个人信息刑事调取的适用限度与法律规制

钱 程

（大连海事大学 法学院，辽宁 大连 116026）

摘要：数字时代，侦查机关依托数字信息技术增强数据收集处理能力，提升案件侦破效能。但是，侦查机关泛用刑事调取措施向网络信息企业调取公民个人信息，存在损害公民隐私权、个人信息权且过度干预企业合法经营的风险。在侦查机关适用信息调取措施的过程中，应当遵循限度理念，即以程序法定原则与比例原则归正侦查机关信息调取的必要限度，以公民个人信息权利与网络信息企业合法权益为信息刑事调取划定适用边界。强化侦查机关个人信息调取措施的法律规制具体从以下方面进行：其一，完善个人信息刑事调取的程序规范机制，按照任意性侦查措施与强制性侦查措施两种属性分别进行法律授权与程序规制，对现有刑事诉讼规范内容予以“信息化”调适，强化对侦查权的法律控制。其二，构建刑事诉讼中公民个人信息保护机制，保障信息主体通过行使信息知情权、信息访问权、信息更正删除权等权利直接、积极地进行个人信息保护。其三，优化企业配合刑事执法的权益保护机制，细化企业协助刑事执法义务，建立企业义务豁免机制，调和执法协助义务与数据合规义务的冲突；赋予作为第三方信息控制者的企业必要的权利，使企业能够以积极方式维护自身的合法权益。

关键词：刑事调取；个人信息权；隐私权；强制性措施；法律规制

中图分类号：D925.2 **文献标志码**：A **文章编号**：2096-028X(2024)02-0091-12

一、问题的提出

数字时代，海量的公民个人信息处于公共职能机构以及网络信息企业等第三方控制之下，调取信息数据已成为侦查机关重要的取证方式。从个人信息处理角度分析，个人信息刑事调取的过程存在“侦查机关—个人信息控制者—个人信息主体”的三方结构，侦查机关绕过公民个人信息主体，对作为刑事诉讼第三方的信息控制者采取调取措施以实现信息收集。侦查机关调取的个人信息呈现体量庞大、类型众多的特点，既包括一般信息，也存在隐私信息。在大数据技术助力下，侦查机关进行信息挖掘、整合，能够对信息主体形成更全面、具体的数字人格认知与社会活动轨迹再现，以寻找案件线索与证据。实践中侦查机关通过信息调取措施广泛获取实时视频信息、电子通讯信息以及行动轨迹信息，显著提升案件侦破能力与办案效率。如2020年包头警方通过调取基站数据和公路卡口视频信息侦破大型诈骗犯罪，共捣毁犯罪团伙8个，抓获团伙成员15名，核查串并案件48起，涉案价值259万余元。①

但是，侦查机关在获享信息调取措施提升办案效能红利的同时，也诱发信息调取措施不当适用侵犯信息主体权利和信息处理者权益的隐患。中国刑事诉讼法律规范整体上生成于传统的、物理性质的社会环境，而非数字化、信息化环境，现行程序法内容对数字技术带来的冲击尚未进行有效的制度反应。② 目前中国的刑事诉讼法律规范中，信息调取措施内容呈现授权色彩，整体规范密度较低，未对侦查机关信息调取权进行严格的程序控制。《最高人民法院、最高人民检察院、公安部关于办理信息网络犯罪案件适用刑事诉讼程序若干问题的意见》（简称《办理信息网络犯罪案件刑事程序意见》）明确将公安机关向网络服务提供者调取电子

收稿日期：2024-03-05

基金项目：2024年度中央高校基本科研业务费专项资金资助项目“个人信息刑事调取的适用限度与法律规制”（3132024317）

作者简介：钱程，女，法学博士，大连海事大学法学院讲师。

① 参见《每天呼出6万个诈骗电话！8个犯罪团伙被捣毁》，载澎湃网2021年1月24日，https://m.thepaper.cn/baijiahao_10923628。

② 参见钱程：《刑事诉讼中个人信息保护研究》，中国政法大学2023年博士学位论文，第119页。

数据的行为作为信息网络犯罪案件的取证手段予以规定,并对公安机关在刑事侦查中调取个人信息的措施进行初步程序规范,但对于侦查措施法律属性的界定仍不明晰,对侦查机关信息调取权的程序控制仍显不足。在规则便利与技术便利的助推下,侦查机关以调取之名广泛获取第三方尤其是互联网企业控制的公民信息,[①]存在侦查机关滥用信息调取权、不当限制公民个人信息权和网络信息企业权益的隐患。一方面,制度层面调取措施发动条件较低,无明确的程序限制,侦查机关基于执法便利倾向于以此方式获取第三方控制的信息数据,且为全面获取信息,侦查机关往往以"整体打包"方式调取信息,致使大量与案件无关的公民个人信息被调取。如"顺亨汽贸公司走私普通货物案"中,侦查机关向网络服务商调取30个涉案邮箱中的20万封电子邮件,但这些邮件并非均与案件具有关联性。侦查机关的"打包式"调取导致信息实际调取范围远超案件侦查所需的应调取范围,电子邮件所承载的公民通信自由和通信秘密权、隐私权等基本权利被不当干预。[②] 另外,实践中存在侦查机关以调取之名长时间、持续性获取公民实时位置信息的做法,此行为属于以持续性、秘密性、实时性方式获取相对人的信息,对公民隐私领域存在干预的可能性,行为属性当属技术侦查措施。侦查机关以刑事调取为名行技术侦查之实,得以规避技术侦查措施严格的适用条件与审批程序。其后,所获取的信息材料也无需按照技术侦查措施的相关要求进行删除销毁。信息调取措施在制度层面的模糊处遇使得侦查机关以不合比例的方式干预公民个人信息权与隐私权,但信息主体对此不知情,权利保障问题因权利被隐秘干预的事实而淡化。[③] 另一方面,侦查机关大量且持续增加的信息调取行为会加重第三方信息控制者履行配合侦查义务的成本,且企业并不因履行配合侦查义务而被免除数据合规义务,依然要承担未经信息主体同意披露个人信息的责任,以及用户信任丧失造成的经济利益损失。网络信息企业处于配合侦查义务与履行数据合规义务的矛盾中,往往对配合调取持模糊甚至消极态度,"滴滴顺风车司机杀人案"中滴滴公司未及时提供信息以及"美国圣贝纳迪诺枪击案"中苹果公司拒绝提供枪击案袭击者手机的破解技术即是典型例证。

基于此,有必要对刑事诉讼中侦查机关调取公民个人信息的相关问题予以解决:刑事程序中公安机关针对企业调取信息的行为属性为何,其适用的边界性何在?如何有效规制侦查机关信息调取行为以平衡打击犯罪、维护社会安全与保护个人信息、维护企业权益之间的关系?笔者对个人信息刑事调取行为的法律属性进行分析,并从侦查机关权力运行、公民个人信息权利保护、网络信息类企业权益保护三个维度讨论此措施适用的必要限度,在此基础上探索个人信息刑事调取的法律规制路径。

二、个人信息刑事调取的法律属性之辨

侦查机关调取数据行为在刑事诉讼法中的属性尚不明确,存在任意性侦查措施、强制性侦查措施,以及依目标信息数据的类型及其承载公民权益判断调取属性等多种观点论争。个人信息刑事调取的法律属性直接影响权力配置、适用程序方面的制度设置,应先行解决个人信息刑事调取措施属性这一基础问题。

(一)制度层面个人信息调取的法律属性不明

在刑事程序规范层面,现有司法解释和部门规章对侦查机关调取数据信息的法律属性界定存在些许矛盾,导致信息调取措施法律处遇不明,程序控制方式模糊。《中华人民共和国刑事诉讼法》(简称《刑事诉讼法》)第54条对公安机关向有关单位和个人收集、调取证据进行概括性授权,电子数据隶属法定证据种类,此授权条款应当包括信息数据类证据形式。但是,《刑事诉讼法》未具体阐述调取的适用程序,难以判断调取措施的法律属性为强制性侦查措施抑或任意性侦查措施。《人民检察院刑事诉讼规则》(2019年)第169条、《公安机关办理刑事案件程序规定》(2020年修正)第174条、《办理信息网络犯罪案件刑事程序意见》第12条将调取作为不限制被调查对象人身、财产权利的措施进行列举,可见,这三个规范将刑事调取界定为任意性侦查措施。但是,《公安机关办理刑事案件电子数据取证规则》第41条、《中华人民共和国数据安全

① 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》,载《法律科学(西北政法大学学报)》2021年第3期,第82-83页。

② 参见谢登科:《论侦查机关电子数据调取权及其程序控制——以〈数据安全法(草案)〉》第32条为视角》,载《环球法律评论》2021年第1期,第60页。

③ 参见张建伟:《司法的科技应用:两个维度的观察与分析》,载《浙江工商大学学报》2021年第5期,第49页。

法》(简称《数据安全法》)第 35 条均规定调取数据应当经过审批手续。《数据安全法》所要求的“经过严格的批准手续”这一审批要件与技术侦查措施的审批程序措辞一致,且“经过严格的批准手续”这一表述在《刑事诉讼法》中仅用于技术侦查措施,故而引发调取措施是否与技术侦查措施属性同为强制性侦查措施的疑问。① 鉴于《数据安全法》未对数据调取措施的审批主体、适用程序进行更具体的设置,难以判断数据调取措施与技术侦查措施的具体适用程序是否相同。刑事调取措施在制度层面的属性尚不明确,侦查机关往往将其作为任意性侦查措施适用。相较于强制性侦查措施,信息调取措施具有明显的执法便利,即发动的法律门槛低,程序要件宽松,但调取的信息类型多样、信息量级庞大,调取方式简单、操作不繁琐。为规避强制性侦查措施严格的程序适用要件,实践中存在侦查机关以信息调取措施代替技术侦查措施的做法,即侦查机关向第三方信息控制者调取信息主体实时性、动态性信息,而不适用以“实时监控”为代表的技术侦查措施,以规避技术侦查措施严格的适用条件和审批程序。②

(二)个人信息刑事调取措施的法律属性界定

在界定个人信息调取措施法律属性之前,需要明确此措施具有以下特点。第一,在个人信息处理流程中,侦查机关调取个人信息的行为属于信息收集行为,而非侦查机关应用大数据技术进行信息查询等信息分析行为。第二,侦查机关调取个人信息为间接信息收集方式,适用于作为个人信息控制者、个人信息处理者的刑事诉讼中的第三方,而非适用于个人信息主体本身。侦查机关调取的范围限于处于第三方控制下的静态、已经生成的信息,持续性、实时性的动态信息收集属于技术侦查措施,而非信息调取措施。第三,个人信息调取措施与查封、扣押措施不同。在多数信息调取的场景中,第三方均需履行配合侦查的法定义务,应提供信息并予以必要的技术支持。若第三方拒绝配合,侦查机关一般通过查封、扣押措施控制数据载体,进而实现信息的强制获取。此情形并不需要对信息调取措施法律属性进行界定,查封、扣押本身均属于强制性侦查措施。此处所讨论的法律属性存疑的个人信息刑事调取措施为第三方同意调取并予以配合情况下,侦查机关的个人信息收集行为是否为强制侦查措施。

侦查措施属性界分不以行使直接强制的有形力作为标准,而是以侵害被处分者基本权利作为标准,③一旦对人民基本权的行使产生部分或全部的影响,便属基本权之干预,④此侦查措施即为强制性侦查措施。中国未形成德国基本权利干预的三步式判断标准,侦查措施属性判断相对困难,个人信息调取措施以隐私权、个人信息权作为干预对象,其法律属性判断更加复杂。在判断调取信息类型的基础上,还需结合信息关联性、信息量级及信息主体是否放弃权利等因素进行综合判断。⑤ 个人信息刑事调取措施属性判断需要进行以下两重因素分析。

1.判断侦查机关调取信息的类型和量级

根据侦查机关调取的个人信息类型进行判断,以隐私性作为界分标准,将调取信息分为一般信息与隐私信息。隐私权是公民基本权利,应保护公民的私人领域免受公权力机关无端干涉。隐私的本质即蕴含对公共领域和私人领域的界分,在有效界定公私领域的基础上,将公权力行使限定在私人领域之外,以隐私权抵御公权力的无端侵入。基于隐私权权利主体“不欲为他人知晓”的内在诉求,当侦查权侵入个人隐私时,必然带有强制性,以此得以解释缘何侦查机关对公民私人空间进行的搜查被视为强制性侦查措施,而对公共空间进行的勘验被视为任意性侦查措施。⑥ 故而,当侦查机关调取的信息类型为公民一般信息时,信息调取措施为任意性侦查措施;当侦查机关调取的信息类型为公民隐私信息时,此措施因干预公民基本权利,当属强制性侦查措施。对于隐私信息的判断,从对泄露该信息是否会给信息主体带来权利损害、社会大多数人对某类信息的敏感度等因素综合判断信息的隐私程度。⑦ 有实证研究将中国公民敏感隐私信息列为“通话记录、

① 参见王仲羊:《调取电子数据的三重维度与优化路径》,载《北京航空航天大学学报(社会科学版)》2023 年第 1 期,第 66-68 页。

② 参见吴桐:《科技定位侦查的制度挑战与法律规制——以日本 GPS 侦查案为例的研究》,载《中国刑事法杂志》2020 年第 6 期,第 83 页。

③ 参见[日]田口守一:《刑事诉讼法》(第 7 版),张凌、于秀峰译,法律出版社 2019 年版,第 54-55 页。

④ 参见林钰雄:《干预保留与门槛理论——司法警察(官)一般调查权限之理论检讨》,载《政大法学评论》2007 年第 96 期,第 199 页。

⑤ 参见何军:《数据侦查行为的法律性质及规制路径研究》,载《中国人民公安大学学报(社会科学版)》2021 年第 1 期,第 78 页。

⑥ 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》,载《法律科学(西北政法大学学报)》2021 年第 3 期,第 90-91 页。

⑦ 参见胡文涛:《我国个人敏感信息界定之构想》,载《中国法学》2018 年第 5 期,第 235 页。

私人信件、私人生活空间、私人照片和录像、性取向和性生活、医疗记录、财务信息、身份证号码等12项内容”。[①] 除了已列举的典型的隐私信息,还存在大量公民个人信息游走于一般信息与隐私信息之间,无法单项、直接地判断其信息类型,难以判断侦查机关对此类信息的收集处理是否会干预公民隐私权与个人信息权。对于此类信息,往往需要结合信息处理者所处理的信息量级以及各种信息之间的关系综合判断。

美国对侦查机关运用GPS和视频监控设备收集公民位置信息、行动轨迹信息,运用手机通联信息记录调取公民通讯信息等措施均以是否侵害公民隐私合理期待的标准进行分析,[②]结合侦查措施干预公民个人信息的隐私程度与信息数量两个因素综合判断是否将干预行为纳入美国《宪法第四修正案》的保护范畴。[③]如果侦查机关干预的信息数量和信息含量是大量的、显著的,则措施侵害性较强,一般认为此种措施侵犯隐私合理期待,将此措施界定为搜查行为。[④] 欲启动搜查程序需要事先申请令状,治安法官审查警察所提供的证据材料,认为符合“可能理由”标准方能颁发搜查令。若侦查机关收集的信息不具有隐私合理期待,则信息收集行为不以搜查程序进行规制,程序启动要求较低,即具备合理怀疑,法院即可颁发法院令。[⑤] 可见,美国通过公民个人信息的隐私程度与侦查机关收集的信息数量两个因素判断相应信息收集行为是否应纳入美国《宪法第四修正案》的保护范畴。此判断的依据为马赛克理论,即单个数据点是单一的瓦片,从其自身角度看似乎并无意义,但当与其他数据点结合时,会呈现一个宽广、全面的图像,就像许多瓷砖组合在一起创建的马赛克图案。[⑥] 2012年“*United States v. Jones* 案”中,美国联邦巡回上诉法院即运用马赛克理论阐释侦查机关GPS追踪行为缘何构成搜查行为,其提出,侦查机关连续28天运用GPS追踪器监控犯罪嫌疑人行动轨迹,通过持续性地获取特定主体位置信息、行动轨迹可以完整描绘个人活动,揭露其个人隐私。美国联邦最高法院认为,侦查机关的长期秘密监控侵犯了公民对隐私的合理期待,构成美国《宪法第四修正案》意义上的搜查。[⑦] 在信息技术时代,国家公权力机关收集信息如同设置马赛克图案一般,成千上万看似平常无害的信息经过分析、设置、整合后,可以呈现前所未见的整体面貌。[⑧] 公民个人对于单一的、零碎的信息或许主观上并没有遭受侵害之感受,但大量的信息累积、聚合能够拼凑出公民的隐私信息,[⑨]公权力机关广泛的信息收集与深度处理存在随时侵入并干预公民隐私领域的风险。[⑩]

鉴于侦查机关调取个人信息的量级、信息之间的关系会影响对调取措施属性的判断,在对信息调取措施属性进行分析时,应当将这两种重要影响因素纳入考量范畴,即结合调取公民信息类型、调取信息的量级、信息之间的关系三重因素综合判断信息调取措施的法律属性。当侦查机关调取的信息为公民隐私信息时,调取措施为强制性侦查措施,当侦查机关调取的信息为公民一般信息时,调取措施为任意性侦查措施;当侦查机关调取的信息难以直接判断为隐私信息,但所涉信息种类众多、信息量级较大、信息间关联性强,通过信息挖掘、整合能够拼凑出隐私信息时,信息调取措施当属强制性侦查措施。

2.判断信息主体是否同意采取调取措施

根据调取信息类型、调取信息量级等因素并不能绝对性地得出个人信息调取措施的法律属性,如果信息主体同意调取,则存在属性转变的可能,即如果信息主体同意侦查机关从第三方调取其个人信息,即便调取的信息为隐私信息或调取的信息类型、量级足以整合成隐私信息,此信息调取措施仍为任意性侦查措施。在刑事侦查理论中,强制性侦查措施与任意性侦查措施以侦查机关干预行为是否未经侦查措施相对人同意即是否实质上侵害或者威胁相对人基本权利为区分标准,强制性侦查措施需具备未经相对人同意并实质干预其基本权利两个要素。权利人放弃权利会对侦查措施属性产生影响,即强制性侦查措施因权利人放弃权利

① 参见吴标兵、许和隆、张宇:《中国公众隐私敏感度实证研究》,载《南京邮电大学学报(社会科学版)》2015年第3期,第82-90页。

② *United States v. Jones*,565 U.S. 400(2012).

③ Paul Ohm,*The Many Revolutions of Carpenter*,Harvard Journal of Law & Technology,Vol.32:357,p.362-363(2019).

④ Renée McDonald Hutchins,*Tied up in Knotts? GPS Technology and the Fourth Amendment*,UCLA Law Review,Vol.55:409,p.409-466(2007).

⑤ 参见田芳:《技术侦查中个人信息保护的法理研究》,法律出版社2021年版,第246-248页。

⑥ Robert Fairbanks,*Masterpiece or Mess:The Mosaic Theory of the Fourth Amendment Post-Carpenter*,Berkeley Journal of Criminal Law,Vol.26:1,p.73-75(2021).

⑦ *United States v. Jones*,132 S.Ct.955(2012).

⑧ *Halkin v. Helms*,598 F.2d 1(D.C.Cir.1978).

⑨ 参见王正嘉:《使用GPS定位之隐私秘密无故侵害》,载《月旦法学教室》2020年第199期,第26页。

⑩ *Osborn v. United States*,385 U.S. at 343(Douglas,J.,Dissenting.)

而不具有强制干预性,转化为任意性侦查措施。但是这种权利放弃必须是侦查措施相对人在熟知权利的内容和放弃的后果的情形下作出,而非不知情下的默示弃权。① 这一点在搜查制度中可以得到佐证,若相对人同意侦查机关进行搜查,则侦查措施为任意性侦查措施,无需搜查证即可进行;若无相对人同意,侦查机关经批准或依职权进行搜查,则属于适用强制性侦查措施。② 但是,作为第三方的信息控制者无权代表信息主体放弃其个人信息所承载的基本权利,信息主体与信息控制者达成的信息处理合意仅限于授权信息控制者处理其个人信息,而非信息主体放弃信息自决权,允许信息控制者代行此权利。故而,侦查机关适用信息调取措施时,第三方信息控制者同意并配合调取并不意味着调取措施为任意性侦查措施,但是若获得信息主体同意,调取措施即为任意性侦查措施。

三、个人信息刑事调取适用的三重限度

侦查机关适用个人信息刑事调取措施需遵循“限度思维”。③ 具体而言,存在三重限度,其一为权力之限,即以程序法定原则与比例原则对侦查权的运行进行限制;其二为权利之限,即以公民权利为侦查机关信息调取行为设定限度,不得过度干预公民隐私权与个人信息权;其三为权益之限,即以网络信息企业权益为侦查机关信息调取行为设定限度,不得对企业科以过重的配合义务。

(一)个人信息刑事调取适用的权力之限

侦查机关适用个人信息刑事调取措施的第一重限度为权力之限,即侦查机关权力行使应当遵循程序法定原则与比例原则,侦查权应当在必要限度内以合法、合比例的方式运行。

1.侦查机关适用个人信息刑事调取措施应当遵守程序法定原则

刑事程序法定原则要求刑事诉讼中公权力干预公民个人基本权利必须具有合法的授权,干预行为应符合法律明定的程序要件,程序行为的后果具有明确性与必然性。④ 依据前文对个人信息刑事调取措施的属性分析,信息调取措施兼具任意性侦查措施与强制性侦查措施的属性,当调取对象为隐私信息且信息主体未弃权时,侦查机关进行信息调取为强制性调取;当第三方信息控制者拒绝配合调取,侦查机关通过查封、扣押信息载体方式实现信息获取时,也属强制性侦查措施。强制性侦查措施只有在符合法律规定的实体要件和程序要件的前提下才可以适用,目前刑事诉讼法缺乏对个人信息刑事调取措施的明确授权与程序规范,强制性信息调取措施缺乏明确的制度依据。适度限制侦查机关的信息调取权,应当以刑事程序法定原则为归正依据,以刑事诉讼法对侦查机关适用个人信息调取措施进行明确授权和程序规范,具体规定信息调取措施的程序适用范围、程序启动要件、程序审批主体和执行主体、程序监督与救济措施等多方面内容。⑤

2.侦查机关适用个人信息刑事调取措施应当遵守比例原则

侦查权的行使应当受到比例原则的限制,即在立法划定限度内合理、必要、妥当地运行,如此才能保证不过度干预公民权利,达到程序正确性要求。德国刑事司法实践中形成了较为成熟的比例原则审查经验,即法院主要结合案件中犯罪行为的严重程度、侦查措施的发动条件、侦查措施对公民权利的干预程度等多种因素进行综合判断,衡量侦查措施的适用是否符合比例原则。⑥ 以 1990 年“Nordrhein-Westfalen 邦电子搜索追缉案”为例,德国联邦宪法法院按照比例原则要求进行实质审查,认为警察机关运用电子搜寻追缉措施不具备“现时危险”,即损害事件并未发生或已经开始,也并无几乎确切之几率即将发生。⑦ 在缺乏具体危险的现实条件下,适用电子搜寻追缉措施对于公民基本权的干预程度与所欲达到的目的之间未形成合理、必要、适度的均衡关系,一定程度上干预措施的适用所造成的“受限制之利益”超过“受保证之利益”,不符合比例

① 参见宋英辉等:《刑事诉讼原理》(第 3 版),北京大学出版社 2014 年版,第 188-191 页。
② 参见孙长永:《侦查程序与人权——比较法考察》,中国方正出版社 2000 年版,第 93 页。
③ 参见李延舜:《个人信息刑事调取行为的法律规制》,载欧阳本祺主编:《东南法学》第 6 辑,东南大学出版社 2022 年,第 118 页。
④ 参见陈卫东、程雷:《刑事程序合法性原则论纲》,载《法律科学(西北政法学院学报)》2004 年第 1 期,第 91 页。
⑤ 参见卞建林、钱程:《大数据侦查的适用限度与程序规制》,载《贵州社会科学》2022 年第 3 期,第 82 页。
⑥ 参见艾明:《新型监控侦查措施法律规制研究》,法律出版社 2013 年版,第 89 页。
⑦ 参见“Nordrhein-Westfalen 邦警察法上之电子搜索追缉是否侵犯信息自决基本权”裁定,载《德国联邦宪法法院裁判选辑(十三)》,中国台湾地区司法机构印行 2011 年版,第 233 页。

原则。[①]

侦查机关适用个人信息调取措施应当遵守比例原则,具体包括以下三项要求。其一,侦查机关的个人信息调取行为应当符合适当性原则要求,即调取行为与调取目的之间的关系是适宜的、妥当的、可欲的。侦查机关信息调取行为涉及的个人信息范围不应超出干预行为欲实现的目的,即禁止不限范围、不限时限地收集、处理公民个人信息。应当限定侦查机关调取公民个人信息只能应用于刑事案件的犯罪侦查,不得用于一般行政执法活动与常态化维稳等用途。当侦查机关信息调取措施目的已经成就或丧失时,应当立即终止调取行为,并应采取信息封存、信息删除等措施防止此前的信息调取措施持续性干预信息主体的权利。[②] 其二,侦查机关的个人信息调取行为应当符合必要性原则要求,即在可达目的的多种干预手段中,个人信息调取措施应当是对相对人权利损害最小、干预强度最低的手段。[③] 若可通过调取非隐私信息或调取措施可以告知信息主体并获得其同意,则侦查机关应当尽可能采取干预程度低的任意性调取措施,而非强制性调取措施。必要性原则与个人信息保护原则中的目的限制原则一致,即侦查机关调取个人信息应基于刑事诉讼目的,并将调取行为的影响范围、影响程度尽可能限于可以实现处理目的的最小范围、最低程度,不得过度处理信息。[④] 其三,侦查机关的个人信息调取行为应当符合均衡性原则要求,即侦查机关信息调取措施所干预的公民基本权利与干预行为所保护的权益形成狭义比例关系,调取措施虽是达成目的所必要的,但是不可给予公民超过调取目的之价值的侵害。[⑤]

(二)个人信息刑事调取适用的权利之限

侦查机关适用个人信息调取措施的第二重限度为权利之限,即以公民隐私权与个人信息权为侦查机关的个人信息调取行为设定限度,规范个人信息调取措施的适用,防止其不当适用损害公民合法权利。

侦查机关适用个人信息调取措施存在不当干预公民权利的风险,表现为两个方面:其一,侦查机关过度调取公民个人信息存在全景式监控风险。目前侦查机关广泛适用信息调取措施,以秘密的、持续的、便利的、廉价的方式控制大量公民个人信息,通过对信息主体基本身份信息、生物识别信息、主要社会关系、就学就医信息、消费记录信息、高频行动轨迹等信息的分析处理能够轻易地、完整地描绘公民的数字人格,以无形方式侵入其隐私领域,对公民进行全景式监控。[⑥] “而且,相比私人对个人信息的非法侵扰,来自国家的不当干预更令人难以察觉,也更难予以抵御。”[⑦]公民个体与侦查机关的个人信息处理能力相差悬殊,信息主体往往并不知晓侦查机关实施了信息调取行为,导致信息主体很难判断风险是否发生、何时发生、缘何发生,更无从谈及主动抵御这种风险的发生。在泛监控环境中,公民对个人信息自主权、隐私安全缺乏控制力,信息主体个人自治、生活安宁、公正对待以及信息安全四项法益均受到威胁。其二,侦查机关不当调取公民个人信息存在埋藏刑事司法错误、侵害公民实体权利的风险。刑事司法容错率低,如若侦查机关调取的个人信息存在不准确、不完整问题,或者后续个人信息处理行为中存在技术性偏差问题,均可能引发公安司法机关就案件事实、证据作出错误判断。目前刑事程序中个人信息权缺位,如果侦查机关向第三方调取的信息存在错误或瑕疵,信息主体对调取行为及后续信息分析行为不知情,难以通过更正权进行信息修正、补充,则错误信息会进入后续刑事程序,可能影响最终裁判结果。刑事程序中因信息质量瑕疵导致无辜公民被错误抓捕的事例在执法实践中屡次出现,如佛山市公安局某派出所将李某身份信息错误登记,使其有了“吸毒前科”,警方未及时更正信息,导致李某在半年内被误抓5次。[⑧] 2007年至2010年媒体陆续曝光22起因个人信息录入错误而引起的网上通缉误认事件,[⑨]均是个人信息处理不当造成刑事诉讼程序适用错误的佐证。此问题在国外刑事司法实践中也曾出现,根据英国《每日电讯报》报道,英国犯罪记录管理局因工作失误将1 570名无辜公

① 参见黄清德:《科技定位追踪监视与基本人权保障》,元照出版公司2011年版,第277-278页。
② 参见裴炜:《刑事诉讼中的个人信息保护探讨——基于公民信息保护整体框架》,载《人民检察》2021年第14期,第10页。
③ 参见刘权:《论必要性原则的客观化》,载《中国法学》2016年第5期,第178页。
④ 参见卞建林、钱程:《刑事诉讼法与个人信息保护法的衔接》,载《国家检察官学院学报》2023年第6期,第150页。
⑤ 参见姜昕:《比例原则释义学结构构建及反思》,载《法律科学(西北政法大学学报)》2008年第5期,第47-48页。
⑥ Susan Freiwald & Stephen W. Smith, *The Carpenter Chronicle: A Near Perfect Surveillance*, Harvard Law Review, Vol. 132: 205, p. 209-221 (2018).
⑦ 赵宏:《从信息公开到信息保护:公法上信息权保护研究的风向流转与核心问题》,载《比较法研究》2017年第2期,第35页。
⑧ 参见《男子因派出所身份登记错误半年被误抓5次》,载法邦网2011年12月14日,https://www.fabao365.com/news/875956.html。
⑨ 参见王彦学:《论网上通缉误认》,载《中国人民公安大学学报(社会科学版)》2010年第6期,第91页。

民错误登记为罪犯,其中大量公民因错误的犯罪记录难以正常求职。①

以公民权利为侦查机关的个人信息调取行为设定限度的理由在于侦查机关适用信息调取措施会对信息主体个人信息权、隐私权形成限制,信息主体虽同意信息控制者按照合意处理其个人信息,但并未放弃个人信息所承载的基本权利。个人信息承载着自主、隐私等多重价值,信息主体认识到其同意信息处于第三方控制下存在风险,并不代表着信息主体必须承担风险,抑或是全然放弃其他的权利保障。② 事实上,信息主体与个人信息之间的联结在信息流动过程中并未被斩断,公民对刑事诉讼中第三方控制的信息依然保有合理的隐私期待。③ 侦查机关在向第三方调取公民个人信息的过程中,不能无视公民作为信息主体享有的权利,无限度干预其隐私权与个人信息权。以公民隐私权与个人信息权为侦查机关的个人信息调取行为设定限度,能够运用个人信息权全面、积极保护个人信息的优势,发挥《中华人民共和国个人信息保护法》中个人信息保护规则对侦查机关信息调取行为的规范作用,强化对侦查机关适用个人信息调取措施引发权利侵害的防范作用。“权利之限”作用的发挥通过“权利肯认—权利行使”路径来实现,即在宪法层面对公民个人信息权利予以肯认,以个人信息基本权利树立国家公权力信息处理者与公民信息主体之间的关系屏障,通过限制公安司法机关不当收集和使用个人信息,避免国家公权力大范围、高强度地介入私人生活和私人领域,防止国家在处理个人信息过程中侵害公民人格尊严与自由发展。相较于隐私权有限保护的特点,个人信息权对公民个人信息进行的是全面保护,信息主体能够以积极方式行使权利,防范侦查机关个人信息调取措施引发的侵害风险。信息主体通过对侦查机关从第三方调取的个人信息提出查询、异议、修改、删除,有助于保证侦查机关收集、使用个人信息的准确性。公民作为信息主体能够以积极方式对侦查机关调取其个人信息行为的合法性、合理性提出质疑,有助于规范侦查机关的信息调取行为,制约侦查权不当扩张。

(三)个人信息刑事调取适用的权益之限

侦查机关适用个人信息调取措施的第三重限度为权益之限。实践中大量信息控制者为网络信息企业,侦查机关适用信息调取措施对第三方信息控制者权益会形成限制。企业的经营权为侦查机关的信息调取措施又划定了一道边界,要求侦查机关合法且适当地适用信息调取措施,不得无视信息控制者的合法权益,过度限制甚至侵害了企业权益。

实践中,侦查机关适用信息调取措施对网络信息企业经营权形成的干预集中体现在以下三个方面。

其一,侦查机关数量众多且持续增加的信息调取行为导致信息控制者履行配合义务的成本升高,企业经营负担加重。以美国苹果公司为例,2013 年至 2022 年苹果公司收到的世界范围内调取设备信息、账户信息的请求在持续攀升,以设备信息为例:2013 年上半年世界范围内执法机关向苹果公司提出调取设备信息请求(含美国)共计 12 442 件,苹果公司提供 9 249 件,占比 74%;2022 年上半年世界范围内执法机关向苹果公司提出调取设备信息请求(含美国)共计 29 022 件,苹果公司提供 22 228 件,占比 77%。④ 执法机关提出请求数增加约 133.26%,苹果公司提供数增加约 140.33%,对于持续、高速攀升的信息提供请求,网络信息企业配合执法义务的成本也随之升高,产生了不小的经营压力。

其二,刑事执法权的强制性与法定义务履行的无条件性使得企业除配合侦查机关调取外几乎别无选择,但是,企业无条件、大规模交付用户个人信息易引发用户信任危机,造成用户流失。作为信息主体的用户,在授权网络信息企业控制并使用其个人信息时,往往并未预判其信息可能用于刑事侦查,也并不希望其个人信息进入刑事程序,这种不被期待的信息处理行为可能损害用户对企业的信任。用户因担心个人信息泄露,可能认为企业在配合侦查机关信息调取过程中未有效履行事前提醒义务、信息交付审查义务,从而拒绝企业继续提供信息技术服务,不再向企业交付个人信息。信息网络企业依托用户交付信息获取经济利益,若因用户信任危机造成用户流失,企业将难以维持并扩充用户规模,这将直接影响企业经济利益。2006 年,美国司法

---

① Christopher Hope & Whitehall, *Criminal Records Bureau Errors Lead to Hundreds Being Branded Criminals*, The Telegraph (2 August 2009), https://www.telegraph.co.uk/news/uknews/law-and-order/5962174/Criminal-Records-Bureau-errors-lead-to-hundreds-being-branded-criminals.html.

② Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, Berkeley Technology Law Journal, Vol.24:1199, p.1204 (2014).

③ 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 143 页。

④ *Transparency Report*, Apple, https://www.apple.com/legal/transparency.

部向谷歌发送传票,要求谷歌披露其用户近两个月的网络搜索记录,用以证明过滤软件无法有效限制儿童访问网络色情内容,但遭到谷歌拒绝,谷歌认为司法部调取用户搜索记录的要求可能会损害公众对谷歌的信任,并暴露其商业秘密,[①]失去用户信息的潜在风险对谷歌而言是一种负担。[②]

其三,企业向侦查机关交付用户个人信息,存在数据合规困境。信息主体与网络信息企业达成处理其个人信息的合意,企业负有保护权利人个人信息不被第三方任意处理的义务,此义务对内表现为公司行为的合规控制。[③] 目前法律法规并未将配合刑事侦查作为企业数据合规义务的免除事由,也未为企业履行两种义务设置协调机制,致使两种义务之间发生冲突。当企业优先履行配合侦查义务时,则陷入数据合规困境,用户因个人信息未得到保护主张企业承担相应责任,用户信心的丧失将直接造成企业经济利益受损。若企业优先保护用户个人信息,则违反法定配合侦查义务,且存在影响侦查、延误破案的严重后果。2018年"滴滴顺风车司机杀人案"即是典型例证,滴滴公司就该案发布的声明体现了企业在履行配合侦查义务中面临的数据合规困境:"就这次沉痛教训,我们恳请与警方以及社会各界探讨更高效可行的合作方案,共同打击犯罪,更好地保护用户的人身财产安全。我们也希望能听到社会各界的建议和经验,如何在保护用户隐私的同时,避免延误破案的时机。"[④]域外也出现过相似案件,在2008年的"*K.U. v. Finland* 案"中,芬兰国内法院与欧洲人权法院对于侦查机关能否以打击网络儿童色情犯罪案件为目的,强制网络信息业者披露用户身份信息存在不同观点。芬兰国内法院鉴于当时芬兰国内法禁止信息处理者未经信息主体同意向第三方披露个人信息,支持网络信息业者以保护用户隐私信息为由,拒绝侦查机关调取信息的要求。[⑤] 但是欧洲人权法院认为,网络用户的隐私权利并不是绝对的,此类保障有时必须服从于其他合法要求,例如防止骚乱或犯罪以及保护公民权利和自由,[⑥]并提出"立法者负有积极的义务协调彼此冲突的权利保护需求"。[⑦] 从网络信息业者角度分析,"立法者负有积极的义务"也包括在立法层面以明确规定解决网络信息业者在保护用户个人信息义务与配合刑事侦查义务方面的履行冲突,使网络信息企业从数据合规困境中解脱。

网络信息企业在参与塑造自由开放的数字生态环境、促进数字经济增长中扮演着重要角色,其合法权益不容忽视。对网络信息企业而言,义务的履行有先后,义务的履行也有限度。[⑧] 刑事诉讼中相关单位与个人负有配合侦查以及提供信息材料的义务,此义务的价值在于控制并惩罚犯罪,维护国家和社会的安全利益,此义务的履行具有优位性,但并非无履行边界。没有绝对的用户个人信息保护,也没有绝对的不受限制的公权力。刑事诉讼中第三方在履行法定配合侦查义务过程中,其自身合法权益也应当得到保护。在"信息主体—信息控制者—侦查机关"这一复合关系结构中,侦查机关对网络信息企业采取刑事调取措施,此措施干预企业合法权益,因此应以符合比例原则的方式进行,以最低程度干预信息控制者权益,且不得对网络信息企业科以过重的配合义务,以免影响企业正常经营。

四、个人信息刑事调取的法律规制路径

强化侦查机关个人信息调取措施的法律规制可从以下三方面进行,即完善个人信息刑事调取的程序规范机制,构建刑事诉讼中公民个人信息保护机制以及优化企业配合刑事执法的权益保护机制。

(一)完善个人信息刑事调取的程序规范机制

完善个人信息刑事调取的程序规范机制的总体思路为对现有刑事诉讼规范相关规定进行"信息化"调

---

① Yuki Noguchi, *Judge Says Google Must Hand Over Search Records*, The Washington Post (15 March 2006), https://www.washingtonpost.com/archive/business/2006/03/15/judge-says-google-must-hand-over-search-records-span-classbankheadfirm-ordered-to-comply-with-narrower-subpoenaspan/39bad66e-784b-4b69-a73f-85dc15507dda.

② *Gonzales v. Google*, Inc.234 F.R.D. 674, 683 (N.D.Cal.2006).

③ 参见王仲羊:《电子数据调取中企业合规义务的困境与应对》,载《中国社会科学报》2023年7月25日,第7版。

④ 《滴滴8月27日起在全国范围内下线顺风车业务》,载《浔阳晚报》2018年8月27日,第A14版。

⑤ *K.U. v. Finland*, ECtHR, application no. 2872/02.

⑥ Adam Bodnar & Dorota Pudzianowska, *Violation of the Right to Respect for Private and Family Life in the Case of K.U. v FINLAND*, Human Rights House Foundation (3 December 2008), https://humanrightshouse.org/articles/violation-of-the-right-to-respect-for-private-and-family-life-in-the-case-of-k-u-v-finland.

⑦ Laurens Lavrysen, *Protection by the Law: The Positive Obligation to Develop a Legal Framework to Adequately Protect ECHR Rights*, in Yves Haeck & Eva Brems eds., Human Rights and Civil Liberties in the 21st Century, Springer Netherlands, 2014, p.69.

⑧ 参见李延舜:《刑事数据调取中网络服务提供者的角色定位及关联义务》,载《法学》2023年第1期,第161页。

适，为个人信息刑事调取措施提供明确的法律授权，并按照任意性侦查措施与强制性侦查措施两种属性分别进行程序规范设计，在制度层面落实程序法定原则与比例原则，强化对侦查机关信息调取措施的法律规制。

其一，明确个人信息任意性调取措施的授权依据与程序规范。《刑事诉讼法》第 54 条第 1 款的规定属于概括性授权，能够为侦查机关采取任意性调取措施提供法律依据，但有必要进行规则细化，明确授权范围以及具体的程序适用规范。在“侦查机关—信息控制者—信息主体”的关系结构中，信息主体同意将信息交予信息控制者并非当然地意味着其放弃数据信息权利，但是调取措施的间接性使得信息主体对自身信息的控制力降低，且信息控制者一般会注明个人信息可能会为第三方所知悉的格式条款，信息主体在一定程度上存在对自身信息被信息控制者再度处理的预见性。当侦查机关信息调取的对象为公民一般信息，或信息主体同意侦查机关从信息控制者处调取其个人信息时，信息调取措施属于任意性侦查措施。《刑事诉讼法》第 54 条能够为侦查机关采取任意性调取措施提供授权依据，但是有必要明确规定：除非信息主体同意，否则调取信息范围限于一般信息，不得以概括性方式调取隐私信息。任意性调取措施的启动由侦查人员自行决定，以关联性作为信息调取范围的判断标准，制作调取通知书，注明需要调取的信息范围，将告知书送达信息控制者。启动任意性调取措施的判断标准较低，单纯要求侦查机关说明其所采取的干预措施有助于厘清犯罪事实的理由，达到关联性标准即可。当警察以特定人为对象而对其个人信息权、隐私权采取较为轻微的干预措施时，至少应达到关联性标准，说明所欲取得的个人信息或多或少有助于证明或否定犯罪事实，[①]这往往用于锁定或排除犯罪嫌疑人。

其二，构建个人信息强制性调取措施的授权依据与程序规范。《刑事诉讼法》第 54 条将刑事调取措施概括性界定为任意性侦查措施，当调取信息量级低、内容为一般信息的对象时，侦查机关调取措施的合法性基础尚可成立。[②] 当调取对象为高量级、隐私信息，且主体未弃权时，隶属强制性侦查措施的信息调取行为则缺乏正当性依据。根据刑事程序法定原则，侦查机关干预公民基本权利必须具有合法授权、干预行为应符合法律规定的程序要件，且《人民检察院刑事诉讼规则》《公安机关办理刑事案件程序规定》《公安机关办理刑事案件电子数据取证规则》等规范对于信息调取措施适用的差异规定也需要《刑事诉讼法》统一解决。故而，刑事诉讼法层面应明确信息调取措施为独立的侦查措施，对侦查机关启动强制性调取措施进行具体授权以及明确的程序设置。第一，明确隶属强制性侦查措施的个人信息调取行为需符合两个要件：其一，调取信息类型为隐私信息，即侦查机关调取的信息属于公民隐私信息，或调取信息的数量、关联程度达到足以拼凑出隐私信息的程度；其二，权利主体并未弃权，即信息主体并未同意第三方信息处理者将其控制的信息交付侦查机关，或信息主体对于侦查机关调取其个人信息并无知情可能。第二，明确侦查机关启动强制性调取措施的程序规定，以解决目前强制性调取措施发动门槛过低、在实践中被滥用的问题。具体而言，欲发动强制性信息调取措施，侦查机关应提出适用信息调取措施的书面申请，写明法律依据、被调取的第三方基本信息、所欲调取的信息类型与信息范围，并阐明特定事实连同依据该事实所作出的合理推论使其相信犯罪活动正在进行，以及其所欲获取的信息材料与特定事实之间存在合理推论关系。第三，确立检察机关对强制性调取措施的审批权，并保留侦查机关对强制性调取措施的紧急决定权。一方面，由检察机关对侦查机关启动强制性调取措施的申请进行审查，认为达到合理怀疑标准即可批准程序启动申请。鉴于法院审查这一理想化的司法令状的方式与中国当前强制性侦查措施权力分配的现实存在较大差异，目前考虑由检察机关对侦查机关发动强制调取措施进行审批，旨在发挥检察权制约侦查权的功能，防止侦查权运行缺乏程序控制、侦查机关恣意启动强制调取措施，造成对相对人权利的侵害。[③] 另一方面，为防止错过案件最佳侦破时间，在规定检察机关审批权的同时，保留侦查机关的相对决定权，即在紧急且必要的情况下，侦查机关有权自行决定向第三方强制调取信息数据。

其三，有效衔接信息调取措施与查封、扣押措施的关系。若第三方信息控制者拒绝配合信息调取措施，

① 参见黄政龙：《美国行动电话定位追踪法规范研究》，载《警大法学论集》2010 年第 18 期，第 206-207 页。

② 参见刘文琦：《冲突与弥合：个人信息刑事调取的数字转型与法律因应》，载中国知网 2024 年 3 月 6 日，http://kns.cnki.net/kcms/detail/62.1015.C.20240304.1346.002.html。

③ 参见贝金欣、谢澍：《司法机关调取互联网企业数据之利益衡量与类型化路径》，载《国家检察官学院学报》2020 年第 6 期，第 137-138 页。

侦查机关欲继续取证则需转为使用查封、扣押方式控制信息载体,进而实现信息的强制获取。制度层面需为调取措施与查封、扣押措施提供衔接路径,即在《刑事诉讼法》中增设“有关单位或个人拒绝配合侦查机关调取或不如实提供相关信息,依据查封与扣押的相关规定进行处理”,进而以《刑事诉讼法》第136条至第145条的查封、扣押规范作为强制获取信息的合法依据,但是有必要完善具体程序。具体而言,侦查机关应提出查封、扣押信息载体的书面申请,写明法律依据、适用对象、所欲调取的信息类型与信息范围,并阐明所欲获取的信息材料与特定事实之间存在合理推论关系。同时,改变目前由办案部门负责人内部审批的方式,以外部审查代替内部审查,由检察机关对查封、扣押措施的启动进行审查批准,认为达到合理怀疑标准时可批准程序申请。

(二)建立刑事诉讼中个人信息权利保护机制

目前中国刑事诉讼制度层面的个人信息权缺乏独立的话语体系,公民缺乏直接的、积极的方式实现个人信息保护,难以抵御刑事程序中公权力机关对其个人信息权利的不当干预。刑事诉讼领域应当明确建立个人信息权利保护机制,为公民个人信息保护提供直接的制度支持。具体而言,在制度层面对个人信息权予以肯认,以隐私权与个人信息权共同作为个人信息保护基础,建立“隐私权—个人信息权”复合型权利保护模式。“隐私权—个人信息权”保护模式在现有隐私权制度建设基础上,引入个人信息权,以隐秘性、私密性作为标准对公民个人信息保护程度进行界分,对隐私信息予以高强度保护,对一般信息予以次高强度保护。个人信息权具体内容包括信息主体享有信息知情权、信息决定权、信息访问权、信息更正权、信息删除权以及解释说明权,信息主体通过直接、主动地行使以上权利能够在信息处理前、处理中、处理后进行信息全程性保护,弥补隐私权消极防御的不足。

个人信息权项下的子权利在不同信息处理场景下的适用程度不同,基于刑事司法具有较高程度的封闭性与强制性,信息主体权利的行使必然受到一定程度的限制。在侦查机关个人信息调取措施适用过程中,应当保障信息主体的信息知情权、访问权、更正权、删除权以及解释说明权。其一,信息知情权是行使其他权利的基础,为保障信息主体知情权的实现,制度层面应明确规定:侦查机关负有信息处理的告知义务,此义务可由第三方信息控制者协助或代为履行。在不妨碍刑事诉讼顺利进行的前提下,应尽可能地保障信息主体的知情权,使其知晓调取行为。如果存在及时告知有碍侦查的法定情形,侦查机关与信息控制者可以采取延迟告知、事后告知的方式。一般情况下,应告知信息主体侦查机关调取的法律依据和信息内容,如果存在不应告知调取内容的法定事由,则仅告知信息主体存在侦查机关调取信息的行为。[①] 其二,信息主体在知晓侦查机关调取其个人信息后,如果对调取信息的完整性、准确性存疑,可申请进行信息访问;经访问核查,调取信息确实存在错误或遗漏的,信息主体有权要求修正、补充信息,保证进入刑事程序的信息客观、准确。其三,若侦查机关所调取的个人信息在刑事程序中已无正当目的需要对其进行处理,信息主体可以主动行使删除权,请求不再留存其个人信息,避免被侦查机关在缺乏正当目的的情况下进行后续信息处理。

(三)优化企业配合刑事执法的权益保护机制

在侦查机关适用信息调取措施的过程中,网络信息服务者的配合执法义务体现为提供其收集存储的信息以及必要的技术协助。作为刑事诉讼中的第三人,其协助执法义务是有限度、有边界的,制度层面不应对其科以过重的执法义务,尤其对于企业型第三人,不得过度挤压其作为经营主体享有的合法权益。优化企业配合刑事执法的权益保护机制应从以下两方面展开。

一方面,制度层面细化企业的配合刑事执法义务,调和执法协助义务与数据合规义务的冲突。其一,明确企业履行配合刑事执法义务的优位性,但对配合程度设定必要的限制。相较于企业数据合规义务,企业配合刑事执法义务具有履行的优位性,此优位性需以明确的法律规定为依据,以正当程序和比例原则为保障,避免对企业科以过重的义务。[②] 应对配合刑事执法义务设定必要限制,即不能与企业合法经营目的存在本质冲突,如果对企业经营目的、经营活动产生实质性损害,则属于要求其过度履行协助义务,企业有权拒绝配合。其二,建立企业协助侦查的豁免机制,支持企业拒绝侦查机关不符合程序规范的协助要求。以网络信息

① 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》,载《法律科学(西北政法大学学报)》2021年第3期,第93页。

② 参见裴炜:《刑事数字合规困境:类型化及成因探析》,载《东方法学》2022年第2期,第162页。

企业豁免协助信息调取为例，企业通过内部审查机制对信息调取主体、信息调取类型与范围等内容进行形式审查，如果存在调取主体不适格、调取内容不明确、被调取的信息主体不存在相关信息、调取程序不符合法定条件、调取措施缺乏法律依据等问题，则企业有权拒绝配合调取或延迟配合调取。[①] 其三，设置刑事侦查中信息控制者告知义务免责机制与告知义务豁免机制，纾解网络信息企业的数据合规困境。网络信息企业作为信息控制者，负有保护其用户个人信息的义务，未经信息主体同意向侦查机关披露信息可能引发数据合规责任，需要在刑事诉讼制度或信息数据保护制度层面设置履行告知义务免责机制与告知义务豁免机制为信息数据企业适度解绑。告知义务免责机制是指，除存在法定保密事由、紧急情形等不适宜告知因素外，允许作为信息控制者的网络信息企业依法告知信息主体关于侦查机关信息调取的基本情况，网络信息企业不因告知行为承担干扰侦查的法律责任。告知义务免责适用应属于常态化情形，而当存在法定保密事由、紧急情形或告知可能妨碍侦查等特殊情形时，启动告知义务豁免机制，免除网络信息企业告知用户其个人信息被调取的责任。[②]

另一方面，在制度层面赋予作为第三方信息控制者的企业必要的权利，使企业能够以积极方式维护合法权益。其一，抗辩权。在公安司法机关对信息控制者启动刑事调取等信息干预措施时，信息控制者享有抗辩权，即有权就公安司法机关干预措施发动的法律依据与事实依据、信息调取范围等提出抗辩。其二，申诉权。在公安司法机关向信息控制者调取其控制的信息过程中，如公安司法机关违反法律规定调取信息、查封与扣押信息载体，信息控制者有权提出申诉或控告。对于此申诉控告，受理机关应当及时处理。对于处理结果不服的，信息控制者可以向同级检察院或上一级检察院申诉。检察机关经过审查核实，认为公安司法机关调取数据行为确实违反法律规定的，通知有关机关及时纠正违法行为。其三，求偿权。《刑事诉讼法》对证人履行作证义务产生的费用设置补助，但是没有关注同为刑事诉讼中第三人的网络信息企业在履行法定义务中承担的经济成本。网络信息企业在配合公安司法机关获取信息数据的过程中，提供人员、设备、技术等方面的支持均会产生经济成本，尤其对于小型、微型企业，这种负担相对更重。在刑事诉讼制度层面应当赋予信息控制者求偿权，对其在配合公安司法机关进行信息调取等活动中付出的经济成本予以补偿，以减轻企业履行配合侦查义务的压力，提高配合的积极性。

五、结语

数字时代，侦查机关广泛应用个人信息调取措施提升办案效能，但在获享刑事执法便利与效率红利的同时，也存在过度限制公民个人信息权利、网络信息企业合法经营权的风险。为保障数字时代法治中的实质公正性与程序正确性，[③]强化刑事程序法治建设，应当在刑事诉讼制度层面对侦查机关的信息调取措施进行必要的法律授权和有效的程序控权，设定侦查机关信息调取权力的合理运行限度，设置符合刑事程序法定原则、比例原则的程序规范。笔者对数字侦查场域强化侦查机关个人信息调取权的程序控制、构建公民个人信息权的独立话语体系、完善网络信息企业配合侦查义务机制进行初步探讨，从权力运行、权利保护、权益保护三个维度划定个人信息调取措施的适用限度，对刑事调取措施规范进行“信息化”调适，强化数字时代侦查权的法律控制，平衡数字时代惩罚、追诉犯罪与保障公民权利、企业权益之间的关系。《十四届全国人大常委会立法规划》将《刑事诉讼法》再次纳入，这是《刑事诉讼法》的第四次修改，也是数字信息技术和刑事诉讼程序深度融合背景下的《刑事诉讼法》修改。期待此次修法对数字时代侦查措施转型以及信息数字类权利保护予以关注，直面数字时代对刑事诉讼的挑战，有效规制数字侦查措施，强化公民个人信息权利保护与企业信息数据权益保护。

① 参见刘甜甜、李卓毅：《向网络服务提供者调取电子数据的性质重释与程序完善》，载《河北法学》2024 年第 3 期，第 199-200 页。

② 参见唐云阳：《网络服务提供者“双重义务”的内在冲突及协调路径》，载《西安交通大学学报（社会科学版）》2023 年第 4 期，第 167 页。

③ 参见李忠操：《数字法治的法理解析：形式、实质与程序》，载《中国海商法研究》2023 年第 4 期，第 52 页。

The Applicable Limitation and Legal Regulation of Criminal Retrieval to Personal Information

QIAN Cheng

(Law School, Dalian Maritime University, Dalian 116026, China)

Abstract: In the digital age, investigative agencies rely on digital information technology to enhance data collection and processing capabilities and improve case detection efficiency. However, while investigative agencies enjoy the benefits of information retrieval measures to improve case handling efficiency, they also induce the hidden dangers of improper application of information retrieval measures to infringe on the rights of information subjects and the rights of information processors. At present, in criminal procedure legal norms, the content of information retrieval measures presents an authorization color, the overall normative density is low, and there is no strict procedural control over the investigative agencies' rights to retrivel information. Driven by convenient rules and technologies, investigative agencies obtain a wide range of citizen information controlled by third parties, especially Internet companies, in the name of retrieval, which hides the risks of investigative agencies abusing their rights to obtain information and improperly restricting citizens' personal information rights and the rights and interests of Internet information companies. In the process of investigative agencies applying information retrieval measures, they should follow the concept of limits. Specifically, there are three limits. The first is to clarify the operating limits of investigative power, that is, to restrict the operation of investigative power based on the principles of statutory procedures and proportionality, and to restore the necessary limits of information retrieval by investigative agencies. The second is to play the restrictive role of citizens' rights, that is, to set limits on the information retrieval behavior of investigative agencies based on citizens' rights, and not to excessively interfere with citizens' privacy rights and personal information rights. The third is to play the restrictive role of the legitimate rights and interests of information processors, that is, to set limits on the information retrieval behavior of investigative agencies based on the rights and interests of network information companies, and not to impose excessive cooperation obligations on companies. Strengthening the legal regulation of the investigative agencies' personal information retrieval measures is carried out in the following aspects: First, improve the procedural normative mechanism for criminal retrieval to personal information, and carry out legal authorization and procedural regulation according to the two attributes of arbitrary investigative measures and mandatory investigative measures, and make "informatization" adjustments to the existing criminal procedure norms to strengthen the legal control of the investigative power. Second, establish a mechanism for protecting citizens' personal information in criminal proceedings, recognize the basic right of personal information at the institutional level, and use privacy rights and personal information rights as the basis for personal information protection. That is, on the basis of the existing privacy system, introduce personal information rights to ensure that information subjects can directly and actively protect their personal information by exercising the right to know information, the right to access information, the right to correct and delete information, and other rights, as well as make up for the shortcomings of the passive defense of privacy rights. Third, optimize the right protection mechanism for enterprises to cooperate with criminal law enforcement, refine the obligations of enterprises to assist in criminal law enforcement, establish an exemption mechanism for enterprises, and reconcile the conflict between the obligation to assist in law enforcement and the obligation to comply with data regulations; grant enterprises as third-party information controllers the necessary rights so that they can safeguard their legitimate rights and interests in an active manner.

Key words: criminal retrieval; personal information rights; privacy rights; mandatory measures; legal regulation