大数据监控措施的法律规制研究

——以隐私权为中心的探讨

赵艳红*

目次

摘要 大数据监控措施即通过大规模、系统化地收集、存储、处理和控制数据而对社会进行的监控，目前已经在侦查中被运用。因此有必要在研究大数据监控对公民权利的影响的基础上，研究如何规制大数据监控的运用。大数据监控可能会侵害公民的隐私权、个人数据权、通信自由权、表达自由权、财产权等权利，其中最有可能被侵害的是隐私权，所以也是我国刑事诉讼中最需要关注的一项权利。大数据监控虽然针对不特定对象，且通常仅监控非内容性信息，但由于对不特定公民的个人信息数据构成现实的威胁，所以仍可能会侵害隐私权。在现代社会，公民将个人信息数据提交给第三方不意味着就放弃了对个人信息数据的权利，要根据侦查机关获取公民个人信息数据的不同情形而判断是否构成对隐私权的侵害。即便公民身处公共场所，或在网络公共领域进行表达、交流，也仍对其中部分信息享有隐私权；而且对于公民在公共场所或网络公共领域所从事的那些不具有合理隐私期待的活动，如果进行长期、密集的监控，也可能会侵害公民隐私权。大数据监控具有侵权的长期性、秘密性、技术性、面广但度轻等特征。对大数据监控进行规制应以《刑事诉讼法》为主体，并辅以其他法律的规制；应当对目前《刑事诉讼法》中的技术侦查制度和立案制度进行改革；对各类大数据监控的法律规制应遵循比例原则，根据其在侦查中的具体作用、监控的对象、内容而进行宽严有别的规制。

关键词 大数据监控 隐私权 法律规制

* 安徽财经大学管理科学与工程学院讲师。本文系安徽省哲学社会科学规划青年项目“大数据监控在刑事侦查中的运用及其规范研究”（项目编号：AHSKQ2018D04）的阶段性研究成果。

一、大数据监控措施在侦查中的运用

所谓大数据监控，即以个人数据为核心，通过大规模、系统化地收集、存储、处理和控制数据而对社会进行的长期的、秘密的、无特定对象的监控。[1] 随着计算机和电子技术的发展，人们的各类信息构成了一个“数字人格”(digital personality)，这种“数字人格”使监控更为便利，大数据技术的发展则进一步强化了监控的力度，人们的所有特征或行为都可被转化为可识别、利用的数据。监控者通过实时数据更新、深度数据挖掘，可以随时查询使用这些数据。因此可以说，科技的发展使针对所有公民的大数据监控成为现实。大数据监控的主体是国家警察机关或安全机关，2013 年曝光的美国国家安全局进行的一系列秘密监控计划清楚地证明了这一点，如“棱镜计划”(Prism)、“上行计划”(Upstream)、“无界线人计划”(Boundless Informant)等。

大数据监控在犯罪预防和刑事侦查中有多种用途，如：用于预防、发现、同步监控犯罪；用于收集证据；用于查找特定对象；用于对特定对象的监控。其中，前几种在侦查中被运用时是针对不特定对象的监控，是从普遍性、一般性的监控中获取证据或信息，而最后一种则是针对特定对象的监控，属于我国现行《刑事诉讼法》所规定的技术侦查措施，已经能够被《刑事诉讼法》规范。所以本文主要探讨的是前几种用途的法律规制问题。

在我国，目前全国各地已经建设了较为发达的公共场所视频监控系统，对于犯罪预防和侦查发挥了重大作用；至今全国公安机关已经普遍设立了公共信息网络安全监察部门，该部门的一项主要职责就是网络监控，发现有害信息时通知有关部门删除或关闭网站，并负责相关案件的侦查取证。另外，我国公安机关正在建设的“金盾工程”综合了“全国公安综合业务通信网”“全国违法犯罪信息中心(CCIC)”“全国公共网络安全监控中心”等系统，[2]构建了加强违法犯罪处理信息化、日常监控普遍化的硬件基础。地方公安机关也建立了一些情报信息系统，如江苏省公安机关的“天网警务大平台”，该系统实现了省内外信息资源的高度整合和关联共享，协调司法、交通、金融、税务、民政等部门，交换获取刑释解教、民航旅客、高速公路收费、银行卡恶意透支、税务登记、社保参保等 19 种数据，其中 11 种实现了实时传输更新。[3] 总体上看，我国侦查机关已经具备大数据监控的能力，且已经运用于实践。

目前在我国司法实践中，通过文本分析、机器学习、数据挖掘等技术，能够运用于侦查的大数据监控主要针对以下几类数据：

1. 个人身份信息数据

个人身份信息数据即能够据此识别个人身份的相关信息数据，包括但不限于姓名、性别、种族、年龄、出生年月日、身份证号码、护照号码、驾驶证号码、工作证号码、身高、体重、指纹、血型、基因信息、遗传特征、健康情况、病历资料、户籍、家庭住址、电子邮件地址等。[4] 个人信息数据部分存储于侦查机关的数据库，部分来自商业企业、个人等数据来源。

---

〔1〕 参见张衡：《大数据监控社会中的隐私权保护研究》，载《图书与情报》2018 年第 1 期，第 71—80 页。

〔2〕 参见董邦俊、黄珊珊：《大数据在侦查应用中的问题及对策研究》，载《中国刑警学院学报》2016 年第 2 期，第 7—13 页。

〔3〕 参见汤强：《信息化背景下侦查权能的扩张与转型》，载《净月学刊》2014 年第 2 期，第 21—26 页。

〔4〕 参见张里安、韩旭至：《大数据时代下个人信息权的私法属性》，载《法学论坛》2016 年第 3 期，第 119—129 页。

2. 业务数据

业务数据即人们进行各项业务活动所留下的数据，这部分数据属于“可以用来识别个人身份的数据”，〔5〕包括政府管理产生的数据、商业数据、金融数据、工作记录数据、通信记录数据等。国家通过赋予大数据处理的相关机构、个人以进行数据留存、数据协助解密甚至数据本地化存储的义务，即可获取各类业务数据以供运用。

3. 行踪数据

行踪数据即通过对人们行动过程的记录而产生的数据，随着交通大数据的产生、智能化视频监控和各类智能穿戴设备的普及，人们的行踪已经成为大数据的一部分，可供随时查询和运用。行踪数据同样部分来自侦查机关自行管理的数据（如视频监控大数据），部分来自其他数据源。

4. 通信数据

通信数据即人们进行各种通信交流活动而留下的数据，包含内容数据和非内容数据，非内容数据也属于业务记录数据，所以这里的通信数据主要指内容数据。由于通信内容数据属于法律严格保护的隐私权对象，所以对通信数据进行监控时必须通过赋予法律义务或施加行政命令等途径获得通信企业的配合。

在针对以上类型大数据所实施的监控中，公民的以下几种权利有可能会被侵害，从而构成刑事诉讼中的强制侦查措施：

1. 隐私权

隐私权是指自然人享有的私人生活安宁与私人信息秘密依法受到保护，不被他人非法侵扰、知悉、搜集、利用和公开的一种人格权。信息时代人们的隐私权最容易受到侵害，大数据监控所针对的几类数据中，属于隐私权客体的数据占多数，如个人的遗传特征、健康状况、通信内容等，所以研究对大数据监控的运用进行规制，主要目的就在于保护大数据中包含的公民隐私权内容，防止在高科技时代公民的隐私权被技术所架空。我国《刑事诉讼法》中虽未明确规定对隐私权的保护，但2012年修法时以技术侦查措施可能涉及公民隐私权为由而将其纳入法律规范，足见已经将隐私权纳入《刑事诉讼法》的保护范围。

2. 个人数据权

个人数据权也可被称为个人信息权，是指个人对其数据被他人收集、存储、转让和使用的过程中所自主决定的利益。〔6〕个人数据权与隐私权并不相同，因为个人数据权的保护对象是隐私权无法涵盖的其他数据权利。虽然美国是在隐私权框架下对个人数据进行保护，但美国法与我国法中的隐私权概念涵盖范围是不同的。〔7〕按照我国学者的主张，个人数据权的主要属性是人格权，也有学者主张个人数据权兼具财产权的性质。〔8〕个人数据权以往在我国仅是一个停留在学术上的概念，但目前《民法典》第111条已经对个人信息的保护有了明确的规定，虽然如有学者所言并未将个人数据权作为绝对权，但也已经承认了个人对其信息享有一定的法益。在域外，刑事诉讼中的个人数据保护并非新问题，而且已经有较为成熟的理论，其中以德国的个人信息自决权为典型。但在我国刑事诉讼领域，对于个人数据权的保护则很少被涉及，因为这是一个近年来才兴起

〔5〕 王秀哲：《大数据时代个人信息法律保护制度之重构》，载《法学论坛》2018年第6期，第115—125页。

〔6〕 参见程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018年第3期，第102—122、207—208页。

〔7〕 参见前注〔4〕，张里安、韩旭至文。

〔8〕 参见前注〔6〕，程啸文。

的问题：在规范层面依据不足，也无法从《刑事诉讼法》的规定中推断出该权利已经被关注和保护；在理论层面，对于是否需要由《刑事诉讼法》保护个人数据权、与侦查需要之间的协调、保护的界限等问题都不明确，所以仍有很大的研究空间。

3. 通信自由权

通信自由权是我国宪法明确规定的一项公民基本权利。大数据监控措施中，对特定关键词、通信内容的过滤和拦截，会直接侵害公民的通信自由权。国外有学者认为，国家对不特定对象进行监控还会间接侵害公民的通信自由，因为人们如果知道无法保障通信秘密，就会放弃使用现代的通信手段。〔9〕但在这种间接侵害能否成立的问题上存疑，因为不能因为国家实施了监控就对其效果进行无限推演，而只能对监控是否直接侵权进行认定。

4. 表达自由权

表达自由权也属于一种宪法上的自由权。从权利客体来看，它是比言论自由更广泛的一种自由权，表达自由包括言论、新闻出版自由、艺术表现自由和集会自由。大数据监控的运用也会对表达自由权造成直接的侵害，如通过过滤软件实现对网络上特定信息的自动过滤、拦截。国外同样有学者认为政府监控会间接侵害公民的表达自由权，〔10〕但同理，不能对监控的效果进行无限推演而得出间接侵害公民表达自由权的结论。

5. 财产权

财产权是公民的基本权利之一，也是《刑事诉讼法》应当重点保护的权利。在少数情况下，大数据监控会侵害公民的财产权，如在进行网络过滤及监控时，将合法且具有经济价值的电子文件错误判断为非法消息而屏蔽、清除。

需要指出的是，大数据监控可能对如上几类公民权利的侵害，指的是可能侵害任意公民的基本权利，而非特指嫌疑人、被告人，这也是探讨大数据监控的法律规制的意义所在。因为犯罪嫌疑人、被告人之外的任何第三人对侦查机关的强制性措施都具有更小的容忍义务，〔11〕所以刑事诉讼法对不特定第三人的权利应给予更严格的保护，对其重要权利的侵害当然更应属于强制侦查措施。

从侦查学的角度来看，大数据监控在侦查中逐渐普遍的运用，使侦查方法发生一定变化，推动了侦查模式的转型，使传统的侦查模式及其法律规制产生一些变化。大数据监控的出现，使侦查权不再限于被动侦查，而是主动向犯罪预防甚至消除犯罪原因条件领域拓展和扩张，前瞻性地向引发犯罪或催生犯罪的相关因素和条件介入和干预；〔12〕侦查权的运行与犯罪行为处于共时状态，犯罪行为时刻处于侦查机关监控之下；侦查权的作用对象也呈现出广泛性、非特定性和弥散性特征。〔13〕在此前提下，对大数据监控的法律规制也应与对传统强制侦查措施的规制有所不同。如在国外，有学者探讨大数据监控下采取截停措施只需具备“预测型合理怀疑”的合理性问题，而不

---

〔9〕 See Human Rights Watch Report, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy*, Printed in the United States of America, July 2014.

〔10〕 Melissa De Zwart, Sal Humphreys & Beatrix Van Dissel, *Surveillance, Big Data and Democracy: Lessons for Australia from the US and UK*, 37 UNSW Law Journal 713,747 (2014).

〔11〕 具体请参见林钰雄：《刑事诉讼法(上)》，中国人民大学出版社 2005 年版，第 305 页。

〔12〕 参见韩德明：《从回溯调查到犯罪治理：侦查权范式的演化趋向》，载《中国人民公安大学学报(社会科学版)》2015 年第 5 期，第 37—53 页。

〔13〕 参见韩德明：《信息化背景下侦查权范式的要素系谱》，载《中国人民公安大学学报(社会科学版)》2016 年第 4 期，第 66—72 页。

再需要传统的“合理怀疑”标准。〔14〕

然而，目前我国侦查机关对大数据监控的运用却基本上处于内部管理和规范状态，〔15〕尚未纳入《刑事诉讼法》规制，虽然2012年《刑事诉讼法》修改增设了技术侦查一节，但我国技术侦查以针对特定对象为要件，〔16〕所以对于大数据监控无法直接适用技术侦查规定进行规制，相关的司法解释也未对大数据监控在侦查中的运用做出规范，而学术界对此问题的研究还远远不足。〔17〕相比之下，域外虽然也面临着如何规制大数据监控的问题，但近年来学术界对此问题较为关注，也出现了一些有分量的研究成果，〔18〕对于究竟如何规制大数据监控问题，国外学者也有不同观点。〔19〕我国《刑事诉讼法》未将大数据监控纳入规范，原因可能是多方面的，但最主要的原因可能就是立法者尚未认识到大数据监控会侵害公民权利并构成强制侦查措施，所以只将针对特定对象的技术侦查措施纳入规范，而忽略了大数据监控问题。因此，为求日后将大数据监控纳入《刑事诉讼法》规制，首先应从理论上探讨大数据监控会侵害公民的何种权利、需要何种程度的法律规制等问题，为其法律规制提供理论基础。

要解决上述问题，首先应对侦查中运用大数据监控是否侵害公民权利进行分析，然后才能解决后续的是否规制、如何规制等问题。但大数据监控是否影响公民权利这一问题，看似简单，实则存在诸多疑问。例如，大数据监控针对的是不特定对象，与针对特定对象的技术侦查并不相同，那么其是否具有与技术侦查相同的侵权性？大数据监控所针对的很多是公民利用网络服务而产生的各种数据，这些数据是否会因为公民自愿提交给网络服务商而失去隐私权、个人数据权？大数据监控还包括针对公民在公共场所、网络公共领域的各种活动进行监控所产生的数据，是否侵害了公民的隐私权等权利？要解决这些问题，就必须运用相关的刑事诉讼原理与公民权利原理，对大数据监控在这些情形中是否侵权进行理论分析，才能为解决大数据监控的法律规制问题提供理论基础。因此，下文将针对上述问题，以我国的大数据监控实践及其法律规制必要性问题为出发点，参考其他国家（主要是英美法系国家）的相关理论和实践，从侦查行为的规制原理角度探讨大

〔14〕 Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 University of Pennsylvania Law Review 328 (2015).

〔15〕 如对于公共场所视频监控系统的管理使用、公共信息网络的安全监察、警务信息平台的运用、各类数据的收集使用等，均由公安机关或其他国家机关自行管理和规范，而未纳入《刑事诉讼法》规范之内。

〔16〕 《刑事诉讼法》（2012年修正）第149条规定：“批准决定应当根据侦查犯罪的需要，确定采取技术侦查措施的种类和适用对象。……”第150条规定：“采取技术侦查措施，必须严格按照批准的措施种类、适用对象和期限执行。”《公安机关办理刑事案件程序规定》第255条第2款规定：“技术侦查措施的适用对象是犯罪嫌疑人、被告人以及与犯罪活动直接关联的人员。”

〔17〕 程雷教授以大数据侦查为研究对象，对如何规制大数据侦查进行了较为深刻的研究，提出要对大数据侦查进行法律控制，可采取侦查规范和数据规范的双重路径，参见程雷：《大数据侦查的法律规制》，载《中国社会科学》2018年第11期。但本文仅限于各类大数据监控措施，所以研究对象更为专门化。

〔18〕 Such as Russell L. Weaver, *Cybersurveillance in a Free Society*, 72 Washington and Lee Law Review 1207 (2015); Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harvard Journal of Law & Public Policy 757 (2014); John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 37 Harvard Journal of Law & Public Policy 901 (2014); Marc Jonathan Blitz, *The Fourth Amendment Future of Public Surveillance: Remote Recording and Other Searches in Public Space*, 63 American University Law Review 21 (2013); Bart W. Schermer, *Surveillance and Privacy in the Ubiquitous Network Society*, 1 Amsterdam Law Forum 63 (2009); etc.

〔19〕 如国外有学者主张政府的大数据监控应被严格规制，参见Marc Jonathan Blitz, *supra* note〔18〕；但也有学者对政府的大数据监控持坚定的支持态度，参见Yoo, *supra* note〔18〕。

数据监控对公民权利的侵害这一命题是否能够成立，然后根据探讨所得的结论，对我国如何调整侦查行为规制理论和规范以实现对大数据监控的规制进行探讨，为日后我国对大数据监控这一相对新鲜的事物进行法律规制提供一些理论借鉴。在我国当前刑事诉讼法治发展阶段，隐私权是大数据监控最可能侵害的权利，因此也是刑事诉讼中最需要保护的一种权利，而个人数据权在刑事诉讼法上的保护在我国仍缺乏成熟的理论，通信自由权、表达自由权、财产权则是在少数情况下才会被大数据监控侵害。所以限于本文篇幅和重点，下文对公民权利的影响分析仅以隐私权为对象，以此折射出大数据时代公民权利保护的问题、原理及路径。

二、大数据监控对公民隐私权的影响

（一）大数据监控对不特定对象隐私权的影响

与传统的侦查监控措施不同，大数据监控针对的是不特定的对象，虽然最终在具体个案中仍会指向特定对象，但在达到目标之前的监控中则是以不特定对象为目标的，所以通常是采取一种大海捞针的方法，即从海量的数据中发现犯罪线索、追踪嫌疑人行踪、收集相关证据，正如美国国家安全局前局长基思·亚历山大（Keith Alexander）所言，为了在干草堆中找到一根针，前提是需要拥有所有的干草。〔20〕但我们通常所探讨地对各种侦查措施的规制都是以针对特定对象为前提的，如搜查、扣押、冻结等，我国2012年修改《刑事诉讼法》所增设的技术侦查措施，是各类侦查措施中与大数据监控最为接近的措施，但我国的技术侦查也是以特定对象为构成要件的。〔21〕而且，正是由于大数据监控针对的是数据巨大的不特定对象，所以对公民个人信息数据的侵入程度往往较浅。如通过对互联网通信数据的常规监控而发现犯罪线索并展开侦查，只有当数据分析工具发现异常的通信数据时，侦查机关才会进行关注，而对普通公民的日常通信数据则并不进行关注，只是作为数据分析的对象而使用，所以与一般技术侦查中针对特定对象的密集监控措施并不相同。那么，针对不特定对象且对个人数据侵入程度较轻的大数据监控是否会侵害公民隐私权等基本权利呢？

对于这一问题，美国曾有学者认为，针对不特定对象的监控不属于美国宪法第四修正案的搜查，因为这种监控与2012年美国联邦最高法院判决的United States *v.* Jones案中警察使用GPS追踪器的情形并不相同，针对不特定对象的监控只是从街面等公共场所收集可用于犯罪调查的证据。〔22〕但这种观点遭到其他学者的有力驳斥，该学者提出两点理由：其一，针对不特定对象的监控是后续针对特定对象监控的前奏，所以从结果而论，针对不特定对象的监控仍会侵害公民受宪法第四修正案所保护的权利；其二，如果针对特定对象的监控构成宪法意义上的搜查，那么针对不特定对象的监控更会构成宪法意义上的搜查，比如把GPS追踪器安装在众多不特定的车辆上，当

---

〔20〕 Miller Kevin, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, 19 Journal of Technology Law & Policy 119 (2014).

〔21〕《刑事诉讼法》第151条规定："批准决定应当根据侦查犯罪的需要，确定采取技术侦查措施的种类和适用对象。"第152条规定："采取技术侦查措施，必须严格按照批准的措施种类、适用对象和期限执行。"《公安机关办理刑事案件程序规定》第255条规定："技术侦查措施是指由设区的市一级以上公安机关负责技术侦查的部门实施的记录监控、行踪监控、通信监控、场所监控等措施。技术侦查措施的适用对象是犯罪嫌疑人、被告人以及与犯罪活动直接关联的人员。"

〔22〕 See Allison Linn, *Post 9/11, Surveillance Cameras Everywhere*, NBC News (Aug. 23, 2011), http://www.nbcnews.com/id/44163852/ns/business-us_business/t/post-surveillance-cameras-everywhere.

然更是宪法上的搜查措施。〔23〕实际上，美国联邦最高法院在判例中已经就此问题表达了观点，如在1983年的United States v. Knotts案中，波斯纳法官就认为即便以追踪器对特定对象在公路上的行动进行追踪不构成搜查，针对不特定对象的遍地撒网式的24小时监控也是会构成搜查的。〔24〕在美国其他运用大数据监控的领域，这一问题似乎也有清晰的答案，如根据美国《外国情报监控法》，情报部门可以在总统授权下收集广泛的通信数据。但由于这种行政授权不符合司法令状的要求，所以可能会导致所获证据无法在普通刑事司法程序中使用，〔25〕无法使用的原因就在于这种具有侵害公民权利性质的大数据监控未经司法令状批准，这就肯定了针对不特定对象的大数据监控也是侵害公民基本权利的。而在其他国家，如英国、法国、意大利，无论是基于预防恐怖主义、严重犯罪而进行的事前监控，还是为了预防犯罪或侦查犯罪所进行的数据留存，均属于法律规制的对象，因为这些均是侵害公民基本权利的国家行为。〔26〕欧盟于2006年颁布的《数据保留指令》中，允许司法机关收集通信源数据、通信对象数据、通信基本数据等六类数据，但不允许收集通信内容数据，而且即便这六类非内容数据也需遵循比例原则，因为《数据保留指令》的目的即在于保护公民隐私权等基本权利。〔27〕

我国学者在探讨大数据监控与公民隐私权的关系时也指出，由于大数据监控具有数据收集的全景化、监控功能的预测化、监控目标的泛在化和全球化等特征，每个人都可能在数字世界中被建立档案，进行数字画像，因此，大数据监控中个人隐私与国家权力之间信息力量严重失衡，隐私面临着不可逆转的破坏性风险。〔28〕虽然我国在法律制度层面尚未涉及针对不特定对象的大数据监控是否侵害公民权利的问题，也未因此问题而引发法治危机，但这一问题却是随着科技发展所迟早要面临的，从近期为数尚不多的有关文献也可看出，已经有学者对此问题进行关注。〔29〕因此，对于这一问题，应当从理论上进行前瞻性的探讨，为日后对大数据监控进行法律规制奠定理论基础。从以下几个方面来看，针对不特定对象的大数据监控同样会侵害公民隐私权等基本权利。

1. 从由小及大、举轻以明重的角度来看，大数据监控会侵害不特定对象的权利。对特定对象的个人信息数据（包括个人身份、通讯、金融等信息）进行监控，即便监控的是非内容信息，根据下文所依据的原理，同样会因能够探知公民生活细节而侵害其隐私权。因此，如果对特定对象的个人信息数据进行监控构成对该人权利的侵害，那么就没有理由认为针对更庞大群体的监控反而不会侵害其权利，因为即便从直觉角度，这也是违反正义原则的，也没有任何可靠的理论能论证其并不侵害不特定对象的基本权利。正是因为如此，美国联邦最高法院才在United States v. Knotts案中表示，虽然针对特定对象在公共场所的活动进行监控并未违宪，但如果警

〔23〕 See Blitz, *supra* note〔18〕, at 69－70.

〔24〕 See Blitz, *supra* note〔18〕, at 70.

〔25〕 See Yoo, *supra* note〔18〕, at 923.

〔26〕 See Céline C. Cocq & Francesca Galli, *The Use of Surveillance Technologies for the Prevention, Investigation and Prosecution of Serious Crime*, EUI Working Paper LAW 2015/41, p.31.

〔27〕 Francesca Bignami, *Privacy and Law Enforcement in the European Union: The Data Retention Directive*, 8 Chicago Journal of International Law 248－252 (2007).

〔28〕 参见前注〔1〕，张衡文。

〔29〕 有关大数据监控与公民权利之间关系的文献，如王燃：《大数据时代侦查模式的变革及其法律问题研究》，载《法制与社会发展》2018年第5期，第110—129页；前注〔1〕，张衡文；王俊秀：《数据监控、隐私终结与隐私通货》，载《探索与争鸣》2018年第5期，第31—35页。

察机关采取的是天罗地网式的监控，则应该有不同的宪法原则的适用，以解释及适用宪法第四修正案的意涵及保障范围。〔30〕在大数据时代，虽然对全体公民的数据信息进行全景式监控对于预防恐怖主义、侦查严重犯罪等目的来说是非常重要的，甚至是必要的，但目的的重要性或手段对于达成目的的必要性并不意味着可以豁免其对公民权利的侵害，或对这种侵害视而不见，仍应正视大数据监控对不特定对象的侵权性，并对其进行必要的法律规制。以美国的情报监控为例，虽然在“9·11”事件之后，美国情报机构依据《外国情报监控法》、12333号行政命令等进行了众多的大数据监控项目，但这些项目仍要受制于情报监控法庭的司法审查，并且要受到是否符合美国宪法第四修正案的审查。〔31〕

2. 从大数据监控对不特定公民个人信息数据构成直接的危险来看，其也构成对公民权利的侵害。认为大数据监控并不侵害公民权利的一种理由是，大数据监控只是收集众多公民的信息数据，但除了对确实与犯罪相关的信息数据会加以关注和使用外，其他公民的信息数据并未被使用，所以并未侵害这部分公民的隐私权等基本权利。〔32〕但这种观点难以成立，因为权利是否被侵害的判断标准并不在于这种权利是否已经被实际侵害，而是在于该权利是否陷于被侵害的危险之中，只要公权力的监控行为将公民的某种权利客体置于随时可被他人利用、损害、泄露的境地，就已经构成了对该权利的侵害。例如，美国联邦最高法院通过卡兹案所确立的“合理的隐私期待”标准就是根据国家是否侵入了公民试图作为隐私而保护的客体而判断国家是否侵害公民隐私权，而并非已经实际对公民隐私造成侵害。〔33〕因为大数据监控对不特定公民的个人信息数据构成现实的威胁，所以已经侵害了公民的隐私权。

3. 大数据监控虽然在多数情况下针对的是不特定对象的非内容性数据，但仍会构成对公民隐私权的侵害。若按监控内容来看，可将公民个人信息数据分为内容性数据和非内容性数据，前者如电子邮件内容、网络聊天内容、交易详情内容等，后者如电子邮件收发地址、IP、电话号码、通信时间等。对内容性数据的监控通常被严格规制，一般要遵循特定案件规则、嫌疑事实规则、必要性规则、令状规则等；对非内容性数据的监控虽然受到的规制相对宽松，但同样也在适用的案件范围、嫌疑事实标准、令状等方面受到一定规范，〔34〕英美法及大陆法国家均是如此，如法国、英国、意大利的大数据监控中，只有基于调查或预防特定犯罪的目的才能实施对非内容性数据的监控，且在授权、时长、续期等方面都有严格规范。〔35〕之所以对看似无害的非内容性数据监控进行规制，是因为：其一，非内容信息也包含着公民的个人信息数据，公民对其中相当一部分享有合理的隐私期待；其二，也是更重要的，是因为将大量的非内容数据拼凑之后，同样可以探知公民的生活细节，这就是美国联邦最高法院在 United States *v*. Jones 一案中所提出的“马赛克”理论，即将零散的公民个人信息数据进行拼凑，就可窥看公民的生活全貌，并因此侵害公民的合理隐私期待。因此，对于判断大数据监控是否侵害公民基本权利这一问题来说，不能以所针对的是非内容性数据为由就

〔30〕 参见李荣耕：《科技定位监控与犯罪侦查：兼论美国近年GPS追踪法制及实务之发展》，载《台大法学论丛》2015年第3期，第871—969页。

〔31〕 Weaver, *supra* note〔18〕, at 1239.

〔32〕 Yoo, *supra* note〔18〕, at 912.

〔33〕 参见[美] 约书亚·德雷勒斯、艾伦·C. 迈克尔斯：《美国刑事诉讼法精解》(第一卷)，吴宏耀译，北京大学出版社2009年版，第73—74页。

〔34〕 参见刘梅湘：《侦查机关实施网络监控措施的程序法规制——以域外法的相关规定为参照》，载《法商研究》2017年第1期，第174—182页。

〔35〕 See Cocq & Galli, *supra* note〔26〕, at 15－16.

否认其会侵害公民权利，而应从其适用的最终效果来判断是否侵权以及侵权程度，只要公民对其中部分个人信息数据享有合理的隐私期待，或通过个人信息的拼凑叠加而探知公民生活细节，那么就会侵害公民的隐私权。

（二）大数据监控与“第三方理论”

在计算机和网络技术飞速发展的今天，人们日益离不开各类网络服务，如网络通信、购物、预定、支付等。但在使用这些服务的同时，人们通常需要提交自己的部分个人信息数据，如进行注册时所提供的姓名、身份证号、银行卡号、手机号码等，在每次使用服务时，还会留下交易时间、金额、地点、内容等信息；而且通常来说，人们也清楚地知道，作为第三方的网络服务商会留存这些数据信息，甚至也知道这些信息可能会在日后的诉讼中被用作对自己不利的证据。在刑事诉讼中，侦查机关确实会从这些第三方服务商处收集各种数据用于侦查取证。那么，是否因为人们明知个人信息数据会被留存而依然使用各类网络服务，侦查机关收集这类个人信息数据就不构成对公民权利的侵害呢？

在美国联邦最高法院1979年判决的Smith *v.* Maryland一案中，多数法官意见认为，即便被告人确实对所拨电话号码有隐私期待，这一期待也是不合理的。因为对于自愿提交给第三方的任何信息，个人就不再享有合理的隐私期待，〔36〕从而形成了所谓的“第三方理论”，自此之后，对于警方收集这种提交给第三方的个人信息是否构成宪法意义上的搜查，就适用该案提出的“第三方理论”。但问题在于，随着科技的发展，“第三方理论”目前在美国面临着严峻的挑战，因为在信息时代人们所运用的几乎全部网络服务都会将个人信息数据提供给网络服务商，包括电子邮件、搜索引擎、社交软件等，而这些网络服务对于现代人来说是不可或缺的，〔37〕在这种背景下，再以“第三方理论”作为判断人们提交给网络服务商的个人信息数据是否具有合理隐私期待就有些不合时宜了，正如美国联邦最高法院大法官索托马约尔（Sotomayor）在United States *v.* Jones一案中所言：

> 这一理论很难适用于数字化时代，因为人们为了日常生活所需必须向第三方提供大量个人信息，为了拨打电话就要向移动服务商提供电话号码；为了上网就要向网络服务商提供网址和邮箱地址；为了网上购物就要提供所购买的书名、商品种类或药品名称；等等。人们的这些个人信息不应该仅因为要使用网络服务必须提供给第三方就失去宪法第四修正案的保护。〔38〕

正是在这种对“第三方理论”的反思下，美国有学者认为，对于电子邮件、电话、短信等现代通信手段来说，人们是否享有合理的隐私期待是值得研究的重要问题。〔39〕虽然也仍有人坚持认为，即便在大数据时代，人们主动提供给各类服务商的个人数据也不再享有合理的隐私期待，无论是某个特定人的个人数据，还是不特定人的个人数据。但这种不顾现实而简单固执己见的观点似乎难以产生足够的说服力，尤其是这种观点忽视了美国法院在近年来一些案件中已经发生的态度变化。如早在2001年的Kyllo *v.* United States案中，联邦最高法院就通过判决而体现了对新技术侵犯公民合理隐私期待的关注；在2010年的City of Ontario *v.* Quon一案中，联邦最高法院虽然

〔36〕 参见前注〔33〕，约书亚·德雷勒斯、艾伦·C. 迈克尔斯书，第98页。

〔37〕 Andrew B. Talai, *Drones and Jones: The Fourth Amendment and Police Discretion in the Digital Age*, 102 California Law Review 756 (2014).

〔38〕 Donohue, *supra* note〔18〕, at 887.

〔39〕 Weaver, *supra* note〔18〕, at 1232.

没有对新科技给人们的权利带来的侵害设置固定的规则，但表达了如下观点：由于信息传播手段的飞速发展，社会对于何为合理行为、何为不合理行为的观念也随之变化；在 2014 年的 Riley *v*. California 案中，法院又通过对公民权利保护与政府行为所能促进的社会利益进行权衡，认定警方未经令状批准而搜查公民手机内容的行为构成宪法上的搜查。这些案例虽然并未直接针对大数据监控是否仍适用“第三方理论”问题，但从中不难看出科技的发展使美国司法更为注重对个人权利进行保护的倾向。不过从总体上看，对于这一问题尚无明确结论，在部分案例中，法院也依然适用“第三方理论”而判决通信一方自愿将通信内容及相关数据提交给第三方，所以就丧失了合理的隐私期待；〔40〕对于警方收集手机基站数据是否侵害公民隐私权的问题，美国联邦下级法院和各州法院在一些案件的判决中也认为，公民对于手机基站数据不享有合理的隐私期待，警方无须按照宪法第四修正案的要求对基站数据进行监控和收集。〔41〕

相对而言，欧盟对这一问题的态度比较明确。根据上述《数据保留指令》，服务商必须根据《数据保留指令》所规定的合目的性、比例性、期限、数据安全等要求进行数据的保留和利用。可见，欧盟并不认为人们使用网络服务而将个人信息数据提交给第三方就失去了对个人信息的权利，虽然这些个人信息数据的隐私程度较低，但仍属于公民隐私权对象的一部分，对国家机关利用这些个人信息数据依然要进行严格的规制，只有在与正在进行的犯罪调查相关的前提下才能进行收集和利用，并且利用之后要进行销毁或匿名化处理。〔42〕 因此，在欧盟的法律体系中并不适用“第三方理论”，这体现出对公民个人信息数据的高度保护。

我国在侦查行为规制理论中，并无类似于美国的这种“第三方理论”，对侦查行为是否侵害公民权利的判断主要是根据这种权利是否有法律依据而具体判断。大数据监控主要可能会侵害的是公民的隐私权，我国以往在刑事诉讼中并不重视公民隐私权，但 2012 年《刑事诉讼法》的修订中增设技术侦查一节，彰显了对公民隐私权保护的立法目的。〔43〕 因此，对于我国对大数据监控的法律规制必要性来说，也首先需要确定大数据监控所针对的公民使用各类网络服务而留存的数据是否属于隐私权对象的问题。根据隐私权的一般原理，参考上述美国的相关理论，可得出如下结论：这种留存的个人信息数据中的相当一部分依然属于公民隐私权的保护对象。

1. 公民将这些个人信息数据提供给服务商，并非选择权使然，实属无奈之举。目前，各类网络服务商所提供的服务均以使用者让渡一定的个人信息数据为前提条件，虽然在使用之前也会对用户进行权利告知（如隐私条款告知），但这并非赋予用户是否让渡个人信息的选择权，而是将让渡个人信息作为使用某种网络服务的前提条件，所以对于人们来说，将个人信息让渡给服务商实则不得已之举，而并非真正基于选择权的自愿让渡。在这种普遍情形下，若直接适用“第三方理论”而认为公民将个人信息提交给服务商就失去了隐私权，无异于否定了公民在大数据时代对诸多个人信息的隐私权，明显有失公正。

2. 退一步说，即便公民确实是出于自愿而将个人信息数据提交给第三方服务商，也是以使用服务商提供的某种服务为目的的，而通常不会想到侦查机关会对这些数据进行监控并用于侦查目

---

〔40〕 Nicole Cohen, *Using Instant Messages as Evidence to Convict Criminals in Light of National Security: Issues of Privacy and Authentication*, 32 Criminal and Civil Confinement 320 - 326 (2006).

〔41〕 Brian L. Owsley, *The Fourth Amendment Implications of The Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 Journal of Constitutional Law 24 - 29 (2013).

〔42〕 Bignami, *supra* note〔27〕.

〔43〕 参见全国人大常委会法制工作委员会刑法室：《关于修改中华人民共和国刑事诉讼法的决定：条文说明、立法理由及相关规定》，北京大学出版社 2012 年版，第 185 页。

的，尤其是不会预见到侦查机关对这些数据的同步监控。所以，公民向第三方提交个人信息数据的目的上的特定性，也不会使提交行为本身就产生丧失针对侦查机关监控的抵御效果。正如前述美国联邦最高法院大法官索托马约尔所言，这些个人信息不应仅因公民要使用网络服务必须被提供给第三方，就失去美国宪法第四修正案的保护。在不实行“第三方理论”的我国，基于同样的道理，人们不应当因为使用某项网络服务就自动丧失了对所提供个人信息的隐私权。

3. 但对于侦查机关监控、收集公民提交给第三方服务商的各类个人信息数据是否侵害公民权利这一问题，要根据具体情况而分别考虑。在公民提交给第三方服务商的个人信息数据中，有相当一部分被转化为服务商的业务记录，如网络服务商对电子邮件或数据传输的记录、移动通信服务商对移动通信数据的记录等。对于这些转变为业务记录的数据，侦查机关进行收集是否侵害公民隐私权，要根据不同情形而具体判断。如果侦查机关只是事后被动地收集业务记录，则只是普通的收集证据行为，不构成数据监控；如果侦查机关事前指令服务商收集某类业务记录供侦查使用，无论是特定公民还是不特定公民的信息，在这类业务记录属于碎片化信息、不会通过拼凑而发现人们生活细节全貌的情况下，仍不构成对公民权利的侵害；只有当侦查机关指令收集的信息能够通过拼凑而窥见公民生活全貌，或指令服务商收集正常业务记录之外的公民其他信息时，才构成对公民隐私权的侵害，因为公民对于侦查机关的长期监控并将信息进行拼凑或对正常业务记录之外信息的收集并无任何预见的可能性，所以理论上对这些个人信息数据具有合理的隐私期待。

（三）公共领域大数据监控与公民权利

随着网络技术、监控科技的发展和普及，目前通过视频监控系统、网络监控技术已经实现了对人们在公共场所和网络公共领域中各种活动的全方位监控，由此形成对公共场所及网络公共领域的大数据监控，通常是从海量的公共场所视频监控、[44]网络公共领域监控数据中寻找有用的部分，用于搜寻特定主体、查获犯罪嫌疑人、收集诉讼证据等。那么，对公共场所及网络公共区域中不特定对象进行的大数据监控，是否会因为人们身处公共场所或信息处于网络公共领域就不构成对公民权利的侵害呢？

在美国的刑事诉讼理论和实践中，早在1924年的Hester *v.* United States案中就形成了“公共领域”(open field)规则，在Katz *v.* United States案之后的Oliver *v.* United States案中，联邦最高法院又重申了这一规则，即公民对其在公共领域的活动不享有合理的隐私期待，因为第四修正案旨在保护不受政府侵扰或监控的私密活动，而公共领域并未提供相似的保护，所以对于在公共领域发生的活动，不存在对其隐私进行保护的社会利益。这表明，虽然Katz案确定了公民的合理隐私期待的判断标准是主客观兼顾的，但这并未否定公共领域规则，公共领域规则依然是宪法第四修正案的核心部分。在这种宏观背景下，公民在公共场所或网络公共领域的活动很难被认定具有合理的隐私期待，如在公共场所视频监控是否侵害公民隐私权的问题上，长期以来，联邦法院和州法院均不太可能判定其构成对公民隐私权的侵害。[45]

但随着科技的发展，美国刑事司法中这一长期实行的“公共领域”规则开始出现松动，这主要是因为理论界首先对该规则进行发难，其后法院在部分案件中吸收了一些理论界的观点并做出积极回应。如针对公共场所视频监控问题，有学者认为，公共场所视频监控在人们不知情的情况下

〔44〕 参见何遥：《公安大数据时代的视频监控》，载《中国公共安全》2019年第Z1期，第148—153页。

〔45〕 Quentin Burrows, *Scowl Because You're on Candid Camera: Privacy and Video Surveillance*, 31 Valparaiso University Law Review 1083 (1997).

对人们的行为进行持续监控，如监控人们在公共场所阅读的信件、所说的话等，这都是对隐私的侵害；还有学者认为，人们在公共场所同样享有隐私权，而且有不被他人关注的权利，法院应当致力于保护人们在特定场所的权利；[46]另有学者更直接指出，即便在公共场所，公民也享有合理的隐私期待，即期待政府不会使用科技手段而侵入其私人领域。[47] 正是在理论界的推动下，司法实践也有所回应，尤其体现在2012年的United States *v*. Jones案中，虽然理由各不相同，但美国联邦最高法院的大法官均认为对琼斯(Jones)的汽车进行长达28天的追踪构成宪法上的搜查，尽管该汽车一直在公共道路上行驶而未进入私人场所。撰写了协同意见的阿里托(Alito)法官认为，通过对个人信息的全面记录，就能由此了解人们的各类生活细节，所以审查标准应当是人们是否能预见自己的各种生活细节被政府记录——如果能预见到，则政府对个人生活细节的长时间监控就构成搜查。虽然该案并不是直接针对公共场所视频监控或网络监控等大数据监控，而且也不是针对不特定对象的监控，但根据该案的逻辑，针对不特定对象的公共场所视频监控或网络监控可运用同样的原理，认定构成对公民权利的侵害。在这种理论的转变下，美国和加拿大法院在部分案件中对公共领域的监控问题做出一些积极裁判，肯认了公民在公共领域的隐私权，如一些根据公民的手机基站转储信息而监控移动轨迹的案件。

而在我国，对于公民在公共场所或网络公共领域是否具有隐私权、侦查机关对公共场所和网络公共领域的监控是否属于强制措施研究较少，而多数研究均是针对《刑事诉讼法》所规定的针对特定对象的技术侦查措施，并且即便在技术侦查的研究中也很少涉及对个人在公共领域的活动进行监控是否属于技术侦查的问题。大数据监控是在大数据技术支持下实现的一种大规模监控，所以也可能会侵害公民权利，即便是针对公共场所或网络公共领域的监控也是如此，这主要是基于如下两点理由。

1. 即便公民身处公共场所，或在网络公共领域进行表达、交流，也仍对其中部分信息享有隐私权。公民在公共场所或网络公共领域的活动是否属于隐私权对象，不能一概而论，有些活动难以具有合理的隐私期待，如在公共场所不加掩饰地大声交流，或在网络上发表披露个人隐私的内容；但对于有些活动，公民仍应具有合理的隐私期待，如在公共场所进行私密性的交流，或在网络公共领域发表隐匿身份的言论。关键之处在于，对于这部分应当享有合理的隐私期待的活动，一般民众难以预料侦查机关会进行密集的监控，往往都是在自认为不会泄露自身隐私的情况下才从事这些活动，而且一般也是出于不欲为人知的动机，否则就不会采取私密交流或匿名发表言论的方式。所以如果侦查机关不加区分地对所有人在公共场所或网络公共领域的所有活动进行监控，必然会侵入人们享有合理的隐私期待的那部分活动，构成对公民隐私权的侵害。

2. 即便对于公民在公共场所或网络公共领域所从事的那些不具有合理隐私期待的活动，如果进行长期、密集的监控，就能够通过将这些信息拼凑起来而探知公民的生活细节，从而侵害公民隐私权。虽然公民在公共场所或网络公共领域的活动也会被其他人观察到，但这种观察一般都是短时的、片段化的，其他人难以通过这种“惊鸿一瞥”而探知某个公民的生活细节。而侦查机关对公共场所或网络公共领域的监控则不同，通常是长期的、密集的，即便并非针对某一特定对象，也会

---

〔46〕 Marc Jonathan Blitz, *Video Surveillance and The Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity*, 82 Texas Law Review 1398 (2004).

〔47〕 Robert D. Bickel, Susan Brinkley & Wendy White, *Video Security Technology Compromise an Essential Constitutional Right in a Democracy, Or Will the Courts Strike a Proper Balance?* 33 Stetson Law Review 304 (2003).

在监控中通过信息拼凑而发现某些被监控对象的不欲为人知的生活细节，如通过对微博、论坛的长期监控，发现某人的活动轨迹、交往对象、收入情况等，这就是所谓的“马赛克效果”，即通过对个人在公共场所的行为的长期监控，就如同个别、细小的瓷砖结合在一起而形成马赛克镶嵌画，足以窥见该人生活全貌。如果对侦查机关的此种监控不加规制，就等于纵容侦查机关通过各种科技手段对公民在公共领域的活动进行任意监控。因此，对公民在公共场所或网络公共领域中那些看似并无合理期待的公开行为，如果要进行长期、密集的监控，仍可能会侵犯公民的隐私权。

三、大数据监控侵害公民权利的特征及其规制路径

从以隐私权为样本对大数据监控措施与公民隐私权之间关系的探讨来看，侦查中运用大数据监控措施时，多数情况下是会侵害公民隐私权的，因此应按照强制侦查措施进行法律规制。但从上述探讨中我们也可看出，大数据监控在侦查中的运用与一般强制侦查措施对公民基本权利的侵害在特征上有所不同，因此，对大数据监控的法律规制也将有其不同的特征。

（一）大数据监控侵害公民权利的特征

1. 侵权的长期性

在大数据监控运用于侦查的几种途径中，当用于收集证据、查找特定对象、对特定对象进行监控时，通常是在个案中运用，属于纯粹的刑事侦查措施，其实施的期限较短，随着侦查的结束而结束。但当大数据监控用于预防、发现、同步监控犯罪时，则兼具行政属性的犯罪预防功能和刑事司法属性的犯罪侦查功能，且这种监控是长期实施的，对于这种兼具行政和侦查属性的长期监控如何进行法律规制是必须首先解答的问题。尤其是在我国公安机关同时具有行政职能和刑事侦查职能的情况下，要研究如何对其基于犯罪预防和监控目的而长期运用大数据监控措施进行法律规制。对此，我国有学者提出过不同建议：有学者认为应当借鉴英国的模式，通过统一的警察职权行为法对行政行为与侦查行为进行统一的授权；[48]但也有学者认为应当突破刑事诉讼程序结构对侦查权概念重新进行定义，设定侦查权的启动条件、限定范围、规制程序，[49]即由《刑事诉讼法》进行规制。究竟如何进行法律规制，需要根据我国的现实情况，并借鉴域外的做法进行充分论证。

2. 侵权的秘密性和技术性

从本质上来说，大数据监控在侦查中运用时，与我国《刑事诉讼法》目前规定的针对特定对象的技术侦查措施是相近的，只不过大数据监控措施针对不特定对象，且具有一定的犯罪预防功能而已。因此，大数据监控对公民隐私权的侵害与技术侦查措施一样，具有技术性、秘密性的特征。但由于《刑事诉讼法》及其司法解释将技术侦查明确限定为针对特定对象，因此在对大数据监控的法律规制中，如何进行规范的协调和整合，也是需要考虑的问题。

3. 面广但度轻

从大数据监控运用于侦查的方式来看，对公民隐私权的侵害基本上都具有“面广但度轻”的特征，即虽然大数据监控的对象范围是所有公民，而非像一般技术侦查措施仅针对特定对象，但大数据监控多数情况下仅以公民的通讯基本信息、业务记录、公共领域的行为或言论等作为监控内容，比一般技术侦查措施对公民基本权利的侵害程度要轻很多，也正是因为如此，域外对大数据监控

〔48〕 参见刘方权：《“两面一体”：公安行政权与侦查权关系研究——基于功能的分析》，载《法学论坛》2008年第4期，第82—89页。

〔49〕 参见前注〔12〕，韩德明文。

的规制一般较之对普通监控措施的规制宽松，甚至并不认为某些大数据监控侵害公民隐私权（如美国法院对业务记录、公共场所视频监控较为普遍的态度是不构成对公民权利的侵害）。因此，对侦查中大数据监控的法律规制应根据其对公民权利侵害“面广但度轻”的特征，按照比例原则的要求，进行力度适当的法律规制。

（二）大数据监控的法律规制路径

在规划对侦查中运用大数据监控的法律规制路径时，应根据如上侦查中运用大数据监控措施侵害公民隐私权的几个特征进行合理、有效的规制。以下将从法律规制的方式、相关制度的改革等几个方面简要论述。

1. 以《刑事诉讼法》为主体进行规制

用于收集证据、查找特定对象、对特定对象进行监控等几种用途的大数据监控措施，属于纯粹的刑事侦查措施，直接以《刑事诉讼法》进行规制即可，但对于兼具犯罪预防及侦查功能的大数据监控措施，则存在以何种法律规制的问题。对此，我们可以先对域外的相关做法进行比较考察。

在域外，各国采取的具体规制方式虽然有所不同，但一个共同的特征是均以宪法或刑事诉讼法的规制为主，而以其他法律规制为辅。如在美国，对于大数据监控主要由《爱国者法案》第215条、《外国情报监视法》第702条、12333号行政命令（由里根总统于1981年签发，对情报收集活动做出授权）进行规范，但这些规范同样严格受制于合宪性审查，尤其是宪法第四修正案对政府的监控行为发挥着重要的制约作用。〔50〕而在德国，除了在《刑事诉讼法》第100条c规定“特别侦查技术手段”的对象可以扩展至“不可避免地被涉及的第三人”之外，第98条a、b还允许采取“栅网追缉”这种大规模数据监控手段筛选犯罪嫌疑人，〔51〕另外，德国还以《数据保护法》等行政法对大数据监控进行规制。法国、意大利两国均区分基于犯罪侦查的司法性监听和基于犯罪预防的行政性监听，〔52〕但法国对于两类监听统一以1991年通过的646号法律在《刑事诉讼法》中增加电讯截留一节进行规范，只不过行政性监听后来又被吸收整合到《国内安全法》之中；意大利对于司法性监听由《刑事诉讼法》第266条进行规范，而对于行政性监听则以2001年颁布的438号法律（《反恐怖主义紧急法》）进行特别规范，该法在性质上属于特别刑事诉讼法。〔53〕

从以上各国的规制方式来看，之所以普遍以宪法或刑事诉讼法为主对大数据监控进行规制，是因为针对不特定对象的大数据监控措施与针对特定对象的监控措施性质类似，都会对公民基本权利构成侵害，只不过程度不一而已，因此以宪法或刑事诉讼法这种高位阶法律对大数据监控进行规制，才能通过对国家权力进行更严格的限制，更好地保护公民权利。而且，在侦查中运用的各类大数据监控措施，最终目的都是刑事追诉，即便兼具犯罪预防与侦查功能的大数据监控也是如此，所以也应以宪法或刑事诉讼法对其进行规范。

我国《刑事诉讼法》在2012年修改时增设了针对特定对象的技术侦查措施，但并未涉及针对不特定对象的大数据监控，而近几年我国陆续颁布的《反恐怖主义法》《国家安全法》《网络安全法》

---

〔50〕 Weaver, *supra* note〔18〕, at 1223－1239.

〔51〕 参见[德] 克劳思·罗科信：《刑事诉讼法》，吴丽琪译，法律出版社2003年版，第72页。

〔52〕 这里的监听，英文原文为“interception”，是一个广义概念，不限于电话监听，还包括对通过电子邮件或其他通过网络的通信的监控。如英国《侦查权力限制法》将作为监听对象的“通信系统”界定为“任何为了便利通信传送而利用电能或电磁能的系统”。

〔53〕 See Cocq & Galli, *supra* note〔26〕, at 9－11.

等行政法律中，虽然有少数条款涉及大数据监控的运用，〔54〕但并未对国家机关如何运用大数据监控做出应有的程序规制。基于如上所述的理由，大数据监控在侦查中运用时会侵害公民基本权利，属于应予规制的强制侦查措施，因此只有以属于基本法律的《刑事诉讼法》进行规范，才能更好地保护公民基本权利。如果以行政法进行规范，难以取得保护公民基本权利的实效，在刑事诉讼中也会给当事人带来法律适用的困难。所以，对于侦查中运用的大数据监控，即便其兼具犯罪预防和刑事侦查功能，也应以《刑事诉讼法》进行规范，从程序及证据两个方面对大数据监控在侦查中的运用进行规制。对于监控的建设、管理、实施、资料保管等方面，也可由行政法规进行辅助性的规范，但要实现与《刑事诉讼法》的协调和衔接，因为在侦查机关收集大数据监控资料作为证据时，其证据能力判断与监控的合法性有密切关系，所以行政法规在进行监控的授权和规范时，应当考虑到刑事司法的要求，以便于刑事诉讼中对监控证据合法性的审查判断。

2. 相关制度的修正

按照如上设想，如果由《刑事诉讼法》对侦查中大数据监控的运用进行规制，则有必要对现有的相关制度进行修正，具体而言主要在于如下两个方面，即技术侦查对象范围的扩大和立案制度的改革。

如前所述，大数据监控与目前《刑事诉讼法》规定的技术侦查措施是相似的，都具有秘密性、技术性特征，但区别在于对象的不同。大数据监控的特征决定了其只有尽可能地搜集更多的信息，才能发现犯罪的相关线索和证据，并用于刑事侦查。然而，仅因为大数据监控针对不特定对象就将其排除在技术侦查措施之外是没有合理根据的，大数据监控同样会侵害公民基本权利，而且侵害的是不特定多数公民的基本权利，侵权范围更广，尽管可能比针对特定对象的监控措施的侵权程度要轻，如针对公民通信基本数据（时间、地点、次数）的监控虽然比针对通信内容的监控侵权程度轻，但依然会侵害不特定公民的隐私权；〔55〕而且某些大数据监控措施也可能与技术侦查措施的侵权程度相当，如通过邮件关键词监控系统监控公民的电子邮件。因此，对大数据监控理应进行与技术侦查同样的法律规制，如果日后我国能够将大数据监控纳入《刑事诉讼法》规制，就应扩大技术侦查的对象范围，将针对特定对象与不特定对象的监控措施均作为技术侦查措施进行规制，只不过可以根据对公民权利的侵害程度而进行宽严有别的规制。

另外，我国《刑事诉讼法》将立案作为侦查的前提，〔56〕侦查机关在立案前不得采取任何强制侦查措施。但对于兼具犯罪预防与犯罪侦查的大数据监控来说，是难以满足先立案后实施的要求的。这种大数据监控的实施是长期的、常态化的，在未发现犯罪时，主要发挥犯罪预防作用，但一旦发现犯罪，就可以同步监控、记录犯罪过程，以供侦查人员发现线索、收集证据。所以，这种大数

〔54〕 如《反恐怖主义法》第45条规定："公安机关、国家安全机关、军事机关在其职责范围内，因反恐怖主义情报信息工作的需要，根据国家有关规定，经过严格的批准手续，可以采取技术侦察措施。"《国家安全法》第42条规定："国家安全机关、公安机关依法搜集涉及国家安全的情报信息，在国家安全工作中依法行使侦查、拘留、预审和执行逮捕以及法律规定的其他职权。"第52条规定："国家安全机关、公安机关、有关军事机关根据职责分工，依法搜集涉及国家安全的情报信息。国家机关各部门在履行职责过程中，对于获取的涉及国家安全的有关信息应当及时上报。"《网络安全法》第28条规定：" 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。"第50条规定："国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。"

〔55〕 Donohue, *supra* note〔18〕, at 864.

〔56〕 参见郎胜：《中华人民共和国刑事诉讼法修改与适用》，新华出版社2012年版，第231页。

据监控的使用使得犯罪预防与侦查之间近乎无界限，正如国外学者所言，新型监控科技的运用使犯罪侦查与犯罪预防（情报收集）之间的界限变得模糊，使侦查模式转型为“预防性的、先发制人的、情报主导的”（prevention, proactive investigations and intelligence-led policing），[57]侦查监控措施的启动并无明显界限，可随时启动。在这种情况下，目前《刑事诉讼法》中的立案制度就会对侦查中大数据监控措施的运用造成阻滞，甚至导致大数据监控在侦查中的运用产生合法性危机。因此，应当根据监控技术的发展以及大数据监控在侦查中的运用现状，对我国的立案制度进行改革，使《刑事诉讼法》的规制范围更广，能够涵盖侦查机关任何时候实施的侵害公民基本权利的监控行为。

3. 根据大数据监控措施的作用、对象、内容而进行区别性规制

如果能够实现《刑事诉讼法》对大数据监控的规制，也应注意遵循比例原则，对其法律规制的宽严应考虑其在侦查中的具体作用、监控的对象、监控的内容而有所区别。

（1）对于将大数据监控措施用作监控特定对象的情形，应当进行较为严格的规制，因为这种情形一般是对内容性信息或公民行为细节的监控，对公民的隐私权等基本权利侵害较为严重，实际上就相当于目前《刑事诉讼法》所规定的技术侦查措施，所以对于这种情形至少要维持目前对技术侦查的规制水平。但如果针对特定公民的监控是针对非内容性信息的，或者针对公民在公共场所的行为，其法律规制可以宽松一些。

（2）对于将大数据监控用作监控不特定对象的情形，则可以进行相对宽松的规制，因为这类情形中对公民权利的侵害程度往往比较轻微，具有“面广但度轻”的特征，所以对其进行规制无须达到与针对特定对象的监控相同的水平。有的大数据监控在侦查中的运用甚至不会侵害公民的任何权利，属于任意侦查手段，无须进行严格的法律规制。但如果针对不特定对象的大数据监控是针对内容性信息的，属于侵害面广且侵害度深的监控措施，如美国的棱镜计划对电子邮件、即时消息、文件传输等内容性信息均可进行监控，对于这类监控措施应进行严格的规制。

（3）如果某种大数据监控除了具有犯罪侦查功能之外，还具有及时制止犯罪的功能，则对这种监控措施的规制可更为宽松，因为《刑事诉讼法》虽然旨在通过对各类强制侦查措施的法律规制而保障公民基本权利，但也不可忽视打击、遏制犯罪的需求，如果通过大数据监控的实施能够有效地遏制未然之罪，有利于保障秩序和安全，对其法律规制就无须太过严格。例如通过网站监控可以发现危害国家安全、诈骗、淫秽等信息并及时采取断开链接、删除等措施，避免犯罪产生实害，对于这种网站监控的实施条件、程序等方面，就无须施加过于严格的限制，而应设定宽松、灵活的条件。

4. 程序及证据规则

对于侦查中大数据监控的运用，要从程序及证据方面进行双重的规制。在程序方面，在对现有的侦查概念、技术侦查适用对象范围进行改造的基础上，根据大数据监控的不同用途和监控内容进行规范。对于兼具侦查及犯罪预防功能且长期实施的大数据监控，应对实施条件、实施主体、实施周期、批准程序、技术标准、监控材料保管及保密等事项做出详细规范；而对于其他三种用途的大数据监控运用，则需从申请主体、申请条件、批准程序、实施程序等方面进行规范。

在证据规则方面，主要是针对非法运用大数据监控而获取证据的排除规则，以及根据大数据监控的科技特征而设置不可靠证据的排除规则，以发挥对侦查取证的引导作用。

对于非法监控证据排除规则来说，由于《刑事诉讼法》中非法证据排除规则从字面上仅限于犯罪嫌疑人、被告人口供等言词证据和物证、书证，若依文义解释，难以涵盖电子数据类证据，相关的

---

〔57〕 See Cocq & Galli, *supra* note〔26〕, at 56.

司法解释也未将非法证据排除的范围涵盖电子数据，而通过大数据监控收集的恰恰基本上就是电子数据。因此，有必要将电子数据正式纳入非法证据排除规则的范围。〔58〕但由于侦查中大数据监控运用的复杂性，对所获证据的非法证据排除应根据其运用目的、监控对象、侵权程度而进行区别对待，做到宽严适当。

另一方面，由于大数据监控涉及数据采集、数据清洗、数据挖掘、数据分析等技术，所以应当有相应的证据规则保障监控证据的可靠性，即如果在监控证据的采集、清洗、挖掘、分析等环节中，如果存在可能会影响数据真实性、完整性的因素，且无法以其他方式确定数据的真实性和完整性的，就应当将该证据排除，以防止因采纳这些不可靠证据而导致错误认定事实。这类证据规则的基本原理为：除非能够确认电子数据的真实性、完整性，否则，如果在其产生、收集、流转、保管环节中存在影响其真实性或完整性的因素，就应当将其排除。

Abstract In criminal investigation, the use of big data surveillance is increasing day by day. Therefore, it is necessary to research whether big data surveillance will infringe on civil rights and provide a theoretical basis for the legal regulation of big data surveillance. Although big data surveillance aims at non-specific objects and usually only monitors non-content information, it may still infringe on civil rights because it poses a real threat to the personal information data of non-specific citizens. In modern society, citizens' submission of personal information data to third parties does not mean giving up their rights to personal information data. We should judge whether it constitutes a violation of civil rights according to the different situations in which the investigative organs obtain personal information data of citizens. Even if citizens are in public places or express and communicate in the network public sphere, they still have the right to privacy of some of their information. Moreover, for those activities that citizens do not have reasonable privacy expectations in public places or network public spheres, long-term and intensive monitoring will also infringe on citizen's privacy rights and other rights. In order to deal with the challenges brought by big data surveillance, we should research the basic connotation and scope of civil rights in the context of criminal procedure, rethink and innovate the technical investigation rules and their theoretical basis in the current Criminal Procedure Law of China, and study the intervention degree of various big data surveillance measures on civil rights.

Keywords Big Data Surveillance, Privacy Right, Legal Regulation

（责任编辑：林喜芬）

〔58〕 参见曾赟：《监听侦查的法治实践：美国经验与中国路径》，载《法学研究》2015年第3期，第170页。