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

赵祖斌
(中南财经政法大学 刑事司法学院,湖北 武汉 430072)

摘要:大数据时代,个人信息附着多重利益,由此决定了个人信息保护与利用是立法乃至包括侦查在内的涉及个人信息处理实践必须遵循的根本性理念。大数据侦查对此理念带来了冲击,实践中重个人信息利用轻个人信息保护,出现了过度收集个人信息、个人信息处理目的泛化、扭曲使用个人信息、个人信息存储期限过长等问题。解决这些问题的根本方法是在合理范围内处理个人信息,"在合理范围内处理"意味着个人信息处理具有正当性和规范性,对个人权益影响合理。"在合理范围内处理"作为平衡个人信息保护与利用的工具,可以限制侦查机关的数据权力,保障数字人权。为确保侦查机关在合理范围内处理个人信息,必须健全个人信息保护制度,重塑强制性措施体系,强化大数据侦查中个人信息处理的监管,完善大数据侦查的规则体系。

关键词:大数据侦查;个人信息保护;个人信息利用;合理处理

中图分类号:D922.16 **文献标志码**:A **文章编号**:2096-028X(2025)01-0056-10

科学技术深刻变革着人类的一切,大数据时代到来的同时社会矛盾也日益复杂化,由此激发的危害国家安全及社会公共利益的行为增多,传统犯罪在技术加持下越来越隐蔽化、组织化、智能化,依托新型技术催生了电信网络诈骗等新型犯罪,并占据了犯罪结构的较大比例,这对作为刑事犯罪治理前端的侦查带来了挑战。人的行为数字化是这些犯罪的共同特征,[①]大数据处理能力作为核心要素促使侦查传统范式转变,以满足更高的技术化、信息化要求,适应犯罪情势,大数据侦查对于数字化犯罪调查取证不可或缺。作为大数据侦查基础性"原料"的数据包含海量个人信息,个人信息对于大数据侦查的价值在新时代犯罪情势中被放大,个人信息的利用达到了前所未有的深度和广度。随之而来的个人信息保护问题也不可忽视。这其实确立了一种基本立场:平衡个人信息保护和利用。

《中华人民共和国个人信息保护法》(简称《个人信息保护法》)第13条规定"为公共利益实施新闻报道、舆论监督等行为,在合理的范围内处理个人信息"及"依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息"不需取得个人同意。第27条规定"个人信息处理者可以在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息"。不同于第13条和第27条规定的在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息,在合理范围内处理个人信息是一项个人信息处理准则。[②] 相较于第13条和第27条的规定,"在合理范围内处理"的"效力"面更广,包括大数据侦查在内的所有个人信息处理场景应一以贯之。一是对"为公共利益实施新闻报道、舆论监督等行为"进行扩大解释,侦查可纳入"等行为"之列;二是侦查过程中也会处理个人自行公开或者其他已经合法公开的个人信息。

然而,除此两种情形外,侦查中个人信息处理仍需在合理范围内进行。侦查虽然是公权力行为,但是仍然要遵守个人信息保护相关法规,在利用个人信息时并不能为了打击犯罪而肆无忌惮,需要在合理范围内处理个人信息。"在合理范围内处理"与"个人信息保护和利用平衡"之间就建立了逻辑关联——个人信息保护与利用的平衡要义是在合理范围内处理个人信息。在侦查视阈中挖掘此二者的内在关联,科学阐释"在

基金项目:2023年度中国博士后科学基金资助项目"大数据侦查中个人信息保护研究"(2023M733922),2023年度中南财经政法大学中央高校基本科研业务费专项资金资助项目"大数据侦查中个人信息保护研究"(2722023BQ034)

作者简介:赵祖斌,男,法学博士,中南财经政法大学刑事司法学院讲师,司法鉴定技术应用与社会治理学科创新基地、博士后流动站研究人员。

① 参见赵祖斌:《论开源情报运用于职务犯罪初步核实》,载《政法学刊》2024年第1期,第6页。

② 参见赵祖斌:《已公开个人信息在合理范围内处理的规范逻辑与实践因应》,载《行政法学研究》2025年第1期,第158页。

合理范围内处理”具有重要价值。笔者试图诠释“在合理范围内处理”的含义,并从大数据侦查角度论证“在合理范围内处理”的根据,以及如何实现“在合理范围内处理”,以期对个人信息保护有所裨益。

一、在合理范围内处理的规范意涵

在合理范围内处理个人信息可从如下方面理解:一是个人信息处理必须符合具备合法性的情形,不能在法定情形之外处理个人信息。合理使用可视为是合理处理的一种参照,个人信息处理在合理使用情形内便具有合理性。二是个人信息处理行为规范,符合一定的标准。现实中,此两种含义并非泾渭分明,比如当非法使用个人信息时,可能存在个人信息处理未基于法定情形,或者个人信息处理行为未符合规范标准的情况。换言之,仅当个人信息处理基于法定情形且符合规范标准时才是合理的。侦查机关基于打击犯罪之需要,运用大数据手段处理个人信息具有合法性基础,即具备了“第一阶”上的违法阻却事由。在获得违法阻却事由后进入“第二阶”,侦查机关必须在履行相应义务以求满足履行职责需要之际兼顾个人信息保护,个人信息处理行为才具备了完整意义上的合法性。①

(一)个人信息处理行为正当

《个人信息保护法》同时使用了个人信息利用、使用、处理等名词。三个名词的确存在差别,又具有内在关联。“在合理范围内处理”内在地规定着个人信息处理行为具有正当性,而这种正当性建立的前提是个人信息可被处理,即个人信息可被利用。“个人信息合理利用”是指在合理范围内发挥个人信息的效能,实现特定目的。可以理解为,在侦查等涉及公共利益,以及企业服务等涉及私人利益的场景中,只要具备正当事由皆可以利用个人信息。其并不指向具体行为,更多的是对个人信息价值挖掘的宏观态度和立场,在整个个人信息保护体系中处于方向性地位,指导着个人信息利用、处理准则、规范等事项的设定。

个人信息利用与处理是分属不同层次的概念,二者存在手段与目的的关系。个人信息处理类似于使用特定的方法对个人信息进行“加工”,挖掘个人信息的价值。实施加工行为的目的在于利用个人信息,此过程便涉及个人信息使用。个人信息利用是个人信息使用的上位概念,个人信息使用是个人信息利用的重要途径和媒介。个人信息使用的另一层意思是“不包括个人信息的存储、加工、传输、提供以及公开,而仅指个人信息处理者对个人信息进行的分析和利用”。② 使用个人信息在具体意义上包括处理,《互联网个人信息安全保护指南》第 3.6 条对个人信息使用作出如下规定:“通过自动或非自动方式对个人信息进行操作,例如记录、组织、排列、存储、改编或变更、检索、咨询、披露、传播或以其他方式提供、调整或组合、限制、删除等。”

个人信息合理使用可视为一项借鉴著作权合理使用的制度,其指个人信息处理者无需取得信息主体同意而直接依据法律规定处理个人信息。③ 合理使用是合理利用的具化,或曰一种情形。《个人信息保护法》第 4 条第 2 款与《中华人民共和国民法典》(简称《民法典》)第 1035 条第 2 款保持一致,将个人信息使用视为个人信息处理行为之一,规定“个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等”。如果大数据侦查中处理个人信息的情形是侦查机关为了履行职责、打击犯罪,那么此场景行为可归结于《民法典》第 999 条、第 1020 条、第 1023 条的情形,侦查机关可以处理个人姓名、肖像、声音等可识别个人的资料。

(二)个人信息处理行为规范

“个人信息保护与利用的平衡,是《个人信息保护法》的基本立场、理念、精神,是理解整部法律的内在体系和核心线索。”④在保护个人信息的基本目的得以实现的情况下,为个人信息的合理利用确定范围、方法等,能够促进个人信息的合理使用。实现保护个人信息和促进个人信息合理利用双重目的的手段和方法,是规范个人信息处理活动。⑤ 个人信息保护、利用的平衡与在合理范围内处理之间存在目的与手段相互契合

① 参见赵祖斌:《已公开个人信息处理规则的构造及适用——以合法处理事由为中心》,载《交大法学》2024 年第 5 期,第 141 页。
② 参见程啸:《个人信息保护法理解与适用》,中国法制出版社 2021 年版,第 71 页。
③ 参见程啸:《论我国民法典中的个人信息合理使用制度》,载《中外法学》2020 年第 4 期,第 1008 页。
④ 申卫星:《论个人信息保护与利用的平衡》,载《中国法律评论》2021 年第 5 期,第 29 页。
⑤ 参见张新宝:《〈中华人民共和国个人信息保护法〉释义》,人民出版社 2021 年版,第 22 页。

的关系。兼顾个人信息保护和利用表明“个人信息保护立场应从信息主体自主支配转向有序共享”,[①]个人信息“有序共享”就集中反映为在合理范围内处理个人信息。个人信息是否在合理范围内处理的表征在于侦查机关是否遵循了个人信息处理相关法律规范,包括个人信息处理目的是否合法、个人信息处理是否遵循了必要性原则、是否采取了个人信息安全保护措施等。

符合法定处理情形,可以处理个人信息仅表明侦查机关享有个人信息合理使用权,但是与其规范地行使该项权力分属不同的范畴。换言之,即使侦查机关基于法定处理情形处理个人信息,但是其个人信息处理行为是否合规仍不确定,仅在规范地处理个人信息时方可视为行使个人信息合理使用权,个人信息处理行为才具备合法性。因为类似于著作权合理使用,合理使用是一种合法行为、无侵害性,[②]所以个人信息合理使用一定是在一定范围内适度地处理个人信息。

《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,应当依法律、行政法规规定的权限和程序进行,且不得超出履行法定职责所必需的范围和限度。该条实际上就规定了侦查机关处理个人信息的目的必须与履行职责相关,而且要严格依照法定程序进行。第33条更是明确规定国家机关处理个人信息活动适用《个人信息保护法》,除有特殊规定之外,同样要遵守相应规则。对此,刑事诉讼法律规范也有所体现,比如《中华人民共和国刑事诉讼法》(简称《刑事诉讼法》)第54条规定公安司法机关在收集调取涉及个人隐私证据时要保守秘密,第64条规定公安司法机关对特定案件中人身安全面临危险的证人等人员采取隐匿个人信息等保护措施。

(三)对个人权益影响合理

侦查机关在法定处理情形中,处理个人信息必须以不严重侵害个人信息主体权益为界限,这就决定了侦查机关必须把握好这个度——在合理范围内处理个人信息,使得个人信息处理行为“符合正义、公平、公益、合理的社会生活准则”,[③]进而满足形式和实质双重合法性。为了维护国家安全、保护人民群众的生命财产安全,基于侦查工作的需要,侦查机关运用一切必要的技术手段搜集犯罪分子及非犯罪分子的个人信息,不可避免地会侵入组织、公民的“领地”,一旦过度收集或者滥用个人信息,既会损害个人权益,也会冲击社会秩序。[④] 假设大数据侦查通过不当处理个人信息以换得犯罪治理提效和公共安全,那么其将因破坏了个人信息保护和利用的平衡而面临着正当性诘问。侦查机关在合理范围内处理个人信息于形式上集中反映为履行个人信息保护义务,依法处理个人信息,而实质却在于避免对信息主体权益造成不合理的侵害。侦查机关在享有个人信息(数据)处理权的同时还有义务保护数据之上承载的原权益人(侦查对象)的相应合法权益。

不可否认,侦查机关处理个人信息在某种程度上侵犯了个人权益,比如检索国家企业信用信息公示系统进行犯罪分子画像的行为会对嫌疑人隐私等权益产生影响。不过,对个人权益有影响也不必然意味着超出合理范围。是否合理主要取决于自主决定权、个人名誉、精神状态、人身财产等个人权益相较于打击犯罪是否具有优先性,即使没有优先性,那么是否将影响控制在最低限度内。基于公共利益处理个人信息实则是对个人信息人格权益进行限制,[⑤]这种限制即使具有法定事由,但仍然需要最小化地侵害个人权益。申言之,谨慎地对待将公共利益作为个人信息处理合法事由,最大限度地做到“公共产品所需要的数据既易于获得,又能有效保障公民权利”。[⑥] 公共利益中隐含着个人利益,维护公共利益的本源在于维护个人利益,况且公共利益并不是任何时候皆具有绝对的优先性,需要在具体情势中进行利益衡量,以确定个人利益与公共利益的平衡。这需要侦查机关等公权力部门在基于维护公共利益处理个人信息时必须兼顾个人利益。

二、在合理范围内处理的作用逻辑

大数据侦查中在合理范围内处理个人信息能够达到个人信息保护与利用平衡之目的的本源在于“在合

① 参见刘艳红:《公共空间运用大规模监控的法理逻辑及限度——基于个人信息有序共享之视角》,载《法学论坛》2020年第2期,第8页。

② 参见吴汉东:《著作权合理使用制度研究》(第4版),中国人民大学出版社2020年版,第112页。

③ 参见吴汉东:《著作权合理使用制度研究》(第4版),中国人民大学出版社2020年版,第113页。

④ 参见洪浩、赵祖斌:《个人信息保护中检察公益诉权配置的根据》,载《内蒙古社会科学》2020年第6期,第89页。

⑤ 参见赵祖斌:《合理使用:侦查中个人信息处理合法性基础新解》,载《中国刑警学院学报》2024年第5期,第117页。

⑥ 参见[美]阿莱克斯·彭特兰:《智慧社会:大数据与社会物理学》,汪小凯、汪容译,浙江人民出版社2015年版,第171页。

理范围内处理”作为一种“工具”能够限制侦查机关的数据权利,从而最终保障数字人权。

(一)平衡个人信息保护与利用的工具

大数据时代的到来,改变了人类的行为方式,诸多行为由线下变为线上,呈现出虚拟与现实相互交错的景象,这离不开信息技术的发展,以及个人信息的支撑。新的技术多会被不当地用于实施犯罪行为,引致犯罪类型发生变化,犯罪手段智能化、隐蔽化,依靠技术实施反制成为共识。本质上而言,犯罪是由人、时间、空间等要素构成的事件,与人身份相关的资料是支撑侦查的原材料。大数据侦查提高了证据线索收集的效率及准确性,为防范、阻止、惩治危害国家安全和人民利益的行为提供了有力支持。但是利用技术手段大规模收集证据线索的行为也对个人信息安全和个人隐私保护带来了严峻的挑战。“个人信息处理是国家、社会信息化发展的必然要求,个人信息保护与处理的冲突却又不可避免。”①大数据侦查对个人信息权益的干预逐步加深,其无论是针对特定对象,抑或是不特定对象皆可能侵害个人信息权益,个人信息权益保护与大数据侦查间的冲突日益显现化。即使大数据侦查在处理数据时必然会威胁个人信息安全,但是并不意味着否定大数据侦查的适用,关键在于大数据侦查要遵循个人信息保护和利用平衡的理念。

个人信息可被处理并不意味着信息主体丧失了权益保护的需求,个人信息处理主体仍然需要“在法律明确规定的合理的限度以内……按照法律规定对个人信息进行利用,但不应对个人信息、隐私造成侵犯,不应以影响数据安全的方式为之利用”。② 当个人信息保护与利用的张力增大,其他利益优于个人信息权益,更加突出个人信息利用的情况下,有必要将个人信息处理限定“在合理范围内”,从而实现个人信息保护和利用的平衡。此时,“在合理范围内处理”实质是一项手段,用其限制干预个人信息权益的权力(利)。个人信息保护和利用不是互斥的,大数据侦查与个人信息保护之间不是对立的。为了打击犯罪可以实施大数据侦查,但是当公权力与私权利发生冲突,为重建和平,或者一种权利必须向另一种权利(或有关的利益)让步,或者二者在某一程度上必须各自让步,③则不能简单地强化个人信息保护,或者过于强调个人信息利用。即使为了个人信息利用不得已“淡化”个人信息保护,但是也必须尽可能地采取相应措施将这种“淡化”控制在合理范围内。

(二)限制数据权力的手段

大数据时代,“犯罪者也难逃‘天网恢恢、疏而不漏’的数据记录和存储体系,数据化已成为犯罪的现实生态。”④因应犯罪治理需要,侦查权在算法等大数据信息技术加持下发生了迭代,由物理性权力演化扩充为包含数据性权力的结构性权力,侦查机关由此享有一种数据权力。数据权力并非大数据权力,不仅意指适用大数据技术对数据进行全新解读,而且是建构于海量、多样数据之上,聚合数据并对数字环境参与者之间的数据流通进行控制的能力。⑤ 数据权力本质是一种以数据为媒介的数据控制能力。侦查机关作为国家机器,拥有涵盖人、事、物等海量的数据,能够依托大数据技术掌握犯罪治理参与主体的信息流动,提取犯罪信息,根据获得的信息生成犯罪情报,以此达到查证案件事实、收集证据、缉捕犯罪嫌疑人的目的。基于犯罪智能化,以及技术主义在侦查中日益显现的趋势,数据权力呈扩张之势,未在合理范围内处理个人信息即是有力的例证。换言之,未在合理范围内处理个人信息与数据权力扩张存在内在逻辑关联性,前者既是后者的表现形式之一,也是条件或曰载体;后者既是前者的本质,也是结果抑或危害。

区别于物理性权力,数据权力作用的场域主要是虚拟空间,或者虚拟与现实交汇的空间,其依托算法,以一种“没有暴力,甚至没有感受到强迫,几乎不被察觉”的方式运行。⑥ 侦查参与主体无法如同物理性权力运行一样感知数据权力之运作,以及其对权力相对人带来的危害。个人信息未在合理范围内被处理,个人信息主体乃至作为个人信息处理者的侦查机关或许也未充分意识到。某种程度上而言,数据权力规范化运行更

---

① 甄世辉、王跃峰:《大数据时代个人信息处理与保护之平衡》,载《社会科学论坛》2021 年第 3 期,第 166 页。

② 参见江波、张亚男:《大数据语境下的个人信息合理使用原则》,载《交大法学》2018 年第 3 期,第 114 页。

③ 参见[德]卡尔·拉伦茨:《法学方法论》,陈爱娥译,商务印书馆 2003 年版,第 279 页。

④ [法]马尔克·杜甘、[法]克里斯托夫·拉贝:《赤裸裸的人》,杜燕译,上海科学技术出版社 2017 年版,第 4-5 页。

⑤ Isabel Hahn, *Purpose Limitation in the Time of Data Power: Is There a Way Forward?*, European Data Protection Law Review, Vol.7:31, p.33 (2021).

⑥ 参见[法]马尔克·杜甘、[法]克里斯托夫·拉贝:《赤裸裸的人》,杜燕译,上海科学技术出版社 2017 年版,第 4-5 页。

多地是依赖权力主体的自省、自觉、自律。权力从“拥有雄厚的资本”转向“拥有丰富的信息”,[①]个人信息是数据权力的核心媒介,个人信息处理既是数据权力运作的一环,也是关键表现形式,其在合理范围内进行的形式目的在于保护个人信息安全,实质目的在于从“源头”根本性地抑制数据权力扩张。

(三)保障数字人权的方式

与数据权力相对的权益形态是以个人信息为媒介的数字权益体系,并不局限于个人信息权益、隐私权,而是以个人信息为轴心的数字人权——“它以双重空间的生产生活关系为社会基础、以人的数字信息面向和相关权益为表达形式,以智慧社会中人的全面发展为核心诉求,突破了前三代所受到的物理时空和生物属性的限制,实现自由平等权利、经济社会文化权利、生存发展权利的转型升级。这既包括前三代人权在智慧发展条件下的数字化呈现及其相应保护,也包括日渐涌现的各种新兴(新型)数据信息权利及其保护,其本质是在数字时代和智慧发展中作为人而应该享有的权利。”[②]大数据侦查对公民个人信息权益的侵害只是打开了“潘多拉魔盒”,更为显著的是会侵害数字人权。不当处理个人信息已不是简单地侵害个人信息权益本身的问题,而是对信息时代中主体身份建构、自由平等和自主性的严重侵蚀。侦查机关与相对人,尤其是犯罪嫌疑人在数字场域中的地位差距进一步拉大,以及技术运用封闭,带来数字鸿沟,形成数字弱势群体。数字化标识难以消除,影响个人就业等权益,甚至损害子女“代际”人权,以及父母妻子及朋友等“毗邻”人权。

数字人权作为第四代人权,数据和信息是其载体,是人在智慧社会中生存和发展所需要的基本权利。保障数字人权是人权保障在数字空间和智慧时代的自然延续和必然要求,其核心在于保护个人信息安全,进而以此为突破口避免个人隐私受到侵犯,弥补信息鸿沟,消除算法歧视,限制大规模监控。从某种程度上而言,个人信息保护制度无法应对人工智能系统给人权保障方面带来的挑战,但是现阶段仍然以个人信息保护为核心点是无可奈何的权宜之策。“在合理范围内处理”既是一种动态平衡机制,也是个人信息保护和利用平衡的砝码,为侦查机关配置在合理范围内处理个人信息的义务,防止其为了侦查办案而过度处理个人信息,引致个人信息保护与利用的失衡,从而达到最大限度地保护公民个人数字人权的目的。

三、在合理范围内处理的违反情形

在《个人信息保护法》正式颁布前,立法者主张个人自行公开或者其他已经合法公开的个人信息处理目的不“符合个人信息被公开时的用途”,个人信息处理便不在合理范围内。[③]《个人信息保护法》正式颁布后放弃了单纯将个人信息处理是否“符合个人信息被公开时的用途”作为“在合理范围内处理”的判断标准。个人信息处理是一个围绕目的形成的“行为集”,其中任何一个不规范行为皆可能视为对“在合理范围内处理”的违反。大数据侦查中个人信息处理未在合理范围内包括个人信息处理目的泛化、个人信息收集过度等多个面向。

(一)个人信息收集过度

大数据侦查以海量数据为依托,因而数据的占有量直接决定了大数据侦查的效果,内含在数据中的个人信息也被广泛收集并呈现出过度化倾向。“过度”是相对于正常、必要而言的,意指个人信息收集超过正常所需的范围。《个人信息保护法》必要性原则要求,个人信息收集必须控制在与实践密切需要的最小范围内,对个人权益影响最小。根据公安部颁布的《规范使用执法场所办案区“四个一律”》的相关规定,违法犯罪嫌疑人被带入办案区后便被要求接受采集个人DNA、指纹等可识别个人身份的生物样本信息,并被录入相应的数据库,以供挖掘线索证据。实践中无差别、不限量地采集个人信息调查取证、筛选犯罪嫌疑人的情况屡见不鲜,正是尝到了利用大量个人信息查办案件的“甜头”,侦查机关企图构建这种在所有案件中可以

① 参见[美]约瑟夫·S.奈:《硬权力与软权力》,门洪华译,北京大学出版社2005年版,第105页。

② 马长山:《智慧社会背景下的“第四代人权”及其保障》,载《中国法学》2019年第5期,第16页。

③ 《中华人民共和国个人信息保护法(草案一次审议稿)》第28条规定:“个人信息处理者处理已公开的个人信息,应当符合该个人信息被公开时的用途;超出与该用途相关的合理范围的,应当依照本法规定向个人告知并取得其同意。个人信息被公开时的用途不明确的,个人信息处理者应当合理、谨慎地处理已公开的个人信息;利用已公开的个人信息从事对个人有重大影响的活动,应当依照本法规定向个人告知并取得其同意。”

复刻的“范式”,形成“大数据侦查中心主义”,高度依赖大数据侦查,进而出现从自身建立的天网工程、金盾工程,以及美图、百度等大型平台公司,以及网吧、旅馆、车站等数据平台无时无刻不在大量收集公民的衣食住行等方面信息的现象。

(二)个人信息使用扭曲

大数据时代,个人信息使用领域增多,其在反对恐怖主义、打击电信网络诈骗等犯罪活动中被广泛使用。在使用领域增多的同时,也出现了个人信息在大数据侦查中被扭曲化使用的现象。侦查机关利用信息收集工具在社交网络等各种媒介上收集海量的个人信息,再利用人工智能工具分析收集到的个人信息,挖掘个人信息之间及个人信息和其他信息之间的潜在联系,然后根据分析得到的潜在联系对个人作“画像”。一方面,将个人信息用于实施大规模数据监控,使得包括刑事犯罪嫌疑人在内的所有公民皆被监控,成为潜在的侦查对象,个人的一举一动皆被侦查机关随时随地掌握,在侦查机关面前处于“裸奔”状态。① 另一方面,受算法歧视的影响,很容易出现类似于“大数据杀熟”的现象。大数据侦查侧重于建构数据与事实之间的相关关系,而非因果关系。侦查机关很容易通过挖掘到的个人言论、行为等各项信息,对环境及个人进行风险评估,一旦从个人信息中获取的情报表明个人基于人种、肤色、生活区域等不同因素而存在更高的实施犯罪行为的危险性,便会据此对个人采取过度盘查、监控等歧视性措施,公民个人会受到不公正的对待。

(三)个人信息处理目的泛化

个人信息处理目的是否特定是判断个人信息处理是否在合理范围内的重要标准之一。从整个个人信息处理合法性基础角度而言,基于打击犯罪处理个人信息具有正当性。但是以大数据侦查视角观之,个人信息处理一定是为了实施大数据侦查,如此才具有狭义层面的正当性,进而符合目的限制原则。此关涉大数据侦查概念的理解和属性的界定。一种观点认为:“大数据侦查是一种侦查理念,它所起到的警示作用是,侦查人员所追求的数据应是全方位的,不能囿于结构化数据。”②此观点揭示了在大数据侦查中利用个人信息的必然性,但是没有揭露大数据侦查的实质。还有观点认为,大数据侦查包含犯罪预测、立案前的调查核实和立案后的侦查行为。③ 大数据时代,犯罪情势的改变促使侦查模式从被动型转为主动型,从人到案侦查途径更加突出,一步式侦查的转变更为显著,前侦查程序和后侦查程序的界限模糊化。④ 从人到案侦查途径内含从案到人侦查途径的流程,大数据侦查仅是侦查的一个“子集”。即使预测性是大数据的本质特征,但是将以大数据为支撑,通过个人轨迹等信息“析出”犯罪热点地区与犯罪高危人群,从而采取措施加强对高危人群和地区控制的行为视为大数据侦查并不妥当。大数据侦查可归结为主动型侦查之列,⑤于犯罪行为发生时同步启动,而提前启动有违大数据侦查的定位。依据“是否会侵犯公民基本权利”来界定,大数据侦查因可能对个人隐私权、财产权、个人信息权益造成侵害而在本质上是一种强制性侦查措施,⑥因而其不可以被用于具有治安管理属性的预测犯罪,以及刑事立案前的调查核实中。这就决定了预测犯罪,以及刑事立案前的调查核实中依托大数据侦查处理个人信息背离了大数据侦查的属性、定位,侵害公民个人基本权利。

(四)个人信息加工不当

大数据侦查需要依托人工智能技术进行,数据、算力、算法是三大支撑要素。数据作为基础“养料”,直接关系到大数据侦查的可行性和准确性。⑦ 一旦使用了瑕疵数据,很可能“误导”大数据侦查,导致大数据侦查得出错误的结论,对公民个人权益产生影响。保障数据质量是开展大数据侦查、避免侦查错误的重要工

---

① 参见程雷:《大数据侦查的法律控制》,载《中国社会科学》2018 年第 11 期,第 162 页。

② 商瀑:《人工智能与刑事侦查:历史变迁、技术分类及未来展望》,载《中国人民公安大学学报(社会科学版)》2020 年第 6 期,第 48 页。

③ 参见白福鼎:《大数据侦查与个人信息保护的冲突及其调和》,载《浙江警察学院学报》2023 年第 3 期,第 106 页。

④ “前侦查程序是侦查启动前侦查权的运行过程,是侦查机关在获得关于犯罪已经发生或已处于预备阶段之可能性的线索时,为判断是否启动侦查程序而展开的侦查前的调查程序。”闾刚:《前侦查程序研究》,南京大学 2017 年博士学位论文,第 41 页。

⑤ 有研究认为:“主动侦查,是指对正在进行或者将要实施的犯罪,通过运用监控措施、侦查策略或情报主导等方法,控制犯罪的实施过程或促使犯罪嫌疑人以侦查人员设定的时间、地点、方式实施犯罪活动,在查获犯罪嫌疑人的同时收集、固定犯罪证据的侦查方式。”杨郁娟:《论主动型侦查与被动型侦查》,载《铁道警官高等专科学校学报》2011 年第 1 期,第 24 页。从“主动”二字出发,主动型侦查是对正在实施的犯罪行为进行调查取证。而对还未实施的犯罪行为采取侦查措施是主动型侦查的观点可能要持否定态度。即使对将要实施的犯罪行为采取相应侦查措施,“将要实施的犯罪行为”一定是有证据证明积极准备实施,比如准备犯罪工具等,否则,主动型侦查便包含预测性侦查。

⑥ 参见胡铭、龚中航:《大数据侦查的基本定位与法律规制》,载《浙江社会科学》2019 年第 12 期,第 14 页。

⑦ 参见赵祖斌:《生成式人工智能对个人信息保护的冲击及纾解——基于侦查场景的分析》,载《情报杂志》2024 年第 11 期,第 176 页。

作,侦查机关在大数据侦查过程中有义务保障包含个人信息的数据真实、可靠。然而,大数据侦查实践中存在侦查机关并未履行保障数据真实、可靠的义务,生成错误结论的现象。一方面,侦查机关自身忽视数据质量保障问题,致使无辜者被纳入犯罪调查之中。另一方面,侦查机关未尽到数据可靠性审查义务,未能识别有误的个人信息,进而导致侦查错误。犯罪嫌疑人会根据大数据侦查"根植"于数据这一特性,进行反大数据侦查行为——释放虚假、不完整数据,以此误导侦查方向。

(五)个人信息泄露加剧

由于大数据侦查以海量数据为基础,仅依靠侦查机关自身掌握的数据无法完成犯罪行为的"显现",需要侦查机关与其他掌握数据的部门进行深度合作。实践中,用于大数据侦查的部分数据来自侦查机关自建数据库,而大部分数据其实来源于企业、其他政府部门。2016年公安部发布的《公安机关信息共享规定》提出加强内外数据整合,实现信息共享。近年来,公安部门提出"专业+机制+大数据"提升公安战斗力,部分地区公安机关与企业达成合作战略,共同挖掘大数据价值,侦查机关借此赋能新质侦查力。这些探索值得称赞,但同时需要注意,侦查机关与其他政府部门及企业共享数据过程中涉及传输、分享等多个环节,环节的增多无疑加大了个人信息泄露的风险。尤其是现如今,侦查机关技术能力较为有限,对第三方企业技术依赖度较高,在请求第三方企业协助时,会将部分数据分享给企业,使企业在某种程度上而言就"享有"了侦查权。侦查权的"外溢",加之企业一旦数据处理操作不当,就可能致使个人信息泄露。此外,在犯罪行为日益跨国化的背景下,实施大数据侦查过程中还涉及数据跨境,个人信息在数据跨境过程中也容易泄露。

(六)个人信息长期存储

个人信息处理遵守必要性原则的另一个要求是个人信息存储期限尽可能短。域外国家在警务实践中通过立法或司法对此进行了确认,比如英国《2018年数据保护法》规定,在执法过程中处理个人信息需要遵循的原则之一便是个人数据存储期限要短于实现处理目的所必要的最短时间。[①]《个人信息保护法》规定:"除法律、行政法规另有规定外,个人信息的保存期限应当为实现处理目的所必要的最短时间。"全国信息安全标准化技术委员会颁布的《信息安全技术 个人信息安全规范》(GB/T 35273-2020)第6.1条规定:"个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间,法律法规另有规定或者个人信息主体另行授权同意的除外。"从保障公民个人信息权益角度而言,大数据侦查同样需要遵守个人信息存储期限最短规则。然而,实践中侦查机关为了顺利实施大数据侦查,遵循有备无患的逻辑,大量收集个人信息并无限期存储,[②]并且在达到处理目的后仍然不及时删除无用的个人信息。这不仅侵犯了公民个人信息遗忘权、删除权,而且会制造数据"噪音",造成数据冗余,降低数据质量。[③]

四、在合理范围内处理的实现路径

(一)健全个人信息权益保护制度

第一,将"个人信息保护与利用并举"写入《刑事诉讼法》。《刑事诉讼法》对于个人信息保护与利用的相关规定较少。第150条规定了技术侦查措施。技术侦查措施与大数据侦查存在交叉,涉及个人信息处理重叠部分可以视为赋予了侦查机关有限的个人信息处理权。第152条和第154条对个人隐私保护作了附带性规定。第152条仅规定保护技术侦查过程中知悉的个人隐私,第154条规定将技术侦查措施获得的材料作为证据使用时,为了保护公民个人隐私等目的,应当采取不暴露有关人员身份、技术方法等保护措施,或者在必要时庭外核实证据。个人隐私与个人信息不同,且上述条文并未将个人隐私权保护作为侦查权规制核心。有必要与《个人信息保护法》对接,将"个人信息保护与利用并举"写入《刑事诉讼法》。

第二,将个人信息权引入大数据侦查。大数据侦查规制必须从行为义务模式迈向权利义务复合模式,构建大数据侦查"权力—权力"和"权力—权利"双向框架。[④] 域外国家基于此在侦查程序中确立了个人信息

① 参见张涛:《智慧警务背景下公安机关处理个人信息的规范建构》,载《公安学研究》2023年第1期,第56页。
② 参见薛悟娟:《大数据时代个人信息的运作模式、理论困境及保护路径》,载《中国海商法研究》2024年第2期,第104页。
③ 参见王仲羊:《侦查中个人信息处理的合法性基础》,载《中国人民公安大学学报(社会科学版)》2024年第1期,第104页。
④ 参见林海伟:《平台控制下个人信息数据的权利配置:对第三方原则的双重反思》,载《治理研究》2023年第3期,第157页。

权或者类似的权利。美国宪法第四修正案确立了一般禁止执法者无搜索票而查阅电脑存储的资料的立场,2014 年美国最高法院在“莱利诉加利福尼亚州案”中认为个人手机如同电脑一样,不再适用附带搜查规则。① 德国联邦宪法法院于 1983 年在“人口普查案”中由一般人权导出了资讯自决权,甚至在 2008 年“秘密线上搜查案”中提出从一般人格权中导出“有关保障 IT 系统之秘密性不可侵犯的基本权利”,②以解决在 IT 系统中大规模搜集个人信息或者监控 IT 系统而脱离资讯自决权保障范围之问题。《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,但是未在大数据侦查中得到确证,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。

第三,保障删除权、更正权、救济权等权利实现。大数据侦查对信息主体个人权益的侵害具有隐蔽性和非即时性的特征,侵害行为的发生一般不为信息主体所知悉,多在事后继续存在且对信息主体产生深远影响。即使大数据侦查中处理个人信息无需经过公民个人同意,但是也应保障公民个人能够在个人信息不完整、不准确时行使删除权、更正权、救济权等权利,删除或者更正个人信息,甚至请求侦查机关对违规违法处理个人信息侵害个人权益的行为承担相应赔偿或补偿责任。

(二)重塑强制性措施体系

尽管《刑事诉讼法》规定的搜查、技术侦查,《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》(简称《电子数据规定》)和《公安机关办理刑事案件电子数据取证规则》列明的通过扣押、封存原始存储介质,现场提取电子数据,网络在线提取电子数据,冻结电子数据,调取电子数据等手段措施与大数据侦查在收集电子数据方面类似,但是在分析数据、挖掘数据、分析关系等方面存在本质区别。现行法律规定的数据收集措施仍然偏向人工化、低阶化,处理的数据、个人信息的量是样本级的,而大数据侦查依托算法,在高算力的加持下,于海量的数据中挖掘信息,将潜在的关系显性化,因而对个人权益的干预程度,是传统电子数据收集手段无法比拟的,理应视之为强制性措施。可以以修改《刑事诉讼法》为契机,将查封、扣押、冻结从侦查中抽离出来,规定为对物强制措施,设定对个人信息、隐私权干预的强制性措施,将大数据侦查作为独立的侦查措施纳入其中。

(三)强化个人信息处理监管

第一,司法审查。司法审查具有两个面向,一是实施令状主义,由司法官对个人信息收集调取签发令状,比如美国规定进入电脑资料库查阅资料,必须由司法官签发搜查令。二是法院行使宪法解释权,比如德国的 IT 系统基本权之确立是由德国宪法法院通过判决的方式扩展宪法权利。遗憾的是,中国并未实施令状主义,除逮捕之外几乎所有的侦查措施皆以行政化方式运行。虽然确立了非法证据排除规则,但是法院重点排除刑讯逼供等非法言词证据。依据《电子数据规定》的规定,法院审查电子数据时重点审查取证是否符合技术标准、手续是否完备等事项,并未将电子数据取证作为重点。权宜之计是将大数据侦查纳入庭审质证之中,依附于质证程序进行司法审查,并以发布指导性案例的方式普遍性地以司法权制约侦查权。

第二,侦查机关内部监管。在传统侦查中,侦查机关以物理性权力调阅个人信息,比如实施查询、检索等措施时一般由县级以上公安机关负责人批准。大数据侦查相较于传统侦查措施而言处于内部零监管状态。从既有经验而言,侦查机关内部实行的行政首长审批和法制审核发挥了重要作用,可以在大数据侦查中沿用此制度。对于确有必要实施大数据侦查的情形,由县级以上公安机关负责人审批,法制科审核,办案部门负责人把关。同时,大数据侦查涉及的各个业务部门在分工负责的同时应该互相制约;上级部门应加大对下级部门的监管力度。

第三,专门监管。设置专门机构加强个人信息保护是目前较为普遍的做法,比如英国建立了信息专员机制,由信息专员监督国家机构收集个人信息的行为。中国成立了中央网络和信息化领导小组,国家互联网信息办公室,负责信息安全管理,但是对于大数据侦查监管鞭长莫及。可以借鉴域外的做法,设置专司个人信

---

① 参见沈定成、凤立成:《警察有权搜查公众手机信息吗?——莱利诉加利福尼亚州案》,载《苏州大学学报(法学版)》2017 年第 1 期,第 137-151 页。

② 参见伯阳、刘志军:《一般人格权之具体体现:新创设的保障 IT 系统私密性和完整性的基本权利——联邦宪法法院对“在线搜查”作出的判决》,载南京大学-哥廷根大学中德法学研究所编:《中德法学论坛》(第 6 辑),南京大学出版社 2008 年版,第 33-50 页。

息保护专项职责的机构,专门受理对侦查机关等公权力机关不当处理个人信息的申诉、检举、控告。

第四,大数据侦查监督。传统依附于审查批捕的侦查监督于大数据侦查规制力有不逮:一方面,大数据侦查游离于法定的侦查措施之外,非检察机关侦查监督内容;另一方面,大数据侦查使用情况不会写入案卷之中,检察机关无法知悉侦查机关实施了大数据侦查,也难以发现大数据侦查违法行为。可以大数据赋能检察机关侦查监督,利用大数据技术对大数据侦查使用的算法以及手段实施情况进行全景式审查。①

(四)完善大数据侦查规则

一是明确适用范围。相较于技术侦查而言,大数据侦查使用的方式不局限于记录、行踪、通信、场所监控,适用的技术手段除了通信监听、信件拦截检查、密拍密录之外,还有数据分析、抓取等,这些手段也可能对公民个人权益造成更为重大的影响。按理而言,大数据侦查的适用范围应小于技术侦查。大数据时代,严格限制大数据侦查的适用不利于打击犯罪。可以比照技术侦查适用范围,确定大数据侦查适用于危害国家安全犯罪,恐怖活动犯罪,黑社会性质的组织犯罪,重大毒品犯罪,利用电信、计算机网络、寄递渠道等实施的重大犯罪案件,以及针对计算机网络实施的重大犯罪等案件。同时,贯彻比例原则,将大数据侦查作为兜底性措施,明确其在其他案件中的适用范围。②

二是明确启动标准。在德国前置侦查中,侦查程序启动标准是有事实证明存在"初期怀疑"。③ 大数据侦查作为主动型侦查,可将"初期怀疑"作为其启动节点,否则,"无异乎侦查员个人主观故意,而缺乏客观性……应以侦查机关知有犯罪嫌疑的客观情况时,侦查程序方为开始进行。"④

三是建立健全实施程序。依托传统侦查措施及技术侦查措施程序无法有效保障大数据侦查规范运行,因此亟须建立体系化的大数据侦查实施程序。首先,构建大数据侦查启动程序,合理配置启动发起权、启动审核权和启动决定权等,根据个人信息类型、主体,结合案件类型及办案情况设置不同的启动程序,紧急情况下,简化启动程序。其次,建立健全告知程序。大数据侦查属于强制性措施,原则上应该设置告知程序。"可以探索建立事后向社会公示、定期向专门机关报告及披露等制度,或与其他商业组织合作并采用隐私政策嵌入等方式达到事前告知的效果。"⑤再次,建立释明程序。大数据侦查存在"算法黑箱",公民个人对于侵害个人权益的行为可以申诉、控告、检举,侦查机关应该在保障个人信息及隐私、商业秘密、国家机密、技术方法安全的情况下向当事人解释说明适用大数据侦查的依据、获取个人信息情况及算法原理等事项。

五、结语

在侦查中运用大数据技术应对犯罪新情势是大势所趋,符合人类发展和犯罪治理规律。大数据侦查虽然具有侵犯公民个人权益的风险,但是规范其适用,限制其处理个人信息或者减少对公民权利的干预,符合当下人权保障趋势,充分体现了对个人权益的重视。因而,大数据侦查之于犯罪治理的内在需求使个人信息处理行为具备正当性,而个人信息权益受保障,公权力适度干预私权利的法逻辑限定了大数据侦查的边界。只有兼顾二者,大数据侦查才具备正当性和合理性。

个人信息利用与保护兼顾的最核心要义是实现个人信息附着利益的动态平衡,⑥强调"在合理范围内处理"归根结底是实现个人信息利益的正义分配。既然正义昭示着平等地分配包括个人信息在内的资源,那么在利用具有公共属性的资源时必须节制有度而不侵犯其他主体利益。由此产生保护个人信息权益和限制大数据侦查权力的两个面向。未在合理范围内处理个人信息既是大数据侦查权运行失范的表现,也是个人信息保护和利用失衡的指征。纠偏个人信息保护和利用失衡的逻辑就在于采取有效的保障权利和限制权力的措施规制大数据侦查,进而规范个人信息处理行为,从而改变轻个人信息保护重个人信息利用的现状。

---

① 参见李小猛:《大数据赋能侦查监督的进路与反思》,载《华东政法大学学报》2023年第5期,第32-44页。
② 参见钱程:《个人信息刑事调取的适用限度与法律规制》,载《中国海商法研究》2024年第2期,第95页。
③ 参见[德]克劳思·罗科信:《刑事诉讼法》,吴丽琪译,法律出版社2003年版,第35页。
④ 何赖杰、林钰雄等:《刑事诉讼法实例研习》,学林文化事业公司2000年版,第309页。
⑤ 陈刚:《解释与规制:程序法定主义下的大数据侦查》,载《法学杂志》2020年第12期,第13页。
⑥ 参见赵祖斌:《从静态到动态:场景理论下的个人信息保护》,载《科学与社会》2021年第4期,第113页。

Processing Within a Reasonable Scope: Balance Between the Protection and Utilization of Personal Information in Big Data Investigation

ZHAO Zubin

(School of Criminal Justice, Zhongnan University of Economics and Law, Wuhan 430072, China)

Abstract: In the digital-transformation era, big data has rendered personal information a vital nexus of multiple interests. Consequently, the protection and utilization of personal information have become fundamental principles in legislation and related practices, especially in criminal investigation. Big data investigation helps provide law enforcement with new means to enhance crime-solving efficiency. For example, analyzing large-scale data can quickly reveal previously hidden patterns. However, it also disrupts the balance between the protection and utilization of personal information. In practice, over-emphasis on using personal information for investigation while neglecting its protection has led to several problems. Excessive collection of personal information is a common issue. Law enforcement often gathers more data than necessary for a case, such as an individual's entire digital footprint including browsing history, shopping habits, and communication records. This violates the data-minimization principle and increases privacy risks. For instance, in an ordinary criminal case, data from multiple digital platforms like e-commerce sites and online communication apps may be collected without a clear link to the crime. The generalization of processing purposes is also concerning. The reasons for processing personal information are no longer strictly tied to specific investigative goals. Information collected for one case can be misused for another case without proper authorization, undermining public trust in law enforcement and weakening the legal and ethical framework. Distorted use of personal information is another obstacle. Data can be manipulated through cherry-picking, misinterpreting statistical analyses, or due to algorithmic biases. In predictive-policing cases, flawed algorithms can unjustly target certain individuals or communities, resulting in discriminatory outcomes. Overly long storage of personal information is risky. It not only increases the vulnerability to data breaches as cyber-threats constantly evolving, but also violates the data retention limitation principle. The longer the data is stored, the more likely it is to be compromised, endangering individuals' privacy and security. The key solution is processing personal information within a reasonable scope. This means the processing should be legitimate, directly related to crime detection, prevention, or prosecution. It also requires standardization, with clear procedures covering data collection, storage, analysis, and disposal to ensure data accuracy, integrity, and security. Moreover, the impact on personal rights should be reasonable, and less-intrusive methods should be explored first. The principle of "processing within a reasonable scope" balances the protection and utilization of personal information, restricts the data-handling power of investigative organs, and safeguards digital human rights, including the right to privacy, data control, and fair data processing. To ensure investigative organs operate within this scope, multiple measures are needed. First, improve the personal information protection system, review and update existing laws considering new data types like biometric data and AI-generated data, and formulate new legislation. Second, reshape the compulsory-measures system, and for digital searches, law enforcement should obtain a warrant clearly defining the search scope, data types, purpose, and privacy safeguards. Third, strengthen supervision, establish an independent body to audit, inspect, and investigate law enforcement agencies, impose sanctions on non-compliant ones, and provide a complaint-handling platform. Finally, refine the rule system for big data investigation, covering data quality control, third-party data use, security, and ethical analysis.

Key words: big data investigation; protection of personal information; utilization of personal information; reasonable processing