

数字法律预防的理论基础与制度构建

郑智航*

内容提要 数字法律预防是在网络空间、数据应用、人工智能系统等数字环境中,运用系统性、前瞻性的数字技术手段预先识别、评估、规避潜在法律风险,从而减少违法行为发生、防范权益侵害的综合性预防机制。数字法律预防具有鲜明的架构化特点。数据驱动是数字法律预防的认识论基础,抽象风险下的法秩序和公共安全是数字法律预防的主要保护客体,行为阻断是数字法律预防的主要效果机制,“全息统御”是数字法律预防的时序位置,人机协同是数字法律预防执行机制的鲜明特征。数字法律预防整体上契合现代法律价值,但受数字法律预防底层结构的影响,不可避免地与现代法律追求的部分价值存在一定的张力或冲突。沿着“法律目—法律关系—预防行为—技术规制”这一脉络构建数字法律预防制度,对于减轻或化解数字法律预防与现代法律价值之间的张力或冲突具有重要意义。

关键词 数字法律预防 预防型法治 风险预防 数字技术 法律价值

DOI:10.14111/j.cnki.zgfx.2026.02.002

目次

- 一、引言
- 二、数字法律预防的底层结构
- 三、数字法律预防的规范逻辑
- 四、数字法律预防与法律价值的张力
- 五、数字法律预防的制度构建
- 六、结语

* 山东大学法学院教授。本文系 2023 年度国家社科基金重大项目“当代中国数字法学基本范畴体系研究”(项目批准号:23&ZD153)的阶段性成果。

一、引言

随着大数据、云计算、区块链、人工智能等新兴技术迅猛发展,人类社会逐渐进入万物皆可连接、皆可计算、皆可智能的数字社会。这些数字技术能够对社会进行全周期、全领域、全时空的状态感知,并在数据搜集、同步分析和自我学习的基础上进行自动决策和精准执行。^①这极大地提升了人们预测和感知未来的能力。从全球范围看,预防型法治的理念以及承载它的统计模型与软件程序逐步渗透到纠纷预防、犯罪预防和风险防控等法律实施领域,推动传统法律预防功能向实时化、智能化和精准化深度变革。

法学界已经开始关注数字法律预防这一问题,并主要从工具论和对象论两个角度展开研究。工具论认为数字法律预防的核心在于通过数字技术的赋能来提升法律的预防功能。^②然而,数字技术在赋能法律预防的同时,也因为数据和算法层面的准确性、透明性等问题,出现技治主义倾向。对象论认为数字技术自身具有一定的风险性,应当成为法律预防的对象,并围绕技术行为的自主性原则、^③行为在先还是技术在先、^④后果控制与动机遏制^⑤等问题,建构一种有关数字技术的预防性伦理和法律。这些研究主要是从具体场景出发,针对预防性行政、预防性执法、预防性警务、预防性治理等问题展开,缺乏对数字法律预防的底层结构、规范逻辑、价值冲突等的深入探讨。

其实,数字法律预防通过独特的技术事实,生成了一种嵌入式的底层结构。这种底层结构深刻影响数字法律预防的规范逻辑。数字法律预防在促进社会整体安全、提升治理效率的同时,也不可避免地会与现代法律追求的部分价值进行一定程度的碰撞。这需从法律制度层面进行回应。因此,本文试图从整全性角度出发,将法律预防置入数字法治的理论框架,分析数字法律预防的底层结构、规范逻辑及其与现代法律价值存在的张力,并据此提出数字法律预防的制度构建路径。

二、数字法律预防的底层结构

所谓数字法律预防,是指在网络空间、数据应用、人工智能系统等数字环境中,运用系统性、前瞻性的数字技术手段预先识别、评估、规避潜在法律风险,从而减少违法行为发生、防范权益侵害的综合性预防机制。从实践来看,数字法律预防主要通过计算社会科学方法,使用可重复的预测指标体系对风险进行概率量化,并进行自动决策和精准执

① 参见齐延平:《数智化社会的法律调控》,载《中国法学》2022年第1期,第78页。

② 参见陈永生:《大数据预测警务的运作机理、风险与法律规制》,载《中国法学》2024年第5期,第165页。

③ 参见芦文龙等:《技术行为的自主性原则:在预防在先原则和行动在先原则之间》,载《科学技术哲学研究》2014年第5期,第74页。

④ See H. Sterling Burnett, *Understanding the Precautionary Principle and Its Threat to Human Welfare*, Social Philosophy & Policy Foundation, Vol.26:378, p.378-410 (2009).

⑤ 参见何怀宏:《建构一种预防性的伦理与法律:后果控制与动机遏制》,载《探索与争鸣》2018年第12期,第11页。

行。这显然区别于传统社会主要依靠经验感知和质性判断的法律预防。因此,阐明数字法律预防的底层结构具有基础性意义。

(一) 数字法律预防的主要形态

在传统社会,各国法律都重视法律预防,但受技术条件的限制,这种法律预防往往依赖专家、执法者和法官等基于个人经验和直觉而形成的经验感知和质性判断。进入数字社会,数字技术的发展极大地提升了法律预防的能力并使其广泛运用于法治的具体场景。

第一是大数据预测警务。作为一种精准预测机制的大数据预测警务,大约发端于20世纪90年代。它主要通过使用犯罪绘图和地理信息系统对犯罪数据的空间分布特征进行精准测绘与动态解析,执法机构能够开展犯罪态势推演与区域风险画像绘制,并据此预测出不同区域未来一段时间内的犯罪风险值,进而形成面向不同地理单元的犯罪风险预警模型,为前瞻性部署防控资源提供量化依据。^⑥经过30多年的发展,大数据预测警务发展的脉络可以归纳为以下三个阶段:从以财产犯罪预测为核心的预测警务1.0阶段,到以财产犯罪预测和暴力犯罪预测为核心的预测警务2.0阶段,再到实现对可能实施犯罪的具体人的预测警务3.0阶段。^⑦从实践效果看,大数据预测警务能够较为精准地预测未来可能发生犯罪的时间、地点甚至人员,据此,执法机构可以合理地配置警力资源,提升犯罪防控的精准性、响应速度与整体警务效能。

第二是数字检察中的犯罪预防。数字检察是检察机关在个案办理过程中识别具有共性特征的问题,应用算法、代码及人工智能等技术对相关数据进行分析与研判,进而生成类案监督线索,并在此基础上推进类案办理与综合监督的活动,从而提升检察履职的精准性、前瞻性和整体效能。^⑧数字检察中的犯罪预防体现为将法律监督关口前移的前端治理机制,旨在借助智能化应用全面赋能法律监督以实现风险识别、主动预警和源头治理。一是类案预防治理。检察机关能够运用数智化工具对案件线索进行交叉比对与关联分析,识别具有共性特征的典型犯罪,将分散于个案中的“小数据”汇聚为反映违法犯罪趋势与治理规律的“大数据”,并在此基础上形成“个案办理—类案监督—系统治理”的犯罪预防路径。^⑨二是防范再犯罪风险。数字检察可以借助大语言模型对法律文书进行全要素结构化处理,分析犯罪行为规律及风险特征,并构建犯罪嫌疑人、被害人画像,揭示制度运行中的薄弱环节,最终服务于再犯罪的前置预防。三是特殊群体精准预防。数字检察能够通过多维数据分析,对涉案未成年人等重点群体的行为风险进行分级评估,并据此实施差异化干预措施。

第三是数字法院中的法律预防。数字法院建设进一步强化了法院的法律预防功能。法院不仅需要借助数字技术防止法律适用环节的形式性错误,还要在统筹兼顾政治效

^⑥ See Derek J. Paulsen, *To Map or Not to Map: Assessing the Impact of Crime Maps on Police Officer Perceptions of Crime*, *International Journal of Police Science and Management*, Vol.6:234, p.235 (2004).

^⑦ 参见前注②,陈永生文,第167-171页。

^⑧ 参见谢登科:《数字检察的类型分析及其发展完善》,载《学术交流》2025年第8期,第56页。

^⑨ 参见高通:《数字赋能与检察权运行》,载《国家检察官学院学报》2025年第6期,第120页。

果、法律效果与社会效果的基础上,强调法院对裁判风险的事前识别能力,在裁判形成之前对司法活动的质量内容进行前置性预防把控。一是推进法律适用情况的主动性审查,预防法律适用错误。数字法院通过推进“智慧提示预警”机制的建设,将文书制作中的常见易错点转化为可识别、可触发的技术规则,在裁判生成阶段即对潜在风险进行提示和校验,以保障公民免受因司法工作人员的个体失误而带来的不公正对待,使裁判风险在形成之前即被纳入可控范围。^⑩二是将矛盾纠纷预防化解关口有效前移,促进高质量司法建议的形成。在全要素数字化转型的背景下,法院从依托个案对社会治理薄弱环节形成碎片化、事后性感知,到依托海量司法数据及内外数据的综合分析,识别社会治理中的趋势性与规律性问题,从而促使司法审判与社会治理真正达成融合互动,发挥“数助治理”的预防性功能。^⑪三是提升当事人从自身视角对司法结果的预测能力,使其对司法效果形成更为清晰、理性的认知,从而实现纠纷源头层面的法律预防。数字法院对司法数据的整合与分析,能够为当事人提供诉讼请求支持率、法律意见、诉讼成本、行动建议及案例参考等信息,助推当事人选择更为理性的纠纷解决路径,体现了数字法院以信息引导实现法律预防的功能。^⑫

(二) 数字法律预防的技术架构

通过对数字法律预防主要形态的梳理和总结,不难发现数字法律预防具有鲜明的架构化特点。它立足于认知和行为的交叉缠绕与共生演化,并通过数据驱动与概率量化形成一种风险预测与干预系统。这套以技术为底层支撑的架构,重塑着数字法律预防的基本范式。

第一,海量数据是数字法律预防的前提基础。与传统法律预防不同,数字法律预防主要建立在海量的大数据基础上。它通过对政务数据、行政处罚数据、司法判决数据、电商交易数据、金融数据、社交数据、位置数据、公共监控视频数据等进行抓取、挖掘和分析,揭示法律运行过程中的隐藏规律,从而对行为形成一种反馈机制。这种数据底座构成了数字法律预防的前提。数据底座凭借数据范围广、数据总量多、数据关联深的优势,构成了数字法律预防的数据支撑。它能够对行业和个人进行画像、支持相关法律信息检索、查询一定范围内个体画像信息等,并对特定人群进行动态监测,及时掌握相关人员的动态信息和潜在风险。

第二,人工神经网络是数字法律预防的重要工具。人工神经网络试图建立具有加工单元、激活状态、输出功能、单元间的联结模式、联结网络活动的传播规则、输入刺激使单元状态产生新水平激活的激活规则、经验影响改变联结模式的学习规则和系统控制的环境等八个基本特性的平行分布加工模型。^⑬它通过这个平行分布加工模型实现自我组织

^⑩ 参见贾宇:《论数字法院》,载《法学研究》2024年第4期,第13页。

^⑪ 参见前注^⑩,贾宇文,第15页。

^⑫ 参见张巧雨:《数助便民:守住“数字”里的民心》,载《人民法院报》2024年12月12日,第2版。

^⑬ See Geoffrey E. Hinton & James A. Anderson eds., *Parallel Models of Associative Memory*, Lawrence Erlbaum Associates, 1989, p.16-20.

和自我学习,从而具有类似生物神经系统的智慧。在数字法律预防过程中,人工神经网络将庞杂的海量数据进行非线性变化,并构建法律预防模型。例如,人工神经网络可以通过分析历史犯罪数据、社会经济因素、地理信息等多维度的数据,构建犯罪预测模型,帮助执法部门提前部署警力。

第三,算法模型是数字法律预防的核心引擎。算法模型在数字法律预防中扮演着关键角色,它是使用海量数据在人工神经网络架构上训练后得到的、参数确定的、可以用于预测或决策的系统。在实践中,用于数字法律预防的算法模型往往以逻辑回归、支持向量机、随机森林以及深度学习等算法为基础,从而使数字法律预防实现从静态合法逐渐走向动态治理。^⑭ 具体而言,相应算法模型贯穿数字法律预防的全过程。首先,在风险识别阶段,通过大数据处理整合多源数据,从多源数据中筛选出与违法违规高度相关的特征变量,再通过算法模型对运动中的数据流进行处理,对特定主体或行为的风险水平进行动态计算,以实现秒级响应。其次,在预警阶段,算法模型依据预测结果输出分级响应风险信号,形成前置性的法律预防反馈。最后,在干预阶段,数字技术将既定规则和决策流程转化为执行依据,系统根据流程自动触发拦截、提示、留痕或转人工复核,以此实现数字空间的高效化、前置性法律预防。

三、数字法律预防的规范逻辑

将数字技术运用于法律预防,不仅提升了法律预防的效果,而且推动了法律预防理念的发展。这种预防理念强调法律预防不仅是宏观结构中一种事前的、预置性的、追求给予特定事件以回应或反馈的制度安排,而且是嵌入社会运作微观过程内部,成为一种实时化、智能化和精准化的治理活动。相较于传统法律预防,数字法律预防在认识论基础、保护客体、效果机制、时序位置、执行机制等方面都有自身独特的规范逻辑。

(一) 数字法律预防的认识论基础

预防的前提是预测,而预测作为一种对自然和社会现象进行逻辑化和顺序化思考的行为具有悠久的历史,并大致经历了“神灵性预测→经验性预测→哲理性预测→实证性预测→大数据预测”这样一个漫长发展过程。^⑮ 神灵性预测主要源于人的恐惧和认知能力低下而形成的超自然偶像崇拜。它强调自然界存在一种能够影响和掌控自然界和人类事务的超自然力量,预测者能够借助天象、物象来进行直接感知。^⑯ 经验性预测是预测者基于原始直觉观测进行的经验性活动,它往往建立在对重复现象单纯的观察基础上,具有较强的偶然性和主观性。有学者认为,经验性预测的重要特征是用曾经获得的直接

^⑭ See Mengnan Du, Ninghao Liu & Xia Hu, *Techniques for Interpretable Machine Learning*, Communications of the ACM, Vol.63:68, p.68-77 (2020).

^⑮ 参见阎耀军:《社会预测学基本原理》,社会科学文献出版社2005年版,第17-34页。

^⑯ 参见卞玉琳等:《从传统占卜到科学预测:甲骨卜辞中气象文化的科学传播》,载《科技传播》2025年第2期,第1页。

经验和间接经验来比附未曾经历的未来事件。^{①⑦} 哲理性预测注重根据社会规律来对未来发展趋势加以推演,并运用理性和逻辑进行社会预测。整体上讲,传统社会的法律预防主要建立在经验性预测和哲理性预测基础上。无论是一般法律预防主义,还是特殊法律预防主义,它们对未来法律风险的认知主要是基于一种现象学和诠释学的考量,并在具体场景中根据预防主体已有的知识和主观价值判断来决定是否应当采取必要的预防措施。^{①⑧} 在具体操作过程中,传统法律预防主要采用伤害原则、比例原则等来判断法律风险是否应当被干预。这种方式往往具有较强的原则性、灵活性和模糊性,并依赖特定的个人经验,难以形成一种可推广的普遍经验。

然而,数字法律预防的认识论基础是数据驱动。数字法律预防借助计算机强大的计算能力寻找纷繁复杂的海量数据之间的相关性,并以此为基础发现法律风险的发生概率,进而实现概率预测到具体法律干预的转化。在此过程中,它不以既有的有关犯罪或违法的理论认知为起点,而是由数据计算来驱动。以犯罪预防为例,传统法律预防以犯罪学理论为基础,认为人身危险性、再犯风险与案件诸多要素之间存在同构关系。人们可以通过将这些因素指标化来预测犯罪行为发生的可能性,并采取相应措施。^{①⑨} 数字法律预防将法律预测问题转换成描述性分析,通过数据的集中趋势、离散程度、频数分布等对收集的数据进行特征分析,然后,利用预测模型、机器学习、数据挖掘等技术对当前和历史数据进行分析,并不断结合实时数据分析调整预测模型,从而最终预测法律风险的发生概率。因此,数字法律预防的认识论基础不是先验理性,而是“大数据,小定律”的数据驱动技术范式。数字法律预防主要通过人工智能依据特定场景、语境和实用需要,从海量“大数据”中,随机提取特定“小定律”,从而对行为形成一种反馈机制。^{②⑩}

(二) 数字法律预防的保护客体

法益保护是法律预防的出发点和最终目标。在初始性预防阶段,法律通过采取事前干预或规制措施,从源头上防范法益损害的发生;在继发性预防阶段,法律通过事中干预或规制措施,防止既发法益损害进一步扩大;在复发性预防阶段,法律通过事后干预或规制措施,防止法益损害的再次发生。^{②⑪} 然而,数字法律预防与传统法律预防对法益的理解有所不同。传统法律预防对于“法益”这一目标客体的理解,更近似于德国警察法意义上的“危害防止”(Gefahrenabwehr)。^{②⑫} 它指向的是已经显现的、可被感知的、对特定法益构成紧迫威胁的具体危险。因此,传统法律预防主要建立在这种具体危险的现实性、高概率性和紧迫性基础上,强调移除已然存在的具体危险源,确保其不致恶化为实然损害,从而对具体法益进行直接保护。

^{①⑦} 参见前注^{①⑤}, 阎耀军书, 第26页。

^{①⑧} 参见[美]劳伦斯·纽曼:《社会研究方法——定性和定量的取向》(第5版), 郝大海译, 中国人民大学出版社2007年版, 第79页。

^{①⑨} 参见王禄生:《论预测性司法》, 载《中国社会科学》2024年第6期, 第84页。

^{②⑩} 参见余成峰:《法律的“死亡”:人工智能时代的法律功能危机》, 载《华东政法大学学报》2018年第2期, 第9页。

^{②⑪} 参见黄文艺:《论预防型法治》, 载《法学研究》2024年第2期, 第25页。

^{②⑫} 参见蒋勇、张晓华:《算法时代预测性警务的兴起及其风险规制》, 载《公安学研究》2023年第2期, 第4页。

数字法律预防的主要保护客体是抽象风险下的法秩序。数字技术的迭代与大规模应用,使数字社会面临着前所未有的严峻风险。在自动化决策与执行的高速运作过程中,任何一个子系统偏离预设目标或遭受外部攻击,都可能导致整体秩序失控,甚至可能引发重大安全风险。这种系统性风险要求数字社会中的法益保护更加敏捷、系统和立体。因此,数字法律预防更加重视对宏观法秩序的塑造,从源头出发预防抽象风险。数字法律预防不再单纯停留于对具体危险的被动清除,而是试图通过技术手段的“滚动反馈机制”,^{②③}对法秩序的运作进行正向塑造与动态修正,将法益不断推向更为稳固和可预期的“被保障”与“可救济”状态之中,使之愈发远离潜在的侵害风险源,最终有效控制潜在侵害的性质、规模、程度与发生可能性。

数字法律预防也高度关注对公共安全价值的保障,强调从整体出发化解抽象风险。数字法律预防建立在万物皆可连接和皆可计算的系统性思维基础上。它并不是从纯粹孤立的偶发结果角度出发来看待个体法益损害,而是将个体法益与个体所处的整体安全状态紧密联系在一起。只有通过法律预防活动,对数字基础设施安全、数字技术系统安全、数据安全、信息安全、数字财产安全进行整全性法律保护,才能从更深层次保障个体法益不受侵犯,实现“整体越安全,个体越安全”的有效法律预防。

(三) 数字法律预防的效果机制

在传统社会,法律预防是作为公民自觉遵守法律的一种补充机制存在的。它强调法律的实现除了依赖于个体自觉遵守法律以外,还需要建立法律预防这种“人为抽样机制(Menschliche Stichprobe)”。该抽样机制强调违法行为的代价性,并通过有限的随机性监督与惩罚,形成对违法行为的威慑效应,从而在实践中推动守法。^{②④}在传统法律预防看来,人们之所以违反法律,是因为人们存在违法的动机,要想防止违法行为发生,就应当通过威慑这一心理强制来抑制违法的欲望。费尔巴哈认为,法律责任意味着痛苦,法律通过“心理强制”使意想犯罪或违法的人自我抑制违法的心理动机,以免违法行为发展为犯罪行为。^{②⑤}贝卡里亚认为,刑罚之所以能够起到阻止罪犯再次犯罪并规诫其他人不要重蹈覆辙的作用的原因是它具有强大的威慑性,并且国家将这种威慑视为刑罚的政治目的。^{②⑥}因此,传统社会主要依靠具有严酷性的法律惩罚措施和引导性的法律教化手段,从心理上抑制违法动机,从而实现社会法律预防的目的。

如果说传统法律预防是通过法律威慑来实现不敢违法的话,那么数字法律预防就是通过阻断行为发生来实现不能违法。德国学者蒂莫·拉德马赫认为,数字社会通过智能监控系统能够有效“读取”文字或“听取”声音,从而区分合法与非法行为,甚至可

^{②③} 参见王伯鲁:《面向未来的科技伦理治理的认识论基础剖析》,载《哲学研究》2024年第4期,第88页。

^{②④} Vgl. Timo Rademacher, Wenn neue Technologien altes Recht durchsetzen: Dürfen wir es unmöglich machen, rechtswidrig zu handeln?, JuristenZeitung 74 (2019), S. 702-710.

^{②⑤} Vgl. Paul Johann Anselm Ritter von Feuerbach, Lehrbuch des gemeinen in Deutschland gültigen peinlichen Rechts, 14. Aufl., Georg Friedrich Heyer's Verlag, 1847, S. 38-39.

^{②⑥} 参见〔意〕贝卡里亚:《论犯罪与刑罚》,黄风译,中国大百科全书出版社1993年版,第31页。

自动识别扒窃、毒品交易或袭击等事件；这些技术在事实层面能够对违法或犯罪行为进行全覆盖的识别和制裁，从而形成了一个违法或犯罪行为的“不可能性结构”，其目标就是要从物理层面阻断违法或犯罪行为的发生。^{②7}在具体实践中，这种行为阻断主要体现在以下方面：一是准入与资格前置审查。通过人脸识别、地理位置匹配等技术，对行为人进行资格审查，从而既规范行为人的行为，又将恶意人员阻隔在外。二是技术性合规强制。它主要强调产品和服务需要满足一定的技术标准来内置行为阻断功能。三是具体行为阻断。它主要是利用算法和自动化决策机制对正在进行的违法或可疑违法行为进行阻断。

（四）数字法律预防的时序位置

从本质上讲，法律预防是国家法律介入私人生活领域和社会生活领域，对自由进行限制的行为。此类介入和限制往往出于法律道德主义、伤害原则、法律家长主义和冒犯原则的考虑。这些主义和原则并非强调直接规制行为本身，而是以行为对特定法律关系的威胁程度作为国家介入的判断依据，从而凸显法律关系在法律行动正当化逻辑中的核心地位。传统法律预防遵循这种逻辑，强调只有在法律风险已经威胁到了具体法律关系，产生了立即显现、可直接量化且具有明确因果关联的损害时，才采取预防措施。在预防措施选择上，主要依靠惩戒、追责等，从而产生强大威慑来遏制不法行为的发生。

在数字社会之中，数字后设机制往往是以广域的弥散状分布深入各种涉利益活动的“毛细血管”与“神经末端”，实现“全息统御”。在此背景下，数字法律预防通过代码化、流程化和自动化等技术，嵌入数字生态的底层架构中，扩张成为一种全域覆盖的全链路活动。^{②8}它在数据收集、数据处理、内容审核、预防措施选择等环节都逐步取代人工，从而使法律预防由传统依赖人类的点状响应模式向数据驱动的系统性模式跃升。^{②9}这种技术嵌入主要包括以下方式：一是网络加密。网络加密是一个在网络传输层应用加密技术确保网络安全的过程。它对原为明文的文件或数据按某种算法进行处理，使其成为不可读的一段代码（通常称为密文）。人们只有在输入相应的密钥之后，才能读出密文的本来内容。^{③0}这种网络加密能够避免传输信息受到外界侵扰，确保信息使用者的身份真实，防止黑客盗取信息行为的发生。二是违规和违法信息筛选。它使用图像识别、语义分析等技术对收集的信息进行分类和处理，系统捕捉违规和违法信息，并提前采取有效预防措施。三是即时监控与主动防御。它通过大规模、系统化地收集、存储、处理和控制系统数据，对社会进行长期的监控，以助于预防者实时掌握特定区域的行为动向，并对违法或犯罪行为进行即时制止，达到“敏捷性治理”的目的。

以违法犯罪数字预防为例，法律预防过程大致可以分为四个环节：一是信息规制环

^{②7} Vgl. Timo Rademacher (Fn. 23), S. 702-710.

^{②8} 参见前注①，齐延平文，第87-88页。

^{②9} 参见蔡翠红：《人工智能时代的网络空间治理：技术嵌入、人类主导与人机协同》，载《学术前沿》2025年第13期，第35页。

^{③0} 参见李凌：《网络加密技术概念、加密方法以及应用》，载《中国科技信息》2005年第21期，第29页。

节。数字法律预防的信息规制由“对信息的规制”和“通过信息的规制”两部分组成。在“对信息的规制”过程中,数字技术会在连动机与意图都尚未形成的信息源头处,通过图像识别、语义分析等技术识别出复杂信息流中可能诱发、衍生、催化法益侵害的内容,从而对其进行筛除或屏蔽。在“通过信息的规制”过程中,数字技术会通过选择性推送等方式改变信息的流量与流向,进而藉由此类信息对“集体意识”或“集体无意识”施加潜移默化的影响,这本身就会在最前端产生“塑造行为逻辑”的强大规制效果。二是意图阻却环节。逸散至外部的少量信息仍可能激发法益侵害的意图。数字技术进一步在架构层面使诸多法益侵害意图不可能真正转化为法益侵害行为。例如,在金融机构高度敏感的风险控制体系中,系统自动拦截与终止可疑的交易活动。即便行为主体具有洗钱、电信诈骗等明确的法益侵害意图,也无法绕过系统屏障而实现犯罪目的。三是行为介入环节。数字法律预防借助系统化的即时监控系统、网络巡查、网络监视等筛选软件或利用浏览器的现有内置功能来全面地实时掌握特定区域的行为动向,并对违法或犯罪行为进行即时制止,更好实现敏捷介入。四是嗣后预防环节。数字法律预防更加注重在单个法益侵害行为“案结事了”之后预防“二次再犯”“模仿犯”的产生,也更为注重控制社会衍生影响。这使得数字法律预防形成了一个“内化循环”的完整闭合空间,从而对潜在的、实然的、嗣后的法益侵害活动进行“全息统御”。

(五) 数字法律预防的执行机制

法律预防的核心是通过事前、事中、事后的干预或规制措施,防止法益损害的发生。在传统社会,这些干预或规制措施主要是由人工来进行的。无论是法律风险的研判,还是干预或规制措施的选择,都由预防者根据具体案情、法律条文和社会影响,凭借个人经验作出。例如,社区居民依靠生活常识发现并报告治安隐患,企业管理者依据行业惯例完善内部合规制度,家长则通过言传身教预防未成年人违法犯罪。这对于形成群防群治的社会治理格局具有重要意义,但是这种人工主导的法律预防模式往往存在主观性强、覆盖面窄、预见性不足等局限,难以应对日益隐蔽和专业的法律风险。

数字法律预防的执行机制具有鲜明的人机协同特征。人机协同是指,通过集成人类智能与人工智能,形成合理有效的交互协调机制,其核心在于既要充分发挥人类在复杂决策、创造性思维和情境理解上的优势,又要利用人工智能在数据处理、模式识别和执行上的优势,共同解决复杂问题。在实践中,人机协同表现为互补人机协调机制、混合人机协调机制和多人多机协调机制等。^③在法律预防过程中,人类在设定法律目标、伦理准则和监管政策的前提下,广泛深入地运用机器学习来对海量数据进行计算,寻找和挖掘数据与法律风险之间的复杂关联。这种人机协同既可以充分发挥人类在复杂决策中的创造性思维与情境化理解能力,又可以深入挖掘数据与法律风险之间的复杂关联,在数据处理、模式识别和具体执行上展现优势。

具体来讲,数字法律预防中的人机协同主要体现在以下方面:一是法律预防任务的

^③ 参见吴信东等:《人机协同》,科学出版社2022年版,第7页。

确定。人工将法律预防的宏观目标分解为具体的任务板块,并根据人机能力的匹配程度制定具体的人机协同模式。^{③②}二是法律风险的识别。人工智能通过对海量数据的计算,识别出行为的异常模式,提出相关量化证据,并向相关人员发出法律风险提示。三是人工调查与核实。人工对精准锁定的高风险法律行为进行评估与核查,并对某些行为进行复杂情感理解和作出伦理道德判断,防止算法歧视与算法偏见。四是将经审查后的法律预防活动以算法化的方式固定下来,嵌入日常运转的数字后设机制系统之中。一旦法律预防嵌入数字后设机制系统,便获得了一种稳定、长效、重心直接下沉至基层生活实践的内驱力,从而成为一种常态化、自动化的系统性机制。

四、数字法律预防与法律价值的张力

数字法律预防是数字技术赋能法治建设的一个重要方面。它通过大数据、人工智能神经网络和机器学习等技术,实时监测社会经济运行中的异常行为,及时采取应对措施,从而提升了法律预防的即时性和精准性,并日趋形成一种预防型法治形态。数字法律预防通过技术手段提前阻断安全风险,从源头保障数字空间的基本秩序与安全;凭借强大的数据基础和算力优势,纠正潜在不公,精准识别社会风险,提升社会治理效率和效能,促进法律实质正义实现;借助自动化决策机制和透明化机制,减少人为干预偏差,增强社会治理的公信力,助推法律程序正义实现。因此,从整体上讲,数字法律预防契合现代法律价值,符合现代法治精神。然而,受数字法律预防底层结构的影响,数字法律预防不可避免地会与部分现代法律价值存在一定的张力,甚至冲突。

(一) 数字法律预防与安全价值的张力

数字法律预防是运用数字技术进行高清治理的一种方式 and 手段。它将现实世界的活动以数字痕迹的方式迁移至网络空间,用计算机语言将社会事实转变为可以随同信息流一起传递的代码。在此过程中,国家借助指数级增长的数据量和强大的计算能力在更加微观的尺度上捕捉社会事实,逐渐形塑一个具备强大社会清晰画像能力的“高清国家”。社会事实和公民个体最大限度地被纳入国家视野,变为国家眼中的“透明体”。^{③③}国家可以通过数字法律预防对社会风险进行及时监测、分析和解决,并追求一种近乎绝对的安全观。数字法律预防在促进国家进行精准防控和穿透式防控的同时,极有可能带来安全泛化,从而背离现代法律安全价值的基本要求。

安全价值是现代法律追求的一个基本价值。它主要包括恐吓的免受、匮乏的免除、内心的安宁、社会秩序的稳定、公共安全的维护、基本权利的保障、信任关系的建立等基本内涵。^{③④}在具体实践中,安全价值具有以下基本特点:第一,安全价值是总体性的。安全价值不是孤立存在的,它以系统论为基础,体现着某一集合中同质观察单位或矛盾各

^{③②} 参见谭玉珊等:《一种人机协同的技术预测方法研究》,载《情报理论与实践》2021年第9期,第163-164页。

^{③③} 参见吕俊延、刘隼飞:《国家的“视力”:技术革命与国家信息能力建构》,载《政治学研究》2023年第5期,第107页。

^{③④} 参见[美]亚伯拉罕·马斯洛:《动机与人格》(第3版),许金声等译,中国人民大学出版社2013年版,第18页。

个侧面之间复杂的关系。因此,安全价值强调通盘考虑各种安全要素,从系统性、整体性和协同性等多维度出发来处理发展和安全、外部和内部、风险和机遇、维权和维稳等重大关系。^⑤第二,安全价值是相对的。安全价值是在秩序与活力之间的一种动态平衡。它强调对国家生存和可持续发展的维护,但不要求完全清除潜在威胁,不是对安全泛化,更不是追求绝对安全。第三,安全价值是有代价的。在安全价值的实现过程中,国家除了需要履行尊重的消极义务外,还需要履行保护和促进的积极义务。这些义务的履行需要支付成本,并受到边际产量递减规律的影响。弗朗西斯科·冈萨雷斯认为,安全并不等于完全消除非法暴力或违法行为,因为实现这一目标可能需要消耗大量资源,而这种不计成本的资源消耗与任由暴力或违法行为消耗等量资源没有本质区别。^⑥

数字法律预防利用技术结构阻却违法行为发生,形成一个违法行为的“不可能性结构”。这很有可能通过严格的、预先设定的规则来追求一种绝对安全,引发安全价值的异化。首先,数字法律预防容易将社会状态简化为社会问题。它借助现代信息技术手段,将离散的社会行为变为网络节点,并将社会的维度和可能性进行层层压缩,直至其变为一个面向行动的二元编码,从而实现社会状态向数据的转化。在数据驱动的经验主义认识论和计算主义的方法论指引下,数字技术将社会状态的复杂性简化为社会问题,并按照问题严峻程度区分为个例、风险、危险和危机,据此为舆情、经济、社会等各项数据设定警报装置。这在一定程度上遮蔽了社会状态中其他因素的意义,从而难以从系统上和整体上看待安全问题。^⑦其次,数字法律预防容易忽视社会模糊性治理的重要意义。模糊性治理是一种利用原则、标准和弹性空间来应对复杂社会冲突的治理方式。这种模糊性既是社会的防火墙,构成了阻止国家权力扩张的屏障;又是社会事实维系原生态的隔离带,构成了滋生社会和个人自主空间的温床。数字法律预防既让国家将原本不应由其掌握的社会事实和信息掌握在手,又进一步压缩了原则、标准和制度弹性的存在空间。通过技术手段实现的全景监控,容易放大安全威胁,形成“寒蝉效应”,不利于激发社会活力。最后,数字法律预防容易忽视安全价值实现中的成本考量。数字法律预防因其在安全价值实现方面具有高度的可视性、敏捷性和高效性等优势而备受青睐。这容易让人忽视安全价值实现的成本,甚至为了实现绝对安全而不计成本。

(二) 数字法律预防与实质正义的张力

数字法律预防作为一种新的法律运行理念,强调法律应当由事后追责的裁判者角色向事前设计和部署安全架构的工程师角色转变。这也就意味着数字法律预防要求法律功能从社会修复转向社会规训。这种理念在大力推进安全价值实现过程中可能会同法律实体正义相碰撞,甚至冲突。

第一,数字法律预防秉持的数据驱动经验主义与作为实质正义认识论基础的实践主

^⑤ 参见中华人民共和国国务院办公厅:《新时代的中国国家安全(2025年5月)》,人民出版社2025年版,第11-12页。

^⑥ See Francisco M. Gonzalez, *Effective Property Rights, Conflict and Growth*, *Journal of Economic Theory*, Vol.137:127, p.127-139 (2007).

^⑦ 参见彭亚平:《照看社会:技术治理的思想素描》,载《社会学研究》2020年第6期,第228页。

义存在张力与冲突。数字法律预防最直接的表现形式就是建立一套基于数据驱动的风险预测与干预系统。这个系统主要遵循“数据—知识—运用”的技术逻辑,强调通过现代信息技术来感知现实世界,并将这些感知转化为数据来进行观察、实验和归纳推理,从而形成人们关于现实世界的一套普遍性知识体系。然而,实质正义往往建立在实践主义认识论基础上。在实践主义看来,实践就是人的存在,人们应当从实践角度出发来理解事实和现实。脱离人这一主体,只是从客体的或者直观形式去理解事实和现实就会犯旧唯物主义的错误。^{③⑧} 实质正义也应当从人的实践出发来理解,强调理性与感性的有机结合。数据驱动经验主义虽然强调了数据来源于现实法律生活,但后续的处理往往不能对人的情感因素进行有效回应,可能背离实践主义要求,不利于实质正义的实现。

第二,数字法律预防自身技术的缺陷影响实质正义的实现。数据、算法和算力是数字法律预防的核心要素。数据不仅是信息的载体,而且是智能化与数字化的基础。它既是数字法律预防的逻辑起点,也是数字法律预防的驱动力。算法是数据挖掘的重要引擎。算力是数字法律预防的基本支撑。然而,在现有技术条件下,数据驱动方法过度依赖历史数据和算法模型,容易出现数据质量不高、算法歧视和算力不足等问题。这可能导致算法过度放大法律风险、法律预测模型滞后社会发展、数字法律预防协同性不足等直接影响实质正义实现问题的出现。以美国的阿勒格尼县算法为例,该算法通过一种名为AFST的风险评分设计系统来预防虐待或忽视儿童的行为。当判断哪些家庭应当被报告至儿童保护热线或将儿童从家中带走时,AFST只是假设儿童伤害的指标,并不能与实际虐待儿童的现实行为画等号。由于掺入大量非相关的经济信息因素,以至于没有房子、没有食物的穷人对自己孩子的照管行为通常被理解为“虐待”,不仅没有保证实质正义目标的实现,反而还会把孩子们带入更高的现实风险当中。^{③⑨}

第三,数字法律预防技术研发的非中立性与实质正义存在张力与矛盾。一方面,数字技术是数字法律预防的重要依托,而数字技术的研发和设计往往要受算法规则设计师、程序员和信息科技公司对数据运用场景、目标和价值认知的影响。^{④⑩} 这在一定程度上造成了数字法律预防技术的非中立性。另一方面,数字法律预防技术的研发、设计和部署都是高度技术性的工作,需要成熟的算法技术和具有应用前景的数字网络平台,这在客观上要求政府与数字企业进行合作,从而为数字资本介入提供了契机。在资本运作逻辑支配下,数字企业和平台往往基于自身专业优势将自我偏好和自我利益植入数字系统中,将数字科技活动逐步转变为实现资本提升与资本积累整体效率的某项专门事业。^{④⑪} 这种剩余价值的追求势必会引起数字技术异化,并与法律的实体正义产生张力和矛盾。

^{③⑧} 参见《马克思恩格斯选集》(第1卷),人民出版社2012年版,第137页。

^{③⑨} 参见[美]弗吉尼亚·尤班克斯:《自动不平等——高科技如何锁定、管制和惩罚穷人》,李明倩译,商务印书馆2021年版,第108-147页。

^{④⑩} 参见胡炯、王裕根:《深刻把握数字社会的正义感知》,载《中国社会科学报》2025年9月17日,第A6版。

^{④⑪} 参见熊小果:《数字利维坦与数字异托邦——数字时代人生存之现代性困境的哲学探析》,载《武汉科技大学学报(社会科学版)》2021年第3期,第328页。

（三）数字法律预防与程序正义的张力

程序正义是独立于实质正义的一种基本价值。它主要通过分工、抑制、导向、缓解、感染等方式来保证法律的有效运行。参与性、公开性、中立性、信息对称性等是程序正义的基本要素。这些基本要素在具体实践中主要通过告知同意规则、职务权限规则、证据规则等表现出来。然而,数字法律预防因其高度的主动性、标准性、技术性往往与这些基本规则存在不同程度的张力或冲突。

第一,数字法律预防与告知同意规则的张力。告知同意规则能够从程序上赋予行政机关处理公民合法权益的正当性。它的价值预设是:个人是自我利益的最好判断者,个人最有资格来判定哪些结果有利、哪些结果有害,并自愿承担由此带来的后果。罗杰·布朗斯沃德认为,个人有时基于特殊考虑,愿意作出损害自己利益的行为,政府通过告知同意能够获得损害个人利益的授权。^④从本质上讲,数字法律预防行为是国家相关部门依据算力和算法处理数据,进行法律自动化实施和精准防控的行为。为了有效实现法律预防,数字法律预防主体会扩展数据集的范围,并有可能在没有征得信息主体同意的情况下收集其身份、通讯、健康、行为轨迹、经济状况等个人信息,甚至是敏感信息和隐私信息。究其原因,主要有以下方面:其一,全面征集信息主体同意必然会带来数字法律预防高额的成本。数字法律预防中的告知同意成本除了开发、部署和维护用于获取、记录、管理和验证同意的系统需要持续的IT投入等直接成本外,还包括频繁、复杂的同意弹窗带来的“同意疲劳”等间接成本。其二,数字法律预防场景的复杂性和开放性使得告知同意变为不可能。数字法律预防是在公共空间展开的,人员具有高度流动性和不特定性,信息认证的难度较大。在客观上,受技术条件和资金投入的影响,并不是每个场景都能够建立相应的告知同意系统。其三,数字法律预防极大地消减了告知同意规则的重要性。数字法律预防与告知同意规则的冲突并非仅源于“全面征集同意”的技术成本和复杂场景的操作难题。更为根本的原因在于,数字法律预防往往发生于国家公权力主导的场景,其合法性基础多来自法律授权和公共利益,而非个体的事前同意和授权。这极大地消减了告知同意规则在数字法律预防中的功能实效。

第二,数字法律预防与职务权限规则的张力。职务权限规则是国家行政机关作出行政法律行为必须遵守的一项重要程序性规则。它主要包括职权法定、职权独立行使、职权分工配合、权力与责任相统一等基本内容。随着算法技术突破外在时空条件的物理限制和内在智识水平的生理局限,数字法律预防在提升治理效能的同时潜藏着权力空转的隐忧,从而使职权行使突破职务权限规则的限制。^⑤其一,就职权法定而言,数字技术超强的穿透性、联结性和可视化容易激发行政机关调查和追究责任的欲望,从而导致扩张行政权力,突破职权法定原则。其二,就职权独立行使而言,按照程序正义的要求,是否采取法律预防和采取何种法律预防应当由法律预防主体来决定。然而,在实践中,数字

^④ See Roger Brownsword, *Consent in Data Protection Law: Privacy, Fair Processing and Confidentiality*, in Serge Gutwirths et al. eds., *Reinventing Data Protection?*, Springer, 2009, p.83-110.

^⑤ 参见展鹏贺:《论数字行政正当程序构造》,载《中国法学》2025年第5期,第107-108页。

技术凭借高度的专业性、技术性、封闭性和系统性,生成了一种技术权力。这种技术权力迫使法律预防主体接受数字技术生成的结论。其三,就职权分工配合而言,突破层级性治理和多属性治理、推行信息共享和社会共治,是开展数字法律预防的关键。但这势必会打破传统的部门边界,不利于国家机关运行效率的提高和公共服务质量的提升。其四,就权力与责任相统一而言,数字法律预防会进一步增强“数据控制效应”,它借助数据架构与算法规则,通过数据集中、平台规则设定、接口权限控制等方式,在组织之间形成事实上的权力再配置,并带来权力过度集中、权责脱节和问责失灵等风险。^{④⑤}

第三,数字法律预防与证据规则的张力。数字法律预防是着眼于法益损害预防,通过事先设计出一整套预防性义务和责任,引导各方主体采取预防性行为和措施的行为。^{④⑥}运用数字技术作出判断和采取相应预防措施理应有相应的证据作为支撑。然而,数字法律预防的算法逻辑和自动化决策机制可能会与证据规则存在张力与矛盾。其一,数字法律预防通过行为数据推测主观意图,这导致证据与待证事实之间的相关性难以证成。从程序正义来看,作为决策依据的证据应当与待证事实存在直接关联性。然而,这种直接关联性不是哲学意义上普遍的抽象联系意义上的概念,而是特殊的具体的概念。^{④⑥}它虽然代表着事物发生的概率性,但绝不是简单地用统计学上的高度关联性来当作法律上的确定性。从数字法律预防的运作逻辑看,它往往根据行为人的数据来预测其行为意图,并采取相应的干预措施。算法通过数据预测出来的行为意图只是一个推测性证据,并非法定证据,而且从这一推测性证据并不能直接得出某个特定主体一定会采取相应行为的结论。其二,算法决策的难以解释性极有可能导致法律预防行为难以被有效质证。国家在采用监测、评估、控制等手段承担法律风险预防义务时,很有可能直接克减或限制公民的权利。行政相对人在承担预防性义务时,有权要求行政主体作出有效解释。然而,算法决策高度的技术性和专业性增加了解释和理解的难度,直接影响行政相对人质证的效果。其三,自动化决策容易导致证据难以被妥善固定和保全。在数字法律预防过程中,系统会自动执行一些命令,例如自动化屏蔽信息、清除系统日志、冻结可疑账户等。这种自动化处理很有可能破坏证据的原始状态,增加后续取证难度。其四,迭代算法可能导致难以排除非法证据。数字法律预防模型一般都采取迭代算法。在此过程中,它极有可能把本身错误的、不完整的或不真实的数据以及违法取得的数据代入下一轮运算中,并不断循环下去,违法取得的数据难以从系统运算中剔除。

五、数字法律预防的制度构建

面对数字法律预防与现代法律追求的安全、实质正义和程序正义等价值之间存在的张力和碰撞,应当在充分理解数字法律预防底层结构和规范逻辑的基础上,加强数字法

^{④④} 参见王锡锌:《数字行政与行政职权配置的变革逻辑》,载《环球法律评论》2025年第5期,第25页。

^{④⑤} 参见黄文艺:《预防型法治的变革效应》,载《北京日报》2024年7月15日,第10版。

^{④⑥} 参见龙宗智:《“大证据学”的建构及其学理》,载《法学研究》2006年第5期,第85页。

律预防的制度构建。构建数字法律预防制度,应在法律目的层面,对数字技术运用于法律预防进行约束,捍卫现代法律的基本价值;应在法律规范层面,从实体和程序两个维度出发,通过科学配置权利与义务、建立全链条调控机制、加强数字技术的规制等方式减轻或化解数字法律预防与现代法律价值之间的张力和冲突。具体而言,可以沿着“法律目的一法律关系—预防行为—技术规制”这一脉络来构建数字法律预防制度。

(一) 数字法律预防的法律目的

从本质上讲,数字法律预防是国家凭借强大数字技术,不断强化以认证能力、信息汲取能力和信息处理能力为核心的国家信息能力,并对社会进行一种以实时化和智能化为主要特征的精确性治理。这种精确性治理推动了法律预防从“经验驱动”转向“数据驱动”,从“模糊感知”转向“精准洞察”,并极大提升了法律治理效能,维护了社会的安定和稳定。但是,数字法律预防依托的数字技术在为法律预防赋能的同时,也有可能借助其超强的流动性、脱域性和时间结构的无序性而实现自我的重新定义和组合,从而生成一种“技术利维坦”。^{①7}因此,数字法律预防应当强化法律目的约束。

首先,数字法律预防应当遵循以保障人的基本权利和尊严为核心价值的法律哲学观。数字法律预防依靠算法预测、大数据建模来实现前置的风险干预。数字法律预防的精准画像、即时响应、自动决策等技术特性,使预防行为冲破时空的束缚,但也带来了数字时代特有的尊严侵害风险,即算法黑箱造成的决策歧视、预测性监控引发的隐私过度侵蚀、数据画像造成的人格碎片化。^{①8}《个人信息保护法》第24条规定自动化决策“应当保证决策的透明度和结果公平、公正”,直接回应数字法律预防的算法尊严侵害问题;第28条对敏感个人信息的严格限制,为数字法律预防的数据收集划定边界。数字法律预防要把这些规范嵌入技术架构之中,采用算法透明化、数据最小化、决策可追溯等手段,将权利和尊严保障从事后救济转向事前预防。

其次,数字法律预防应当遵循国家积极作为与权力依法运行相结合的法律政治观。数字法律预防的核心是利用数字技术实现前置性风险防控。一方面,数字风险的跨域性、隐蔽性、传播性远超传统风险,单靠市场自治或者个人防御无法解决,必须依靠国家主动构建数字法律预防体系。《网络安全法》第6条明确规定了国家对网络安全风险的监测和防御义务;《数据安全法》第22条也设立了国家数据安全工作协调机制,均体现出国家积极作为的定位,为数字法律预防提供了制度保障。另一方面,数字法律预防赋予了权力更强的技术干预能力。大数据监控、自动化拦截等手段如果不加以约束,很容易发生异化。为此,《个人信息保护法》第13条严格限制个人信息处理者处理个人信息的法定情形,保证数字法律预防的数据收集符合权利保障的要求。《互联网信息服务算法推荐管理规定》第24条规定了算法备案制度,使得数字法律预防的核心工具可以被追溯。

^{①7} See Michel Callon, *Society in the Making: The Study of Technology as a Tool for Sociological Analysis*, in Wiebe E. Bijker, Thomas P. Hughes & Trevor J. Pinch eds., *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, The MIT Press, 1987, p.83-91.

^{①8} 参见郑玉双:《人工智能与人的尊严的法理建构》,载《浙江学刊》2024年第6期,第37-40页。

最后,数字法律预防应当遵循以人为本、技术向善的法律伦理观。数字法律预防以算法预测、大数据画像为手段,这种“未发先防”的特点容易产生特有的伦理风险。预测性监控可能会超出合理限度,过度收集行为数据压缩了个体自主的空间,算法主导的预防决策可能缺少伦理校准,把个体标签化、工具化。这是数字法律预防不同于传统法律预防的伦理难题。中国已经有针对性地构建起伦理约束体系。《生成式人工智能服务管理暂行办法》第5条规定,鼓励生成式人工智能技术在各行业、各领域的创新应用,生成积极健康、向上向善的优质内容,探索优化应用场景,构建应用生态体系。《互联网信息服务算法推荐管理规定》第17条赋予用户选择不针对其个人特征的算法推荐服务的权利,防止算法对个人的过度支配。数字法律预防要将这些伦理要求嵌入技术架构之中,使技术始终成为捍卫人尊严、保障自由的工具,实现数字法律预防技术逻辑与伦理价值的统一。

(二) 数字法律预防关系中的权利义务配置

国家预防权是国家通过法律、行政等手段,对可能引发严重社会危害的突发事件进行预防、监测、预警和应对的权力。在数字时代,这种国家预防权主要包括数据信息收集权、风险分析评估权、行为监管与干预权、预警与信息披露权等内容。数据信息收集权是指,国家在法定程序和目的范围内,为维护公共安全所进行的非针对性、大规模的数据采集或者向平台、企业等数据控制者或处理者调取为进行风险分析所必需的数据的权力。风险分析评估权是指,预防主体利用算法模型对收集到的数据进行分析,以识别、评估和划分风险等级,并对涉及数字社会的国家安全、公共安全领域及时进行合规风险画像的权力。^{④⑨}行为监管与干预权是指,预防主体对涉及国家安全、公共安全等风险事项,根据风险等级不同采取不同强度干涉的权力。这些干预主要包括实时数据监控、算法识别预谋行为、自动化封锁、数据画像、社会信用评级等。预警与信息披露权主要是指,对于具有广泛影响的系统性风险,政府向社会或特定群体发布预警信息,防止风险扩散的权力。^{⑤⑩}

当然,国家的数字法律预防权也应当遵循一定的限度。具体来讲,这种限度主要体现在以下方面:第一,国家不得运用数字技术对思想言论进行预测性惩罚。预防的对象应是具有客观紧迫危险的行为,而非思想。绝对禁止仅基于个人的言论倾向、社交关系、浏览记录等数据,通过算法预测其未来的犯罪可能性,并通过施加干预措施对其造成实质性不利后果。第二,国家不得运用数字技术对涉及人格尊严与自治的领域进行法律预防。法律应当禁止基于基因信息的社会性预判、禁止对完全私主体领域的介入,家庭内部、私人住宅内无涉公共利益的行为不应成为预防性监控的对象。第三,国家不得完全运用数字技术对公民作出重大权益处分。在自动化决策时,禁止在无人工介入、无合理解释、无有效救济渠道的情况下,仅凭自动化决策对公民作出重大权益处分。

^{④⑨} 参见王贵松:《风险行政的组织法构造》,载《法商研究》2016年第6期,第13页。

^{⑤⑩} 参见曾智洪、王梓安:《数字监督:大数据时代权力监督体系的一种新形态》,载《电子政务》2021年第12期,第59页。

在数字法律预防过程中,公民既享有一定的权利,也需要履行一定的义务。就权利而言,公民除了享有数字身份权、隐私权、肖像权、数字安全权等实体性权利外,还享有知情与透明化权利、异议与纠错的权利、救济与赔偿的权利等程序性权利。为公民设定法律义务本质上属于对权利的限制或干预,必须遵循法律保留原则。公民的数字法律预防义务主要包括:一是数据提供义务。在特定、法定的高风险领域,公民有义务提供与风险直接相关的、必要的个人信息。二是行为配合义务。公民应配合必要性检查,对于基于合理怀疑的、非侵入性的、短暂的预防性措施(如安检、实名认证),公民负有合理的容忍义务。三是主动纠错义务。在网络安全、数据安全等领域,公民可以要求特定主体(如关键信息基础设施运营者)履行主动设置防护措施、及时修补漏洞等义务。

(三) 数字法律预防行为的调控机制

数字法律预防行为构成了从数字技术部署到信息处理,再到干预决策这样一个递进式逻辑闭环。每个环节都有可能违背数字法律预防的目的,因此,需要构建一套全链条的数字法律预防行为的调控机制。

第一,建立数字法律预防系统部署前的整体评估机制。从通用工程的层面来看,数字法律预防系统往往具有一经封包部署,后续就难以调整修正的技术特性,而且广泛链接公安、银行、电信等诸多重要的API端口,处于“牵一发而动全身”的信息交换枢纽位置。一方面,应当对数字法律预防系统部署的必要性进行评估。可以根据比例原则对风险发生的可能性以及危害是否达到需要系统性法律干预的阈值进行预判,并对拟部署的系统能否直接或有效地阻断该风险的发生进行判断。另一方面,应当采取“成本—收益”分析方法对数字法律预防系统部署需要支出的直接成本、间接成本和可以取得的社会收益进行考量,评估数字法律预防的经济效益。

第二,建立数字法律预防的有序退出机制。现实生活中,可能因保护的法益不再具有被侵害可能性、技术迭代更新、组织目标调整等因素,既有的数字法律预防没有继续存在的必要性。然而,前期数字法律预防积累了大量数据,布置了大量数字设备,极有可能存在安全风险。因此,建立数字法律预防的有序退出机制就显得尤为重要。首先,应当擦除与销毁本地服务器与云端存储的数据,防止数据残留引发隐私泄露或不当利用。其次,应当同步切断其与公安、交通、通信等部门的数据交换接口,注销相关的访问权限与密钥,防止废弃系统因接口未关闭而沦为数据泄露的“后门”。再次,应当对不再使用的前端感知设备及时切断电源、网络连接或予以拆除,防止其成为“僵尸节点”。最后,应当建立退出过程透明化的公示与反馈机制。相关主体应向社会公开退出原因、涉及的数据范围、数据销毁的处理结果以及相关设备的处置方案,保障公众的知情权。

第三,建立数字法律预防中的信息处理机制。数字法律预防由海量数据驱动,底层信息处理机制直接影响数字法律预防的正当性和科学性。建立合理的信息处理机制对于提升数字法律预防质量具有重要意义。首先,明确将数字法律预防系统采集的信息定性为情报线索。数字法律预防系统是基于相关性计算而作出的可能性推测。这种推测在本质上有别于基于证据因果性的社会真实。应当将其定性为情报线索,而不能被视为

法律事实。^{⑤①}其次,应当建立基于风险等级的跨部门数据调用审查机制,并根据数据敏感度与预防事项的风险等级,建立分级审查与留痕规则。对于不针对特定相对人的一般性数据,其调用可采用备案制,以形式审查为主;对于涉及公民隐私、商业秘密等高敏感数据的跨部门调用,则必须经过严格的权限审批与合规性审查。最后,应当针对部分紧急信息建立特别的快速调处机制。对确有必要、明显轻微、频繁发动且即时性较强的干预所需要的信息流,可以有限度地引入概括性的知情同意原则。该原则通过事前向社会公众公开清晰的介入规则与算法逻辑,在确保相对人知情权与算法透明度的基础上,允许系统对该类紧急信息直接进行自动化识别与处置,同时又为其预留相关的救济程序。^{⑤②}

第四,建立数字法律预防中的“人在回路”机制。“人在回路”要求通过制度性安排将人类判断嵌入具体决策回路,使机器预测结果必须经由人类的实质审查、修正或确认,方可产生具有法律意义的效果,从而实现“有意义的人类控制”。^{⑤③}长期以来,“人在回路”被视为修正算法错误、应对系统性风险、推动技术性程序正义的标准性解决方案,并已被不同程度地吸纳进人工智能治理的相关立法与政策框架之中。^{⑤④}因此,在数字法律预防的制度设计中,有必要将“人在回路”确立为数字法律预防行为的一种调控机制。首先,应当建立关键节点人工确认机制,确保数字法律预防中“人在回路”得以落实。关键节点是指数字法律预防行为可能对个人权利义务产生实质性不利影响,或者显著提升干预强度的决策阶段。在上述节点上,有关算法决策仅提供风险评估结论或行动建议,而不得直接触发具有法律效果的预防行为。其次,参照《个人信息保护法》第24条关于自动化决策拒绝权的规定,在数字法律预防中,应当明确人工介入的强制触发机制。对于通过自动化分析作出的预防性判断,若可能对个人权益产生重大影响,则不得仅依赖算法输出直接转化为具有法律效果的预防措施,而应当为当事人提供请求人工审查的通道。最后,建立人工复核与责任记录机制,防止高度自动化的数字法律预防弱化甚至消解有关主体的责任意识。数字法律预防应用的算法或自动化系统并不具备承担法律责任的主体资格,相关决策的最终责任仍应由参与决策并行使判断权的人类主体承担。^{⑤⑤}为避免形成责任真空,需要在制度上要求数字法律预防中的人工复核与责任记录同步运行,并确保相关记录具备可追溯性,以便于事后监督、合法性审查与责任认定。

(四) 数字法律预防技术的规制

由于信息收集的不完整、案例统计模型的代表性不足、技术过程的开放性不够等因

^{⑤①} 参见李训虎:《侦查情报化之批判》,载《法学》2024年第7期,第137页。

^{⑤②} 参见林喜芬、张一武:《电信网络诈骗案件中紧急止付制度的检视与完善》,载《云南社会科学》2023年第3期,第130页。

^{⑤③} 参见陈悦:《论自动化行政中算法决策风险的“人在回路”治理模式》,载《行政法学研究》2024年第4期,第37页。

^{⑤④} See Therese Enarsson, Lena Enqvist & Markus Naarttijärvi, *Approaching the Human in the Loop-Legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three Contexts*, Information & Communications Technology Law, Vol.31:123, p.123-124 (2022).

^{⑤⑤} 参见王苑:《完全自动化决策拒绝权之正当性及其实现路径——以〈个人信息保护法〉第24条第3款为中心》,载《法学家》2022年第5期,第77页。

素,会削弱数字技术在法律预防应用中应有的客观性和中立性。数字法律预防不但需要从具体运用层面进行法律归化,还需要对技术本身进行规制。

第一,建立数字法律预防技术研发的伦理审查机制。数字法律预防技术研发是数字法律预防的前提。它具有应用场景丰富、涉及人群规模庞大、对公民权利义务具有直接影响等特点,应当遵循严格的伦理审查标准。数字法律预防技术研发伦理审查的核心是以人的基本权利和尊严保护为底线,通过对数字法律预防技术可能引致的权利侵害风险进行识别与合理性判断,进而以非确定性的科技伦理规范促使技术在源头即与“技术向善”目标保持一致。需要强化科技伦理审查管理责任主体的职责意识,重点加强审查数据收集、存储、加工、使用等处理活动和研究开发数据新技术活动是否符合国家相关规定,以及算法、模型和系统的设计、实现、应用等是否遵守公平、公正、透明、可靠、可控等原则。

第二,建立数字法律预防技术应用的准入机制。运用于法律预防的数字技术应当严格符合特定的技术标准、安全标准和伦理标准。不同于一般意义上的数字技术应用,数字法律预防的关键特征在于其前置性介入风险治理,因此,准入机制应当对进入法律预防体系的技术进行前置规制。在具体实践中,数字技术的运用应当符合《网络安全法》《新一代人工智能伦理规范》《人工智能生成合成内容标识办法》《网络安全技术 人工智能生成合成内容标识方法》等相关规定,并通过构建标准化、可验证的技术披露机制,实质确立数字法律预防技术的前置程序性条件。这主要包括审查数字预防技术开发主体和服务主体是否具备相应从业资格,是否建立完善的数据治理机制、透明度治理机制、风险管理机制、质量监测机制、使用评估机制、强制性的歧视检测机制、应急机制等内容。

第三,建立数字法律预防技术应用的机制。数字法律预防不仅是行政权的一种运行模式,而且是一项涉及众多主体的复杂的技术工程。合理确定法律预防中数字技术工程责任具有重要意义。^⑤当数字技术运用于法律预防不当并给社会或个人造成严重损害时,首先需要区分是数字法律预防系统自身的问题,还是法律预防主体使用的问题。倘若是数字法律预防系统自身的问题,需要进一步根据数据安全、算法合规、个人信息保护、技术伦理等具体领域来确定数字技术研发者和平台应当承担的相关责任。在此过程中,也要看到数字技术自身发展的不足,将因技术自身不完善所产生的原生风险和因人为操作、管理或恶意利用导致的次生风险明确区分开来。

六、结 语

数字法律预防是数字技术融入法律预防、防范法律风险发生的一种综合性预防机制。它以数据驱动的计算主义为方法论基础,并充分利用计算工具诊断法律问题,借助

^⑤ 参见吴晓江:《技术的特性、欲望、评价和预防性伦理——德国技术哲学学者波塞尔、李文潮演讲述评》,载《世界科学》2004年第11期,第39页。

计算程序形式确立分析法律问题的基本框架,通过计算技术形成技术和法律的相互反馈机制,对数据集中混杂变量的相关性进行归纳总结,计算法律风险发生的概率,促使相关部门或机关采取相应的预防措施。^{⑤7} 这种技术与法律治理的融合,极大地提升了法律预防的精准性和即时性。然而,在具体实践中,倘若数字法律预防过分运用,不仅会消耗大量的公共资源,而且容易扩张权力干预社会的范围、限缩个人的自治空间、降低社会的发展活力。因此,需要充分认识到数字法律预防的限度,并将数字法律预防与法益损害的事后救济机制有机结合,从而形成“前瞻防御”与“有效善后”的动态治理体系。

Abstract: Digital legal prevention refers to a comprehensive preventive mechanism that operates within digital environments, such as cyberspace, data-driven applications, and artificial intelligence systems, by employing systematic and forward-looking digital technologies to identify, assess, and avert potential legal risks in advance, thereby reducing the occurrence of unlawful conduct and preventing infringements of rights and interests. Digital legal prevention is characterized by a strong degree of structuralization. Data-driven approaches are the epistemological foundation of digital legal prevention. Legal order and public safety under abstract risks constitute the primary objects of protection for digital legal prevention. Behavioral blocking is the main effective mechanism of digital legal prevention. ‘Holographic governance’ represents the temporal position of digital legal prevention, while human-machine collaboration is the defining characteristic of its implementation mechanism. Digital legal prevention is consistent with modern legal values. However, due to its underlying structural foundations, digital legal prevention inevitably gives rise to a certain degree of tension or conflict with partial values pursued by modern legal systems. Constructing a system of digital legal prevention along the analytical trajectory of ‘legal purposes–legal relationships–preventive measures–technological regulation’ is of significant importance for alleviating or resolving the tensions or conflicts between digital legal prevention and the fundamental values of modern law.

(责任编辑:赵毅宇)

^{⑤7} See Rediet Abebe et al., *Roles for Computing in Social Change*, at <https://dl.acm.org/doi/10.1145/3351095.3372871> (Last visited on October 30, 2025).