刑事司法科学与治理
Criminal Justice Science & Governance
2025 年 第 6 卷 第 1 期

大数据侦查中个人信息利用与保护的平衡 *

刘琪娇

中南财经政法大学刑事司法学院，武汉

摘　要 | 大数据时代，海量数据为侦查工作提供了前所未有的机遇，但同时也对个人信息保护提出了严峻挑战。如何在有效利用大数据提升侦查效率的同时，保障公民个人信息安全，成为亟待解决的难题。侦查机关利用个人信息可以快速进行身份识别和轨迹追踪、行为模式分析与关系网络构建、犯罪工具溯源与重点人群分析。但全量化收集个人信息、多方主体的介入，以及信息共享对公民的个人信息安全带来了隐患和挑战。法律机制的不健全、技术发展带来的挑战和观念偏差与监督缺失，导致了个人信息保护与利用失衡。因此，必须从立法层面和实践层面加强对个人信息保护，纠正观念偏差，完善法律机制，规制大数据侦查，加强个人信息保护，合理使用新技术与完善监督机制，以期寻求个人信息保护与利用的平衡。

关键词 | 大数据；个人信息利用；个人信息保护；侦查

传统上，犯罪侦查是人力密集型模式，依靠现场勘查、摸底排队、组织辨认等步骤进行，该模式基于侦查人员以往的办案经验，细致分析案件的每一个细微线索。随着网络犯罪和智能化犯罪的日益增多，侦查机关积极拥抱新技术，发展出了一种以数字空间为背景、数据为核心、算法为手段、数据价值追求为目标的大数据侦查新模式。近年来，大数据技术应用的成果日益显著，我国公安部推动的“金盾工程”“天网工程”和“雪亮工程”等大数据平台，为侦查工作提供了强大的技术支持。[1] 然而，机遇与挑战并存，由于大数据侦查缺乏明确的法律规定，导致部分大数据侦查行为陷入“无法可依”的困境。个人信息保护体系尚不完善，在大数据侦查中侵犯个人信息的行为时有发生。与此同时，大数据侦查技术应用的不透明性和广泛性以及侦查人员的观念偏差也加剧了个人信息失控风险。

*基金项目：中南财经政法大学中央高校基本科研业务费专项中研究生科研创新平台项目“大数据侦查中个人信息的利用与保护平衡研究”（202410711）资金资助。

［1］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.

因此，平衡大数据侦查与公民个人信息保护之间的关系，已成为当前法律研究和实践领域亟待解决的重大课题。目前，国内的相关研究对大数据侦查的法律定位尚未形成统一的认识，现有的法律在解释和规制大数据侦查方面存在明显局限。个人信息缺乏系统的保护，监督救济机制也有待完善。对此，学界普遍认为有必要将个人信息权引入刑事诉讼法体系。另外，学者们针对侦查启动的时点、数据收集与处理、监督和救济等多个环节，提出了一系列的举措。这些研究各有侧重，虽取得了一定成果，但未能全面涵盖个人信息在侦查工作中的收集、存储与使用全流程，同时也缺乏对法律理论与侦查实践的深度融合分析。基于此，本文将在现有研究成果的基础上，通过深入解读现行法律规定，系统剖析个人信息在大数据侦查过程中的实际应用问题，构建更加系统化、规范化的个人信息保护机制。

一、大数据侦查中个人信息利用与保护的冲突

个人信息因其社会性和价值性，已成为大数据时代侦查破案的重要线索和依据。通过“互联网＋警务”模式，大量个人信息得以广泛共享，极大地丰富了侦查机关的信息资源。与传统侦查方式相比，通过大数据的侦查手段，围绕信息流进行分析，侦查机关能够更快速、准确地锁定犯罪嫌疑人，揭示犯罪网络，便于应对更加复杂的犯罪行为。然而，多方主体的介入增加了个人信息受侵犯的风险，不仅使犯罪嫌疑人的信息无所遁形，也使得案件之外的第三方的个人信息难以得到有效保护。更为严重的是，“深挖余罪”的侦查行动进一步加剧了这种对个人信息的侵害。[1]

（一）大数据侦查对个人信息的利用

第一，进行身份识别与轨迹追踪。大数据技术的主要优势在于可以通过对散落在不同平台、看似互不相关的个人信息进行关联分析，以达到个人身份的精准识别和行为的全面追踪。它可以帮助侦查机关突破传统侦查手段的局限，从海量的信息中提取出有价值的线索。利用数据挖掘、机器学习等技术，对个人的基本信息与行为轨迹数据进行关联分析，建立个人身份与行为之间的映射关系。例如，将电话号码与地理位置相联系，并与购物记录、互联网行为等数据相结合，能够准确地确定个人的真实身份，同时还原其活动轨迹。在一起网络诈骗案件中，警察通过对受害者的网上通讯记录及交易记录进行分析，确定了犯罪嫌疑人的IP地址和身份信息，并将其抓获。[2]在一起系列命案中，警方通过对案发现场DNA、指纹等信息进行比对，并结合其社会网络、活动轨迹等，最终确定了犯罪嫌疑人，为破案提供了重要依据。

第二，进行行为模式分析与关系网络构建。传统侦查手段往往局限于对单一数据源的分析，而大数据技术可以实现多源数据的融合分析，从而揭示犯罪嫌疑人的行为模式和更深层次的关系网络。通过图数据库、社交网络分析算法（如社区发现算法、中心性分析算法）等技术，分析个人的浏览记录、购买记录等信息，揭示点击、浏览、深度访问网页及登录App等情况。这些信息在侦查中有三大应用场景：一是计算行为频率以挖掘犯罪规律；二是追踪历史事件以重构事件序列；三是挖掘重点人员的网络访问偏好。[3]这有助于侦查机关建立个人标签模型，掌握目标人员的完整网络行为轨迹，了解其生活方式、行为特点以及可能的犯罪动机。此外，将通信记录、社交网络数据、资金往来信息进行关联分析，能够构建出个人的关系网络图。在此基础上，可以进一步分析网络中的关键节点、社区结构、资金流向等信息，发现隐藏在表面之下的关联关系，例如犯罪团伙的组织结构等。这在打击团伙犯罪中发挥着重要的价值。

第三，进行犯罪工具溯源与重点人群分析。随着移动支付和线上购物平台的兴起，用户的消费与交易数据大量集中于互联网平台。通过分析用户的消费行为变化，能够精准锁定可疑交易，追溯犯罪线索。例如，在恐怖袭击案件中，美国警方曾成功利用商业机构的交易记录，以涉案物品为线索，缩

［1］罗亚文．冲突与协调：侦查阶段隐私权保障研究［J］．重庆社会科学，2022（9）：117–128.

［2］平安舟曲．舟曲县公安局刑警大队成功破获一起电信诈骗案［EB/OL］．［2025–03–14］．https://mp.weixin.qq.com/s/DVcx5mbQSTq21X6tw4xLtA.

［3］商瀑，李亚可，郭楼禄．基于用户画像技术的大数据侦查：一个框架的分析与设计［J］．中国人民公安大学学报（社会科学版），2022，38（3）：32–43.

小了侦查范围。[1]如今，用户在移动设备上的每一次点击都生成了消费数据，清晰地勾勒出重点人员的网购历史，这为查明犯罪工具的属性与成分，判断其与案件的关联程度，并挖掘上游犯罪提供了重要线索。同时，针对涉毒、涉网、涉药等犯罪活动，由于犯罪团伙成员之间通过社交行为和言语互动形成稳定的联系，通过结合个人的基本信息和社交互动数据，侦查机关能够推断用户所在社群的自然属性，进而挖掘出犯罪团伙。例如，在网络贩毒案件中，侦查机关通过对微信用户的数据画像，成功锁定了涉嫌贩毒的重点人员，并最终查获了同案犯。[2]此外，通过分析社交媒体的语音留言等互动数据，多国刑事执法机构也成功刻画了发帖群体的用户画像，锁定了重大可疑人员。[3]

（二）大数据侦查与个人信息保护的冲突

尽管依托大数据侦查的模式，对公民的个人信息进行分析，可以帮助侦查机关快速锁定犯罪嫌疑人，打击犯罪，但大数据技术对个人信息的收集和利用无疑会引发一系列问题，不可避免地会对这些个人信息造成侵犯。大数据侦查所赖以生存的信息库越完备，越会加剧个人信息被侵犯的风险。

首先，全量化收集个人信息模糊了侦查机关的权力边界。侦查机关作为打击犯罪的重要力量，其获取数据信息的行为本应在法律的严格约束下进行。然而，放眼当前各国的刑事司法实践，侦查机关在获取数据信息方面已不再局限于特定案件的犯罪嫌疑人。无论是与案件直接相关还是间接相关，甚至是与案件毫无关联的个人信息，都可能被纳入收集范围。这种做法不仅违背了个人信息保护的基本原则，也超出了侦查机关应有的权力界限。例如，在对犯罪嫌疑人的住所进行搜查时，这一行为不仅直接针对犯罪嫌疑人本人，而且不可避免地会波及其家庭成员的私人物品。[4]因为住所作为一个生活共同体，其内部空间及存放的物品往往难以清晰界定属于哪一位具体成员。当侦查手段进步到大数据侦查领域，情况就变得更加错综复杂。特别是在预测性大数据侦查阶段，侦查机关为了更有效地提前预防高危犯罪类型、精准锁定高危犯罪人员或及时保护可能处于危险中的被害人，开始广泛利用先进的大数据分析技术，对不特定的大量人群进行全面而深入的数据监测。[5]这种监测不再局限于传统侦查手段中的特定嫌疑人或案件相关线索，而是将视野拓宽至整个社会层面，通过收集、整合和分析海量的个人信息数据，试图从中发现潜在的犯罪风险点和异常行为模式。其覆盖范围之广、数据处理量之大，使得每一个人，无论是否与案件直接相关，都可能被纳入数据分析的范畴，进而在大数据系统中留下痕迹，形成个人数据档案和数据画像。这种广泛的数据收集和分析，虽然有助于提升侦查效率，但也引发了关于个人信息和数据安全的广泛担忧。

其次，多方主体收集个人信息引发全景式监控危机。大数据侦查背景下，数据收集主体由传统的侦查机构拓展至政府部门、网络企业和第三方数据提供商。由于各机构所掌握的数据来源及数据处理方式各不相同，因而大大拓展了数据搜集的范围与深度。但是，由于各主体在信息采集、存储和使用上的标准与规则不尽相同，有的甚至会出现漏洞，给了全景式监控以可乘之机。例如，在电信诈骗案件中，侦查人员在对电信诈骗犯罪进行打击的过程中，可以从电信网络运营商那里获得数据资料，包括通话记录、短信内容、位置信息等，来追踪犯罪嫌疑人的活动轨迹，并锁定犯罪嫌疑人。但是，一旦犯罪嫌疑人的身份曝光，就会引起强烈的社会反

---

［1］［美］埃里克·西格尔．大数据预测——告诉你谁会点击、购买、死去或撒谎［M］．北京：中信出版社，2014：62.

［2］平安广西网．微信朋友圈发暗语，民警破译缉毒贩［EB/OL］．（2020-07-28）［2025-03-14］．https://chaxun.pagx.cn/news.html?aid=39984.

［3］Khelif K，Mombrun Y，Backfried G，et al. Towards a Breakthrough Speaker Identification Approach for Law Enforcement Agencies：SIIP［C］//European Intelligence & Security Informatics Conference．IEEE Computer Society，2017：32-39.

［4］张全涛．大数据时代侦查机关获取公民数据信息的权力边界与实践规制研究［J］．中国人民公安大学学报（社会科学版），2023，39（3）：30-44.

［5］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.

响。一些民众基于对犯罪的愤怒、对犯罪嫌疑人的不满，自发地进行“人肉搜索”，利用已曝光的个人信息，快速挖掘、传播更多的个人隐私信息。在此过程中，不但犯罪嫌疑人的个人隐私会被毫不留情地曝光，甚至会波及与之有关的无辜者，大量的私密、敏感的个人信息被大肆散布，个人信息的安全性遭受了前所未有的侵犯。此外，在视频大数据侦查的场景中，摄像头作为重要的侦查工具，被广泛应用于公共场所和关键区域，以捕捉犯罪嫌疑人的行踪。然而，基于视频图像侦查的基本原理，摄像头在捕捉犯罪嫌疑人的同时，也会记录并分析监控范围内的所有人员活动。这意味着，即使案外第三人并未涉及案件，只要他们处于摄像头的监控之下，就有可能被扫描、识别和分析。这种无差别的数据收集方式，虽然有助于侦查机关快速锁定目标，但也对公众的个人信息构成了潜在威胁。

最后，侦查机关与其他主体的信息共享引发个人信息泄露风险。大数据战略的深入实施对刑事侦查工作产生了深远影响，侦查机关正在积极整合高质量的数据资源，加速推进数据的整合和共享。这一举措主要通过三大途径展开：一是与其他行政机关的数据互联互通，二是与网络信息服务企业的信息共享，三是公安机关内部的数据资源共享。[1] 首先，侦查机关在办案过程中，往往需要获取嫌疑人的各类信息，这些信息可能分散在工商、税务、银行、通信、房地产等多个行政机关的数据库中。要实现高效侦查，侦查机关就需要与这些行政机关建立信息互联互通机制。然而，由于不同行政机关的数据信息系统在安全标准、存储方式和加密方式等方面存在差异，大量信息在跨部门传输中容易出现安全漏洞，增加个人信息泄露的风险。其次，随着互联网的普及，公民的个人信息很容易被网络信息服务企业所掌握。侦查机关在办案过程中，有时需要借助这些企业的数据信息来追踪嫌疑人的行踪、分析嫌疑人的社交关系等。但这种信息共享也存在着风险。一方面，这些网络信息服务企业的数据安全保障方面存在漏洞，容易导致信息泄露；另一方面，侦查机关收集和使用这些信息的过程中如果未严格按照相关规定进行操作，也可能侵犯公民的隐私。最后，侦查机关内部的数据资源共享虽然是提高侦查效率的重要手段，但如果缺乏完善的内部数据共享机制，也可能导致个人信息泄露。例如，如果不同级别、不同区域的侦查部门之间的数据共享程度低，侦查人员可能需要通过繁琐的手续才能获取所需数据，这不仅降低了侦查效率，还可能因为复杂的流程导致数据泄露。此外，如果数据系统存在权限设置不合理、安全防护措施不到位等问题，也可能被不法分子利用，导致数据泄露。

二、大数据侦查中个人信息利用与保护失衡的原因

个人信息的挖掘与分析，作为大数据侦查的重要手段，在精准锁定犯罪嫌疑人、推动案件的快速侦破方面发挥着重要作用。然而，侦查机关在实践中往往倾向于过度采集并利用个人信息，为了达到破案的目的，有时甚至会超越法律的界限，冒着侵犯公民个人信息的风险。出现这种情况，有以下几个方面的原因。

（一）重个人信息利用而轻保护的观念偏差

部分侦查机关在开展大数据侦查时，过于追求侦查效率，而忽视了对个人信息的保护。这种“效率优先”的观念导致实践中存在过度收集和滥用数据的现象。基于对公共利益的追求，公权力机关凭借其强制力履行惩治犯罪的职责。然而，权力的每一次行使，皆会在公民权利的范畴内产生或积极或消极的影响。大数据侦查的实施最大可能是对公民个人信息的侵害。[2] 一方面，现行法律对个人信息保护的规定尚不完善，相关保护措施也未能形成有效体系。对于大数据侦查行为的法律规范较为模糊和宽泛，缺乏具体的操作标准和明确的限制条件，这在一定程度上为侦查人员留下了较大的自由裁量空间。另一方面，侦查人员在办案过程中，往往会把重点放在寻找线索、搜集证据上，而忽略了对公民个人信息的合理保护。

部分侦查人员可能存在缺乏必要法律素养和专业知识的问题，对个人信息保护的相关法律法规不够熟悉，导致在实务中难以做到依法依规办案。例如，在对经济犯罪案件进行侦查时，往往会利用大

［1］胡锦涛．公安机关侦查工作中公民个人信息保护问题研究［D］．北京：中国人民公安大学，2022.

［2］洪刚．信息网络犯罪技术侦查的法律控制［J］．中国应用法学，2022（1）：135–150.

数据平台，广泛搜集与案件相关的各类信息，以便快速地锁定犯罪嫌疑人的资金流动及交易网络。部分侦查人员可能会采取“撒网式”的数据收集，这种方式不仅会搜集犯罪嫌疑人的交易记录、车辆信息、出行轨迹等直接相关信息，还可能不慎将与其有业务往来但并未涉案的第三方企业的财务信息、员工个人信息、客户资料等敏感数据一并纳入收集范围。更为严重的是，个别警务人员超范围调阅嫌疑人的个人信息，甚至有极少数人违法出售这些信息以牟取私利。抑或是未对调取的电子数据进行加密存储，导致大量公民个人信息被黑客窃取并公开售卖。这种重个人信息利用而轻保护的观念偏差，使得个人信息保护在侦查过程中被边缘化，进一步加剧了利用与保护的失衡。

（二）大数据侦查法律规制的缺失

首先，现行法律对大数据侦查的定位和规范存在明显空白。《刑事诉讼法》虽然规定了传统侦查措施，如证据收集调取、勘验检查和技术侦查，但并未将大数据侦查明确列为一种独立的侦查手段。[1]大数据侦查涉及对海量数据的收集、分析和挖掘，其技术性和复杂性远超传统侦查方式，然而法律未能针对这些新型侦查行为制定专门的程序规范，导致实践中缺乏明确的法律依据和操作指引。

其次，大数据侦查程序有待建立健全。大数据侦查因其涉及对个人信息的深度挖掘与分析，以及对数据资源的广泛利用，更接近于强制性侦查措施的特征，理应将大数据侦查归类为一种强制性侦查手段。[2]程序法定原则要求强制性侦查措施的类型、适用范围和执行流程必须由法律明确规定，但大数据侦查的审批程序、数据使用范围及期限等关键环节缺乏具体规定，使得侦查机关在操作中容易过度扩张权力，侵犯公民个人信息权利。

此外，技术侦查与大数据侦查高度相似，二者在实践中已结合。例如，《电子数据规定》第9条明确指出，在进行网络远程勘验时，若需要采取技术侦查措施，应当依法经过严格的批准手续。[3]这一规定体现了对技术侦查措施适用的严谨态度和对公民个人信息的慎重保护。然而，值得注意的是，尽管技术侦查在刑诉法及配套规定中有所体现，但对于大数据侦查这一新兴侦查手段，相关法律并未明确其具体范畴和归属，刑诉法及配套规定并未清晰界定哪些大数据侦查措施应当被视为技术侦查的范畴，这导致技术侦查与大数据侦查在实践中的界限变得模糊不清，实践中存在规避严格审批程序的现象。这种法律规制的滞后性和不完善性，是大数据侦查与个人信息保护之间冲突难以有效调和的关键因素。

（三）个人信息系统保护的缺位

首先，个人信息权未明确，法律适用模糊。我国法律体系中，个人信息权尚未作为一项独立的权利得到专项立法确认。尽管《民法典》和《个人信息保护法》对个人信息保护作出了一些规定，但这些规定更多是原则性的，缺乏对个人信息权的明确定义和权利边界的清晰划分。实践中，个人信息权常与隐私权、名誉权等概念混淆使用，导致法律适用模糊。这种混淆使得个人信息保护的范围和力度受到限制。与此同时，公法和私法对个人信息保护均存在不足，公法侧重于对公权力的制约，但在大数据侦查中，侦查机关的权力缺乏有效约束；私法则侧重于民事权益的保护，但难以应对公权力对个人信息的侵害。这种双重不足使得个人信息保护缺乏系统性和针对性。

其次，有关个人信息保护的立法分散且保护力度不足。虽然《数据安全法》和《个人信息保护法》从宏观层面对个人信息保护作出了原则性规定，但这些法律并未针对大数据侦查中的特殊情境提出具体规则。[4]例如，《个人信息保护法》第34条虽然规定国家机关处理个人信息需遵循法定权限和程序，但未明确大数据侦查中数据收集、分析

---

［1］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.

［2］胡铭，龚中航．大数据侦查的基本定位与法律规制［J］．浙江社会科学，2019（12）：12–20+155.

［3］《关于电子数据收集提取判断的规定》第9条规定：“为进一步查明有关情况，必要时，可以对远程计算机信息系统进行网络远程勘验。进行网络远程勘验，需要采取技术侦查措施的，应当依法经过严格的批准手续。”

［4］黎晓露．个人信息权引入刑事诉讼的理论证成与体系化建构［J］．河北法学，2021，39（12）：139–155.

和使用的具体限制。[1]在刑事司法领域，相关法律和规范性文件零散且效力有限。《刑事诉讼法》中关于个人信息保护的条款（如第64条对证人、被害人个人信息的保密义务）多为原则性规定，缺乏具体的操作细则，导致在实践中难以落实，且《刑事诉讼法》仅规定了证人、鉴定人、被害人等特定人员的个人信息保护措施，但对被追诉人的个人信息保护却未提及。此外，《公安机关办理刑事案件程序规定》虽然对证据收集调取行为进行了规范，但未对大数据侦查中的数据挖掘和分析行为设定明确的限制[2]，导致侦查机关在实践中可能过度扩张权力。

最后，个人信息救济途径匮乏。“公民自由的本质确切无疑地存在于每个人在遭到侵害时能够获得法律保护的权利。”[3]大数据侦查目前尚处于发展阶段，相关的法律法规和救济措施尚不健全，因此在保护个人信息方面往往显得力不从心。目前我国对违法侦查的救济主要通过追究刑事责任、进行国家赔偿和非法证据排除来实现，但这些手段的有效实施依赖于违法侦查行为的准确识别。然而，在大数据侦查中，个人往往难以有效识别自身的权利是否受到违法侦查的侵害。同时，由于法律尚未明确确立公民的个人信息权，大数据侦查又游离于法定侦查措施之外，公民在寻求权利救济之时，往往陷入“权无所依，法无可循”的困境之中。即便公民意识到自己的个人信息受到侵犯，并尝试依据《中华人民共和国国家赔偿法》来申请赔偿，也会因该法律中缺乏针对大数据侦查侵权的具体赔偿条款而难以获得应有的赔偿。事实上，相比于向法院提起诉讼寻求救济，被侵害人更倾向于向检察机关提出申诉，但这一途径同样存在问题。例如，只有当侦查机关在大数据侦查过程中，非法获取并滥用公民个人信息，且此情节严重到构成犯罪的程度时，才能对相关责任人员进行刑事追究，并且定罪的范围往往仅限于非法获取、出售或者提供个人信息的明确行为。而对于那些在大数据侦查中，因操作不规范、监管不到位导致的不当收集、过度使用或者疏忽泄露个人信息等行为，虽然也对公民的个人信息安全造成了侵害，但由于法律规定的局限性，这些行为往往难以被追究刑事责任，只能由相关部门给予警告、责令限期整改等相对较轻的处罚措施。[4]此外，非法证据排除规则的适用范围狭小，程序制裁作用有限。法律救济途径的不足，使得大数据侦查中个人信息利用行为更加肆无忌惮。

（四）技术发展带来的挑战

第一，数据挖掘技术扩张个人信息收集范围。数据挖掘是一种运用先进的计算技术和算法，对大规模数据集进行深度探索和分析的过程。通过挖掘数据背后的隐藏模式、关联关系和潜在规律，能够揭示出数据所蕴含的有价值信息，为决策制定提供科学依据。数据挖掘主要涵盖三种情形：一是“无中生有”，即从数据中发掘出犯罪线索；二是数据画像，通过数据分析构建出详细的特征描述；三是犯罪预测，利用数据模型对犯罪行为进行预判。[5]目前，数据挖掘技术对于大量情报的获取提供了有力的支持，最大程度发挥了数据的有效

［1］《个人信息保护法》第34条规定：“国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度。”

［2］《公安机关办理刑事案件程序规定》第62条规定：“公安机关向有关单位和个人调取证据，应当经办案部门负责人批准，开具调取证据通知书，明确调取的证据和提供时限。被调取单位及其经办人、持有证据的个人应当在通知书上盖章或者签名，拒绝盖章或者签名的，公安机关应当注明。必要时，应当采用录音录像方式固定证据内容及取证过程。”第63条规定：“公安机关接受或者依法调取的行政机关在行政执法和查办案件过程中收集的物证、书证、视听资料、电子数据、鉴定意见、勘验笔录、检查笔录等证据材料，经公安机关审查符合法定要求的，可以作为证据使用。”

［3］［美］吉尔贝·希纳尔．杰斐逊评传［M］．王丽华，等译．中国社会科学出版社，1987.

［4］王长杰．大数据侦查与个人隐私信息保护平衡问题研究［J］．中国人民警察大学学报，2022，38（9）：55–62.

［5］何军．数据侦查行为的法律性质及规制路径研究［J］．中国人民公安大学学报（社会科学版），2021，37（1）：78–85.

性。[1]但是，由于案件相关信息与无关信息的区分难度较大，数据挖掘技术的广泛应用，使得侦查机关在收集数据时容易过度扩张范围，将大量与案件无关的个人信息纳入侦查范围。“无中生有”侦查，作为一种非常规的侦查手段，其启动并不受犯罪事实条件的严格制约。这种侦查方式往往基于一种预设的假设或疑虑，而非确凿的犯罪事实。因此，在实施过程中极易跨越合法的界限，对公民的信息权构成不当侵犯。数据画像技术能够整合分析海量数据，勾勒出侦查相对人的详细轮廓，使得其在大数据侦查的视野下变得如同透明人一般，毫无隐私可言。犯罪预测也并非万无一失，它存在着概率性错误的风险，可能将无辜者错误地判定为潜在犯罪嫌疑人。此外，犯罪预测还可能受到模式化偏见的影响，导致对某些特定群体或个体的歧视性对待。这些都对公民的个人信息权利带来了威胁。

第二，算法黑箱掩盖侵犯个人信息行为。算法在大数据侦查从传统数据查询比对向智能化数据整合与挖掘的转型过程中起到了至关重要的作用，它推动了大数据侦查迈向智能化侦查预警、全方位监控与精准决策的新阶段。但是，算法以其强大的计算分析能力和不为公众所知的决策机制会给公众的个人信息带来隐患，首当其冲的就是算法可能存在违规收集个人信息的情形。算法决策与其他非算法自动化决策的本质区别在于其机器自主性。这种自主性体现在机器能够在无人类直接干预的情况下，依据周围环境信息或其他相关数据自主做出选择与决策。这种能力不仅限于执行固定算法或机械运算，而是指机器程序能够自我学习、优化，甚至生成并演化出独特算法来应对各种情况。[2]由于缺乏透明性和公开性，算法的运行呈现出“技术黑箱”的特征。[3]算法黑箱的存在对个人权利的行使施加了一道屏障，其将决策权置于技术复杂性构建的不透明领域。侦查机关和个人信息主体对算法决策过程缺乏了解，导致他们在信息获取和决策判断能力上处于劣势，难以有效应对算法黑箱带来的风险。如果个人无法知晓其信息被侵犯的事实，也就无法及时采取积极措施维护自身权利。个人权利的逐渐退却为算法决策权的肆意扩张提供了空间。此外，算法决策系统的研发与构建过程中需要多方参与，尤其是私营机构的加入，使得公共机构对决策系统的掌控能力受到严重限制，增加了算法决策权滥用的风险。若一些私营机构为了追逐私利，在算法技术中植入特定程序，导致个人信息流向市场，被不良资本利用，公共机构也难以知悉。

（五）大数据侦查监督制约力度不够

大数据侦查具有主动性和强制性，为避免其过度蚕食公民的个人信息权益，理当受到严密且有效的监督与约束。然而，在当前既有的程序监管体系下，大数据侦查的运用却面临监督缺失的困境。首要问题在于内部控制机制的虚化。尽管外力监督被视为保障算法决策公正性和透明度的重要手段，但内部控制作为防范内部风险的第一道防线，其重要性同样不容忽视。我国侦查机关通过内部职能划分和层级管理实施内部控制，试图为算法决策筑起一道监督之网，但这一体系存在根本性缺陷。职能划分上，侦查人员既为“运动员”，又兼“裁判员”，此双重身份之下，出于维护部门利益的考虑，对监督对象在个人信息采集与运用中的违法行为，或视而不见，或纵容其行，这明显与权力控制的初衷背道而驰。[4]层级管理上，信息的纵向传递存在诸多障碍，如信息失真、传递延迟等问题频发，影响上级监督的时效性和有效性。同时，外部监督的效能也显得力不从心。在检察监督方面，目前主要采用被动监督模式，即依赖侦查机关主动提供线索或案件，这大大限制了检察监督的主动性和全面性。由于线索来源有限，检察监督难以构建起全面有效的监督体系。此外，传统的案卷审查方式在处理智能化、网络化的侦查行为时显得捉襟见肘，效率低下。更为严重的是，侦查机关可能并未将大数据侦查活动的全过程记录入案卷，导致这类侦查行为无法受到检察监督，成为监督的“盲

［1］王玉清．大数据背景下数据挖掘技术在公安侦查中的应用［J］．科技传播，2019，11（2）：127–128.

［2］彭诚信，［美］瑞恩·卡洛，迈克尔·弗鲁姆金，等．人工智能与法律的对话［M］．陈吉栋，等译．上海人民出版社，2018.

［3］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.

［4］詹建红，张威．我国侦查权的程序性控制［J］．法学研究，2015，37（3）：139–157.

区”。[1]至于司法监督，法律未赋予法院司法审查的权力，加之面临着算法决策专业性和复杂性挑战，以及司法资源有限性制约，使得许多违法侦查行为难以及时得到纠正和制裁。而且，大数据侦查活动通常发生在审判程序之前，法院难以对其进行直接及时的监督。

三、大数据侦查中个人信息利用与保护平衡的进路

在大数据侦查中，由于数据分析不可避免地会对个人信息进行过度收集和挖掘，保护个人信息已经成为社会共识，其重要性毋庸置疑。然而，鉴于个人信息既具有公共属性又包含个人属性，因此在尝试加强对个人信息保护时，不可避免地会遇到一系列障碍与挑战。本文将从以下几个方面加强对大数据侦查中的个人信息保护，以期寻求个人信息利用与保护的平衡。

（一）树立个人信息利用与保护并重理念

在侦查工作中，个人信息保护与侦查效率往往存在一定的冲突。为了平衡这两者，侦查机关应树立“个人信息利用与保护并重”的理念。此外，大数据侦查行为有效控制的关键在于培养侦查人员的法治思维，在选任和培养过程中，除注重技术能力外，还需强化责任意识。[2]第一，侦查机关可以通过定期的培训和教育活动，更新侦查人员的法治观念，提升职业操守，并加深对个人信息保护法律法规的认识和重视程度，使其在工作中自觉遵守相关规定。第二，在内部侦查办案规定中，需明确并强化个人信息保护措施，将个人信息利用与保护置于同等重要地位，细化侦查人员在收集、使用、存储和销毁个人信息过程中的具体要求和操作流程。同时，建立严格的大数据侦查滥用惩罚机制，根据侵权行为的严重程度实施分层次惩处。通过制度性约束，规范侦查人员行为，促使他们树立个人信息保护意识，从源头上减少个人信息滥用风险。第三，为了进一步强化个人信息保护的重要性，侦查机关的绩效考核体系应引入双重标准。除了传统的破案效率指标外，还应将个人信息保护作为重要的考核指标之一。对于违反规定的侦查人员或部门，在绩效考核中予以体现，从而激励侦查人员更加重视个人信息保护。

（二）明确大数据侦查的法律定位与程序规范。

首先，通过修订刑事程序法来构建一套完善的大数据侦查规范体系。基于程序合法性的严格要求，刑事诉讼法中的侦查措施部分应明确纳入大数据侦查的相关内容，具体指出侦查机关在依法履行侦查职责的过程中，利用先进的信息技术手段，对各类数据库进行深度的数据查询、精准的比对分析、智能的挖掘处理以及必要的信息共享等行为，均应当被视为大数据侦查的重要范畴。[3]当侦查机关计划采用大数据侦查手段时，必须遵循大数据侦查的特定程序规范，确保操作的合法性与合理性。

其次，整合立法资源，强化个人信息保护。在《数据安全法》和《个人信息保护法》的基础上，针对大数据侦查的独特性和复杂性，有必要制定专门的法律或规范性文件，以全面、具体地规范大数据侦查中的数据收集、分析和使用行为。修订《刑事诉讼法》，增加对个人信息保护的具体操作细则，明确侦查机关在数据收集、存储和使用中的义务和责任。在《公安机关办理刑事案件程序规定》等规范性文件中，增加对大数据侦查中数据挖掘和分析行为的明确限制，防止权力过度扩张。

最后，规定大数据侦查区别于普通侦查措施的应用范围和程序规范。目前，我国《刑事诉讼法》等相关法律尚未对大数据侦查作出明确规定。尽管《关于电子数据取证的若干规定》以及《电子数据取证规则》从电子数据取证的视角对大数据侦查进行了规范，但仍需在《刑事诉讼法》的侦查体系中进行具体规定和细化。例如，对于大数据侦查中涉及的侦查措施，应根据其性质和强度进行分类管理。对于数据收集和挖掘力度大、性质明显的侦查行为，应明确规定为强制性侦查措施，规定其适用条件和程序要求。而对于侦查强度一般或需根据具

[1] 李小猛．大数据赋能侦查监督的进路与反思[J]．华东政法大学学报，2023，26（5）：32–44.

[2] 于阳，魏俊斌．冲突与弥合：大数据侦查监控模式下的个人信息保护[J]．情报杂志，2018，37（12）：147–155.

[3] 卞建林，钱程．大数据侦查的适用限度与程序规制[J]．贵州社会科学，2022（3）：78–86.

体情境判断其性质和强度的侦查措施，则应建立相应的审查判断机制，必要时可引入专家辅助判断。对于违反程序规定的行为，应明确相应的法律责任，并为侦查对象提供充分的法律救济途径。[1]遵循比例原则的目的正当性要求，大数据侦查应当被严格限制在应对重大犯罪案件的范畴内，对此可以参照技术侦查措施的相关规定和适用范围。同时，实施大数据侦查还需满足必要性条件，即在穷尽所有其他可行的侦查手段，且确认这些手段对公民基本权利的侵害程度较低或不存在侵害的情况下，方可考虑启动大数据侦查。对大数据侦查要设立更为严格的审批标准和证明标准，并签发专门的令状，根据案件严重程度的不同，明确相应的侦查措施、侦查范围及侦查期限，以确保侦查行为的针对性和适当性。[2]此外，还需设立紧急情况下的例外规则。若侦查人员有合理理由认为，若不立即获取相关数据或启动大数据侦查，可能导致证据灭失或其他严重后果，应允许其在未取得令状的情况下先行采取紧急侦查措施。事后，侦查人员需提供详细的办案经过说明，并补充申请相关令状，以确保程序的合法性和完整性。

（三）构建大数据侦查中个人信息保护机制

首先，将个人信息权引入刑事诉讼领域。“在我国强职权主义诉讼模式下，法律赋予公安司法机关收集使用个人信息的强大权力，以至于‘权利—权力’关系呈现出一种跛脚的状态。”[3]大数据时代，个人信息保护已成为共识，但个人信息兼具公共与个人属性，权利化保护面临挑战。将个人信息权引入刑事诉讼需遵循刑事诉讼制度原理，平衡权利保障与犯罪控制的价值，实现与相关法律的制度衔接，并重视规则调整。第一，要遵循公共利益优先原则和比例原则。刑事诉讼以维护公共利益为首要价值，必要时可合法干预个人信息权，但信息主体需承担容忍义务。另外，个人信息的利用必须符合刑事诉讼的目的，且应当采取对个人信息权益影响最小的必要手段进行。第二，在个人信息权的具体构造上，要赋予信息主体权利，施加信息处理者义务。“调整信息主体与信息处理者之间关系的根本目的在于合理地配置权利义务，进而恰当地分配利益，从而最终达到保护个人信息安全的目的。”[4]信息主体应当享有受合理限制的知情权、信息访问权以及更正、删除、限制处理权等，以达到对公权力进行制约的目的。相应地，信息处理者应当履行告知、配合义务和信息安全保护义务，确保个人信息安全。第三，应当建立个人信息权利保障机制。包括建立多元化监督体系，综合运用内部审批和司法审查，对信息收集处理过程进行全方位把控，推动程序正当化。《个人信息保护法》赋予了个人在个人信息处理活动中享有知情权、自决权、删除权、更正权等权利，但这些权利在大数据侦查中尚未得到确证，理应在《刑事诉讼法》和《中华人民共和国人民警察法》等法律规范中构建个人信息权利体系。[5]

其次，区分个人信息类型进行分层保护。“个人信息保护的逻辑起点在于使用，关注点并非是否为他人知晓，而是是否为他人正当、合理地收集、使用。”[6]在这一框架下，将个人信息进一步分为“一般信息”和“敏感信息”予以分别保护，能更好地平衡大数据侦查与个人信息保护。“一般信息”不直接涉及个人隐私或财产安全。例如，姓名、电话号码、电子邮件地址等。虽然这些信息也可能被用于不正当目的，但其风险相对较低。对其应采取基本的保护措施，如设置密码、定期更新等。在大数据侦查中，应尽量避免过度收集或使用一般信息，以减少不必要的风险。对于已经收集的一般信息，应妥善保管，并确保其不被非法获取或

---

［1］何军．数据侦查行为的法律性质及规制路径研究［J］．中国人民公安大学学报（社会科学版），2021，37（1）：78–85.

［2］张晶．大数据侦查中的信息隐私权保护［J］．北京航空航天大学学报（社会科学版），2023，36（6）：57–69，79.

［3］郑曦．作为刑事诉讼权利的个人信息权［J］．政法论坛，2020，38（5）：133–144.

［4］赵祖斌．从静态到动态：场景理论下的个人信息保护［J］．科学与社会，2021，11（4）：98–116.

［5］赵祖斌．在合理范围内处理：大数据侦查中个人信息保护与利用的平衡［J］．中国海商法研究，2025，36（1）：56–65.

［6］裴炜．论个人信息的刑事调取——以网络信息业者协助刑事侦查为视角［J］．法律科学（西北政法大学学报），2021，39（3）：80–95.

滥用。“敏感”在英文中的含义之一是“高度反应或易受影响”[1]，这也就决定了敏感信息需要得到更大程度的保护。以欧盟的《通用数据保护条例》（GDPR）为例，该条例规定了当处理特殊类别的个人数据（即敏感数据，如种族、民族、政治观点、宗教或哲学信仰、工会会员身份、基因数据、生物特征识别数据、健康数据、性生活或性取向等）时，数据控制者（即负责处理个人数据的一方）不仅需要证明其处理活动的合法性（例如基于数据主体的明确同意、履行合同义务、履行法定义务等），还必须采取额外的安全保障措施来确保这些敏感数据的安全。[2]“敏感信息”之所以被视为敏感，并非因为其私密性或个体不愿公开，而是源于在收集与处理这些信息时，必须采取更为严格的审慎态度，以防止一旦泄露可能对个人重要权益造成的侵害。因此，保护个人信息，尤其是敏感信息，关键在于确保它们在整个周期内得到合法、恰当的处理与利用。在大数据侦查中，除非有明确的法律授权和充分的理由，否则不得随意获取或使用敏感信息。在收集这类敏感信息的过程中，要遵循严格的数据接入制度的隐私保障和数据调取制度的程序审批规范。[3]

最后，构建侵犯个人信息的救济机制。一方面，完善侵犯个人信息的惩戒机制。在现行法律的框架下，应制定多样化的惩戒措施和完善程序性惩罚机制，以便更有效地打击侵犯个人信息的违法行为，保护公民的个人信息安全。轻微行为应进行内部纪律处罚，严重行为应追究刑事责任，特别严重案件可采取“从业禁止”措施。[4]在处理个人信息侵权案件时，公安机关应承担证明侦查行为合法性的责任。另一方面，增加个人信息受侵犯的救济途径。“无救济则无权利”，在刑事侦查中，应明确救济机制，保障不同诉讼参与人的救济权利，如复议申请等。由于大数据侦查行为的广泛性和隐蔽性，应完善大数据环境下的代表人诉讼制度。允许个人信息保护机构代表受侵害者参与诉讼，保障个人信息权利，并建立更完善的国家赔偿制度，增加关于大数据侦查侵犯个人信息的具体赔偿规定，明确赔偿标准、程序和范围，确保被侵害人能够获得相应的赔偿。拓宽非法证据排除规则的适用范围，将大数据侦查中获取的非法证据也纳入排除范围，增强程序制裁的作用。此外，建立更加便捷、高效的救济渠道，如设立专门的个人信息保护机构或热线，为被侵害人提供法律咨询和援助，降低司法成本。

（四）应对技术发展带来的挑战

第一，对数据挖掘行为进行明确限制。制定详细的数据收集指南，区分哪些数据属于案件相关信息，哪些属于无关信息，限制侦查机关在数据收集时的范围，避免将大量与案件无关的个人信息纳入侦查范围。对于“无中生有”的侦查方式，应设定严格的启动条件，确保其在有充分理由和证据支持的情况下才能启动，同时建立审批机制，对“无中生有”侦查的申请进行审查和监督，防止滥用权力侵犯公民信息权。在进行数据画像时，应采取脱敏、匿名化等处理手段，保护个人信息不被泄露。对犯罪预测模型进行定期评估和审计，发现并纠正其中的偏见和歧视问题，引入多元数据和算法，提高犯罪预测的准确性和公正性，减少概率性错误的发生。

第二，规制算法权力。首先，贯彻算法透明原则。“阳光是最好的消毒剂”。总体上，大多数学者认同算法透明原则作为提升算法可解释性和可问责性的一种重要手段。学者们普遍认为，算法透明原则是一种事前规制方式，要求算法的开发者或应用者，公开包括算法逻辑、输入数据类型、预期输出结果等在内的算法关键要素。[5]算法透明原则的终极目标是对算法自动化决策进行有效规制，而实现算法透明，就如同揭开黑箱的神秘面纱，让“阳光”照亮自动化决策的每一个环节。算法透明原则在增强侦查机关的可问责性和保障个人信息主

---

［1］张勇．敏感个人信息的公私法一体化保护［J］．东方法学，2022（1）：66–78.

［2］宋素红，闫巧妹．敏感个人信息法律责任体系研究［J］．新闻与传播研究，2024，31（6）：87–100，128.

［3］张全涛．大数据时代侦查机关获取公民数据信息的权力边界与实践规制研究［J］．中国人民公安大学学报（社会科学版），2023，39（3）：30–44.

［4］程濡锦．大数据侦查背景下的个人信息保护研究［D］．北京：中国人民公安大学，2024.

［5］沈伟伟．算法透明原则的迷思——算法规制理论的批判［J］．环球法律评论，2019，41（6）：20–39.

体的参与权、知情权和质疑权两个方面发挥效用。其一，一旦出现算法决策导致的偏差或问题，依据公开的算法信息，可以明确地追究相关操控者的责任。其二，算法透明原则确保了潜在的被侵权人在决策过程中享有平等的参与权，例如通过参加听证会等方式，使他们能够充分阐述并表达自己的合理诉求。同时，确保个人信息主体能够了解算法如何收集、处理和使用其个人信息，这种知情权不仅有助于个人信息主体在事后依据公开的算法信息，对算法决策的公平性和合理性提出质疑，并要求决策者对其质疑给予关注和回应，也能使第三方（尤其是专业人士）对算法进行监督，特别是对涉及个人信息处理的环节进行重点审查，防止违规收集和使用个人信息，从而推动算法的改进与优化。其次，建立多元平衡机制。算法的应用涉及公共机构、私营机构和个人信息主体，这三方相互制约，共同维系着权利与权力的结构均衡。[1]作为公权力的代表，公共机构在制定算法准入规则时，不仅要参照行业标准和市场惯例，更应广泛听取个人信息主体及相关方的意见和建议，以确保规则的公平性和合理性，从而平衡个人信息主体与私营机构之间的力量关系。而私营机构，作为技术领域的私权力主体，在公权力可能侵犯个人信息权益时，应发挥其制衡作用。例如，当公共机构试图直接从平台获取个人信息时，私营机构有权要求其提供明确的法律授权，否则有权拒绝提供，以此保护个人信息主体的合法权益。个人信息主体应积极参与三方制衡，对私营机构违法收集个人信息的行为，应向公共机构举报；对公共机构滥用算法决策权，应行使质疑权、申诉权和司法诉权，推动权力与权利的平衡。

（五）构建大数据侦查多元监督格局

首先，要强化内部控制机制。其一是明确角色分离原则，实施侦查与监督职能的严格分离，确保侦查人员不兼任监督职责。可以设立专门的内部监督部门，负责对大数据侦查活动的合法性、合规性进行审查和监督。推广“双人规则”，即关键侦查行为需由两名以上不同职能的人员共同参与，以减少权力滥用的风险。其二是优化层级管理机制，加强信息的透明度和即时性，利用现代信息技术建立高效的内部报告和反馈系统，确保上级机关能迅速、准确地获取大数据侦查活动的信息，减少信息失真和延迟。实行定期审计和随机抽查制度，对大数据侦查的使用情况、数据处理的合法性和保护措施进行审查，及时发现问题并予以纠正。

其次，要加强外部监督效能。一方面，要推动检察监督从被动转为主动[2]。在应对大数据侦查范式所带来的新型侦查手段时，检察机关可以引入大数据技术辅助检察监督，利用数据分析工具对侦查活动进行实时监测和风险评估，确保大数据侦查权被严格限制在合法且有效的数字化框架内。为此，应加快构建公安机关与检察机关之间的大数据共享平台，消除信息隔阂，确保侦查信息能够顺畅对接与流通，实现对大数据侦查活动的全链条、动态化监督。另一方面，要完善司法监督体系。“现代刑事诉讼是以审判为中心的诉讼，建立审判权对侦查权的制约和引导机制是审判中心主义的题中之义和重点内容。”[3]立法明确法院对大数据侦查行为的司法审查权，允许在特定情况下（如涉及严重侵犯个人信息时）由法院进行事前审查或事中干预，并建立大数据侦查活动的司法备案制度，要求侦查机关在采取重大侦查措施前向法院提交备案材料，接受法院的合法性审查。也要加强法院对侦查行为的后续监督，如通过审理相关案件时发现侦查违法的，应依法追究责任并作出相应裁决。

四、结语

在新一代信息技术的强劲推动下，大数据侦查得以迅猛发展并广泛应用，其重要性不容小觑。然而，这一趋势在显著提升侦查效率的同时，也给公民的个人信息保护带来了前所未有的挑战与冲击。面对这一现状，亟需从立法层面与实践层面对大数据侦查进行规制和对个人信息进行保护。在大数据侦查与个人信息保护的权衡之中，两者并非非此即彼的“二元对立”关系。事实上，大数据侦查与个人信息保护是相互依存、相互促进的“双生花”，

［1］蔡星月．算法决策权的异化及其矫正［J］．政法论坛，2021，39（5）：25–37.

［2］詹建红，侯刘果．大数据侦查中个人信息保护的困境及其破解［J］．经贸法律评论，2025（1）：140–158.

［3］詹建红，张威．我国侦查权的程序性控制［J］．法学研究，2015，37（3）：139–157.

能够达成一种动态的平衡共生。个人信息保护与大数据侦查的运作机理和发展趋势相协调，大数据侦查的规范运用能够有力推动对个人信息全面而有效的保护。未来，随着大数据技术的不断发展，需持续关注大数据侦查中的个人信息保护问题，不断优化和完善相关制度与机制，以期在保障公民个人信息权益与提升刑事司法效能之间找到最佳平衡点，推动法治社会的持续进步与发展。

（责任编辑：郭志姣）

Balance Between the Utilization and Protection of Personal Information in Big Data Investigation

Liu Qijiao

School of Criminal Justice, Zhongnan University of Economics and Law, Wuhan

Abstract: In the era of big data, massive amounts of data provide unprecedented opportunities for investigative work, but they also pose severe challenges to personal information protection. How to effectively utilize big data to improve investigation efficiency while safeguarding citizens' personal information security has become an urgent problem to be solved. Investigative agencies can quickly conduct identity verification and trajectory tracking, behavior pattern analysis and relationship network construction, crime tool tracing, and key population analysis by utilizing personal information. However, the comprehensive collection of personal information, the involvement of multiple parties, and information sharing pose hidden dangers and challenges to citizens' personal information security. The inadequate legal mechanisms, challenges posed by technological developments, and conceptual biases coupled with a lack of oversight have led to an imbalance between the protection and utilization of personal information. Therefore, it is necessary to strengthen personal information protection from both legislative and practical perspectives, correct conceptual biases, improve legal mechanisms, regulate big data investigation, enhance personal information protection, and rationally use new technologies while improving oversight mechanisms, with the aim of striking a balance between the protection and utilization of personal information.

Key words: Big data; Utilization of personal information; Protection of personal information; Investigation