中外法学 Peking University Law Journal
Vol. 36, No. 1(2024)pp. 199－218

“普遍嫌疑”及其规制

以德国法为借鉴

施鹏鹏 *

摘　要　“嫌疑程度”理论，要求刑事诉讼的启动必须至少有初始嫌疑，不能仅凭单纯的猜测。但随着“犯罪预防优先”理念的渗入以及警务情报机构向刑事司法的渗入，以大规模监控、大规模数据储存以及大数据分析为典型代表的犯罪预防方法开始成为各国强力遏制犯罪尤其是有组织犯罪的重要工具。因为这些犯罪预防方法不需要达致任何程度的嫌疑，故其实施依据的标准可称为“普遍嫌疑”。“普遍嫌疑”对刑事诉讼的价值、无罪推定及公民的个人基本权利保障均造成了极大的冲击甚至颠覆，因此从基本权干预的角度，应确立法律保留、比例原则以及救济机制以进行规制。

关 键 词　普遍嫌疑　大规模监控　大规模数据储存　大数据分析　基本权干预

现代刑事司法正面临着新型犯罪与科技革命的双重影响：一方面，犯罪手段日益更新，新型犯罪层出不穷，各国政府还普遍面临着结构严密、隐蔽性强、危害性大的有组织犯罪以及日益猖獗的国际恐怖主义活动威胁；另一方面，借由科技发展所形成的战略犯罪治理(operative Verbrechensbekämpfung)理念日益受到青睐，大数据分析、电子信息提取、网络监控等正日益取代传统的取证方式，成为预防与打击犯罪最有力的工具。由此，“打击犯罪”与“保障人权”这一刑事诉讼的传统命题在新的时代背景里被赋予全新的含义。

在打击犯罪方面，现代的战略犯罪治理理念强调预防与打击的交叉融合，且“犯罪预防优先”日益成为共识，警务情报机构的权限逐渐延伸至刑事司法领域，[1]危险防御(Gefahren-

* 中国政法大学纪检监察学院教授。本文系2021年北京社科基金规划项目专项重点项目“域外检察制度现代化研究”(项目编号：21FXA001)的阶段性研究成果。

[1] Vgl. Michael Kniesel, “Neues” Polizeirecht und Kriminalitätskontrolle, Kriminalistik 1996, S. 229.

北大法律信息网www.chinalawinfo.com/　北大法宝www.pkulaw.com/

abwehr)成为警务工作的重中之重。现代科技手段尤其是大数据分析为“犯罪预防优先”提供了强大的支撑。例如,美国警方 2008 年便提出了“预测警务”(predictive policing)的概念,依托电脑技术对各种数据进行分析,预测将来可能发生的犯罪并进行针对性防控。警方通常利用 IBM Blue CRUSH、SPSS 等数据分析软件,预测某一区域发生犯罪的可能性或者预测某人犯罪的可能性。在分析区域发生犯罪的可能性时,主要以过去已发生犯罪的时间、地点、方式等统计数据、罪犯的居住地信息、在某一地点及特定时刻发生的特定事件或活动(例如流行音乐会)、天气、社交媒体信息等数据为依据,估算这些不同的因素在各个地点发挥的作用,然后得出特定区域在该时刻的危险指数。[2] 在分析个人犯罪的可能性时,犯罪前科以及其他的警务数据、个人的居住地以及社交媒体信息均可以作为分析依据。如果警方认为某人有潜在的犯罪危险,将对其实施特别监控或者将其标记为危险分子。芝加哥便设有所谓的“侦查清单”(heat list),警方往往在这一清单上列明有可能成为暴力犯罪的行为人或受害者的人员,人数可达数百。[3] 与美国类似,欧洲大陆近年来亦大力开发及引入预测警务系统,旨在应对日益猖獗的恐怖主义犯罪及其他严重侵扰社会秩序的犯罪。如德国巴伐利亚州于 2015 年率先投入使用预测警务系统。巴伐利亚州和巴登符腾堡州当下投入使用的是犯罪预测监视系统(pre crime observation system,简称 PreCobs),该系统仅限于对入室盗窃犯罪的分析预测。[4] 2018 年,德国黑森州警方购买了美国 Palantir 公司的软件,用以打击伊斯兰恐怖主义犯罪以及有组织犯罪,现正在测试阶段。[5] 中国亦不例外。公安机关正在逐步建立健全依托于互联网、云计算、数据挖掘等技术的“智慧警务”,其“以海量数据整合为基础,运用信息化技术将分散、模糊的数据有序地关联起来,对其进行全面、多维度分析,从而科学地揭示事物发展趋势,进而提高公安决策的系统性与科学性”。[6] 以北京市怀柔警方为例,其于 2013 年起开始投入使用“犯罪数据分析和趋势预测系统”,该系统以怀柔公安所掌握的历史案件数据为基础,将犯罪案件分为入室盗窃案、强奸案、杀人案、诈骗案、抢劫案等八大类,通过多种预测分析模型,预测各类型犯罪的高发时段、地点,据此怀柔警方实现了更精准的警情预报,可以更高效地配置警力资源。[7]

但战略犯罪治理理念也引发了对个人权利保障的担忧,尤其是理论界及实务界所普遍关

〔2〕 Vgl. Tobias Singelnstein, Predictive Policing: Algorithmenbasierte Straftatprognosen zur vorausschauenden Kriminalintervention, NStZ 2018, S. 2.

〔3〕 A. a. O.

〔4〕 Singelnstein (Fn. 2), S. 1.

〔5〕 Vgl. Hessische Polizei testet neue Software zur Terrorabwehr, URL: http://www.faz.net/aktuell/politik/inland/palantir-technologies-hessische-polizei-testet-neue-analysesoftware-zur-terrorabwehr-15530046.html(Aufgerufen am 27. Dezembe 2023).

〔6〕 王懂懂、魏永忠:“大数据 3.0 时代:智慧警务建设的实践与思考”,《广西警察学院学报》2018 年第 1 期,第 65—70 页。

〔7〕 参见《北京怀柔警方建预测犯罪大数据系统》,载中国新闻网:http://www.chinanews.com/fz/2014/06-17/6290205.shtml,最后访问日期:2024 年 1 月 2 日。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

注的刑事诉讼“警察化”(Verpolizeilichung)或者“情报机构化”(Vergeheimdienstlichung)现象。因为任何以数据分析为基础的犯罪预防机制都必须以大范围的个人信息收集为前提。在尚无信息表明有具体的犯罪事实发生时,仅依托数据及算法推测具有某些特征的人群具有犯罪的可能性,这与现代刑事诉讼及基本人权保障的诸多基本理念存在明显的冲突。尤其是信息社会的海量数据收集事实上将所有公民均置身于“普遍嫌疑”之中,而此时的刑事诉讼甚至还尚未启动,“普遍嫌疑”的规制便成为现代刑事司法的全新命题。

因此,围绕这一命题,笔者将首先在刑事诉讼中系统地引入嫌疑程度理论,探讨“普遍嫌疑”的核心要义。在此基础上,笔者将重点阐释现代刑事司法中“普遍嫌疑”的典型制度外化形式及其对刑事诉讼基本理念的冲击。最后笔者还将以公法上的基本权干预为视角建构“普遍嫌疑”的约束机制。正如科林格里奇困境(Collingridge Dilemma)所阐释的,“一项技术的社会后果不能在技术生命的早期被预料到。然而,当不希望的后果被发现时,技术却往往已经成为整个经济和社会结构的一部分,以至于对它的控制十分困难。这就是控制的困境。当变化容易时,对它的需要不能被预测;当变化的需要变得明显时,变化却变得昂贵、困难和耗时间,以致难以或不能改变”。[8] 现代刑事司法在面临科林格里奇困境如何使技术更具可改正性、可控制性和可选择性,这需要法学界投以更大的关注,避免刑事司法从“侦查中心主义”进一步沦为“情报中心主义”。

一、嫌疑程度理论与“普遍嫌疑”

(一)嫌疑程度理论

依程序的基本法理,刑事诉讼的启动即意味着国家公权与公民私权产生冲突与对抗的开始,因而对公民的人身自由、财产乃至生命将产生极为重大的影响,故刑事诉讼奉行较严格及谨慎的启动标准,不可仅凭“单纯的猜测”,这是世界各国的通例。例如在德国,启动侦查程序的动因有三,即因职务活动知悉犯罪行为、刑事报案、刑事追诉申请。[9] 但是刑事追诉的启动以所谓的初始嫌疑为充分必要条件,即经由具体的事实证明的、以犯罪侦查经验为依据的线索表明存在可追诉的犯罪行为;单纯的猜测不能构成启动侦查的依据。[10] 在实践中逐渐发展出了“前置侦查”程序,在启动正式侦查之前承担判断是否存在初始嫌疑的功能。在日本,为了开始侦查,侦查机关需要“认为存在犯罪”,而认为存在犯罪的理由就是侦查的线索,包括侦查机关自己发现的和非侦查机关报告的,对这些线索侦查机关需要审核以确定是否存在犯罪。如果“认为存在犯罪”就应开始侦查,这也就是所谓的“认知犯罪”的过程,先认知犯罪方可侦查

---

〔8〕 David Collingridge, *The Social Control of Technology*, New York: St. Martin's Press, 1980, p. 11.

〔9〕 Vgl. Claus Roxin/Bernd Schünemann, Strafverfahrensrecht, 29. Aufl., 2017, § 39 Rn. 2-14.

〔10〕 A. a. O.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

犯罪。[11] 而随着程序进程的深入,相应的证明标准也随之提高,因为可适用的侦查手段及强制措施无论在广度还是在强度上均有较明显的提升。在学理上,我们可将这一变量称之为"嫌疑程度"(Verdachtsgrad)。[12]

"嫌疑程度"指随着刑事诉讼程序的逐渐推进,采取及适用各种特殊侦查手段、强制措施乃至作出有罪判决所需要达到的证据标准。这一概念清晰地表明了刑事诉讼逐渐推进的核心变量。从证明的角度看,刑事诉讼程序实际上是不断收集证据、查明事实以确定被指控人犯罪嫌疑程度的过程,包括两种情况:一是初始的犯罪嫌疑随着相关证据的不断出现逐步增强最终达到定罪的标准,犯罪嫌疑人最终成为被定罪的犯人;二是初始的犯罪嫌疑在进一步的侦查中并未强化至定罪的程度,甚至可能还在减弱,由此可能出现刑事诉讼程序终止或者被指控人无罪释放的结果。因此,相比于中国学术界所广泛使用的证明标准层次理论,"嫌疑程度"的概念可以更好地表述刑事诉讼不同阶段对于证据标准的要求。以德国刑事诉讼为例,依诉讼程序的不同阶段,犯罪嫌疑主要划分为如下几个级别:[13]

1. *初始嫌疑*(Anfangsverdacht)

初始嫌疑是开启侦查程序的前提条件。依《德国刑事诉讼法典》第152条第2款之规定,只要有"充分的实际线索"(zureichende tatsächliche Anhaltspunkte),除法律另有规定外,检察机关负有对所有应追诉的犯罪行为采取措施的义务,这便是"初始嫌疑"。初始嫌疑主要包含四个要素:①行为;②行为符合某种犯罪的构成要件;③具有诉讼法上允许的证据形式证明该行为;④不存在程序阻碍(Verfahrenshindernis)。程序阻碍是指有可能导致程序终止的事由,例如法院不具有管辖权(主要针对具有外交豁免权的人犯罪的情形)、被告人不具有刑事责任能力等。这种嫌疑只要达到微弱的盖然性程度(geringe Wahrscheinlichkeit)即可。

2. *充分嫌疑*(Hinreichender Tatverdacht)

充分嫌疑是检察机关提起公诉以及法院作出开启主要审判程序裁决的前提条件(《德国刑事诉讼法典》第170条第1款以及第203条)。当犯罪嫌疑人实施犯罪并获得有罪判决的可能性大于无罪的可能性,即达到"优势盖然性"(überwiegende Wahrscheinlichkeit)的标准时,存在"充分的犯罪嫌疑"。

3. *紧迫嫌疑*(Dringender Tatverdacht)

紧迫嫌疑是签发待审羁押令以及为鉴定精神状态命令安置监视的前提条件。根据《德国刑事诉讼法典》第112条的规定,如果被指控人具有紧迫的犯罪嫌疑并存在羁押理由时,允许

---

〔11〕 参见田口守一:《刑事诉讼法》(第5版),张凌、于秀峰译,中国政法大学出版社2010年版,第45—46页。

〔12〕 中国学术界有类似的理论,即证明标准的层次论。但相比于"证明标准"这一概念,"嫌疑程度"的表述直截了当地反映了证据标准所依据的变量,更为直观、精细,且避免了与庭审的定罪标准相混淆。详见下文的论述。关于证明标准层次论,可参见陈光中:《构建层次性的刑事证明标准》,载陈光中、江伟主编:《诉讼法论丛(第7卷)》,法律出版社2002年版,第4页。

〔13〕 Vgl. Michael Huber, Grundwissen-Strafprozessrecht: Tatverdacht, JuS 2008, S. 21 f.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

对其命令待审羁押。根据《德国刑事诉讼法典》第 81 条第 1 款及第 2 款的规定，仅当被指控人具有紧迫的犯罪嫌疑时，法院才可以为了准备对被指控人的精神状态作鉴定而命令将其安置于公立精神病院并进行监视。如果基于具体的事实可以认为被指控人有很大可能性(große Wahrscheinlichkeit)是实施犯罪行为的行为人或者共犯，包括可罚的未遂行为，则达到紧迫的犯罪嫌疑程度。但如果存在不可消除的程序障碍或者阻却违法、不承担刑事责任以及免除刑罚的事由，可以阻碍达致紧迫嫌疑程度。

4. 法官确信(Richterliche Überzeugung)

法官确信是犯罪嫌疑的最高程度，也是法庭作出有罪判决的证明标准。根据《德国刑事诉讼法典》第 267 条，如果被告人被判决有罪，则判决理由必须指出认为已证实的事实(für erwiesen erachteten Tatsachen)，且此些事实具备犯罪行为的法定特征。

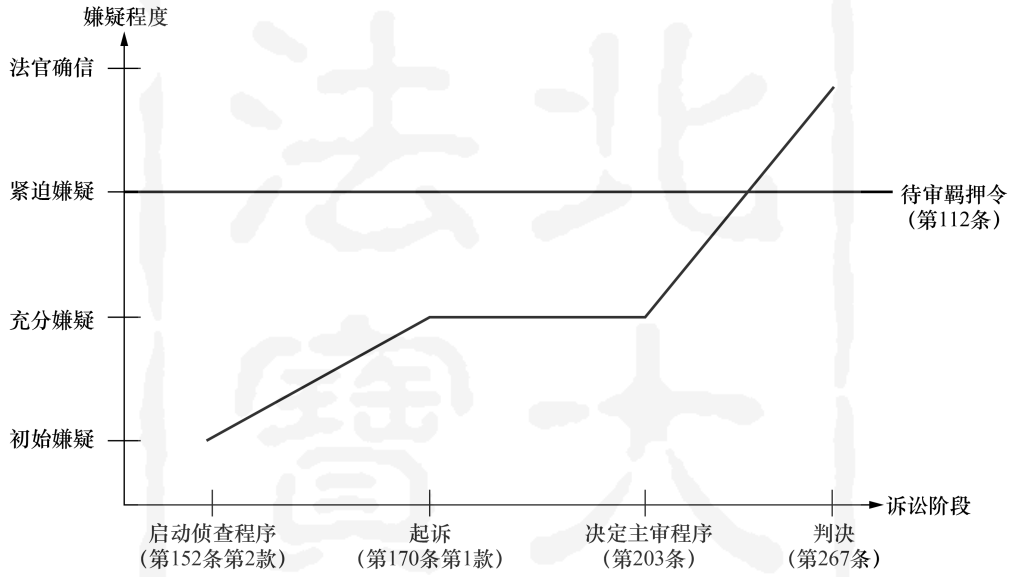

图 1　德国刑事诉讼各阶段的嫌疑程度

不难看出，德国刑事诉讼之所以将嫌疑程度作为各诉讼阶段的证据要求，实际上是比例原则思想的体现，即被调查对象具有多高程度的犯罪嫌疑，就必须为了查明犯罪这一公共利益而忍受多高强度的干预。[14] 这也反映了嫌疑程度理论与无罪推定原则之间的关系：虽然任何公民在法院依法确定有罪以前，应被推定为无罪，但这种推定的无罪状态在判决前的诉讼阶段实际上体现为不同程度的犯罪嫌疑。而在从完全无犯罪嫌疑到犯罪嫌疑达到法官确信程度的过程中，犯罪嫌疑人、被告人将相应地受到不同强度的刑事诉讼措施的干预。无罪推定的正当程序要求与查明犯罪事实的需要之间达成合比例的平衡。

〔14〕 Huber (Fn. 13), S. 21.

北大法律信息网www.chinalawinfo.com/　北大法宝www.pkulaw.com/

(二)“普遍嫌疑”概念的提出

如前所述,“嫌疑程度”理论,要求刑事诉讼的启动必须至少有初始嫌疑,不能仅凭单纯的猜测。但随着“犯罪预防优先”理念的渗入以及警务情报机构向刑事司法的渗入,一种基于大规模监控及大数据建构与分析的高科技手段以针对不特定公民进行犯罪布防的新做法开始成为各国强力遏制犯罪尤其是有组织犯罪的重要工具。因此,与传统的刑事侦查手段相比,这些犯罪预防方法不需要达致任何程度的嫌疑,即任何公民,基于诸如年龄、性别、出身或者行为等特定情况均可能列入特殊预防对象,即使具体并无实际理由表明其涉嫌实施了犯罪行为。我们称这一取证标准为“普遍嫌疑”。可见,“普遍嫌疑”是最低级别的“嫌疑程度”,主要针对尚未发生或虽发生但尚未启动侦讯程序的犯罪行为。

在尚未启动正式侦讯程序的阶段,刑事追诉机关可以使用一定的调查手段,以确定是否存在需要追诉的犯罪行为。但由于此时只是存在轻微的“普遍嫌疑”,允许使用的调查手段也相应地仅限于不侵犯相对人权利的非强制性措施,例如盘问、跟踪盯梢、向周围人打听消息等。但我国在初查阶段可使用的手段种类和强度要高于德国,包括查询、鉴定、勘验等。这是由于我国的立案标准高于德国的侦查启动标准,所以我国的初查相比于德国的“前置侦查”,承担的调查任务更重。德国的前置侦查阶段很多只是存在普遍嫌疑,而我国的初查阶段在很多情况下都已达到了初始嫌疑的标准,即已经通过接受检举、控告等方式发现了具体的犯罪线索。

普遍嫌疑是在具体犯罪发生或被发现之前针对不特定多数人产生的犯罪嫌疑。如果犯罪已经发生且被发现,只是犯罪嫌疑人不明,侦查机关为确定嫌疑人身份而进行大规模采样、大数据摸排等,并不属于本文所称的“普遍嫌疑”。这种情况下虽然也有大量人员处于被怀疑的状态,但其嫌疑源于具体案件显示的线索和证据,而非笼统的犯罪可能性“标签”。举例说明,如果发生了一起恐怖袭击案件,有监控显示犯罪嫌疑人是身着阿拉伯长袍的中年男子,于是警方通过在数据库中检索所有来自阿拉伯国家的40至50岁之间的男性信息进行排查,这不属于普遍嫌疑,而是已经达到了初始嫌疑;如果尚未有线索表明发生了具体的恐怖主义犯罪,而警方仅仅依靠以往犯罪预防的经验认为所有从阿拉伯国家入境的中年男性均有可能实施恐怖主义犯罪,进而调取相关数据筛选出“可疑人员”一一盘问,这便属于普遍嫌疑。如果说对于初始嫌疑的程度较为合适的表述是“在猜测与了解之间”(zwischen Vermutung und Wissen),则“普遍嫌疑”则是在“猜测与预测之间”(zwischen Vermutung und Prognose)。更为重要的是,“普遍嫌疑”这一概念尚未进入刑事诉讼的领域,也因此摆脱了诸多正当程序条款的约束,对公民的基本人权保障造成了极大的威胁。

二、“普遍嫌疑”的制度外化

依调查方式的不同,“普遍嫌疑”具有多种外化形式,较为典型的主要包括(但不限于):①大规模监控,以实时观察与记录发现并干预犯罪,包括公共视频监控、公共网络监控等;②大规模数据储存,以海量数据,尤其是个人数据,存储创造信息优势,包括通信往来数据存留、

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

DNA 样本收集等;③大数据分析,以数据整合分析发现与预测犯罪,包括预防性排查侦缉与公开网络大数据分析等。以上“普遍嫌疑”外化的制度形式可以统称为“普遍嫌疑”措施。不同类型的“普遍嫌疑”措施所涉及的程序机理并不相同,所可能侵害的基本权利类型亦有区别,故应分别展开论述。

(一)大规模监控

在技术层面,大规模监控主要利用计算机技术、图像采集技术等对不特定多数人的活动进行实时的观察、记录,以便及时发现犯罪迹象并介入干预,主要包括在公共物理空间的监控(视频监控)以及公共虚拟空间的监控(网络监控)。

公共视频监控系统主要由大量监控摄像头组成的输入子系统、信号传输与存储子系统以及中心控制室的监视屏幕输出子系统组成。作为一种可以直观、实时呈现特定区域动态画面的措施,公共视频监控可获取的信息具有多元化的特征,除人的体貌特征、行为举止、物品的外观及移动轨迹以外,在先进技术的支持下还有可能获得公民的通信内容(例如短信或者网络聊天记录)、手机密码、说话口型等隐藏于人员活动中的细微信息。公共视频监控最初应用于商业领域,主要在银行、商场等半公共场所安装,以威慑盗窃、欺诈等违法犯罪行为。而后逐渐应用至公共机构内,例如学校、政府机关等,尤其是道路交通监控。之后又发展到在街道、车站、广场等各种完全的公共空间,形成较大规模的公共视频监控系统。根据安装场所和主体的不同,公共视频监控大致可以分为社会监控和政府监控两类:前者是指在银行、商场、学校、社区等半公开场所由场所管理者安装实施的监控系统;后者是指在公共道路、车站、广场等公共设施等完全公开的场所由政府安装实施的监控系统。两类监控系统通常相互独立,但不排除有整合成统一的大规模监控系统的趋势存在。这种整合将带来的是“一加一大于二”的效果,公共视频监控将不再是七零八落的“孤岛”,而是呈现地毯式的覆盖。在监控范围日趋扩大的同时,视频监控技术的发展也使得监控效果大大提升。一方面,图像抓取与处理技术的提高降低了信息提取的难度,例如,图像分辨率提高使得被观察人员的衣着相貌中的细微特征也可被清晰捕捉;另一方面,面部识别、车牌号码识别等智能分析系统逐渐代替人工观察,能够更加快捷、准确地发现有用信息。

如果说公共视频监控系统主要针对现实的物理空间,则公共网络监控系统则主要针对虚拟的网络空间,但两者的机理类似。公共网络监控系统主要针对特定的可以公开进入的网页进行持续的监控或者在全网进行持续的、全面的特定关键词过滤。随着信息时代的到来,通过虚拟网络社会的监控甚至可获得更全面、完整、隐私的数据。从技术手段讲,公共网络监控主要包括:其一,人工或利用软件自动抓取网站内容并进行相关关键词检索,发现犯罪线索,例如,德国联邦刑事调查局在稽查税务犯罪时可以使用“X-Spider”程序可以搜查网页信息自动检索有嫌疑的活动;[15]其二,人工或利用软件根据特定的关键词拦截、屏蔽、删除具有违法嫌

〔15〕 Vgl. Christian Rückert, Zwischen Online-Streife und Online-(Raster-)Fahndung-Ein Beitrag zur Verarbeitung öffentlich zugänglicher Daten im Ermittlungsverfahren, ZStW 129(2017), S. 302.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

疑的网络内容;其三,隐匿身份进入需要注册登录、但无需身份验证的论坛、微博等半公开网络空间,监控其内容信息。

可以看到,大规模监控的基本特点在于对象不特定、覆盖范围广以及可实时远程观察。在犯罪控制领域中,大规模监控兼具犯罪预防与犯罪打击功能:一方面,在犯罪发生之前,被监控区域的人、事、物可以通过监控系统实时、直观地呈现在监控人员面前,为其发现可疑犯罪迹象并及时阻止犯罪提供条件,同时监控的存在也是对不法分子的震慑,在一定程度上能够破坏犯罪实施的秘密性条件,预防犯罪发生;另一方面,一旦犯罪发生,监控即可对犯罪过程进行记录与存储,为后续的刑事追诉提供侦查线索与证据。由此可见,大规模监控是以不特定多数人均具有潜在的犯罪嫌疑为依据,在有具体事实表明犯罪发生之前,观察、记录被监控区域的所有人、事、物等多元化的信息,为发现犯罪或将来可能的刑事侦查、安全防卫等活动作准备,体现了"普遍嫌疑"的基本思想。

(二)大规模数据储存

大规模数据储存,指利用现代信息技术长期存储海量数据于计算机内并将其按照一定的数据模型组织的措施。在犯罪治理领域所运用的大型数据库主要包括三类:一是司法机关自有的数据库,例如,我国公安机关所掌握的全国基本人口信息数据库、罪犯DNA数据库等;二是其他公共机构的业务管理数据库,如工商、税务、银行、学校等围绕业务领域所建立的数据库;三是私营机构的商业经营数据库,较为典型的如阿里巴巴、腾讯、百度等互联网大公司的数据库。在信息时代及风险社会的背景下,个人数据的价值日益显现,尤其是对于犯罪预防与侦查。侦查机关为在犯罪治理中取得信息优势,提前存储具有潜在犯罪危险的人员信息,既可以在很大程度上限缩嫌疑范围,也可以供后续可能发生的刑事追诉调取使用。以通信往来数据存留及罪犯DNA数据库为例。

通信往来数据存留是指公权力机构强制电信运营商存储用户的通信往来数据并保留一定的时间,以供未来可能的犯罪侦查或国家安全等特定的目的而加以调取使用的制度。而通信往来数据(Verkehrsdaten)则指在电信服务提供过程中所收集、处理、使用的数据,主要包括呼叫者与被呼叫者的电话号码及其他识别码、通话的起止时间及时长、所使用的服务类型以及移动通话时的设备识别码、位置信息、动态IP地址等数据。通信往来数据虽然并不涉及具体的通信内容,但能够反映一定的个人信息,以电话为例,通信往来数据可以反映"谁与谁在何时通话了多长时间",在移动通话中还能够反映通话地点。而当大量的通信往来数据汇集在一起,侦查机关便能够利用信息技术获知用户的动态通信状况,例如只接收来电、频繁更换SIM卡、总是去往某地等。由此,通信往来数据可以应用于犯罪防控,帮助侦查机关或者情报机关获得犯罪线索。例如2006年,欧盟为有效防范恐怖袭击以及维护欧盟各成员国家的安全出台了《数据存留指令》,要求各成员国通过立法强制电信与网络运营商存储指令所规定的通信往来数据,以供公权力机关调取和使用。德国、法国、意大利、西班牙等均进行了立法转化,确立了

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

符合各自诉讼法典的通信往来数据存留制度。[16] 可以看出，通信往来数据存留制度针对的是使用通信设备的不特定公众，所秉承的犯罪预防思路属于极为典型的“普遍嫌疑”。

DNA 数据库，指利用 DNA 分型技术、计算机技术以及大型数据库管理技术建立起来的，用以存储与比对违法犯罪人员、犯罪现场遗留人体物质的 DNA 数据信息的系统。在刑事诉讼领域，DNA 数据库通常以受到刑事追诉的犯罪嫌疑人或者已决犯为对象。例如英国原则上只针对犯有夜间盗窃、性犯罪和暴力犯罪三种罪行之一的已决犯提取 DNA 样本。美国也仅收集已决的暴力犯罪者和性犯罪者的 DNA 图谱。但随着制度的发展，采样对象在两国均有向被逮捕的未决犯以及更多类型的罪犯扩张的趋势。[17] 在德国，采集对象为满足下列两个条件的被指控人：①具有重大犯罪行为或侵犯性自主权犯罪行为的嫌疑；②基于犯罪行为的类别或实施方式、被指控人的性格或其他信息有理由认为，将来其有可能因有重大犯罪行为进入刑事诉讼程序（《德国刑事诉讼法典》第 81g 条第 1 款）。《法国刑事诉讼法典》第 55-1 条、第 76-2 条以及第 154-1 条对刑事诉讼各个阶段 DNA 物证提取的条件进行了详尽的规定，“为进行调查之必要，司法警官、共和国检察官及预审法官可在法定条件下向可能提供犯罪信息的任何人，或者存在一项或数项合理的事由怀疑实施或试图实施犯罪的任何人，进行必要的取证，以对比所提取的痕迹和线索，进行技术的、科学的检验”。但需要特别注意的是，DNA 数据的收集虽然基本上以特定罪名的既决犯为对象，但目的却是为了在将来可能发生的刑事诉讼中为确定犯罪嫌疑人的身份做准备，具有犯罪预防的性质。因此，可以认为，罪犯 DNA 数据库的基本原理体现的是对前科人员的“普遍嫌疑”，推定受过刑事追诉的某类罪犯均有再次实施犯罪的高风险。

综上，可以认为，大规模的数据储存以采集不特定对象、信息敏感度高以及可能涉及公民隐私及其他基本权利的数据为技术特点，为将来可能进行的刑事追诉创造信息优势支持，兼具预防与打击犯罪的双重功能。也正因为如此，倘若未构建周密成熟且合乎法治要求的限制，则公民（既可能是普通公民，也可能是有前科的公民）将处于“普遍嫌疑”的状态。

（三）大数据分析

大数据分析，是指对大量、多样且及时更新的全数据进行整合与分析，以发现事物之间的相关性、预测事物的发展趋势。运用大数据分析主要具有三种的思维特征：一是相关性思维，即重视事物之间的相关关系，即使不知为何相关，其运用方式包括通过观测关联物来观测某一现象以及通过数据挖掘发现不易从表面看出的相关关系；二是整体性思维，是指运用整体的数据，而不局限于抽取部分样本，由此应当获取较为全面的数据，并以此为依托整合各部分数据所展现的片段信息，拼凑出整体的有用情报；三是预测性思维，是指基于相关关系的分析，基于

〔16〕 虽然欧盟的《数据存留指令》于 2014 年 4 月由欧洲法院正式宣布无效，但不影响各国已经转化为国内法的数据存留规定的效力。

〔17〕 参见王志刚：《DNA 证据的应用与规制》，知识产权出版社 2015 年版，第 164—169 页。

北大法律信息网www.chinalawinfo.com/　北大法宝www.pkulaw.com/

对各类关联因素的考虑预测事物的发展趋势。[18] 受此一思维影响,以大数据分析为手段的新型预测性犯罪治理模式日益受到青睐。犯罪治理中的大数据分析主要包括三个环节:首先,确定分析目标。通常情况下,大数据分析可用于预测犯罪高发地区、预测高危犯罪人员、识别犯罪线索三类目标的实现。对于地区犯罪活动的预测可以作为调配警力资源、确定布防力度的依据;对于个人犯罪概率的预测则可能作为受警方重点盘查与管控的依据;对于犯罪线索的识别则可以为警方进一步的调查核实甚至立案侦查提供方向。此外,由于各种类型的犯罪具有不同的特点和关联数据,因此上述目标必须结合具体的犯罪类型方能更加具体可行。其次,获取大数据。以确定的目标为导向,获取其所涉研究范围的所有数据。获取数据的来源既包括刑事追诉机关或其他机构所拥有的数据库,也可以是网络上可公开获取的各类数据。最后,分析大数据、得出结论。根据目标的实现需要,对于大数据的分析既可以采用简单的数据比对,也可以进行深度的数据挖掘,或设计复杂的算法模型预测犯罪,最终得出可有助于犯罪预防的结论。

在国际范围内,犯罪侦防中的大数据分析具有多种应用模式,常见的有预防性排查侦缉和公开网络大数据分析。预防性排查侦缉是指为排查潜在的犯罪行为人以预防犯罪,依据犯罪侦查经验确定查找人员的特征,以这些特征为标准对包括未涉案人员在内的个人数据进行自动比对,以从大量人员中筛选出具有案件"犯罪嫌疑人特征"(Verdächtigenprofil)的人员,其中所使用的个人数据包括刑事追诉机关及其他公共或私营机构所存储的数据。例如2001年秋季,德国便曾为了找出潜在的恐怖分子而在联邦范围内实施了大规模的预防性排查侦缉。起因是"9·11"事件后,时任德国联邦内政部部长的奥托·席利(Otto Schily)建议实施一揽子安全政策以减小潜在的恐怖分子风险。当时在德国高校学习的约5万穆斯林学生被认为可能对国家安全造成威胁。因此,各州使用了预防性排查侦缉来寻找"休眠者"(即潜藏的恐怖分子)。排查的特征依据为:男性,学生,18—40岁,来自26个被怀疑是恐怖分子聚集地的国家之一,经济独立,有语言天赋,喜欢旅游,频繁申请旅游签证,友好可亲以及可能受过飞机驾驶训练。由此,侦查机关在联邦范围内收集了大约600万条数据记录,然后盘问了大量被筛选出的"嫌疑人"。[19]

公开网络大数据分析是指利用计算机软件对社交媒体、网络论坛、博客等公开或者半公开网络平台上可任意获取的海量数据加以分析,以获取有用情报的措施。这些数据不仅包括任何人均可以无条件浏览下载的数据,也包括一些必须进行用户注册但不进行身份验证的交流论坛中可以获得的数据。例如,德国联邦刑事调查局使用PERKEO程序用以识别儿童色情

---

[18] 参见王燃:《大数据侦查》,清华大学出版社2017年版,第54—61页。

[19] Miguel Ángel Cano Paños, El rasterfahndung en el derecho procesal penal alemán y su aplicación práctica en la lucha antiterrorista, Revista Electrónica de Ciencia Penal y Criminología (en línea), 2003, núm. 05-06, p. 06:1-06:14.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

图片;使用“网络侦查工具”(INTERMiT)对网络上的可罚内容进行自动搜索;等等。[20] 与预防性排查侦缉相比,二者的区别在于分析目标、数据来源与分析方式的不同:公开网络大数据分析以识别犯罪线索为目标,使用的是从公开网络平台可以任意获取的即时数据,利用软件设计相应的算法进行较为深层的数据挖掘;预防性计算机排查侦缉以筛查潜在的犯罪嫌疑人为目标,使用的是刑事追诉机关或者其他机构存储的个人数据,包括不可公开获取的数据,由刑事追诉机关确定排查目标的特征并进行机器比对。

中国当下也有不少地方应用大数据分析进行犯罪防控。例如,据媒体报道,厦门市在开展“扫黑除恶”专项斗争的工作中,依托厦门市政法信息共享平台专门研发了“扫黑除恶”模块,拓宽了涉黑涉恶犯罪线索的发现渠道。2018 年 7 月,厦门市扫黑办通过“扫黑除恶”模块的数据分析,获得一条重要数据线索——张某具有房屋“套路贷”共性行为特征,且反复多次,并被群众举报涉嫌暴力讨债,与涉黑涉恶典型犯罪套路贷案件高度相似。市扫黑办与市公安局迅速联动,思明区公安分局通过对该线索的深入调查及对张某与关联人员的深入挖掘,迅速掌握了一个人数众多的“套路贷”犯罪团伙。9 月 11 日,警方通过前期掌握的情况,组织统一收网行动,一举抓获 2 个团伙、47 名“套路贷”犯罪嫌疑人。[21]

可以看到,在有具体线索表明犯罪发生前,大数据分析可基于与犯罪相关的数据现象推测犯罪发生地、潜在的犯罪嫌疑以及可疑的犯罪迹象,由此将具有犯罪相关特征的不特定多数人置于“普遍嫌疑”之中。

三、“普遍嫌疑”对刑事诉讼基本理念的冲击

与传统的侦查手段不同,无论是大规模监控、大规模数据储存还是大数据分析等,这些以“普遍嫌疑”为取证标准的新型手段以不特定多数人为对象,在正式刑事程序启动前便全方位记录、观察、分析公民的社会生活并截取可能的犯罪场景,立足犯罪预防,为将来可能启动的刑事打击程序作充分的准备。传统刑事诉讼的基本理念也受到了全方位的冲击。

(一)诉讼价值:预防犯罪与打击犯罪的交叉融合

如前所述,“普遍嫌疑”体现的是预防性思维,基于新型技术手段的应用既可以震慑不法分子从而防止犯罪发生,也能够大大提高刑事追诉机关及时、主动发现违法犯罪的能力,从而在犯罪发生之时立刻转而发挥侦查功能。由此,犯罪预防与犯罪打击之间的转换几乎在瞬间完成,使得二者之间的界限变得模糊,对于刑事诉讼中传统的打击犯罪的理念造成冲击。

一方面,刑事诉讼中的“预先性打击”(antizipierte Repression)将可能成为常态,现代刑事法治的基本理念受到冲击甚至颠覆。“预先性打击”,又称为“刑事追诉的预先处理”(Strafver-

[20] Rückert (Fn. 15), S. 302.

[21] 参见《厦门用“大数据”扫黑除恶:从“人工排查”转向“数据摸排”》,载凤凰网,http://tech.ifeng.com/a/20180920/45175015_0.shtml,最后访问日期:2023 年 12 月 27 日。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

folgungsvorsorge)，指在基于初始嫌疑的侦查程序启动前，公权力机构已经为查明将来可能发现的犯罪行为作准备的一般性调查活动。[22] 由此，现代法治国的法律保留原则(Prinzip des Gesetzesvorbehalts)以及司法审查原则也一并受到挑战及颠覆。例如，依法律保留原则，国家机关干预公民的基本权利，必须事先取得明确的法律授权基础，始得为之。具体到刑事司法领域，刑事诉讼法是授权国家机关进行犯罪侦查的基本法。但以“普遍嫌疑”为基础的许多“预先性打击”措施并未获得刑事诉讼法的授权，主要由侦查情报部门所掌握，也摆脱了中立司法官的审查。

另一方面，打击犯罪扩大化、调查对象边界模糊也将成为常态。传统的刑事诉讼所针对的是具体的犯罪嫌疑人以及所涉嫌的犯罪行为，所有的犯罪要件均需初步的证据证明，以避免公权力肆意侵害公民的个人权利和自由，这在各国的刑事诉讼法典中均有体现。例如中国《刑事诉讼法》第109条规定，“公安机关或者人民检察院发现犯罪事实或者犯罪嫌疑人，应当按照管辖范围，立案侦查”。《德国刑事诉讼法典》第152条第2款规定，“只要存在足够的事实依据，除法律另有规定外，检察院负有对所有应追诉的犯罪行为采取措施的义务”。《法国刑事诉讼法典》第40-1条规定，“有地域管辖权的共和检察官认为已获悉的行为构成犯罪，且由已知身份及住所的人所实施，则应提起公诉”。但以“普遍嫌疑”为基础的诸多犯罪预防手段主要是对不特定多数人进行监控以便获得信息优势，并利用数据分析技术筛查出可能与犯罪有关的线索，在有具体线索表明犯罪发生前尽早介入干预潜在的犯罪行为。因此，在很多情况下，“犯罪嫌疑人”和“犯罪行为”均处待定状态，甚至可能并不存在，这便会导致调查对象边界的无限扩大，让公民处于长期的不安定状态。例如前所论及2001年德国对5万穆斯林学生所进行预防性的排查侦缉，排查的结果却令德国官方感到震惊，因为在近600万条的数据记录中，并未抓获所期待的恐怖主义“休眠者”，却只抓到一些可能的福利救助欺诈者(Sozialhilfebetrüger)。因此，如果将刑事诉讼看作经过层层过滤最终确定真正罪犯的“漏斗式”模型，[23]则在“普遍嫌疑”理论的支撑下，进入“漏斗”接受筛选的人员基数将大大增加，“伤及无辜”的机率也大大提升了。

(二)诉讼原则：对无罪推定原则及基本人权保障的冲击

“普遍嫌疑”对无罪推定原则毫无疑问将构成极大的冲击，甚至可以认为，“普遍嫌疑”的主要机理便是一定程度上的有罪推定，例如大规模的DNA样本收集。如前所述，几乎各国均允许对暴力犯罪者和性犯罪者的DNA进行采取并建设成数据库，以便为将来可能发生的类似刑事案件作调查准备。这一制度的基本机理是暴力犯罪者和性犯罪者再次实施类似犯罪行为的机率高于常人，而不是无罪推定。当然，对于曾实施特定类型危害大且累犯率高罪名的既决

---

[22] Vgl. Dennis Bock, Zur Antizipation künftiger Strafverfolgung als Teil einer modernen Strafrechtspflege, ZIS 2007, S. 130.

[23] Vgl. Thomas Baumann, Staatsanwaltschaftliche Ermittlungstätigkeit In Deutschland, Umfang und Struktur der Verfahrenserledigung, WISTA 2015, S. 77.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

犯进行必要的权利限制，这符合比例原则的设定。但应注意，随着犯罪预防理念的兴起，各国在犯罪数据库的建构上无论是在犯罪类型还是在罪犯特征方面均呈现明显的扩张趋势，一些国家的个人信息数据库甚至已远远超出了“罪犯”的范畴，这势必对无罪推定原则造成了极大的冲击。

除此之外，以大规模监控、大规模数据储存以及大数据分析为代表的“普遍嫌疑”措施，还将对普通公民的基本人权造成严重威胁及伤害，尤其体现在个人信息自决权（隐私权）以及通信秘密权。

所谓个人信息自决权，指个人有自主决定其个人信息的披露及使用，并决定何时、在何种程度上公开其私人生活情况的权利。一般认为，这些“个人信息”，涵盖了所有涉及一个已被识别身份或可被识别身份的自然人的信息，包括可直接或间接地用于识别自然人身份的姓名、编号、位置数据、网络标记以及可以反映人的体格、生理、基因、心理、经济、文化或社会方面特征的其他信息（德国《联邦数据保护法》第 46 条）。鉴于信息化社会所带来的隐忧，各国普遍确立了个人信息自决权。例如在美国，个人信息自决权源自隐私权的扩展，通过理论与诸多判例的推进，隐私权的内涵已从最初消极的“不受干扰的权利”逐渐演变为主动的“个人信息控制权”，并形成宪法上的自决性隐私和信息性隐私两大领域，个人信息虽仍作为“信息隐私”冠以隐私权的名义进行保护，实际上与个人信息自决权的保护模式无异。在德国，个人信息自决权经由 1983 年的人口普查案〔24〕得以正式确立，德国联邦最高法院以《基本法》第 2 条第 1 款以及第 1 条所保障的一般人格权为出发点，论证了个人信息自决权所应具有的核心内容，将其与隐私权并列，均属于一般人格权发展出的具体人格权。在德国理论界，信息自决权与隐私权之间究竟属于包含关系还是并列关系尚存争议，但在保护的外延上则基本观点一致。简而言之，公民享有保持安宁、不受他人打扰、妨碍的权利，公民的私人信息、私人谈话、私人财产、亲属关系、情感生活状况等各类私人生活事项，有保持隐秘状态，不为他人获知的权利。未有刑事诉讼法的授权，侦查机关不得随意获取个人信息。因此，无论是监控，还是数据储存与分析，事实上都将普通公民的日常生活状态（如在监控场所的言行、网络的表达等）甚至是私人生活的敏感信息（如 DNA、病历等）〔25〕纳入犯罪预防及打击的视野下。倘若未加限制，则科技时代的公民生活，将置身于无所不在的窥探及监控网格中，无论是在现实的物理世界，还是在虚拟的信念世界。

通信秘密权严格意义上也属于广义的公民个人隐私权，但考虑到其在社会生活中的特殊重要地位，多数国家的宪法将其单列。通信秘密权的保护对象主要包括信件秘密、邮政秘密及电信秘密三类：①信件秘密的范围不局限于日常所说的“信件”，而是包括所有具有实体的个人消息，与形式、制作方式以及内容均无关。同时，法律并不要求寄送必须密封，即使是公开的寄

〔24〕 BVerfGE 65，1（42）.

〔25〕 参见张新宝：“从隐私到个人信息：利益再衡量的理论与制度安排”，《中国法学》2015 年第 3 期，第 38—59 页。

北大法律信息网www.chinalawinfo.com/　北大法宝www.pkulaw.com/

送(如明信片)也不意味着发件人同意国家机关自动获取其通信内容。②邮政秘密包含提供邮政服务的邮政公司所进行的所有实体的邮件快递,主要涉及信件秘密保护范围之外的货物、杂志、大量投放的印刷品等不含私人消息的邮件。③电信秘密的范围是全部非实体的经由电信设备进行的通信,例如利用固定电话、移动电话等进行的通话、短信及电子邮件。电信秘密以保护私密性为目标,因此,诸如无线电台或者公开网页上的对话之类的公开通信形式不在该基本权利的保护范围之内。此外,通信秘密权的保护范围不局限于通信内容,还包括反映通信基本情况的附加信息,尤其是通信双方、通话时长以及通信频率等信息。[26] 可见,前文所论及以打击恐怖主义为名的通信往来数据存留制度便严重威胁了通信秘密权。事实上,这在许多国家均有争论,尤其是德国。2010年,德国联邦宪法法院便宣布《电信法》第113a与113b条以及《德国刑事诉讼法典》第100g条关于调取通信往来数据的规定因侵犯《基本法》第10条第1项规定的通信秘密权而无效,先前施行期间电信业者搜集、存储的通信往来数据应当立即全部删除。德国联邦政府对此反应激烈,尤其是其间发生了多起涉嫌严重危害国家的暴力犯罪预备(参见《德国刑法典》第89条a)。[27] 联邦政府认为,通信往来数据存留制度的废除将使德国全境处于恐怖主义的阴影之下。最终,德国联邦议会还是形成折衷方案,通过了全称为"确立通信往来数据的存储义务以及最长存储期限的法律"(Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten),确立了诸多保障机制,[28] 力图在预防恐怖主义犯罪和保障公民通信秘密权之间寻求平衡。

可见,"普遍嫌疑"措施无论之于无罪推定,还是公民的基本权利都存在严重的威胁,这是因为无论是大规模监控、大规模数据储存以及大数据分析,都存在干预范围广、干预对象不确定、控制手段乏力等特点,片面追求犯罪预防的效果,势必使公民的基本权利处于不可预测且不安定的状态。这也是为什么"普遍嫌疑"的规制理应引起理论界及实务界的高度重视。

四、基本权利干预视角下我国"普遍嫌疑"的规制

如前所述,"普遍嫌疑"这一概念尚未进入刑事诉讼的领域,也因此摆脱了诸多正当程序条款的约束。但从基本权干预[29]的角度看,以"普遍嫌疑"为基础的诸多公权力行为严重侵害了公民的基本权利,无论是否属于刑事诉讼法的规制范围,都需要遵循宪法上对基本权利干预

---

[26] Vgl. Andreas Funke/Jörn Lüdemann, Grundfälle zu Art. GG Artikel 10 GG, JuS 2008, S. 780-783.

[27] 例如2011年9月8日,柏林和巴登—符腾堡州的一些公司举报,一名德裔黎巴嫩人和一名巴勒斯坦人在不同公司均订购了可疑的大量冷却用剂,其成分可以与其他的材料共同加工制成极其易爆的混合爆炸物。德国警署随即抓捕了这两名犯罪嫌疑人,避免了恐怖袭击的发生。

[28] 例如数据销毁机制、损害赔偿机制等。

[29] Roxin/Schünemann (Fn. 9), § 29 Rn. 3 ff. ; Amelung, Rechtsschutz gegen strafprozessuale Grundrechtseingriffe, 1976, S. 14 ff.

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

设置的正当化要求，受到法律规制。我国宪法上虽未明确规定保护个人隐私、个人信息或数据的基本权利，但部门法规定的诸多权利可以成为解释宪法上基本权利条款内涵的重要素材，为普通权利上升为宪法位阶的基本权利提供支撑。尤其在2021年《个人信息保护法》和《数据安全法》颁布之后，个人信息作为当今数字时代公民的重要人格利益，愈发受到重视。许多学者也对我国宪法位阶上的个人信息权进行了理论证成，认为个人信息权能够借由“人权条款笼罩下的《宪法》38条人格尊严及40条通信自由和通信秘密”解释得出。〔30〕这一基本权利的证成为我国规制以“普遍嫌疑”为基础的各类公权力行为提供了前提支撑。同时，根据现代的干预概念（der moderne Eingriffsbegriff），只要对公民的基本权行使产生的影响是可预见的且可归责于国家公权力行为，就构成基本权干预。因此，前述“普遍嫌疑”措施均构成基本权利干预，应符合干预正当性的要求，即遵循法律保留和比例原则。如公民基本权利受到措施的不当干预，还可诉诸一定的救济机制。

（一）法律保留

法律保留指严重侵害公民基本权利的行为，应该由法律进行授权。我国台湾地区的林钰雄在评价刑事司法领域中现代基本权干预概念的作用及局限时指出，“（法治国的两难）：一方面，刑事诉讼不能成为宪法基本权保护的化外之地，另一方面，过度细节的法律授权要求将会导致侦查活动动辄得咎，寸步难行”。〔31〕而这一评价同样适用于“普遍嫌疑”措施。

在比较法上，各国对于“普遍嫌疑”措施的法律授权不局限于刑事诉讼法，还包括警察法、电信法、数据保护法等相关法律。以德国现行的通信往来数据存留制度为例，《电信法》便作了非常周密的规定，例如通信往来数据存留的目的仅得为了侦防犯罪，且仅为以下三种目的使用：一是刑事追诉机关为追诉特别严重的犯罪行为而调取；二是安全防卫机关为防御人的身体、生命或者自由以及联邦或州存续的具体危险时而调取；三是存留义务主体为履行对其他公权力机构（刑事追诉机关、安全防卫机关以及情报机关）问询IP地址的答复义务而使用（德国《电信法》第177条）。在其他任何情况下，任何机构和个人不得获取已存留的通信往来数据。

又如公共视频监控。法国对于视频监控系统的建立执行严格的许可证制度，由国家信息和自由权委员会（CNIL）进行合法性及比例性审查。进入刑事诉讼领域，法国2004年的贝尔本二号法律增设了在特定地点或车辆的录音与拍照（即视频监控）。法国宪法委员会重申（2004年3月2日第2004-492号判决），“适用这些强制措施的犯罪必须极有可能对个人安全、尊严甚至生命造成严重损害”（判决理由第16点），否则便构成1789年《人权宣言》第9条意义上的“不必要的严苛”（une rigueur non nécessaire）。因此，贝尔本二号规定了极为严格的适用条件，包括仅适用于法国《刑事诉讼法典》第706-73条所规定的有组织犯罪，须应由预审法官

〔30〕 张翔：“个人信息权的宪法（学）证成——基于对区分保护论和支配权论的反思”，《环球法律评论》2022年第1期，第59页。

〔31〕 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”，《政大法学评论》2007年第96期，第192页。

北大法律信息网www.chinalawinfo.com/　北大法宝www.pkulaw.com/

(必要时还应经自由羁押法官)批准且在公诉时效届满后,所有相关的录音、录像材料将被销毁。[32]《美国联邦政府关于安装公共视频监控系统的法律模型》中第 302 条明确指出,除法律授权以外,禁止将公共视频监控系统作为自动识别之用。[33] 英国 1988 年《数据保护法》要求公共视频监控系统的操作者必须确保公平合法地收集数据、捕获的图像均具有相关性,且数据保存不超过必要的时间。

我国对于"普遍嫌疑"措施的法律授权主要集中在《数据安全法》《个人信息保护法》和《刑事诉讼法》中。《数据安全法》第 35 条授权公安机关、国家安全机关依法维护国家安全或者侦查犯罪的需要调取数据;《个人信息保护法》第 34 条则是授权国家机关可以在履行法定职责所必需的范围和限度内依照法定权限和程序处理个人信息。二者均可作为"普遍嫌疑"措施中进行个人信息或数据的收集与处理的法律依据。如果说这两类条款为个人信息或数据进入刑事诉讼领域打开了合法的"输出口",那么《刑事诉讼法》第 54 条第 1 款则为其打开了"输入口",该条款授权刑事司法机关向有关单位、个人收集、调取证据,包括个人数据和信息在内。前述条款相结合方可为数据和信息的收集、传输、使用等各个环节提供完整的合法性。但上述法律依据具有一个共同的特点,即授权的概括性,其并未针对具体可收集的数据类型、范围及审批的具体程序等作出明确规定。虽然如林钰雄所指出,在刑事诉讼领域基于侦查的灵活性要求不宜进行过细的法律授权,但就"普遍嫌疑"措施而言,其对基本权利的损害程度会因为收集的数据类型、信息隐私程度、数据量以及数据分析的手段等产生极大的差别,仅对其进行笼统、概括的授权显然不能实现合理、有效的规制。以大数据分析为例,仅收集海量数据并进行简单的数据比对,与应用较为复杂的算法模型从海量数据中挖掘个人信息,甚至形成个人的"人格画像",两者之间的干预强度相差甚大,不能一概而论。因此,未来我国在"普遍嫌疑"措施的法律规制方面应当考虑对干预强度较大的措施专门设置更为具体的法律授权依据,当前的概括授权仅可用于干预强度十分轻微的措施。

此外,我国《个人信息保护法》还特别对公共视频监控的设置作出规制,即"在公共场所安装图像采集、个人身份识别设备,应当为维护公共安全所必需,遵守国家有关规定,并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的,不得用于其他目的;取得个人单独同意的除外"。对于公安机关设置的公共视频监控,公安部此前曾在 2016 年 11 月发布过一版《公共安全视频图像信息系统管理条例(征求意见稿)》。从内容上看,条例规定了公共视频监控系统的建设范围、主体、位置、明示标识要求等具体规则,同时强调任何单位和个人,不得利用公共安全视频图像信息系统非法获取国家秘密、工作秘密、商业秘密或者侵犯公民个人隐私等合法权益。但是基于部门立场的考量,这一规范性文件总体仍然以鼓励

[32] 参见施鹏鹏:"正当程序视野下的反有组织犯罪:法国的经验与教训——以'贝尔本二号法律'为中心",《中国刑事法杂志》2011 年第 11 期,第 118—127 页。

[33] 参见公安部治安管理局、公安部第一研究所编著:《国外城市视频监控系统应用与管理》,群众出版社 2012 年版,第 144 页。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

社会力量建设视频监控系统并且与政府方面进行资源整合为导向，在安装主体的监督管理、使用前提限制、透明性要求等方面有所欠缺。

（二）比例原则

除法律保留外，“普遍嫌疑”措施的适用还应符合比例原则的要求，即需要回答如下四个方面的问题：①合法目的：措施是否为了追求符合法律的目的？②有效性：这一目的是否主要由该措施促进实现？③必要性：是否不存在更加温和的、可以有效达到目的的措施？④适当性：即使不存在更加温和的措施，该措施本身是否可能与其所追求的目的不成比例？比例原则的要求不仅体现在措施法律授权依据的内容设计上，还约束措施的实际实施。

在法律授权依据的内容设计方面，比例原则通常体现为干预措施实施的各项实体和程序要件。首先是目的要件。无论是大规模监控、大规模数据储存还是大数据分析等手段，首先应确立合法的目的。仍以前述德国通信往来数据存留制度为例，其仅能适用于重大犯罪的追诉和重大法益具体危险的预防。相比之下，目前我国在“普遍嫌疑”措施目的方面的要求则较为宽泛，只要是“为依法维护国家安全或者侦查犯罪的需要”“为履行法定职责”或“维护公共安全的目的”，均可实施。未来在制定更加具体的法律授权依据时，应当根据措施的干预强度大小设置目的要件，进一步细化各类措施适用的案件范围。例如，对于干预性较强的大数据分析技术或利用公共视频监控进行面部识别、行迹追踪等，可以将其适用范围限制为严重危害国家安全的刑事案件、严重侵害公民人身权利的案件以及其他可能造成严重社会后果的刑事案件。对于情节轻微或者性质并不严重的刑事案件，则不允许使用此类强干预性措施。其次是有效性要件，即应当有一定的事实可据以推测使用大规模监控、大规模数据储存或大数据分析等手段能够实现法定的犯罪预防或追诉目的。抽象来看，“普遍嫌疑”措施对于实现犯罪预防目的的有效性几乎是不言自明的，但在个案中某项措施对具体犯罪类型的预防或具体侦查目的的实现是否具有促进作用，还应当有一定的证据加以证明。再次是必要性要件，即只有当采取其他方式难以实现犯罪预防或侦查目的时方可动用此类“普遍嫌疑”措施，且措施的实施也应以目的所需的必要范围为限。这一点在《个人信息保护法》第 34 条的表述中已经有所体现，即个人信息的处理“不得超出履行法定职责所必需的范围和限度”。以此为基础在进一步设置“普遍嫌疑”措施的具体授权依据时，也应将措施的适用限制在为实现合法目的所必需的范围内。最后是适当性要件，即要求措施的实施应当与案件的重要性合乎比例。这尤其体现为措施收集的数据类型、范围以及使用的数据分析手段等，应当与拟查明的犯罪的严重性相适应。除此之外，比例原则的适当性要求还体现在程序要件的严格程度应当与措施的干预强度相适应。以德国对“普遍嫌疑”措施的程序规制为例，在刑事诉讼中调取通信往来数据和采集 DNA 数据等干预性较强的措施，通常要求原则上由法官命令实施，只有在“迟延就有危险”的紧急情况下才能由检察院及其侦查人员命令，但对于公开网络数据的收集等干预程度一般的措施则不需要获得法官命令。中国当下对于“普遍嫌疑”措施的实施还主要由行政机关（或者侦查机关）进行内部审查，且具体程序规则并未公布，因此在审批主体的中立性和审批程序的透明性方面还有待加强。在比例原则的指导下，我国未来在制定“普遍嫌疑”措施的法律授权依据时便可

北大法律信息网www.chinalawinfo.com/　北大法宝www.pkulaw.com/

以按照上述实体和程序要件进行具体设计。

除此之外,在立法尚未修改的当下,我国也可直接按照比例原则的要求对“普遍嫌疑”措施的具体实施加以规制。例如,根据有效性的要求,对大数据分析措施的应用应当保障结果的准确性。在大数据分析措施中,筛查条件的相关性影响着结果的准确性。无论是依据侦查经验确定与犯罪相关的可观测特征,还是根据大数据分析得出的数据相关关系设计的犯罪预测算法模型,均只能得出盖然性的结论。为有效实现犯罪预防的目标,侦查机关不能仅是“广撒网”,更应“控制网格形状抓准真正想要的鱼”,因此必须对筛查犯罪嫌疑人的过程加以规制,确保筛查条件的选择及算法模型的设计符合犯罪预防的逻辑与经验。

又如,根据必要性和适当性原则的要求,在刑事诉讼中 DNA 数据库的建构方面,我国应仿效德国、法国的规定,仅适用暴力犯罪以及性犯罪的既决犯,而不宜扩及所有人群。事实上,中国在 21 世纪初业已建立了统一的全国公安机关 DNA 数据库和“打拐”DNA 数据库,其中全国公安机关 DNA 数据库由现场物证库、人员样本库(包括违法犯罪人员、犯罪嫌疑人、特殊保护群体等的数据)、亲缘样本库(包括不知名尸体、失踪人员、失踪人员亲属的数据)、基础数据库(按照中国地域、民族人群所收集的数据及其基因频率资料)、灾害识别库(因恐怖活动、刑事犯罪、意外事故以及自然灾害死亡的个体数据)组成。相比之下,我国 DNA 数据库的收集对象范围更广,为避免过度干预公民的基本权利,不仅应当控制 DNA 数据的获取,还应当区分不同类型的 DNA 数据库设置不同的用途限制,同时设置数据访问权限、定期删除非必要数据等制度防止 DNA 数据的滥用。此外,对于公共视频监控遵循的“为维护公共安全所必需”这一要件应当进一步细化解释,仅能在敏感的犯罪多发区域安装,而不能遍地撒网。根据行业调查公司 IHS Markit 的最新数据,2018 年,中国安装了 3.5 亿台摄像头,约 4.1 人/台,且预测未来公共场合的摄像头和监控设备会越来越多。[34] 故对此类措施适用的必要性亟待作进一步规范。

(三)救济机制

从权利保障的有效性看,完备的救济机制是确保普通公民基本权免受“普遍嫌疑”任意或不当侵害的最后手段。通常而论,法治发达国家往往确立了如下四项救济机制:

一,通知义务。传统的通知义务要求向措施所涉及人告知措施的具体内容及实施情况,如事前告知有碍于目的的实现,则至少应在措施结束后告知。我国《个人信息保护法》第 35 条已明确规定,国家机关为履行法定职责处理个人信息,应当依照本法规定履行告知义务;有法律、行政法规规定应当保密或者不需要告知的情形的,或者告知将妨碍国家机关履行法定职责的除外。“普遍嫌疑”措施作为一类针对不特定多数人的犯罪侦防手段,为保证其预防与打击犯罪的效果,一般应采用事后告知,但问题在于对象的不特定性与广泛性使得针对所有对象履行通知义务不具有可行性,且在干预程度轻微的情况下也不具有必要性。因此,通知义务的履行

[34] 参见《2021 全球摄像头达 10 亿:中国 5.6 亿台、美国 8500 万台》,载公共安全物联网大数据中心:https://seiot.com.cn/detail/12558.htm,最后访问日期:2023 年 12 月 24 日。

北大法律信息网www.chinalawinfo.com/ 北大法宝www.pkulaw.com/

可采取折中的办法，仅针对干预性较强的手段，例如公共视频监控中通过自动识别、放大技术以及使用大数据分析技术筛选出高危人员名单的措施，应对其中个人权利受到严重侵犯的主体进行事后的通知。通知义务的履行是后续当事人提起诉讼、申请进行证据排除以及对执法人员进行惩戒等救济途径实现的前提。

二，向法院提起诉讼的权利。各主要发达国家均允许受到公权力行为侵害的公民提起民事诉讼、行政诉讼甚至是宪法诉讼，由中立的法官对基本权干预行为的合法性及必要性进行审查。但在我国建立这一救济机制还存在诸多难题，如由谁起诉、向谁起诉、以何种依据提起何种类型的诉讼等。实践中，由于“普遍嫌疑”措施所涉及的相对人众多，如果个人提起私益诉讼，仅就个人的基本权利受损程度来看，很难达到“诉的利益”这一要件。《个人信息保护法》的出台提供了个人信息保护公益诉讼这一途径，即对于个人信息处理者违法处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。理论上，实施“普遍嫌疑”措施的国家机关也属于个人信息处理者，当其处理行为侵害了众多个人权益，便可以成为公益诉讼的对象。但实践中的个人信息保护公益诉讼大多是针对进行个人信息处理的私主体或其主管的行政机关，尚未出现对刑事追诉机关个人信息处理行为提起诉讼的先例。究其原因，一方面是由于当前“普遍嫌疑”措施的法律授权依据具有概括性，很难认定措施对个人信息造成了不当侵害；另一方面，由于我国长期使用“普遍嫌疑”措施进行犯罪侦防，国家机关甚至民众已“习以为常”，尚未树立此类措施严重侵害个人信息基本权利的意识，且多数情况下基于维护国家安全、实现犯罪预防和打击的公共利益的考量，对个人信息利益侵害的容忍度普遍较高。因此，未来是否能够在细化“普遍嫌疑”措施法律授权依据的前提下，确立个人信息保护公益诉讼作为措施的救济机制之一尚有待讨论。

三，证据线索的转化与非法证据排除。由于“普遍嫌疑”措施并非均依据刑事诉讼法所实施，故据此所获得的证据材料能否在刑事诉讼中作为证据使用，这在理论上存在争议。德国法所采用的“假设侦查流程理论”值得借鉴。此处的“假设侦查流程理论”是指，假设措施是在侦查启动后实施，以刑事诉讼法中同类证据的取证规则为标准，判断其是否具有证据资格。[35] 故我国可借鉴这一理论，对于“普遍嫌疑”措施所获得的证据材料，也应比照《刑事诉讼法》及相关司法解释进行证据的合法性审查。

四，对违法实施行为的制裁机制。对违法实施“普遍嫌疑”措施的国家机关和个人，应当承担行政责任及民事责任。构成犯罪的，还应依法追究刑事责任。我国《数据安全法》第44—52条、《个人信息保护法》第66—71条均规定了违法从事数据处理和个人信息处理活动所应承担的法律责任，也适用于实施“普遍嫌疑”措施的国家机关和个人。

应当说，自1979年中国颁布第一部刑事诉讼法以来，学术界更多对侦查行为的合法性及正当性投入精力，也取得了丰硕的学术成果。但随着现代科技的发展以及信息时代的到来，刑事诉讼“警察化”或者“情报机构化”的现象应当引起我们高度的重视。信息采集、大数据分析

〔35〕 Vgl. Kai Sackreuther, in: BeckOK StPO, 29. Ed. 1.1.2018, § 161 Rn. 15 f.

北大法律信息网www.chinalawinfo.com/　北大法宝www.pkulaw.com/

以及人工智能对当下及未来刑事诉讼所带来的冲击势必是深刻且遥远的，也必将远远超过我们这代学人贫瘠的想象力。我们或许离史蒂文·斯皮尔伯格所执导的电影《少数派报告》并不遥远，未来或许可以预知，罪犯在实施犯罪前便已受到了刑罚。而当我们愈发靠近这个场景，便应愈发保持高度的警惕，避免新型警察国家的出现。

Abstract: According to the "suspicion degree" theory, the initiation of criminal proceedings is at least based on a preliminary suspicion, and cannot be based solely on simple guesswork. However, with the permeation of the concept of "priority of crime prevention" and the increasingly participation of intelligence agencies in criminal justice, crime prevention approach, represented by large-scale monitoring, large-scale data storage and big data analytics, has become an important tool of states to suppress crime forcefully, especially organized crime. Because these crime prevention methods can be implemented without achieving any degree of suspicion, the standard on which they are based is called "general suspicion" causing great impact —even subversion— on the value of criminal proceedings, the presumption of innocence and the protection of citizens' fundamental rights. Therefore, from the perspective of intervention on fundamental rights, the principle of legal reservation, the principle of proportionality and relief mechanisms should be established in order to regulate the "general suspicion".

Key Words: General Suspicion; Large-scale Monitoring; Large-scale Data Storage; Big Data Analytics; Intervention with Fundamental Rights

(责任编辑：吴洪淇)

北大法律信息网www.chinalawinfo.com/　北大法宝www.pkulaw.com/