刑事司法科学与治理
Criminal Justice Science & Governance
2020 年 7 月第 1 卷第 1 期

Research on Personal Information Protection from the Perspective of Big Data Investigation

Liu Shengyun

Southwest University of political Science and Law, Chongqing

Abstract: With the rapid development of science and technology, big data technology is widely used in the field of criminal investigation, and synthetic investigation, predictive investigation and active investigation become the advantages of big data investigation. The use of personal information in big data investigation is increasing day by day, which intensifies the security and protection of citizens' personal information. At present, protection of citizens' personal information in big data investigation faced with the following difficulties: the expansion of the subject of infringement, the universality of the object of infringement, the secrecy of the way of infringement, and the severity of the harmful consequences. The reasons are the lack of legal regulation, the limitation of internal prevention and control, the convenience of access channels, and the increase of leakage risk. Identification is necessary to strengthen the constitutional legal regulation, perfect the internal prevention and control mechanism, construct the pre-examination mechanism and establish the relief guarantee mechanism in the investigation of the inherent aggression of big data to citizens' personal information.

Key words: Big data investigation; Personal information; Investigative powers; Investigative procedure

Received: 2020-05-19; Accepted: 2020-06-28; Published: 2020-07-09

文章引用：刘圣运．大数据侦查视域下的个人信息保护研究［J］．刑事司法科学与治理，2020，1（1）：207–220.
https://doi.org/10.35534/cjsg.0101016

大数据侦查视域下的个人信息保护研究

刘圣运

西南政法大学，重庆

邮箱：365462950@qq.com

摘　要：随着科学技术的迅猛发展，大数据技术广泛应用于刑事侦查领域，合成侦查、预测侦查、主动侦查成为大数据侦查的优势所在。大数据侦查中个人信息的利用日益增多，加剧了公民个人信息的安全与保护等问题。当前大数据侦查中公民的个人信息保护面临如下困境：侵权主体的扩张性、侵权对象的广泛性、侵权方式的隐秘性以及危害后果的严重性。其原因具体为法律规制的缺失、内部防控的限制、获取渠道的便捷、泄露风险的增加。鉴于大数据侦查对公民个人信息固有的侵犯性，需要加强宪法法律规制、完善内部防控机制、构建事前审查机制、建立救济保障机制。

关键词：大数据侦查；个人信息；侦查权；侦查程序

收稿日期：2020–05–19；录用日期：2020–06–28；发表日期：2020–07–09

1　问题的提出

大数据时代的到来深刻改变了人们的生产、生活模式，使得日常学习、工作等人类实践活动深深地打上了“数据”痕迹，公民个人的日常活动几乎实现了全部数据化。在认识到大数据

给人们带来便利的同时，我们也应注意到大数据不可避免地把公民个人信息的安全性造成潜在的威胁，公民信息泄露已是常有的事。大数据未来健康发展和广泛应用的基础和前提是数据应用的安全，数据挖掘、预测分析的核心是坚决反对侵害公民的隐私权［1］。个人信息的安全问题，从某种程度上说已成为人身安全问题［2］。现实生活中各种公民个人信息暴露引发的人生、生命、财产安全问题，无不深刻凸显了个人信息保护的重要性、紧迫性，着重加强对公民个人信息的保护便显得尤为重要。

科技作为第一生产力，开启了侦查机关在侦破刑事案件领域的一扇崭新的大门，驱使着侦查机关应用大数据技术来犯罪监控、预防以及刑事侦查。在人类信息保护的发展历程中，政府对公民信息自由与安全构成极大的威胁［3］，在刑事侦查领域，大数据侦查已是常态，但是大数据侦查对公民个人信侵犯具有潜在的威胁，如何实现二者之间的平衡便非常重要。随着《网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》等规范的出台，以及《信息安全技术个人信息安全规范》（2019 年修订中）等围绕个人信息安全的国家标准的陆续发布，在我国数据安全以及个人信息保护领域有着举足轻重的现实意义，凸显出保护公民个人信息的强化，大数据侦查的制度化约束与规范成为必然趋势。

2　大数据侦查的优势所在

大数据技术在侦查活动的应用，提高了侦查线索的获取能力，促使证据收集变得高效便捷，丰富了侦查破案方式，为侦破复杂、疑难案件提供了可能。在此意义上，大数据侦查作为现代刑事科学技术发达的新鲜产物，是刑事司法领域现代化的发展趋势及未来走向。

2.1　合成侦查的深化

囿于刑事技术，传统侦查主要依靠侦查人员的现场勘查、调查访问、摸底排队收集案件线索和证据。各地区、各层级、各部门之间的信息数据融合度不高，即时的传输性较差，存在严重的信息壁垒是信息技术落后的通病，未经过严格程序审批，难以得到相互的信息资源协助。信息壁垒不仅造成了侦查资源的浪费以及侦查效益的降低，而且极易错过最佳的侦查战机，影响案件的侦破。随着信息技术的快速发展，犯罪手段日益隐蔽化、智能化、高科技化，非接触性犯罪案件越来越多［4］，这必然增加侦查破案的难度与力度。日益复杂和高发的犯罪形势以及犯罪数据生态化催生了大数据时代合成侦查模式的出炉。合成侦查是侦查机关根据犯罪新形势、侦查新要求所做出的战略性抉择；大数据时代的合成侦查，是各警种、各部门和各地区在海量异构数据的基础上，把大数据技术作为支撑条件，以大数据思维为引领的新型合成侦查模式［5］。这并非简单地整合侦查人员与侦查部门的一项工作，而是将资源、信息、技术、方法

https://doi.org/10.35534/cjsg.0101016

等有效合成，打破传统侦查的思维局限。金盾工程、大数据侦查平台的竣工并日益完善，有效地提升了侦查数据资源的开放度、共享度，推动侦查活动向纵深发展，为案件侦查提供坚实的信息和线索支撑。大数据侦查能够带动各部门共享信息资源与情报红利，从内部打破数据壁垒，实现 1+1>2 的价值配比［6］。

2.2 预测侦查的实现

在小数据时代，案件的侦办遵循“案件发生—侦查介入—证据收集”的侦查路径，所采取的侦查手段往往具有顺序上的递进性和环节上的反复性。此办案模式中侦查机关往往是在犯罪行为发生后才介入到具体案件的侦办过程，使得侦查行为仅具有事后的惩治功能，其本质上是一种消极的应对措施［7］。大数据的核心价值就是预测。大数据预测技术在侦查领域的运用，开启了侦查破案的新模式，即“数据收集—数据建模—信息挖掘 / 碰撞 / 比对—预测犯罪”，预测侦查成为现实。大数据技术促使侦查活动从“物理空间”转向“数据空间”，使得数据信息逐渐成为侦查决策和行动的关键因素。通过数据挖掘技术，筛选海量数据中有价值的线索、信息，为侦查情报的获取、收集、分析和处理等侦查工作提供有力的支持，进行犯罪侦查的预测。申言之，一是对已发生的刑事案件开展预测侦查。侦查机关利用大数据技术，在分析犯罪数据的基础上，挖掘隐性信息，获取有价值的侦查线索，进行数据间的关联性分析，确定案件发生的时间、地点，进行逃亡路线或者作案目标的预测。二是预测未发生的刑事案件。侦查人员梳理历史犯罪案件，根据数据分析结果总结犯罪特点，研判出各类型犯罪活动规律，能够大致预判犯罪事件具体要素；进行犯罪预测与风险防控，合理部署警力与配置资源，实现侦查效能最大化，进而减少犯罪的发生。因此，预测侦查改变了侦查介入的时间点，使得侦查机关及侦查人员掌握更加主动获取犯罪线索的局面，实现了感知犯罪和预测犯罪的同步化［8］。侦查工作的适当前移，有利于进一步掌控侦查主动权，减少犯罪带来的严重后果，降低犯罪修复成本。

2.3 主动侦查的推进

传统侦查活动中，物质交换是犯罪活动记录的主要方式，信息是以原始的物理化形态呈现；由于信息网络的不发达，加上侦查介入的时间滞后以及其他因素对犯罪现场的破坏，导致犯罪过程中很多信息难以保存下来。因此，侦查机关所获取的线索、证据是有限的。长期以来，造就了侦查机关及侦查人员处于被动局面。大数据技术的应用促使侦查机关在侦查活动中掌握着更多的主动权，极大地改变了传统侦查中侦查人员的被动地位。借助大数据技术，侦查机关具备了在案发后主动获取案件相关信息的能力，架构起大数据平台与数据库的关联性，但仍是“回溯型”侦查模式［9］。首先，丰富的侦查资源是大数据侦查开展的基础。信息时代的数据留痕技术便利了犯罪侦查的追踪溯源，人们日常的活动轨迹都会在数据空间留下痕迹，丰富的信息

数据资源便成为侦查机关开展侦查活动的重要基础。其次，大数据技术和平台的强有力支撑。在大数据技术的帮助下，侦查人员充分利用数据模型算法，寻找数据间的关联性，逐渐减少对口供的依赖；利用大数据平台对案件信息及其他相关数据进行搜索、碰撞、挖掘，全面开展大数据侦查实践活动，为案件侦破提供丰富的线索来源，从而固定案件事实。促使“以人为中心”要线索、要证据的侦查取证思维方式向“以数据为中心”的新型侦查取证思维方式的转变[10]。大数据背景下的主动侦查便利了证据的获取，提高证据的真实性与可靠度，能够更好地应对影响社会稳定较大的侵财型犯罪案件。

以往侦查程序中因“有形力”的侦查强制措施吸收了信息收集行为，公民个人信息的干预姿态并未展现出来[11]。数据为王的信息时代，当信息质变为权力的基础时，国家权力与公民权利的双向互动呈现出紧张而又相互依赖的关系[12]。由于大数据侦查的运行必然要求最大化地采集公民各种信息，且其收集范围还处于不断扩张的趋势。在刑事侦查领域，侦查机关通过对数据库中的公民个人信息进行数据分析、整合，是发现数据间的隐性关系，从而深入地获取侦查线索和情报；但个人信息数据作为公民人格权的延伸，天然有着诉诸保护的需求[13]。在公安大数据的战略背景下，侦查机关重视对公民个人信息的应用及分析，对个人信息、数据的依赖必将冲击侦查程序，往往牵涉到侦查权与个人信息权之间的博弈问题。

3　大数据侦查中个人信息保护的困境

侦查权能的强化从某种意义上是一个权力向电子和信息化技术的渗入和运作的过程[14]。具有天然干预性、扩张性和监控性的侦查权，在大数据技术的发展助推下，逐渐展现出对个人信息深度侵犯的姿态，客观上加剧了对个人信息的侵犯与威胁[15]。大数据在侦查程序中的深度利用，丰富侦查线索的获取方式，实现了侦查破案效益的最大化。但此举某种程度上剥夺了公民的信息自决权和知情权，并在客观上加重了公民个人信息泄漏的风险和后果[9]，使得大数据背景下的个人信息保护为代表的人权保障呈现出错综复杂的局面。

3.1　侵权主体的扩张性

传统意义上，自然人往往是侵犯公民个人信息的犯罪主体，但是随着科学技术的迅猛发展，个人信息的侵权主体已经发生改观。大数据时代的悄然到来，公民个人信息通过数据化的形式被储存于各大数据资源库中，丰富的数字化痕迹信息便利了社会主体的利用。在大数据时代，人类社会逐渐发展成为一个“大数据监控社会”，社会上每一个人正逐渐成为透明的人[16]。与此同时，合法获取、存储公民个人信息的主体范围也大幅度扩展，政府机关、商业机构、民间团体等组织都通过建设的数据库进行着数据信息的收集工作。大数据技术背景下个人信息全

https://doi.org/10.35534/cjsg.0101016

面收集和循环利用，使得信息主体逐渐丧失了对个人信息的实际控制，控制主体已经由个人演变为社会组织和政府机构，控制权能也由个人向组织转变［17］。大数据侦查的运用改变了侦查权的权力分布格局，使得侦查权逐渐呈现社会化与弥散化的姿态［18］，现阶段的数据库资源并非主要由侦查机关掌控着，反而是由社会机构、商业机构掌握着。虽然侦查机关自身拥有大量的数据库资源，但是侦查机关开展大数据侦查实践活动过程中，往往更多需要利用社会机构、商业机构数据库的公民个人信息，进而挖侦查线索、获取犯罪信息，从而推动国家—社会—个人多方参与的新型侦查权能分布格局的形成。如此，现阶段以合法形式收集、管理和存储公民个人信息的主体已经涵盖了个人、社会、国家，而且主要是社会力量而非侦查机关在大数据侦查实践活动中发挥重要的作用。在大数据侦查模式下，侵犯公民个人信息的主体从个人、法人延伸到公权力机关，对公民的人身安全与人格尊严形成威胁，加剧了公民不安的心理状态［19］。

3.2 侵权对象的广泛性

在前数据时代，侦查机关的办案模式更多是依靠现场勘查、摸底排队、侦查讯问等活动，并不过多地倚重大数据侦查中的个人信息。而且，技术的局限性抑制着个人信息的收集，侦查机关获取个人信息的能力是有限的。传统侦查视野下侦查的对象往往是特定的，因而侦查过程侵犯个人信息的对象也是个别的、特定的。大数据技术发展、运用已经逐渐形成了“数据为王”的大数据社会，数据留痕使得公民的个人信息难以像以往一样受到深度的保护。侦查机关的网络监控、“天网工程”以及“金盾”大数据平台等项目建设并取得了长足进步，从而为深度收集公民个人信息奠定了基础，“一种无限普遍化的‘全景敞式主义’的国家监控形态”已成为现实［20］。大数据侦查模式下，侦查破案已基本不受时空的限制，跨省跨国追捕已成为常态，信息互联互通、网上电子取证已成为可能；侦查对象由个案特定人群，扩展为全体社会成员。由于大数据侦查应用的数据不仅仅是“样本”，而是“全部”，只要是与案件有关的数据都会被采集、利用，即使与案件并无直接关系的案外人员的数据信息同样被侦查机关应用到犯罪侦查中，显然存在较大的安全隐患，即全体公民的各种信息都成为了其分析对象。正如有学者所言：大数据侦查是一种不以犯罪嫌疑为前提的广泛监控，任何人都可能成为潜在的侦查对象［21］，全体公民甚至全球民众都极有可能成为潜在侵权的对象。而侦查过程中大数据挖掘分析得越精准、应用领域越广阔，个人隐私和数据安全保护就会变得越紧迫［22］。这必然会给社会成员的正常生活带来一定的困扰，公民个人信息权无法得到充分保障。

3.3 侵权方式的隐秘性

前数据时代，侦查机关侵犯个人权利表现为刑讯逼供和扣押财产等“有形侵权”［23］。无论是刑讯逼供行为，还是扣押财产行为，都是有迹可循的侵权方式，且这种侵权方式往往是

建立在当事人知情的基础上；刑讯逼供会在犯罪嫌疑人身体上留下伤痕或对其精神造成伤害，侵犯财产则会表现出当事人财物的减损。然而在大数据时代，侦查权侵害的权利类型发生转换与升级，隐私权、个人信息权等涉及人格尊严的基本权利逐渐成为侦查机关青睐的对象。侦查机关利用大数据技术对海量存储信息进行数据挖掘、碰撞获取侦查线索与案件信息，此过程对公民个人信息的干预具有前所未有的隐秘性与深刻性，而当事人对个人信息被收集、利用的过程，可能完全不知晓亦无法抗拒。公民的个人信息往往就悄无声息地被侦查机关所利用。大数据侦查过程中的技术程序与法律程序处于不透明的状态，这就出现大数据侦查决策机制中的“黑箱效应”， 由此更加凸显了大数据侦查行为侵权方式的秘密性。因此，在大数据时代，侦查机关侵犯公民权利较之于传统侦查更为严厉、隐秘，因其“侵权的无形化”对公民个人信息、数据侵害更具有杀伤力。

3.4 危害后果的严重性

在前数据时代，由于技术的限制，数据储存并不全面，即使存在损失也比较直接且可被估量，因此，丢失的数据往往非常有限的。然而，大数据时代的到来，丰富了数据储存的规模及模式，无论是侦查机关自有数据库，还是其他外部数据库，其数据库进行数据存储是全面、多样的，而且是会以结构化的方式对数据进行处理，单一数据的信息承载量呈现出爆炸式的增长。个人信息一旦泄露便呈现全网爆炸式扩散，后果将不堪设想。个人信息与数据主体的切身利益密切相关，个人信息的泄露，轻者仅仅是财产的损失，重者则危及人的生命。保护个人信息是信息社会健康发展的基础，进而保障公民独立的生活权利免受侵扰，实现社会和谐与稳定。大数据技术的运用某种程度上扩张了数据公司追踪、获取公民个人信息的权力，大数据公司通过各自的数据库对公民的个人信息进行储存，使得数据的集聚化程度猛然增强。海量的数据资源及数据库的建设，增加了侦查机关信息获取的渠道，但也为网络黑客侵入大数据平台盗取数据信息埋下了隐患。一旦大数据平台数据的丢失，将会导致个人信息的泄露并且增加了对个人的社会声誉以及财产、生命安全造成损害的风险，这样的泄露结果比起以往的侵权更加严重和难以控制[9]。2016 年 8 月我国山东女孩徐玉玉因电信诈骗而致死的悲剧事件，引发社会的广泛关注，这就是个人信息泄露导致生命受损的严重后果。这也警示我们，只有增强信息保护的意识和能力，才能最大限度地保护好自身的合法权益。

4 大数据侦查与个人信息保护冲突的原因

随着科学技术的发展，刑事侦查技术在侦查领域的应用也达到了前所未有的深度，嵌入侦查实践的同时，也加剧了对个人信息的冲击。大数据侦查对个人信息的侵犯既有法律规范方面

https://doi.org/10.35534/cjsg.0101016

的缺失，也有侦查机关自身体制的缺陷。大数据技术方便了侦查机关信息收集机制的快速形成，但是这种机制本身也存在信息泄露的风险。

4.1 法律规制的缺失

当前我国个人信息保护的法律体系不完善，相关的法律法规基本处于零散混乱的状态，缺乏专门的个人信息保护法，法律规制的缺失助长了侦查机关对公民个人信息侵犯的扩张权能。据统计，我国有近 40 部法律、30 余部法规，约 200 部规章及其它规范性文件涉及个人信息保护［24］，虽然存在如此之多个人信息保护方面的法律、法规及文件，但是上述个人信息保护条款不集中、适用不明确、处罚不具体、基本概念模糊，在实践中难以发挥实际作用，而且真正规制侦查机关收集、使用信息的法律规范并不多。大数据技术使得侦查机关的侦查权能急速扩张，侦查领域个人信息保护方面的立法长期处于真空状态。我国《宪法》尚未明示公民个人信息权，第 38 条规定人格尊严仅具有私法上人格权的指示性功能；第 39 条规定的非法搜查仅限于住宅自由的物理空间，并不包括虚拟空间中的个人信息与数据；仅在第 40 条的规定通信自由和通信秘密受法律保护，范围过窄，而且是授权侦查机关基于侦查犯罪需要依据法律程序可以对通信进行检查；宪法层面关于个人信息保护的碎片化规定［11］，并不足以规制侦查程序中对个人信息的侵犯。2009 年《刑法修正案（七）》虽然增加了“出售或非法提供公民个人信息罪”，但是该罪是针对自然人犯罪，并非严格意义上限制侦查机关权力的行使，因此不属于限制侦查机关采集使用公民个人信息的强制性规定。现行《刑事诉讼法》中关于个人信息保护的关注基本处于缺失状态，仅有个别条款涉及隐私权保护；而且是要求侦查人员对个人信息的保密，缺乏对侦查行为侵犯个人信息的规制。从保护公民权利、限制侦查权力的视角审视大数据侦查相关的限权性规定，公安部 1997 年发布的《计算机信息网络国际联网安全保护管理办法》第 7 条纯粹属于禁止性规定，没有责任条款，而且并非专门规制侦查机关。无论是宪法层面，还是法律规范层面，亦或规章层面，个人信息保护的适用规则均不全面，尤其是刑事诉讼领域尚未构建起信息领域的保护规则，加剧了大数据侦查对公民个人信息的侵犯。

4.2 内部防控的限制

内部防控体系的建设与完善向来是公安部的一项重要任务。早在 2008 年公安部就开启了执法规范化建设周期，多次召开全国性会议进行相关工作的部署；先后下发各种纲领性文件来推动全国公安机关执法规范化建设，进而弥补立法不足与司法实践缺位所带来的规制漏洞，但是作为内部控制体系的规范性文件难免存在局限性。一是在信息收集方面缺乏门槛要件，未进行类型及层次区分。没有个人信息层级加以划分，并且缺乏前置性要件，加剧了侦查机关与犯罪嫌疑人之间力量的不对等。二是过于重视情报信息系统的构建。在内部控制体系下，侦查机关

在构建情报信息系统的过程中，需要收集、使用大量的公民个人信息，但是部分侦查机关在利用相关信息侦查破案过程中，过分追求侦查效益，忽视了对侦查过程的规制与监督，使得侦查机关的权力运行过程难以得到控制。具体表现在：侦查过程中情报信息的收集、存储与共享中缺少事前控制与审查，只能在出现违法犯罪现象之后，才能进行事后救济与回应。 三是侦查人员对大数据侦查的实践特质认识不足。侦查机关基于大数据侦查可观的破案效益，并没有从本质上认识到大数据侦查的特殊性，仅仅是将其当作一种警务变革模式，在内部控制上放任了侦查权的隐形扩张［11］，由此容易导致忽略其对个人信息的侵犯。

4.3 获取渠道的便捷

传统侦查模式中信息获取主要是依靠调查走访、现场勘查，数据、线索的获取一定程度上是有限的。大数据时代背景下，公安部金盾二期工程顺利完成并竣工验收，公安部门的大数据平台汇集着海量的信息数据，“全国公安一片云”已是公安机关的常态［25］。国家基于社会治理、犯罪侦查的需要，致力于收集公民个人信息，建立海量的公民数据库；必要时，也有获取外部数据库信息资源的权限。在刑事侦查实践中，网络运营商面对侦查机关的办案请求几乎是有求必应，而且法律也明确规定网络运营商有配合侦查机关办案的义务，因此，面对侦查的办案需要形成了特有的倾斜态度。由此，公民在面对具有天然扩张性的公权力侵犯时，还要防备第三方主体对个人信息的获取的可能性。其结果是公民的个人信息在国家和网络运营商面前无所遁形，隐私权的范围、空间受到更多压制，乃至荡然无存，公民彻底沦为“透明人”［7］。多种因素的叠加使得侦查机关信息获取方式变得更加便捷，为侦查破案大开方便之门。但是此过程中也便捷了侦查机关滥用权力侵犯个人信息的侵犯。因此，公安机关亟需出台相关大数据侦查领域的规范性文件，对侦查人员信息的收集、获取、使用行为进行控制，进而更好地保护公民个人信息。

4.4 泄露风险的增加

快速发达的信息社会，互联网领域的个人信息危机愈发严重，数据泄露风险来源主要是黑客攻击。大数据时代数据库的价值高、数量大特点，更容易受到黑客和病毒的青睐。高度融合的海量信息蕴藏巨大价值的同时，也存在信息泄露的风险，信息安全隐患成为当前社会面临的重大问题。人们的生活都被高度数据化，公民的任何举动都会留下电子“脚印”或电子“指纹”［26］，“裸奔时代”已成为不争的事实［27］，侦查机关使用无处不在的电子监控，结合人像数据和面部识别软件，足以确定任何在公开和半公开场合个人的身份信息［28］。大数据时代，奥巴马政府曾把大数据称为“未来的石油”，数据的价值正得到前所未有的体现［29］，数据价值增加的同时也加剧了数据信息泄露的风险。公民个人信息在大数据侦查中具有极大的应用

https://doi.org/10.35534/cjsg.0101016

价值和应用潜力，其利用频率与侦查效率、效益存在正相关性，客观上增加了个人信息泄露的风险。在大数据侦查模式下，公民个人信息数据的深度融合与高度整合，促使侦查机关信息获取能力提高的同时，也降低其信息处理成本；但是侦查过程中数据挖掘对公民的个人隐私造成潜在的威胁［30］。因其对个人信息的分析进行时多角度、深领域、全方位的，能够将获取的潜在信息进行二次比对、多元碰撞，发现更多隐藏的规律。因此，在大数据时代，一方面公民的个人信息变得更为弥足珍贵，另一方面，相对以往信息泄露的风险骤然加剧。

5　大数据侦查中个人信息的保护路径

大数据在犯罪侦查的应用与公民个人信息保护间存在严重的二律背反现象，详细、精准、广泛的大数据应用加剧了个人隐私和信息安全被侵犯的风险［9］。在大数据、人工智能时代，国家权力的运行与公民权利的行使正在发生着深刻而巧妙的变革，两者间的双向互动模式发生改观，并随着时代的进步不断发展而继续深入下去，急需法律规定的修正、补充乃至重构。鉴于大数据在犯罪侦查中对公民个人信息固有的侵犯性以及个人信息泄露后造成的严重危害性，应当加强宪法法律规制、完善内部防控机制、构建事前审查机制、建立救济保障机制。尤其需要厘清大数据侦查与公民个人信息保护之间的关系，在有效保护公民个人信息的同时实现精准的犯罪打击。

5.1　加强宪法法律规制

基本的人权保障作为衡量法治国家的主要标志之一，在当今国际社会各界达成广泛的共识。侦查权在大数据技术发展的背景下摆脱了传统法律框架在起点环节上的约束，规制侦查权的法律空白已经出现［18］。而大数据侦查过程中使用的数据往往涉及到公民的基本权利，其中最为主要的便是个人信息。从我国目前的法律体系来说，缺乏完整、全面的框架性规则体系对公民基本权利中个人信息的保护。大数据侦查作为刑事侦查制度的重要组成部分，必须受到法律的规制，才能更好地在打击犯罪与保障人权两端实现动态平衡。为此，一是有必要考虑将个人信息权纳入宪法保护体系，以根本大法的形式确立个人信息权的地位，进而影响侦查程序的设计。二是通过修改《刑事诉讼法》相关法律条文，明确大数据侦查和相关措施的含义、界限，规定其适用条件与适用范围，确保个人信息不被用于非刑事犯罪侦查目的以外用途。三是完善《刑法》条文规制严重侵犯公民个人信息的侦查行为，促使侦查机关及其工作人员严格按照法律赋权、严格遵守法定程序开展大数据侦查。四是必要时制定《个人信息保护法》，科学、全面地明确公民个人信息的保护范围，构建个人信息安全的全面保护机制，从而更好地保障个人信息不被政府部门、社会组织、大数据公司随意收集、使用，进而确切地规范侦查机关对公民个人信息

的获取、采用。上述宪法法律的完善能够形成一套完整、多维与大数据时代相适应的法律保护体系，对公民个人信息安全的保护无疑具有重要而现实的意义。

5.2 完善内部防控机制

大数据库和大数据平台的建立过程中，侦查机关对个人信息的利用尚未给予足高度重视，缺乏相应的制度机制约束侦查人员收集、保管和利用信息数据的行为。因此，首先，出台大数据侦查的规范性文件，规范工作流程。明确侦查机关获取公民个人信息的渠道、权限、范围，制定严谨具体、操作性强的侦查取证规范指引，细化工作程序与操作方式，通过严格的规范来规制侦查人员的信息获取、使用等权限，最大限度上保证收集信息的准确性、可靠性与真实性，避免侦查权的滥用。其次，侦查机关应当构建起大数据侦查的追溯体制，实行操作日志与操作留痕机制，保证数据的使用流向有迹可循。可以借助专业的“数据溯源”（Provenance of the Data）技术来保证数据记录的实现，通过技术性回溯手段防止大数据侦查行为的滥用。最后，要健全信息监管机制与监督机制，促进信息收集、使用的规范化建设。明确侦查机关的法制部门或监察部门对大数据侦查行为的监督权，确保侦查人员正确使用内部数据资源，及时发现并制止侦查人员侵害公民个人信息的行为，一旦存在滥用公民个人信息的行为，必须对相关人员进行必要的问责。必要时可以设置专门的信息监察机构，赋予其个人信息保护的专项职责与监察职能，加强对侦查机关信息收集的监督［11］。通过专门的信息监察人员，督促侦查人员正确使用数据的权利。通过上述相关具体措施，构建起侦查机关内部的控制措施，全面保护个人信息在整个环节中的利用，从而实现各项规章制度和程序规定数据化、流程化，对执法活动全方位管理、监督、预警。

5.3 构建事前审查机制

为了防止案件侦办过程中侦查机关权力的滥用和失范，有必要构建侦查机关获取公民个人信息的事前审查机制。部分大陆法系国家（以德国为代表）对大数据侦查实行法官令状审批制。我国刑事诉讼构造未来发展趋势必然对侦查行为确立司法审查原则或者令状原则。但目前按照我国司法实践，实行法官令状审批制的条件尚不成熟，主要基于以下理由：首先，由于剥夺或限制公民人身自由的逮捕、指定居所监视居住等强制措施可由公安机关或检察机关自行批准，如果贸然对大数据侦查行为实行法官令状审批制有违我国司法实践令状统一性，也是与强制性措施体系均衡性要求相悖。其次，对大数据侦查行为实行法官令状审查制有违侦查行为法治化的整体性。法治的整体性必然要求法治发展具有渐进性［31］；在我国尚未对逮捕、搜查等常规侦查行为实行令状审查机制前，不可超越对大数据侦查行为实行令状制。最后，已有不少实行法官令状审批制的国家司法实践表明：对于侦查初期的技术侦查、大数据侦查等特殊侦查手

https://doi.org/10.35534/cjsg.0101016

段，法官令状审批制并未展现出应有姿态，更多是流于形式［32］。根据我国当前的侦查实践，切实可行的方式是实行检察官审批制，辅之构建侦查机关内部审批机制［33］。具言之，侦查机关利用外部数据库的个人信息时，应按照要求向中立的检察机关提出申请，检察机关在审核案件后发布符合条件的令状。重视对侦查机关获取外部数据库公民个人信息行为的监督，可以考虑在侦查机关内部与外部建立全程留痕的回溯性技术监督程序［3］，运用技术手段监督个人信息的规范利用。而那些由侦查机关使用自有数据库（如公安内网数据库的数据、接入公安网的政府及社会数据）的个人信息时，可由公安机关内部审批程序来自主进行。

5.4 建立救济保障机制

大数据侦查犹如一把“双刃剑”，它既能有效促使刑事案件的快速侦破，但又会对公民个人信息权造成一定的侵犯。当公民的个人信息受到侵犯时就需要相应的救济保护机制，建立大数据侦查中公民个人信息的救济保护机制，应当从两个维度方面考虑：首先，应当赋予当事人对大数据侦查的相对知情权。知情权是公民的基本权利之一，是当事人在刑事司法程序中获取所受控告及强制措施的性质和理由的权利［34］。基于“黑箱效应”，侦查机关对大数据的秘密运用往往涉及公民人身、自由等权益。因此，对处于弱势的当事人而言，侦查人员在确保正常办案的前提下，应当告知犯罪嫌疑人大数据侦查的分析结果、数据源等内容。其次，应当保障公民的事后救济权。所谓，无救济则无权利，事后救济作为权利的必然延伸；当大数据侦查行为侵犯公民个人信息时，当事人有权依法寻求救济。公民可选择的救济途径主要有两种：一是赋予当事人“数据辩护权”。当事人知晓相关数据来源、数据分析结果后，可以提出异议并针对错误的数据请求更正，必要时申请复议；也可以直接另行提出与大数据分析结果相反的其他证据，通过申请非法证据予以排除，从而对形成对侦查权力的制约；二是当事人享有国家赔偿权。公民可以通过相应的投诉处理机制或者司法救济机制，请求对大数据侦查过程中是否侵犯公民个人信息进行裁定，经裁定确认存在违法使用公民个人信息的行为，信息主体应有权获得国家赔偿。公民的知情权与更正权是保障信息主体信息权，防范信息管理者、使用者、控制者滥用公民个人信息的重要制度安排［18］。在刑事侦查领域中，建立完善的救济保障机制才能更好保护公民的个人信息。

6 结语

大数据技术在犯罪侦查中的兴起和广泛应用，毫无疑问为侦查机关有效预防犯罪、控制犯罪、打击犯罪提供了新路径；但作为一个新生事物，其带来的风险和挑战变得更加巨大。在大数据侦查活动的具体开展过程中，过度收集、使用公民个人信息显现出侦查机关对公民个人基本权

利的一种“冒犯”。完善相关法律法规，对大数据侦查进行法律定位，明确侦查机关大数据侦查权限在个人信息方面的使用范围，在有效打击犯罪的同时，平衡侦查扩张性与公民个人信息保护之间的冲突。任何权力的行使需要进行内部的规制，引入具体、全面的侦查内部控制机制，则能够使大数据侦查在法治的轨道内运行良好。构建事前审查机制，预防案件侦办过程中侦查机关权力的滥用和失范。侦查权的天然扩张性总是不可避免地对公民权利造成损害，因此，建立事后救济机制有助于公民权利受损后的修复。总体而言，在凸显社会稳定和国家安全为主的中国现代社会，刑事侦查领域中公民权利保障弱势境地的转变，在完善法律规定的同时，仍需要同步改进相关的制度设计；通过法律和制度的改进，合理、有效地规避侦查权能对公民个人信息造成的潜在风险，最终在保障公民个人信息与提高侦查效益之间创造共赢的局面。

基金项目

本文获重庆市治安三特项目资助（项目编号：2019ZAST020）。

参考文献

[1] [美] 埃里克·西格尔. 大数据预测 [M]. 周昕，译. 北京：中信出版社，2014：39.
[2] 吴苌弘. 个人信息的刑法保护研究 [M]. 上海：上海社会科学院出版社，2014：1.
[3] 程雷. 刑事司法中的公民个人信息保护 [J]. 中国人民大学学报，2019（1）：105.
[4] 刘启刚，马凯. 大数据在非接触性犯罪治理中的应用 [J]. 中国刑事警察，2018（5）：23.
[5] 王超强. 论大数据时代的合成侦查模式 [J]. 广州市公安管理干部学院学报，2017（3）：15.
[6] 陈刚. 大数据时代犯罪新趋势及侦查新思路 [J]. 理论探索，2018（5）：114.
[7] 冯姣. 大数据与犯罪侦查：机遇、挑战及应对 [J]. 苏州学刊，2019（5）：115.
[8] 曹凤，彭知辉，陈亮. 公安情报学前沿问题研究 [M]. 北京：中国人民公安大学出版社，2017：175–200.
[9] 于阳，魏俊斌. 冲突与弥合：大数据在侦查监控模式下个人信息保护 [J]. 情报杂志，2018（12）：148.
[10] 郑群，张芷. 大数据侦查的核心内容及其理论价值 [J]. 山东警察学院学报，2018（6）：51.
[11] 蒋勇. 大数据时代个人信息权在侦查程序中的导入 [J]. 武汉大学学报，2019（3）：156.
[12] 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（2）：47.

[13] 王燃. 大数据时代的模式变革及其法律问题 [J]. 法制与社会发展，2018（ 5 ）：127.
[14] 汤强. 侦查权能的扩张与转型 [J]. 净月学刊，2014（ 2 ）：23.
[15] 刘鹏. 论信息化侦查与个人信息保护 [J]. 中国人民公安大学学报，2015（ 1 ）：47.
[16] 王燃. 大数据侦查 [M]. 北京：清华大学出版社，2017：160.
[17] 王秀哲. 大数据时代个人信息保护法律制度之重构 [J]. 法学论坛，2018（ 6 ）：119.
[18] 程雷. 大数据侦查的法律控制 [J]. 中国社会科学，2018（ 11 ）：123.
[19] 皮勇，王肃. 大数据环境下侵犯公民个人信息犯罪及其防控——以数据空间为视角 [J]. 吉首大学学报，2017（ 5 ）：79.
[20] [法] 米歇尔·福柯. 规训与惩罚 [M]. 刘北成，译. 上海：生活·读书·新知三联书店，2012：242.
[21] 李双其. 大数据侦查实践 [M]. 北京：知识产权出版社，2019：407.
[22] 新玉燕，李克. 大数据：政府治理新时代 [M]. 北京：台海出版社，2016：66.
[23] 付黎明. 大数据侦查中个人信息保护策略研究 [J]. 警学研究，2019（ 4 ）：108.
[24] 陈超. 论个人信息权法律保护的刑事立法模式 [J]. 华北水利水电大学学报（ 社会科学版），2018（ 2 ）：86–91.
[25] 谢明睿. 大数据侦查模式下的公民个人信息权保护研究 [J]. 湖南警察学院学报，2018（ 5 ）：24.
[26] 董邦俊，黄珊珊. 大数据在侦查应用中的问题及对策研究 [J]. 中国刑警学院学报，2016（ 2 ）：10.
[27] 张兆瑞. 智慧公安：大数据时代的警务模式 [M]. 北京：中国人民公安大学出版社，2015：162.
[28] Hu M. Biometric ID Cybersurveillance [J]. Social ence Electronic Publishing，2013，88（ 4 ）：1475–1558.
[29] 王燃. 大数据时代个人信息保护视野下的电子取证 [J]. 山东警察学院学报，2015（ 5 ）：126–135.
[30] 杨婷. 论大数据时代我国侦查模式的转型 [J]. 法商研究，2018（ 2 ）：35.
[31] 卓泽渊. 论法治的整体性 [J]. 现代法学，2003（ 2 ）：15.
[32] Nyst C，Falchetta T. The right to privacy in the digital age [J]. Journal of Human Rights Practice，2017.
[33] 程雷. 秘密立法宏观问题研究 [J]. 政法论坛，2011（ 5 ）：83–84.
[34] 钱育之. 知情权：犯罪嫌疑人的基本权利 [J]. 求索，2007（ 8 ）：91.