江西财经大学
JIANGXI UNIVERSITY OF FINANCE AND ECONOMICS

学校代码 _____
密　　级 _____
中图分类号 _____
UDC _____

硕士学位论文
MASTER DISSERTATION

论文题目（中文）：大数据侦查中的个人信息保护问题研究

论文题目（英文）：Research on the Personal Information Protection in Big Data Investigation

作　　者 _____　　导　　师 _____
申请学位 硕士　　培养单位 法学院
学科专业 诉讼法学　　研究方向 刑事诉讼法

二〇二一 年 六 月

摘　要

当下的信息时代，使犯罪愈发隐蔽化、新型化和虚拟化，基于打击犯罪需要，催生出以大数据驱动的新型侦查模式——大数据侦查。大数据侦查是指通过利用数据技术，对存储于网络平台或计算机系统中的海量数据信息进行收集、整合、比对、挖掘等，进而发现犯罪线索、收集犯罪证据、缉获犯罪嫌疑人和预测犯罪的侦查模式。与传统侦查模式相比较，大数据侦查具备侦查空间数据化、侦查技术智能化、侦查行为主动化等特征，是当下时代的必然选择。然而，由于现阶段我国《刑事诉讼法》并未有大数据侦查的相关规定，加之个人信息保护的法律缺失及数据共享机制的混乱，使大数据侦查运行下对个人信息保护的问题凸显。大数据侦查中的个人信息有其特殊性，主要包括海量性、易获性、动态性及主体多元性，需在权利保障和程序规制等角度探讨大数据侦查中保障个人信息的制度构建，以期在保障个人信息安全的前提下，最大限度的发挥大数据侦查的效能。

大数据侦查中保护个人信息的理论基础包括个人信息保护理论、信息隐私权理论、价值平衡理论及分层保护理论。个人信息本身价值呈现多元化特征，其中包含道德价值、商业价值及政治价值。刑事诉讼历来追求惩罚犯罪和保障人权之间的价值平衡，在大数据时代，两者价值体现为侦查机关对个人信息利用与保护。在大数据侦查过程中，通过对个人信息利用促进侦查高效化，其上位利益正是国家打击犯罪的需求，而对个人信息的保护便体现出对公民基本人权的保障。

目前，大数据侦查下对个人信息保护的挑战，具体包括：其一，现有立法难以保障刑事程序中的个人信息。虽近年来我国在刑法、民法、行政法中就个人信息保护的相关立法都取得了相应的进展，但因对刑事司法领域中个人信息保护缺乏直接性、有效性及原则相冲突性等，难以在刑事诉讼中直接适用。其二，大数据侦查技术易对个人信息造成“隐秘性”侵犯。传统侦查中，侦查机关侵犯个人权利的违法侦查行为较为集中在讯问和搜查程序中，这种侵权通常有迹可循，但基于大数据侦查的技术层面，对个人信息利用过程的不透明性极易造成侵犯个人信息的隐蔽性。其三，对数据的依赖加深对个人信息的过分收集。信息的充分采集是保障大数据侦查中数据利用发挥其最大效用价值的基础前提，加之大规模数据监控为数据采集提供的有力渠道，加深了司法实践中侦查部门对个人信息的过分采集。其四，数据挖掘等技术应用加大对个人信息保护难度。大数据侦查中数据挖掘技术模糊了信息边界，其对个人信息的深度侵入性特征使个人信息更加难

以保护。其五，服务于大数据侦查运行的数据共享大幅度扩张。数据共享平台的搭建虽打破了信息交流壁垒，但也造成侦查机关调取程序被架空，长此以往，将会直接影响个人信息在刑事侦查中的合法有效利用。其六，海量数据存留对个人信息造成风险。数据存留是数据采集的延伸，是不规范数据库的体现，缺乏规范管理加之数据库安全系数问题，有黑客入侵、网络攻击、数据滥用等风险，不利于个人信息保护。

大数据侦查中对个人信息保护的路径构建，应对不同信息类别进行分类保护，结合大数据侦查本身兼具任意性和强制性多重属性成分，明确不同侦查阶段的数据适用规则，同时构建针对数据挖掘的特殊程序，完善大数据侦查运行的审批监督机制，规范数据共享平台，健全数据存留管理。

【关键词】大数据侦查　个人信息　数据分析技术　立法规制　权利保障

Abstract

In the current information age, crime is becoming more concealed, new and virtual. Based on the needs of fighting crime, a new big data-driven investigation model-big data investigation has been born. Big data investigation refers to the use of data technology to collect, integrate, compare, and excavate massive amounts of data and information stored on network platforms or computer systems to discover criminal clues, collect criminal evidence, seize criminal suspects and predict crimes The investigation mode. Compared with the traditional investigation mode, big data investigation has the characteristics of digitization of investigation space, intelligence of investigation technology, and initiative of investigation behavior. It is an inevitable choice of the current era. However, at this stage, my country’ s Criminal Procedure Law does not have relevant regulations on big data investigations, coupled with the lack of personal information protection laws and the confusion of data sharing mechanisms, making the problem of personal information protection under big data investigations prominent. Personal information in big data investigations has its particularities, mainly including mass, easy access, dynamics, and subject diversity. It is necessary to discuss the construction of a system to protect personal information in big data investigations from the perspectives of rights protection and procedural regulation. On the premise of ensuring the security of personal information, maximize the effectiveness of big data investigations.

The theoretical basis for protecting personal information in big data investigations includes personal information protection theory, information privacy theory, value balance theory, and layered protection theory. The value of personal information itself presents diversified characteristics, including moral value, commercial value and political value. Criminal litigation has always pursued a balance of value between punishing crimes and protecting human rights. In the era of big data, the values of both are reflected in the use and protection of personal information by investigative agencies. In the process of big data investigation, through the use of personal information to promote the efficiency of investigation, its superior interests are exactly the needs of the

country to fight crime, and the protection of personal information reflects the protection of the basic human rights of citizens.

At present, the challenges to personal information protection under big data investigation include: First, it is difficult for existing legislation to protect personal information in criminal procedures. Although my country has made corresponding progress in the relevant legislation on personal information protection in criminal law, civil law, and administrative law in recent years, it is difficult to protect personal information in the field of criminal justice due to the lack of directness, effectiveness, and conflicting principles. It is directly applicable in criminal proceedings. Second, big data investigation technology can easily cause "secret" infringements on personal information. In traditional investigations, the illegal investigations of investigative agencies that infringe on individual rights are more concentrated in the interrogation and search procedures. Such infringements are usually traceable, but based on the technical aspects of big data investigations, it is very easy to make the process of using personal information opaque. Cause infringement of the concealment of personal information. Third, the reliance on data deepens the excessive collection of personal information. Adequate collection of information is the basic prerequisite to ensure the maximum utility value of data utilization in big data investigations. In addition, large-scale data monitoring provides a powerful channel for data collection, which deepens the excessive collection of personal information by the investigation department in judicial practice. Fourth, the application of data mining and other technologies has made it more difficult to protect personal information. Data mining technology in big data investigation blurs the boundaries of information, and its deeply intrusive features on personal information make it more difficult to protect personal information. Fifth, data sharing for big data investigation operations has expanded significantly. Although the establishment of a data sharing platform has broken the barriers to information exchange, it has also caused the retrieval procedures of investigative agencies to be emptied. If this happens, it will directly affect the legal and effective use of personal information in criminal investigations. Sixth, the retention of massive data poses risks to

personal information. Data retention is an extension of data collection. It is a manifestation of non-standardized databases. The lack of standardized management combined with database security issues can bring risks such as hacker intrusion, network attacks, and data abuse, which is not conducive to personal information protection.

The path construction of personal information protection in big data investigation should be classified and protected for different information categories, combined with the arbitrariness and mandatory multiple attributes of big data investigation itself, clarify the data application rules for different investigation stages, and construct data mining We will improve the approval and supervision mechanism for big data investigation operations, standardize the data sharing platform, and improve the management of data retention.

【 Key Words 】 Big Data Investigation; Personal Information; Data Analysis Technology; Legislative Regulation; Rights Protection

目 录

引 言【注：引言部分应适当阐述文献综述内容】

大数据实为一种数据集合，其主要特征包括规模大（volume）、速度快（velocity）、类型多（variety）及价值高（value），[1]伴随着时代的快速演变，逐步开展为对具备以上“4V”特征的数据进行技术升级，贯穿初始采集、过程分析及最终利用的全过程，以形成当下热门的新型信息技术。作为一种新兴技术和理念，大数据正逐步渗透人类生活，并逐渐改变人类处理问题的思维及方式。不论是美国开展的“大数据研究和发展计划”，[2]还是日本实行的“智慧日本 ICT 战略”，[3]抑或是德国的“数字议程（2014-2017）”，[4]均体现出近些年来国际上对大数据技术应用的重视与追捧，我国对此亦持积极态度。

2012 年 7 月，国务院颁发了《“十二五”国家战略性新兴产业发展规划》，其中明确提出要发展“新一代信息技术产业”，并强调其为未来重点发展方向之一。而后一年，工信部发布的《关于数据中心建设布局的指导意见》为我国数据中心的高效建构和优化布局指明方向。2015 年 4 月，我国首家大数据交易所，即贵阳大数据交易中心建成，给数据的流通及利用提供有力渠道。经过 4 个月后，《促进大数据发展行动纲要》的颁布引领拥有数据资源的主体树立开放共享理念，并逐步开展相关行动。同年 10 月，“实施国家大数据战略”在十八届五中全会被正式提出，意味着与大数据相关的应用及其发展，已被提升至顶层设计之高度。2016 年 3 月，“十三五规划纲要”中开始提倡要全面促进大数据发展活动。[5]

随着政策的推行落实，公、检、法、司部门开始重视大数据的运用，逐步将大数据技术应用于刑事司法领域。公安机关前期构筑的信息化平台给大数据技术奠定深厚基础，使之在刑事侦查工作中顺利打开局面，而后随着技术层面的不断成熟与进步，催生出智慧警务模式的形成。在此背景下，大数据侦查顺应时代，应运而生。

---

[1] 参见史卫民：《大数据时代个人信息保护的现实困境与路径选择》，《情报杂志》2013 年第 12 期，第 155 页。

[2] 李国杰、程学旗：《大数据研究：未来科技及经济社会发展的重大战略领域——大数据的研究现状与科学思考》，《中国科学院院刊》2012 年第 11 期，第 647 页。

[3] 魏江红、李彬、祝慧琳：《制定我国大数据战略与开放数据战略：日本的经验与启示》，《东北亚学刊》2016 年第 6 期，第 25 页。

[4] 张影强、张大璐、梁鹏：《发达国家推进大数据战略的经验与启示》，《国际经济分析与展望（2017-2018）》，第 369 页。

[5] 参见王燃：《大数据侦查》，清华大学出版社 2017 年版，第 24-25 页。

大数据侦查是当下时代的必然选择。一方面，因当前复杂犯罪态势的出现，传统侦查难以应对。即犯罪分子开始利用科技提升其犯罪能力，犯罪时空、犯罪因果联系呈现的复杂交织状态，使得当前犯罪愈发凸显隐蔽、新型化特征。相关官方数据表明：2012 年，全国侦破涉及网络犯罪案件累计 11.8 万余起，抓获犯罪嫌疑人 21.6 万余人。[6]2017 年，中央政法工作会议指出：“中国网络犯罪占犯罪总数的 1/3，并以每年 30%以上的速度增长。”[7]2019 年 11 月，最高人民法院发布的《网络犯罪司法大数据专题报告》中指出，近两年网络犯罪案件已结 4.8 万余件，涉网案件数量呈逐年上升趋势，相应的在刑事案件总体中的所占比例亦逐年增多。在占案件总量比例近三成以上的诈骗案中，涉及网络诈骗案件的比例有 19.16%。该类案件因犯罪分子是在已获取受害方个人信息的前提下实施，精准诈骗形式大大提高了诈骗得逞的可能性。[8]2020 年，据长沙市警方公布的官方数据显示，电信网络类新型违法犯罪案件已占刑事案件比重高达近四成。[9]

另一方面在于侦查技术的不断升级，使得大数据在侦查领域显现出巨大的应用空间。如 2016 年，泉州市丰泽区检察院构建的“智慧检察大数据分析平台”，实现了数据采集、趋势研判和预警处置三大功能，有效辅助侦查决策，实现精准打击。[10]2017 年济南市公安构筑智能化警务实战体系，实施智慧防控，设立涵盖 200 多个分析模型的“预警超市”，实现跨区域平台数据分析、可视化事前预警形式和智能化实时推送方式等，指导警力精准投放、精细防范，取得该市全范围立案比例同比下降 8.1%，日均刑事报警 50 起左右，连续 7 年命案全破，267 天街面“两抢”零发案的好效果。[11]

然而，大数据技术在促进侦查高效智能化发展的同时，也暴露出刑事司法领域中个人信息保护的新法律难题，其中备受关注的便是大数据侦查运行下对个人信息保护的问题。侦查机关借力于信息技术的发展，在网络监控、数据平台等建

6 参见李建利、李宇尘：《大数据在刑事侦查中的应用研究》，吉林大学出版社 2017 年版，第 1 页。
7 汤瑜：《中国网络犯罪占犯罪总数 1/3 每年 30%速度增长》，资料来源：民主与法制时报 http://e.mzyfz.com/paper/808/paper_14970_4302.html，访问日期：2021 年 3 月 18 日。
8 参见刘婧：《依法打击网络犯罪 维护清朗安全网络环境》，资料来源：中国法院网 https://www.chinacourt.org/article/detail/2019/11/id/4644723.shtml，访问日期：2021 年 3 月 18 日。
9 参见李青、廖隆章：《长沙警方通报多起电信网络新型违法犯罪案件》，资料来源：民主与法制网 http://dfcn.mzyfz.com/detail2020.asp?r=t&dfid=17&cid=226&id=411690，访问日期：2021 年 3 月 18 日。
10 参见叶永坚、林扬阳：《泉州丰泽检察院打造“大数据+智慧检察”收效显著》，资料来源：泉州长安网 http://qz.pafj.net/2017/zfyw_0718/2623.html，访问日期：2021 年 3 月 18 日。
11 参见马永文：《实施“三个一”为引领的智慧警务全力打造新时代“安全泉城”品牌》，《山东法制报》，2018 年 2 月 13 日，第 4 版。

设方面取得的成就，为深度收集公民个人信息提供了有力渠道，数据碰撞、数据挖掘等技术应用在案件侦办及犯罪预警等方面处于举足轻重的地位。而与此同时，大数据技术的广泛应用却也将公民个人信息置于史无前例的全方位“超现代化”信息监控和多领域信息存储当中。由于现阶段我国《刑事诉讼法》并未有大数据侦查的相关规定，加之个人信息保护的法律缺失及数据共享机制的混乱，极易引发侦查权的膨胀，带来一系列法律问题，司法实践中已出现了滥用个人信息等违法行为，二者之间的冲突愈发明显，已是亟待解决的现实难题。

一、大数据侦查中个人信息的概述

（一）大数据侦查的基本理论

1. 大数据侦查的概念

欲准确推进程序的适用及运行，则需把握大数据侦查的基本理论，以辨析及明确其概念界定作为切入点。关于大数据侦查的定义，虽学界表达方式有所不一，但大多数学者在其中都重点强调其技术特征，阐述信息的收集及利用对现代侦查所发挥的核心功能。对其概念的释义，目前大致可以分为两类：一类是将数据技术作为侦查背景，强调该技术为案件侦查提供了数据基础、方法指引及专业处理，以高效实现侦查目的；[12]另一类是以大数据技术推动侦查模式的革新为出发点，由内到外的更新侦查理念、重构侦查模式，以释义大数据侦查。[13]

然而，传统侦查是否因大数据而实现根本上的实质转型，学界莫衷一是。有观点对此持肯定态度，主张大数据侦查不仅针对已然犯罪，亦重视对未然犯罪的预防，并凸显技术性特征，是通过采取数据挖掘等技术方式，固定证据、证明犯罪或预测犯罪的一种现代化侦查模式。[14]相反，亦有学者提出目前学界太夸大于大数据对侦查的影响，对此观点提出质疑，认为大数据只是侦查的一个要素，并未导致侦查实践发生根本性变革。[15]

当前以大数据技术应用为主的智慧警务模式在侦查工作中发挥至关重要的作用，其承袭了历史不同阶段的应用模式，并有了创新式的发展。[16]大数据侦查的对象可以分为两类：一类是与传统侦查的对象一致，即对已发生的、确已立案的犯罪活动进行侦查；另一类则是基于大量概括性数据分析得出的犯罪预测，针对尚未发生或者即将发生的犯罪活动予以预警，从而起到风险防控的作用。

单从前类针对已然犯罪的侦查活动，大数据侦查可被视为系处于信息社会中传统侦查在虚拟空间侦查能力上的强化和升级。具体而言，侦查活动是司法实践中侦查人员和犯罪事实之间进行的信息互换的过程。[17]在这一过程当中，侦查人员通过对侦查活动中获取的犯罪分子遗留下的动态信息引导侦查人员的实践认知，

---

12 参见李蕤：《大数据背景下侵财犯罪的发展演变与侦查策略探析——以北京市为样本》，《中国人民公安大学学报（社会科学版）》2014 年第 4 期，第 154 页。

13 参见何军：《大数据与侦查模式的变革研究》，《中国人民公安大学学报（社会科学版）》2015 年第 1 期，第 72 页。

14 参见杨婷：《论大数据时代我国刑事侦查模式的转型》，《法商研究》2018 年第 2 期，第 29 页。

15 参见彭知辉：《“大数据侦查”质疑：关于大数据与侦查关系的思考》，《中国人民公安大学学报（社会科学版）》2018 年第 4 期，第 28-29 页。

16 参见张可：《大数据侦查之程序控制：从行政逻辑迈向司法逻辑》，《中国刑事法杂志》2019 年第 2 期，第 133 页。

17 参见樊崇义、张自超：《大数据时代下职务犯罪侦查模式的变革探究》，《河南社会科学》2016 年第 12 期，第 43 页。

从而形成犯罪事实过程的回溯。传统的侦查模式大致采取的摸底排查、现场勘查、询问、讯问和技术侦查等各种侦查行为，获取涉案人员的案件信息，基本环节包括“立案——现场勘查——现场分析认识——确定犯罪嫌疑人——破案”，形成“信息引导认知”的运行模式。而大数据侦查就已然犯罪的侦查基本环节包括：“立案——案件数据的收集、分析研判——确定犯罪嫌疑人——破案”，形成“数据引导认知”的行为模式。就两者的运行模式进行比较分析，发现模式构成基本一致，仅是空间上存在变化，即由传统的现场勘查等侦查措施变化为对案件数据的收集及研判分析，侦查行为从现实空间向虚拟空间延伸，大数据侦查为传统侦查模式提供了技术支持，使其在当下时代得以强化和升级。

而就后类基于数据的分析研判对犯罪行为进行预警的这一侦查行为，便不同于传统侦查。以类型理论划分，侦查存在被动型及主动型两种侦查模式。被动型侦查模式的侦查对象针对的是已然犯罪，而后者侦查模式针对的是未然犯罪，包括进行时或将要实施的犯罪行为。[18]基于犯罪时空的难以逆转，一般认为，被动型侦查模式更加符合犯罪规律及侦查本质。然而，当下复杂的犯罪态势致使往常依托密集人力和经验法则的回溯型侦查模式已捉襟见肘。

而以数据驱动的大数据侦查模式为主动型侦查模式的实施创造了条件，提供了强有力的基础，推动传统侦查模式由被动型向主动型转变。该转变主要基于大数据技术中所包含的预测分析功能，借力于该强大技术，驱使侦查行为的介入时间大大提前。[19]如 2015 年以来，浙江省嘉兴市平湖公安构建的“可视化智慧平台系统”，该系统发挥大数据技术的中枢功能，通过智能分析研判及有效预警防控，致使该区实现连续十五天刑事警情零现象。[20]大数据侦查改变了以往的思维定式，形成了以数据为核心的发散性侦查思维模式。

有学者就此提出质疑，认为侦查启动的时间通常在立案之后，由此主张犯罪预测不属于案件侦查范畴。[21]然而，该观点明显片面化。在刑事司法中，刑事侦查实属一个重要阶段，其基本功能除查明犯罪事实以外，还包括犯罪预防和减少犯罪发生。[22]以往，我国大部分学者都是根据《刑事诉讼法》第 108 条第 1 款规定来理解侦查的内涵，并由此主张须在立案之后才能启动侦查。[23]

尽管传统侦查的概念基本形成通说，但目前就侦查活动而言，具有明显的启

---

18 参见彭知辉：《“大数据侦查”质疑：关于大数据与侦查关系的思考》，《中国人民公安大学学报（社会科学版）》2018 年第 4 期，第 28-29 页。

19 参见于阳、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》，《情报杂志》2018 年第 12 期，第 148 页。

20 参见李建立、李宇尘：《大数据在刑事侦查中的应用研究》，吉林大学出版社 2017 年版，第 2-3 页。

21 参见彭知辉：《‘大数据侦查’质疑：关于大数据与侦查关系的思考》，《中国人民公安大学学报（社会科学版）》2018 年第 4 期，第 29 页。

22 参见王梦瑶：《大数据背景下侦查创新研究》，中国人民公安大学 2018 年博士学位论文，第 31 页。

23 参见王燃：《大数据侦查》，清华大学出版社 2017 版，第 31 页。

动时点前移的趋势。[24]以初查这一行为为例，从法律层面来说，2016 年出台的《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》中明确表明初查过程中收集、提取的电子数据可以作为证据使用，并有学者专门就初查行为应属任意性侦查措施还是强制性侦查措施展开研讨，以期完善初查行为的法律规制；[25]在司法实务中，因犯罪事实或犯罪嫌疑人的无法确定，时常会采取一定的调查措施将案件初查。由此可见，不论在立法层面抑或司法实务中初查都被认定为侦查，以明确立案作为侦查的起点来质疑大数据侦查的犯罪预警并非属于侦查范畴的这一观点具有一定局限性。

综上，大数据侦查模式较之传统侦查模式，外延要更宽，技术性更强，目的更加全面，其弥补了传统侦查模式的不足，并推动了传统侦查在信息时代的转型及升级，是当下时代应对复杂犯罪态势的必然选择。其具体是指通过利用数据技术，对存储于网络平台或计算机系统中的海量数据信息进行收集、共享、整合、比对、挖掘和分析，进而发现犯罪线索、收集犯罪证据、缉获犯罪嫌疑人和预测犯罪的侦查模式。

2. 大数据侦查的特征

其一，侦查空间的数据化。信息化时代亦是触物留痕的时代，促使与现实空间相对应、相平行的虚拟数据空间形成，人们的行为呈现现实空间和虚拟空间的交叉融合，使我们每个人几乎都可以在数据空间中找到与自己相对应的数据。大数据侦查则是在该平行数据空间中所展开。[26]大数据技术推动了物的数据化，实现了非结构化的多类信息向结构化标准信息转换的现实途径，[27]使侦查人员可根据现实空间的人、事、物去找到其对应的数据痕迹，再通过数据清洗、挖掘、碰撞、比对、聚合分析等技术将犯罪线索从数据空间往返至现实空间，通过在两空间的交叉、数据之间的碰撞，会显现出更多潜在的犯罪线索，继而利于案件侦破。

其二，侦查技术的智能化。数据运算实为大数据侦查模式的运行中枢。即大数据侦查运行的基础在于对所搜集的数据信息的开发应用，而其中的数据往往会达到“TB”甚至“PB”的海量级别。[28]正是基于此，面对海量的数据信息单纯依靠传统的人工分析显然是微不足道，且不切合实际的，而必须凭借专门的智能算法，并依托于数据碰撞、数据挖掘等技术支撑。数据碰撞技术旨将多方数据进行

---

[24] 参见裴炜：《个人信息大数据与刑事正当程序的冲突及其调和》，《法学研究》2018 年第 2 期，第 50 页。
[25] 参见梁坤：《论初查中收集电子数据的法律规制——兼与龙宗智、谢登科商榷》，《中国刑事法杂志》2020 年第 1 期，第 39-40 页。
[26] 参见王燃：《大数据侦查》，清华大学出版社 2017 年版，第 35-36 页。
[27] 参见倪春乐：《大数据侦查的样态和机理》，《中国人民公安大学学报（社会科学版）》2019 年第 5 期，第 43 页。
[28] 参见王燃：《大数据时代侦查模式的变革及其法律问题研究》，《法制与社会发展》2018 年第 5 期，第 112 页。

对比、碰撞，再依据专业平台自动生成的重合或交叉数据结果进行深度分析的技术，其一般遵循确定对象、筛选数据、数据碰撞及研判分析的步骤。如因某地出现多起电话诈骗案件，侦查人员通过收款账户的取款信息，逐一调取取款监控视频，发现取款人为同一名青年男子，并且在取款时均有拨打电话的行为，于是侦查人员以此为切入点，通过调取每次取款地点附近的通信基站数据，并根据监控视频中的男子每次拨打电话的起止时间来确定基站数据的时间范围，将两者数据进行碰撞，得出的交叉数据进行分析，便可锁定犯罪嫌疑人的电话号码，再反向查获犯罪嫌疑人。[29]而数据挖掘技术则侧重发现潜在隐含信息，通过将不同渠道收集的浅表化、零散化、碎片化数据进行整合聚类分析，以提取其中有效信息的过程。整体而言，大数据侦查的各运行阶段都会运用到数据算法、智能分析等技术，其运行过程以数据为载体，通过对数据采集、清洗、比对、挖掘和分析从而发现犯罪线索，侦破案件。[30]可见，大数据技术开启了案件分析的智能化时代。

其三，侦查行为的主动化。相对于以往依靠举报、报案等形式开展的“被动式”侦查，大数据技术促使侦查人员可依托于大数据智能算法，推动侦查权的作用时段向犯罪的早期阶段延伸，实现主动型侦查的现实可行性，凸显犯罪预警功能，解决了以往在案发初期因与犯罪行为之间存在时间上的延迟和滞后导致难以主动侦查的问题。以非法集资案件为例，大数据侦查犯罪预警的运行模式系基于对既往涉及该类案件的犯罪活动轨迹、主要人物特征、资金基本流向等情况的充分了解和掌握，通过规模性分析历年涉及该类案件的数据样本，借助数据平台自动生成的分析结果，建立相应的数据预警模型，再将该模型用至当地的实时监测中，便能自动识别出异常数据，继而触动该预警机制，随之查处异常数据对应的犯罪案件。以往非法集资类案件因涉案人员繁多、金额巨大、侦查难度大等问题，极易引发重大社会矛盾，而随着我国“以网治网”的监测预警体系的形成，经过集中整治，非法集资风险总体可控，并取得 2020 年全年共侦办该类案件 6800 余起，涉案金额 1100 余亿元，抓获犯罪嫌疑人约 1.6 万的好成绩，[31]发挥了侦查权对犯罪行为的实时控制效能。

（二）个人信息的界定

个人信息概念之界定直接关乎个人信息保护规则的适用及规制范围，然而各国对个人信息的概念并未有统一的界定标准，因而有探讨的必要性。

---

[29] 参见王燃：《大数据侦查》，清华大学出版社 2017 年版，第 117-118 页。

[30] 参见何军：《大数据与侦查模式变革研究》，《中国人民公安大学学报（社会科学版）》2015 年第 1 期，第 77-78 页。

[31] 参见熊丰：《2020 年公安机关立案侦办非法集资犯罪案件 6800 余起》，资料来源：正义网 http://news.jcrb.com/jsxw/2021/202101/t20210108_2240217.html，访问日期：2021 年 3 月 18 日。

欧盟在《一般数据保护条例》(GDPR)中指出：“‘个人数据’是指已识别到的或可被识别的自然人的所有信息”，新加坡的《个人数据保护法》中指出个人信息是指可通过信息单独识别或通过与其他信息结合后识别出个人的信息。而在美国，基于培植本国的信息产业，促进行业发展，对个人信息保护采取了“补充已有法律（主要是隐私权保护法律）+行业自律”的立法模式，经过长期的发展，致使至今美国的信息隐私保护法呈现出“多、杂、乱”的分散局面，存在众多不协调、不理性且内容不一的联邦和州法律规则。美国法律虽对个人信息并没有统一的界定标准，[32]却常以可识别个人身份的信息（personal identifiable information）指代个人信息。

在国内，学界对“个人信息”的内涵界定，主要存在“隐私型”“关联型”及“识别型”三种学说。“隐私型”定义模式许是受到英美国家相关立法及理论学说等影响，将个人信息直接定义为隐私。但结合我国现状来看，该定义明显过于狭隘。虽就个人信息与隐私的关系界定方面，学界多呈现不同的观点阐述，但不论是“个人信息包含说”，抑或是“个人信息与隐私二分说”，都凸显出个人信息较隐私范围更加广泛之特征，如若单以隐私定义个人信息，保护范围的狭隘性则无法覆盖除个人隐私以外的其他个人信息全范围，在此前提下，则难以对个人信息进行有效保护。“关联型”定义模式则侧重个人与信息之间的关联性，主张个人信息是指与个人相关的一切事项。[33]虽在大数据时代，与个人相关的信息呈现喷发式态势，但该种定义过于宽泛，若将与个人相关的所有信息都认定为个人信息予以保护的话，明显不利于对个人信息的合理使用。“识别型”的定义模式则强调的是信息与信息主体之间被直接或间接识别出来的可能性，该定义亦是学界通说。如齐爱民教授提出个人信息是指一切可以识别到本人的信息的总和。[34]我国《网络安全法》第 76 条第 5 项的规定亦是典型的“识别型”定义。

综上可以看出，“识别性”的定义模式不仅是世界主流立法所采取的模式，亦是我国立法实践中所采用的主流观点。但基于“可识别”本身的弹性范畴，致使“可识别”的信息范围界限模糊化，即如今的信息时代，技术的升级应用已经可以将即便是不具有识别性的个人信息转化为可识别性信息。例如指纹、DNA 等信息不需要任何其他信息即可识别到个人，而经济状况、个人性格特征等信息通过信息聚合效应或借助其他信息亦可将个人予以识别。在这种“只要外部条件充分，任何信息都具有可识别性”的情况下，极易出现需要保护的个人信息被泛化。对此，需对个人信息进行分类处理，才得以适应时代发展，搭建可行保护措施。

---

[32] 参见孔令杰：《个人资料隐私的法律保护》，武汉大学出版社 2009 年版，第 108-109 页。
[33] 参见吴苌弘：《个人信息的刑法保护研究》，上海社会科学院出版社 2014 年版，第 14 页。
[34] 参见齐爱民：《论个人信息的法律属性与构成要素》，《情报理论与探索》2009 年第 10 期，第 28-29 页。

（三）大数据侦查中个人信息的特殊性

1. 个人信息的海量性

传统侦查活动中，侦查机关办案并不倚重个人信息，当然，受当时技术条件的限制，也无法深度收集个人信息。随着“向科技要警力”“科技强警”等理论指引，“金盾工程”“智慧公安”等公安信息化建设成果愈发卓著，加之信息在侦查领域的价值愈发凸显，促使侦查部门对数据信息的十分依赖。目前，侦查部门已掌握了大量的警务数据，并呈现无上限的不断扩充趋势。

早在 1998 年，为实现刑侦一线的战略目标，增强犯罪治理能力，“金盾工程”的建设方案被提出，核心内容即是创新并优化公安部门的通信网络和计算机信息系统。2006 年，初步建立的通讯信息网络、应用数据库及共享平台的顺利完成，为大数据技术在侦查的应用奠定了数据基础及多层架构，随后工程二期的完善，基本实现了公安内部的信息化。[35]而后接连开展的“三基”工程建设、“三项建设”“大情报战略”及“智慧公安”建设，促使各地侦查部门开展探索大数据与犯罪分析业务，旨在通过对海量信息的深度融合应用，挖掘其中犯罪线索，以提升刑侦效能。

大数据侦查在运行过程中所需要的信息数据系通过建库的方式存储，宏观上大致分为基础性信息资源库、专门的数据信息资源库以及针对新型犯罪案件的正在建设的新型信息库等。[36]其中包含的数据信息种类多样，包括姓名、性别、年龄、电话号码、身份证号、学历等个人基本信息；血型、指纹、虹膜、DNA 等个人生物特征信息；收入和财产情况、银行账号、病史等个人敏感信息等。整体而言，公安内部信息系统已涵盖刑事、监管、交通等领域高达 PB 级的数据信息，[37]凸显数据的巨型特征。

2. 个人信息的易获性

一方面，基于数据共享战略的部署落实，侦查机关借助相关政策推进，同步享有了信息共享渠道，使其极易获取来自其他政府部门的数据信息。随着《关于加强信用信息共享及司法协助机制建设的通知》《政务信息资源共享管理暂行办法》[38]等数据共享战略的部署落实，加之国家数据及各级政府部门数据共享网站的纷纷建立，为公安部门“引数据入库”提供渠道，致使公安机关内容信息库覆盖

---

35 参见张可：《大数据侦查之程序控制：从行政逻辑迈向司法逻辑》，《中国刑事法杂志》2019 年第 2 期，第 132 页。

36 参见楼叶：《大数据背景下警务数据挖掘的法制化》，中国人民公安大学 2019 年硕士学位论文，第 8 页。

37 参见张兆瑞：《智慧公安——大数据时代的警务模式》，中国人民公安大学出版社 2015 年版，第 1 页。

38 参见裴炜：《个人信息大数据与刑事正当程序的冲突及其调和》，《法学研究》2018 年第 2 期，第 49 页。

范围愈发全面，侦查机关借此亦同步享有了信息共享的红利，[39]即极易获取政府通过人口普查、社会保障、医疗、教育、税收等方面收集到的各类大量数据信息。

另一方面，基于依法协助调查的需要。根据《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》第 3 条及在《网络安全法》《反恐怖主义法》《反间谍法》中的类似规定，使侦查机关极易获取企业、个人等第三方社会层面的数据资源，包括互联网信息、视频监控信息、通讯信息、银行卡信息及如保险、民航、邮政、房产、出租车、物流等各类社会服务信息等，实践中甚至已经出现公私合作现象。如 2015 年，浙江省高级人民法院与国内某网络购物平台签署战略合作协议，以其用户收货地址作为司法文书送达地址。[40]通过该合作，法院可以掌握当事人的身份信息、消费信息、住址信息等。

3. 个人信息的动态性

个人信息的动态性是指信息实时更新、主动反馈以及自动生成。信息的实时更新主要体现在大数据侦查中信息采集时的智能化、实时化。传统的信息采集往往通过人工事后录入的方式，而随着物联网的发展，通过全景式网络监控加之智能传感等技术即可自动完成信息的自动采集工作，大大扩展了信息的采集量，并且保证了信息的同步性特征。主动反馈和自动生成主要基于大数据侦查的技术应用，体现在数据分析环节的科学多元化。传统的信息化侦查不仅面临的信息资源有限，而且信息分析工具单一，仅以侦查人员的经验型主观判断为主，以数据翻阅、查询和检索等初步数据分析方式为辅，侦查人员分析能力的强弱直接影响信息中隐藏的案件线索被发现的可能性。而当下面对庞大的信息资源，自然诞生出与之相匹配的信息分析技术。如通过数据挖掘发现数据之间的潜在信息，通过数据画像刻画犯罪嫌疑人的模拟形态，通过犯罪网络关系分析了解犯罪群体之间的分工联系等，在信息完成分析之后，结果会以立体化的数据图或结合图像等形式对侦查人员进行全面性反馈，利于侦查人员更为直观、深入的获取线索。

4. 个人信息的主体多元性

以往的实地走访、摸底排查等传统的侦查过程中，侦查对象仅局限于一个或特定的几个犯罪嫌疑人，而大数据侦查的运行根植于其所获取的各类数据信息，上文亦有所阐述，我国大数据侦查的数据来源广泛且具备海量性、易获性等特征，这便意味着侦查对象从特定个体发散成为不特定的社会成员，呈现出不以犯罪嫌疑为前提，收录个人信息的主体泛化现象。

---

[39] 参见蒋勇：《大数据时代个人信息权在侦查程序中的导入》，《武汉大学学报（哲学社会科学版）》2019 年第 3 期，第 158-159 页。

[40] 参见陆玫：《浙江高院与阿里合作 法律文书寄到淘宝收货地址》，资料来源：搜狐新闻 http://news.sohu.com/20151124/n427933546.shtml，访问日期 2021 年 3 月 18 日。

与以往活动于物理空间的犯罪不同，延伸至虚拟空间的网络犯罪活动，由于其电子数据自发的发散性、分离性等特点，致使相应的侦查范围需扩张至多个不特定位置与场合，并需利用实时监控等方式进行行踪拓展、轨迹分析。[41]大数据侦查为实现空间、时间的重构，可将相关信息进行整合。在此过程中，则需利用不特定社会成员的个人信息一并进行数据分析，加之现有的多领域数据监控及现代信息抓取智能技术的愈发全面成熟，基于侦办案件需要，监控中所收录的各类个人信息都能成为潜在的侦查分析对象。可见，在大数据侦查中所搜集、利用的个人信息具有主体多元性特征。

[41] 参见李双其等著：《大数据侦查实践》，知识产权出版社 2019 年版，第 10 页。

二、大数据侦查中个人信息保护的理论基础

（一）个人信息保护理论

随着社会信息化的逐渐发展，个人信息成为与物质、能量同等重要的新型资源，促使整个社会对信息的开发利用。个人信息虽给社会带来诸多效益，却也使信息主体的权益更易受到侵害，这便是个人信息保护理论产生的缘由。[42]

个人信息本身所承载的价值呈现多元化特征，其中主要包含道德价值、商业价值及政治价值。[43]道德价值凸显人格权属性。随着个人信息记录的数字化形态出现，加之可识别性特征，个人不再是活生生的个体，而是成为以名字、符号和标识为载体的档案，形成个人在数字空间的“信息化形象”，指向现实空间中的信息主体。商业价值凸显财产权属性，其可追溯到个人资料财产化理论。虽不少学者对个人资料财产化理论提出质疑和批判，但都是基于认同个人资料已成为市场上畅销的商品所引发的争论。[44]时代发展至当下，个人信息已成为了一种新型资产，是社会生存和发展的崭新生产力。如企业可通过数据整合技术，将其收集和积累的消费者信息汇总并进行精细化处理，以预测消费者的购物倾向，对产品进行精确定位，并有针对地制定营销策略，以达到促进营销的目的，凸显个人信息的商业价值。

政治价值源自于个人信息中的社会属性部分。身处信息时代的我们，时刻需要社会提供的信息资源及利用该资源所搭建的公共服务，在享受其所带来的福利的同时，需付出对价的个人信息。为预防突发事件的发生，对社会进行有效治安管理，在公共领域安装监控摄像头已是常规做法，对个人信息的收集、利用及处理已成为提高国家治理能力的主要手段之一。这便意味着出于社会治安、公共管理、国家安全等需要，国家公权力所及之处必然会涉及到公民个人信息，加之信息时代的技术强化，致使公民个人信息收集更加快捷、内容更加丰富、信息关联度极高。在此背景下，个人信息的多元价值虽愈发展现，却也意味着所涉及的公民个人信息范围及内容更加深度且广泛，极易造成侵犯，亟需进行保护。

（二）信息隐私权理论

信息隐私权理论系由传统隐私权理论发展演变而来。传统隐私权理论多以个人为视角，将个人视为私密性生活的部分来界定隐私的概念范畴，致力于保护私人生活，及保障个人的独处状态或对自我信息的控制，大致可分为三大类：“独

---

[42] 参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，《中国法学》2015 年第 3 期，第 45 页。

[43] 参见袁泉：《个人信息分类保护制度的理论基础》，《上海政法学院学报》2018 年第 3 期，第 30 页。

[44] 参见孔令杰：《个人资料隐私的法律保护》，武汉大学出版社 2009 年版，第 74-88 页。

处权说”“有限地接近自我说”和“个人信息控制权理论”。[45]

“独处权说”最早出现在 1890 年，于沃伦和布兰蒂斯合著的隐私权奠基之作——《论隐私权》中，但两人并未明确界定隐私概念，而是沿用由库利（Thomas Cooley）法官提出的独处权，认为个人有权选择自己的生活方式，除非存在明确合法依据，否则不受外界的干涉与侵害，[46]并认为个人人格不容侵犯这项基本原则是隐私权的理论基础。[47]但由于未明确限定不受外界干扰的事项范畴，加之人格权本身即是一个相当模糊的概念，由此不少学者在“独处权说”的基础上进行延伸，逐渐形成“有限地接近自我说”。有限接近的隐私权理论强调人人均有权将自己的事务保留，自行决定公众一般可了解其多少的个人情感、私人行为及事务，该理论将“独处权说”的与世隔绝、不受外界干扰的状态一脉相承，却又超出了“独处权”的范畴。“有限接近自我说”强调个人有权自行选择披露自己事物的范围或者决定他人接近自我的最低限度，其以人际关系为出发点，引发了信息控制权理论的产生并推动其发展。[48]“个人信息控制权理论”强调隐私应该是个人控制个人信息的能力。20 世纪中后期，随着信息革命的出现及个人信息的技术发展，信息价值愈发凸显。在此背景下，以个人信息控制权为核心的信息隐私权理论在美国应时而生。

从域外的相关立法来看，早已将个人信息上升为“权利”进行保护。如美国联邦最高法院在 1977 年的惠伦诉罗案（Whalen v.Roe）中将“信息性隐私权”阐述为自然人享有控制其个人信息被披露的权利以及享有独立作出免受政府影响的决定的权利。[49]目前我国的相关立法虽未将个人信息上升为“权利”，但已明显将其当作一种“权益”进行保护，不仅在《民法典》中就个人信息的相关规定有所体现，甚至已有学者提出在刑事司法领域，个人信息权系作为一种刑事诉讼权利，需对其进行保护。[50]

以往侦查中出现的刑讯逼供、非法拘禁等违法侦查产生侵害人身权利等问题，《刑事诉讼法》予以重点关注并通过出台法律及相关司法解释有效规制，而随着“经验依赖型侦查”向“数据驱动型侦查”转变的侦查背景下，个人信息有关的权利也应成为在侦查领域中新的个人权利保障的核心内容。当下的《刑事诉讼法》领域中个人信息保护的法律空白明显过于滞后，伴随着数据利用技术的愈发成熟，个人信息的保护需加快提上日程。

---

45 参见孔令杰：《个人资料隐私的法律保护》，武汉大学出版社 2009 年版，第 63 页。
46 Thomas M.Cooley, *Law Of Torts,* Calllaghan &Company,2nd ed, 1888, p. 29.
47 Samuel D.Warren and Louis D. Brandies,*The Right to Privacy,*Harvard Law Review.Vol.4,No.5,1980,p.205.
48 参见孔令杰：《个人资料隐私的法律保护》，武汉大学出版社 2009 年版，第 62-74 页。
49 See Whale v.Roe,429 U.S.589,1977. 转引自何渊：《数据法学》，北京大学出版社 2020 年版，第 35 页。
50 参见郑曦：《作为刑事诉讼权利的个人信息权》，《政法论坛》2020 年第 5 期，第 133-144 页。

（三）价值平衡理论

刑事诉讼中历来存在惩罚犯罪和保障人权两种价值之间的冲突与平衡。当下信息时代，犯罪分子开始运用科学思维、利用信息技术实施犯罪，犯罪手段和形态的日新月异，使得犯罪愈发的隐蔽化、新型化和虚拟化，这便要求国家需提升打击犯罪的能力以应对当今的复杂犯罪态势。大数据技术的应用给大数据侦查带来新型数据分析方法及数据思维模式，不仅实现了侦查技术上的升级，亦引发侦查思维上的革新，使其较之传统侦查模式有着无法比拟的综合优势及应用前景。同时，信息社会中个人信息凸显的价值及优势，必定催发了侦查领域对个人信息的依赖，而随着侦查技术的不断升级必然伴随国家对公民个人信息的不断深入，从而引发侦查机关对个人信息利用与保护之间的矛盾。

在信息时代，侦查机关对个人信息的利用与保护便是惩罚犯罪与保障人权两者价值的直接体现。大数据侦查通过对个人信息的利用促进侦查高效化，其上位利益正是国家打击犯罪的需求，而主张个人信息保护便体现对公民基本人权的保障。上文有所提及，现代化信息技术愈发成熟，可实现对不同领域中的个人相关数据信息进行有效整合，形成个人的“人格剖面图”，关涉个人的方方面面，体现信息主体的人格尊严和自由价值。[51]从域外的相关立法也可体现。美国将个人信息权视为是一种具有强烈人格权属性的隐私利益，为了保护“个人不被打扰的权利”，强调侵犯个人信息权将会对人格自由和尊严的损害，对个人信息保护主要通过隐私权相关的法律予以规制，并将隐私权的价值理念视作个人信息权保护的基础理论之一。欧洲的个人数据保护理论的建立之基亦是为了保护人的尊严，认为个人数据亦应当由数据主体掌控，体现个人意志。[52]

我国《宪法》第 40 条系对个人通信自由和通信秘密等个人信息最权威、最原则性的保护。[53]通常来说，国家不得干涉、侵害公民的个人信息，除非是出于保护国家利益或社会利益等，[54]但这也并非意味着国家为查明案件事实可以无限度的利用公民个人信息。惩罚犯罪和保障人权是刑事司法中不可分割的两个方面，面对多元冲突的价值利益，可通过程序设置等方式综合考量，借力于立法规制实现对不同利益上下位阶的合理安排，以寻求最佳的平衡点。

---

[51] 参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，《中国法学》2015 年第 3 期，第 45 页。

[52] 参见高富平：《个人信息保护：个人控制到社会控制》，《法学研究》2018 年第 3 期，第 92 页。

[53] 参见李亮：《新刑事诉讼法中个人信息保护的检视与路径探索》，《海南大学学报（人文社会科学版）》2014 年第 2 期，第 90 页。

[54] 参见谢登科：《论技术侦查中的隐私权保障》，《法学论坛》2016 年第 3 期，第 35 页。

（四）分层保护理论

以立法规范是否呈现比例化与精细化为区分，可将个人信息保护模式划分为统合性保护模式和层级化保护模式。[55]传统的个人信息保护模式主要采取的是统合性保护模式，即采用了统一立法的方式，对个人信息并未予以区分规制。[56]在欧盟，《个人数据保护法》虽在初始仅针对政府机构，但在 1995 年《个人数据保护指令》中将公共机构和私人机构一并纳入调整的范畴，形成统一的立法模式。在美国，虽基于信息经济发展的考量采取了部门立法模式，但其初期对个人数据保护的立法亦是只针对政府机关的数据处理行为，制定了 1974 年《隐私法》，而后因发现部分商业部门也在大规模的处理个人数据，于是将立法范围扩张至包括商业部门。实际上，许多最初仿效美国进行部门立法模式的国家，在后期都改采为统一的立法模式。[57]

统合性保护模式虽具有全面系统、易理解执行等优点，却违背比例原则，未充分考虑不同的信息需要进行区别保护，呈现立法的粗疏化。因信息本身存在不同类别，致使在信息收集、利用及处理之时对个人造成的风险呈现大小各异，需区分不同的个人信息予以不同程度的保护及利用。层级化保护模式以比例原则为轴心，对个人信息进行类型化区分保护，呈现的梯度保护模式符合宽严相济的程序特点，满足信息时代对个人信息保护的现实需求。如荷兰法律将数据划分为一般与敏感，规定在取得检察官授权的情况下，针对相对严格的犯罪，警察可以获取一般信息，如果其中包含敏感信息，则警察必须获得逮捕令，并明确其使用的案件范围仅限于特别严重的犯罪。[58]

目前，国内针对大数据侦查背景下个人信息保护问题的相关学说中，都有提及将个人信息予以分类或分层保护的立法建议。[59]侦查部门内部的信息系统呈现内容详尽、范围广泛、真实程度高等特点，加之个人信息本身包括一般信息与敏感信息的分类界限，这便要求对信息进行分类别、分层级保护，使得不同的信息类别在收集、利用、分析、转移等的范围和归责不等同化一，给予不同程度的保护，以期在保护个人信息的基础上，最大程度的发挥大数据侦查的应用价值。

---

55 参见王仲羊：《刑事诉讼中的个人信息保护——以科技定位侦查为视角》，《理论月刊》2020 年第 12 期，第 117 页。

56 参见袁泉：《个人信息分类保护制度的理论基础》，《上海政法学院学报》2018 年第 3 期，第 33 页。

57 参见郭瑜：《个人数据保护法研究》，北京大学出版社 2012 年版，第 108-109 页。

58 参见王仲羊：《刑事诉讼中的个人信息保护——以科技定位侦查为视角》，《理论月刊》2020 年第 12 期，第 117 页。

59 参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，《中国法学》2015 年第 3 期，第 51 页。

三、大数据侦查对个人信息保护的挑战

大数据技术是一种超越以往常规数据库操作范围的数据获取思维，[60]其能够关注并获取到多样混杂海量数据之间的相关关系。[61]大数据侦查正是基于对该技术的利用而催化出的侦查模式，通过利用各种方式搜集到的海量碎片化数据搭建出一个可满足于不同侦查需求的“百宝囊”，不仅为侦破案件提供高效有力渠道，亦为社会治理提供精准预测，甚至还能“深挖余罪”“顺藤摸瓜”。然而，目前我国《刑事诉讼法》中并未有大数据侦查的相关规定，亦未构建针对个人信息的适用规则，加之信息技术运行与传统规则之间难以衔接，造成大数据侦查运行过程中对个人信息保护的严重缺失。

（一）现有立法难以保障刑事程序中的个人信息

近年来，我国关于个人信息保护的制度建设在不断强化。2012 年，《关于加强网络信息保护的决定》的通过打开了我国个人信息保护的立法篇章，其中确立了的关于个人信息保护制度的合法性、正当性、必要性等基础性原则也为之后颁布的多部法律文件奠定基础；2013 年修订的《消费者权益保护法》首次从立法层面详细规定了个人信息保护条款；2015 年《刑法修正案九》增设“侵犯公民个人信息罪”开启对个人信息的刑法保护；2017 年发布的《网络安全法》第四章就个人信息保护作出了相对全面的规定；2019 年《个人信息保护法》被列入立法议程；2020 年的《民法典》对个人信息各项权益保障作出了细化规定。[62]可见，在民法、刑法、行政法中对个人信息保护的立法都取得了相应的进展，可刑事诉讼法却仍然空缺。然而，仔细考究，不难发现现有立法并不能直接适用于刑事司法领域。

从刑法层面上看，难以直接对大数据侦查中的个人信息进行有效保护，简而概之，即缺乏直接性和有效性。虽我国《刑法》规定了侵犯公民个人信息罪，但一方面，该罪名主要规制的是单位及个人，且主要规制的是“出售、非法提供”两种行为，就侦查机关工作人员违规泄露公民个人信息的这一行为，可以以该罪名有效规制，然而就信息的不当收集及使用等侦查行为致使公民个人信息遭受侵害时便无法通过该法条予以保护。可见，刑法的法律规定不能完全涵盖刑事司法领域，尤其是具体到大数据侦查领域的所有问题。另一方面，司法实践中处罚力度低的现实情况，致使难以发挥应有的震慑效果。例如由最高人民法院发布的典

60 参见李媛：《大数据时代个人信息保护研究》，华中科技大学出版社 2019 年版，第 1 页。
61 参见［英］维克托维克托·迈尔·舍恩伯格、［英］肯尼思·库克耶：《大数据时代》，盛杨燕、周涛译，浙江人民出版社 2013 年版，第 27-96 页。
62 参见裴炜：《个人信息保护法与刑事司法的分离与融合》，《中国政法大学学报》2020 年第 5 期，第 149-160 页。

型案例“周滨城等侵犯公民个人信息案”中，各被告人非法出售或购买公民个人信息数量分别高达193万余条、100万余条、7万余条等，行为均已构成侵犯公民个人信息罪，最终判处有期徒刑最高才一年十一个月，并处罚金四万元人民币，最低判处缓刑，并处罚金五千元至四千元不等。[63]可见，在司法实践中侵犯公民个人信息案最终被判处的刑罚并不高，低的处罚力度与现实中可依据个人信息获得的巨大利益相比，并未起到有效的震慑效果。

从民法层面上看，适用原则与刑事诉讼法中的价值目的相冲突。个人信息保护制度多提倡尊重个人的信息自决权，由此主张知情同意原则。然而就该原则而言，是难以适用于刑事侦查领域的。首先，知情同意原则会对侦查行为产生阻碍。顾名思义，该原则包含“知情原则”和“同意原则”，强调信息主体应该知道并同意其个人信息被采集及利用等情况。而在刑事侦查中，侦查活动大多具有强制性，甚至一些侦查取证活动需要在秘密的情况下进行。为达到打击犯罪、确保诉讼程序的顺利进行等目的，侦查过程中涉及到个人信息时，不仅不会事前告知信息主体，亦会要求占有个人信息的第三方主体不予告知，这便难以满足“知情”原则要求。

其次，上文有所提及，大数据侦查系基于信息数据而进行的侦查措施，若适用知情同意原则，极易成为犯罪嫌疑人用来与侦查行为对抗的“武器”。人习惯于趋利避害，倘若司法实践中，侦办案件需对犯罪嫌疑人相关个人信息进行收集、利用时还需要经过其知情并同意，明显不利于开展侦查工作，降低侦查效能。再者，依据相关法律法规，基于侦查的需要，信息控制者还有如实提供的义务，因此“同意”原则基本也难以适用。

即便出于人权保障的考量，防止侦查行为的无限扩张，主张需要征得信息主体的“知情同意”，也并不符合实际。一方面，大数据侦查中的数据库涉及面极广，信息量的庞大致使侦查部门面对的信息客体亦是极其庞杂的，这种客观现实无疑加大了履行成本，不易获得信息主体的同意。另一方面，基于大数据侦查本身的技术性，除对数据进行采集之外，大多致力于数据的二次分析挖掘，致使信息处理呈现频次高、自动性及场景复杂等特征，在这种情况下，侦查部门基于知情同意原则需每一次的数据利用都要征得信息主体的同意是不切合实际的。

可见，现有的个人信息保护立法并不能适用于刑事侦查领域，个人信息保护的法律缺失加之目前大数据侦查的缺乏法律规制，导致在运行过程中对信息的采集范围、方式、途径及相关信息的使用规则等方面，存在着诸多的问题。

---

[63] 参见黄海英：《最高法发布侵犯公民个人信息犯罪典型案例》，资料来源：中国长安网 http://www.chinapeace.gov.cn/chinapeace/c54227/2017-05/09/content_11664900.shtml，访问日期：2021年3月18日。

（二）大数据侦查易对个人信息造成“隐秘性”侵犯

以往侦查机关侵犯个人权利的违法侦查行为通常有迹可循。例如，刑讯逼供会使犯罪嫌疑人肢体上存在淤青、勒痕等明显的伤残痕迹，且对于侵权行为，当事人都是处于明知的状态下。[64]而在大数据侦查中，数据的运行、决策往往依托的是机器设备和编码规则，过程的不透明性意味着对个人数据信息利用过程的封闭性，在此背景下，极易对个人信息造成“隐秘性”侵犯。

一方面，基于大数据侦查中对信息分析的技术应用。互联网时代催生出非接触性犯罪，该犯罪与以往犯罪最大的不同在于其隐蔽性特征。非接触性犯罪的实施主要借助于计算机网络的虚拟空间，依托信息技术手段，在没有与受害人直接接触的情况下，便可实施侵犯国家、社会或个人合法权益的行为，该类犯罪突破地域限制，将传统的现实空间犯罪向数据犯罪延伸。[65]大数据侦查在对该类案件侦破中发挥着至关重要的作用，借助数据技术捕捉虚拟空间的犯罪线索。但在侦查过程中，由于数据来源、运算过程、模型参数的不可视化，亦会造成“侵权的无形化”。

大数据侦查在侦破案件过程中一般遵循着数据准备、确定方向、数据分析、信息验证、确定犯罪嫌疑人等步骤，常用典型方法包括数据调取、数据碰撞、数据挖掘、数据面像及犯罪网络分析等。[66]大数据侦查的各个方法运行都需要技术支撑，继而对基础数据的利用都是置于虚拟的数字化空间。随着侦查人员输入准备好了的数据合集，计算机系统内部会自动将关联数据进行整合，所获得的“数据线索”将通过可视性方式提供给侦查人员，从而为下一步案件侦查提供线索。但是，机器的数理逻辑与人类的主观经验思路毕竟不同，人类会通过因果逻辑思维阐述一件事的“因”和“果”。然而机器所得出的“结论”仅能阐述“结果”，并不会阐释该“结果”产生的原因。信息利用过程的无形化，加剧了对个人信息的“无形侵犯”，伴随着侦查技术的日益成熟，该种侵权方式将会愈发隐秘。

另一方面，基于大数据“监控”。18 世纪中后期，英国哲学家边沁提出了“全景式监狱”的理念，[67]阐述在该理念下被监督者（所有公民）处于随时可能受到监视的状态，但却不知道何时受到监视的类似全景式监狱的现象。[68]在当下的信息时代，该理念所描述的现象似乎已经出现。随着城市视频监控设施的完善及“互联网+”的普及应用，全方位、多领域的实时监控将公民处于公共场所的动态信息尽

64 参见付黎明：《大数据侦查中个人信息保护策略研究》，《警学研究》2019 年第 4 期，第 108 页。
65 参见李鹏：《大数据在非接触性犯罪侦查中的应用研究》，《山西警察学院学报》2018 年第 4 期，第 77-78 页。
66 参见王燃：《大数据侦查》，清华大学出版社 2017 年版，第 109 页。
67 参见程雷：《大数据侦查的法律控制》，《中国社会科学》2018 年第 11 期，第 162 页。
68 参见顾理平：《大数据时代隐私信息安全的四重困境》，《社会科学辑刊》2019 年第 1 期，第 97 页。

数收录，不同角度下记录各类信息，使现代人在无处不在的视频监控中无处遁形。大数据侦查通过选取并整合数据监控中特定时空范围内的信息，以建立虚拟空间，欲对案件事实进行假设性还原。虽打破了时空限制，为侦查提供多元化解决路径，却也侧面加深了大数据侦查对个人信息侵犯的隐秘性。实践中基于侦办案件需要，侦查机关并不会事先告知信息主体便通过监控探头获取了所需数据，如此一来，信息主体对自身信息的初始收集便毫不知情，而后大数据侦查依托于该数据基础，利用虚拟空间进行数据整合利用这一过程更是无法知晓。

加之上文有所提及，基于侦破案件的需要，监控中各类收录信息都能成为侦查分析对象，呈现出不以犯罪嫌疑为前提，收录信息主体泛化的现象。在大数据侦查依靠多领域数据监控，借助于现代信息抓取智能技术，使得侦查对象从特定个体发散成为不特定社会成员的这种情况下，侦查侵犯客体的全员性特征致使其造成的危害远非传统侦查所能相比。

（三）对数据的依赖加深对个人信息的过分采集

信息的充分采集是保障大数据侦查中数据利用发挥其最大效用的基础前提，正是基于对信息的“渴望”，引发了司法实践中侦查部门对个人信息的过分采集。数据时代，大范围监控与网络侦查为信息采集提供有力渠道。犯罪监控机制是大数据侦查的运行机制之一，[69]通过实时监控，可实时捕捉或提取犯罪的相关信息，在此前提下，所获取的信息量大不同于以往的实地走访、摸底排查等传统侦查所采集的信息。同时，在进行网络侦查时，侦查人员会利用技术图形将相应软件程序植入侦查对象的电脑以搜集其犯罪证据，为便于侦查以及确保信息的完整性，一般来说侦查人员都会将犯罪嫌疑人与该案件无关的其他私密信息一并搜集，然而，公民个人信息涵盖的种类繁多、类型多样，但并非所有信息都需要运用在刑事侦查领域，当下司法实践中，对信息的采集已明显超过适度。

2018 年侦查机关依靠人脸智能识别系统在张学友演唱会中屡抓逃犯共 5 名，[70]2020 年 2 月，侦查机关利用 DNA 比对技术将尘封近 28 年的南京医科大学女大学生奸杀案告破。[71]由于在个人信息中的生物样本可以关联到特定个人，生物特征识别技术的应用在当下案件侦办中的作用及地位日益凸显，因而激发了侦查机关对该类个人信息的过分采集欲望。在我国现有的侦查程序中，关乎人身检查的程序规制并未有严格限制，在 2014 年《规范使用执法场所办案区“四个一律”》的规

69 参见何军：《大数据与侦查模式变革研究》，《中国人民公安大学学报（社会科学版）》2015 年第 1 期，第 78 页。

70 参见王阳：《在张学友演唱会上抓逃犯的人脸识别技术真的靠谱吗？》，资料来源：腾讯网 https://new.qq.com/cmsn/20181003/20181003004107.html，访问日期：2021 年 5 月 5 日。

71 参见田芳：《DNA 数据库比对技术在刑事侦查中运用的合宪性问题》，《南大法学》2021 年第 1 期，第 17 页。

定颁布之后，致使实践中只要犯罪嫌疑人处于到案状态，不论最终结果如何，公安机关都会一律将其信息先行采集。[72]据统计，自 2000 年我国在上海成立首个 DNA 数据库后，全国性侦查部门 DNA 数据库应用系统便逐见雏形，早在 2015 年 9 月，系统中便已收录近 4000 万条 DNA 信息，[73]至今全国刑事 DNA 数据库已近 1000 万个，并仍处于继续加速扩编状态。[74]随着大数据侦查对数据库的日渐依赖，更进一步加深了侦查部门对信息采集的动机，实践中已多次出现对个人信息的过分采集事件。如在山东滨州学院发生的一起宿舍失窃事件，为抓获小偷，当地公安机关竟组织采集校内 5 千多名男生的 DNA，并收集被采集者的姓名、年龄、身份证号和家庭住址等个人信息；[75]为侦破“武汉女大学生遇害案”，侦查机关竟采集案发地周围高校数千名男性师生的 DNA 信息。[76]

DNA、人脸等生物特征信息是可直接关联到特定个人的，具有唯一性、稳固性和可识别性强等特征，不论是 DNA 比对技术抑或是人脸识别技术，实质上都是以大数据处理技术为基础的产物，随着大数据侦查的广泛运用，公民个人信息的保障将面临极大的挑战。根据侦办案件需要，除对犯罪嫌疑人以外，经常还需对被害人及其他相关人员进行生物信息的采集，如指纹、毛发等取证或鉴定措施，实践中亦存在违规对被害人等其他相关人员违法取样等情形。这些个人生物信息等敏感信息的获取、利用、保存及如何处置，目前都未有明确的管理机制，若被随意查阅、利用及泄露，对公民个人信息造成的危害将难以弥补。

（四）数据挖掘等技术应用加大对个人信息保护难度

大数据真正的价值不在于“大”，而在于其对海量数据的技术分析利用。大数据侦查亦是如此，依赖于规模化的数据技术应用。例如通过数据挖掘技术，侦查机关可以获得不同层次的价值信息：一是具有浅层次价值的统计分析数据；二是具有深层次价值的数据隐含信息。[77]而对于侦查机关而言，后者价值才是其追求的侦查所需，并已逐步成为未来侦查核心技术的发展趋向。

数据挖掘可被视为 OLAP 的高级阶段。[78]从技术层面上看，数据挖掘有机结合

---

[72] 参见蒋勇：《大数据时代个人信息权在侦查程序中的导入》，《武汉大学学报（哲学社会科学版）》2019 年第 3 期，第 159 页。

[73] 参见刘烁：《全面深化公安机关 DNA 数据库建设发展应用，切实提升精确打击犯罪能力和服务实战水平》，《刑事技术》2016 年第 1 期，第 1 页。

[74] 参见田芳：《DNA 数据库比对技术在刑事侦查中运用的合宪性问题》，《南大法学》2021 年第 1 期，第 17 页。

[75] 参见郭丝露：《被忽视的身体权和隐私权，寝室失窃，全校男生验 DNA》，资料来源：南方周末 http://www.infzm.com/content/94920，访问日期：2021 年 3 月 18 日。

[76] 参见杨京、戴维：《女大学生返校时遇害 数千男性师生被采血验 DNA》，资料来源：腾讯网 https://news.qq.com/a/20131120/001848.htm，访问日期：2021 年 3 月 18 日。

[77] 参见庄乾龙：《刑事案件中大数据整合行为定性及其适用规则》，《法学研究》2020 年第 12 期，第 46 页。

[78] OLAP 是一种在线分析工具，能允许用户以交互方式浏览数据仓库信息，并对其中数据进行多维分析，且能及时地从变化和不太完整的数据中提取与企业经营活动密切相关的信息。

了多种学科技术，包括数理统计、模式识别、数据可视化、图像处理、空间数据分析等，延伸出定性归纳、关联挖掘、聚类分析、异常分析等应用功能。[79]从应用层面上说，数据挖掘过程主要包括了基础准备、规律分析和明确表达。基础准备是对海量数据库中所需数据的提取，具体指数据挖掘技术依托于相关数据源中的所需数据集合；规律分析是指通过算法技术，自动化的将数据集合中的潜在价值提炼出来；明确表达即分析结果的可视性，以可理解的方式将挖掘出的新的信息价值表达出来。以手机数据为例，通过对机主的通话、短信和微信等通讯原始数据分析，可以挖掘出联系人信息、详细通讯频率、所处地理位置、无限网络数据等信息，继而得到该机主的行动轨迹、高频联系人、转账记录等敏感信息。[80]

传统的案件侦破过程主要依靠人力密集型侦查模式，即针对各类证据和线索的分析梳理，主要依托于侦查人员的人力和经验分析，致使以往的犯罪信息处理能力呈现单一性、低效性特征。而当下的数据挖掘技术，在海量数据库的基础上，通过系统中的数据算法，快速使原本散乱的数据信息根据需要进行有规律的排列组合，自动生成数据之间的整合汇总，将潜在的有效信息逐一显现，促进侦查的高效智能化。例如在一起贪污贿赂案件中，侦查人员以华某的手机数据、话单数据、银行数据等为基础，利用大数据平台的智能挖掘技术，获取了有关华某性格特征、人际交往关系、资金流转等方面的详细信息，借此筛选出可疑的行贿人员。与此同时，针对华某手机短信，通过关键词检索筛选出部分可能与案件相关的敏感短信，如由深圳供电局短信告知的用电度数和金额，曾向公安朋友咨询过办理香港移民手续等敏感短信，作出华某在深圳可能存在房产，赃款可能转移至香港地区等推断，巧妙利用所得数据信息，最终成功破获此案。[81]

数据挖掘技术的成熟同时加深了大数据侦查对个人信息的深度侵入性，其模糊了信息边界，使个人信息更加难以保护。巨型数据库中的数据系由结构化和非结构化数据组成，原本数据的杂乱无序，不一定会对个人信息造成侵犯，但通过对数据有意识的重组排列、反复分析、深度挖掘等，对个人信息的侵犯将不言而喻。例如美国塔吉特超市拥有专业的与顾客相关的数据分析模型，利用该数据分析结果对用户进行个性化推荐，使其先于同行精准营销商品。然而，一次通过对某一女性购买了润肤产品、大型挎包、维生素及宝宝用毯等购物信息的精准分析，推断该用户已怀孕，于是便推送怀孕产品优惠券给对方，不料对方竟是一个刚满17岁的女孩。女孩父亲到超市抗议，以此质问该超市竟鼓励未成年少女怀孕，而

[79] 参见李建利、李宇尘：《大数据在刑事侦查中的应用研究》，吉林大学出版社2017年版，第85页。
[80] 参见王燃：《大数据侦查》，清华大学出版社2017年版，第123-126页。
[81] 参见王燃：《大数据侦查》，清华大学出版社2017年版，第98页。

事后才被告知自己女儿的确怀孕的事实。[82]可见，数据挖掘技术的应用使敏感信息通过对非敏感信息的分析即可轻易获取。个人敏感信息虽不完全等同于个人隐私，但因该类信息高度关联个人尊严，泄露和滥用将会给信息主体带来严重损害，故应赋予其与隐私同等的严格保护，而技术的成熟加大了对敏感信息的保护难度，突破了传统的信息保护原则，对个人信息保护带来冲击，这亦是传统隐私法所无法规制的。

（五）服务于大数据侦查运行的数据共享大幅度扩张

在线开放理念的贯彻落实，实现了大数据资源的整合共享。公民的各类信息本是由多方主体所掌握，随着物联网、云计算等应用，各机构数据库通过互联网相互连接，共同为大数据侦查提供所需的原始业务数据信息。当下的数据共享不同于以往，以各省为单位建立的公安大数据平台，在空间上实现了跨区域、跨警种、跨部门的数据交换、共享和查询，还增添智能传感、射频识别等技术，实现共享数据的实时自动化更新，呈现即时同步性特征。如目前以 Hadoop（分析式处理平台系统）技术框架所搭建的公安大数据平台，结合分区虚拟技术实现异地数据查询及分析。[83]某市公安局建立了“防控一体化”大平台，实现“一键式查询”，通过系统网络便可快速获取特定个人的全面信息。[84]诚然，数据共享平台的搭建能够实现信息利用的最大化价值，打破了数据信息交流的壁垒，使零碎分散的数据集中化。但同时也让公民的各类信息无需经过任何程序即可归入警务数据系统，信息的易获性特征，不利于对个人信息的保护。

通常来说，网络信息业者都应当遵守个人信息保护的合目的性原则要求。[85]但现实往往会出现例外情形，如依据《网络安全法》第 28 条规定，使数据控制者将本是基于经营目的收集并处理的个人信息提供给刑事侦查使用等情形。相对于侦查机关而言，网络信息业者具有技术、资源和业务优势，实践中甚至有些数据只能通过网络信息业者才能获取，尤其在侦办涉及网络犯罪等类型的案件中网络信息业者凸显的作用将尤为明显，而随着我国国内司法协助义务的不断强化，加之数据共享平台的不断完善，致使侦查机关能够直接跳过司法协助的复杂程序即可获取个人信息。

另外，情报信息的检索分析原本属于侦查部门的内部制度运行，并不对外产生相应的法律效果。然而大数据侦查在运行过程中时常会利用情报分析来推动侦

---

82 参见《纽约时报：塔吉特读心术——用户数据分析的魔力》，资料来源：中文互联网数据咨讯网 http://www.199it.com/archives/32969.html，访问日期：2021 年 3 月 18 日。

83 参见王梦瑶：《大数据背景下侦查创新研究》，中国人民公安大学 2018 年博士学位论文，第 34 页。

84 参见王燃：《大数据侦查》，清华大学出版社 2017 年版，第 162 页。

85 参见裴炜：《向网络信息业者取证——跨境电子数据侦查新模式的源起、障碍与建构》，《河北法学》2021 年第 4 期，第 72 页。

查进程，虽然在共享平台上的信息查询看似仅为检索信息，但在本质上实为一种证据调取。[86]在数据实时共享的平台下，数据事先即已存储于公安部门的数据库中，侦查人员仅需数字验证下即可调取相关信息，无需任何程序规制。在以往的侦查活动中，对涉及公民隐私的数据信息一般需要侦查人员经过严格的审批程序后方能实地调取或查阅。而当下的便捷获取使原本的调取程序机制被架空，不能发挥应有的规制效果，长期下去，将会直接影响在刑事侦查中个人信息的合法有效利用。

（六）海量数据存留对个人信息造成风险

数据存留是指对一段时间内经过处理所得的或是通过其他路径所接收的数据进行的保存归档，可以说数据存留是数据采集的延伸，是不规范数据库的体现。上文有所提及，大数据侦查在运行过程中十分依赖于数据，数据库中的数据量与侦查需要成正比关系，这进一步催发出数据库的巨型特征，并呈现无上限的不断扩充趋势。然而当下侦查部门内部并未就数据存留问题进行规范管理。虽我国《刑事诉讼法》相关规定有明确侦查人员对涉密的信息应当主动保密和限制用途，并应及时销毁与案件无关的材料，但仍然存在规定不够细化、缺乏可操作性特征，如保管期限、如何管理等问题并未明确。对个人信息的存储同样可能引发对公民个人信息的侵犯。早在 1987 年的 Leander v.Sweden 案中，欧洲人权法院就明确单纯的信息存储行为本身即有可能构成对个人数据的不当干涉。[87]

缺乏规范管理的数据存留对个人信息造成的风险体现在侦查机关自身的数据库安全系数问题。据了解，公安机关采集到的公民个人信息经整理后会存储至档案库或数据库中统一管理，然而就数据库本身的安全建设问题仍需提高。一方面，有黑客入侵的风险。由于计算机操作系统在初始编程时更偏重于实用性，致使该系统整体上存在明显的安全漏洞，在此背景下，网络黑客能通过远程操控，利用解码攻击、代码植入等技术侵入网站或私人终端，以获取网站内部数据库信息等，造成信息泄露。[88]实践中发生过多起公安机关信息系统被黑客入侵事件。如 2014 年，据媒体报道，连云港市公安局车管系统遭黑客入侵后，非法删除 1. 4 万多条交通违章记录，非法获利 600 多万，使国家损失高达 1000 多万元。[89]

另一方面，有网络攻击的风险。2014 年以来，我国超过 55%的计算机感染恶

---

86 参见蒋勇：《大数据时代个人信息权在侦查程序中的导入》，《武汉大学学报（哲学社会科学版）》2019 年第 3 期，第 159 页。

87 参见裴炜：《互联网时代个人数据概念重构及保障性规范探索——以欧洲相关制度和判例为视角》，《法治现代化研究》2018 年第 2 期，第 26 页。

88 参见肖成俊、许玉镇：《大数据时代个人信息泄露及其多中心治理》，《内蒙古社会科学（汉文版）》2017 年第 2 期，第 188 页。

89 参见于英杰：《男子“黑”进车管系统 消 1.4 万条违章获利 600 万》，资料来源：南方网 http://it.southcn.com/9/2014-11/10/content_111881400.htm，访问日期：2021 年 3 月 18 日。

意软件，恶意软件打开计算机系统的入侵通道，一旦有非法入侵者便可直接访问系统内部的个人终端、私密文件、登入密码等数据，并可横向延伸感染范围，通过同一网络直接连接相关联的其他设备。[90]2018 年，据官方数据显示，我国政府、医疗、研究机构等部门中的核心信息系统已成为勒索病毒的重点攻击目标。该处提及的“勒索病毒”是一种针对计算机系统的新型病毒，其主要通过程序木马、网页、电子邮件等方式进行传播，一旦电脑感染，将会带来巨大损失。[91]

同时，还体现在侦查人员利用职务便利非法滥用数据信息方面。早在 2017 年，我国基础信息库已存储有效人口信息 13.99 亿，[92]当前公安机关的信息库中除了基本的户籍信息、网监信息和通讯信息等外，还包括与犯罪相关全国重大案件、在逃人员、盗抢汽车、未名尸体、失踪人口等信息库。大到人口户籍、国民基因等信息，小到公民个人身份、日常通讯等记录，如此宽泛的数据库存难免对公民个人信息的保护埋下隐患。侦查部门系统内部的信息平台能让警务人员依据相关证件即可快速查询任意公民的个人信息，如户籍、地址、车辆牌照、行踪轨迹等。虽公安部有下达禁止违规查询等相关规定，但实践中已多次出现私人信息的违规查阅、调取及非法获利等现象。如 2017 年至 2019 年，犯罪人潘某群利用妻子殷某在武汉市公安局经侦支队的民警身份，通过公安机关内部信息查询系统获取所需的车辆行动轨迹、出行记录等公民个人信息，开展相应业务，非法获利 31.57 万元不等。[93]

此外，在运用大数据侦查模式进行违法犯罪信息比对时，通常会查阅到犯罪嫌疑人以往的违法记录，部分办案人员存在将该类信息随意透露的情形，不仅使当事人承受极大的心理压力，同时影响其正常的社交。[94]实践中对于侦查部门中不准确的信息记录亦会造成对信息主体的不良影响，由此已有相当一部分学者主张在刑事诉讼领域中建立“被遗忘权”，认为目前存在数据“遗忘”的现实需求，不论是犯罪分子抑或是被错误追诉的无辜者，都有从刑事司法中“脱身”的需要，以免终身难以摆脱。[95]

---

[90] 参见《21 个触目惊心网络犯罪统计数据》，资料来源：搜狐网 https://m.sohu.com/a/270687289_100002744/，访问日期 2021 年 3 月 18 日。

[91] 参见王小群、韩志辉、徐剑、朱天等：《2018 年我国互联网网络安全态势综述》，《保密科学技术》2019 年第 5 期，第 6 页。

[92] 参见刘奕湛、程士华：《国家人口基础信息库已存储有效人口信息 13.99 亿》，资料来源：新华网 http://www.xinhuanet.com//2017-11/21/c_1121989048.htm，访问日期：2021 年 3 月 18 日。

[93] 参见赵思维：《民警用公安系统查婚外情等获刑》，资料来源：澎湃新闻 https://www.thepaper.cn/newsDetail_forward_9471151，访问日期：2021 年 3 月 18 日。

[94] 参见陈华：《大数据侦查侦查权与隐私权的冲突及其宪法调适》，《江苏警官学院学报》2019 年第 5 期，第 74-75 页。

[95] 参见郑曦：《作为刑事诉讼权利的个人信息权》，《政法论坛》2020 年第 5 期，第 134 页。

四、大数据侦查中个人信息保护的完善

信息社会无疑推动人类社会的迅速发展，致使相对滞后的治理方式及治理模式需要不断革新。大数据侦查促进传统侦查模式的转型升级，规范路径应既要遵循传统的规范框架，更要探索对个人信息保护的新兴路径。大数据侦查运行过程中对公民个人信息的利用是国家治理模式顺应时代的必然要求，然而上文有所提及，现有的立法难以保障刑事司法领域中的个人信息合理适用，权衡之下，最好的路径构建是需在侦查语境下，结合个人信息保护和侦查程序的基本规则，规范大数据侦查模式的运行过程，以期探索大数据侦查中对个人信息利用及保护之间的最佳平衡点。

（一）对不同信息类别进行分类保护

侦查部门现有的数据库虽有分领域建立，但并未将数据本身进行严格区分，欲在程序上对个人信息提供保护，则需区分不同类型的个人数据。

当前，个人信息的分类方式主要是根据特定的属性而进行的抽象类型划分。主要包括：其一，以可识别性的强弱为分类标准。该种分类是以信息能否在特定场合中直接识别到特定个人来判定。[96]直接个人信息是指具有单独可识别能力的信息，如身份证号码、电话号码、指纹、虹膜等；而间接个人信息则是需要结合其他信息才能识别自然人的信息，如性别、出生日期、婚姻状况、邮政编码等。然而，上文有所提及，在当下的信息时代，技术的升级应用已经可以将即便是不具有识别性的个人信息转化为可识别性信息。基于大数据侦查本身的技术特征，数据的二次挖掘应用会使得信息本身的识别性程度更加模糊化，在这种情况下，依据可识别性的强弱划分个人信息则缺少确定性，难以起到确切保护的效果。

其二，以敏感度的高低为分类标准。依据该种分类，可将个人信息分为敏感个人信息和一般个人信息，两者以信息的敏感度为划分标准。2013 年工业和信息化部颁布的《信息安全技术公共及商用服务信息系统个人信息保护指南》中即采用该种分类方式。然而，该类划分标准极具主观性色彩，判定信息的敏感度与一国特定的历史文化背景相关，致使认定为敏感信息的信息范围在不同的国家有所区别。如与我国国内就敏感信息的列举种类不同，在欧盟 2016 年颁布的相关法律中则列举了“哲学信仰、个人基因数据、生物特征数据、性取向”四类个人敏感信息。[97]尽管范围有所区别，但却可借鉴国外相关规定，结合本国的文化背景，根据信息的敏感程度指定特殊的细分领域，再以严格的审批程序予以规制。

---

[96] 参见何渊：《数据法学》，北京大学出版社 2020 年版，第 54 页。

[97] 参见韩旭至：《个人信息类型化研究》，《重庆邮电大学学报（社会科学版）》2017 年第 4 期，第 67 页。

其三，以信息主体为分类标准，可将个人信息分为一般人群和特殊人群的个人信息，特殊人群包括未成年人、公众人物、企业高层管理人员等。身份的区别直接造成两者属性的区别，主要凸显在个人信息的保护方式及程度上，某种特殊群体的个人信息具备不同的特征，从而适用特殊的法律规则。[98]如较之普通人的个人信息，就公众人物的个人信息保护程度会更加宽松，法律规定可在公众利益范围内对其个人信息予以处理。[99]再比如，针对未成年人的个人信息法律会予以专门的特殊保护。我国《刑事诉讼法》第 286 条、《最高人民法院关于人民法院在互联网公布裁判文书的规定》第 4 条及第 8 条等相关法律条文足以凸显这一特征。该种分类方式可为大数据侦查就特殊主体给予特殊保护提供一定的方法指引，但基于实践考量，将个人信息划分为一般信息与敏感信息更适合当下数据全面性特征。

将信息分为一般信息与敏感信息已成为域外法治国家的共识，我国亦已通过发布法律规定及司法解释确认了该种划分的合理性，但欲将一般信息与敏感信息进行准确划分，则必须解决敏感信息究竟应包括哪些类别的问题。对敏感信息的界定方式存在法律列举及综合考量两种模式，[100]基于目前的信息技术快速发展趋势，当下对敏感信息更适宜作列举规定，日后再结合司法实践的经验等对其进行填充。

在刑事诉讼中，敏感信息的范围界定应充分考虑目的的正当性，同时满足犯罪治理的现实需求。不论是域外抑或是国内，都已列明敏感信息的大致范畴。如欧盟颁布的《通用数据保护条例》第 9 条、我国发布的《信息安全技术 个人信息安全规范》第 3.2 条规定及由两高发布的《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》中所列举的个人敏感信息种类。[101]综合相关立法考量，结合司法实践中曾出现的涉及信息滥用的相关实例，个人敏感信息至少应当包括行踪轨迹信息、生物识别信息、医疗健康记录、性生活与性取向、犯罪前科等信息，这几类信息一旦滥用将会严重影响到公民的人格尊严等，同时在司法实务中极易成为公权力机关及个人利用职权非法获利的工具，将其明确为个人敏感信息范畴符合保障公民个人信息安全的初衷。

侦查机关较之其他信息处理者具有更为强大的信息收集和利用权能，其汇总的个人信息不仅数量繁杂，且种类多样，其中更是包含了大量个人隐私信息，这就要求在大数据侦查中对个人信息的保护应当避免“一刀切”形式，而需区分不

98 参见韩旭至：《个人信息类型化研究》，《重庆邮电大学学报（社会科学版）》2017 年第 4 期，第 68-69 页。

99 参见杨立新：《人格权法》，法律出版社 2015 年版，第 269 页。

100 参见胡文涛：《我国个人敏感信息界定之构想》，《中国法学》2018 年第 5 期，第 245 页。

101 参见程雷：《刑事司法中的公民个人信息保护》，《中国人民大学学报》2019 年第 1 期，第 112 页。

同类别的个人信息，并相应的予以不同程度的保护。如将数据库中的个人敏感信息另行存储，并通过数据脱敏技术、加密技术等来保障个人敏感信息，同时设置访问权限，明确只有案件侦办人员才能进入查询或利用。基于当前大数据侦查对个人信息的利用横向涉及犯罪预警、犯罪初查、犯罪侦查等全过程，纵向包含信息采集、存储、共享、挖掘分析等多领域，为充分切实保障公民信息，未来立法应对大数据侦查的运行阶段明确划分，结合不同类别的个人信息，层级化设置侦查机关的权利义务。

（二）明确不同侦查阶段的数据适用规则

大数据侦查是一个动态发展的开放性体系，其较之传统侦查更加广阔，既包括发挥防控目的的犯罪预警，也包含对已然犯罪的案件侦查，内涵的复杂性导致难以将其划入特定的类型侦查措施。[102]基于程序法定主义，加之大数据侦查本身兼具任意性与强制性等多重属性成分，可以通过定性控制对其划分阶段，并根据不同侦查阶段相应设置不同程度数据适用规则，将其纳入法治轨道，以达到在打击犯罪过程中实现人权保障的目的。

大数据侦查的法律属性问题，学界仍存在较大争议，有学者认为应将大数据侦查纳入到现有强制性侦查措施的规则体制中；[103]有学者则表示并不认同将大数据侦查认为是一种强制性侦查措施，并从大数据侦查与技术侦查的范围、特征及程序要求等方面进行分析论证大数据侦查亦非属于技术侦查行为；[104]亦有学者主张大数据的法律属性既不是搜查，也不是调取，更不能被视为技术侦查。[105]种属划分将直接导致大数据侦查行为法律依据、适用原则、适用程序及监督审查等诸多差异，有研究的必要性。

一般而言，侦查措施分为任意性侦查措施和强制性侦查措施，关于两者的界定，国内外学界主要存有两种立场，分别是“侦查相对人是否同意说”“是否侵犯公民的基本权利说”。前者是根据受侦查人同意或允诺与否为前提而进行的侦查行为分类，后者则认为区分两者的关键在于合理判断侦查措施对公民基本权利的侵犯程度。[106]在侦查运行过程中并不干预公民的基本权利的是任意性侦查措施，

---

102 参见陈刚：《解释与规制：程序法定主义下的大数据侦查》，《法学杂志》2020 年第 12 期，第 9 页。

103 参见胡铭、龚中航：《大数据侦查的基本定位与法律规制》，《浙江社会科学》2019 年第 12 期，第 14-15 页。

104 参见于阳、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》，《情报杂志》2018 年第 12 期，第 148 页。

105 参见程雷：《大数据侦查的法律控制》，《中国社会科学》2018 年第 11 期，第 167 页。

106 参见张可：《大数据侦查之程序控制：从行政逻辑迈向司法逻辑》，《中国刑事法杂志》2019 年第 2 期，第 140 页。

反之，会妨碍甚至限制、剥夺公民基本权利的则是强制性侦查措施。[107]我国《刑事诉讼法》中并未明确区分或释明强制性侦查措施及任意性侦查措施，但有通过列举的方式阐述，如在《刑事诉讼法》第二编中规定了搜查、扣押、冻结、技术侦查等强制性侦查措施。

从立法层面来看，我国《刑事诉讼法》中的侦查措施基本上都带有强制色彩，[108]不以受侦查人的同意或允诺为前提。从司法实务层面上说，如果以被侦查人是否同意为标准来划分侦查措施的任意性或强制性，那是不是就意味着即便侦查机关对被侦查人进行会侵犯其极具隐私的侦查行为，在被侦查人同意的情况下就可将该侦查行为归为任意性侦查措施呢？如此说来，明显不符合实际。因此，对于两者区分界定应以“是否侵犯公民的基本权利”为标准较为适宜。

强制性侦查措施可进一步进行划分，根据涉及公民基本权利的种类，可细分为关涉隐私权的、关涉财产权的及关涉人身权的侦查措施。[109]基于该分类，学界普遍观点主张由于大数据侦查在运行阶段会关涉到公民的隐私权，应被纳入强制性侦查措施予以规制。然而在现实情况下，侦查阶段还存在许多利用大数据技术进行的初步分析等辅助行为，这类行为不会对公民基本权利进行干预，甚至完全无关于公民隐私权，如对初始采集的公民非敏感信息以及根据采集到的数据进行建模等行为，显然不属于强制性侦查措施范畴。可见，基于大数据技术内涵的开放性和不确定性特征，致使以此为应用核心的大数据侦查难以明确地归入特定种类的侦查措施。[110]根据这一属性特征，较为适宜的做法是对大数据侦查进行分段控制，并根据不同阶段体现的属性特征，设置不同程度的数据适用规则。

结合当下大数据侦查的实际运行，可将其划分为：犯罪预警阶段、犯罪初查阶段及犯罪侦查阶段。犯罪预警阶段，旨在对犯罪行为的基础性预测，通过概括性数据分析得出类似“犯罪地图”等信息，指引侦查。目前司法实务中，主要开展的是对某一地区犯罪活动的预测、对某个人犯罪概率的预测及对某类犯罪线索的识别预警[111]。对犯罪活动的预测系基于犯罪活动与地理位置之间的密切联系，通过总结以往案发地所呈现的历史规律，来预测未来犯罪活动。对某个人犯罪概率的预测实际就是针对高危犯罪人员的预测，其原理与高危地区的犯罪预测本质上是相同的，即是通过对以往高危分子身上凸显的特征数据进行归纳分析，构建一定的算法模型。对某类犯罪线索的识别预警指的即是上文所列举的针对非法集资

---

107 参见张可：《大数据侦查措施程控体系建构：前提、核心与保障》，《东方法学》2019 年第 6 期，第 89 页。

108 参见孙长永：《强制侦查的法律控制与司法审查》，《现代法学》2005 年第 5 期，第 73 页。

109 参见张可：《大数据侦查措施程控体系建构：前提、核心与保障》，《东方法学》2019 年第 6 期，第 89 页。

110 参见陈刚：《解释与规制：程序法定主义下的大数据侦查》，《法学杂志》2020 年第 12 期，第 9 页。

111 参见王燃：《大数据侦查》，清华大学出版社 2017 年版，第 93-94 页。

案件所构建的预警监测模型，通过对大数据异常数据挖掘功能实现预警。

可见，无论基于何种模式，在犯罪预警阶段对数据的应用主要体现在对以往数据的概括性分析，从而构建数据模型，以提高犯罪防控效率。由于该阶段针对的是不特定案件及不特定行为人，呈现预测对象泛化、不确定性等特征，未造成对特定个人信息的干预，[112]更加符合任意性侦查措施范畴，继而在该阶段，适用数据应用的一般规则即可，无需进行严格规制。如若需要针对特定个人信息进行挖掘予以犯罪预测，则需适用特殊程序予以规制。

而犯罪初查阶段与犯罪侦查阶段之间的区分节点是非常模糊的。但根据 2015 年由两高一部颁布的《关于办理网络犯罪案件适用刑事诉讼程序若干问题的意见》中所规定的初查启动要件表明，犯罪初查阶段至少应已具备具体、特定的犯罪事实或线索为开始，到侦查正式立案为界点。[113]根据《人民检察院刑事诉讼规则（试行）》第 173 条规定，初查阶段本应属于任意性侦查范畴，但该项规定显然已难以规制当下的大数据侦查运行模式，则应当对初查的相关规定进行完善。在适用条件上，应当明确在初查阶段启动大数据侦查的事实门槛条件，以防止侦查机关任意启动大数据侦查而导致的常态化的全民大规模监控。同时，原则上不得采取数据挖掘等深度分析类侦查技术，只能进行查询、比对等初级分析应用，但基于当下侦办新型犯罪案件的需要，可以经程序审批后适用为例外。

立案后的犯罪侦查阶段，主要体现在对特定侦查相对人的数据进行收集分析等适用。对于侦破案件、收集证据、查找特定犯罪嫌疑人等用途的大数据侦查本质上符合强制性侦查措施范畴。有学者主张将技术侦查措施的宏观规范直接适用于大数据侦查领域。[114]然而就现有规定而言，直接适用将会严重限制其应有效能。我国《刑事诉讼法》第 150 条明确规定了技术侦查的适用对象范围，《公安机关办理刑事案件程序规定》中亦明确规定该侦查的适用主体及适用方式。然而，大数据侦查措施在实践运行中包含发挥风险防控作用的预警系统、打击犯罪为主的技战法运用及实现动态管理的职能管理系统等运行样态，[115]不仅注重破案的“质”，更加强调破案的“量”，若将技术侦查措施严格的运用范围、适用主体及程序规定等相关法律完全适用于大数据侦查领域，明显限缩了大数据侦查的应用领域，限制其应有效能。

处于犯罪侦查阶段的数据利用包括数据准备（采集、清洗、转换、集成）、

---

112 参见裴炜：《数据侦查的程序法规制——基于侦查行为相关性的考察》，《法律科学（西北政法大学学报）》2019 年第 6 期，第 51 页。

113 参见裴炜：《个人信息大数据与刑事正当程序的冲突及其调和》，《法学研究》2018 年第 2 期，第 56 页。

114 参见胡铭、龚中航：《大数据侦查的基本定位与法律规制》，《浙江社会科学》2019 年第 12 期，第 17 页。

115 参见张可：《大数据侦查之程序控制：从行政逻辑迈向司法逻辑》，《中国刑事法杂志》2019 年第 2 期，第 133-135 页。

数据挖掘等方式，先通过数据准备明晰侦破案件思路，而后通过数据挖掘明确犯罪目标。[116]在数据准备阶段，最需规制的是数据采集行为。数据采集应遵循比例原则，采集信息前应衡量所采集的信息对于案件侦查是否必需，能否通过其他途径达到侦查目的，采集目的应明确说明，并通过程序授权等方式规制，采集的信息类别不得超出完成侦查目的所必要的范围，若采集的信息中含有个人敏感信息或需扩张数据采集范围，则需经过侦查机关负责人审查批准后方可进行。而处于该阶段的数据挖掘技术，基于其技术性特征，则应针对性的构建特殊程序，予以更为严格的程序规制。

（三）构建针对数据挖掘的特殊程序

上文有所提及，通过数据挖掘等技术，任何碎片化信息都有可能经过清洗、重组而转化为个人敏感信息，由此，单从细化该技术适用的信息类型并不能产生有效规制的效果。基于其对公民个人信息干预程度的进一步增强，可借鉴域外相关立法，构建针对数据挖掘的特殊程序。

针对刑事司法中运用大数据技术可能会侵犯公民基本权利的问题，大陆法系往往通过增设详细的规定予以规制，主要区别体现在各国所针对的权利类型不同。如欧盟以保障公民隐私权为主旨，主要依据《欧洲人权公约》《欧盟通用数据保护条例》等相关法律来规制大数据侦查。而德国则以保护公民的信息自决权为出发点，相应地增设详细的实施规则，如为规范计算机排查侦缉等特殊侦查措施运行，德国《刑事诉讼法》第 98 条进行了严格的规定，具体包括：一是明确适用案件类型；二是明确启动条件；三是需经过司法令状批准后方能实施；四是关于数据的后续处理设定了相应程序。[117]从计算机排查侦缉的实质内容上看，该种侦查措施采用的技术就是数据挖掘技术。[118]对此，为规范我国大数据侦查下数据挖掘技术的适用，可形式上制定特殊程序，在实质上细化数据挖掘技术适用的案件类型与范围，以确保在数据挖掘过程中个人信息的充分保障。

其一，在适用范围方面。鉴于数据挖掘等技术应用难以预判数据的最终分析结果，亦考虑到数据挖掘结果对信息主体的权力干预性强，该项技术应仅限于侦查严重犯罪时方能使用，其范围可参考我国《刑事诉讼法》第 150 条中关于技术侦查措施对重罪范围的相关规定。

其二，在适用对象方面。参考域外国家的相关立法，在大数据技术适用对象

---

116 参见何军：《大数据与侦查模式变革研究》，《中国人民公安大学学报（社会科学版）》2015 年第 1 期，第 78-79 页。

117 参见胡铭、龚中航：《大数据侦查的基本定位与法律规制》，《浙江社会科学》2019 年第 12 期，第 15-16 页。

118 参见宗玉琨译注：《德国刑事诉讼法典》，知识产权出版社 2013 年版，第 53-55 页。

问题上采取了相关性原则，体现在该侦查技术的被适用对象必须是有证据证明或被合理怀疑的与案件相关的犯罪嫌疑人、被告人。考虑到现有的巨型数据库中包含大量公民个人信息，应明确数据挖掘技术仅能适用于犯罪嫌疑人、被告人等与犯罪活动直接相关的人，并不得随意扩大范围。

其三，在适用主体方面，只限于案件侦办人员，同时配备专项权限技术设施。值得一提的是，尽管现在司法实务中，已为警务人员配备专门的数字证书和警务 U 盘用来登入公安信息网和传输文件，但该种方式是需通过计算机来使用，系统中留存的使用记录难以保证是否是数字证书持有者操作。另外，实践中利用职权非法泄露等现实案例足以证明该种方式的管理不当，难以形成有效的反向规制。就此，可通过增设虹膜或指纹识别等多种安全方式，确保数字证书持有者本人进入使用。一方面，提高信息的安全性；另一方面，便于事后的责任倒查。

其四，严格规范数据挖掘技术的审批程序。大数据侦查本质上亦是一种侦查措施，其审批程序的制度设计可与我国《刑事诉讼法》中已有的相关规定相协调，如需报请侦查机关负责人审批。基于数据挖掘的技术性特征，适用则需以获得更加严格的审批授权为前提。作为刑事侦查措施，应当遵守必要性原则。然而，我国现有的法律针对程序启动的要件并未作出具体的规定，只提及了“根据侦查犯罪的需要”，这样模糊的规定不足以认定该技术适用的必要性。必要性原则要求数据挖掘技术不是必要的时候不得采用，即只有在穷尽其他侦查措施的情况下，方能适用，并应与所侦查犯罪的严重程度成比例。为此，立法应明确侦查部门提交审批时的客观证据要求，即侦查部门在申请启动数据挖掘技术时应证明该适用符合必要性原则，且不采用数据挖掘技术的结果危险性。审批主体需依据侦查机关提供的相关证明要件，来判断是否适用数据挖掘技术的必要性后再决定批准与否，以防止数据挖掘技术的滥用。

其五，完善事后监督与救济程序。鉴于数据挖掘技术特征，事前监督并不具有可行性。上文有所提及，数据运算过程的不可视化难以事先明确数据挖掘后的信息内容，而通过事后监督则有利于反向规制技术合理适用。具体包括建立定期备案及报告机制、事后通知制度。定期备案及报告机制是指侦查部门就侦办案件过程中对大数据侦查措施的整体适用情况定期加以备案并报告。对此，可在侦查机关内部专设信息利用监督部门，并实行层级管理，即需定期向上一级侦查机关信息利用监督部门提交情况报告。事后通知制度是针对所利用的信息主体而言的，知情同意原则在刑事程序中的难以适用并非意味着对信息主体的完全不告知，可以在不妨碍侦查行为顺利进行的前提下，分阶段、分程度的予以告知。以秘密侦查措施为例，考虑到案件本身的侦查难度等现实情况，为确保案件侦办的顺利进

行，侦查机关可根据案件侦办情况对侦查相对人的知情权进行暂时性限制。[119]同时赋予信息主体申诉控告权，明确当侦查人员对其信息进行非法利用时，可向检察机关提出申诉控告，反向规范数据挖掘利用。

（四）完善大数据侦查运行的审批监督机制

实践中常出现个人信息滥用等问题，最大的原因之一便是监督机制的缺失。从域外的相关经验来看，较为完善的监督程序往往结合书面审查、现场监督等多种方式，并贯穿于侦查的全过程。[120]但监督程序的整体构建不应仅以监督功能的实现为考量标准，同时还需要衡量侦查效能等价值目标。[121]目前学界大多主张通过建立外部监督机制以期打破大数据侦查中“制度上封闭性”，却忽视了大数据侦查本身“技术上的封闭性”。

在刑事诉讼中，针对技术侦查措施实行的是公安机关内部审批监督机制，这是出于实践的考量。一方面，检察机关虽是法定监督机关，但对于技术侦查措施的整体运行情况缺乏详尽的了解，以致难以对该适用进行直接有效监督；另一方面，审判机关虽可通过证据审核或者依据非法证据排除规则等方式对技术侦查措施予以间接监督，但大部分由技术侦查措施获得的案件材料都不会作为证据使用，使得间接监督方式落空。[122]可见外部监督模式难以成效。出于当下大数据侦查的技术性考量，可参照对技术侦查措施的监督方式，兼顾大数据侦查措施适用的灵活性，构建以侦查负责人审批为主，技术人员参与为辅的内部监督机制。即主要采取书面审批方式，根据所涉的信息敏感程度实行分级审批。同时，在侦查机关内部体系增设专门的技术监督部门，指派具有个人信息相关工作经验并熟练应用计算机系统的专业技术人员担任侦查部门内部的个人信息保护专员，负责所处部门的个人信息监管工作及对外对接工作。一方面，对相应的技术应用领域进行专业有效监督；另一方面，强化信息技术支持，以切实保障公民个人信息。

（五）规范大数据侦查的数据共享平台

根据《民法典》第 1035 条规定，收集、处理自然人个人信息的，应当遵循合法、正当、必要原则。在大数据侦查中的数据共享仍应贯彻该三大原则，同时还应遵循最小化使用原则，最小化使用原则是指应在满足于使用目的的范围内获取个人信息，不得随意扩大信息的收集或使用范围。[123]虽依据我国相关法律，第三方平台负有司法协助的责任与义务，但应当明确即便在数据共享的背景下，信息的

---

119 参见陈刚：《解释与规制：程序法定主义下的大数据侦查》，《法学杂志》2020 年第 12 期，第 7 页。
120 参见刘计划：《侦查监督制度的中国模式及其改革》，《中国法学》2014 年第 1 期，第 259-262 页。
121 参见陈刚：《解释与规制：程序法定主义下的大数据侦查》，《法学杂志》2020 年第 12 期，第 7 页。
122 参见程雷：《刑事司法中的公民个人信息保护》，《中国人民大学学报》2019 年第 1 期，第 109 页。
123 参见王利明：《数据共享与个人信息保护》，《现代法学》2019 年第 1 期，第 54 页。

使用及管理仍属于第三方机构，侦查部门仅能基于案件侦办依法要求数据控制第三方提供特定范围内的数据，而非使用、控制抑或是占有第三方全部的数据资源。

保护个人信息的逻辑起点在于是否正当收集及合理使用。为规范大数据侦查的数据共享，应健全执法合作的调取机制，可联合各行业顶层部门统一建构数据调取程序，明确侦查部门与第三方数据平台之间调取的标准、方式及范围等事项。主要包括：其一，完善第三方平台的内部数据管理。考虑到数据本身的复杂多样性，第三方平台应根据国家相关立法建立数据分类框架，抑或结合侦查机关以往调取的数据记录，将其所掌握的内部数据系统进行类型划分，以便于层级化的调取措施。其二，明确对接渠道，统一执法机关申请调取方式。推行线上调取方式，如设立统一在线申请门户网站、官方电子邮件等方式提出申请。通过统一在线申请，不仅优化调取渠道、提高效率，同时因经过线上严格的身份认证方能使用以确保调取过程的安全性。其三，根据调取信息的敏感程度等级划分，明确可任意或需严格审查才能调取的信息范围。如需调取敏感信息，则应比照我国《公安机关办理刑事案件程序规定》第 57－59 条以及《公安机关执法细则(第三版)》9-02 细化了的调取程序性规定。其四，预留紧急调取数据空间。主要应对的是侦查机关若无法及时调取相关数据，则导致犯罪后果扩大等场景，为防止紧急调取数据空间的滥用，未来立法需明确适用条件。如出现可能危及国家安全、社会公共安全等严重犯罪，因情况紧急应允许侦查人员对相关数据先行调取。[124]

（六）健全数据存留管理机制

在大数据侦查运行导致海量数据存留的背景下，基于对个人信息保护之目的，侦查部门应完善对获取信息后的履行保管、销毁等义务。近年来，已有国家开始针对数据留存进行单独立法，如在 2014 年英国通过的《数据留存和调查权法案》，[125]也有国家将数据留存纳入国家安全法等法域中予以规定，如 2015 年德国颁布的《数据留存法案》。[126]我国虽未有数据留存的单独立法，但在部分规定中有提及数据的留存期限。如《网络安全法》第 21 条规定，网络信息业者需要留存用户网络日志，时间期限使不少于六个月。不难发现，现有规范呈现分散化、初步性特征。数据留存实际上延伸了侦查机关的手足，应增设数据保存限制原则。

数据保存限制原则是由公平信息实践原则发展演变而来，强调数据控制者对数据保留的最低时限不得超出完成特定司法目的所需时间。该原则在欧盟 1995 年

124 参见裴炜：《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》，《法律科学（西北政法大学学报）》2021 年第 3 期，第 94 页。

125 参见周杰：《比例原则下电子通信数据留存之限度——<欧盟 2006/24 号指令>无效案》，《苏州大学学报（法学版）》2018 年第 3 期，第 150-160 页。

126 参见师索、陈玮煌：《犯罪侦查中网络通讯数据留存制度的欧洲法审视》，《西南政法大学学报》2018 年第 6 期，第 16-30 页。

《数据保护指令》中正式确立，随着数据保护意识的增强，逐渐成为各国数据保护的普遍性原则。[127]但各国立法对存留期限有不同模式：一种是设立统一存储时间，进一步细化包括设立固定存留期限、设立最高或最低存留期限、设立区间存储时间。如 2015 年澳大利亚颁布的《TIA 修正案》中规定了固定存留期限为 2 年；英国在 2014 年《数据保留与侦查权法案》规定交流数据的存留时间最多 12 个月。[128]另一种是根据数据类型设立区别存留时间。如在德国，数据存留的时限以人的年龄为考量因素，成年人 10 年、青少年 5 年、儿童 2 年。也有国家将警察对个人资料的储存时限一般设定为 1 年，若该资料仍是执行警察任职期间所需，则可延长至 5 年。[129]结合我国目前现状，对数据的存留更适宜用第二种模式，需综合考量不同类型数据，区别设置不同的存储时间。至于数据具体存留期限，应在充分实证调研的基础上，权衡不同数据的敏感程度、实际效用和留存成本等因素，合理设置留存数据期限。

127 参见栾兴良：《数据保护原则视阈下大数据侦查的立法规制》，《湖北警官学院学报》2020 年第 5 期，第 13 页。

128 参见裴炜：《犯罪侦查中网络服务提供商的信息披露义务——以比例原则为指导》，《比较法研究》2016 年第 4 期，第 99 页。

129 参见栾兴良：《数据保护原则视阈下大数据侦查的立法规制》，《湖北警官学院学报》2020 年第 5 期，第 13 页。

结 语

近年来，国家愈发重视个人信息方面的保护构建，在民法、刑法及行政法领域中就相关立法及研究都取得了相应进展，唯独刑事司法领域仍处于空缺状态，留下了的灰色空间不利于规制当下大数据侦查模式的程序运行。大数据侦查是当下时代应对隐蔽、新型化犯罪的必然选择，是侦查措施与时俱进的必要体现。为填补刑事诉讼中个人信息保护的法律空缺，有效规范大数据侦查的有序运行，最好的路径构建需在侦查语境下，结合个人信息保护和侦查程序的基本规则，以探索大数据侦查中对个人信息利用及保护之间的最佳平衡点。针对目前存在的现有立法难以保障刑事程序中的个人信息、易对个人信息造成“隐秘性”侵犯、对个人信息的过分采集、数据挖掘等技术应用加大对个人信息的保护难度、服务于大数据侦查运行的数据共享大幅度扩张及海量数据存留对个人信息造成风险等问题，可行对策包括应对不同信息类别进行分类保护、明确不同侦查阶段的数据适用规则、构建针对数据挖掘技术的特殊程序、完善大数据侦查运行的审判监督机制、规范数据共享平台及健全数据存留的管理模式，以期在有效保护个人信息的前提下，最大程序地发挥大数据侦查的应有效能。

参考文献

著作类：

1、孔令杰：《个人资料隐私的法律保护》，武汉大学出版社 2009 年版。

2、吴苌弘：《个人信息的刑法保护研究》，上海社会科学院出版社 2014 年版。

3、王燃：《大数据侦查》，清华大学出版社 2017 年版。

4、李建立、李宇尘：《大数据在刑事侦查中的应用研究》，吉林大学出版社 2017 年版。

5、李双其等：《大数据侦查实践》，知识产权出版社 2019 年版。

6、张兆瑞：《智慧公安——大数据时代的警务模式》，中国人民公安大学出版社 2015 年版。

7、张民安：《信息性隐私权研究》，中山大学出版社 2014 年版。

8、何渊：《数据法学》，北京大学出版社 2020 年版。

9、郭瑜：《个人数据保护法研究》，北京大学出版社 2012 年版。

10、李媛：《大数据时代个人信息保护研究》，华中科技大学出版社 2019 年版。

11、杨立新：《人格权法》，法律出版社 2015 年版。

12、宗玉琨：《德国刑事诉讼法典》，知识产权出版社 2013 年版。

13、陈瑞华:《刑事证据法学》，北京大学出版社 2012 年版。

14、［英］维克托维克托·迈尔·舍恩伯格、［英］肯尼思·库克耶：《大数据时代》，盛杨燕、周涛译，浙江人民出版社 2013 年版。

15、[奥]曼弗雷德.诺瓦克:《民权公约评注：联合国〈公民权利和政治权利国际公约〉》，毕小青、孙世彦译，生活·读书·新知三联书店 2003 年版。

16、[英]约翰·密尔：《论自由》，程崇华译，商务印书馆 1959 年版。

17、[日]松尾浩也：《日本刑事诉讼法》，丁相顺译，中国人民大学出版社 2005 年版。

18、[日]田口守一：《刑事诉讼法》（第 5 版），张凌、于秀峰译，中国政法大学出版社 2010 年版。

19、皮勇：《刑事诉讼中的电子证据规则研究》，中国人民公安大学出版社 2005 年版。

20、龙宗智：《司法改革与中国刑事证据制度的完善》，中国民主法制出版社 2016 年版。

期刊类：

1、李薇：《大数据背景下侵财犯罪的发展演变与侦查策略探析——以北京市为样本》，《中国人民公安大学学报（社会科学版）》2014 年第 4 期。

2、何军：《大数据与侦查模式的变革研究》，《中国人民公安大学学报（社会科学版）》2015 年第 1 期。

3、陈刚：《解释与规制：程序法定主义下的大数据侦查》，《法学杂志》2020 年第 12 期。

4、王利明：《数据共享与个人信息保护》，《现代法学》2019 年第 1 期。

5、刘计划：《侦查监督制度的中国模式及其改革》，《中国法学》2014 年第 1 期。

6、陈刚：《解释与规制：程序法定主义下的大数据侦查》，《法学杂志》2020 年第 12 期。

7、师索、陈玮煌：《犯罪侦查中网络通讯数据留存制度的欧洲法审视》，《西南政法大学学报》2018 年第 6 期。

8、裴炜：《犯罪侦查中网络服务提供商的信息披露义务——以比例原则为指导》，《比较法研究》2016 年第 4 期。

9、王仲羊：《刑事诉讼中的个人信息保护——以科技定位侦查为视角》，《社会与法治》2020 年第 12 期。

10、史卫民：《大数据时代个人信息保护的现实困境与路径选择》，《情报杂志》2013 年第 12 期。

11、殷建立、王忠：《大数据环境下个人数据溯源管理体系研究》，《情报科学》2016 年第 2 期。

12、程雷：《刑事司法中的公民个人信息保护》，《中国人民大学学报》2019 年第 1 期。

13、周杰：《比例原则下电子通信数据留存之限度——<欧盟 2006/24 号指令>无效案》，《苏州大学学报（法学版）》2018 年第 3 期。

14、胡文涛：《我国个人敏感信息界定之构想》，《中国法学》2018 年第 5 期。

15、张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，《中国法学》2015 年第 3 期。

16、陈刚：《解释与规制：程序法定主义下的大数据侦查》，《法学杂志》2020 年第 12 期。

17、胡铭、龚中航：《大数据侦查的基本定位与法律规制》，《浙江社会科学》2019 年第 12 期。

18、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》，《情报杂志》2018 年第 12 期。

19、栾兴良：《数据保护原则视阈下大数据侦查的立法规制》，《湖北警官学院学报》2020 年第 5 期。

20、张可：《大数据侦查之程序控制：从行政逻辑迈向司法逻辑》，《中国刑事法杂志》2019 年第 2 期。

21、张可：《大数据侦查措施程控体系建构：前提、核心与保障》，《东方法学》2019 年第 6 期。

22、裴炜：《数据侦查的程序法规制——基于侦查行为相关性的考察》，《法律科学（西北政法大学学报）》2019 年第 6 期。

23、裴炜：《个人信息大数据与刑事正当程序的冲突及其调和》，《法学研究》2018 年第 2 期。

24、孙长永：《强制侦查的法律控制与司法审查》，《现代法学》2005 年第 5 期。

25、李鹏：《大数据在非接触性犯罪侦查中的应用研究》，《山西警察学院学报》2018 年第 4 期。

26、顾理平：《大数据时代隐私信息安全的四重困境》，《社会科学辑刊》2019 年第 1 期。

27、蒋勇：《大数据时代个人信息权在侦查程序中的导入》，《武汉大学学报（哲学社会科学版）》2019 年第 3 期。

28、刘烁：《全面深化公安机关 DNA 数据库建设发展应用，切实提升精确打击犯罪能力和服务实战水平》，《刑事技术》2016 年第 1 期。

29、裴炜：《个人信息保护法与刑事司法的分离与融合》，《中国政法大学学报》2020 年第 5 期。

30、王仲羊：《刑事诉讼中的个人信息保护——以科技定位侦查为视角》，《理论月刊》2020 年第 12 期。

31、杨婷：《论大数据时代我国刑事侦查模式的转型》，《法商研究》2018 年第 2 期。

32、彭知辉：《“大数据侦查”质疑：关于大数据与侦查关系的思考》，《中国人民公安大学学报（社会科学版）》2018 年第 4 期。

33、樊崇义、张自超：《大数据时代下职务犯罪侦查模式的变革探究》，《河南社会科学》2016 年第 12 期。

34、梁坤：《论初查中收集电子数据的法律规制——兼与龙宗智、谢登科商榷》，《中国刑事法杂志》2020 年第 1 期。

35、倪春乐：《大数据侦查的样态和机理》，《中国人民公安大学学报（社会科学版）》2019 年第 5 期。

36、王燃：《大数据时代侦查模式的变革及其法律问题研究》，《法制与社会发展》2018 年第 5 期。

37、孙骁：《大数据侦查与个人信息保护的冲突与平衡》，《江西警察学院学报》2019 年第 5 期。

38、郑曦：《作为刑事诉讼权利的个人信息权》，《政法论坛》2020 年第 5 期。

39、齐爱民：《论个人信息的法律属性与构成要素》，《情报理论与探索》2009 年第 10 期。

40、高富平：《个人信息保护：个人控制到社会控制》，《法学研究》2018 年第 3 期。

41、陈华：《大数据侦查侦查权与隐私权的冲突及其宪法调适》，《江苏警官学院学报》2019 年第 5 期。

42、谢登科：《论技术侦查中的隐私权保障》，《法学论坛》2016 年第 3 期。

43、袁泉：《个人信息分类保护制度的理论基础》，《上海政法学院学报》2018 年第 3 期。

44、庄乾龙：《刑事案件中大数据整合行为定性及其适用规则》，《法学研究》2020 年第 12 期。

45、裴炜：《互联网时代个人数据概念重构及保障性规范探索——以欧洲相关制度和判例为视角》，《法治现代化研究》2018 年第 2 期。

46、肖成俊、许玉镇：《大数据时代个人信息泄露及其多中心治理》，《内蒙古社会科学（汉文版）》2017 年第 2 期。

47、王小群、韩志辉、徐剑、朱天等：《2018 年我国互联网网络安全态势综述》，《保密科学技术》2019 年第 5 期。

48、韩旭至：《个人信息类型化研究》，《重庆邮电大学学报（社会科学版）》2017 年第 4 期。

49、裴炜：《向网络信息业者取证——跨境电子数据侦查新模式的源起、障碍与建构》，《河北法学》2021 年第 4 期。

50、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》，《法律科学（西北政法大学学报）》2021 年第 3 期。

学位论文类：

1、李媛：《大数据时代个人信息保护研究》，西南政法大学 2016 年博士学位论文。

2、王梦瑶：《大数据背景下侦查创新研究》，中国人民公安大学 2018 年博士学位论文。

3、楼叶：《大数据背景下警务数据挖掘的法制化》，中国人民公安大学 2019 年硕士学位论文。

外文类：

1、Samuel D.Warren and Louis D. Brandies, *The Right to Privacy,* Harvard Law Review, 1980.

2、Ruth N.Cohen, *Whose File is it Anyway,National Center for Civil Liberties*, Civil Liberties Trust, London, 1982.

3、Priscilla Regan, *Legislative Privacy: Technology, Social Values, and Public Policy,* University of North Carolina Press, 1995.

4、Orin S·Kerr, *Searches and Seizures in a Digital World,* Harvard Law Review, 2005.

致 谢

三年硕士时光转瞬即逝，满腹言语在提笔之时却又不知该从何谈起。导师的谆谆教诲、亲人的支持陪伴、同学的鼓励安慰，一切的一切难以用三言两语来承载心中的感激之情。

求学三年期间，最庆幸的是遇到恩师。学术钻研之路比我想象中艰难，之所以能坚持不懈地走下来，是因为有老师的耐心教导、悉心栽培。感谢老师一次次不厌其烦的解惑和指引，让我在研究生生涯中不断提升了自身的专业能力，也感谢老师一直以来的鼓舞和肯定，让我在学习过程中愈发的自信。愿老师身体健康，诸事顺利。

感谢家人的陪伴支持，是家人铸就的坚实后盾才让我得以勇往直前的追求自己所想所愿，也很惭愧，即将毕业的我还有些许迷茫，未明确未来就业方向。愿将来能不负所望，报答父母的养育之恩，愿父母永远幸福安康，顺遂无忧。

感谢好友的鼓励安慰。研究生阶段有幸能遇到一群志同道合的同窗好友，大家一起打打闹闹，嬉嬉笑笑，缓解了不少在校期间的学业压力，愿未来大家能心想事成，顺顺利利。

毕业之际，感触颇多。学生生涯即将画下完美句号，将来会一如既往地坚持奋斗，砥砺前行。愿未来可期，做光明磊落、坚毅勇敢的法律人。