Dispute Settlement 争议解决, 2026, 12(9), 9-17
Published Online September 2026 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2026.129249

Hans汉斯

数据侦查中个人信息保护的问题检视与解决对策研究

冯睿琪

西北政法大学公共安全法学院，陕西 西安

收稿日期：2026年7月31日；录用日期：2026年8月26日；发布日期：2026年9月3日

摘　要

数字技术与侦查活动的深度融合使数据侦查已成为犯罪治理的核心力量，但其在权力运行与个人信息保护之间形成了深刻的内在张力。如何在这一张力中划定侦查权边界、防止个人信息权益被过度克减，已成为亟待回应的命题。数据侦查的回应性、监控性与预测性三重形态在启动时点、干预强度与作用逻辑上存在显著差异，其暴露出的过早启动、过度收集、主体外溢、深度分析、泄露风险及决策偏差等问题，根源在于传统规制体系未能有效应对数字技术带来的权力扩张与权利保障之间的结构性失衡。为此，应当构建差异化的侦查启动门槛、梯度化的审查机制、隐私计算与区块链协同的技术治理路径，并切实落实数据主体的基本权利，形成权力控制、技术治理与权利保障三位一体的规制体系，从而在犯罪防控与人权保障之间实现动态平衡，推动数据侦查从权力单边扩张转向权力与权利的良性互动。

关键词

数据侦查，个人信息保护，权力规制，权利保护

A Study on the Examination of Issues and Countermeasures for Personal Information Protection in Data Investigation

Ruiqi Feng

School of Public Security, Northwest University of Political Science and Law, Xi’an Shaanxi

Received: July 31, 2026; accepted: August 26, 2026; published: September 3, 2026

Abstract

The deep integration of digital technology into criminal investigation has made data-driven inves-

文章引用: 冯睿琪. 数据侦查中个人信息保护的问题检视与解决对策研究[J]. 争议解决, 2026, 12(9): 9-17.
DOI: 10.12677/ds.2026.129249

tigation a core tool for crime governance, yet its operation creates inherent tension with personal information protection. Delineating investigative boundaries and preventing undue infringement upon personal information rights thus poses a pressing legal issue. The responsive, surveillance, and predictive modes of data-driven investigation differ in initiation timing, intervention intensity, and operational logic. Problems such as premature initiation, excessive collection, subject spillover, in-depth analysis, leakage risks, and decision-making biases originate from the traditional regulatory framework's failure to address the structural imbalance between digitally enabled power expansion and rights protection. To remedy this, a tripartite regulatory system—encompassing power control, technical governance, and rights protection—should be established via differentiated initiation thresholds, graded review mechanisms, privacy computing combined with blockchain, and enforceable data subject rights. This would achieve dynamic equilibrium between crime prevention and human rights protection, steering data-driven investigation from unilateral power expansion toward constructive power-rights interaction.

Keywords

Data-Driven Investigation, Personal Information Protection, Power Regulation, Rights Protection

1. 引言

自《中共中央 国务院关于构建数据基础制度 更好发挥数据要素作用的意见》[1]印发以来，以数据为关键要素的数字时代飞速发展，数据要素深刻改变着生产方式、生活方式。与此同时，新型犯罪行为与犯罪行为治理手段样态也随之出现，数智时代下犯罪与侦查之间的博弈相较以往也愈发呈现出数据化、网络化、智能化的特点，新型数字犯罪摆脱传统单一网络化工具这一行为载体扩张至多元数字生态[1]，以数据驱动(Data-driven investigation)为主导的数据侦查[2]也蓬勃发展。数据侦查的出现，不仅是侦查主体与时俱进不断进行自我优化的应有之义，也是应对迭代迅速的新型犯罪的必然之路。

数字技术赋能下的数据侦查通过整合、碰撞案件中涉及的多源异构数据并且对相关数据规律进行分析，其极大提升犯罪治理效能的同时，其过限发展不断突破着“用隐私换安全、用信息换公平”的合理限度：在数据采集、分析、流转的全过程中，极大范围调取、应用数据对犯罪嫌疑人甚至与案件无关的广大公民的个人信息权益进行了不同程度的侵犯，导致公民个人信息权益不断克减。基于此，本文在对数据侦查中的个人信息保护进行理论阐释的基础上，对其在实践中存在的问题进行检视并针对性地提出规制路径，以实现数据侦查与个人信息保护的良性互动。

2. 数据侦查中个人信息保护的理论阐释

2.1. 数据侦查的基本范畴

数据侦查是指侦查机关在刑事诉讼活动中，利用数字技术收集、处理、分析与犯罪案件相关数据，为收集证据、查明案情、查获犯罪嫌疑人、预防和控制犯罪而进行的专门调查活动。为了使研究更为全面，本文所称数据侦查采用广义理解，涵盖立案前的初查阶段与立案后的侦查阶段采取的各类数据处理活动。

基于侦查介入犯罪的时间节点与运行逻辑，数据侦查可区分为回应型、监控型与预测型三种形态。

[1]https://www.gov.cn/gongbao/content/2023/content_5736707.htm.

回应型数据侦查是指在犯罪行为发生后，侦查人员发现犯罪嫌疑，利用数字技术收集、挖掘相关数据对案情与犯罪嫌疑人进行分析，以查明犯罪事实、锁定犯罪嫌疑人的调查活动，具有事后性、被动性；监控型数据侦查是指在犯罪行为的预备或正在实施时，侦查人员主动利用公共场所视频监控、网络信息与数据的实时监控、通信基本信息监控等监控手段[3]对具有犯罪风险的特定时空与特定人群的数据进行持续性采集，以期发现犯罪线索并在第一时间侦破案件的调查活动，具有事中性、主动性；预测型数据侦查是指在犯罪行为着手或发生之前，侦查人员为了预防犯罪，利用大数据分析技术与风险数据模型对高危犯罪地区进行识别与对高危犯罪人员进行管控等[4]，以测算犯罪行为发生的概率并采取预防性干预措施的调查活动，具有事前性、强主动性。

因此，相较于传统侦查，数据侦查具有由事后启动向事前启动、由被动介入到主动干预、由追诉犯罪到既追诉犯罪也预防犯罪的特点，且在基本权利的干预上也呈现由弱到强的发展趋势。传统的规制手段已经呈现出局限性与滞后性，需要对数据侦查进行与时俱进的规制。

2.2. 数据侦查与个人信息保护的内在张力

对于来源者与所有者的公民而言，信息是其数字人格的具体组成部分，是个人信息权利的客体，具有重要的保护价值；对于使用者的数据侦查机关而言，信息是独立的权力基础，是使权力得以实现和有效运行的能源和催化剂[5]，具有重要的工具价值。信息对于公民和侦查机关不同价值取向，使得数据侦查与个人信息保护之间存在着此消彼长的内在张力：数据侦查的运行逻辑要求尽可能最大化地获取数据以提升犯罪控制力度与事实查明能力，即数据越丰富、维度越多、时效性越强，侦查效能越高；而个人信息保护的根本诉求则要求将数据采集与处理限定在最小范围，即数据越少、留存越短、干预越轻微，权利保障越充分。

数据侦查与个人信息保护之间的角力本质上是侦查权力行使与个人信息权利保障的制衡。个人信息权利是受《中华人民共和国宪法》(后文简称《宪法》)所保护的公民基本权利。《宪法》第 38 条所确立的保障人格尊严的条款，其保护范畴涵盖了“生命、身体、精神以及与个人的生活相关联的权利或利益”[6]，而个人信息与公民的数字生活高度相关，其蕴含了重要的精神性人格价值，其应当构成防御公权力不当干预的坚固屏障。同时，侦查权作为由《宪法》等相关法律授予的国家权力，其行使旨在通过追诉犯罪以实现维护社会政治经济制度的根本目的，当数据侦查权运作时，所获取的承载个人信息的数据的数量和质量直接决定了犯罪控制的效能。于是，权力端追求最大化以提升打击精度，权利端要求最小化以守护人格尊严，构成了数据侦查与个人信息之间难以消弭的内在紧张关系。

3. 数据侦查中个人信息保护的问题检视

3.1. 数据侦查前端：过早启动与过度收集

(1) 数据侦查的过早启动

根据《中华人民共和国刑事诉讼法》(后文简称《刑事诉讼法》)的规定，侦查的启动应当以立案为前提，而是否立案则由侦查机关在管辖范围内主动发现犯罪事实或者犯罪嫌疑人，或由法定主体对报案、控告等材料进行审查而进行决定。因此，侦查应当在犯罪事实发生之后启动，然而，数智技术使侦查具备了与犯罪行为发生同步启动而对犯罪行为进行动态监控，一旦符合算法设定的某种特征就触发侦查行为；甚至早于犯罪行为发生而针对犯罪时空、犯罪人以及被害人进行预测从而介入的能力[7]，即在初查时就利用数据技术开启调查活动。虽然数据侦查启动时点早一定程度推动了对犯罪的控制与治理，但与此同时这种数据侦查导致对个人信息的干预程度，远超其追诉犯罪所能获得的收益。无论监控型数据侦查还是预测型数据侦查，二者的运作原理都存在一定的有罪推定倾向，都先入为主地判定不特定第三人

具有犯罪风险而将相关个人数据进行收集并置于相应的数据模型或算法模型之中，使得公民的个人数据信息在不知情的情况下通过极隐蔽的方式被侦查机关采集并用于是否犯罪的筛漏，对公民的知情权与信息自决权造成极大的侵犯。

(2) 数据侦查的过度收集

在数智时代下，物理行为皆可转化为虚拟数据。因此，犯罪主体的犯罪行为从犯意的产生到犯罪的实施以及犯罪后的逃逸轨迹、涉案财物处置等情况都会通过“天眼工程”“雪亮工程”在实时监控下的信息数据记录、犯罪嫌疑人的通信记录、浏览器搜索记录、银行转账记录等以数据形态体现，只要公安机关对系统内的数据库进行检索或者与拥有数据的第三方企业合作并根据权限对数据进行调取，即可对上述所有信息进行掌握。实践中，侦查人员为了成功追诉犯罪，在海量数据中尽可能多地进行数据挖掘以证明犯罪行为的存在，严重侵害公民个人信息权益。《中华人民共和国个人信息保护法》(后文简称《个人信息保护法》)第 6 条规定，应当限于实现处理目的的最小范围，意味着在数据侦查中，侦查人员收集公民数据信息时不仅要基于收集证据、侦破案件的打击犯罪目的，还要在此目的下根据案件的实际情况对可以佐证犯罪行为确实存在，且符合同一认定理论的数据以对公民影响最小的方式进行收集，而不是超过实现侦破案件或者预防犯罪的目的将能收集到的数据尽数打包。

3.2. 数据侦查中端：主体外溢与深度分析

(1) 数据侦查的主体外溢

我国《刑事诉讼法》第 54 条和 108 条的规定，我国行使侦查权的主体为公安机关和检察机关，其他主体可以依法行使协助义务。在实践中，因互联网企业、网络平台等第三方主体掌握着海量的数据与专业的技术，侦查人员为了节约警力、提高效率，往往会选择与第三方主体达成合作，获得算法等技术支持与服务器及云数据库的访问权限[8]，形成警企协作与第三方技术协助的普遍模式。侦查机关与第三方主体合作显著提高了数据侦查的效率与精准度。然而，一些侦查机关与科技企业或网络平台通过技术外包等合作路径，推动数据的收集、分析甚至决策逾越法律规定的边界，使侦查主体向不具备法定侦查权限的第三方主体扩散[9]。现行法律法规并未对第三方主体的协助范围划定边界，数据侦查权力边界模糊问题使公民个人信息脱离了法定保护框架，且长此以往第三方主体以技术协助之名行侦查权之实将会进一步破坏“权力－权利”的动态平衡，造成公民个人信息权益的进一步克减。

(2) 数据侦查的深度分析

数据侦查的分析阶段以算法为核心，对所采集信息进行更深层次的挖掘与重构。算法的聚合数据关系与拓展数据分析场景的功效，使得无论数据侦查对象的个人信息数据多么繁琐复杂，算法都能够识别行为关联，推断行为规律及动因，进而触及深层隐私。此外，在预测型侦查中，侦查人员将通过理论研究或实证验证的预测因素运用于通过大数据技术收集和处理的大量数据，在算法的支持下获得犯罪的概率或者预期值，并基于此指导侦查行动[10]。该模式忽视了不同案件下实际情况的细微差别，通过极其隐蔽的方式对侦查对象的个人信息进行了深度挖掘与计算，并完成对其人格的数字化解构与预测。马赛克理论(Mosaic theory)从原理层面揭露了犯罪嫌疑人权利保护与科技取证之间的矛盾，并强调信息聚集效应对个人权利带来的不利影响：即便数据侦查过程中所获取的单条信息独立来看无足轻重，但不同平台的数条信息汇聚便能使数据碎片拼接成完整的马赛克图片，以数据精确还原一个人的生活全貌，让公民的隐私几近完全曝光在侦查机关之下，使权力与权利的天平在信息时代严重失衡。

3.3. 数据侦查末端：泄露风险与决策偏差

(1) 数据侦查的泄露风险

在“十四五”规划以及科技兴警战略的指导下，数字技术与公安工作进一步融合，通过建设全国重

点实验室、培育国家技术创新中心、推动地方科技创新平台建设等，科学规划和合理布局公安领域技术创新平台，对警民创新主体有机融合模式进行探索，科技创新平台下的数据资源共享也得以发展，不断提高多元主体参与的侦查协作效率。然而，以与其他行政机关、与网络信息业者以及公安机关内部的共享为主要渠道的数据资源共享[11]推动了海量个人信息的流转，在目前相对滞后的法律规制与技术的黑箱化运作会产生一定的风险：在共享过程中侦查人员、技术辅助人员、系统运维方等多主体均有接触个人信息的权限，数据流转节点繁多，技术的不健全抑或是操作人员的疏漏都可能导致公民个人信息的泄露。在规制方面，并无法律法规对数据共享过程进行程序上的规范与引导；在监督方面，共享主体间除了签订保密协议对行为进行内部监督以外缺乏有效的监督机制。法律规制的缺位内部监督的薄弱难以消弭公民个人信息的泄露风险以及泄露以后对个人信息权益产生的不良影响。

(2) 数据侦查的决策偏差

在数智时代，人工智能与大数据等数字技术深度嵌入侦查之中，并对其运作机制产生影响。在数据侦查广泛使用之前，侦查人员运用经验法则作出决策，决策偏差源于执法经历、性格情绪等个体因素，现代刑事司法则赋予公民的知情权、异议权等诉讼对抗能力予以纠偏[12]。相较之下，数据侦查借助算法将数据置入预先设定的指令与构建好的模型，经数据碰撞后输出分析结果，其决策过程突破了对经验法则的运用和以诉讼对抗能力纠正决策偏误的模式。但数据质量、参数设置等问题可能导致算法偏差，进而固化为自动判定规则，系统性地对特定群体作出过高风险评判，使其在不知情中遭受行踪、消费等敏感信息监控。这种决策偏差扭曲了公民的数字人格呈现，进而可能引发后续错误的法律评价，而此时公民所拥有的围绕个人信息权能的诉讼对抗能力无法进行纠偏。即使《个人信息保护法》第 24 条规定了个人有权拒绝通过自动化决策作出的决定，但在侦查语境下，该条款的适用尚无明确程序通道：当事人既无法知晓算法对其作出的风险评估依据何种特征、权重及逻辑，也无从对错误标签提出异议或要求删除。

4. 数据侦查中个人信息保护存在问题的解决对策

4.1. 限定数据侦查的启动门槛

数据和算法嵌入侦查之后，侦查权的运行形态发生了深刻分化。根据侦查权介入犯罪的时间节点与运行逻辑之不同，前文将数据侦查分为回应型侦查、监控型侦查与预测性侦查三种类型。这三种侦查形态在启动时点与对公民权利的干预程度上存在显著差异，因此，启动门槛的限定亦不能采取“一刀切”的方式，而应当根据干预程度越强，启动门槛越高的原则设定差异化的规则。

第一，针对回应型侦查，应当恪守传统“立案－侦查”的事后启动模式。回应型侦查的启动时点仍在犯罪行为发生之后，本质上仍属于对已发生犯罪的被动回应。数据技术的引入并未改变侦查事后追诉的本质属性，因此也不应降低其启动的门槛，回应型侦查应当继续坚持《刑事诉讼法》的规定，即公安机关先在管辖范围内，审查是否存在犯罪事实需要追究刑事责任而决定是否立案，在立案后则进入侦查程序对案件进行侦破。为了防止立案的虚置，应当强化检察机关的立案控制权[13]。侦查机关立案时应当向检察机关提出申请，并且说明立案后用何种数据侦查措施侦查案件，经批准后才能进行侦查。

第二，针对监控型侦查，应当设定合理怀疑标准并限定监控对象范围。首先，所谓合理怀疑标准，是指基于较为综合性的具体的事实和情况，有相当理由相信某区域、群体或个人存在较高的犯罪概率，例如不仅凭第三方平台预警的购买软件中对与犯罪行为高度相关的物品的搜索记录、浏览器中关于实施某一犯罪行为细节的浏览记录、社交软件中关于存在产生犯罪行为倾向的讨论记录等，而是多条线索综合下的合理怀疑。这一标准低于立案所需的犯罪事实发生的标准，但高于无明确对象的无差别监控。其次，监控对象不应无限扩展，而应围绕合理怀疑所指向的特定区域、特定时段或特定人员展开。具体而

言，应当明确监控的空间范围、时间范围和人员范围，避免将监控手段泛化为日常治理工具。此外，监控过程中一旦发现与初始怀疑无关的信息，应依法予以封存或销毁，不得用作其他用途，并且一旦发现无犯罪嫌疑的人，应当立即停止监控。

第三，针对预测型侦查，应当进行严格的风险评估并限定案件范围。在风险评估方面，预测性侦查依托智能算法模型，对数据集进行深度挖掘，并识别数据间的潜在关联，构建犯罪风险预测模型[14]。由于缺乏完善的运行规则，预测型侦查在启动标准中易违背程序法定原则与无罪推定原则。因此，启动前必须进行严格的风险评估，要求预警所依据的数据模型具备可验证的准确率与较低的误报率，且预警结论须经人工复核，排除单纯算法输出即启动侦查的情形。同时，评估报告应当载明预警所依据的具体数据来源、算法逻辑及风险等级。在案件范围方面，预测型侦查过程中会对不特定对象启动较大范围的信息采集，故为了保护个人信息权益，启动范围应当限缩在社会危险性极大的刑事案件，如危害国家安全犯罪、恐怖活动犯罪、有组织犯罪以及严重暴力犯罪等案件；对于一般性的普通刑事案件，原则上不启动预测性侦查，以发挥其犯罪预防效能的同时，最大限度地减少对公民个人信息权益的过度干预，实现犯罪防控与权利保障之间的平衡。

4.2. 构建梯度化的审查机制

数据侦查对个人信息的处理贯穿收集、存储、使用、传输、分析的全流程，其涉及数据的体量之大、对个人信息权益的干预程度之深，让现有的侦查规制体系暴露出一定的滞后性。《个人信息保护法》虽然对敏感信息进行界定，但其第二章第三节只是抽象地规定了国家机关处理个人信息的规则而未对侦查的边界进行限制，《中华人民共和国数据安全法》第 35 条也未对严格的审批手续进行明确规定。因此，有必要以个人信息分级为基础，构建相应的梯度化侦查与审查机制，使数据侦查在必需的范围和限度内运行。

数据分级是梯度化审查机制构建的逻辑起点。可以依据数据侦查活动对个人信息权益干预的由弱到强将侦查中的数据分为三个层级：第一层级为一般数据，即姓名、联系方式、职业等不涉及个人私密领域的基础身份信息和简单的社会交往信息。这类信息的社会公开程度较高，侦查机关可以通过常规询问、查询公安数据库等途径获得，对公民基本权利的干预程度较低；第二层级为重要数据，即通话记录、交易记录、单独点位的位置数据、网站的浏览记录等数据，这类数据虽未触及敏感隐私，但在聚合后能够揭示个人生活习惯与行为模式，拼凑出较为完整的数字画像，对个人信息权益构成实质性干预；第三层级为敏感数据，即生物识别数据、宗教信仰、通讯内容、金融账户、行踪轨迹、医疗健康等数据，这类数据因涉及人格尊严、人身及财产安全，其对个人信息的干预风险已与技术侦查措施具有同质性，应适用最严格的程序控制。

在数据三级分类的基础上，应建立与之对应的三级审查机制。一般数据的收集适用第一梯度的审查。一般数据对个人权益的干预程度较低，由侦查部门负责人进行形式审查，主要检查法律文书是否正确、履行手续是否齐全、查询范围是否与侦查目的一致；重要数据的收集、分析适用第二梯度的审查。重要数据的收集、分析已经对个人信息权产生了干预，因此审查标准应当相应提升，有县级以上侦查机关负责人进行审批，重点审查调取行为的必要性、所涉信息与案件关联的紧密程度，以及是否存在其他干预程度更低的替代措施；涉及敏感数据的收集、挖掘与分析则适用第三梯度的审查。对涉及敏感数据的收集、挖掘与分析无异于对基本权利的重大干预，应当受到最严厉的控制，即引入检察机关作为外部审查主体。在审查时，检察机关应遵循比例原则，对数据处理的目的正当性、手段必要性、比例相称性等维度进行全面审查，并就是否批准作出书面决定。此外，对于涉及大规模数据分析或预测性侦查的情形，侦查机关还应在申请时一并附上数据算法与分析模型合理性的说明，交由检察机关进行审查。

4.3. 协同运用隐私计算与区块链技术

在数据侦查存在的问题中，权力主体外溢导致除了公权力主体的侦查机关以外，第三方企业也能大范围收集甚至处理公民的个人信息数据；数据的泄露风险导致数据一旦泄露则完全脱离了所有者及储存者的控制；数据错误或缺失导致的算法决策偏差导致公民存在被错误监控并追诉的可能。上述问题都值观地体现了数据侦查中与个人信息相关数据的处理上存在过度“可见也可用”的问题，更体现了追求效率的数据利用与追求安全的数据保护之间的价值冲突。面对这一问题，单纯依靠制度规范难以弥合技术与实践之间的鸿沟，亟需从技术治理层面寻求突破。而隐私计算与区块链技术的协同运用回应了这一迫切需求：区块链技术实现了数据的“可用不可见”，隐私计算技术则实现了数据的“可见不可用”，二者相互协同有望从技术层面解决数据“可用也可见”的问题。

隐私计算是在保护敏感信息隐私安全的前提下完成数据处理与计算的一类技术，其是面向数据采集、传输、存储、处理、共享、销毁等全生命周期中隐私保护的计算理论和方法[15]。隐私计算技术可以在不泄露原始数据的前提下，将数据所有权、管理权和使用权分离，进而完成对数据的分析计算。在侦查方面，运用隐私计算技术的侦查机关无需调取第三方的原始数据，而是通过算法协议进行匿踪查询，或是搭建可信执行环境实现信息查询[16]。隐私计算遵循最小数据原则，其原始数据不出域使得作为查询方的侦查机关在无法获得具体查询对象具体信息的同时只能获得与查询结果直接相关的数据，在保护公民个人信息不被曝光且海量收集的同时收集证据，抓获犯罪嫌疑人。区块链技术则是一种去中心化的分布式账本技术[17]，通过链式数据结构、多节点分布式存储和加密算法，确保上链数据难以篡改的同时做到全程留痕。在数据侦查中，区块链技术能够记录数据从获取、流转到使用的全过程，形成不可更改的审计日志，任何对数据的访问与操作均有迹可循，从而保护公民个人信息相关数据在流转过程中可视化并且被篡改。

隐私计算与区块链的结合，在数据侦查中将会形成“数据可用不可见”与“数据可见不可用”的双重保障。在数据维度，隐私计算消解了企业数据共享的合规顾虑，使侦查机关在不获取原始数据的前提下联合金融、电信、政务等多源异构数据进行融合分析，区块链则为隐私计算的全过程提供留痕保障，确保数据来源明确、流转可视，两者共同纾解了“数据孤岛”困境；在个人信息保护维度，隐私计算通过非对称密码、差分隐私等技术限缩侦查权行使边界，使侦查人员最小化、针对性地获取匿名化处理过的公民数据，坚持最小必要原则在数据侦查中的落实；而区块链技术的透明化、可视化则有助于对数据从查询到流转的全过程与数据提取是否遵循了比例原则进行监督管理，也有助于公民个人信息权益在受到侵害时更加有效地获得救济。

4.4. 落实数据主体的个人信息权利

落实数据主体在个人信息方面的基本权利将会推动公权力运行与私权利保障的进一步平衡。我国《个人信息保护法》第四章规定了个人在个人信息处理活动中具有知情权、查阅权、更正权与删除权等一系列，然而，因为侦查活动的封闭性与在强大国家机关面前公民话语的无力性，使得上述基本权利往往在侦查中被虚置，且经数据技术嵌入后的侦查更因为技术的专业性、算法的黑箱性与数据使用的海量性而导致数据主体的个人信息权益遭受侵害。因此，有必要在数据侦查中落实上述权利，使数据主体能够直接主动地保护、救济自身个人信息权益。

完善数据主体基本权利应当将保障数据主体的事后知情权放在首位。《个人信息保护法》第 35 条规定了国家机关履行法定职责处理个人信息的告知义务，而侦查在追诉犯罪的特殊性使得个人信息保障方面不能侧重事前的知情同意：侦查以查明犯罪事实、查获犯罪嫌疑人为主要目标，如果要求侦查机关在数据侦查时就告知个人信息来源者的公民，在趋利避害心理下犯罪嫌疑人往往选择采取行动逃避打击妨

碍侦查。因此，侦查机关在数据侦查时的告知节点不能在侦查的开端，而是应当在侦查终结或者告知数据主体不妨碍侦办案件时，以书面形式向数据来源者告知其数据被处理的基本情况并获得其本人签字。

落实数据主体的异议权是纠正侦查机关偏误的关键环节。异议权建立在告知权的基础上，即在数据主体被告知其数据被处理并对侦查机关处理数据行为的欠准确性提出质疑后，侦查机关进行审核并作出行动。异议权的行使限制：在申请的范围上，数据主体应就数据侦查中所获取数据是否正确、是否遗漏、是否过时三个方面提出异议；在申请的次数上，对同一事项的异议权请求次数进行限定，使数据主体审慎使用权利；在侦查机关的回应上，申请侦查机关作出相应的更正或补充，侦查机关应进行明确记录并进行审核，若实际情况与申请人所述相符，应当及时进行更改、补充并告知申请人。

保障数据主体的删除权则是落实个人信息基本权利的最终落脚点。删除权的范围不应当仅限于侦查机关主动销毁与案件无关的数据[18]，而是应当进行扩张，让数据主体也能主动行使删除权，具体体现在以下两个方面：一是根据异议的内容请求侦查机关对与真实情况不相符合的数据进行删除，另一方面则是在刑事诉讼程序进行完毕后，请求公安机关对与已结束的刑事案件有关的相关数据进行删除。刑事案件的审判终结意味着侦查机关留存涉案当事人数据的合理期限已经结束，继续留存数据既是对侦查目的正当性的违背，亦是对公民个人信息的侵犯。在案件办理结束后，经数据主体申请与侦查部门程序性审核，不同类别的数据可以分别对待：当事人敏感隐私数据的使用应立即删除，不得留存用于后续使用；而公开数据或者对其他案件有用的数据，则在不妨碍侦查的情况下对申请人进行释明，确保删除权的行使既不过于苛刻，也不流于形式。

5. 结语

在数字技术与侦查的深度融合下，数据侦查已然成为犯罪治理的核心力量。数据侦查以其强大的数据整合能力与智能分析效能，极大地提升了侦查的效率。然而，在数据侦查的过程中，侦查权不断扩张，造成了过早启动、过度收集、主体外溢等显著的问题，使个人信息面临被过度干预甚至侵害的风险。其中显现的问题不仅是技术应用的偶发瑕疵，更是权力规制缺位下的结构性后果。因此，应当着力推动上述问题的解决，即通过差异化的侦查启动门槛、建立梯度化的审查机制以及落实数据主体的基本权利，形成权力控制、技术治理、权利保障的全面规制路径。随着数字技术的持续迭代，数据侦查与个人信息保护之间的张力将长期存在。只有不断在权力行使与权利保障间构建动态平衡，不断优化制度设计与技术治理，才能使数据侦查从悬于公民头顶的达摩克利斯之剑，转化为守护安全与自由并重的法治之盾，真正实现犯罪防控与人权保障的正和博弈。

参考文献

[1] 刘艳红. 数字犯罪的刑事可罚性研究[J]. 浙江大学学报(人文社会科版), 2026, 56(1): 15-31.

[2] 陈亮. 论数据侦查的基本原理[J]. 中国人民公安大学学报(社会科学版), 2025, 41(2): 102-113.

[3] 纵博. 侦查中运用大规模监控的法律规制[J]. 比较法研究, 2018(5): 82-105.

[4] 张全涛. 从被动应对到主动防控: 我国预测性侦查的理论证成与规制选择[J]. 中国人民公安大学学报(社会科学版), 2022, 38(3): 20-31.

[5] 裴炜. 个人信息大数据与刑事正当程序的冲突及其调和[J]. 法学研究, 2018, 40(2): 42-61.

[6] 林来梵. 宪法学讲义[M]. 北京: 清华大学出版社, 2023: 1-496.

[7] 何军. 数据侦查启动时点问题研究[J]. 中国人民公安大学学报(社会科学版), 2023, 39(1): 89-100.

[8] 詹建红. 大数据侦查的行为规制主义路径: 理念检视与规则优化[J]. 当代法学, 2024, 38(6): 16-29.

[9] 詹建红, 李长江. 大数据侦查职权外溢的程序性风险及其规制[J]. 新文科教育研究, 2026(2): 154-170.

[10] 陈永生. 大数据预测警务的运作机理、风险与法律规制[J]. 中国法学, 2024(5): 165-184.

[11] 刘玫, 陈雨楠. 从冲突到融入: 刑事侦查中公民个人信息保护的规则建构[J]. 法治研究, 2021(5): 34-45.
[12] 蒋勇. 大数据侦查中的算法权力构造及其规制路径[J]. 中国人民公安大学学报(社会科学版), 2024, 40(3): 33-42.
[13] 谢佑平. 人工智能时代我国刑事司法改革的双重使命[J]. 政法论丛, 2024(5): 84-98.
[14] 马莉蓉, 张艳. 算法治理视域下预测性侦查的风险防控与程序规制[J]. 贵州警察学院学报, 2026, 38(3): 73-81.
[15] 郑志明, 何积丰, 唐立新, 等. 隐私计算的关键理论与前沿应用[J]. 中国科学基金, 2024, 38(4): 603-611.
[16] 韩关锋, 陈刚. 隐私计算在大数据侦查中的应用研究[J]. 中国人民公安大学学报(社会科学版), 2023, 39(4): 60-69.
[17] 何悦. 区块链电子取证技术的公安应用及法律规制研究[J]. 法治研究, 2024(3): 57-71.
[18] 王仲羊. 行踪轨迹侦查的治理模式转型与制度建构[J]. 公安学研究, 2024, 7(4): 40-57+123-124.