【刑事诉讼法学】

刑事数据调取中网络服务提供者的角色定位及关联义务

李延舜

【摘　　要】侦查机关向网络服务提供者调取数据已成为刑事侦查新常态，但也因此带来一系列实践操作和规范层面的问题，危及公民的隐私及数据权利等。解决这些难题，除刑事诉讼法上重新定位数据调取侦查措施属性外，还可从规范数据披露行为入手。通过界定网络服务提供者在数据侦查中扮演的角色，厘清其关联义务，进而规制刑事数据调取行为。网络服务提供者身兼经营者、公共服务提供者及网络规则重要缔造者三种角色，相应地承担“隐私及数据保护”“协助执法”“参与塑造自由、开放的数字生态”三种义务。这其中，不同义务的并存与博弈、义务之间的优先性以及彼此义务的有限性等，都是值得深入探讨的问题。只有厘清了刑事数据调取中网络服务提供者的义务体系及义务履行事宜，才能有效平衡“国家利益”、“社会公共利益”、用户“隐私及数据权益”及网络服务提供者自身的“经营权益”。

【关 键 词】网络服务提供者；刑事数据调取；数据披露；隐私权

【作者简介】李延舜，河南大学法学院。

【原文出处】《法学》（沪），2023.1.151～163

【基金项目】本文为2021年度国家社科基金一般项目“互联网企业数据合规义务研究”（编号21BFX094）的阶段性成果。

一、问题的引出

大数据不仅改变了政务和民生，对刑事侦查也产生了巨大影响。人们发现，自己在网络空间留存的各种记录可能成为对自己不利的呈堂证供，而侦查机关正对这些记录虎视眈眈。同时，网络服务提供者面对侦查机关的数据调取请求也呈现出不同样态，近年来的几个国内外案例说明了这一点。国际方面，第一个是卡彭特案，[①]该案中，美国联邦最高法院最终裁定警方必须事先获得法院的搜查令才能追踪公民的手机位置信息，而在此案之前，按照惯常理论——第三方当事人规则[②]——警方完全可以径直从电信服务商手中获得该定位信息。第二个是韩国“N号房”事件。案发后，面对警方要求提供非法视频上传者个人信息的诉求，运营商Telegram一直未予配合。Telegram创始人Pavel面对记者询问缘由时谈道：“我认为个人隐私，以及我们保护个人隐私的权利要比我们所畏惧的事情更为重要，比如恐怖主义。”[③]在他看来，这顶多算是“技术的黑暗面”。事实上，国外警方要求网络服务提供者协助侦查的案例已有不少，尤为出名的是苹果三次向FBI说“不”事件。国内方面，第一个是2017年深圳共享单车肇事逃逸案，深圳一名女性骑行ofo单车将一行人撞倒后逃窜，深圳交警数日后发布通报称：“共享单车肇事，嫌疑人逃逸，企业拒不配合调查，交警将依法查办”。不久，ofo发布声明，称“基于保障用户信息安全，ofo对于内部资料查询与审核有严格的程序规

定，虽在过程中引发双方沟通上的误解，但ofo还是在事发当天将所需数据提供给相关单位。”④第二个是2018年滴滴顺风车司机杀人案，该案案情简单，争议焦点在于平台能否以保护用户隐私为由，迟延或拒绝向侦查机关披露个人信息。滴滴公司事后发布声明：“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……如何在保护用户隐私的同时，避免延误破案的时机。”⑤

上述案件各有意义，卡彭特案说明法院已经意识到警方径直向网络服务提供者调取个人数据的行为需要予以规范，“N号房”案则表明某些网络服务提供者认为保护用户隐私和数据权利比协助侦查更为重要，ofo案表明网络服务提供者与侦查机关间的协查机制不健全，滴滴案则表明网络服务提供者已经认识到协助执法义务和保护用户隐私及数据权利义务间的冲突，并渴望在对话的基础上达成一种平衡保护方案。“记录改变了一切”，“记录”使得网络服务提供者深刻地改变了刑事侦查模式，尤其是参与侦查主体结构，“形成了国家—社会—个人三方参与的新型侦查主体分布模式，社会力量而非侦查机关在侦查权行使过程中的作用愈发重要。”⑥

然而，刑事侦查中向网络服务提供者调取数据行为的常态化也带来一系列问题。实践层面上，如平台在履行数据报送义务时，数据报送事项过多、范围过宽、报送程序不健全、报送安全性保障滞后等多种因素的存在，导致平台数据存在实践困境。⑦更常见的是，为防止数据遗漏或多次调取，网络服务提供者往往会选择扩大数据调取范围，如“顺亨汽贸公司走私普通货物案”所反映的情况，网络服务商向侦查机关披露了30个涉案邮箱中20万封电子邮件，而这些邮件并不都和案件具有关联性。⑧规范层面上，主要体现在数据保护类法律与刑事诉讼类法律的脱节。换句话讲，《个人信息保护法》《网络安全法》及《数据安全法》中规定的数据处理规则能否适用于刑事侦查？举例而言，数据侦查行为是否同样遵循《个人信息保护法》规定的合法、正当、必要、诚信、公开、透明、质量等原则？侦查机关是否是该法第三节规定的“国家机关”？究其根源，在于当前数据治理架构主要是从个人主义视角出发，而忽略了其中的社会性问题。⑨这种理解角度的差异使得我国的数据治理和数据保护立法不注重区分公私领域，如将《个人信息保护法》中的“权利束”理解为个人自主控制范式下的一组民事权利，⑩基本上忽略了刑事司法机关对个人信息调取的特殊性，并由此导致适用的模糊。欧盟这方面的法律实践给我们很多启示。《一般数据保护条例》(以下简称GDPR)第2条第2款d项将“有关主管部门为预防、调查、侦查、起诉刑事犯罪、执行刑事处罚、防范及预防公共安全威胁而进行的个人数据处理”排除在适用范围之外。欧洲议会和欧盟理事会在通过GDPR不久发布了《针对警察和刑事司法机关的数据保护指令》(以下简称(EU)2016/680)，专门用以规范刑事司法领域的数据处理，其核心宗旨是：在预防、调查、侦查或起诉犯罪以及执行刑事处罚时，仍应尊重并保障自然人的基本权利和自由。主要条款如第4条(数据处理的主要原则)、第6条(对数据主体进行分类)、第7条(区分基于事实的数据和基于评估的数据)、第10条(敏感个人数据的处理)、第25条(执法机关记录日志义务)以及第47条(监管机构的权力)等都与GDPR有所不同。

我国刑事司法领域数据处理规则的模糊性使得网络服务提供者经常陷入合规困境，如有学者指出面对协助执法义务和用户数据保护义务，“刑事合规面临的现实且急迫的挑战并不在于因违法违规行为触发刑责的风险，而在于规则本身因缺位、错位等使得企业面临进退维谷的合规义务冲突。”⑪互联网企业往往通过隐私政策在多种义务间作出安排，如《微信隐私保护指引》规定“履行法定义务或法定职责所必需”时，处理用户个人信息无须事先征得信息主体的同意。⑫这种“同意的例外”表明了网络服务提供者协助执法义务的优先性，公民的隐私及数据权利被平衡掉了。但问题在于，网络服务提供者仅是用户个人数据的持有者，而非基本权利拥有者。即使基于合法事由进行数据披露，也要考虑数据主体根据其与网络服务提供者之间的关系而提出的“合理预期”，要充分考量个人数据的类型及对用户的影响，“能否适用平衡条款在很大程度上取决于案件的

具体情况。然而,隐私和数据保护的基本权利始终是平衡的一个因素,它们不可能被轻易地超越,而且应该占据较高的权重。"[13]面对刑事数据调取,网络服务提供者应有更多的考量,扮演更重要的角色。

二、刑事数据调取中网络服务提供者的角色定位及相关义务

作为刑事数据调取的"数据池"及数据保护义务的当然主体,网络服务提供者理应成为刑事侦查的重要参与力量而非仅是配合者。而要实现此转变,需探讨网络服务提供者在刑事侦查中所扮演的角色,并由此界定其义务。之所以遵循这个分析路径,是因为不同的身份(或角色)跟特定的权利、义务、权力、责任相连,"身份体是人们赖以生存和发展的组织或群体……身份体作为利益配置单位,通过确定成员身份界定身份体内外关系,实现其内部身份关系的制度安排。"[14]在基本法律要素配置方面,依"身"定"份"是公平正义的体现,下将立足于"经营者""公共服务提供者"和"网络规则重要缔造者"三重角色并展开其关联义务之阐述。

(一)经营者——隐私及数据保护义务

网络服务提供者的初始角色就是经营者,通过提供网络服务以获取利润,即使是"免费"使用的App,经营者也能通过获取用户的海量个人信息并经"个性化推荐"赚取利润。与"经营者"身份相对应,网络服务提供者的主要义务是保障用户的隐私及数据安全。具体而言,可以从以下三个方面予以分解:第一,法律条文中涉及网络服务商"应当如何""不得如何"的内容,都是"义务"。前者如《民法典》第1035条,规定了处理个人信息处理应当遵循的基本原则,就是典型的义务总纲;后者如《民法典》第1038条,规定了信息处理者不得泄露、篡改或向他人非法提供个人信息。《网络安全法》《数据安全法》《个人信息保护法》等也都规定了网络服务提供者的隐私及数据保护义务。这种义务,从个人信息处理的各个节点出发,大体上可以分为数据收集阶段的义务(如充分告知并取得授权、必要性义务等)、数据存储阶段的义务(如安全保管、限期持有义务等)、数据处理阶段的义务(如合目的性义务等)、数据转移、披露或共享阶段的义务(如限制共享、重新取得授权义务等)。此外,贯穿个人信息处理各阶段的,还有数据安全义务、数据分级、分类保护义务、数据质量义务,以及尊重数据主体的各项数据权利等义务。第二,"从设计着手隐私"义务。今天的数字经济已经告别了野蛮生长,开始强调秩序。今天的数字经济已经从"追逐效率与利润"转向追求公平合理的制度设计。毫无疑问,消费者隐私及数据保护肯定是其中重要一环。历史地看,隐私及数据保护正在经历一个"先伤害、后弥补"的过程,未来的互联网企业隐私及数据保护义务应从设计着手隐私,"把隐私主动地嵌入数据开发与挖掘技术、商业操作、网络架构中,把隐私保护看作是数据资源利用的核心问题之一而不是依从性问题"。[15]第三,重要、敏感数据披露与共享时的"评估"及"告知"义务,这也是与协助执法义务最为相关的一项。《个人信息保护法》第55条规定,个人信息处理者应当对"向其他个人信息处理者提供个人信息、公开个人信息"及"其他对个人权益有重大影响的个人信息处理活动"两种情形事前进行风险评估。显然,刑事侦查中的个人数据调取对当事人影响及风险不可谓不大,网络服务提供者在协助执法过程中应评估数据披露带来的可能后果,并在重要或敏感数据披露后,在排除"保守国家秘密""不利于后续侦查"等事由的前提下,向相关数据主体履行告知义务。

需要说明的是,上述三个层面的分解都是基于法律义务而非道德义务,即使是"从设计着手隐私",也应放置在"数据合规"的背景下,将其定性为法律义务。《数据安全法》第27条和第28条就鲜明地体现了这一点——数据处理前就应考虑隐私及数据权利问题。

(二)公共服务提供者——协助执法义务

通过考察相关法律文本,我们发现网络服务提供者背负的法律义务大致包括协助执法、数据留存、保护用户信息、管控违法信息和违法活动四类。[16]这四类涵盖了对"私"和对"公"两方面,尤其是对"公",从社会治理角度讲,"企业某种程度上转化为监管者的延伸,集中表现为政府监管职责的下移;其所承担

的信息收集、存储、审查、监控、披露、报告义务直接服务于执法活动。”[17]张新宝教授也指出,“守门人”企业借助技术和管理优势在互联网生态系统中具有强大控制力,在权力结构上具有“公”的属性。[18]此即网络服务提供者基于另一种身份而背负的义务——公共服务提供者及其协助执法义务。一方面,新公共行政理论改变了以往的“单一决策”而与其他行动者共同决策,从以“政府为中心”转向“以公众为中心”,[19]其路径正是通过合作、协商、伙伴关系,共同实现对公共事务的治理;另一方面,网络服务商具有资本、技术、数据、平台等方面的优势,由其协助执法具有便宜性。

具体而言,该义务可分解为如下三种:第一,信息收集及存储义务。依发现嫌疑的主体不同,分为辅助和主动的信息收集及保存义务。前者指执法机关发现特定嫌疑后,网络服务提供者的辅助执法义务。如《网络安全法》第50条规定网络运营者在收到有关部门就违法信息停止传输的命令后,要保存相关记录;后者指网络服务商主动发现违法违规信息时,在向有关部门报告的同时,负有保存相关记录的义务。如《互联网群组信息服务管理规定》第11条规定,服务提供者除依法采取处置措施外,还要保存有关记录,并向有关主管部门报告。此外,信息收集及存储也有时限规定,如《互联网直播服务管理规定》第16条、《互联网群组信息服务管理规定》第13条也分别规定了六十日、不少于六个月的留存期限。第二,审查监控义务。这可分为一般审查监控义务和特殊审查监控义务两种,前者指网络服务提供者在日常经营中承担的信息审查监控义务,如《网络安全法》第47条,当出现监控不力时,还可能引发《刑法》第286条的“拒不履行信息网络安全管理义务罪”;后者是针对个案,对已形成嫌疑的特定主体进行的信息审查监控。第三,信息披露与报告义务。此义务与前述两种义务相连,同样可分为“基于一般信息收集与审查监控所产生的违法信息报告义务”和“个案执法中的信息披露义务”。综上,三种义务在“常态”与“特殊状态”两个语境下是一脉相承的,而特殊状态时的数据收集、审查监控及披露义务正是刑事数据调取中网络服务提供者协助义务的典型样态。

(三)网络规则重要缔造者——参与塑造自由与开放的数字生态义务

除经营者、公共服务提供者外,网络服务提供者还有一层重要的身份,即网络规则重要缔造者。换言之,数字时代的网络服务提供者不是在反映而是在塑造某种社会规范,[20]其工具便是“代码”。“代码构筑了网络空间,空间使个人和群体能或不能。”[21]那么,网络服务提供者如何通过代码规训互联网的呢?主要分两步:第一步,通过“缺省性规则”事先设定网络空间的权利义务分配。缺省性规则的意义在于,其对于权利义务的初始分配将自动生效。“缺省性规则的内容及其偏袒性问题是先契约的,即存在于当事人通过谈判达成契约去做出修改之前。”[22]在民众进入网络空间之前,初始权利义务的分配已经设定完成。第二步,通过协议。“协议造就了管理数字生活的法律制度……服务条款、保密条款、授权协议和其他法律文件都是数字生活中的指导性工具……同时也是新法律制度的起点。”[23]各类协议事实上承担了数字生活中“法律”的地位,民众进入网络空间之后,二次权利义务的分配以“协议”方式完成。就此而言,今天的互联网和智能产品企业就像是一个世纪前的铁路公司和电报电话公司,它们“创造和统治着我们的交流空间,并因此控制着我们的生活,这种控制程度远远超过其他任何私人群体。”[24]

如果现实世界的首要主体是自然人,那网络空间的首要主体就是网络服务提供者。网络服务提供者在“提供新的服务方式的同时,也确立了该服务方式下基本的信息交换规范和网络社区的基本伦理。”[25]尤其是互联网巨头们倾力打造的数字平台,更是汇集成一个个功能强大的生态系统。那么,迅速扩张的互联网巨头们,负有何等相应的义务呢?代码既可以创造一个自由的世界,也可以创造一个沉重且充满压迫的世界。作为一种治理模式的代码,它“不能简化为法律,也不能简化为市场……这种治理模式应该认可并允许以下情况:各种人造物品和架构以种种方式对用户进行‘设定’,其中涉及的方

式应该受到检查”。[26]不同的(网络空间)版本支持不同的梦想,对网络服务提供者来说,参与塑造自由、开放的数字生态环境是其应承担的商业伦理和法律义务。

具体而言,提出两个层面的要求:第一,遵循合法性,将现代法的价值当作网络服务提供者们数据处理活动的最高准则。《数据安全法》第8条规定,数据处理应当遵守法律、法规,尊重社会公德和伦理,遵守商业道德和职业道德,承担社会责任。事实上,该条对网络服务提供者提出了超越法律义务范围的要求,目前虽没有明确的条款或文件指明这些伦理内涵有哪些,但不能否认,互联网的本性就是自由和开放,网络服务提供者有义务将其作为行动纲领,而不得肆意违反。第二,保障个体民主参与网络治理和网络生态建设的权利。网络服务提供者往往通过算法进行社会治理,将个体视为算法治理的对象。英国有个发生于2013年的案例,41岁的残疾人马克·海明斯拨打了急救服务电话“999”,并立刻向接线员反映了他的病情。接线员先是问了一个问题:“还有其他症状吗?”接下来询问了更多问题:“你有腹泻或呕吐吗?”“你的上腹部有没有压迫感或刺痛感?”“你先前有没有诊断出其他病症?”在病痛的煎熬中,海明斯无奈又痛苦地回答了所有问题,并第三次请求派救护车。通话结束前,接线员得出结论:“从你反馈的情况看,你不需要救护车。”两天后,海明斯被发现且不久就去世了,死因是胆结石阻碍胰管引发的心脏病。原本只需要一个常规手术就可救治的病,却因救助中心的算法分诊系统而丧命。海明斯的遭遇点明了一个残酷的现实,就是在算法世界中,“事态的发展方向,已经为他设定好了。他不能拒绝与接线员交谈,也不知道‘需要急救’和‘不需要急救’(这样的算法分类)的存在。他只是在事先安排好的‘水体’中生活。”[27]这就是公民话语在数字生态建设过程中的参与缺失。

三、刑事数据调取中网络服务提供者多重义务的对立性并存

网络服务提供者“三位一体”的身份,决定了其在刑事侦查中必然产生各类义务的并存。欧洲刑警组织于2021年发布了SIRJUS项目第三次报告,报告指出,当前欧洲各国向企业调取数据时,企业延迟或拒绝配合的理由主要有九种,既有实质性原因如缺少法律依据或依据不准确、调取请求中相对人错误、没有相关数据,也有程序性原因如申请不符合企业程序、申请内容过于宽泛、申请缺乏案件性质的必要信息、缺少有效的身份验证等。[28]这些理由典型地反映出刑事数据调取中附着于网络服务提供者身上的多重义务以及在多重义务间的权衡。而之所以在网络服务提供者身上聚集多重义务,根本原因在于个人信息承载了多种价值和追求。需要保障的权益类型如此多,需要履行的义务种类也随之产生,并以一种对立性并存的方式体现出来。

(一)数据披露与数据保护

刑事数据调取中网络服务提供者背负的典型对立性义务就是数据披露和数据保护,前者指向“公”,后者指向“私”,前者的典型行为是“向侦查机关披露个人信息”,后者的典型行为是“限制共享、保护隐私”。两类义务的冲突性对立既有观念层面的,又有具体义务履行层面的。

观念层面上,数据披露与数据保护背后的考量是安全与隐私的对立。人们往往将隐私与安全置于天平的两端,并认为在打击犯罪面前无隐私。确实,恐怖袭击、绑架、儿童买卖与儿童色情犯罪、毒品交易等严重犯罪无时无刻不在触动人们的神经,立法者深知:“选民们对刑法理论知之甚少,但大致能够明白自己乐意看到何种结果:即犯下选民们所畏惧之罪行的人,他们应受到定罪和惩罚。因而人们可以合理地假设,立法者乐于制造这些结果,从而继续获得选民的推举。”[29]换言之,在刑事诉讼领域,立法者“并不在乎被追诉人的权利”,立法机关无法创造出能够保护他人隐私的刑事诉讼规则,因为大多数选民是将自己视为潜在的犯罪受害者,而不是犯罪者。“许多人愿意接受在政府面前隐私越来越少的事实,因为对那些害怕的人而言,隐私是可有可无的奢侈品”。[30]但我们也该清醒地认识到,在案件侦破与隐私的利益衡量中,前者并不是压倒性考量因素。2013年斯诺登事件后,《华政顿邮报》联合美国皮尤

研究中心进行了一份调查，其中56%的调查者认为为了应对恐怖主义允许国家安全局追踪美国人的通话记录；[31]波士顿马拉松爆炸案后，《时代周刊》联合美国有线电视新闻网又发起一次民意调查，61%的美国人表示，与反恐相比，他们更担忧政府借用反恐名义制定新的安全政策，49%的受访者表示不愿意为了反恐而牺牲自由和隐私。[32]更值得重视的是，隐私是一种基础性价值，隐私本身意味着一种安全。试想打着“公共安全”的名义牺牲不特定多数人的隐私，这是不是用“安全”换取“安全”？现代社会是风险社会，“不确定性的丧失给人们带来漂浮感和焦虑感，使得人们越来越期待未来的风险能在当下获得解决……随着人类掌握信息能力的提升，往往导致人们越来越倾向于将风险当作危险来加以处理……这导致了一种极为强烈的对未来进行全面控制的妄念。”[33]

具体义务履行层面的对立性并存表现更多，这里以“加密”为例。加密是保障在线隐私及安全的重要因素，也是网络服务提供者履行“设计和默认的数据保护”义务的体现，该义务不仅体现于一般性的数据保护法，也适用于专门性的刑事司法，(EU)2016/680第20条即规定了该义务。但在是否为国家安全机关开放应用程序权限或给加密系统开后门的激烈争议中，网络服务提供者往往陷入选择的两难。2022年9月16日，联合国发布了名为《数字时代的隐私权》的报告，报告中指出：“联合国大会和人权理事会在一些决议中强调了加密技术在保障人权方面的重要性，呼吁各国不要干涉加密技术……但各国政府时常会限制加密的使用”。[34]通常情况下，网络服务提供者既可以采用托管加密，也可采用端对端加密，两者的区别在于是否存在通信双方以外的包括服务提供者在内的第三方拥有通信密钥。一般来说，托管加密因拥有更多的知情方，其加密系统被入侵的风险更高。但若服务商统一采用端对端加密，那不可避免会阻碍刑事数据的调取及案件的侦破。除加密技术外，网络服务提供者还常通过限制用户数据留存期限来提升用户的隐私和数据水平，如钉钉“密聊”、支付宝“悄悄话”等采用“阅后即焚”模式，这也给刑事数据调取带来“提供不能”的可能。

(二)辅助监控与信任维持

协助执法义务是一项框架性义务，既指向个案侦破中的数据披露，也指向常态下与预测警务相关联的辅助监控。网络服务提供者辅助监控义务凸显了当前国家在数字治理中的两个倾向：一是“储存一切”而非“有需要时再去获取”，二是政府与互联网企业的协作共治。在“国家管平台，平台管用户”的数据治理模式下，[35]公权力机关对特定主体的监控，离不开网络服务提供者的协助。尤其是预测警务的出现，这一新型数据治理方式因缺乏必要的法律规制，使得以下观察至为重要：“公共和私人数据正在走向混合……数据的丰富也使得个人和非个人数据之间的区别变得毫无意义……更重要的是，不同类型(个人)数据与授予它们的保护水平之间的法律差异正在被掏空”。[36]Douglas法官严肃地向社会发出警告：“社会越来越容忍政府利用公民的体己获得公民的私人信息：我们生活在一个危险的社会中，政府随时可能侵入公民秘密的私生活领域。”[37]

而一旦企业数据库向政府开放，民众可能对两者都失去信任。信任在数字治理和数字经济中占据重要地位。就前者而言，如德国1983年进行的人口普查，公众的抗拒心是如此之强，以至于这项普查四年之后才真正展开。接下来的一次人口普查则生生推迟到了2011年，还充满了虚假的注册信息。[38]就后者而言，信任缺失对数字经济带来致命打击。原本，用户基于“相信企业会保护且不会滥用”才将个人信息提供给网络服务提供者，这种“数字信任”蕴含着用户对数字产品与网络服务提供者利用个人数据是使其受益而非致损的基本信念。[39]这种信任也是部分学者在数据隐私保护领域引入“信义义务”的根基之一。[40]信义义务是作为强势一方的网络服务提供者对那些因为接受信任邀请而处于不利地位的用户产生的关照、保密和忠诚义务，越是平台型网络服务提供者，对用户的控制度越高，对信义义务的要求度越高。[41]而信任维持义务之证成除“信义义务”理据外，还可从《个人信息保护法》中的“诚信原则”及数据治理的“法律与伦理”并举(如《数据安全法》第8

条)推出。就此而言,信任维持义务的具体指向是在“法律”和“协议”的范围内收集、使用用户数据,不能超出用户提供个人数据时的合理预期。商业实践中,保护消费者隐私、赢得客户信任成为众多互联网企业塑造品牌形象的良机。2006年,美国司法部以传票形式要求谷歌披露用户近两个月的搜索记录,遭到谷歌拒绝。谷歌富有创造力地提出,“失去用户信息的潜在风险”对谷歌而言是一种“负担”。[42]苹果公司也曾因拒绝政府请求披露用户信息而广受赞誉。2015年12月,美国加州圣贝纳迪诺发生严重恐怖袭击,FBI查获了犯罪嫌疑人赛义德·法鲁克的苹果手机,苹果总裁蒂姆·库克不仅拒绝给手机解锁,还发布公开信称FBI的要求“破坏了我们的政府旨在保护的那种权利和自由”。[43]

(三)权力遵从与权利制衡

现实生活中,鲜有网络服务提供者能抗拒基于刑事侦查需求而进行的协助执法义务,直观原因就在于刑事侦查行为的“权力属性”。2013年,雅虎首席执行官玛丽莎·梅耶尔在解释为什么雅虎没有保护其用户隐私时称,“如果你不遵守,这是叛国罪。”[44]可见,“权力属性”比“义务设定”更容易让网络服务提供者配合,“权力”因素也比“权利”事宜更受到网络服务提供者的重视,因为违抗权力的后果是显而易见的。但必须指出,这种基于“利害得失”的行为倾向虽合乎“常情”却不符合“法理”。面对刑事数据调取行为的扩张趋势,网络服务提供者是不加考虑地配合,还是审慎地决定每一次披露,这个选择不仅关系到刑事司法中的隐私及数据保护,也关系着如何“将权力关进制度的笼子里”。换言之,网络服务提供者在刑事数据调取中既应遵从权力,又应保障权利,并力图用权利制衡权力。

这里的权利既包括网络服务提供者自身的经营权利,也包括刑事侦查中的公民实体性权利(以隐私权和数据权利为典型)和程序性权利(以知情权为典型)。在数据法领域,相关法律规定了数据主体的各项权利,但“权利诉求的扩张并未同步强化权利主体实现该诉求的能力,相反,信息革命使得这种能力无论在识别侵害风险方面,还是在有效救济方面,均不断弱化。”[45]当然,这是世界范围内个人信息保护的难题,著名学者施瓦茨早有清醒认识:“数据挖掘与数据比对等大数据技术是对已经留存于社会各领域的海量数据进行后续深度应用的过程,只规范收集不规范使用的第四修正案及搜查法规范,导致在美国数据挖掘式的侦查行为基本上不受规范。”[46]相比个人,网络服务提供者的技术优势和社会资源更强,更容易在数据侦查中保障权利和制衡权力,比如它们可以通过技术设计、完善协助执法机制、程序性义务履行或舆论政策等来实现这一目标。

除对网络服务提供者抱有期待之外,也应正视网络服务提供者自身的权力及义务之违犯。平台型的企业权力在当代社会中有新的形式和特点,“它们不靠权利,而靠技术;不靠法律,而靠正常化;不靠惩罚,而靠控制。”[47]再者,掌控信息者拥有权力,因为信息是个人认知、判断和行为的前提,一方主体可以通过占有信息并控制另一方主体获取信息的渠道和程度,构成信息性权力的来源。[48]因此,在刑事数据调取中,网络服务提供者既不应盲目披露,又不应强强联合,而应清醒认知自己的多重义务,并在个案中审慎地作出决定。总之,在权力与权利的碰撞中,突出的一个表现就是“不平等”,这正是导致网络服务提供者三种义务中,协助执法义务是最容易被接受和执行,而一旦出现网络服务提供者拒绝向侦查机关披露用户数据事件都会引起广泛关注的原因。

四、网络服务提供者多重义务间的优先性及有限性

我国当前立法并未关注网络服务提供者在协助执法事宜中的义务协调问题,原因在于我国“一体调整”的立法模式,“立法者注意到了对国家机关处理个人信息的活动进行法律控制的必要性,但对国家机关处理个人信息的行为如何进行法律控制,仍是一个未完成的命题。”[49]个人信息的行政处理如此,个人信息的司法处理同样如此,这也是欧盟在制定GDPR不久随即出台(EU)2016/680指令的原因。相关规则的缺位必然使得网络服务提供者面临多重义务冲突,继而需要考虑多重义务间的优先性和有限性问题。

(一)多重义务履行的优先性探讨

对这个问题的探讨从2008年欧洲人权法院审理的K.U. v. Finland案[50]说起。该案中,嫌疑人在网站上虚构了一名未成年女孩(年仅12岁)的性交易广告。侦查人员要求服务商提供嫌疑人的注册信息,服务商以芬兰相关立法中存在"保密条款"为由拒绝提供。受害人在穷尽本国救济无果后,诉至欧洲人权法院。法院认为,本案中服务商基于隐私权保护所产生的保密义务不足以阻却侦查机关获取相关信息的诉求。显然,本案中隐私保护义务与协助执法义务之间,后者胜出。该案件的最终处理结果是芬兰修改了相关法律,2021年欧盟制定条例授权特定网络信息业者为打击网络儿童色情之目的,主动监测、评估和报告可疑信息或行为,同时规定企业关于此类用户个人信息处理的活动不适用GDPR相关规定。[51]

在我国,《民法典》和相关数据保护类法律都有"基于国家安全、重大社会公共利益等"个人信息保护义务的例外条款,这些例外条款所要保护的价值构成了信息保护义务的限制因素。换句话说,"例外"成为义务冲突时的首要选择——网络服务提供者的协助执法义务与数据保护义务并非平行关系,而是存在优先性。这很容易理解,GDPR第6条规定了六种合法性基础,GDPR第9条第1款规定了禁止处理特殊类型个人数据,第2款就规定了例外情形。形式上看例举了数据处理的正当理由,实质上却是法律要保护的多种法益以及优先顺序——所要保护的法益越重要,该行为背后的义务越是具有优先性。由此,义务履行之优先顺序转换成了利益衡量问题。

法律规定的"例外条款"之本质就是为了保护国家利益或社会公共利益而暂时对企业或个人利益进行限制,也因此,对网络服务提供者而言,如果协助执法义务有助于实现国家安全或社会安全,那该义务自然优先于隐私及数据保护义务。这也符合大多数人的日常判断——安全胜于隐私,因为只要触及刑事犯罪,就与"安全"脱不开干系。事实上,人们很少将"安全"与"隐私"放在同一个天平的两端,总是下意识地"用隐私换取安全"。但是,这是一种"一刀切"式的权衡。一方面,"不安全的代价是真实且触目惊心的,失去隐私的代价则是抽象而模糊的。并且只有在某人面对泄密后果时,这个代价才会变得具体明确。这就是为什么当我们拥有隐私的时候,会低估它的价值,而当我们失去时,才认识到它的真正价值。"[52]另一方面,在刑事侦查中探讨公共利益,不能仅指向案件受害者利益,也不单指向案件的顺利侦破和打击犯罪,更非迅速抓到坏人后、消除恐惧的公众安全感,而是要糅合各种利益于一身,并在此过程中提炼公共利益。从这方面讲,公共利益的认定需要"可能被牺牲或限制的一方利益主体"的积极参与和对话,否则,其"公共性"会受到质疑。

所以,一切并非想象的那么简单。首先,国家利益、公共利益和个人利益都是"不确定性概念",存在大量的模糊地带,需要在个案中发现、论证和阐释。再加上时机处于刑事侦查阶段,任何一种义务的履行对国家、社会、经营者或个人都可能产生重大影响。第29条工作组(欧洲数据保护委员会前身)曾出具一份"为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚目的"而进行数据处理的意见,认为"对本宪章承认的权利和自由的任何限制都必须由法律明文规定,并尊重其本质。在遵守相称性原则的前提下,可以并仅在必要且真正符合普遍利益的目标时进行限制……对私人生活的干扰、对个人数据的干预应仅限于必要且与可预见的普遍利益目标相称,即预防、调查、侦查或起诉刑事犯罪或执行犯罪处罚……这些例外或限制条款应作狭义解释,尤其是事关公民的基本权利。处理个人数据应有充分的保障,并保证完全的问责制和透明。"[53]可见,尽管欧盟也认可数据控制者或处理者有协助执法的义务,但该义务之履行并非没有条件,当该义务之履行不符合"相称性"、对"公共利益"做任意扩大性解释或者"问责制缺失"时,数据控制者有正当理由拒绝履行义务。(EU)2016/680指令更是在29条工作组意见的基础上,将刑事司法领域的个人信息处理规则进行了细化,尤其是第三章"数据主体权利"、第四章"控制者和处理者义务"和第六章"独立监管机构",

权力与权利明确，义务与责任清晰，当执法机关做出违背该指令的数据处理行为时，网络服务提供者有充足的理由拒绝披露，或者转向独立的监管机构寻求有效救济。其次，从行动来看，网络服务提供者多种义务间的优先性考量应纳入“数据保护影响评估”中来，并在评估中作出判断。无论GDPR(第35条)还是我国《个人信息保护法》(第55条)都规定了数据处理者该义务，(EU)2016/680指令第27条亦规定了该义务——如果某种类型的处理，特别是使用新技术，并考虑到处理的性质、范围、背景和目的，可能会对自然人的权利和自由造成高风险，数据控制者和处理者应进行数据保护影响评估，同时应考虑为应对这些风险而设想的保障措施、安全措施以及其他确保保护个人数据和证明遵守本指令的机制。基于权力扩张的天性，寄希望于侦查机关自缚手脚、保守谦抑是不可能的，唯有网络服务提供者(尤其是守门人企业)积极参与到刑事数据调取中来，设置协助机制的审查门槛，对数据调取的法律依据、案件性质、当事人适格、法律程序、数据类型、数据影响、权利告知等作出判断，更好地履行其法律义务。

(二)多重义务履行的有限性界定

对网络服务提供者而言，义务的履行有先后，义务的履行也有限度。以加密为例，2020年初，苹果公司第三次拒绝在其加密服务中为刑事执法机关开设后门，一方面是这种后门设置需要调整iOS系统进而影响所有用户，另一方面是后门一旦存在，将不可避免地为犯罪分子所利用。[54]联合国《数字时代的隐私权》报告也就此发表意见：第一，对加密的管制有可能损害人权，试图限制加密的政府通常无法证明它们所施加的限制对于满足特定的合法利益是必要的，因为有各种其他手段和方法为执法或其他合法目的提供所需信息；第二，大多数加密限制对隐私权和相关权利的影响不符合比例原则，因为此举不仅影响目标个人，还会影响到广大民众；第三，加密工具中的强制“后门”所产生的责任远远大于其被认定为犯罪嫌疑人或安全威胁的特定用户的用处。[55]可见，尽管各方对加密及管制的立场和看法有所不同，但有一点是确定的，即网络服务提供者应在多重义务间进行平衡，义务的履行要适度，不可轻易牺牲任何一方正当权益。

第一，刑事司法中的数据保护义务有限。尽管一再强调刑事数据调取中的数据主体权利，但不容置疑的是，这种强调更多的是一种防御性权利，体现在侦查机关和网络服务提供者身上就是一种消极保护义务。亦即，刑事侦查领域中的数据主体权利克减是案件侦破、打击犯罪的必然现象，“保护受刑事调查或参与刑事调查的人的基本权利并没有错，但暗示(通过引入数据主体权利)他们可以控制并同意或反对处理其数据的建议是不合适的”。[56]此外，在“隐私与安全”的背景下讨论刑事数据调取，采用更严格的规则和更有效的方式处理用于执法目的的个人数据，才有可能实现更高的隐私和数据保护标准。[57]

第二，网络服务提供者的协助执法和数据披露义务也有边界。Holmes谈到，刑事司法义务并非毫无边界，也并非以泛化的“打击犯罪”目的即可取得合法性，而是需要针对具体的刑事司法举措进行合比例的规制，并体现为刑诉法的明确规定。[58]这种限度可以从以下几个方面展开：首先，目的限制和法律依据方面，侦查机关在调取数据时，必须在《调取证据通知书》上载明案件大致情形、所调取数据与案件侦破之间的关系以及数据调取行为的法律依据，而网络服务提供者需对上述要素进行形式上的审查，网络服务提供者不能接受模糊的表述，如“打击犯罪”“保护公共利益”“打击恐怖主义”等，要有明确的指向。其次，所调取数据的类型、主体、事项需在《调取证据通知书》上阐明，这既是刑事数据调取合比例原则的要求，也是网络服务提供者履行协助执法义务的适当标准。数据类型方面，《数据安全法》第21条规定的数据分级、分类保护应有所体现；调取数据主体方面，嫌疑人、罪犯、被害人、证人等应有不同程度的数据披露范围；调取数据反映的事项方面，应与案件事实有高度关联性。最后，勇于拒绝侦查机关不合乎程序规范的数据调取请求。《数据安全法》第35条规定公安机关、国家安全机关调取数据需经“严格的批准手续”。2022年8月30日，最高法、最高检、

公安部联合发布《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》，第14条也规定了个人信息刑事调取行为的程序性规范，侦查机关应依规范而行。

第三，参与塑造网络空间数字生态义务应有底线与坚守。还是以韩国“N号房”事件为例，英国前首相特蕾莎·梅曾公开批评Telegram等小型平台可能会迅速被罪犯和恐怖分子占据。面对质疑，Telegram团队称：“近年来，像Facebook和谷歌这样的大型互联网公司已经成功劫持了隐私的话语权。他们的营销人员让公众相信，保护隐私最重要的是让帖子对特定对象不可见这类表面工具，从而让公众不去深究私人数据被交给营销人员和其他第三方的潜在问题。”Telegram强调，它的隐私理念中最重要的两点分别是保护私人谈话不被第三方(政府、雇主)窥探，以及保护个人数据不受第三方(如营销人员、广告商等)侵害。[59]Telegram团队对隐私的重视、对隐私规则的理解非常深刻，但也要认识到，隐私权从来就不是一项绝对性权利。刑事司法中，网络服务提供者片面地强调一种义务而完全忽视另一种义务都不可取。《数据安全法》第28条规定，开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。该条既是网络服务提供者数据保护义务的体现，也是其参与塑造网络空间数字生态的底线。这些数字生态主要涉及数据生命周期设计、加密系统是否应当为公权力机关开后门、数据控制主体对数据主体个人数据处理的限度、公私合作与公私独立的尺度、定期发布透明度报告等问题。

综上，网络服务提供者多重义务履行的优先性和有限性探讨都旨在规范刑事数据调取行为，核心目标是保障用户的正当权益及规制大数据侦查权，若“政府对于来自第三方的私人信息的处置被划到保护范围之外，其结果是，当政府搜查或起获由第三方持有的私人信息时，政府的行为既不需要具备合理性，也不需要任何司法授权。”[60]刑事数据调取中，网络服务提供者仅是个人信息的控制主体，不能替代用户(权利主体)决定是否放弃个人信息上所承载的基本权利。相关法律和实践将调取数据视为一种任意性侦查措施，无疑会对数据主体的隐私及数据权利等带来巨大危害。对网络服务提供者而言，协助执法仅是其履行法律义务的一个方面，作为网络空间规则的重要结构者和海量个人信息的持有者，不能对与其身份相关联的其他义务视而不见。

注释：

①See Carpenter v. United States, 138S. Ct.2206; 585 U.S. (2018).

②参见李延舜：《个人信息保护中的第三方当事人规则之反思》，载《法商研究》2022年第4期，第76-89页。

③蒋琳：《风暴眼中的Telegram：社交软件该为打击犯罪牺牲隐私吗?》，载微信公众号“隐私护卫队”，2020年4月11日。

④欧阳李宁：《共享单车肇事嫌疑人逃逸，企业不配合警方调查？ofo：误解》，载澎湃新闻网，https://m.thepaper.cn/newsDetail_forward_1704814，2022年12月8日访问。

⑤《滴滴8月27日将下线顺风车业务 两高管被免职》，载百度网，https://baijiahao.baidu.com/s?id=1609831384371336913&wfr=spider&for=pc，2022年12月8日访问。

⑥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161页。

⑦参见刘权：《论网络平台的数据报送义务》，载《当代法学》2019年第5期，第5-6页。

⑧参见谢登科：《论侦查机关电子数据调取权及其程序控制》，载《环球法律评论》2021年第1期，第60页。

⑨See Salome Viljoen, A Relational Theory of Data Governance, 131 The Yale Law Journal 573(2021).

⑩参见王锡锌：《国家保护视野中的个人信息权利束》，载《中国社会科学》2021年第11期，第115页。

⑪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161页。

⑫参见《微信隐私保护指引》，载微信官网，https://weixin.qq.com/cgi-bin/readtemplate?lang=zh_CN&t=weixin_agreement&s=privacy，2022年12月8日访问。

⑬[荷兰]玛农·奥斯特芬：《数据的边界》，曹博译，上海人民出版社2020年版，第150页。

⑭马俊驹、童列春：《身份制度的私法构造》，载《法学研究》2010年第2期，第59页。

⑮李延舜:《大数据时代信息隐私的保护问题研究》,载《河南社会科学》2017年第4期,第69页。

⑯参见皮勇:《论网络服务提供者的管理义务及刑事责任》,载《法商研究》2017年第5期,第14-25页。

⑰裴炜:《针对用户个人信息的网络服务提供者协助执法义务边界》,载《网络信息法学研究》2018年第1期,第33页。

⑱参见张新宝:《互联网生态"守门人"个人信息保护特别义务设置研究》,载《比较法研究》2021年第3期,第17页。

⑲参见竺乾威:《理解公共行政的新维度:政府与社会的互动》,载《中国行政管理》2020年第3期,第47页。

⑳See Jeffrey Rosen, The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google, 80 Fordham Law Review 1535(2012).

㉑[美]劳伦斯·莱斯格:《代码2.0:网络空间中的法律》,李旭、沈伟伟译,清华大学出版社2009年版,第98页。

㉒[美]弗兰克·H.伊斯特布鲁克等:《公司法的逻辑》,黄辉编译,法律出版社2016年版,第147页。

㉓[美]拉里·唐斯:《颠覆定律:指数级增长时代的新规则》,刘睿译,浙江人民出版社2014年版,第18页。

㉔郑戈:《算法的法律与法律的算法》,载《中国法律评论》2018年第2期,第84页。

㉕邹晓玫:《网络服务提供者之角色构造研究》,载《中南大学学报(社会科学版)》2017年第3期,第64页。

㉖Julie E. Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Life, New Haven, CT: Yale University Press, 2012, p.185.

㉗[美]约翰·切尼-利波尔德:《数据失控:算法时代的个体危机》,张昌宏译,电子工业出版社2019年版,第222页。

㉘See SIRIUS EU Digital Evidence Situation Report(3id Annual Report)2021,转引自裴炜:《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164-165页。

㉙William J. Stuntz, The Pathological Politics of Criminal Law, 100 Michigan Law Review 505, 529(2001).

㉚李延舜:《公共视频监控中的公民隐私权保护研究》,载《法律科学》2019年第3期,第57页。

㉛See Washington Post & Pew Research, Majority Views NSA Phone Tracking as Acceptable Anti- terror Tactic, Washington Post, June 10, 2013.

㉜参见[美]特蕾莎·M.佩顿、西奥多·克莱普尔:《大数据时代的隐私》,郑淑红译,上海科学技术出版社2017年版,第125页。

㉝鲁楠:《科技革命与法律演化的两个面相》,载《当代美国评论》2019年第1期,第75-76页。

㉞唐雨晰:《联合国〈数字时代的隐私权〉》,载微信公众号"网络法理论与实务前沿",2022年11月1日。

㉟参见单勇:《数字看门人与超大平台的犯罪治理》,载《法律科学》2022年第2期,第88页。

㊱Broeders, et al., Big Data and Security Policies: Towards a Framework for Regulating the Phases of Analytics and Use of Big Data, 33 Computer Law & Security Review 309, 321(2017).

㊲Soborn v. United States, 385 U.S. at 343(Douglas, J., Dissenting).

㊳参见[德]阿希姆·瓦姆巴赫、汉斯·克里斯蒂安·穆勒:《不安的变革:数字时代的市场竞争与大众福利》,钟佳睿等译,社会科学文献出版社2020年版,第91页。

㊴See Dennis D. Hirsch, Privacy, Public Goods, and the Tragedy of the Trust Commons: A Response to Professors Fairfield and Engel, 65 Duke Law Online 83(2016).

㊵参见吴伟光:《平台组织内网络企业对个人信息保护的信义义务》,载《中国法学》2021年第6期,第45-60页;解正山:《数据驱动时代的数据隐私保护——从个人控制到数据控制者信义义务》,载《法商研究》2020年第2期,第71-84页。

㊶See Jack M. Balkin, The Fiduciary Model of Privacy, 134 Harvard Law Review Forum 11, 33(2020).

㊷See Gonzales v. Google, Inc.234 F.R.D.674, 683(N.D. Cal.2006).

㊸Tim Cook, A Message to Our Customers, APPLE(Feb.16, 2016),转引自郑戈:《算法的法律与法律的算法》,载《中国法律评论》2018年第2期,第84页。

㊹Alex Dickinson, Yahoo CEO Feared Jail Over NSA Scandal, New York Post, September 12, 2013.

㊺裴炜:《个人信息大数据与刑事正当程序的冲突及其调和》,载《法学研究》2018年第2期,第47页。

㊻Paul M. Schwartz, Regulating Governmental Data Mining in the United States and Germany: Constitutional Courts, the State, and New Technology, 53 William and Mary Law Review 354(2011).

㊼[法]米歇尔·福柯:《福柯集》,杜小真选编,上海远东出版社2004年版,第343页。

㊽See B.H. Raven, Power and Social Influence, in Ivan Dale Steiner & Martin Fishbein(eds.), Current Studies in Social

Psychology, NY: Holt, Rinehart and Winston, 1965, p.127-145.

㊾王锡锌:《行政机关处理个人信息活动的合法性分析框架》,载《比较法研究》2022年第3期,第94页。

㊿ See K.U. v. Finland, no.2872/02, ECHR 2 December 2008.

(51) See Regulation(EU) 2021/1232 of the European Parliament and of the Council, https://eur-lex.europa.eu/legal-content/EN/TXT/uri=CELEX% 3A32021Rl232, last visited on October 15, 2022.

(52)[美]布鲁斯·施奈尔:《数据与监控——信息安全的隐形之战》,李先奇、黎秋玲译,金城出版社2018年版,第235页。

(53)第29条工作组:《关于主管当局为预防、调查、侦查或起诉刑事犯罪或执行刑事处罚以及以自由流动的目的处理个人数据的第03/2015意见》,载欧盟委员会官网,https://ec.europa.eu/newsroom/article29/items/itemType/1308, 2022年12月8日访问。

(54) See Daniel Howley, Apple's Tim Cook Defends Decision to Fight, DOJ on iPhone "Backdoor", Yahoo Finance, February 27, 2020.

(55)参见唐雨晰:《联合国〈数字时代的隐私权〉》,载微信公众号"网络法理论与实务前沿",2022年11月1日。

(56) Mark Leiser & Bart Custers, The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680, 5 European Data Protection LaW Review 367, 378(2019).

(57) See Sajfert Juraj & Quintel Teresa, Data Protection Directive(EU) 2016/680 for Police and Criminal Justice Authorities(December 1, 2017), Available at SSRN, https://ssrn.com/abstract=3285873, last visited on October 10, 2022.

(58) See Allison M. Holmes, Citizen Led Policing in the Digital Realm: Paedophile Hunters and Article 8 in the Case of Sutherland v Her Majesty's Advocate, 85 The Modern Law Review 219, 231(2022).

(59)参见蒋琳:《风暴眼中的Telegram:社交软件该为打击犯罪牺牲隐私吗?》,载微信公众号"隐私护卫队",2020年4月11日。

(60) Fred H. Care, Government Data Mining: The Need For a Legal Framework, 43 Harvard Civil Rights-Civil Liberties Law Review 485(2008).

Role Orientation and Related Obligations of Network Service Providers in Criminal Data Retrieval

Li Yanshun

Abstract: It has become the new normal for criminal investigation that Investigative agencies access data from Internet service providers, but also brings a series of practical operation and normative level problems, and endanger the privacy and data rights. To solve these problems, in addition to repositioning the attributes of data access investigation measures in the criminal procedure law, we can also start by regulating data disclosure practices. By defining the role of internet service providers in data investigation and clarifying their associated obligations, criminal data access behavior is thereby regulated. Internet service providers play three roles: operators, public service providers and important network rule makers, and accordingly assume three obligations:"privacy and data protection""public service and assistance to law enforcement", and "participation in shaping a free and open digital ecology". Among them, the coexistence and game of different obligations, the priority of obligations, and the limited nature of each other's obligations are all issues worthy of in-depth discussion. Only by clarifying the system of obligations of network service providers and the fulfillment of obligations can we effectively balance the "national security and social public interest", the "privacy and data rights" of users and the "business interests" of internet service providers themselves.

Key words: internet service provider; criminal data access; data disclosure obligation; right of privacy