**Dispute Settlement** 争议解决, 2023, 9(3), 787-794
Published Online May 2023 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2023.93105

Hans汉斯

# 大数据侦查的法律规制

## ——个人信息保护的冲突到融入

**陈　舒**

华东政法大学，刑事法学院，上海

收稿日期：2023年3月22日；录用日期：2023年5月5日；发布日期：2023年5月12日

## 摘　要

**目前大数据侦查的实践样态包括以犯罪侦破为目标的精准运用以及以犯罪预防为目标的预警系统。大数据侦查相较于传统侦查措施在大数据时代对于犯罪侦破和犯罪预防具有天然优势。然而，大数据侦查引发的全景式监控风险、数据共享风险以及刑事侦查与行政执法的混同风险，使得个人信息保护的引入变得紧迫起来。要对大数据侦查的法律规制和个人信息保护的关系树立理性认知，以比例原则为规范工具，将大数据侦查纳入刑事诉讼立法中，实现平衡各方主体利益的合理制度安排。**

## 关键词

**大数据侦查，个人信息，犯罪预防，风险，比例原则**

# Legal Regulation of Big Data Investigation

## —Conflict and Integration of Personal Information Protection

**Shu Chen**

Criminal Law School, East China University of Political Science and Law, Shanghai

Received: Mar. 22nd, 2023; accepted: May 5th, 2023; published: May 12th, 2023

## Abstract

**At present, the practice pattern of big data investigation includes the accurate application of crime detection as the goal and the early warning system aiming at crime prevention. Compared with traditional investigation measures, big data investigation has natural advantages for crime detection and crime prevention in the era of big data. However, the risk of panoramic monitoring, the risk of data sharing and the risk of confusing criminal investigation with administrative law enforcement caused by big data investigation, make the introduction of personal information pro-**

文章引用: 陈舒. 大数据侦查的法律规制[J]. 争议解决, 2023, 9(3): 787-794.
DOI: 10.12677/ds.2023.93105

**tection become urgent. It is necessary to establish a rational cognition of the relationship between the legal regulation of big data investigation and the protection of personal information, take the principle of proportionality as a normative tool, and incorporate big data investigation into the legislation of criminal procedure, so as to achieve a reasonable institutional arrangement that balances the interests of various subjects.**

## Keywords

**Big Data Investigation, Personal Information, Crime Prevention, Risk, Principle of Proportionality**



## 1. 引言

随着国家大数据战略的推进和落实，大数据已成为各个领域的应用热点。政策层面的大数据也渗透到刑事司法领域之中，大数据技术在刑事侦查中的应用成为理论界和实务界论争的焦点，其对于个人信息保护的挑战是打击犯罪与保障人权两大刑事诉讼价值的冲突体现。然而，目前的研究成果往往直接跳过了对用以论证大数据侦查应用广度的实践样态的采集，未区分以犯罪侦破为目标的精准运用和以犯罪预防为目标的预警系统，导致法律规制探讨缺乏针对性。本文将对大数据侦查的内涵外延进行梳理，透析大数据侦查背后存在的个人信息保护风险；进而从域外各国刑事司法对个人信息保护的模式中寻找可借鉴之处；最后基于风险社会治理和个人信息的公共属性论证大数据侦查的正当性，以比例原则为规范工具，为个人信息保护融入大数据侦查寻求制度进路。

## 2. 问题背景：大数据侦查的内涵外延

### 2.1. 大数据侦查的界定

清晰的概念界定是探讨实践困境和法律规制的前提，作为一项新兴事物，需要对其内涵外延进行讨论。何为大数据侦查，大数据在侦查程序中的应用是否意味着传统侦查模式的现代化转型，学界对此一直存有争议。有的学者认为大数据是侦查信息化的一个面向，夸大大数据对侦查的影响反而不利于大数据在侦查领域的适用[1]。另一部分学者则认为大数据侦查是区别于现有法定侦查措施的一项强制性侦查措施；更有学者进一步指出一场由技术引发的侦查模式转型势在必行[2]。第一种观点具有一定的合理性，面对大数据这样一项新兴的并且在不断发展的技术，尤其是涉及到侦查模式这一庞大的基础性概念时，其定性问题以及对其法律规制的讨论应当有所慎重。然而，大数据在侦查活动中的适用早有尝试，并且随着大数据技术的纵深发展，其对侦查活动的渗透也变得无孔不入，大有裨益。由此，对于大数据侦查的界定，以及在制度构建中如何平衡打击犯罪与保障人权的双重价值，成为刑事司法领域中不可回避的课题。

学界目前对于大数据侦查的界定可以概括为两个层面：从广义角度看，大数据侦查包括大数据侦查思维、大数据侦查模式、大数据侦查方法、大数据侦查机制等完整的体系；从狭义角度看，大数据侦查强调侦查中对大数据技术的运用[3]。笔者认为不能仅从狭义角度界定大数据侦查，侦查中对大数据技术的运用只是其中的一个面向，还应当看到利用大数据技术进行的以犯罪预防为目标的前端侦查活动，并且这一类前端侦查活动中往往暗藏着更多对个人信息侵害的风险。学界、实务界在讨论大数据侦查时普遍将这一前端侦查活动纳入侦查活动中进行讨论，并由此引发其是否违背刑事诉讼中无罪推定原则的讨

论[1]。笔者认为讨论大数据侦查一系列问题时首先应当厘清的前提是，以犯罪预防为目标的前端侦查活动与以犯罪侦破为目标的侦查活动是并列关系，将二者强行相融会导致后续法律规则构建缺乏科学性和针对性。

### 2.2. 大数据侦查的实践样态

目前大数据技术在刑事侦查层面的应用主要有两种实践样态，一是以犯罪侦破为目标的精准运用，二是以犯罪预防为目标的预警系统。

#### 2.2.1. 以犯罪侦破为目标的精准运用

大数据技术在犯罪侦破中的精准运用深化了侦查线索的挖掘，包含初阶、中阶和高阶三个层次[4]：初阶运用是数据信息的检索，从传统线下线索收集到线上数据的一键式查找，从而提高侦查效率；中阶是数据信息的对比，通过同类数据信息库和不同类数据信息库的数据交叉比对，实现侦查范围的缩小；高阶运用是数据信息的深入挖掘，通过数据的关联性分析实现案件串并或者犯罪证据、相关人员的发现。

#### 2.2.2. 以犯罪预防为目标的预警系统

根据《刑事诉讼法》第 109 条的规定，刑事案件侦查的启动点为立案，而立案的前提是“发现犯罪事实或犯罪嫌疑人”，因此传统侦查活动是在刑事案件发生后进行的回溯。而利用大数据技术实现以犯罪预防为目标的预警是一个前端侦查活动，它不应纳入以犯罪侦破为目标的侦查活动之中，因此并未引起启动节点的前移进而导致立案程序的虚化。公安机关的二元职能属性又指向另一组关系，即其与公安机关行政执法职能的区别。笔者将通过下述的案例梳理三者间的关系。

2016 年某地公安机关通过数据预警平台进行“数据巡控”时，发现某博客网站中存在不良敏感词，为进一步确认犯罪事实，经侦部门联合网安部门和某数据服务公司，对内网、外网数据进行综合分析，确定了领导传销犯罪的核心人员及组织架构，帮助固定相关证据，实现了案件的侦破[5]。此案中，公安机关利用网络抓取技术进行数据巡控是其履行行政执法职能的体现，旨在维护良好的网络环境；而在发现与传销犯罪相关的敏感词后，借助大数据公司提供的数据服务系统判定传销犯罪的存在，是利用大数据技术进行的前端侦查活动，这为后面侦查取证、案件侦破工作的顺利开展提供有力引导。

## 3. 问题透析：大数据侦查对个人信息保护的挑战

2012 年《关于加强网络信息保护的决定》的通过开启了我国对于个人信息的立法保护。而后所采用的是分散立法模式，相关制度散见于《民法典》《刑法》《网络安全法》《消费者权益保护法》等法律法规之中。然而，唯独在刑事司法领域，未窥见对于公民个人信息保护的前进脚步。在 2021 年落地的首部针对个人信息的专门立法——《个人信息保护法》中，同样未对刑事司法领域的个人信息保护问题给出具体全面的规定，仅有个别条文规定了委任性规则。总体上看，我国刑事司法领域的个人信息保护并未跟上大数据侦查发展的脚步，但大数据侦查背后却暗藏着对公民个人信息侵害的各类风险。

### 3.1. 全景式监控风险

大数据时代下，公民的工作、生活、社交等行为都会产生数字留痕。当公权力与信息技术相结合时，容易产生福柯所描述的一种无限普遍化的“全景敞式主义”的国家监控形态。全景式监控风险在大数据侦查中的一个表现是侦查参与主体的社会化。技术的专业性让第三方顺势进入侦查的参与主体之中，这是技术红利转化为司法红利过程中不可避免的侦查权力外溢现象([6], p. 7)。侦查参与主体的社会化扩张包括两类，一是参与数据平台建设的第三方，二是负有被动履行协助义务的第三方。前者是指通过与侦

[1]因为它是犯罪活动还没有开始之前就产生的预警，涉及到侦查人员对预测结果如何应用以及侦查人员如何进一步采取行动等问题。

查机关签署战略合作框架协议等方式共建数据平台的第三方，如江苏泰安公安与华为公司签署合作框架协议，成立“泰安智慧公安生态应用示范中心”[2]。后者是指在案件侦查过程中依法应当向侦查机关履行协助义务的第三方，《网络安全法》第 28 条规定了电信业务者、互联网服务提供者协助侦查机关监控和提供信息的义务。电信业务者、互联网服务提供者收集、存储了公民的各类个人信息甚至是个人敏感信息，这些数据来源于用户使用服务前对于隐私条款的同意，而实践中往往出现的情形是，若用户不点击确认同意提供隐私条款中要求的信息，则无法启动相关服务。由此，大数据侦查下侦查参与主体由单一的“权力机关－个体”结构转变为多元的“公权力机关－社会－个体”三层级结构。如此的全景式监控下，和自身密切相关的个人信息反而成为公民无法触及的盲区。

### 3.2. 数据共享风险

大数据侦查的依托是能够容纳海量数据的大数据平台，数据资源的共享为平台建设提供了重要支撑。其中公安机关的数据资源共享渠道分别为与其他行政机关的共享、与网络信息业者的共享以及公安机关内部的数据资源共享[7]。以与其他行政机关的共享为例，多通过签署联合框架协议书的方式，如北京市公安局、北京海关等五部门在 2011 年就签署了《北京市五部门行政资源整合机制框架协议书》。然而，这些数据共享的做法没有接受足够的合法性审查以及有效的监督，不同部门、系统间的数据互通有无，无法对数据的流通去向和存除进行制约。这种失控也由于缺少严格的法律规制而外化为实践中的一些问题。例如，部分侦查人员利用工作便利获取个人信息甚至出售个人信息以此牟利。肖某原系衡阳市公安局刑侦支队五大队民警，2017 年肖某因投资失败急需资金，开始售卖公民个人信息牟利，由于肖某自己的数字证书没有公安“云搜索”平台的高级查询权限，他盗用几名同事的数字证书将查询到的公民户籍信息、行踪轨迹信息等出售给买方，先后共获利 181 万余元[3]。对于公民个人信息的获取通过数字验证和人机交互的方式即可实现，缺乏应有的法律规制。

### 3.3. 刑事侦查与行政执法的混同风险

学界在讨论大数据侦查的风险预警功能时，往往将目光聚焦在此时的侦查行为是否与无罪推定原则相冲突，以及是否导致立案程序的虚化这两个问题上。然而笔者在前文已经提到，以犯罪预防为目标的前端侦查活动与以犯罪侦破为目标的侦查活动是并列关系，不能简单地将前端侦查活动纳入侦查之中一概讨论。除此之外，由于行政程序和刑事诉讼程序具有宽松严苛的差异，还需要注意到大数据侦查中前端侦查活动与行政执法活动的混同风险。

由于我国公安机关具有行政执法以及刑事侦查的二元职能属性，完善行刑衔接机制的前提是厘清行政执法与刑事侦查的界限。实践中出现了一种“权力挪用”的方式，即通过形式较为便利的行政执法权来达到本应通过程序较为规范的刑事侦查权才能达到的目的([8], p. 118)。有学者对搜查运行机制进行实证考察时发现，公安机关在实践中会使用行政检查代替对犯罪嫌疑人的人身搜查，治安检查代替刑事诉讼中的场所搜查，拘传、拘留、逮捕等刑事到案强制措施在适用时，通常被《中华人民共和国人民警察法》中的留置、口头传唤等行政措施替代([8], p. 119)。在大数据语境中，公安机关基于社会治理进行的数据处理行为应当定性为以治安管理为目的的行政执法行为；若是基于打击犯罪进行的数据处理行为应当定性为以犯罪预防为目的的前端侦查行为。在前文提到的数据平台建设以及数据共享的情形下，对于

[2]泰安市公安局与华为技术有限公司签署合作框架协议，并为“泰安智慧公安生态应用示范中心”揭牌。这标志着双方将共同携手，进一步发挥科技创新引领作用，提升警务智慧化水平，显著增强泰安公安服务实战能力，支撑全市公安信息化的可持续发展。参见《泰安市公安局与华为公司签署合作框架协议 全力打造“智慧公安”》，载《搜狐网》2018 年 5 月 14 日，https://www.sohu.com/a/231587244_455266。

[3]参见《湖南一民警出卖公民个人信息获利 181 万买奢侈品，一审被判刑四年六个月》，载《新晨晚报》2020 年 4 月 6 日，https://baijiahao.baidu.com/s?id=1663235754120764775&wfr=spider&for=pc。

公民个人信息的调取只需通过数字验证和人机交互即可实现，若不建立完善的程序规范，刑事侦查和行政执法的界限极易混淆，将加剧国家权力对于公民个人信息的不当控制及使用。

## 4. 域外借鉴：个人信息在各国刑事司法中的保护路径

### 4.1. 域外各国主要模式

面对大数据侦查中展现出个人信息保护问题，域外各国在发展该项侦查技术的同时，也根据自身的法治传统和国情在刑事司法领域中形成了不同的个人信息保护路径，以期通过法定程序的规制实现犯罪控制和正当程序的双重价值。本文选取了欧盟、美国及德国三种极具代表性的模式，分析各自的特点以及在中国法律体系框架中的可借鉴性。

#### 4.1.1. 欧盟：专门法案模式

20 世纪下半叶，欧盟就开始为个人信息保护构建新的法律规则。而为了应对信息时代的新挑战，欧盟在 2016 年通过了被称为史上最严数据立法的《通用数据保护条例》(下文简称 GDPR)，但其中第二条明确规定该法案不适用于为刑事犯罪以及刑事处罚的执行。故而又制定了《以犯罪预防、调查、侦查、起诉或刑罚执行为目的的个人数据保护指令》，旨在解决刑事司法中个人信息保护问题。该指令第十八条规定，数据主体在刑事诉讼中享有的各项权利[4]。由此欧盟以 GDPR 为统领，与特殊领域立法一同形成了统一的个人信息保护法律体系。

#### 4.1.2. 美国：隐私权模式

作为英美法系的代表性国家，美国在刑事司法中对于公民个人信息保护采用的是隐私权模式。联邦宪法第四修正案关于搜查及隐私保障的判例法一直以来都被奉为规范政府各类获取信息行为的圭臬([9], p. 164)。1967 年 Katz 案确立了“合理隐私期待”标准[5]，打破了 1928 年 Olmstead 案[6]中确立的物理入侵标准，将第四修正案的保护对象扩大到公民的隐私利益之上。随着大数据时代的到来，“合理隐私期待”的内涵不断扩充，2014 年 Riley 案[7]中确认了公民对私人手机中存储的数据信息具有合理的隐私期待；2018 年的 Carpenter 案[8]中控方以警方调取的犯罪嫌疑人 127 天的手机基站位置信息指控其抢劫罪的成立，联邦最高法院最后确认公民对手机基站位置信息享有合理的隐私期待。由此可以得出，美国是通过判例的方式将个人信息纳入隐私权范畴，以第四修正案对搜查要求的令状原则规范刑事司法中对于公民个人信息的获取、使用。

#### 4.1.3. 德国：个人信息权模式

作为大陆法系国家的典型代表，德国将对公民个人信息的刑事司法保护导入刑事诉讼法典之中的模式也极具代表性。德国联邦宪法法院 1983 年的《人口普查法案》依据一般人格权发展出了信息自决权，开启了对个人信息的保护。作为成文法国家，德国在刑事诉讼法典中直接规定了大数据侦查的相关内容。例如，刑事诉讼法典第九十八条 a、b 和第九十八条 c 对计算机排查侦缉和数据对比进行了具体的规定([9], p. 165)，包括适用情形、启动条件以及后续的数据发还和销毁。其中第九十八条 a、b 对于计算机排查侦缉行为规定，“只有其他手段对于查明案件事实或查找行为人的行踪的希望相当渺茫的情况下，才得命令采取此项处分”，表明了德国对于刑事程序中使用大数据侦查的谨慎态度[10]。

[4] 参见欧盟法律法规数据库：https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL%3A2016%3A119%3ATOC。
[5]Katz v. United States, 389 U. S. 387 (1967).
[6]Katz v. United States, 389 U. S. 387 (1967).
[7]Riley v. California, 134 S. Ct. 2473 (2014).
[8]Carpenter v. United States, 138 S. Ct. 2206 (2018).

### 4.2. 域外模式的可借鉴性

欧盟对于个人信息保护的立法采取的是公、私一体的模式，GDPR 这一法案中的基本原则、具体规则适用于公、私两个领域立法，另外在刑事司法领域以专门法案对个人信息进行保护。美国坚持以第四修正案为圭臬，在搜查与隐私权保障的框架内规制刑事侦查权对于个人信息的干预。德国从个人信息自决权的人格权属性出发，在刑事诉讼法典中设置具体、严格的法定程序。基于成文法传统以及个人信息的人格权属性定位，德国的立法模式对我国更具借鉴意义。

德国延续了欧洲大陆二战后形成的重视人格尊严、个人自治的法律传统，发展出信息自决权这一人格权。我国 2021 年 1 月 1 日开始施行的《民法典》在人格权编中专门对隐私权和个人信息保护作出规定，调停了人格权还是财产权的归属争议，与德国对权利类型的判断形成一致。尽管 2021 年 11 月 1 日开始施行的《个人信息保护法》是针对个人信息保护的专门立法，但对于国家机关处理个人信息仅作出原则性的规定，这也就指向了在《刑事诉讼法》中对大数据侦查的权限、程序进行规定。

## 5. 制度进路：从理性认知到制度完善

### 5.1. 理性对待大数据侦查规制与个人信息保护的关系

面临上述提到的大数据侦查对于个人信息保护的挑战，需要对大数据侦查规制与个人信息保护的关系建立理性认知，看到大数据侦查的必要性以及个人信息的公共价值。

#### 5.1.1. 大数据侦查的必要性

大数据侦查是在风险社会中实现刑事司法治理体系和治理能力现代化的应有之义，也是实现国家治理体系和治理能力现代化的一个面向。“风险社会”一词最早由德国社会学家贝克提出，他指出在风险社会中必须把伤害的缓解与分配作为核心问题。大数据时代是一个信息社会，也是一个别样的风险社会。近年来，随着犯罪活动呈现出的隐形化和技术化，各国为防止危害后果的加剧开始更加侧重犯罪的预防，犯罪治理模式从而呈现出风险治理的特征。大数据侦查不单纯从个案出发挖掘与犯罪案件相关的信息的优势，为社会向风险预防的转型提供了重要手段。

同时，大数据侦查也是面对当前网络犯罪高发态势的重要治理工具。最高人民检察院网上发布厅发布的数据显示，2020 年全国检察机关起诉涉嫌网络犯罪 14.2 万人，同比上升 47.9%，其中黑灰色产业生态圈和集团化、跨境化趋向明显 [9]。对新型网络犯罪带来的犯罪治理难度的上升以及犯罪线索数据化的特点，传统的侦查手段针对性不足，而大数据侦查不论是从犯罪侦破和犯罪预警上都有着天然优势。

#### 5.1.2. 个人信息的公共属性

不论是欧洲的个人信息权模式还是美国的隐私权模式，都认可个人信息的私人属性，由此引申出的个人信息保护控制论观念深入人心。然而，这两种模式也并不排斥个人信息的公共属性。例如在“人口普查案”的判决中德国宪法法院尽管提出了“信息自决权”的概念，但并不认可个人对其个人数据享有绝对的排他支配权，个人数据保护仍然要受比例原则等的限制[11]。美国部分学者也在批判过度个人主义的隐私保护方式，认为确切的隐私单元是群体而非个人，隐私保护需要群体协调，个人主义的隐私保护的结果是无隐私[12]。

随着网络化、数据化时代的发展，个人信息的公共属性愈发得到认可，建立在个人主义下的传统个人控制理论已经不能适应大数据时代个人信息利用的新环境。因此对于个人信息保护在刑事侦查中的导

[9] 参见《2020 年检察机关起诉涉嫌网络犯罪人数上升近五成》，载《最高人民检察院网上发布厅》2021 年 4 月 7 日，https://www.spp.gov.cn/spp/xwfbh/wsfbt/202104/t20210407_514984.shtml#1。

入应当对个人信息的公共属性有理性认知，为了国家安全或公共利益的需要，公民享有的个人信息权利在一定程度上要有所限缩，以实现平衡各方主体利益的合理制度安排。

### 5.2. 规范工具——比例原则

比例原则以人权保障为逻辑起点，其本质是对基于公共利益需要而限制公民权利的国家权力进行限制[13]。比例原则滥觞于德国十九世纪的警察法时代，用于审查目的和手段之间的关系，该原则的适用从警察执法领域发展到一般行政法领域，最后被吸收为公法的一般原则。其中，德国联邦宪法法院 1958 年的药房案被认为是比例原则在司法实践中完全展开的标志性案件，该案判决中确立了比例原则的“三阶理论”，即其项下包括三个呈线性递进的子原则。首先是适当性原则，该原则是指国家措施必须适合于增进或实现所追求的目标，具体到大数据侦查中，要求侦查机关展开大数据侦查必须是仅以犯罪侦破与犯罪预防为目的。这一原则也渗入到对于技术侦查措施的规制中，《刑事诉讼法》第一百五十二条第三款规定“采取侦查措施获取的材料，只能用于对犯罪的侦查、起诉和审判，不得用于其他用途”。其次是必要性原则，指在相同有效达到目标的各种手段中，选择对公民权利最小侵害的手段，即若适用传统侦查措施能够实现侦查目的的，就不得运用大数据侦查。最后是狭义的比例原则，强调手段所欲达到的目的和采取该手段所引发的对公民权利的限制两者之间是否保持平衡。大数据侦查欲达到的犯罪侦破和犯罪预防目的，势必会对公民的个人信息进行干预，德国刑事诉讼法典对于计算机排查侦缉行为的适用规定“只有其他手段对于查明案件事实或查找行为人的行踪的希望相当渺茫的情况下，才得命令采取此项处分”[10]，是立法中比例原则的体现，这也与刑事诉讼追求打击犯罪和保障人权间的平衡相呼应。对于大数据侦查的法律规制应将比例原则在法律规范中体现，并以比例原则为指引构建系统的、严格的具体规范。

### 5.3. 具体规范

#### 5.3.1. 明确大数据侦查的法律属性

对大数据侦查进行法律规制的前提是明确其法律性质，目前《刑事诉讼法》未将大数据侦查列入法定侦查措施之中。公安部颁布的《公安机关执法细则(第三版)》(以下简称《细则》)中认识到了运用大数据技术进行的侦查工作不同于传统侦查措施，单列了“查询、检索、比对数据”这一侦查措施[11]，但由于《细则》属于内部规范，大数据侦查仍处于无法可依的状态。因此应当在《刑事诉讼法》“侦查”这一章节内将大数据侦查定性为一项单独的侦查措施，并对该侦查措施的程序要求进行细化，完善配套的非法证据排除规则。并且，立法中应当将以犯罪侦破为目标的精准运用和以犯罪预防为目标的预警系统区分开来。目前理论界和实务界仍对于以犯罪预防为目标的预警是否能够纳入侦查控制范围存在争议。大数据主动发现犯罪线索的原理在于通过对海量案件数据进行大规模样本训练，挖掘类案规律并建立相应的预警规则[14]。这就不同于基于维护网络空间环境的治理行为，若不将其纳入刑事诉讼程序严格规范，退而将其界定为行政执法行为，将出现前面论述的权力挪用风险。并且由于前端侦查行为针对的是非特定的数据主体，应设定更为严格的程序，充分贯彻比例原则，最大限度平衡个人信息保护的个人利益和犯罪治理的公共利益。

#### 5.3.2. 数据平台建设主体与使用主体分离

当前数据平台的建设在公安机关主导下呈现自建、自批、自用的局面，不利于监督和制约，无法保

[10]《德国刑事诉讼法典》第九十八条 a、b。

[11]《公安机关执法细则(第三版)》29-02 规定：“查询、检索、比对数据进行下列侦查活动时，应当利用有关信息数据库查询、检索、比对有关数据：(1) 核查犯罪嫌疑人身份的；(2) 核查犯罪嫌疑人前科信息的；(3) 查找无名尸体、失踪人员的；(4) 查找犯罪、犯罪嫌疑人线索的；(5) 查找被盗抢的机动车、枪支、违禁品以及其他物品的；(6) 分析案情和犯罪规律，串并案件，确定下步侦查方向的。”

障数据流转的合法性和必要性。将数据平台的建设主体与使用主体分离，可以防止侦查机关为了自身的侦查利益而滥用侦查权。如我国台湾地区在《通讯保障及监察法》中对于侦查机关的通讯监听这一类技术侦查中设计了申请、审查、执行主体的分离制度([6], p. 13)。这一分离下数据平台的建设主体可以依托第三方行政机关，杭州等地已尝试设立大数据资源局，统筹全市数据资源管理工作。并且由于侦查行为的不可诉，在相关环节出现纰漏时公民可以通过行政复议、行政诉讼的方式实现救济。

#### 5.3.3. 信息主体的知情权及救济程序

2016 年发布实施的《关于推进以审判为中心的刑事诉讼制度改革的意见》第十七条提出要健全当事人、辩护人和其他诉讼参与人的权利保障制度，其中包括依法保障当事人的知情权。明确信息主体享有知情权这一基础性权利，与程序正当原则相联结，也是确保控辩平等的重要武装。信息主体的知情权对应的是侦查机关的告知义务，当然基于刑事司法程序的顺利进行以及公共安全的需要，法定事由出现告知可能有碍侦查时侦查机关可以推迟告知信息主体。“无救济则无权利”，法律若不为权利提供救济，那么这一权利难以发挥其应有的价值，应当明确公民在大数据侦查中知情权受到不法侵害时包括申诉在内的一系列救济手段。

## 6. 结语

在我国刑事侦查全面拥抱大数据技术，以及个人信息保护全面深入的背景下，刑事司法领域中对个人信息保护的缺位显得置身事外。对此应当在理论层面进行更深入的研究，以回应大数据侦查带来的个人信息侵害风险，实现平衡各方主体利益的制度安排，平衡打击犯罪和保障人权的双重价值，为风险社会的有序发展提供有力保障。

## 参考文献

[1] 彭知辉. “大数据侦查”质疑: 关于大数据与侦查关系的思考[J]. 中国人民公安大学学报: 社会科学版, 2018, 34(4): 25-32.

[2] 杨婷. 论大数据时代我国刑事侦查模式的转型[J]. 法商研究, 2018, 35(2): 25-36.

[3] 王燃. 大数据侦查[M]. 北京: 清华大学出版社, 2017: 32.

[4] 张可. 大数据侦查之程序规制: 从行政逻辑迈向司法逻辑[J]. 中国刑事法杂志, 2019(2): 131-144.

[5] 单丹, 王铼. 大数据在网络非法集资案件侦查中的应用[J]. 中国人民公安大学学报: 社会科学版, 2017, 33(4): 84-91.

[6] 胡铭, 张传玺. 大数据时代侦查权的扩张与规制[J]. 法学论坛, 2021, 36(3): 5-14.

[7] 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构建[J]. 法治研究, 2021(5): 34-45.

[8] 左卫民. 规避与替代——搜查运行机制的实证考察[J]. 中国法学, 2007(3): 114-125.

[9] 程雷. 大数据侦查的法律控制[J]. 中国社会科学, 2018(11): 156-207.

[10] Schwartz, P.M. (2011) Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology. *William and Mary Law Review*, **53**, 363.

[11] 王泽鉴. 人格权法: 法释义学、比较法、案例研究[M]. 北京: 北京大学出版社, 2013: 200.

[12] Fairfield, J.A.T. and Engel, C. (2015) Privacy as a Public Good. *Duke Law Journal*, **65**, 385.

[13] 王锡锌. 个人信息国家保护义务及展开[J]. 中国法学, 2021(1):145-166.

[14] 王燃. 大数据时代侦查模式的变革及其法律问题研究[J]. 法制与社会发展, 2018, 24(5): 110-129.