环球评论

# 数字时代刑事侦查与隐私权保护的界限

## ——以美国卡平特案大讨论为切入口

朱嘉珺

**内容提要**:手机基站定位信息作为一种能够揭示犯罪嫌疑人具体行为轨迹的电子数据,正在为警方新的取证热点。尽管该类数据涉及手机用户的个人信息,却为通信服务运营商所事实存储并处置。因此,围绕着手机基站定位信息的隐私性、权属纷争,以及警方进行手机搜查、证据采集的程序要求等,美国司法界以卡平特案为契机,在全国展开了激烈的争论。本案不仅涉及隐私信息标准的制定,还探讨了数字信息时代司法、执法有效性与公民隐私权益间的权衡问题,更进一步将问题延伸至了包括云计算、物联网在内的刑侦技术发展新领域。因此,对本案的研究不仅有助于了解美国在技术升级背景下对刑事侦查与隐私权保护界限的思考脉络,通过梳理其裁判沿革与理论发展,更可为我国隐私权保护标准的制定提供有益借鉴。

**关键词**:电子证据　隐私权　刑事侦查　大数据侦查　手机基站定位信息

朱嘉珺,苏州大学法学院讲师。



2018 年 6 月 22 日,美国联邦最高法院对万众瞩目的卡平特案〔1〕作出最终宣判,裁定警方从通信服务运营商那里获取的手机基站定位信息(Cell-Site Location Information, CSLI)——即手机与信号发射塔进行通信连接时产生的包含具体地理位置信息的做法,属于联邦宪法第四修正案中的"搜查"行为,需要搜查证。这是联邦最高法院首次将第四修正案的保护范畴拓展到了手机定位数据上,也是最高法院面对数字信息时代刑事侦查涉隐私权保护议题做出的首个裁决。自 2017 年最高法院从第六巡回区法院调取案件卷宗后,卡平特案就引发了各方的高度关注,谷歌、苹果、微软等十四家顶尖高新科技公司更

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

是联合提交了一份声明,呼吁对第四修正案进行革新。在持续了大半年的激烈交锋后,法院最终以 5:4 的意见比艰难地推翻了上诉法院支持警方的立场,认定在没有搜查证的情况下获取手机基站定位信息的做法属于违宪,并将案件发回重审。

本案虽已告一段落,但裁决书中的理论却被众多评论家视作具有里程碑式的意义,影响深远。“今天的裁决正确意识到了保护手机中高度敏感的定位数据的必要性,同时它还为保护其他敏感数字信息,包括电子邮件、智能家居装置,以及其他未来科技的案件指明了方向。”〔2〕美国社会之所以对卡平特案的反响如此强烈,是因为其触动了数字科技高速发展下的敏感神经——人们对数字信息所拥有的隐私权范畴。这不仅是美国社会的难题,也是包括中国在内的全世界的难题。根据 2019 年 8 月的统计数据,我国智能手机用户已超 8 亿。〔3〕 这意味着,智能手机已经完全融入并开始支配我们的日常生活。与此同时,刑事侦查也迎来了数字化变革,电子监控、网络追踪、个人信息数据采集等新型侦查手段不断涌现,尤其是智能手机,更是成为了当下刑事侦查的重点目标。在个人特质日益数字化的当下,以智能手机为代表的电子设备早已脱离了普通物品的范畴,它囊括了手机用户的社交、喜好、作息等众多私人生活信息要素,对它的窥探将无可避免地触及隐私。如今,对隐私等个人信息的侵犯已经成为了世界各国建设数字社会的“阿克琉斯之踵”,尤其在政府动用公权力进行数字侦查时,如何权衡执法效率与保障公民的隐私权之间的取舍,已经并将长期成为重要课题。本文即以卡平特案及其引发的全美大讨论为切入口,阐述美国在技术升级的情况下所面临的刑事侦查证据采集的隐私权难题,以及进行的裁判沿革与理论发展,并以此为鉴,探讨我国在数字时代解决刑事侦查与隐私权保护之间界限难题的进益之法。

## 一 卡平特案的案情综述与争议焦点

卡平特案从一起普通的刑事案件发展为推动美国司法改革的标志性案件,共历时 9 年。随着 2012 年琼斯案〔4〕和 2014 年莱利案〔5〕关于警方数字侦查涉嫌侵犯个人隐私权的宣判,美国司法界对高新技术条件下公权力与个人隐私保护的界限正在逐步勾勒,这也成为了“卡平特标准”最终制定的理论基础。

### (一)案件事实

2011 年 4 月,四人因持枪抢劫而被捕。警方通过联邦《存储通信法》的 § 2703(d)(以下简称“D 法令”),在一名嫌犯手机中获取了其与在逃同案犯的非法“交易记录”,其中就包括本案的诉讼当事人卡平特(Timothy Carpenter)。依据记录,警方除了取得涉案人

〔2〕 Louise Matsakis, The Supreme Court Just Greatly Strengthened Digital Privacy, *Wired*, June 22, 2018, https://www.wired.com/story/carpenter-v-united-states-supreme-court-digital-privacy/,最近访问时间[2020-04-29]。

〔3〕 中国网信网,“第 44 次《中国互联网络发展状况统计报告》”, http://www.cac.gov.cn/2019-08/30/c_1124938750.htm,最近访问时间[2020-04-29]。

〔4〕 United States v. Jones, 565 U.S. 400.

〔5〕 Riley v. California, 132 S. Ct. 2473.

员的身份信息、通话记录外，还有一项重要内容，就是在逃人员的手机基站定位信息，包括通话的拨出地和接入地信息。根据手机基站定位信息，警方证实了嫌疑人的手机在每一起抢劫实施时都处于犯罪发生地0.5英里到2英里范围内，并据此对所有嫌疑人提起了涉嫌持枪抢劫的刑事诉讼。一审被定罪后，卡平特及其同伙桑德斯(Sanders)提起了上诉。

在向第六巡回区法院提起的上诉中，卡平特的理由是，警方根据D法令获取手机基站定位信息的做法是违宪的，因为要符合“第四修正案”中定义的“搜查”，必须基于相当理由标准获得搜查证，而本案探员却绕过了该环节，仅是从治安法官处获得搜查令就开展了对涉案当事人的隐私信息调查，由此获得的证据信息必须予以排除。上诉法院否定了该理由，认为公诉方用以定罪的关键证据手机基站定位信息属于商业记录，并非个人隐私，不受宪法保护。随后联邦最高法院正式受理该案。

(二)核心争议焦点

本案的争议焦点在于“第四修正案”对隐私权的保护范畴以及手机基站定位信息的具体属性。在以大法官罗伯茨(Roberts)为首的法庭意见看来，1967年卡马拉案〔6〕的判决，已经将第四修正案的立法目的明确，即“保护个人的隐私和安全免受政府的强权入侵”，确认了“保护个人，而非保护领地”的立场。由此，案件的核心旨在确定手机基站定位信息是否属于个人隐私。

无线通讯公司的数据库存有大量手机和信号发射塔(也就是基站)的信息传输记录，这些手机基站定位信息同时也反映了手机机主行经的地点，因此成为了检方认定机主与案件存在关联的重要证据。关于其属性如何确定，多数派意见指出：“这类数据资料——由第三方掌握的个人定位信息——并不完全契合此前的所有先例。相反，对定位记录的请求更像是横跨于两条解决隐私权的不同路径的特例。”〔7〕这里所指的两条解决路径，分别是以诺茨案〔8〕和琼斯案〔9〕为代表的处理定位追踪的案件，以及以史密斯案〔10〕和米勒案〔11〕为代表的处理调取个人信息的案件。

根据先例，涉及定位追踪装置的侦查，重点在仪器的精密度上，利用GPS实施长期追踪被认为是对个人隐私权的侵犯，因此警方必须申请搜查证；而涉及调取个人信息的案件，重点在被调取信息是否属于商业信息，如果是，则可适用第四修正案的例外原则——“第三方准则”，信息所有人在自愿将个人信息泄露给第三方时已经放弃了享有第四修正案的隐私权保护。然而多数派认为，手机基站定位信息并不属于这两种情况。一方面，与GPS记录车辆的运行轨迹不同，手机基站定位信息记录的是个人移动轨迹，“提供了一个窥视他人生活的便捷窗口”，包括家庭、政治、宗教和性关系在内，五年的数据保留期“给予了警察接触此前未知信息的机会”。〔12〕因此，它揭示的个人信息量和敏感程度具有无

〔6〕 Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523, 528 (1967).

〔7〕 Carpenter v. United States, 138 S. Ct. 2206; 585 U.S. (2018), p. 7.

〔8〕 United States v. Knotts, 460 U.S. 276 (1983).

〔9〕 United States v. Jones, 565 U.S. 400 (2012).

〔10〕 Smith v. Maryland, 442 U.S. 735 (1976).

〔11〕 United States v. Miller, 425 U.S. 435 (1979).

〔12〕 See Carpenter v. United States, 138 S. Ct. 2206; 585 U.S. (2018), p. 12 - 13.

可比拟性。另一方面,不同于银行交易记录和电话外拨记录,机主对后台定位信息的授权并非自愿。在信息社会,由于个人无法选择脱离手机和网络,也就意味着机主被迫承担了与电信公司共享定位数据的风险。但是,第三方拥有定位信息的事实并不能超越机主对该信息享有的隐私权。

与此同时,以肯尼迪(Kennedy)法官为首的少数派却并不认同上述观点,理由主要包括:(1)目前电信公司可对手机基站定位信息进行公开合法的交易,且市场估值极高,所以此类信息属于商业数据;(2)此类信息存储于电信公司数据库的事实,使得机主无法主张对相关信息的所有权或处分权,因而并不适用第四修正案的"合理的隐私权期待"标准;(3)此类信息揭示的隐私性并没有超过商业记录的范畴,可适用"第三方准则";(4)过分限制警方的搜查权限将给司法效率带来严重打击,也会给许多原本合法且极具价值的调查行为带来威胁。[13]

可以看到,多数派与少数派的意见形成如此大的反差,主要在于不同于以往任何信息,手机基站定位信息兼具了对个人具体信息的关联和对第三方的商业价值,而其认定又同时关乎对个人隐私权的保护与对司法效率的隐忧。因此,尽管最高法院最终认定,手机基站定位信息的本质所展露出的深度、广度和复杂度,以及收集该信息的不可避免性和自动性,都一再揭示出,第三方对此类信息的收集并不会贬损该信息获得第四修正案保护的价值,但法院决定谨慎适用判决结果,并强调既不会推翻之前其他案例的判决结果,也不会对监控技术和工具的使用进行质疑,更不会对定位信息的商业化利用持否定态度。

## 二 卡平特案争议背后的理论梳理

纵观卡平特案的各类争论,无一例外聚焦于如下三个问题:什么样的个人数据属于需要宪法保护的隐私信息?信息时代警方进行数字侦查涉嫌侵犯个人隐私权的判断标准该如何制定?当前的立法与司法该以怎样的态度来应对信息技术快速变革下的政府安保手段升级与个人隐私保护间的冲突?这三个问题依次递进,共同构成了当前刑事司法发展中不可回避的障碍。仔细梳理各路争议不难发现,问题的焦点"手机基站定位信息"背后分别站着三方——手机用户、电信网络运营商以及警方,而这三方同时又代表了数据内容关联人、数据实际控制人和政府部门。所以,问题的实质是围绕着电子数据所展开的个人隐私权、信息控制权和司法执法权之间的利益权衡,造成本案法庭意见如此撕裂的根本原因,正是各方利益侧重的结果。然而,这种利益的侧重绝非无的放矢,是有着深刻的立法轨迹和司法原则发展予以支撑的,因此,有必要对以"第四修正案"为基础发展出的电子侦查界限在审判原则上的理论沿革进行系统梳理以厘清卡平特案判决的关键作用和历史意义。

### (一)从传统向高技术环境演进的"第四修正案"裁判标准

1792 年通过的《美国联邦宪法第四修正案》(*U. S. Const. amend. IV*),旨在保护"人民

〔13〕 See Carpenter v. United States, 138 S. Ct. 2206; 585 U. S. (2018), pp. 17 – 18.

的人身、住宅、文件和财产不受无理的搜查和扣押;除根据相当理由证明标准,经口头或书面宣誓,且具体说明搜查地点和扣押的人或物外,不得签发搜查和扣押证”。经过两百多年的发展,目前联邦法院对执法机关的搜查取证行为是否属于“第四修正案”中需要符合相当理由证明标准的“搜查”,主要有两种判断方式:一种是建立在财产法基础上,以是否入侵他人不动产为基本原则的“入侵测试”(Trespass Test);另一种是以对个人隐私权的合理期待为主要内容的“卡兹测试”(Katz Test)。

**1. 早期的“入侵测试”**

“入侵测试”的判断标准非常清晰,即只要是侦查人员以获得信息为目的对嫌疑人的私人领域实施物理上的侵入,便构成“搜查”。由于该标准强调了“私人领域”(即不动产)和“物理入侵”两个明确的构成要素,在很长一段时间里,纯粹的监听手段并不被视为违宪。1928 年的奥姆斯特德案中,警方利用窃听器在公共街道上窃听嫌疑人室内通话的行为,由于不存在物理进入私人住宅或办公地的情况,从而不被法院判定为“搜查”。[14] 该案成为了早期判定窃听与搜查关系的标志性案件,该裁判标准一直被予以遵循,直至 20 世纪 60 年代“卡兹测试”的出现。

**2. 改进的“卡兹测试”**

“卡兹测试”来自 1967 年的卡兹案,由主审法官哈兰(Harlan)在认同意见中提出。该测试围绕着隐私权保护提出了两点要求:一是个人需要展现出对隐私权的主观期待;二是社会认同个人对隐私权的期待是合理的。“卡兹测试”不再从侦查行为的构成出发,而是立足于被侦查的信息,分别从个人与社会两个方面来衡量信息的隐私性,也被称为“合理的隐私权期待测试”。作为将“隐私权”的概念首次引入到第四修正案裁判标准中的案件,卡兹案扩大了宪法对个人隐私权的保护范畴,也终结了奥姆斯特德案开创的“公开场合窃听不构成搜查”的判决被遵循的历史。在卡兹案中,警方在公共电话亭内安装窃听器以窃听嫌疑人通话的行为被认定为“搜查”,因为窃听他人通话的行为违反了“个人合理的隐私权期待”。[15]

**3. “卡兹测试”的拓展之一:空中监视技术提升的影响**

侦查技术的不断升级衍生出的监听和监视两条路径格外引人关注。在前数字监控时代,监视主要依赖地面和空中观察,而根据“卡兹测试”,理论上,只要警方在公共场合以平常视角对嫌疑人的财物实施观察,都不属于第四修正案所规定的“搜查”,但这一判断标准在空中监视技术提升时遇到了挑战。

有三个时常被援引的典型判例,分别是 1986 年的瑟奥罗案、[16]道化工厂案[17]以及 1989 年的莱利案。[18] 三个案件均涉及警方动用飞行器进行空中监视,但对“合理的隐私权期待”标准却作了不同的注解:其一,在瑟奥罗案中,警方乘坐私人飞机在嫌疑人住宅

〔14〕 See Olmstead v. United States, 277 U. S. 438 (1928).

〔15〕 See Katz v. United States, 389 U. S. 347 (1967).

〔16〕 See California v. Ciraolo, 476 U. S. 207 (1986).

〔17〕 See Dow Chemical v. United States, 476 U. S. 227 (1986).

〔18〕 See Florida v. Riley, 488 U. S. 445 (1989).

上空进行拍摄。法院认为,私人飞机的飞行区域属于公共航道,由于任何人都可以乘坐飞机在该区域俯瞰,且不存在对私人领地的物理入侵,因而嫌疑人对这个视角不存在合理的隐私权期待。其二,在道化工厂案中,警方雇佣商业摄影师用航空测绘相机对工业大楼进行拍摄。由于该案动用的飞行设备和拍摄设备属于普通大众并不具有的高精度监控设备,因而被法院划入涉嫌侵犯隐私权的设备行列中。不过由于该案的侦查对象是对外开放的工业大楼,设备并未拍摄到私密细节,因此警方的行为依然不构成“搜查”。其三,在莱利案中,警方动用普通商用直升机在嫌疑人住处上空进行裸眼观察。因为该类型直升机十分常见,且行使在公共航道内,法院认定警方的行为不属于“搜查”。

从上述案件的法院意见中可以看出,尽管法院适用的裁判标准都是“卡兹测试”,但对“隐私权期待的合理化”判断却做了调整。瑟奥罗案中,法院只考虑了警方的监视地点;道化工厂案中,法院认为动用高精度设备的做法是超出公众对在此区域内不暴露隐私的期待的,属于技术越界;而莱利案虽然属于裸眼观测,法院依然对警方动用飞行器的型号和方式提出了要求。在这一期间,法院对警方监控技术能力的提升有所警惕,不过对技术是否越界的判断主要建立在公众的使用和认知上。

**4.“卡兹测试”的拓展之二:地面追踪手段升级引发的难题**

相较于空中监视领域,地面追踪技术的发展带给“卡兹测试”的考验更甚。从 20 世纪 80 年代的蜂鸣器,到 2000 年后的 GPS 追踪设备,再到如今手机基站定位信息定位,数字侦查设备的发展模糊了私人领域侵入的界限,让法院必须对“卡兹测试”不断作出修正。

(1)蜂鸣器追踪:公共空间与私人空间的严格界限

1983 年的诺茨案[19]和次年的卡罗案[20]是警方使用蜂鸣器进行侦查的标志性案件。诺茨案中,警方依靠在嫌疑人预购的化学品存储桶内安装蜂鸣器,追踪到了嫌疑人的制毒窝点。而卡罗案中,警方同样在嫌疑人购买的乙醚罐里安装蜂鸣器,却未实施追踪,而是为了获取对方在特定时间段内待在屋内活动的信息。法院的判决依据蜂鸣器使用的区域而发生了显著差异,前者发生在高速公路上,个人驾车行驶于公共道路被认为是自愿向任何人传递其定向穿越特定道路的事实,因而不存在合理的隐私权期待;而后者发生地点却是屋内,警方依靠接收屋内电子设备发出的讯息,对公共视角触及不到的情形进行无差别监控,将给嫌疑人在房屋中的隐私权益带来极大威胁。两案的判定给刑侦技术使用的合法界限作了清晰的划分,即使手段相似,在公共空间和私人空间的使用给个人造成的合理隐私权期待也是不同的。

(2)GPS 追踪:“马赛克”理论的形成

2012 年的琼斯案[21]是联邦最高法院审理的执法机构使用数字监控设备的真正第一案。不同于以往的监控手段,警方通过安装在嫌疑人车辆底盘上的 GPS,实现了对该车长

〔19〕 See United States v. Knotts, 460 U. S. 276 (1983).

〔20〕 See United States v. Karo, 468 U. S. 705 (1984).

〔21〕 See United States v. Jones, 565 U. S. 400 (2012).

达28天的追踪,并获得了2000页的行车轨迹数据集。GPS追踪打破了传统的、物理性的跟踪模式,在获取信息的密集度和持续度上也达到了前所未有的程度。对此,法院对"合理的隐私权期待"理论再次进行了修正:一是嫌疑人长达28天的移动轨迹能否可为一名普通人所全部观察到;二是社会能否期待警察可以在如此长的时间内掌握被监视人的每一个行踪。此外,本案还引出了新的问题——数字设备信息高度汇集可能引发对敏感信息的越界。法官阿利托(Alito)和索托马约尔(Sotomayor)强调,对个人位置信息的扫描超过一定时间,叠加的信息量足以揭示该人的生活轨迹和具体细节,实际增强了对他人隐私权的侵犯。这一论断首次直面了数字侦查技术突破性的弊端,被称为"马赛克理论"(mosaic theory),同时也是构成卡平特判决结果的关键理论。

(3)手机信息调取:法院直面智能手机的独特性

"马赛克理论"的提出,使司法系统开始正视数据汇集量与信息敏感度之间的关系。而2014年的莱利案,则是最高法院首次就智能手机高信息存储量的特殊性发表意见。该案主要讨论警察搜查被逮捕的嫌疑人手机是否需要再次申请搜查证的问题。根据逮捕附带搜查规则(Search Incident to Arrest, SITA),政府有权对依法逮捕的嫌疑人的周身财物进行搜查,然而这一例外是建立在周身财物揭示信息范围有限的前提下的。法院认为,智能手机在收集信息的方式、种类和规模上都与钱包、记事本、名片夹等随身携带的传统财物有着本质区别,"手机不仅以数字的形式包含了众多此前只能在家中找到的敏感记录,还囊括了大量以任何形式在家中也无法找到的记录"。[22] 据此,法院否定了逮捕附带搜查规则对手机搜查的适用,并认可了手机作为存有大量敏感信息的数字设备的独特性,是公权力利用个人手机进行侦查的里程碑式案例。可以说,正是有了上述案件裁决的层层铺垫,才有了卡平特案关于执法部门获取手机基站定位信息的最终认定的出台。

(二)立足于商业机构和执法部门的例外原则——"第三方准则"

作为在卡平特案讨论中被反复提及的理论,"第三方准则"初始并没有确定的概念,而是以例外的形式被法院适用和归纳,最终被学界概况为"如果信息为第三方所有或所知,则为第四修正案之目的,个人缺乏对上述信息的合理的隐私权期待"。[23] 还有一种更为简洁的表述,即"通过泄露给第三方,主体放弃了所有的对泄露信息的第四修正案权利"。[24] 可以看出,"第三方准则"的制定并非站在信息主体的立场上,而是考虑到了信息传输的多种可能,若主体和第三方之间存在合法合理的信息泄露,则构成主体对信息隐私权保护的自动放弃,也就为执法机构打开了一扇方便之门。追溯"第三方准则"的历史发展,关于信息主要存在两种分类模式:个人交谈与商业记录,以及元数据和内容信息。

1. 个人交谈与商业记录

(1)举报人系列案件的适用:"第三方准则"最早适用于1952年的昂李案。[25] 该案中被告将自己贩卖鸦片的罪行主动告诉了朋友,而朋友却是警方安插在他身边的线人,这位

〔22〕 See Riley v. California, 134 S. Ct. 2473 (2014), p. 2491.

〔23〕 Daniel J. Solove, A Taxonomy of Privacy, 154 *U. Pa. L. Rev.* 477, 526 (2006).

〔24〕 Orin S. Kerr, The Case for the Third-Party Doctrine, 107 *Mich. L. Rev.* 561, 563 (2009).

〔25〕 See On Lee v. United States, 343 U. S. 747 (1952).

朋友用便携式录音设备将对话内容录了下来,并最终成为检方起诉的重要证据。法院认为,虽然线人进行了秘密摄录,罪行却是被告主动告知的,作为谈话方之一,线人的录音行为并不构成窃听。该案的认定随后成为了一系列线人、举报人秘密录音案件的裁决依据。

(2)商业记录案件的拓展:对话理论进一步延伸,第三方商业机构开始成为"第四修正案"的适用例外。1976 年的史密斯案〔26〕和 1979 年的米勒案,〔27〕不仅是"第三方准则"涉商业记录的经典案例,也被认为构筑了该理论适用的最大范围。史密斯案的第三方是电信公司,通过让电信公司在嫌疑人家用电话上安装拨号记录器,警方获得了电话骚扰的记录。米勒案的第三方是银行,为证明被告购买了非法制酒的设备,检方要求法院传唤银行以提供被告的存款、支票等银行交易记录。两案的共同点在于要求第三方提供的信息都是被告主动告知的,无论是拨打的电话号码,还是进行的存贷交易,本质都是为了实现商业服务而进行的商业机构与被告的对话。因此,这里的第三方实际上是常规商业谈话的参与方,依据此前的线人对话理论,第四修正案并不禁止政府直接获取此类商业记录。

(3)委托性商业记录案件的局限:商业记录涵盖的范围是如此之广,无限度适用"第三方准则"势必会给第四修正案的保护形成冲击,因而史密斯案和米勒案裁决的适用一直饱受诟病。2001 年的弗格森案〔28〕中,警方依据医院提交的尿检报告,对毒品检测成阳性的被告提起诉讼。本案中关于普通医学检测报告是否适用"第三方准则"引发了争议。一方面,医疗检测报告属于医院提供医疗服务的证明,符合商业记录特征;另一方面,报告中包含了病人对医院保守身体健康秘密的信任与托付。因此,对"第三方准则"的适用需要进一步思考在违反信任关系的前提下,如警方得到其中一方的同意,获取信息是否构成"搜查"的问题。遗憾的是,法院回避了这一争议,这个问题久而未决,被斯卡利亚(Scalia)法官形容为"在第四修正案的法律体系内留的一道尺寸和形状未有定论的口子",争议也延续至今。〔29〕

**2. 元数据与内容信息**

(1)信息内容分类的开端:联邦法院对内容信息与元数据(非内容信息)的区分,最早来自于邮件。根据 1877 年杰克森申请案的法庭意见,警方不得随意搜查密封的信件和包裹,却可以直接审阅报纸、杂志等印刷品,后者不属于第四修正案保护的范畴。〔30〕这一认定的理论基础在于,密封的邮件和包裹中含有不想透露给非收件人的信息,而附赠的印刷品包含的信息原本就是对外公开的,所以无证搜查并不侵犯任何人的隐私权。由此,以寄件人的意愿为出发点,信息内容成为了"第三方准则"适用的原始理论基础。

(2)内容信息与元数据的区分:依据上述分类理论,密封的邮件同样包含两类信息,隐含在邮件内的信息,以及写在信封或包裹外的信息:前者是寄件人想要传递给收件人的

〔26〕 See Smith v. Maryland, 442 U. S. 735 (1976).

〔27〕 See United States v. Miller, 425 U. S. 435 (1979).

〔28〕 See Ferguson v. City of Charleston, 532 U. S. 67 (2001).

〔29〕 法官戈萨奇(Gorsuch)在卡平特案的反对意见中也提到了委托在商业记录中的意义,他指出,当委托人将数据(商业记录)委托给第三方时,并不等于丢失了任何在数据(商业记录)中所应当受到的第四修正案保护的权利。See Carpenter v. United States, 138 S. Ct. 2206; 585 U. S. (2018), GORSUCH J., dissenting, p. 14.

〔30〕 See Ex parte Jackson, 96 U. S. 727, 733 (1877).

讯息,后者则是寄件人为了投递邮件而传达给邮局的讯息。由此,邮件内是寄件人真正想要传达的内容信息,而邮件外则是实现商业交易的元数据,邮局只享有元数据的知情权和披露权。将类似情形作进一步延伸:如打电话实质存在双重交流,一重是拨号,可视作拨号人与电信公司的交流,电信公司接收到拨号指令后即连接上了接话人,第二重就是拨号人与接话人的直接对谈。可以看出,拨号指令相当于信封上的投递地址,是实现商业交易的必要信息,而通话内容相当于邮件中密封的讯息,是发出人真正想要传递的内容。由此,"第三方准则"事实上区分了元数据和内容信息的差异。

(3)内容信息与元数据的多重叠加:内容信息与元数据的区分曾在一定程度上有助于"第三方准则"的适用,成为认定警方侦查是否需要搜查证的重要指标。然而,随着数据信息的复杂化,这种分类对例外原则的适用开始出现阻碍。典型例子如电子邮件,由于地址和内容处于同一页面上,邮箱服务平台对邮件的扫描不可避免地会把内容信息一并包含进来,此时信息属性同时兼具元数据、内容信息、商业记录以及人际交流;再如在浏览器内输入 URLs 链接,特定的 URLs 链接明确指向特定的页面内容,然而 URLs 本身又由纯数据构成,兼具了元数据和内容信息以及商业记录的属性。[31] 随着全面数字信息化时代的到来,对信息的二元区分显然无法适应当前环境的需求。

## 三　卡平特案的评析:数字时代隐私权保护的重构

上述对美国电子侦查裁判理论发展的梳理可以看出,美国对个人隐私权保护的理解以财产法为基础,自不动产权属范畴开始延伸,同时涵盖个人与社会认知,随着科技发展而逐步超脱实物约束、具有高度抽象性的信息保护。随着司法理念对隐私权边界从有形向无形的突破,侦查目标信息内容量的激增也在反向制约着侦查手段的进一步升级。由此,当汇集了远程监控、数字追踪、商业数据采集、智能手机搜查等诸多难题于一身的卡平特案出现后,争议的引爆在所难免。尽管对"卡兹测试""第三方准则"以及紧急收缩政府电子侦查权限上存在着较大分歧,卡平特案带给人们深思的方向却是一致的,即数字时代如何构建刑事侦查与隐私权保护的界限,这不仅涉及对信息隐私性的量化,还涉及信息背后各方权益的协调以及对当前侦查环境数字化的长远审视。

### (一)搜查信息量的扩大化——隐私信息的标准重塑

什么是隐私权?根据雷蒙德·瓦克斯(Raymond Wacks)的说法,能被广为接受的隐私权定义仍未出现,不过最基本的含义是使人们能实现自我思考和感受的意愿。[32] 此处,"思考与感受"就是信息,而"自我"代表了独立与不受外界影响。早期人们认为,对隐私权的保护就是对信息载体(即实物)的保护,因而产生了基于财产法的"入侵测试"。直至卡兹案,法院对保护对象的关注从财产转向了人本身,也就有了"合理的隐私权期待"

〔31〕 See Peter C. Ormerod & Lawrence J. Trautman, A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age, *28 Alb. L. J. Sci. & Tech.* 73 (2018).

〔32〕 See Raymond Wacks, *Privacy: A Very Short Introduction*, Oxford University Press (2d ed, 2015), pp. 34 – 35.

测试。所谓期待,强调的是人的主观意愿,这种意愿既包含隐私信息所有权人自身的意愿,也包含社会主流人群的看法和意愿。由于意愿是抽象的,隐私权的保护界限开始日渐模糊,对隐私侦查的限制也开始从实质性接触向非实质性接触扩展。随着大数据侦查的出现,司法界扩大了隐私信息的构成范围,将对隐私信息的理解构筑于众多信息的分析归纳之上。这种对隐私信息的界定扩大化以侦查技术水准为依托,并在最高法院对手机基站定位信息的分析上得到了极致展现。

凭借庞大的数据量和五年的存储期,手机基站定位信息能细致展现个人的生活习惯与日常状态。然而作为第三方存储的数据集,对其关键信息的掌握必须依靠大数据分析,这也就意味着警方无法按照普通信息存储载体的标准展开侦查。正是基于这些特殊性,联邦最高法院总结了四个判定搜查此类数据是否侵权的要素:(1)隐蔽性:强调社会对政府执法的合理预期,即民众普遍认为执法机关不会对个人在数年内的所有运动轨迹进行秘密监控;这一要素可看作对政府机关利用大数据实行广泛监控的一种辖制。(2)持续性:对标的是数据的可追溯性,目前数字化的普及以及芯片、云端对数据存储能力的爆发式增长,使得对数据信息的单次搜查就能获得相当于追踪数年的总量;因而,不能再将搜查时间和搜查次数作为衡量搜查程度的唯一标准,大数据侦查在时间和空间上都具有超越以往的持续性。(3)无差别性:强调数据信息的覆盖范围,这类数据几乎植根于所有智能手机终端,因此有必要抬高公权力对此类数据的获取门槛,有助于降低政府机关将非目标信息也纳入信息搜查范围的风险。(4)入侵性:将这类数据与日常信息作了界分,对个人家庭、政治倾向、宗教信仰、健康状况等信息的细致掌握无疑是对其隐私权利的侵犯。[33]

可见,手机基站定位信息的特质让美国司法界对隐私信息有了新的理解和诠释,数据量的叠加成为了衡量隐私性的关键要素,而数据的普遍性与易获得性也让法院高度警惕。尽管还没有清晰的限制标准出台,但法院明确表达了对执法人员热衷选择“高效、简易、便捷”的侦查手段的担忧,这也加速了司法界对隐私权保护标准的重塑。

### (二)数据控制方的中间立场——隐私权保护的利益协调

“第三方准则”赋予执法机关相对自由的侦查权,提升了办案效率,同时区分了商业记录和个人信息,使第三方商业机构对商业记录的控制权得到了较为充分的展现。然而,这些优势在面对手机基站定位信息这类数据时,却陷入了前所未有的困境。一方面,这类数据深刻记录了手机用户数年内所有的活动轨迹,能充分揭示个人的生活习惯、业余癖好等涉隐私信息;另一方面,这类数据为电信运营商所实际存储和控制,具有与其他涉隐私信息截然不同的商业价值。这种矛盾特质为缩小“第三方准则”的适用范围找到了切入口,也让司法界开始审慎思考商业机构在“搜查”中所处的立场。

首先,手机基站定位信息与商业记录最大的不同,是不具有自主传递性。无论是银行交易票据单的填写,还是电话的拨出,都是信息主体主动参与的结果,在享受银行和电信

〔33〕 Susan Freiwald & Stephen Wm. Smith, The Carpenter Chronicle: A near-Perfect Surveillance, *132 Harv. L. Rev.* 205, 219 – 220 (2018).

公司服务的同时,信息主体非常清楚披露特定信息的必要性。但绝大多数手机用户可能根本不知道,自己每时每刻使用手机的情况会被发射给附近的手机基站,并存储于网络运营商的数据库中;即使在与网络运营商签订服务协议时明知传递个人信息是实现服务运转的基本要求,这种明知也并不包括后台会自动记录机主位置信息等细节。因此,这类数据并不具有"第三方准则"所要求的自主传递性,更多的是使用手机时无意识传递的结果。

其次,手机基站定位信息具有商业价值的现实并不能阻断手机用户对其享有的隐私权。由前述可知,这类数据是手机运行中自动生成的,并非属于手机用户自主选择与网络运营商共享的数据。此外,这类数据"揭示的信息具有无可比拟性",[34]通过细致描绘机主的生活轨迹,手机用户被迫承担起了隐私被暴露的风险,而这种风险在智能手机必备的现代根本无法避免。由此,手机基站定位信息价值数十亿美元的事实并不能直接抵消大众对其合理的隐私权期待。如果考虑到这类数据的复杂性,应当承认网络供应商对庞大数据的所有权和控制权,并否定个人对数据库具有合理的隐私权期待;但当特定数据关联到个人每一天生活的细节时,这种隐私权的合理期待就存在了。因此,主流观点认为,必须尽快制定新的审查标准,以回应个人对隐私权的合理诉求。

最后,确立网络运营商的角色地位是合理构建新搜查标准的关键。传统的"第三方准则"所适用的信息二元区分标准,即内容信息与元数据、人际交谈与商业记录的分类,在数字时代已经凸显弊端。2010 年的沃莎科案[35]就抛出了这样一个问题:在警方侦查需要的前提下,电子邮件服务商是否有对邮件内容的披露权?事实上,出于技术需要,服务商读取邮件具体内容已成为行业内默认的事实,而传统的信息二元界定法已然无法解决这个矛盾。对此,学界将解决问题的切入点放在了网络平台的角色定位上。2014 年的《国会调研报告》指出,信息是否需要宪法保护的关键在于网络服务商在信息交流中的作用,如信息可归类为信息主体与第三方的对话,则第三方属于参与者,享有信息披露权;如信息并非主体意欲传递给第三方的内容,则第三方仅是承载信息的中转站,对信息不享有任何处置权,包括披露权。[36] 该方法的提出反映出了美国法律界在信息保护思路上的重大转变:比如对定位数据的侦查,就可考虑信息主体的意愿,当用户视平台为信息接收者时,则平台属于信息交流的参与方,当用户将平台仅作为信息存储地或有明确的信息传递对象时,则平台只属于信息承载方或中间人。当然,如何对主观要件"用户发送信息的意愿"进行量化,也是个难题。在卡平特案中,法院将可追溯的定位时间限制在七天,该思路可为量化信息主体的合理隐私权期待指出一条研究方向。

### (三)数字化侦查环境的限制——卡平特标准的长远审视

卡平特案首次将第四修正案的保护范畴拓展到了手机定位数据上,其对"合理的隐私权期待"的重新诠释,对"第三方准则"适用范围的压缩,对数字侦查手段的探索性限

〔34〕 Carpenter v. United States, 138 S. Ct. 2206; 585 U. S. (2018), p. 12.

〔35〕 See United States v. Warshak, 631 F. 3d 266 (6th Cir. 2010).

〔36〕 See Richard M. Thompson II, *The Forth Amendment Third-Party Doctrine* 13 (Congressional Research Service Report No. 7 - 5700 2014).

制,开创了司法史上对电子侦查限制的新裁判标准,被称为“卡平特标准”。然而,这个标准无论是在理论构建、还是应用延伸上都存在着太多引人诟病的地方,以至于最高法院都不提倡下级法院对此标准的拓展性适用。尽管如此,“卡平特标准”已然成为了美国法律界直面数字侦查对个人隐私权侵犯的评判基石,并引发了更多思考和忧虑。

**1. 难以形成概括性的一般准则**

由于卡平特标准侧重于具体问题的解决,没有形成一般准则,可能会带来实践中的诸多问题。最高法院反复提及手机基站定位信息的特殊性对判决结果的影响,保留了数据变化推翻理论的可能,为今后卡平特标准的调整预留了相当大的空间。(1)回溯性定位数据与实时定位数据:正如前文提到的,数据的回溯性使得警方的侦查事半功倍,节约大量的时间和资源,而实时定位数据侧重位置移动的即时情况,信息量无法与回溯型数据相比,若将卡平特标准延伸至此,则会赋予个人在物理移动中过于宽泛的隐私权益。[37] 可见,法院对执法机构侦查历史数据的审查要比实时数据严格。(2)短期定位数据与长期定位数据:卡平特标准的适用中有一个“多于七天”的时间限制,理论依据是,超出一周的移动轨迹足以揭示个人的涉隐私信息。不过法院并未对此作出更多解释,这也使警方面对“少于七天”的手机基站定位信息的侦查情形存在适用标准的空白。(3)手机基站定位数据与手机信号塔转储数据:手机信号塔转储数据,是指信号发射塔中存储的手机发射历史数据。此类数据与手机基站定位信息的区别在于,后者依据目标手机来获取与手机相联系的基站发射塔位置信息,而前者则是依据特定犯罪需要来获取犯罪发生时段内相关场景附近的基站发射塔所有数据。所以,二者在搜查目的、形式和方法上都存在着较大差异。不过就数据量而言,从塔式转储技术中获取的虽然多为瞬时数据,但与信号发射塔窗口期相连的手机量多达成百上千,目前对此类数据的搜查标准仍在讨论中。

**2. 对政府执法将形成消极影响**

少数意见对卡平特标准的主要批评之一,就是法院冒着犯错的风险对第四修正案涉及的科技内涵做了过于详尽的解读,实际上完全忽视了科技进步带给司法效率的优势。批评意见援引了科尔(Orin S. Kerr)的“均衡调整理论”(equilibrium adjustment theory),强调科学技术的发展同时带给政府部门刑侦技术、执法手段,和犯罪人实施犯罪、反侦查手段上的改变,以及二者的联系和制约。[38] “相互制约的因素如何实现平衡,围绕着新型科技的财产规范与隐私权期待标准如何构建,在目前科技高速发展的环境下是难以被确立下来的。”[39] 肯尼迪法官的担忧不无道理。依据“均衡调整理论”概括的六种情形,(1)政府部门使用新的侦查工具的情境;(2)罪犯使用新技术逃避侦查的情境;(3)利用新技术实施新型犯罪和施展新手段的情境;(4)社会或政策改变滋生出新型犯罪和新侦查手段的情境;(5)没有发生新变化的现状;(6)警方与罪犯同时改变方法想要反击对方的情境。[40] 可以看出技术发展对犯罪实施和刑事侦查产生的各种影响,反映出面对技术升

〔37〕 See Rafael Andres v. State of Florida, SC 15 – 1095 (Fla. 2018).

〔38〕 See Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, *125 Harv. L. Rev* 476 (2011).

〔39〕 Carpenter v. United States, 138 S. Ct. 2206; 585 U. S. (2018), KENNEDY J., dissenting, p. 18.

〔40〕 See Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, *125 Harv. L. Rev* 489 (2011).

级,各方应对举措提升的必然性和必要性。因此,最高法院急于遏制政府机关利用手机基站定位信息的优势进行执法,是忽视了这类数据产生的背景,缺乏对司法效率的思考。实际上正是由于智能手机的普及强化了犯罪嫌疑人合伙作案的能力,那么依据利益均衡等式,执法机关利用 CSLI 提升执法效率也就有了相应的合理性。

**3. 引发社会对数字科技发展侵蚀个人隐私权的连锁拷问**

卡平特标准的出台,可看作法律界推动设立数字科技入侵个人隐私权标准的初步尝试。不过,手机基站定位信息的复杂属性仅是解开了数字社会生态圈的冰山一角,随着卡平特案破开的裂痕,更多的问题开始引人深思:第一,智能设备的云存储规范:目前,物联网建设已经初具规模,通过传感器与各类物体的连接,智能网络能将“任何事物”的运行情况存入云端。从目前实现的应用领域看出,智能家居、智能健康等产业都存在对个人的生活情况、生理数据的收集情况,由于相关信息都存储于云端,为商家所事实占据并处置,因此当执法机构直接调取云端数据时,存在着严重的监管缺失与法律空白。第二,生物基因数据监管:继指纹识别以后,面部识别也成为了最热门的刑侦手段之一。然而个人对自己的面部数据的生成与使用却没有完全的控制能力。同样,目前验证 DNA 的商业网站也在悄然兴起,这些数据的实质也都是实现商业价值的个人隐私,而目前对该类生物识别数据的商用化并未引起各方的足够重视。第三,人工智能分析带来的隐忧:各类 APP 对个人基本信息的获取早已为人所诟病,然而即使获取的仅是被认为具有商业价值的公开信息,如购物、浏览、照相等记录,网络平台依然能通过大数据分析解读出个人隐私信息,这给数据监管提供了挑战。还有学者指出,智能手机利用 AI 技术,能在后台和云端对手机信息重新进行归类和整理。如人工智能在手机云相册中将所有皮肤裸露的照片归在“内衣”类别下,此类信息是否仍属于隐私信息,依据卡平特标准显然无法解决。[41]

## 四　卡平特案的启示:我国刑事侦查与隐私权保护界限的划分

2019 年 6 月工信部发布 5G 商用牌照,标志着我国正式进入 5G 时代,也意味着数字化社会建设进入了崭新阶段。在数字时代,电子数据既展现了传统证据所不具备的复杂特点,也催生出了与之相匹配的新型侦查模式的诞生——大数据侦查。虽然大数据侦查的技术实质极易侵犯个人隐私,但当前对该侦查模式却缺乏定性与法律规范。仅有 2016 年最高人民法院、最高人民检察院、公安部联合出台的《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》为我国电子数据的提取与审查判断明确了方向,但规定内核也并未上升到保障被侦查人的隐私权层面。要科学合理地划分刑事侦查与隐私权的边界,必须把握三个层面,刑事侦查的定位、隐私权的确立标准,以及被侦查数据的权属界分。尽管我国目前在上述三个层面的研究都处于起步阶段,但以卡平特案为契机,或可为今后规范大数据侦查与保护个人隐私权提供某种借鉴。

---

〔41〕 See Peter C. Ormerod & Lawrence J. Trautman, A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age, *28 Alb. L. J. Sci. & Tech.* 148 (2018).

### （一）我国刑事侦查属性的再定位

侦查技术的不断升级，使大数据侦查模式成为了我国刑事侦查发展的新兴力量。有学者将大数据侦查定性为“针对已经发生或者尚未发生的犯罪行为，在以云计算为基础的技术平台上采取数据挖掘的方式，固定证据、证明犯罪事实或者预测犯罪，推进侦查活动顺利进行的一种现代化的侦查模式”。[42] 这种定性突出了大数据侦查的技术特点，强调信息采集与分析对现代侦查的主导作用，对推动数字社会侦查模式的全面转型有着积极的促进意义。但同时，学界对大数据侦查与传统侦查间的关系又存在较大争议：较为主流的观点将大数据侦查与传统侦查作明显切割，认为“大数据侦查的法律属性既不是搜查，也不是调取，亦不能被视为技术侦查”，[43] 而应作为一种新兴措施独立规制；也有观点认为大数据侦查与传统侦查既存在差别又存在联系，不应割裂，而应将大数据侦查纳入到现有强制性侦查措施的规制体系中。[44] 造成观点分歧的根本原因在于，学界对数字时代新兴侦查模式的变化与本质并未形成清晰的认知。而以对手机基站定位信息的侦查作为参照，则可对大数据侦查的认知误区作如下纠偏：

**1. 大数据侦查并不局限于虚拟空间**

有观点认为，作为传统侦查的补充，大数据侦查只能对虚拟空间的犯罪发挥功效。这实际上是对大数据侦查本质的误解。大数据侦查并不仅是应用大数据技术来收集和分析数据信息，更是对智能生态体系下犯罪的应对。在更为庞大的智能生态框架下，每一个事物都将与网络连接，共同构成庞大物联网的一环。由此，对任何物体的侦查，实质都是对数据的侦查，在物理空间发生的案件，实际也都与数据网络息息相关（如自动驾驶汽车伤人、利用智能音箱实施恐吓等）。由此，在数字社会的构建下，大数据侦查的范围必然同时涵盖物理空间与虚拟空间。

**2. 大数据侦查与搜查、调取存在重叠**

根据我国刑事诉讼法第 134 条相关规定，搜查主要针对与犯罪有关的人身、物品、住处等有形物或地点进行搜索，且需要被搜查人与见证人在场；而调取主要针对与犯罪事实相关的物证、书证、视听资料等实物证据，需要被调取的单位和个人确认调取内容。[45] 有分析认为，鉴于大数据侦查获取的数据信息量远大于“与犯罪事实相关”这一调取前提条件，且作为侦查对象的数据信息并非有形物或地点，因此大数据侦查与传统侦查存在显著差异。然而，这一分析仅考虑了大数据侦查收集分析数据的技术特点，并未预见到数字环境下的侦查现实。数字生态圈的构建不仅扩大了手机、电脑的信息存储量，还使家电、医疗设备、交通工具等与数字网络直接挂钩，因此，对物品、人身和地方的搜查，实质都是对数据载体的搜查。此外，调取的本质是向特定持有人获取证据，数据在民事法律上拥有固定权属的事实，使得侦查机关只能通过调取来实现。[46] 因此，数据信息量的差异并不能

〔42〕 杨婷：《论大数据时代我国刑事侦查模式的转型》，《法商研究》2018 年第 2 期，第 29 页。

〔43〕 程雷：《大数据侦查的法律控制》，《中国社会科学》2018 年第 11 期，第 167 页。

〔44〕 参见胡铭、龚中航：《大数据侦查的基本定位与法律规制》，《浙江社会科学》2019 年第 12 期，第 16 页。

〔45〕 参见《公安机关执法细则（第三版）》第 9－02 条。

〔46〕 参见胡铭、龚中航：《大数据侦查的基本定位与法律规制》，《浙江社会科学》2019 年第 12 期，第 17 页。

否定大数据侦查与调取存在重叠的事实。同时,就手机基站定位信息的特点而言,该类数据既为个人手机所收集,又存储于第三方的数据库中,意味着警方对数据的获取必须同时面对信息主体和网络运营商,如果仅从第三方数据库收集数据的过程考虑,则忽略了作为机主的数据主体的意见和立场。因此,大数据侦查措施实质包含了搜查与调取,是在复杂数字环境下对传统侦查模式的兼容与升级。

**3. 大数据侦查包含监控与追踪**

我国《刑事诉讼法》对技术侦查的内涵与外延均未作详细说明,目前仅有《公安机关办理刑事案件程序规定》第255条将技术侦查的范围概括为记录监控、行踪监控、通信监控、场所监控等。针对这一规定,有分析认为,监控手段的突出特征就是同步即时性,这与大数据侦查的数据比对、分析的技术特点存在明显差异,因此技术侦查无法容纳大数据侦查。〔47〕不过,手机基站定位信息的出现,却让二者找到了交集。作为记录手机用户地理位置的数据,其兼具回溯性与即时性,也同时满足查询、挖掘、比对和追踪的特点。同时,与GPS追踪类似,其叠加也能清晰反映个人的行使轨迹,同样具有秘密性与技术性特征。因此,大数据侦查也能涵盖监控与追踪。

### (二)个人隐私界定标准的确立

大数据侦查模式的构建,实质是数字时代侦查人员对数据信息的渴求,也对数据安全的建设和个人隐私权的保护提出了更高的要求。目前,学界对个人信息保护的一大研究方向是参考欧盟的《通用数据保护条例》和《以犯罪预防、调查、侦查、起诉或刑罚执行为目的的自然人个人数据保护指令》,以此为依据,执法机构对个人信息的收集、管理和处理可以获得一定的借鉴。但是,当涉及个人隐私信息的范畴界定时,如《通用数据保护条例》在第9条列举的属于个人敏感数据的七大类别(包括种族或民族、政治观点、宗教、哲学信仰、工会成员身份、涉及健康、性生活或性取向的数据、基因数据和生物识别数据),就难以实行具体操作。首先,个人敏感数据不等于个人隐私信息。正如"卡兹测试"所强调的,在隐私的界定上存在个人与社会两个层面的价值判断,社会对敏感信息的理解并不必然与个人权益密切相关,需要进行综合评判。其次,不同国家、文化背景对隐私信息的敏感程度也存在不同。就上述列举的敏感信息来看,种族、民族和工会身份等都不触及国人的敏感点,而健康、性、基因等带有全人类共性的敏感信息可列为隐私信息范畴。第三,隐私的界定需要明确的理论支撑和量化标准。数字生态圈的构建依赖各类数据的传输,其中手机基站定位信息,虽不具有传统隐私类数据的特征,却在经过分析后能切实反映私密性,正代表着当前电子数据的发展方向。面对这种复杂的数据类型,有必要借鉴"马赛克"理论,以数据量级与隐私性的联系为重要参考,对标准的确立始终保持动态与细致的平衡,明确能实现科学合理的量化、机动准确的操作,才是符合现代法治理念的隐私信息界定标准。

### (三)个人、商业信息平台与政府三方协调的信息保护均衡机制的构建

我国在制定《刑事诉讼法》时并未将比例原则确立为基本原则,导致了刑事侦查手段

〔47〕 参见程雷:《大数据侦查的法律控制》,《中国社会科学》2018年第11期,第167-168页。

缺乏制约机制的现状,不仅造成了搜查、扣押电子数据滥用的倾向,也严重威胁到公民个人的隐私权利。[48] 从宏观层面,比例原则的引入当然是必要的,依据适合性、必要性和相称性三项子原则,可以有效指导电子数据侦查所代表的国家公共利益与公民个人基本权利间的关系在法律制定上的体现。在微观层面的具体操作上,还需构建一个充分协调个人、商业信息平台和政府三方的信息保护均衡机制作为对比例原则的补充。参照美国"第三方准则"的发展历程,攸关个人信息的商业数据正越来越成为执法机关侦查的重点目标,而作为第三方的商业信息平台则不可避免地成为信息保护均衡机制中不可或缺的重要一环。电信公司存储的数据正逐渐脱离纯粹的商业化,而朝着敏感化、隐私化的方向发展,反过来说,越来越多的敏感信息出于数字社会的建设需要而汇集于商业机构,因此,对此类信息的侦查与商业信息平台和信息主体都密切相关。2018 年的滴滴女乘客被杀案,妨碍及时侦查的重要一环就出现在滴滴客服拒绝向警方提供司机的个人信息上。目前,尽快制定要求第三方平台有义务协助警方办案规定的呼声非常高,但有义务提交信息是一方面,另一方面还需要对提交的信息进行筛选,抬高个人信息的审查门槛,以保障信息主体的基本权益。随着信息权属的日渐复杂,即需要高度警惕侦查技术侵蚀隐私权的风险,又要充分考虑技术对犯罪能力的提升。可以引入"均衡调整理论",比照不同情境下技术对执法效率和犯罪破坏力的影响,同时以保障信息主体与的基本权益为准则,以此维持对个人隐私保护与侦查效能的动态平衡。

[**Abstract**] As one of the digital evidences that can reveal a suspect's behavior trace, Cell-Site Location Information (CSLI) is becoming a forensics hotpot nowadays. Though involving the personal information of cellphone users, CSLI is factually stored and managed by wireless carriers. As a result, by taking the Carpenter v. United States case as the entry point, a heated debate has been carried out in the American judicial circle on the privacy and ownership of CSLI, cellphone search by police and the procedural requirements on evidence acquisition. This case involves not only the establishment of the privacy information standard, but also the equilibrium between judicial efficiency and personal privacy, even issues relating to policing technology in such new fields as cloud computing and the Internet of Things. Therefore, the study of this case not only is conductive to understanding the line between privacy protection and criminal investigation against the background of technical upgrading in the USA, but also provides useful references for the adoption of the standard on privacy protection in China in the digital era.

(责任编辑:贾 元)

〔48〕 参见陈永生:《论电子通讯数据搜查、扣押的制度建构》,《环球法律评论》2019 年第 1 期,第 10 - 12 页。