刑事司法科学与治理
Criminal Justice Science & Governance
2025 年 第 6 卷 第 1 期

侦查中个人信息调取行为的法律规制

——以第三方信息平台的提供义务为切入点

刘千硕

中南财经政法大学刑事司法学院，武汉

摘　要 | 随着大数据时代的来临，个人信息数据化的生态已基本形成，第三方信息平台在侦查机关调取个人信息过程中逐渐成为核心节点，其协助行为对侦查效率和个人信息安全具有重要影响。然而，我国现行法律对第三方信息平台协助侦查的规制存在明显不足，使得其在协助侦查的实践中面临角色冲突和权利保护不足的问题。本文以侦查中个人信息调取行为的法律规制为研究对象，针对第三方信息平台在协助侦查中的超范围行为、信息泄露风险及程序瑕疵等现象，提出以比例原则和个人参与原则为核心的规制路径，建议完善平台告知义务、优化信息分类管理、加强程序性规范，以实现侦查效率与个人信息保护的平衡。通过对法律体系的分析与优化建议，为大数据时代下侦查与信息治理的协调发展提供了理论支持和实践参考。

关键词 | 个人信息保护；数据型侦查；第三方信息平台；信息调取

一、引言

随着互联网信息技术的进步与发展，第三方信息平台成为网络服务的主要提供者。用户为了享受网络服务带来的诸多便利，会授权各种第三方信息平台收集、管理其个人信息，第三方信息平台也就成为公民个人信息的实际管理者。因此，侦查机关若想调取个人信息，就需要第三方信息平台协助。需要注意的是，本文所讨论的第三方信息平台指那些在提供服务过程中，出于商业利益的考量，对用户个人信息进行搜集和处理的非政府组织。在大数据的浪潮下，第三方信息平台的范畴已经从传统的服务提供商，如电信运营商、银行和其他金融服务机构、运输公司等，扩展到了包括互联网巨头在内的新型数据企业。例如，腾讯、百度和阿里巴巴等公司，它们通过互联网服务收集用户数据，进行分析和利用，以为用户提供更加个性化的服务，并创造商业价值。

通过对第三方信息平台的定义进行梳理，可以看出让第三方信息平台嵌入侦查犯罪治理，使原有的侦查互动过程受到第三方信息平台的影响，公民

的权利保障诉求难以得到国家的有效回应。有鉴于此，本文对个人信息调取的各项法律依据予以重新审视，深入分析第三方信息平台的角色冲突与行为失范的内在机理，提出切实有效的措施改进第三方信息平台协助调取个人信息的行为，以缓解角色冲突和行为失范。

二、平台[1]在协助调取个人信息时的作用

平台能够借助自身优势，帮助侦查机关更有针对性、更有效率地调取个人信息，这便是平台在侦查信息调取中的作用。具体来说，这些作用主要体现在两个方面：一是平台直接将个人信息提供给侦查机关，无需借助技术分析；二是平台对其管理的个人信息进行技术处理后，再提供给侦查机关。

（一）不需要借助技术分析的信息

不需要借助技术分析的信息提供，是指平台在为用户提供服务过程中产生的信息数据。这些个人信息无需再加工，可以直接进行提取、检索和调用，供侦查机关使用。侦查机关利用这些个人信息，能更有效地揭露案件事实，使办案效率大幅提高，对有效打击犯罪意义重大。

具体来说，平台直接为侦查机关提供的个人信息包括平台用户的实名认证信息、IP地址、通讯信息、购物记录以及浏览记录等。通过这些个人信息，可以获知信息主体的相关活动。在我国司法实践中，侦查机关利用平台直接提供的个人信息侦破案件的例子不胜枚举：在最高法指导案例105号和106号的网络赌博案件侦办中，侦查机关利用腾讯公司和阿里巴巴公司所提供的聊天记录和转账记录，确定涉案人员的赌博行为以及相关赌资、赌场信息，为案件的破获提供了重要依据和线索；在浙江警方侦办的破坏计算机信息系统犯罪案件中，警方调取的阿里云服务器关于犯罪嫌疑人的流量日志，可用于证明涉案服务器被技术攻击并进行相应处理的事实，这便是平台提供给侦查机关浏览记录信息数据来侦破案件的典型例证。除此之外，平台还与侦查机关建立了长期、持久的合作关系，在常态化的侦查工作中提供个人信息。例如深圳市公安局与腾讯公司成立了“天下无贼反信息诈骗联盟”，提供诈骗分子的网络行为、行踪轨迹、转账记录等，以此来实现对诈骗分子的追踪和行为认定。其他诸如阿里巴巴的“阿里聚安全”“天朗计划”等警企合作计划，也是通过上述模式获取相关个人信息来实现案件侦破的。

（二）需要借助技术分析的信息

在侦查实践中，部分侦查机关需要的个人信息可能并不存在，或个人信息存在加密的情况。这就要求平台对原有的个人信息进行技术加工处理，包括对个人信息进行技术分析和对加密的个人信息进行解密，然后再将其提供给侦查机关，以推动侦查工作进展。

1. 通过对个人信息的分析使调取行为针对性提升

平台在商业活动中利用特定的算法，对个人信息进行分析，主动获取公民的喜好等信息，并由此向用户定向推送更加个性化的信息资源等方式，获得更为客观的盈利。平台在协助侦查机关分析个人信息的过程也是如此：对海量个人信息进行加工，在个人信息之间建立联系，构建涉案人员的相关“数据画像”，从中推断出在网络空间何人于何时进行何种行为，以减少侦查机关的工作量，提升侦查工作的针对性。

2018年，浙江温州苍南警方为侦破一起特大安全套制假案件，委托阿里巴巴公司进行技术协助。阿里巴巴公司通过对平台内安全套包装盒、说明书等包装材料的购买记录和相关的物流信息的分析，对涉嫌用户的转账记录和相关物流信息进行比对，形成个人信息关系网，以此为警方确认犯罪团伙的制假售假行为提供依据。最后构建出该团伙的制假售假的活动版图，向警方提供该团伙的组织脉络、人员身份及遍布多地的黑窝点，从而一举侦破此案件。除此之外，IBM公司旗下的i2公司、美国的Palantir公司以及我国上海的蓝灯软件科技公司，都可以利用自身专门的个人信息分析技术进行比对、碰撞，为侦查机关理清案情，在个人信息之间建立有效的联系，以此来确认犯罪活动，锁定犯罪嫌疑人，并最终实现案件侦破。

---

［1］为了使行文简洁流畅，以下将“第三方信息平台”简称为“平台”。

2. 协助解密加密的个人信息

部分犯罪分子为逃避打击，利用互联网技术手段，对其在第三方信息平台产生的个人信息进行加密，阻碍侦查机关有效调取个人信息，给侦查工作、电子数据取证工作带来实质性挑战。鉴于此种情况，第三方信息平台借助技术优势帮助侦查机关解密加密的个人信息就显得格外重要。协助解密加密的个人信息，是指第三方信息平台依照专门的法律法规，运用数据技术的优势，对用户自行加密的个人信息及相关的设备进行破解，从而较为高效地收集获取情报信息及证据。随着加密技术和移动设备及网络账户解锁密码的广泛使用，第三方信息平台协助侦查机关解密的行为越发频繁。其中最典型的案例就是苹果协助解密案件：2015年美国加州发生枪击恐袭案，造成重大伤亡且涉案人员被当场击毙，案件侦查因此陷入困境。但在犯罪现场的调查中，执法人员发现了一部属于被击毙嫌疑人的iPhone手机，这部手机很快被视为解开案件的重要线索。为了进一步侦查，美国联邦调查局的办案人员持法院颁发的搜查令，要求苹果公司提供协助，以便从涉案的iPhone中提取信息。虽然此案最终结果是苹果公司拒绝协助解密，但是这也从侧面反映了这些第三方信息平台有能力帮助侦查机关解密以调取加密的个人信息。

三、平台协助调取个人信息的法律依据

目前，世界各国已对第三方信息平台协助侦查机关调取个人信息的行为做出初步规定，相关条文散见于各处。梳理这些法律法规，能够理清个人信息调取行为的法律框架，并为调取行为提供依据。

（一）存储个人信息的相关规定

个人信息的存储是个人信息调取的前提和基础，没有个人信息的存储，也就不存在个人信息的调取。然而，不加规范的个人信息存储可能不利于个人信息保护。因此，世界各国都对平台存储个人信息做出了严格而明确的规定。从法律渊源来看，这些规范既有规定于专门的数据保护法规当中的，也有规定于单行法当中的，散见于各处。梳理和总结相关规定，有利于廓清平台存储个人信息相关法规的基本轮廓。

我国立法针对平台存储个人信息做出了相应的立法尝试。《个人信息保护法》第四条规定，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，明确了平台对于个人信息的存储是其处理个人信息必不可少的一个环节，以概括性的规定肯定了个人信息存储的重要性；紧接着，第十七条规定平台应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息的存储期限；第十九条又规定，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。《个人信息保护法》的这些法律条款规定了平台进行个人信息存储所要注意的事项，同时为其他部门法和相关法规进一步细化存储个人信息的具体规定提供了法律依据。例如，《网络安全法》第二十一条规定，网络运营者留存相关的网络日志不少于六个月，此项条款是对《个人信息保护法》中个人信息存储期限的具体化，明确了平台对于个人信息存储的最低存储期限；再如，《中华人民共和国电子商务法》第31条规定：“电子商务平台经营者应当记录、保存平台上发布的商品和服务信息、交易信息。商品和服务信息、交易信息保存时间自交易完成之日起不少于三年；法律、行政法规另有规定的，依照其规定。”《中华人民共和国证券法》第137条规定：“证券公司应当妥善保存客户开户资料、委托记录、交易记录和与内部管理、业务经营有关的各项资料，任何人不得隐匿、伪造、篡改或者毁损，上述资料的保存期限不得少于二十年。”这些法律又对平台存储的不同类型的个人信息进行了详细规定，并区分了不同类型的个人信息的最低存储期限。此外，个人信息存储的相关规定还散见于各部门规章中。例如，2018年11月实施的《公安机关互联网安全监督检查规定》第十条规定，公安机关在对互联网安全进行监督检查时，要特别关注平台是否依照法律规定对用户的注册信息以及网络日志进行记录和保存，不仅强调了平台进行个人信息存储的必要性，而且要求有关机关进行检查。

就国外立法而言，欧盟《数据留存指令》（已废除）是一部针对平台存储个人信息行为的专门性立法，并在其序言部分明确了立法目标，即在欧盟层面协调平台保留个人信息的义务，并确保这些个人信息可用于调查、侦查和起诉每个成员国在

其国内法中定义的严重犯罪，这就为其成员国或其他国家具体规定平台存储个人信息的行为提供了指导和法律依据。除了对个人信息存储进行一般性规定外，各国又对存储个人信息的类型和存储期限做出了立法探索，散见于各处，在此并不进行一一列举，而是选取其中比较典型的范例。例如，美国《自由法案》要求电信运营商对电话细节记录进行留存，如呼出号码、接收号码、通话时间、时长等，但是对通话内容的留存做出了严格限制；其他国家如丹麦、爱沙尼亚、希腊、西班牙等都明确规定平台存储个人信息期限至少为一年。通过对国内外的信息存储规定进行梳理可以发现，虽然《个人信息保护法》以概括性的条款规定了平台存储个人信息的注意事项，但是我国并没有一部类似欧盟《数据留存指令》（已废除）的专门性的法律来对平台存储个人信息进行一般性规定。此外，我国立法大多规定平台应对何种类型个人信息进行存储，但是何种个人信息不应存储并没有详细的规定。最后，同国外立法相比，我国平台存储个人信息的期限总体时间较短。基于此种种，可以借鉴其他国家关于个人信息数据存储规定，明确存储个人信息的具体内容和相关限制，延长存储的期限，并在整个法律体系中形成统一规定。

（二）配合侦查机关调取个人信息的相关规定

梳理调取个人信息的相关规定，能为平台协助侦查机关进行具体的调取行为提供法律依据。在我国具体的侦查实践中，个人信息调取行为仍可以归到普通技术侦查或者侦查技术的范畴。可以明确，平台协助侦查机关调取个人信息，即在侦查行为中提供案件相关材料，源自传统刑事诉讼体系中作为案外人的第三方主体的协查义务。即使处于大数据时代，协查义务的本质依旧没有变化，只是义务主体和具体内容发生了变迁，因此在调取个人信息过程中，也可以应用普通的调取证据相关规定。新修订的《刑事诉讼法》第五十四条规定，法院、检察院和公安机关有权向有关单位和个人收集、调取证据；第一百五十二条规定，有关单位和个人对公安机关的技术侦查措施应当配合并加以保密，同时还以多个条款明确了技术侦查的具体实施程序。[1] 这些法律规定都可以作为平台协助侦查机关调取信息的概括性规定，以应对特殊情况下缺乏相关规定的情况。除了《刑事诉讼法》中的兜底性规定，我国专门的数据立法也对调取个人信息的行为作出了规定。首先是《数据安全法》第三十五条明确规定，为了维护国家安全或基于犯罪侦查的需要，公安机关和国家安全机关可依法获取相关数据。在此过程中，侦查机关必须遵循国家相关法规，并通过严格的审批程序合法执行数据调取。同时，相关组织和个人也有义务提供必要的协助与配合。《网络安全法》第二十八条规定，平台应当提供相应的技术支持和协助，以方便侦查机关的取证工作；第七十七条也要求公民和组织应当向国家安全机关、公安机关和军事机关提供必要的支持和协助。

就国外立法而言，各国对于个人信息调取的相关规定和我国类似，都是由一部法律的概括性规定延展到其他部门法的具体规定。以德国为例，《德国刑事诉讼法》规定，检察官和警察可以依据犯罪侦查的概括性条款，要求平台提供相应的个人信息并将其应用于侦查活动。此项条款为平台调取个人信息提供了一般性指导，同时也为其他部门法细化此条款提供了法律依据。德国《联邦数据保护法》规定，侦查机关在侦查重大复杂的犯罪案件时，若为排除非嫌疑人或为识别满足与案件有关条件的人所必需的措施，且其他措施对于案件侦查效率明显更低的情况下，可以向平台调取个人信息，由此细化了平台协助侦查机关调取个人信息的具体情况。由此可见，就平台协助侦查机关进行机制化的个人信息调取而言，我国相关规定与世界各国的规定并无较大差别。

（三）提供技术协查的相关规定

我国对平台提供技术协查作出了相应的立法尝试。《个人信息保护法》第五十一条及相关条款规定，相关个人信息处理者也有在案件侦查中对侦查机关提供个人信息和解密去匿名化的协助义务。这些规定为平台协助侦查机关对个人信息进行技术处理提供了依据。我国其他法律也对此规定进行了细化，针对

[1] 程逸凡．公安行政执法过程中的第三方数据利用法律规则研究［D］．北京：中国人民公安大学，2020.

不同类型的犯罪案件要求平台提供不同种类的技术协助。例如，《反恐怖主义法》第十八条规定，电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关的职务活动提供技术接口和解密等技术支持和协助，也就是所谓的协助解密；《反有组织犯罪法》强调的是电信业务经营者、互联网服务提供者对“公安机关侦查有组织犯罪提供技术支持和协助”；《反电信网络诈骗法》要求互联网服务提供者为公安机关办理电信网络诈骗案件依法调取证据提供技术支持和协助。这些法律法规都在具体的案件类型和协查行为上进行了详细的要求。

针对平台提供技术协查的相关规定，也得到了各个国家的重视。依旧以德国为例，德国《刑事诉讼法》的相关规定明确执法部门可以根据一般性法律规定直接应用网络上公开的个人信息，但是对于复杂案情可以根据特殊的规定与程序要求平台对个人信息进行二次加工比对，满足侦查需要后应该及时删除。这项规定肯定了平台为侦查机关提供技术协助的合法性，但是针对具体案件该使用何种技术，此法并没有进行详细规定。对于具体的技术协助的相关规定散见于各国具体的部门法和相应的公约协议之中，在此并不一一列举，而是从中挑选几部具有代表性的法律法规。例如，美国《通信协助执法法》《爱国者法案》《外国情报监视法》以及欧盟《网络犯罪公约》中都有相关规定，要求平台针对各自法律规定的范围内提供给侦查机关相应的技术支持或为侦查机关提供“技术后门”。[1]这与我国相关立法要求平台提供技术接口或提供解密技术支持具有异曲同工之妙。由此可见，我国和西方国家对于平台为侦查机关提供技术协助的相关规定都很重视，相关规定符合现实发展要求，顺应了国际主流方向，同国际接轨，体现了自由与安全的平衡。

四、平台协助调取个人信息行为中的角色冲突与失范

第三方信息平台具有向侦查机关提供个人信息的协查义务，而作为用户个人信息的实际控制者，其又负有对个人信息保护的义务。这种依据公法产生的个人信息提供义务和依据私法产生的个人信息保护责任产生矛盾冲突，若任其无序发展，必定会影响侦查活动的正常开展，并严重威胁公民的个人信息安全。

（一）平台协助调取个人信息行为的角色冲突

侦查机关要求平台进行的个人信息留存、技术监控、信息披露等个人信息提供行为已成为常态，这是平台配合侦查工作所必须履行的协查义务。然而，与此同时，平台还是服务的提供者，对其用户的个人信息拥有实际的控制权，同用户签订服务协议，要遵循契约精神，依照协议正确处理用户的个人信息，负有保护用户所交予个人信息的义务，对于个人信息的处理不能擅自越界，剥夺用户的自决权。

从侦查机关的角度来看，平台要履行协查义务，为侦查机关提供平台用户的相关个人信息。平台为了配合侦查机关，甚至可能直接越过用户，在用户不知情或不同意的情况下，将用户个人信息毫无保留地交予侦查机关，这实际上是对用户个人信息的一种侵犯。而从平台用户的角度出发，平台要履行个人信息保护的义务，不得擅自向侦查机关披露个人信息，这又是对协查义务的违背。平台既要履行提供个人信息的协查义务，又要注意保护个人信息的义务，这使其陷入矛盾之中：保护个人信息就意味着提供个人信息受阻，提供个人信息就可能造成个人信息的泄露风险，不利于保护。因此，协查行为中的角色冲突，实际上是平台作为私权利主体，其调取行为背后所蕴含的公权力行为之间的冲突，也就是公法和私法之间的矛盾冲突。

这种矛盾冲突在现实中的表现不胜枚举，除了上文提及的苹果公司拒绝协助美国联邦调查局侦查取证外[2]，2017年，美国推特公司对国土安全部等政府机构提起诉讼，抗议其提出的协助请求。该诉讼起因于政府机构要求推特披露一位用户的个人信息，该用户因多次发表针对执政党的批评性言论而受到关注。推特公司坚称，在缺乏证明该用户涉嫌违法或犯罪的证据下，政府机构索取用户身份信

［1］杨敏．网络服务提供者的侦查协助机制研究［D］．重庆：重庆邮电大学，2019．

［2］腾讯科技．苹果不配合以色列公司帮助FBI破解嫌犯的iPhone［EB/OL］．（2019-03-02）［2024-03-04］．http://digi.tech.qq.com/a/20160329/041953.html．

息的要求是对宪法权利的侵犯。[1]这种角色冲突实际上反映的是公权力扩张和公民基本权利延伸的趋势，是国家公权力与公民私权利的二元互动在网络社会中的映射。

还需要注意的是，除了平台本身的角色属性外，平台在具体实践中的不恰当行为也加剧了这种冲突。首先就是平台对于其用户个人信息收集和利用的具体方面，并没有进行实质性的告知。但这并不是说平台没有履行对平台用户的告知义务，而是普通公民无法真正地了解到平台对于其所提供的信息究竟是如何处置的。这是因为平台对信息的管理是一项庞大、复杂且持续的工程，并且该工程无法综合性地完成。另外，平台无法违背协查义务拒绝侦查机关的调取行为，但是可以通过其他手段来缓解矛盾。例如进行有效的告知，提前使平台用户有效知晓调取行为，让用户自己决定是否需要以个人信息的暴露来换取服务，是否有必要在调取行为之前对个人信息进行更改。通过有效的告知，平台所管理的个人信息的自决权实际上还掌握在用户自己手中，从一定程度上说，这也是一种个人信息的保护。但是，如果告知不能有效落实，个人信息保护和个人信息提供义务之间的矛盾不仅不会缓解，还会加剧。国内外不少学者已经意识到，如果这种告知义务依旧流于形式，无法取得用户的实质同意，这种形式甚至会成为侵害用户隐私权的一把利剑。因此，学界也尝试对这种同意制度进行实质性突破。但是，无论是何种优化变通路径，似乎都从侧面反映了用户实质知情同意的困难。也正是在这个意义上，有研究表明，在规则设计上增加用户控制，并不必然导致用户隐私保护水平的提升[2]。例如，美国法与计算机科学专家艾瑞·伊斯拉·瓦尔德曼（Ari Ezra Waldman）通过观察个人信息保护领域法律的内生性特征（legal endogeneity），认为企业对于个人信息保护规则的合规应对可能反噬个人信息保护的初衷，并最终可能演变为“为合规而合规”。[3]

（二）平台协助调取个人信息的行为失范

上文从宏观层面探讨了平台在协查行为中，因角色冲突产生的公法与私法之间的矛盾。接下来将从协查行为的具体运作入手，阐述平台在提供个人信息过程中的行为失范。

1. 履行协查义务过程中信息泄露风险

首先，大体量、多种类的个人信息是多元主体的结合体，涉及个人信息数量越多、交互越频繁，就越容易增加泄露风险。[4]而且，国内外不少平台为了更高效、更有针对性地配合侦查机关调取个人信息，可能会对侦查机关进行访问授权，即在特定情况下经过访问授权，侦查机关可以和平台共享个人信息资源，也就是所谓的“技术后门”。比较典型的例子就是苹果公司同意在涉及任何人迫在眉睫的死亡或严重身体伤害的紧急情况下，侦查机关可以和苹果公司进行个人信息共享；又如美国优步公司规定，如果乘客在自认为的紧急情况下，可以通过软件的内置功能进行紧急报警，警方由此可以及时得知用户实时位置、车辆及人员信息。这种“技术后门”确实提高了信息调取的效率和针对性，但也极易被不法分子通过网络技术攻破，从而使平台的个人信息暴露无遗，进而被不法分子窃取，增加泄露风险。

此外，个人信息的应用场景不受三维空间的地域限制，然而侦查机关在办案过程中却存在地域管辖。不同地域主体向平台的跨区域调取行为，势必会产生相应的泄露风险。由此，超地域调取行为的延伸带来了多主体对于个人信息的诉求。例如，除公检法等司法机关外，依据《工商总局关于进一步做好查处网络传销工作的通知》第3条、《电子商务法》第25条等规定，各级工商、市场监管、税务、网信等部门都有权向第三方平台信息调取个人

---

［1］澎湃新闻．推特把美国国土安全部告了：被要求交出批评特朗普的用户信息［EB/OL］．（2017-04-07）［2024-03-04］．https://www.thepaper.cn/newsDetail_forward_1656813.

［2］Carolan E，M Rosario Castillo-May é n．Why more user control does not mean more user privacy：An empirical（and counter-intuitive）assessment of European e-privacy laws［J］．Virginia Journal of Law & Technology，2015，19（2）：325-388.

［3］Waldman A E．Privacy Law's False Promise［J］．Washington University in St．Louis，2020，10（3）：116-123.

［4］戴昕．数据界权的关系进路［J］．中外法学，2021，33（6）：1561-1580.

信息，且平台应当提供。[1]但是，平台作为商业主体，在调取行为中处于相对劣势，对于要求其履行协查义务的要求的真实性甚至合法性进行核查，缺乏法律依据和实质性的权力，对调取需求无法进行强制性的核查确认，对于其调取行为的程序履行没有切实的救济途径，这些都是个人信息泄露风险滋生的温床。

2. 平台超范围、超比例地提供信息

上文所述平台进行自建数据库，并在平台内部根据个人信息的敏感程度进行分类。在履行协查义务过程中，根据涉案类型，有针对性地授权侦查机关自行进入数据库进行收集，或者将个人信息打包提供，通过分类处理实现个人信息保护和个人信息利用的平衡。但这种处理方式毕竟只是一种理论上的理想状态，平台涉及的个人信息包括多元主体的多种数据，对大体量、多种类的个人信息进行分类分级工作，需要投入大量的时间、精力以及相应的物质资料，用于技术研发突破和运营管理。这些平台归根结底还是追求经济利益的商业主体，不可能不考虑成本和技术层面的因素，无法在实际运行过程中完全按照理论预想，将信息进行完美的分类分级。反而更可能出于成本考量或限于技术瓶颈，将个人信息不加筛选地完全打包给协查机关，提供的个人信息大概率会超出原本的侦查请求范围，违背个人信息提供的比例原则。同时，平台将个人信息交予之后，并未考虑个人信息回收处理和访问授权撤销的问题，使大量与案件无关的个人信息被曝光，暴露在公共视野之中，公民个人信息的泄露风险激增。

3. 协查过程中的程序失范

在个人信息调取过程中，实际上仍存在具体程序失范的问题，即在实践中是否严格按照程序规范执行。首先，从调取行为的具体程序规定来看，《电子数据取证规则》第41条规定：“公安机关向有关单位和个人调取电子数据，应当经办案部门负责人批准，开具《调取证据通知书》，注明需要调取电子数据的相关信息，通知电子数据持有人、网络服务提供者或者有关部门执行。”然而在实践过程中，调取行为的任何一方不遵从程序，都会造成程序失范。对于侦查机关来说，向平台调取个人信息时，可能会出现不经审批直接要求调取个人信息、调取过程中因种种原因无法向平台出具《调取证据通知书》，以及调取内容与调取通知书内容不符等情况。面对这些情况，平台会因侦查机关的身份压力，无法对这些失范的调取行为加以拒绝和限制，反而会直接提供要求的个人信息，助长了侦查机关的失范行为。对于平台来说，某些规模较大的平台会对侦查机关调取个人信息的行为进行限制，出于个人信息保护的需要或其他考虑，即使侦查机关的调取程序符合规范，仍可能遭到部分平台的拒绝，或平台故意抬高调取个人信息的门槛，给侦查机关制造困难，导致侦查机关不能准确及时地获取相关个人信息，不利于侦查活动的开展。这些程序失范如果不加以约束，势必会对个人信息的调取造成更大的危害，使行为和目的背道而驰。

4. 协查义务功能异化

平台在配合侦查机关调取个人信息的过程中，还衍生出一种新型的协查方式，即侦查机关同相关平台签署相关合作协议，并以此来规定个人信息报送的内容及方法。但是在立法常态化、机制化的背景下，这种协议并没有相应的法律规定来约束，而且这种协议一般是不公开的。较低的约束力为侦查机关进行个人信息查询调取提供了极大的便利性，从而有可能借机进行无关个人信息的查询使用。即使平台明知侦查机关对个人信息的利用与侦查行为无关，在合作协议的背景下也只能被迫提供个人信息。这种行为不仅严重危害公民隐私，而且为协助义务的功能异化提供了空间，为权力寻租创造了可能。

五、平台协助调取个人信息行为的法律规制

对于角色冲突和行为失范的具体规制，要以理论为先导，提出相关规制原则，并在这些原则的指导下探究具体的规制措施，从而对个人信息调取形成有效约束，促进个人信息保护和侦查现代化的共同发展。

（一）基本原则

对于侦查机关向平台调取公民个人信息行为的

[1] 贺娇．网络综合治理体系下网络平台证据提供义务的优化路径[J]．证据科学，2023，31（2）：217-228.

规制，要遵循以下原则。

1. 个人参与原则

个人参与原则是个人信息保护中的一项重要基本原则，是指平台用户对平台所储存管理的个人信息拥有实际的自决权，有权要求平台对其储存处理个人信息的行为进行告知，自主决定对其个人信息的处置，用户还有权向平台查询自己个人信息的处理情况。[1]也就是说，对于个人信息的调取，要根据案件的具体情况，将各阶段个人信息的利用情况告知用户，让用户参与到个人信息调取当中，保障其知情权和异议权等。但是需要注意的是，基于特定案情的需要，某些情况下的调取行为需要保密，此时个人参与原则可能会受到一定限制，但这些限制并不意味着对该原则的彻底放弃。

2. 合法性原则

由于侦查机关向平台调取个人信息的行为属于新兴事物，法律的更新速度无法跟上不断变化的社会现实。然而，合法合规是任何侦查行为都必须遵循的，因此，面对这种矛盾冲突，尤其需要构建相应的法律体系来规范侦查机关的个人信息调取行为。首先应从宪法视角介入，强调以数字权利为代表的新型信息权、隐私权衍生出的“第四代人权理论”的重要性，不断提升政府在发展数字技术方面的主导权和保障数字人权得以实现的行为能力，从个人信息调取中信息保护的上位概念阐述其重要性[2]，为调取行为的规制提供法理依据。然后再以此为依据明确性质，界定行为界限，通过具体有效的立法，为侦查机关的行为提供具有操作性的具体化程序，切实做到有法可依、有法必依。

3. 比例原则

由于此类调取个人信息的侦查行为存在侵犯公民隐私权的倾向，可能会对公民与国家之间的信赖保护关系造成侵害。因此，需要对目的、手段和结果之间的关系进行考量，严格以比例原则为指引，坚持必要性和适度原则，即确有实施的必要，其他手段无法实现目的，并在衡量目的和结果之后选取侵害利益最小的行为。具体可分为以下几点：首先，依据比例原则，要求平台对不同的个人信息进行分类，然后根据调取个人信息的类型进行合比例、分等级、分层次地提供。其次是必要性和适度性的要求，调取行为的启动必须是确有必要，采取其他损害较低的行为无法达到预期效果时才实施，并且对于个人信息的调取不宜追求数量多、范围广，而应以恰好满足侦查需要为限。

（二）具体措施

基于上述原则的探讨，需以此为依据，针对调取个人信息行为中出现的矛盾冲突，有的放矢地寻找具体规制措施，以下是由此展开的讨论。

1. 切实履行平台的告知义务

上文提及平台既负有协助侦查机关提供个人信息的义务，同时又要承担保护平台用户个人信息的责任，这种矛盾冲突是平台不可避免的。既然平台的角色定位无法改变，缓解这一矛盾冲突的关键就在于要求平台切实履行告知义务，即针对侦查机关利用调取公民个人信息的行为，平台要在事前或事后进行单独强调和特殊表明。

具体而言，在调取行为发生之前，平台需要向即将使用服务的用户公布平台的个人信息利用协议规定，并且需要将侦查机关的调取行为进行单独强调和特殊标明，使用户对侦查机关使用其个人信息的行为有所预期。而在调取行为发生之后，如果并没有特殊的保密事由，平台应该向平台用户告知侦查机关对其个人信息进行的操作，以及调取的个人信息范围和目的，保证协查行为的公开透明。在此方面可以借鉴美国苹果公司及谷歌公司定期发布的透明度报告，向平台用户汇报相关的协助内容来保证用户的知情权。

2. 平台依比例原则区分个人信息数据的类型

正如上文所述，平台在提供个人信息的过程中，存在违背比例原则超范围地将个人信息打包给侦查机关的情况。若想有效对这种行为进行规制，首先要做的就是对个人信息进行分类区分。在分类时可以借鉴欧盟相关立法，依据个人信息的敏感程度进行列举并划定种类，这更加符合时代发展趋势。个人信息的敏感程度越高，意味着公民越不想让其为公众所知，这也是公民个人信息需要格外保护的部分。

---

［1］王燃．大数据时代个人信息保护视野下的电子取证——以网络平台为视角［J］．山东警察学院学报，2015，27（5）：126–135.

［2］莫纪宏．论数字权利的宪法保护［J］．华东政法大学学报，2023，26（4）：6–16.

因此，基于这种标准进行划分要考虑以下因素：首先是个人信息的隐私程度。例如家庭住址、情感经历、身体状况等隐私程度较高的个人信息，所需的保护程度就越高；相应地，公民公开在外的如姓名、性别等个人信息，隐私性较低，在保护方面无需给予过多关注。其次是将个人信息传播对主体的影响作为考量因素，此项因素与上一条较为相似，区别在于上一条是从静态角度考量个人信息的隐私程度，而此项因素是从动态角度考量：传播对主体影响大，说明此类个人信息较为隐私敏感。此外，个人信息以数据化形式呈现，数据的积累就是个人信息的集聚，量变引发质变，当对同一个体调取的个人信息达到一定数量后，在大基数的个人信息中更易对相关敏感个人信息造成侵犯。因此，对于个人信息敏感程度种类的划分，在一定程度上也要考虑数量因素。有了对个人信息的有效划分，就可以在侦查机关调取行为的过程中，根据案件侦查的现实要求来提供相应类别的个人信息，从而避免平台为图方便而不加区分、超范围地提供。

3. 对平台协助调取个人信息中的程序失范进行问责

通过上文对调取行为程序失范的讨论可知，无论是平台还是侦查机关，在调取个人信息的过程中都可能存在不合程序规范的行为。对这些程序失范行为进行问责，以明确的责任、严重的后果、不容忽视的失范成本为手段，对平台协助侦查机关调取个人信息行为进行规制，势必能在一定程度上缓解调取行为中的程序失范，从而规范调取个人信息的行为，提高侦查工作的效率。对于侦查机关来说，若在调取过程中不遵守相关的程序规范，非法调取或以调取的名义进行权力寻租，平台不仅可以拒绝其调取请求，同时还应该向其主管部门反映，追究主要参与人员或机关主要负责人的相关责任，对其进行内部批评惩戒，情节严重的应追究其相应的刑事责任；而平台若不能拒绝侦查机关不合程序的调取行为，甚至超范围提供个人信息，导致公民个人信息泄露，应认定为平台的失范行为，除了给予必要的罚款、批评警告外，还应该将其列入“个人信息保护黑名单”进行公示，降低其社会公信力，在行业内形成警示作用；而对于侦查机关正当履行调取个人信息的程序后，平台无正当理由拒不提供、拖延提供用户个人信息的情况，也应该追究其相关责任，以保障侦查工作顺利进行，同时也可追究平台的主要负责人，限制其进行特定活动，若因平台阻碍对侦查工作产生严重后果，还应追究其主要负责人的刑事责任。

4. 提供技术保障减少调取过程中个人信息泄露风险

侦查机关的调取行为是遵循“个人信息主体—平台—侦查机关”的逻辑链条运行的。三者虽看似是一个整体，但是在调取过程中实则各自分散，个人信息泄露的风险不容忽视。再加上上文所提及平台会出于调取的便利性为侦查机关提供“技术后门”，由此产生被不法分子攻击的风险。因此，对于调取行为中个人信息泄露风险的规避，应该从个人信息的收集到利用各个环节予以高度重视。首先，平台需要提高自身技术能力，打造更高水平的防火墙，以应对不法分子对个人信息的攻击窃取；其次，平台需要对用户个人信息泄露风险进行及时预警，通过技术手段，当用户个人信息被非法手段干预时，能及时报警并通知给平台和用户，以便对个人信息泄露的潜在趋势进行预防和补救。还需注意的是，在调取过程中，平台需要做到操作留痕，对调取的具体情况形成记录，以便信息主体查询和后续的监督。

5. 提供个人权利的救济

在个人信息调取过程中，不仅要保障公民的基本权利，同时还应保障其权利受损后的救济权利。除了上文提到的平台要切实履行告知义务以保障公民的知情权外，赋予公民个人对于个人信息的异议权和更正权也十分重要。所谓异议权，就是公民如果认为平台或侦查机关进行的个人信息调取行为违背了相关的法律法规及程序规范，或对调取的个人信息范围是否合比例、超范围存在疑问，可以向有关机关进行复议，若经查实确有问题，则调取行为无效；而更正权是指，当公民发现平台提供给侦查机关的个人信息与事实不符，或提取范围错误，可以要求平台对自己个人信息进行及时的更正，从而有效保障个人信息的准确度。

六、结语

随着我国改革的不断深入，国家治理体系和治理能力现代化的目标正在逐步实现。通过分析侦查机关向第三方信息平台调取个人信息的行为，可知

借助第三方信息平台进行个人信息调取对新时代侦查行为具有重要作用，同时也明晰了其调取行为的理论依据。从实际侦查工作中可能出现的潜在问题出发，分析调取行为中存在的矛盾冲突，并以此为突破口进行具体的法律规制。而具体的规制应以理论原则为先导，遵循人本原理，因此对侦查机关的调取行为也要进行有效的规制。

本文在了解侦查机关调取行为运行路径的基础上，深入了解并阐述了以数字权利为代表的新型信息权、隐私权衍生出的“第四代人权理论”的重要性，以期能够为个人信息保护提供源源不断的动力，为调取行为提供有力的规制依据，防止其无序发展。唯有如此，才能实现侦查工作与个人信息保护的完美平衡，推进智慧警务与侦查的现代化，实现侦查工作的质的飞跃，真正贯彻总体国家安全观，践行新型安全发展理念，构建更高水平的平安中国。

（责任编辑：郭志姣）

Legal Regulation of the Act of Access to Personal Information in Investigations
—Taking the Provision Obligations of Third-Party Information Platforms as an Entry Point

Liu Qianshuo

Criminal Justice School, Zhongnan University of Economics and Law, Wuhan

Abstract: With the advent of the big data era, the ecology of personal information digitization has basically been formed, and third-party information platforms have gradually become the core nodes in the process of access to personal information by investigating authorities, and their assisting behaviors have an important impact on the efficiency of investigation and personal information security. However, China's current laws on the regulation of third-party information platforms in assisting investigations are obviously insufficient, making them face the problems of role conflict and insufficient protection of rights in the practice of assisting investigations. This paper takes the legal regulation of personal information retrieval in investigation as the research object, and for the phenomena of over-scope behavior, information leakage risk and procedural defects of third-party information platforms in assisting investigation, this paper proposes the regulation path centered on the principle of proportionality and the principle of personal participation, and suggests perfecting the platform notification obligation, optimizing the information classification and management, and strengthening procedural norms, so as to achieve the balance between the efficiency of investigation and the protection of personal information. The analysis and optimization of the legal system provide theoretical support and practical reference for the coordinated development of investigation and information governance in the era of big data.

Key words: Protection of personal information; Data-driven investigation; Third-party information platform; Information retrieval