式解决某些以不确定或概率形式出现的事由，虽有利于解决复杂因果关系的结果归责，但可能侵袭事实判断[①]。因此，数据累积犯的因果问题必须引入规范评价。一旦将数据累积犯的因果判断拘泥于事实判断，微量行为与结果便难以建立直接、确定的现实联系。根据“事实存疑有利于被告人”原则，应宣告行为人无罪或者至多未遂，这样一来，行为人将犯罪行为化整为零反而能够逃脱刑法制裁，这显然违反了刑法的法益保护目的。数据累积犯因果关系具有从部分到整体、从现实到假定的判断次序。规范评价侵袭事实判断的表现是拔高个别行为的危害性、夸大其严重性，虚置了整体结果在因果认定上的作用，使数据累积犯成为极端的抽象危险犯。

2. 不能采用重叠的因果关系

数据累积犯的因果关系模式不能采用重叠的因果关系。重叠的因果关系是典型的多因一果，行为与结果联系紧密，可以在结果原因分析中确定各个行为如何相互作用以及因果贡献大小。数据累积犯中的个别行为数量庞多、危害微量，行为如何相互作用并不清晰，难以通过对结果的原因分析评判个别行为的具体作用。因此，数据累积犯的因果关系只能立足于真实的累积效应是否存在、行为是否具有作用于未来的危险趋势、以及行为对阈值的威胁情况等特征点构建。如上文所述，数据累积犯构成要件的预设结果包括单独行为引起的现实结果以及与他人大量类似行为具有关联的假定结果。数据累积犯的因果关系判断，不仅需要关注累积犯的阈值，也需要关注提示行为已经具有威胁阈值可能性的阈值警戒线。数据收集型累积犯中的“超出网站日均流量三分之一”就是典型的阈值警戒线。现实危害超越阈值警戒线的个别行为具有向数据累积犯发展的可能性，现实危害低于阈值警戒线的个别行为，因为行为欠缺足够的违法性，不宜纳入数据累积犯的视野。至此，数据累积犯的因果关系应分为行为危害超越了阈值警戒线的显性因果，以及带有规范评价下与真实累积效应相关、严重威胁阈值的隐性因果，它们如同海上冰山，水面上的显性部分清晰可见，水面下的隐性部分需根据前者科学评估。相应地，数据累积犯的因果构造应当采用“特定因”（Specific Causation）与“一般因”（General Causation）的构造，特定因涵盖个体因果关系，关注污染源致害的现实性；一般因涵盖类别因果关系，关注污染源致害的可能性[②]。

3. 对“特定因”与“一般因”的判断

“特定因”属于事实判断，“一般因”属于规范评价。“特定因”是将危害超过了阈值警戒线的现实结果归因于特定行为的过程，通常不存在判断难题。需要引起重视的是对“一般因”的判断。成立数据累积犯的“一般因”，既需要证明行为具有真实的累积效应，也需要证明行为严重威胁阈值。行为是否具有真实的累积效应，建立在对行为方式、技术门槛、现实结果、行为动机、行为回报与风险、行为人身份、案件查证难度等因素的综合考察上。以利用爬虫的数据收集型数据累积犯为例，如果服务器的日志充分，可以分析出特定爬虫占用的资源比例，对特定爬取行为起到的作用进行精准的定量分析。如果发现爬取者恶意地变换IP进行爬取，尽管理论上服务器可以运用浏览器指

①李会彬：《刑法因果关系中事实判断与规范评价的区分》，《政治与法律》，2022年第4期。

②陈伟：《疫学因果关系及其证明》，《法学研究》，2015年第4期。

纹以及其他的安全产品分辨攻击者,然而这也会耗费大量人力、物力。在这种情况下,恶意变换IP体现了行为存在真实的累积效应。凡是体现利诱性、具备隐蔽性的行为,或者法律责任不合比例的情形,都能确认具有诱使他人冒险实施同类行为的可能性。

在行为是否严重威胁阈值的判断问题上,需要重视以下三个问题:其一,行为是否严重威胁阈值的判断根据是行业内的技术规定。数据累积犯是借助累积犯理论产生的犯罪解读方式,底层逻辑建立在数字科技以及一份份技术文件之上。隐性、显性因果本质上可以视为是对特定领域内的特定数据风险进行观察、识别与评估的法律重述,风险评估的准确程度依赖技术的发达程度。其二,参照系的选择不同,得出的阈值不同。向一条流入湖泊的小河排放少量污水的行为,对河流的局部水质而言是抽象危险或者具有可罚性的累积危险,对湖泊而言,排放行为的危害程度只是极其轻微、可以忽略不计的累积危险。特定数据累积危险行为对于计算机信息系统正常运行、特定数据、信息合法利用造成的影响,需要结合选定的参照系综合评判。参照系的选择错误将不当拔高或者降低阈值,进而影响对数据累积危害行为可罚性的评估。其三,不宜简单地将司法解释规定的罪量要素作为阈值对待。阈值是积量成罪质变的标志。司法解释规定的罪量要素与阈值混同,将使阈值丧失场景性。更何况,阈值应当由做为前置性规范的技术标准确定。目前司法解释所规定的数量要素并没有得到前置性技术标准的支持,其规范功能仅在于作为“情节严重”或“后果严重”的认定依据。

(二)数据累积犯因果关系排除

1. 应排除没有真实累积效应的行为

数据累积犯的核心在于真实的累积效应,应当排除没有真实累积效应的行为。刑法中存在诸多以累计结果作为犯罪成立条件的罪名,如果不着重提示真实的累积效应,则难以区分累积犯与此类犯罪。在盗窃罪的基本罪状中,既有犯罪数额累计的数额较大,也有犯罪次数累计的多次盗窃,但没有人会把盗窃罪理解为累积犯。此外,应当否定泛化运用累积犯理论的观念。有观点认为,可以借助累积犯理论,运用帮助信息网络犯罪活动罪规制网络账号恶意注册行为[①]。该观点值得商榷。帮助信息网络犯罪活动罪的理论源头是共同犯罪,网络账号恶意注册行为的危害性来自账号后续使用。如果没有后续使用行为,原子化的网络账号的数量累计仅是量的累计,社会危害性在于扰乱网络账号注册秩序而非侵害财产、个人信息等法益。“在现阶段对恶意注册行为本身的规制理论不足的情况下,需要从行为方式、行为结果等流程上选取特定的构罪事由加以刑法适用”[②]。累积危险行为的危险性来源于行为本身,不需要再借助其他行为威胁法益,本文所列举的三种数据累积犯对于法益的威胁均源自收集行为、攻击行为、分析行为本身固有的危险。行为危害微量,可以在质上融合、量上叠加,而且危害结果可以归因于累积行为本身,这才是数据累积犯因果判断时需坚持的行为、结果识别标准。

2. 特定因的事实认定与一般因的规范评估

数据累积犯存在扩大适用的风险,必须严格把握特定因的事实认定与一般因的规范评估。一是应当避免因考察视角错位导致的扩大处罚。地域性的考察方式可能会导致恣意且不正当的处罚[③]。局部视角下累积危险不足的行为,可能会被作为数据累积犯因果关系的起点对待。在环境犯罪中,不具有利益相关性的偶发行为尽管可能侵害人身或财产法益,但没有被不同主体大量实施

①郭玮:《累积犯视域下网络账号恶意注册行为的规制》,《法学杂志》,2020年第1期。

②庄嘉:《流量造假犯罪核心与外延行为的刑法规制》,《青少年犯罪问题》,2023年第5期。

③[德]赫尔穆特·查致格,尼古拉·冯·马尔蒂茨著;唐志威译:《气候刑法——一个未来的法律概念》,《南大法学》,2022年第6期。

的可能性，即便造成局部破坏，也不可能积累出对生态环境的整体威胁[①]。数据累积犯中的结果具有整体性，在因果关系考察上应当从整体视角把握数据累积危险行为对数据安全的影响。需要特别关照数据处理对象与其他计算机信息系统之间的交流程度，准确评估行为的严重程度。二是应当对行为危险程度进行具体细致的考察，避免危险判断抽象与空洞。对危险程度进行具体细致考察不代表认可累积犯是具体危险犯。在抽象危险犯成立与否的问题上，应具体判断行为本身是否蕴含发生危险的属性。许多客观上污染环境的行为在生活中十分常见，不妨碍对累积行为增加“创设法不容许风险”这一实质限制。这一点与数据累积犯因果关系判断是一致的，数据累积犯也是创设法所不允许风险的行为。在水污染犯罪领域，《德国刑法典》的做法是设立“微量条款”[②]以实现出罪，这相当于我国《刑法》第13条的但书规定。《德国刑法典》关注污染行为有害影响的排除，要求具体细致判断污染行为及其程度。《关于办理环境污染刑事案件适用法律若干问题的解释解释》（法释[2023]7号，以下简称“《环境污染司法解释》”）第1条第5项规制的隐蔽性排放具有典型的累积犯特征，如果不考虑查处时污染行为导致的现实结果，难免会使人质疑处罚根据不在于隐蔽性排放行为，而在于逃避监管的犯罪方式。

3. 避免对不同犯罪场景适用同一阈值

在生态环境中，生态系统由不同要素组成，不同要素受污染的方式及程度各有不同。土壤具有明显的区域性，水体次之，空气无国界之别、可以自由流动，这就导致不同生态要素的污染方式及其相应污染阈值没有统一标准，应当各自确定。承认阈值概念，就意味着必须以动态视角观察行为由因到果的变化。阈值所代表的成立犯罪所必须的重大性门槛是确定的。现实生活中存在一些自然发生的损害环境品质的现象或者行为，但是这些现象或行为在法律上未必具有可罚的违法性。从这个角度上讲，阈值警戒线的概念也是必要的。相应地，累积犯中通常理解的阈值是整体结果的阈值。《环境污染司法解释》第1条第3项、第4项关于超过国家或者地方污染物排放标准3倍以上、10倍以上的规定，即是注意到污染物种类对阈值的影响。只是污染物排放标准以浓度作为计量单位，完全可能存在排水口的瞬时浓度超标但总体上污染排放物不足以污染环境的情况，此时就应当考虑是否可以运用微量条款实现出罪或者宽缓化处理。在数据累积犯中，阈值为司法解释规定的罪量要素所遮盖，数据累积犯中不同行为种类的阈值的精准确定更加困难。网络社会规范极其庞杂，刑法只是法律系统的末端[③]。如果说确定阈值的目的在于准确评估行为的危害性，将司法解释规定的罪量要素理解为实害结果或者处罚条件，将阈值标准交由前置技术标准确定更加合适。

[责任编辑：郑　毅]

①李川：《二元集合法益与累积犯形态研究——法定犯与自然犯混同情形下对污染环境罪“严重污染环境”的解释》，《政治与法律》，2017年第10期。

②《德国刑法典》第326条第6款规定：由于垃圾数量小，显然可以排除对环境，尤其是对人、水域、空气、土地、可食动物或植物的有害影响的行为不处罚。

③刘艳红：《网络时代社会治理迭代升级与犯罪控制协同化的刑事政策》，《社会科学辑刊》，2024年第1期。