数字司法实践的刑事程序规制

——以《刑事诉讼法》再修改为背景

郑 曦

摘 要 数字时代，为适应刑事案件办理的新需要，公检法机关积极推进数字司法实践，提升了案件办理质效，但也带来了一些问题，需要在修改《刑事诉讼法》时予以规制。《刑事诉讼法》规制数字司法实践，宜采用“原则性要求+关键性规范”模式。按照此种模式，首先应提出强调权利保障、坚持控辩平等、合理定位办案人员和工具关系这三项原则性要求，其次应将数字取证、数据处理和人工智能辅助办案作为规制的关键问题，最后从合理引入新兴权利、大力增强辩方力量、藉由数据安全保护限制公权力三个角度展开《刑事诉讼法》规范层面的修改完善。抓住《刑事诉讼法》修改的契机对数字司法实践进行规制，能有效缓解此种实践所带来的副作用，确保其在法治的轨道上顺利运行。

关键词 数字司法实践 《刑事诉讼法》修改 原则性要求 关键问题 规范展开

问题的提出

数字时代新技术的应用改变了人类生活方式，也使犯罪形态发生显著变化。互联网的虚拟空间成为犯罪的重要场域，大数据、人工智能等技术也可以成为犯罪工具。不但一些传统犯罪呈现出涉网的特征，基于数据捕捉、深度伪造等技术而实施的以数据为对象的新型犯罪更是层出不穷。[①] 面对犯罪形态的更新，刑事司法领域的侦诉审工作亦不得不进行数字化革新，以适应数字时代刑事案件办理的需要。

我国公检法机关向来对新型技术应用态度积极，其中公安机关最早开展数字化建设。近年来，公安机关又依托网络技术、大数据技术、人工智能技术推动数字侦查进程，不仅建成了较为完善的信息网络和应用系统，还以“数字警务”为目标开展智慧侦查等模块的建设，形成了完备的数字化建设体系。更值得注意的是，部分案件的侦查取证工作实际向刑事立案前延伸，通过视频监控、手机数据检测以及其他大数据、人工智能识别手段，提前开展犯罪治理工作。检察机关的数字化建设进程可以追溯到2000年。近期，为适应数字时代对检察监督提出的新要求，检察机关积极推进

* 郑曦，法学博士，北京外国语大学法学院教授。本文系教育部人文社会科学重点研究基地重点项目“程序法治下的网络安全研究”（23JJD820004）的阶段性研究成果。

① 参见刘艳红：《网络时代社会治理的消极刑法观之提倡》，载《清华法学》2022年第2期，第176页。

“数字检察”建设，将科技创新成果与法律监督工作深度融合，建立法律监督数字模型及配套系统，以“数字革命”促进刑事检察工作的质效提升。[①] 2016 年最高人民法院提出“智慧法院”建设目标，[②] 大力加强新技术在审判工作中的运用；近年来又提出“数字法院”建设目标，[③] 建设内容涵盖以网络为载体的案件信息公开、依托现代技术平台的案件管理、智能语音文字转化、智能化司法信息检索、智能诉讼服务等，助力审判提质增效。

无论“数字警务”“数字检察”抑或“数字法院”，公检法机关的数字司法[④]实践都显著改变了刑事案件办理的基本模式，极大提升了办案效率。然而，数字司法实践也不可避免地带来了一些问题：其一，在观念层面，数字司法实践的直接动力来自公检法机关对提升刑事案件办理质效的要求，带有明显的追诉倾向，缺乏对诉讼参与人特别是犯罪嫌疑人、被告人权利保障的关照，某些情形下甚至对当事人诉讼权利造成不当侵害。其二，在技术层面，数字司法实践通常由中央层级的公检法机关各自从上而下部署和推动，在改革措施的设计和实施上，三机关之间缺乏沟通和联动，进而形成“各自为战”的状态。例如，因数字化办案平台端口的不匹配导致案件证据推送困难。其三，在规范层面，数字司法实践未能与已有立法形成良好的衔接和互动。例如，《数据安全法》第五章“政务数据安全与开放”和《个人信息保护法》第二章第三节“国家机关处理个人信息的特别规定”中均规定了国家机关处理数据和个人信息的义务。公检法机关作为“国家机关”，应当在办理刑事案件时履行相应义务。但这些义务如何履行，以及与这些义务相对应的、《数据安全法》和《个人信息保护法》所规定的知情同意权等权利如何在刑事诉讼中予以保障，仍缺少规范层面的衔接规定。

数字司法实践带来的上述问题，与相关改革缺乏统筹、往往仅反映部门利益、头痛医头脚痛医脚的风格直接相关。在此种情况下，既然《刑事诉讼法》再修改已经被全国人大列为一类立法规划项目，[⑤] 就有必要借此契机，在《刑事诉讼法》修改中对数字司法实践作出回应、规范和引领，以确保数字司法实践在法治化的轨道内顺利展开。

一、《刑事诉讼法》规制数字司法实践的模式

在明确了有必要在《刑事诉讼法》中对数字司法实践进行规制这一前提之后，接下来需要回答的问题是，应当采取何种模式进行规制。对此，按照《刑事诉讼法》对数字司法相关问题进行规制的粗细程度排列，至少有三种可供选择的规制模式。

第一种模式是《刑事诉讼法》仅对数字司法相关问题作出原则性的要求，而将具体规则交由司法解释、部门规定等位阶较低的规范性文件或其他领域性法律文件，如《数据安全法》《个人信息

① 参见高景峰：《数字检察的价值目标与实践路径》，载《中国法律评论》2022 年第 6 期，第 35－36 页。

② 参见罗书臻：《周强在最高人民法院信息化建设工作领导小组二〇一六年第一次全体会议上强调 坚持需求和问题导向 破解难题补齐短板 推进人民法院信息化建设转型升级》，载《人民法院报》2016 年 1 月 30 日。

③ 参见张军：《最高人民法院工作报告——2024 年 3 月 8 日在第十四届全国人民代表大会第二次会议上》，载最高人民法院公报网站，http://gongbao.court.gov.cn/Details/91879661d9288abc72798a23b1ecec.html，2024 年 11 月 4 日访问。

④ 公安机关并非司法机关，但“数字警务”建设与司法密切相关，故本文在广义下使用“数字司法”一词，不做严格区分。参见卞建林：《立足数字正义要求，深化数字司法建设》，载《北京航空航天大学学报（社会科学版）》2022 年第 2 期，第 24 页。

⑤ 参见《十四届全国人大常委会立法规划》，载中国人大网，http://www.npc.gov.cn/c2/c30834/202309/t20230908_431613.html，2024 年 8 月 15 日访问。

保护法》中加以规定。此种模式可以被称为“原则性要求”模式。此种模式的优点在于，能够有效保证《刑事诉讼法》的规定具有长久生命力，不至于因技术发展或司法机关实践变化而频繁修改变动，避免陷入“今天规定区块链、明天规定元宇宙、后天规定生成式人工智能”般的“一事一立法”的窘境，维护《刑事诉讼法》的稳定性。进一步看，《刑事诉讼法》只对数字司法的相关问题做原则性的规定，也契合其作为高位阶之国家基本法律的地位。但“原则性要求”模式亦有“致命”弱点：一是将具体规则交由司法解释、部门规定等规定，增加了部门立法、自我授权的风险。此种风险的存在绝非杞人忧天，而是已被多次证明。检法机关对取保候审、监视居住等强制措施期限的歪曲解释即是其例，[①] 公安机关对技术侦查适用案件类型的扩张规定更为典型。[②] 二是由司法解释、部门规定、领域性法律文件规定的具体规则常常难以得到遵守。由于司法解释、部门规定等位阶较低、部门属性较强，除非以多个部门联合发布的形式颁发，否则常无法得到所有办案机关的认可。而《数据安全法》《个人信息保护法》等领域性法律文件与刑事司法的关系较为疏离，很可能在刑事司法实践中被漠视，如《海关法》中涉及刑事诉讼的条文常不被重视即是例证。由于存在这两方面的重大缺陷，“原则性要求”模式很难成为《刑事诉讼法》规制数字司法实践相关问题的明智选择。

第二种模式是《刑事诉讼法》不仅要有针对数字司法相关问题的原则性的要求，还要尽可能地对其他已经呈现出来或未来极有可能呈现出来的问题做完整细致的规定。此种模式可以被称为“全面规范”模式。“全面规范”模式相较于“原则性要求”模式，其优势在于：其一，规制数字司法具体规则的法律位阶较高。由《刑事诉讼法》这一基本法律予以规定，能够体现国家对此问题的重视，并在一定程度上实现国家对数字司法实践的统筹规划；其二，挤压基于部门利益而钻法律空子的空间。由《刑事诉讼法》对具体问题进行细致明确的规定，甚至对未来可能出现的问题作出预先规定，使得部门立法曲解法律的可能性降低，实现法律规定的统一协调，防止规范之间的矛盾冲突；其三，保证相关规定得到普遍遵守。相对于司法解释、部门规定或领域性法律文件，《刑事诉讼法》在刑事司法领域更能得到公检法等各个机关的重视和认可，从而能够确保相关规定得到遵守和执行。然而，“全面规范”模式虽然具有上述显著优势，其缺陷亦十分明显：一是过于求全求细的规定难以应付技术的飞速发展以及司法实践的复杂变化，从而可能导致某些条文在不久的将来就变得过时，而另一些问题又需要在条文中予以规定，如此一来，频繁的修法会导致《刑事诉讼法》的稳定性降低，影响其权威；二是要求在当下即对未来可能出现的问题作出预先规定，对立法者提出了巨大挑战。由于法律人与技术的天然疏离关系，[③] 此种要求难免显得过于强人所难。由此看来，“全面规范”模式亦非《刑事诉讼法》规制数字司法相关问题的最佳选项。

第三种模式是《刑事诉讼法》在对数字司法提出原则性要求的基础上，不求全责备地细致规定所有相关问题，而是仅针对其中较为重要的关键性问题作出规范层面的规定，并将其他重要程度较低甚至细枝末节的问题交由司法解释、部门规定等位阶较低的规范性文件或《数据安全法》《个人

①《刑事诉讼法》规定取保候审最长不得超过 12 个月、监视居住最长不得超过 6 个月，但最高人民法院和最高人民检察院均将其规定为公检法三机关分别可以决定 12 个月的取保候审和 6 个月的监视居住。参见《刑事诉讼法》第 79 条、最高人民法院《关于适用〈中华人民共和国刑事诉讼法〉的解释》第 162 条第 2 款、最高人民检察院《人民检察院刑事诉讼规则》第 102 条和第 112 条。

②《刑事诉讼法》第 150 条规定公安机关对危害国家安全犯罪、恐怖活动犯罪、黑社会性质的组织犯罪、重大毒品犯罪或者其他严重危害社会的犯罪案件可以采取技术侦查措施，而公安部《公安机关办理刑事案件程序规定》第 263 条将“其他严重危害社会的犯罪案件”做了极大的扩张解释，使得公安机关对几乎所有可能判处七年以上有期徒刑的刑事案件都可以采取技术侦查措施。

③ 参见左卫民：《关于法律人工智能在中国运用前景的若干思考》，载《清华法学》2018 年第 2 期，第 119 页。

信息保护法》等领域性法律文件做具体规定。此种模式可以被称为“原则性要求 + 关键性规范”模式。相较于前两种模式，该模式相对折中，兼具“原则性要求”模式保证《刑事诉讼法》规定长效稳定以及“全面规范”模式缩小法律空当、保证规定得到普遍遵守的优势，又能在一定程度上缩减上述两种模式的缺陷和不足，是当前《刑事诉讼法》规制数字司法的“相对合理”[①] 选择。但该模式下仍有三方面问题需要回答：一是《刑事诉讼法》规制数字司法实践的“原则性要求”有哪些？二是基于这些原则性要求，应当着重解决哪些“关键性”问题？三是针对这些关键性问题，应作出何种具体规定？

二、《刑事诉讼法》规制数字司法实践的原则性要求

在“原则性要求 + 关键性规范”模式下，首先需要确定《刑事诉讼法》面对数字司法实践时应当提出何种原则性要求。根据数字时代发展的趋势和数字司法实践的逻辑，至少有以下三项原则尤其值得重视。

（一）充分强调权利保障

刑事诉讼权利是当事人或其他诉讼参与人基于其主体资格而根据其利益考量自由实施诉讼行为之权利。保护刑事诉讼权利，就是保护人的自由、尊严，也是落实宪法“国家尊重和保障人权”规定之要求。然而数字司法实践使得刑事诉讼权利的保护遭遇诸多挑战，主要表现在以下几个方面。

第一，数字司法实践导致正当程序原则所要求的当事人参与权受到减损。刑事诉讼涉及公民生命、自由、财产等最重要法益的限制与剥夺，需有合法程序彰显此种限制与剥夺的正当性。而根据正当程序的要求，刑事诉讼程序应当尽可能地公开、透明，以保障当事人或其所委托之人为其利益而有充分参与。然而数字司法实践使得当事人依其主体地位而行使的参与权遭遇阻碍。基于商业利益、专利技术保护的考量以及专业知识的鸿沟，应用于数字司法的新型技术或工具往往具有秘密、封闭的特征，例如许多学者所主张的算法解释就面临现实困难。[②] 在此种新型技术或工具对刑事诉讼程序的进展发挥重要作用的现实情况下，作为刑事诉讼主体的当事人欲行使其参与权，就因技术的封闭秘密特征而面临难题，减损了刑事诉讼程序的公开、透明性，也阻碍了正当程序的推进。

第二，数字司法实践使得作为诉讼主体的当事人对刑事诉讼程序和结果的控制能力下降。受刑事诉讼程序影响的当事人应当有权通过其行为，对程序推进在一定程度上发挥决定作用，并对最终结果产生影响，以获得较好的结果。[③] 这是刑事诉讼公平正义的题中之义，也是上文所述的参与权的自然逻辑延伸，因此刑事诉讼中向来在一定程度上许可和尊重当事人对刑事诉讼的此种控制。但数字司法实践使得刑事诉讼的程序和实体决定权部分落入工具之手，不仅当事人难以控制程序进展和实体结果，甚至公检法机关的办案人员对刑事诉讼的掌控也在逐渐丧失。

第三，数字司法实践使得作为诉讼主体的当事人在其诉讼权利受到损害之后难以获得救济。“无救济则无权利”已是共识，为保证当事人在权利受损之后获得救济，我国《刑事诉讼法》规定

① 参见龙宗智：《相对合理主义》，中国政法大学出版社 1999 年版，第 3 页。

② 参见辛巧巧：《算法解释权质疑》，载《求是学刊》2021 年第 3 期，第 101 页。

③ See Robert S. Summers, “Evaluating and Improving Legal Process-A Plea for ‘ Process Values’ ”, *Cornell Law Review*, Vol. 60, No. 1 (1974), p. 26.

了复议、上诉、申诉、控告等制度。然而数字司法实践使得刑事诉讼权利受损后相应的救济途径变窄，救济难度增大。早在2016年美国的卢米斯案中，因新型技术应用导致当事人在对质权受到损害后难以获得救济的问题就已引起广泛关注。[①] 如今在我国的数字司法实践中，公检法机关所作出的决定或裁判常借助于新型技术，其结论借“科学”之名而愈发笃定。欲将其推翻则需要更多的努力，于是刑事诉讼本就存在的程序惯性在数字时代下进一步增加，[②] 权利受到侵害后获得救济愈发困难。

《刑事诉讼法》修改中面对数字司法实践所带来的诉讼权利保障问题，应当强调刑事诉讼权利保障的价值追求，以抵消新型技术运用带来的公正障碍，尤其要确保正当程序在刑事诉讼中的实现。首先，应在两个层面保障数字司法实践中的当事人参与权，一是确保作为诉讼主体当事人在数字司法实践场景下，能够知情并在场参与涉及其利益的处理问题，二是保证数字司法实践的结论通过公开、透明的刑事诉讼程序为当事人所知，防止公权力的滥用。其次，应确保当事人在数字司法实践中亦能“有充分的机会富有意义地参与刑事裁判的制作过程”而影响办案人员的心证，“对裁判结果的形成发挥其有效的影响和作用”，[③] 使当事人对刑事诉讼程序和结果重新恢复应有的控制。再次，应赋予当事人适应数字司法实践的救济手段，其中一个可能的路径是适当引入知情同意权、数据访问权、更正权、反对权、被遗忘权等新兴权利，实现对数字司法实践新变革的回应，对此下文将详述。

（二）继续坚持控辩平等原则

诉讼是一种通过摆事实、讲道理解决争端和纠纷的程序，然而能够摆事实、讲道理的前提是双方的力量大体平衡、地位相对平等，不得一方压制另一方。刑事诉讼中，控方以国家机器为后盾，天然具有远强于辩方的力量。于是各法治国家均以不同方式刻意实现控辩的相对平等、以利于对抗说理，例如英美国家将控方当事人化，我国设置专家辅助人制度、值班律师制度等，均是出于维护控辩平等原则的考虑。然而数字司法实践进一步拉大了本就明显存在的控辩力量差距，给控辩平等原则带来了冲击，造成了控辩力量的“数字鸿沟”。

一方面，控方的力量因数字司法实践得到大幅增强。首先，控方的取证能力提升。通过运用云计算、数据挖掘、智能引擎等新技术手段，侦查机关可以对互联网上的数据进行抓取和分析，并对特定信息进行标识和提示，进而高效地获取具有证据价值的数据。[④] 此外侦查机关还可以借助网络搜查的手段，打破传统侦查模式下取证所受到的时间和空间束缚，实现取证的远程化和无接触化。其次，控方的证据处理能力拓展。在办理网络犯罪等复杂案件时，控方所掌握的、以数据形式呈现的证据数量往往十分惊人，以传统的方式进行证据的校验、审查、判断已经难以有效应对。而在数字司法实践中，控方应用智能化工具处理海量、庞杂证据，不但效率更高，而且常常更为准确，提升了案件办理质效。再次，控方的案件管理能力也得到增强。数字司法实践中所使用的智能化工具，大多具有案件档案管理、案件分配和预警、文书模板推送、音视频记录、语音文字转换、程序跟踪、司法业绩考核等功能。通过这些功能的运用，控方能够通过数据画像，[⑤] 对刑事案件办理开展整体性控制，增强刑事追诉能力。

---

① *Loomis v. Wisconsin*, 881 N. W. 2d 749 (2016).
② 参见郑曦：《刑事诉讼中程序惯性的反思与规制》，载《中国法学》2021年第3期，第249页。
③ 陈瑞华：《刑事审判原理论》，法律出版社2020年版，第80页。
④ 参见孔祥贤、申晨：《大语言模型技术在公安领域的应用及未来展望》，载《广东公安科技》2024年第3期，第7页。
⑤ 参见高景峰：《数字检察的价值目标与实践路径》，载《中国法律评论》2022年第6期，第47页。

另一方面，辩方的力量在数字司法实践中被实际减损。其一，决定辩方利益的算法不公开。基于科技企业的商业利益保护需要而不公开的算法，却直接对辩方的诉讼利益产生影响。此种封闭、秘密的算法可能导致程序和实体上的不公。面对“算法黑箱”，辩方无法获得充分的证据开示，亦无法展开有效的反对和质疑，[①] 在诉讼中形成力量弱势。其二，辩方缺乏应对控方数字化刑事追诉手段的能力。相较于控方以国家机器为后盾而拥有的数据、算力、算法资源，作为个体的辩方不具备数字化相关的专业知识和处理数据的能力。倘若控方以履行证据开示义务之名对辩方进行“数据倾倒”，则很容易令辩方陷入数据的汪洋之中，[②] 从而使控方以形式正义的方式取得实质不正当的诉讼优势地位。

在刑事诉讼控辩双方力量在数字司法实践中被进一步拉大的趋势下，《刑事诉讼法》在修改中应当再强调坚持控辩平等原则。除在原则层面上对控辩平等原则进行强调之外，还应在制度层面作出进一步相对细致的规定。具体而言，应当从增权和限权两个角度着手。增权是指增强辩方在应对数字司法实践方面的能力，例如为其提供获得数字化专业人员帮助的机会，向其做适当和有限的算法公开等，对此下文详述；限权是指限制控方从数字司法实践中获得的力量优势，对“数据倾倒”等严重违反控辩平等原则的做法予以限制甚至禁止。如此一来，通过《刑事诉讼法》的修改，确保数字时代的刑事诉讼仍然能够基于控辩平等原则而保有摆事实、讲道理的程序本来面貌。

（三）办案人员与工具关系的合理定位

社会生活以人为目的，[③] 作为其一部分的刑事司法亦不例外。在刑事诉讼中，人应当被视为主体，而且这种主体地位应当得到尊重和保障。然而数字时代下，人工智能等新型技术的应用，使得作为“物”的工具逐渐出现了某些主体性特征，甚至具有“类主体”地位，[④] 挤压或削弱了人的主体地位。此种现象亦发生在刑事诉讼领域，典型的体现是智能化工具的应用对公检法人员办理案件履行职权形成阻碍。

首先，数字司法实践中的工具应用限制了案件办理的独立性。《刑事诉讼法》第 5 条规定人民法院依法独立行使审判权、人民检察院依法独立行使检察权，这样规定的目的就在于确保案件办理的独立性，以避免外来干扰。然而工具在刑事案件办理中的广泛应用，却实际地从此种案件办理权限中分得一杯羹。以法院为例，数字司法实践的推进让法官在审理案件时越来越依赖工具，智能化办案系统的类案推送、量刑辅助、模型构建等功能都在改变法官的心证过程，而传统的举证、质证等法庭审理活动对法官心证的影响相对下降。除此之外，开发和运营智能化工具的科技人员也可能通过工具对法官的案件审理产生影响，让司法辅助业务外包变异为部分司法职能外包，使得法官审判变成法官 + 智能化工具审判或法官 + 智能化工具 + 科技人员审判。

其次，数字司法实践中的工具应用可能使得办案人员成为“橡皮图章”。工具在刑事案件办理中所发挥的作用越来越大，在一定程度上侵蚀了公检法人员案件办理权限，甚至在某些场景下实际代替办案人员作出结论。此种忧虑绝非虚幻的想象，而是在实践中已被证明的事实。例如在哥伦比亚的一个民事案件中，法官就使用生成式人工智能工具 ChatGPT 作出关于自闭症儿童医疗保险费用

① *People v. Lopez*, 50 Misc. 3d 632 (N. Y. Sup. Ct. 2015).
② 参见程龙：《论大数据证据质证的形式化及其实质化路径》，载《政治与法律》2022 年第 5 期，第 100 页。
③ 参见［德］康德：《道德形上学探本》，唐钺译，商务印书馆 2012 年版，第 46 页。
④ 参见骆正林：《数字空间、人工智能与社会世界的秩序演化》，载《阅江学刊》2023 年第 6 期，第 90 页。

的判决，甚至在判决书中直接引用其与 ChatGPT 的对话作为裁判依据；[①] 在印度的一个刑事案件中，法官在是否保释的问题上参考了 ChatGPT 的意见，并据此作出拒绝被告人保释申请的决定。[②] 在我国，各种智能化工具也在不同程度上影响公检法人员的案件办理工作，办案人员很难拒绝工具做出的看似具有高度“科学性”的意见，从而可能使得其办案结论过度依赖工具。

第三，与上述两点相应，数字司法实践中的工具应用可能使得司法责任追究面临困难。党的二十届三中全会《决定》再次强调落实和完善十八届三中全会提出的“审理者裁判、裁判者负责”的司法责任制，[③] 而司法责任制下错案追究制度的核心在于追究得出错误办案结论的办案人员相关责任。然而问题在于，如上文所述，在数字司法实践背景下，办案人员的案件办理权限受到工具限制，甚至特定场景下的案件办理结论实际由智能化工具做出，那么在出现错案时，就难以根据司法责任制的追责原则予以追究。或者，即便办案人员确实应当承担责任，他们也可能将责任推给工具，这会进一步造成司法责任制落实困难。

针对上述问题，有必要合理定位办案人员与工具之间的关系，明确人相对于工具的主导性地位，实现刑事案件办理中工具对人的辅助作用。对此，公检法机关已有认识，例如 2022 年最高人民法院《关于规范和加强人工智能司法应用的意见》第 5 条依据“辅助审判原则”，规定“坚持对审判工作的辅助性定位和用户自主决策权，无论技术发展到何种水平，人工智能都不得代替法官裁判，人工智能辅助结果仅可作为审判工作或审判监督管理的参考，确保司法裁判始终由审判人员做出，裁判职权始终由审判组织行使，司法责任最终由裁判者承担。”但是以司法文件的形式作出的规定，位阶太低、效力不高、适用范围有限，无法满足数字司法实践需要。因此，有必要在此次《刑事诉讼法》修改中吸纳相关内容，明确规定刑事案件办理的主体是公检法机关的办案人员，而工具在刑事诉讼中只能作为辅助者，其意见仅供参考。

三、《刑事诉讼法》规制数字司法实践的关键问题

按照《刑事诉讼法》规制数字司法实践的“原则性要求 + 关键性规范”模式，在确定原则性要求后，《刑事诉讼法》修改中应对数字司法实践中的关键问题有所关照和回应，其中以下三个问题尤其值得关注。

（一）数字取证

如上文所述，数字司法实践中新型技术和工具的运用显著提升了控方的取证能力，但也极大减损了辩方权利。因此《刑事诉讼法》修改中应充分关注数字取证问题，尤其通过两方面措施的强化，实现数字取证中对公权力的必要限制和对公民权利的合理保障，以契合强调权利保障和坚持控辩平等之数字司法实践的原则性要求。

一方面，应当加强对网络在线收集提取证据的监督制约。较之以往传统的取证方式，网络在线

① See Purvish M. Parikh, Dinesh M. Shah and Kairav P. Parikh, “Judge Juan Manuel Padilla Garcia, ChatGPT, and a Controversial Medicolegal Milestone”, *Indian Journal of Medical Sciences*, Vol. 75, Issue 1 (2023), p. 4.

② Taniya Dutta, “Indian Judge Uses ChatGPT for Views on Bail Plea of Murder Accused”, https://www.thenationalnews.com/world/asia/2023/03/29/indian-judge-uses-chatgpt-for-views-on-bail-plea-of-murder-accused/(last visited on August 18, 2024).

③ 参见《中共中央关于进一步全面深化改革 推进中国式现代化的决定》，载中国政府网，https://www.gov.cn/zhengce/202407/content_6963770.htm，2024 年 8 月 18 日访问。

收集提取证据作为应对数字时代犯罪网络化特征的手段，借由网络实施超越地理限制的证据提取，是数字取证之典型方式，对公权力运行和公民权利保障均有较大影响。针对网络在线收集提取证据，现有的规范性文件如 2016 年最高人民法院、最高人民检察院、司法部《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》（以下简称“2016 两院一部《电子数据规定》”）和 2019 年公安部《公安机关办理刑事案件电子数据取证规则》（以下简称“2019 公安部《电子数据取证规则》”）中已有相应规定。然而，相关规定均是从公权力运行的视角展开，对网络在线收集提取证据的适用对象、实施方式、数据保全方式、流程记录、网络远程勘验规范等进行了较为详细的规定，[①] 但在权力行使限制和权利保障方面仍有疏漏。针对此种情形，《刑事诉讼法》修改中较为稳妥的选择是，参考 2019 公安部《电子数据取证规则》第 33 条“网络在线提取或者网络远程勘验时……用技术侦查措施收集电子数据的，应当严格依照有关规定办理批准手续。收集的电子数据在诉讼中作为证据使用时，应当依照刑事诉讼法第一百五十四条规定执行”这一规定，将网络在线收集提取证据中用技术侦查措施收集电子数据的情况明确地纳入技术侦查范畴，并在此框架内构建网络在线收集提取证据在权力规制和权利保护方面的相关制度。

另一方面，应当发挥非法证据排除规则对数字取证的规制作用。现行《刑事诉讼法》第 56 条并未将电子数据纳入非法证据排除规则的适用对象；2016 两院一部《电子数据规定》第 24 条规定的电子数据合法性审查规则、第 27 条规定的电子数据收集提取程序存在瑕疵时的排除规则与第 28 条规定的基于电子数据真实性的排除规则，从制度本质上看均与非法证据排除规则存在明显差异。[②] 如此一来，理论上电子数据就不属于非法证据排除规则的适用对象，实践中也常出现关于非法取得的电子数据是否应当排除的争议。在数字司法实践中，以非法数字取证获取电子数据的情形并非鲜见。为遏制此种非法取证行为，《刑事诉讼法》修改时应拓展非法证据排除规则的适用对象，对电子数据亦适用此规则，从而对数字取证予以规制。具体而言，可以选择在现行《刑事诉讼法》第 56 条第 1 款第 2 句的“物证、书证”后增加“等”字，或直接将电子数据和其他证据种类明确列入法条中。相对而言，第二种修改方法更为简单明确，有助于避免争论、便于适用，进而确保数字取证行为的合法性。

（二）数据处理

数字司法实践中，数据成为办案平台搭建、智能化工具运行的基础和原料，数据处理亦成为基本办案手段。数据处理连接着刑事诉讼的各方，与权利保障、控辩平等、人与工具关系合理定位的原则性要求均有重大联系，为此《刑事诉讼法》修改中应对数据处理问题有足够关注，特别应注意以下三个要点。

第一，应从国家总体安全观的高度认识数字司法中的数据处理问题。数字司法实践中的数据处理在便利案件办理的同时，也可能存在篡改、破坏、泄露或者非法获取、非法利用等非法处理的情形，[③] 从而引发数据安全风险。数字司法实践中所处理的数据包含大量《数据安全法》第 21 条所指的重要数据，甚至有国家核心数据，一旦被非法处理可能危及国家安全。因而，仅从刑事司法制度的视角看待该问题是不够的，必须从中央提出的总体国家安全观的高度予以审视。有鉴于此，《刑

① 参见 2016 两院一部《电子数据规定》第 9 条，2019 公安部《电子数据取证规则》第二章第四节。

② 参见谢登科：《非法电子数据排除的理论基点与制度建构：以数字权利的程序性救济为视角》，载《上海政法学院学报（法治论丛）》2023 年第 3 期，第 64 页。

③ 参见《数据安全法》第 21 条。

事诉讼法》修改中应对数据处理问题进行原则性规定，要求数据处理合法正当，保障数据安全。

第二，应注意与《数据安全法》《个人信息保护法》等相关法律的协调。作为领域性法律，《数据安全法》和《个人信息保护法》中已有涉及数字司法的内容，如《数据安全法》第五章“政务数据安全与开放”可以适用于公检法机关，第6条明确规定公安机关、国家安全机关在各自职责范围内承担数据安全监管职责，《个人信息保护法》第二章第三节“国家机关处理个人信息的特别规定”亦适用于公检法机关。对于这些规定，在修改《刑事诉讼法》的过程中应当予以梳理，以实现法律间协调。对于其中的重要内容，可在《刑事诉讼法》中再予以明确规定；对于其他一般性规定，可以藉由“国家机关”的概念将《数据安全法》《个人信息保护法》的规定做“统一纳入”的原则性许可，[①] 无需再做细致规定。

第三，应对刑事诉讼领域的数据监管机制作出总体性安排。一是确定监管对象，将刑事司法领域的各类数据处理活动纳入监管范围。作为监管对象的数据处理活动，不但包括对具有证据属性的数据进行的处理，也包括对刑事司法活动中形成的案件行政管理数据的处理。其间需主要监管数据处理是否遵循合法原则，有无造成对公民合法权益的侵害。二是明确被监管的数据处理者。数字司法实践中值得严格监管的数据处理者主要是公检法等公权力机关，因为其所处理的数据不但数量极多，而且直接影响公民的诉讼权利和利益，一旦失控可能给国家利益、公民权益均带来巨大影响。相对的，当事人、律师等私主体在处理数据时，不但量少且影响轻微，不应作为主要监管对象。三是规定数据监管主体。尽管《数据安全法》第6条规定公安机关、国家安全机关在各自职责范围内承担数据安全监管职责，但在刑事司法领域，该类侦查主体的追诉性过强，缺乏独立和中立性，且对刑事诉讼没有全流程参与，难以展开全流程监管。相较而言，检察机关是唯一相对中立又全程参与刑事诉讼所有阶段的机关，同时具有宪法规定的“国家法律监督机关”之地位，因而《刑事诉讼法》在修改时可以考虑将其确定为刑事诉讼领域的数据监管主体。

（三）人工智能辅助办案

数字司法实践中最为典型的做法就是在司法领域引入以人工智能为代表的智能化工具。人工智能工具的引入改变了刑事案件的办理方式，特别是生成式人工智能的应用使得办案人员对工具的依赖程度进一步加深。面对人工智能在刑事诉讼各个阶段广泛运用的现实，《刑事诉讼法》修改中除需合理定位办案人员与工具之间的关系、明确人工智能只能作为辅助办案手段之外，还要重视以下三个问题，以确保人工智能应用中人与工具关系的协调、权力与权利的平衡。

一是应对人工智能辅助办案提出准确性要求。尽管以“高科技”的面目示人，但应用于刑事司法的人工智能的决策准确性常常远低于人们的预期，这在其他国家的司法实践中已经得到证明。[②] 之所以出现这样的准确性偏差，一方面是因为科学技术的发展本身就是以允许发生错误、不断纠正错误为前提的，另一方面则是因为司法领域人工智能所依赖的数据未必有足够的准确度，算力和算法的科学性也需不断提升。面对这样的现实，《刑事诉讼法》修改中应当对人工智能辅助办案提出准确性方面的一般规定。例如，可以对数据的准确性、算力和算法的科学性作出原则性的要求，要求公检法机关运用相对成熟的人工智能技术；要求对用于刑事诉讼的人工智能进行自动化决策的检验与校正，以提供其准确性之保障；要求在案件作出结论前，对办案人员进行人工智能可能出现准

① 参见程雷：《刑事诉讼中适用〈个人信息保护法〉相关问题研究》，载《现代法学》2023年第1期，第91页。

② See Christopher Slobogin, “Principles of Risk Assessment: Sentencing and Policing”, *Ohio State Journal of Criminal Law*, Vol. 15, No. 2, (2018) p. 584.

确性偏差的提示，以防止办案人员对人工智能的盲目信任。

二是应重视人工智能辅助办案中的公平公正问题。人工智能辅助办案可能在实体和程序两个层面影响案件的公平公正办理。实体层面上，在人工智能封闭秘密的算法中可能隐藏歧视性因素，如美国 COMPAS 量刑辅助系统对不同种族被告人的社会危险性评估带有歧视性偏差。① 程序层面上，人工智能辅助办案可能导致辩方诉讼权利行使困难和控辩力量对比失衡，例如出现如上文所述的使当事人的参与权难以实现、对程序的控制能力下降等现象。为此，《刑事诉讼法》修改中可以考虑加强对案件办理公正性保障机制的规定，如要求办案人员对其为何最终接受人工智能的意见进行必要的解释，对证据开示、质证权保障等作出更为严格的规定。健全保障性机制可以有效降低人工智能辅助办案所带来的公平公正方面的风险。

三是应预防人工智能辅助办案带来的机械司法风险。人工智能秉持技术逻辑，其底层基础是数学，即便面对复杂的刑事案件，也必须将所有输入的案件信息转化为“0”与“1”的数字进行运算，方可得出结论。这种去价值化的、冰冷的人工智能技术逻辑固然有其客观冷静之优势，但与案件办理中的情感投入、价值判断的需求却未必相符。过度依赖此种技术逻辑可能使得案件办理伴有僵化色彩，带来机械司法之风险。因此，《刑事诉讼法》修改中应对此种机械司法风险予以警惕。除明确办案人员与人工智能的关系定位以及在案件办理中的权限区分外，还可以通过排除某些特定事项中的人工智能参与、禁止将采纳人工智能意见作为办案人员考核指标、强调办案人员对人工智能意见的拒绝和否定权力、规定决策作出前提供相应提示等方式，降低机械司法风险，强化办案人员在案件办理中的主体地位和主导作用。

四、《刑事诉讼法》规制数字司法实践的规范展开

根据“原则性要求 + 关键性规范”的模式，欲以《刑事诉讼法》规制数字司法实践，需依照权利保障、控辩平等和人与工具关系合理定位的原则性要求，针对上述关键问题进行规范层面的修改完善，具体应从三个角度展开。

（一）合理引入新兴权利

“我们的时代是一个迈向权利的时代，是一个权利倍受关注和尊重的时代，是一个权利话语越来越彰显和张扬的时代，”② 权利时代与数字时代的交融与碰撞，带来的是“新兴权利不断展现”。③ 知情同意权、数据访问权、更正权、反对权、被遗忘权等数据权利对刑事诉讼逐渐产生影响，使得“如同桅杆顶尖”的刑事诉讼权利体系亦因新兴权利的频频“叩门”而做出“强烈的摆动”。④ 对于这些事实上已对刑事诉讼产生一定影响的新兴权利，《刑事诉讼法》在修改时不能视若无睹，而是有必要对其做出合理、适当的引入和肯认，以促进权利保障和控辩平等等规制数字司法实践的原则性要求的达成。

明确刑事诉讼领域应引入的新兴权利种类需从三个方面进行考量。一是此种新兴权利的引入是

① See Julia Angwin, etc., “Machine Bias: What Algorithmic Injustice Looks Like in Real Life”, https://www.propublica.org/article/what-algorithmic-injustice-looks-like-in-real-life, last visited on August 19, 2024.

② 张文显、姚建宗：《权利时代的理论景象》，载《法制与社会发展》2005 年第 5 期，第 3 页。

③ 姚建宗：《新兴权利论纲》，载《法制与社会发展》2010 年第 2 期，第 3 页。

④ ［德］拉德布鲁赫：《法学导论》，米健、朱林译，中国大百科全书出版社 1997 年版，第 120 页。

否符合刑事诉讼数字化转型和数字司法实践发展的时代需求。所谓符合此种时代需求，首要的就是对此种新兴权利的肯认，需能够缩小因数字化带来的控辩力量差距，对当事人权利保障有利。二是此种新兴权利的引入是否会对刑事诉讼中的其他权利及其承载的价值造成过大的冲击。任何一种新兴权利的引入，都会与其他权利产生竞争甚至冲突，甚至给刑事诉讼权利体系带来冲击。但问题的关键在于，需考虑不同权利所承载价值之间的位阶关系，[①] 并考虑此种引入是否会带来过高的成本。三是此种新兴权利的引入是否已有规范基础。倘若某项新兴权利在《刑事诉讼法》或其他相关规范性文件中已有规范雏形，那么对其做正式的肯认便有规范基础，相应的立法和实践适用上的阻力和难度也能相对减少。

根据上述三方面因素，可以考虑在《刑事诉讼法》修改中引入以下几项新兴权利。

一是知情权。知情是刑事诉讼权利得以行使和保障的前提。面对数字司法实践，知晓公权力机关运用新型技术和工具的事实、了解其所处理的事项、理解此种运用对诉讼进程和结果的影响，对于当事人而言至关重要。我国《刑事诉讼法》及相关规范性文件有多处关于“告知”的规定，[②] 将告知的事项拓展至数字司法实践中新型技术和工具的运用问题，不至于给刑事诉讼权利体系带来剧烈冲击，且已有相关规范作为参考。故而，引入作为新兴权利的知情权意义重大且难度不高，《刑事诉讼法》修改中应当予以考虑。

二是数据访问权。我国《刑事诉讼法》第 40 条规定的阅卷权制度，不但有权利主体从被追诉人到辩护人的偏移，且适用范围过于狭窄，仅限于“诉讼文书 + 证据材料”的“案卷材料”，无法适应数字司法实践中数据处理带来的新需求。针对此种现实，可以参考欧盟适用于刑事司法领域数据保护的第 2016/680 号指令中关于“数据访问权”（right of access）的规定，[③] 允许辩方获取与案件相关的数据。目前我国《个人信息保护法》第 45 条关于个人有查阅复制其个人信息权利的规定与数据访问权接近，在此基础上，《刑事诉讼法》修改中可以考虑引入数据访问权，以对阅卷权进行拓展和改造，应对数字司法实践中的保障权利和维护控辩平等之需求。

三是封存、删除权。案件相关数据在数字司法办案系统中长期存储，固然有利于后续对案件进行追踪、预防再犯等，但却给当事人、特别是被定罪的罪犯摆脱案件影响、完成教育矫正、回归正常生活带来了阻碍。有鉴于此，我国《刑事诉讼法》第 286 条规定了未成年人犯罪记录封存制度，2022 年最高人民法院、最高人民检察院、公安部、司法部《关于未成年人犯罪记录封存的实施办法》对该制度做了细化规定。而欧盟第 2016/680 号指令第 16 条走得更远，直接规定了“擦除权（right to erasure）”，允许数据主体请求删除相关数据。[④] 根据党的二十届三中全会《决定》关于“建立轻微犯罪记录封存制度”的要求，[⑤] 并在犯罪记录封存的制度基础上，参考欧盟第 2016/680

① 参见王利明：《民法上的利益位阶及其考量》，载《法学家》2014 年第 1 期，第 82－83 页。

② 例如《刑事诉讼法》第 34 条规定应依法告知被追诉人有权委托辩护人、第 36 条应告知犯罪嫌疑人有权约见值班律师、第 46 条规定应告知被害人等有权委托诉讼代理人、第 120 条规定讯问时应告知犯罪嫌疑人享有的诉讼权利和相关法律规定、第 162 条规定公安机关侦查终结应告知犯罪嫌疑人及其辩护律师案件移送情况、第 173 条规定人民检察院应当告知认罪认罚的犯罪嫌疑人所享有的诉讼权利和认罪认罚的法律规定等，此外最高人民法院《关于适用〈中华人民共和国刑事诉讼法〉的解释》、最高人民检察院《人民检察院刑事诉讼规则》、公安部《公安机关办理刑事案件程序规定》中也有相关规定。

③ “Directive（EU）2016/680”，https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri = CELEX：32016L0680&from = EN，last visited on August 19，2024.

④ “Directive（EU）2016/680”，https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri = CELEX：32016L0680&from = EN，last visited on August 19，2024.

⑤ 参见《中共中央关于进一步全面深化改革 推进中国式现代化的决定》，载中国政府网，https://www.gov.cn/zhengce/202407/content_6963770.htm，2024 年 8 月 18 日访问。

号指令第 16 条和我国《个人信息保护法》第 47 条的规定，《刑事诉讼法》的修改应吸纳封存、删除权，允许包括已被定罪罪犯在内的当事人在符合法定条件的情形下申请封存、甚至删除与刑事案件相关的犯罪记录等数据。

针对这些新兴权利在刑事诉讼中如何具体实现的问题，例如权利行使的时空条件、以何种方式实施、相应的义务主体为何者、如何实现制度和技术层面保障等，笔者在以往的研究中已有论及，限于篇幅，此处不再赘述。①

（二）大力提升辩方力量

以实现对数字司法实践的规制为目标，《刑事诉讼法》在修改中应大力提升辩方力量，使其具备与控方进行平等对抗的能力，以落实权利保障和控辩平等之原则性要求。然而如上文所述，数字司法实践背景下辩方力量的相对弱势，主要是因为应用于刑事诉讼的算法不公开导致辩方相关诉讼权利难以行使，以及辩方缺乏应对控方数字化刑事追诉手段的能力，于是提升辩方力量也应从这两个方面着手展开。

一方面，可以要求进行有限的算法公开。应用于刑事诉讼领域的算法之所以呈现出封闭秘密的特征，固然有其合理根据。从维护合法商业利益的视角看，一味要求科技企业公开算法，会挫伤其研发的积极性，不利于产业的持续稳定发展。然而刑事诉讼中的算法封闭确实严重影响当事人刑事诉讼权利的行使，且由于刑事诉讼关系到生命、自由、财产等最重要的法益，一旦出错后果难以承受。因此，从平衡商业利益和刑事诉讼利益之间关系的思路出发，可以要求对应用于刑事诉讼领域的算法进行审慎、有限地公开。此种“有限”可以体现在几个方面：一是公开算法的情形特定，仅案件存在重大疑点、控辩双方有较大争议、对案件办理有重要影响的情况下才需考虑公开算法；二是算法公开的对象受限，除办案人员之外，只向受算法直接影响其诉讼权利和利益的当事方公开；三是需有特定方法防止算法公开外溢，例如可以要求各方以签订保密协议等方式控制公开范围，确保算法公开不至于对科技企业造成明显不合理的利益损害。而对算法有限公开的场景、对象、范围等发生争议时，首先应当以各方协商的方式予以解决，协商不成时应由具有裁决性权力的公权力机关，例如审判阶段的法院、审前阶段的检察院作出决定。此种由公权力机关最终决定的方式在国外的司法实践中已有先例，② 既契合公权力机关作为刑事案件办理者的角色定位，也利于解决争议、推进刑事诉讼程序进展。

另一方面，应为辩方提供获得数字化专业技术帮助的途径。相较于控方，辩方在数字时代的劣势集中体现于数据处理能力的羸弱上，因此从控辩平等的目标出发，除应对控方的“数据倾倒”等不当数据处理行为予以限制之外，还需为辩方提供数据处理方面的专业帮助途径。第一种可行的途径是由专家辅助人为当事人提供数据处理协助。我国《刑事诉讼法》第 197 条第 2 款规定了“由专门知识的人”即专家辅助人出庭可以就鉴定意见提出意见，2016 两院一部《电子数据规定》第 21 条规定专家辅助人可以在法庭上操作电子数据的展示、并就相关技术问题作出说明。基于上述规定，《刑事诉讼法》修改可以进一步扩展专家辅助人的职权，使其能够为当事人提供数据处理方面的协助。这将有助于解决辩方当事人及其辩护律师缺乏数字化相关专业知识的困境，提升辩方的数据处理能力，从而实现对公民权利的保障以及对控辩平等原则的维护。第二种可能的路径是允许辩

① 参见郑曦：《数字时代的刑事诉讼变革》，法律出版社 2023 年版，第 15－21、278－282 页。

② *People v. Lopez*, 50 Misc. 3d 632 (N. Y. Sup. Ct. 2015).

方从科技企业处获得数据处理方面的帮助。当前，控方以司法辅助职能外包之名从科技企业处获得数据处理等数字化技术的协助已是常态，甚至得到了高层的认可。[①] 既然如此，从控辩平等的思路出发，允许辩方向科技企业寻求数据处理方面的支持又有何不可？《刑事诉讼法》修改若能肯定此种已然在实践中出现的现象，不仅可以彰显权利保障的价值追求，而且在宣示和规范两个层面上也具有重要意义。当然，辩方向科技企业寻求技术支持需以一定经济实力为基础，这也可能引发平等方面的问题，需予以关注并逐步解决。

（三）藉由数据安全保护实现公权力限制

如上文所述，数字司法实践带来的刑事诉讼领域的数据处理活动，不但涉及公权力行使与公民权利保护之间的关系，还可能对国家安全、公共利益造成影响，因而需从总体国家安全观的高度予以审视，重视数据安全保护。与此同时，由于公权力机关是刑事诉讼领域最主要的数据处理者，从数据安全保护的需求着手，亦可以实现对公权力运行的限制，合理定位办案人员与工具的关系，防止公权力滥用。

其一，应对刑事诉讼领域的数据进行分类分级。数据分类分级是数据安全保护的前提，有助于针对性地采取不同的保护措施，这在刑事诉讼领域亦不例外。由于数据分类是按照数据的来源、内容、作用等属性而展开的，刑事诉讼领域中的数据可以大体分为个人数据和政府数据，其中个人数据可再分为身份数据和行为数据，政府数据可细分为公安数据、检察数据、审判数据和其他数据等；[②] 而数据分级是按照“数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度”[③] 所做的区分，刑事诉讼领域中的数据亦可按照《数据安全法》第 21 条分为国家核心数据、重要数据和一般数据。《刑事诉讼法》修改应对刑事诉讼领域的数据分类分级作出规定，为公权力行使和公民权利保护提供参照标准，使数据安全保护有据可循。

其二，应对数据处理展开全流程安全监管。数据处理有其全生命周期，包括数据的生产、收集、存储、管理、使用、加工、传输、提供、公开、删除等流程。[④] 而在刑事诉讼领域，数据处理亦需经历上述流程，且其中任何一个流程都可能出现数据非法处理之风险，从而给数据安全保护带来威胁。因此，对刑事诉讼中的数据处理活动开展全流程安全监管具有显著必要性，《刑事诉讼法》修改应对此予以重视，特别是关注数据的收集、存储、传输和删除这四个极易发生安全风险的节点：数据的收集常涉及上文所述的数字取证问题，其间易出现公权力机关滥权的问题；数据的存储中可能因存储的介质、方式、地点、时长等引发数据泄露、篡改之忧虑；数据的传输中发生数据泄露、丢失、篡改、破坏或被非法获取和利用的可能性亦存在，尤其是在当前各个机关办案系统不统一、端口不适配的情况下，此种风险更为显著；数据的删除中则会有数据应删未删或不应删而删除的可能。对于这些重点环节，《刑事诉讼法》修改中可以“重其所重、轻其所轻”地作出相应规定，以降低数字司法实践中的数据安全风险。

其三，应对科技企业参与数字司法实践作出必要的限制。由于公检法机关本身对新型技术的陌生，数字司法实践不得不以司法辅助职能外包的形式向科技企业寻求技术支持，由科技企业提供平

① 参见李阳：《孟建柱在全国司法体制改革推进会上强调 主动拥抱新一轮科技革命 全面深化司法体制改革 努力创造更高水平的社会主义司法文明》，载《人民法院报》2017 年 7 月 12 日。

② 参见郑曦：《刑事司法数据分类分级问题研究》，载《国家检察官学院学报》2021 年第 6 期，第 11－12 页。

③ 参见《数据安全法》第 21 条。

④ 李怀胜：《数据全生命周期安全风险及其刑法回应路径》，载《苏州大学学报（哲学社会科学版）》2023 年第 3 期，第 75 页。

台搭建、系统研发和维护等服务。其间科技企业必然需获得数据处理的权限，方可给予上述技术支持，于是科技企业亦成为刑事司法领域重要的数据处理者。由于刑事诉讼中的数据可能是重要数据甚至是国家核心数据，从数据安全保护的角度看，应当对科技企业的数据处理权限予以限制。对于国家核心数据，应严格禁止科技企业进行处理；对于重要数据，应对科技企业的处理活动采取严格的监管措施。为实现此种限制和监管，应厘清公权力机关与科技企业之间的公私合作关系，并在具体办案人员与科技企业之间设置交往屏障，防止科技企业利用数字司法实践中的司法辅助工作，借由工具运用对案件办理造成不应有的影响，以确保办案人员与工具、科技企业各司其职，实现相互关系的合理定位。

藉由数据安全保护实现公权力限制，可以确保公权力在法律规定的“笼子”里行使，防止其对公民权利造成侵害。这对保护公民权利、维护控辩平等的前述原则性要求的实现，亦有补益和促进作用。

结　语

数字时代下“新的文明”[①] 正深刻而全面地重塑着人类社会生活。作为社会生活的一部分，刑事诉讼也不可避免地面临机遇与挑战，而数字司法实践正是对此种机遇与挑战的回应。如同其他新鲜事物，数字司法实践在促进刑事诉讼数字化变革、提升案件办理质效的同时，也带来了这样或那样的不适或者问题。在此种情形下，抓住《刑事诉讼法》修改的契机，以“原则性要求 + 关键性规范”的模式规制数字司法实践，能够最大程度地趋利避害，促使数字司法实践及其带来的变革符合刑事诉讼的根本价值追求和基本原理原则。这有利于公民权利在刑事诉讼中得到更为充分的尊重和保障，避免新型技术对刑事诉讼造成畸形改变或导致对人的压制和压迫，从而最大限度地实现数字司法实践在法治化的轨道上运行，以适应数字时代需求的方式顺利运行。

（责任编辑：魏晓娜）

① ［美］阿尔温·托夫勒：《第三次浪潮》，朱志焱、潘琪、张焱译，生活·读书·新知三联书店 1983 年版，第 43 页。