法学研究 Chinese Journal of Law
Vol.44，No.2（2022）

纪检监察机关大数据监督的规范化与制度构建

杨建军*

内容提要：多地纪检监察机关开展的大数据监督实践探索，推动了权力监督制约机制的现代化，也引发了对于大数据监督正当性的追问。当前的大数据监督实践，缺乏规范化的大数据支撑和明晰的大数据监督准则，在制度层面存在赋权不足和限权不足的问题。完善大数据监督制度，既需要对纪检监察机关共享大数据予以制度赋权，也需要强化对纪检监察机关大数据监督的权力制约，化解数据处理规则与监督规则、数字逻辑与法律专业逻辑之间的冲突。应明确纪检监察机关对政务大数据的共享权力，及其对政法类数据与法律监督类数据的调取和使用规则；规范纪检监察机关技术调查手段的使用；改进非立案情形下的数据查询制度。纪检监察机关在查办涉嫌刑事犯罪的案件时，还应对照刑事诉讼证据规则搜集、调取和固定证据，避免证据因违反法定程序而被排除。

关键词：纪检监察　大数据监督　个人信息保护　政务数据

引　言

数据应用技术的不断突破，为改进和创新监管、监督机制提供了技术可能。通过数据捕获、清理、聚合、挖掘和解释等步骤不断完善算法，计算机系统逐渐具备了处理快速变化、类型多样的数据的能力。技术的进步也不断推动社会治理的数字化转型以及监管技术的广泛运用。从全球范围来看，随着数据分析工具的日益强大，政府扩大了监控范围。〔1〕大数据被很多国家运用于警务活动，包括预测性警务、大规模监控和大数据 DNA 分析等。〔2〕在美国，政府监管机构和一些私人机构收集大量数据，“并使用先进的机器学习工具进行分析，以更好地监督和了解非营利组织”。〔3〕在英国，税务和海关管理局使用大数据系统检测税务欺诈和逃

* 西北政法大学法治学院教授。
本文系 2017 年度国家社科基金一般项目“惩戒性党内法规与国家法律的冲突与化解研究”（17BFX014）的阶段性成果。

〔1〕参见［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 29 页。

〔2〕See Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 Wash. L. Rev. 42 – 55 (2014).

〔3〕See Lloyd Hitoshi Mayer, *The Promises and Perils of Using Big Data to Regulate Nonprofits*, 94 Wash. L. Rev. 1335 (2019).

税行为，并取得不菲成绩。〔4〕事实表明，当代执法工作高度依赖技术驱动，“它整合了大量信息、机器学习算法和人工智能来识别和跟踪潜在的违法者”，且比以往任何时候都依赖更广泛的数据，如犯罪数据、个人数据、关联数据、位置数据、环境数据等，而这些数据主要来自“不断增多的传感器和监视源网络”。〔5〕

在中国，大数据也被运用于多个领域。在警务领域，多地警务部门建立了“大数据警察支队”或相关机构。〔6〕在检察领域，2021 年 6 月 15 日，中共中央印发《关于加强新时代检察机关法律监督工作的意见》，明确要求“加强检察机关信息化、智能化建设，运用大数据、区块链等技术推进公安机关、检察机关、审判机关、司法行政机关等跨部门大数据协同办案”，以支持和保障检察机关的法律监督工作。在纪检监察领域，多地纪检监察机关先后开展了大数据监督的探索。早在 2015 年，作为中国“数谷”的贵阳市即启动了“数据铁笼”反腐行动。〔7〕2017 年，广西壮族自治区玉林市纪检监察机关借助民生资金监管平台推进大数据监督。〔8〕2018 年，沈阳市纪检监察机关开发了“集监督、公示、分析、预警等功能于一体的正风肃纪大数据监督平台”。〔9〕大数据可以映射人际关系，对不同的数据集通过标识进行连接，有助于在联合数据中得出推导结论。〔10〕大数据还有助于监督机关更多地汇聚“长尾数据”，将散落在不同空间的数据汇总起来，形成数据合力，提高监督工作效率。多级多地的实践表明，运用大数据开展纪检监察监督，已然成为纪检监察机关青睐的监督方式。如何在理论上认识纪检监察机关的大数据监督，此种权力监督制约模式在实践中会面临哪些问题，应当通过何种制度构建确保其在法治的轨道上规范化运行，这是本文重点关注并尝试回答的问题。

一、纪检监察机关大数据监督的实践

纪检监察机关的大数据监督，是指纪检监察机关运用大数据技术对各类公权力行使主体的行为进行的监督，包括运用大数据跟踪权力运行、发现案件线索、调查取证、查办案件等，以及通过大数据“自动化决策”等方式发现问题并作出监督决策。当下纪检监察机关开展的大数据监督，是纪检监察机关基于党内法规及国家监察法律法规概括性赋予的权力，在对各种公权力履行监督制约职能时，结合大数据技术进行的创新和探索。

纪检监察机关开展的大数据监督，不同于公安机关等部门的大数据侦查、大数据监控或预测性警务。大数据侦查主要是指刑事办案机关依法“对存储于网络与计算机系统中的海量数据进行收集、共享、清洗、对比和挖掘，从而发现犯罪线索、证据信息或者犯罪嫌疑人的侦查措施与方法”。〔11〕公安机关的大数据监控，即“以个人数据为核心，通过大规模、系统化地

〔4〕 See Bart van der Sloot & Sascha van Schendel, *Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study*, 7 J. Intell. Prop. Info. Tech. & Elec. Com. L. 116 (2016).

〔5〕 See Sarah Lamdan, *When Westlaw Fuels ICE Surveillance: Legal Ethics in the Era of Big Data Policing*, 43 N. Y. U. Rev. L. & Soc. Change 256 – 257 (2019).

〔6〕 参见张涛：《论大数据警务及其法律控制》，《北京科技大学学报（社会科学版）》2020 年第 3 期，第 69 页。

〔7〕 参见连玉明主编：《大数据蓝皮书：中国大数据发展报告 No. 4》，社会科学文献出版社 2020 年版，第 298 页以下。

〔8〕 参见朱力强、农青静：《广西：“大数据”助力监督提质增效》，《中国纪检监察》2018 年第 23 期，第 52 页。

〔9〕 林白芹、师长青、杨巨帅：《沈阳大数据监督实践探索与启示》，《中国纪检监察》2020 年第 17 期，第 23 页。

〔10〕 参见前引〔1〕，施奈尔书，第 50 页以下。

〔11〕 程雷：《大数据侦查的法律控制》，《中国社会科学》2018 年第 11 期，第 156 页。

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”，其主要运用于犯罪预防和公安侦查领域。〔12〕预测性警务指的是通过监控、收集、分析、整合大量数据，“为前瞻性的犯罪预防提供信息的警务策略”，〔13〕其目的是对犯罪作出预判，以“更高效地调动、部署、指挥警察力量以完成警务工作”。〔14〕纪检监察机关的大数据监督，与公安机关的大数据侦查、大数据监控、预测性警务的共性在于，都可能作出某种预测，也都可能进行个案查办。它们的差异主要在于，前者主要运用于对党员领导干部的权力监督，后三者主要针对普通公民的违法犯罪行为进行侦办或预防；前者的制度规范总体上还不明晰，后三者则有刑事诉讼法等系列法律法规作为基本依据。

目前，纪检监察机关大数据监督的实践做法主要包括：其一，汇聚数据并建立数据平台，为大数据监督提供数据资源。大数据监督的实践，离不开监督行为与大数据资源及数据平台的结合。为此，纪检监察机关将权力行使行为标准化、数据化，并将行权数据接入大数据监督系统，以便监督者及时比对相关数据。例如，沈阳市纪检监察机关曾经通过系统连接、数据库备份、数据采集直报等方式，将全市2346家财政预算单位的项目资金物资数据60.9亿条纳入系统。〔15〕数据的汇聚离不开大数据监督平台。“系统集成、数据交换及采集、数据加工、数据调度、运算识别及处理”等平台，〔16〕是比对和处理数据的核心连接点。其二，运用大数据发现、查证和查处公权力运行中存在的问题。监督者主要通过线上公开平台，对具备“业务流转、在线审批”特征的公权力运行流程是否规范进行监督。基层群众也可以通过网络公开平台，对公权力行使不规范、不正当、违法违规乃至犯罪等行为进行举报监督。〔17〕纪检监察机关通过“对系统数据进行加工、运算和比对”，查找和分析资金、项目、物资运行过程中存在的廉政风险点。〔18〕“大数据的一个关键贡献是能够在普通人类评估无法分析的数据集中找到有用的相关性。”〔19〕通过特定算法推动大数据“自动化”比对和碰撞（对两个或两个以上数据库资源进行智能比对），纪检监察机关可实现依靠人力所不易获得的权力运行监督效果，发现权力运行中的疑似违法违纪行为，获取违法违纪线索；合理的算法甚至可直接得出权力运行违法违纪的初步监督“结论”。若发现存在违法违纪线索或者违法违纪概率较大的公权力行使行为，纪检监察机关可以按照相关程序共享或者查询大数据系统，有针对性地进行个案调查、取证和事实核查，再结合其他证据、事实、党内法规和法律法规等，对违法违纪者给予纪律处分、政务处分等。

---

〔12〕 参见赵艳红：《大数据监控措施的法律规制研究——以隐私权为中心的探讨》，《交大法学》2020年第4期，第133页。

〔13〕 魏怡然：《预测性警务与欧盟数据保护法律框架：挑战、规制和局限》，《欧洲研究》2019年第5期，第87页。

〔14〕 李晶：《美国“预测性警务”的发展与困境（上）》，《现代世界警察》2021年第3期，第72页。

〔15〕 参见前引〔9〕，林白芹等文，第23页。

〔16〕 安徽省纪委监委：《安徽望江：打通资源壁垒，借力大数据提升监督实效》，https://www.ccdi.gov.cn/gzdt/jdjc/202108/t20210818_248511.html，2022年2月25日最后访问。

〔17〕 例如，广西壮族自治区通过微信平台公示民生项目、监督举报内容和方式，实现了自治区、市、县、乡镇、村、屯六级全覆盖。参见前引〔8〕，朱力强等文。

〔18〕 参见龙在宇、许然：《一张全国名片：沈阳大数据监督》，《廉政瞭望》2020年第18期，第33页；赵妍：《基于行政权力档案数据化的正风肃纪大数据监督平台建设》，《中国档案》2020年第11期，第60页以下；前引〔16〕，安徽省纪委监委文；浙江省纪委监委：《浙江江山：建设公权力公开运行和大数据监督平台》，https://www.ccdi.gov.cn/gzdt/jdjc/202107/t20210720_246447.html，2022年2月25日最后访问。

〔19〕 前引〔2〕，Joh文，第42页。

综合来看，各地纪检监察机关开展大数据监督的具体做法不完全相同，甚至存在非常大的差异。由于大数据技术发展水平不一，各地纪检监察机关调动大数据的资源和能力也不同。一些省级纪检监察机关能够通过数据汇聚尝试建立数据监督平台，而基层纪检监察机关能够使用的大数据监督手段、能够调动的大数据资源总体较为有限，往往只能提出“大数据监督”的构想，而难以建立高效的大数据监督平台。各地纪检监察机关在大数据监督的探索和实践中，既有运用大数据平台或者互联网平台对公权力进行日常化、一般性监督的做法，也有运用大数据开展案件初步核查进而对案件进行最终查处的做法；既有通过大数据信息系统跟踪权力运行的做法，也有利用大数据算法实现监督的“自动化决策”、精准发现权力运行问题的做法。

纪检监察机关青睐大数据监督的深层原因可能在于：其一，数据技术有助于推动权力监督方式的现代化。在条件具备的情况下，“互联网的发展能够在国家和社会之间相互进行赋权和改造”，国家和社会都能够从互联网的发展中受益，互联网还能够对国家权力进行约束。〔20〕进入 21 世纪，数据库成为“现代监控技术的心脏”。〔21〕数据技术的发展和大数据的不断汇聚，有助于推动纪检监察监督迈向信息化、现代化，告别单纯依靠人力的传统监督方式。其二，运用大数据技术能使监督更加高效。相比传统的监督模式，大数据监督的优势在于：（1）实时监督。大数据监督可以实现对权力的“全领域、全流程、全天候的制约”，〔22〕实时监测、记录和跟踪被监督者的行为。〔23〕（2）自动化挖掘信息。大数据监督可实现数据信息的自动化挖掘，“从杂乱无章的话单、账单、房产、车辆等海量数据中梳理出当事人的行踪轨迹、人际关系、通话规律、资金房产等信息，对犯罪嫌疑人进行立体式数据画像，并挖掘出其高频联系人、异常通话记录、大额转账等敏感信息”。〔24〕通过数据实时聚合和分析技术，“监控和大数据分析的自动化程度不断提高”。〔25〕（3）精准高效。大数据处理系统有助于聚合来自不同时段和空间的碎片化数据，其获取的被监督者的信息链条更加全面、完整、准确，更有助于建立“闭环式”的监督体系。借助强大的信息采集、分析和协同能力，纪检监察机关的大数据比对、大数据算法能更加精准地反映问题，快速筛查异常数据信息，提高监督的效率。〔26〕其三，大数据可通过回归分析、聚类分析等数据挖掘技术，发现特定行为之可能发展规律，〔27〕建立网络空间与现实空间的内在关联，并在此基础上作出一定预测。预测功能有助于推动传统的事后监督、惩戒方式变为事前事中的预测、警戒方式，使被动监督转为主动监督，使“不敢腐”“不想腐”“不能腐”的权力监督理想更易实现。大数据监督还有助于为具体的案件办理提供更多证据，有助于更加客观地呈现权力行使的流程和轨迹，同时还能运用数据证据弥补物理空间侦查取证的不足，降低纪检监察机关对于口供证据的依赖程度。

〔20〕 参见郑永年：《技术赋权——中国的互联网、国家与社会》，东方出版社 2014 年版，第 11 页以下。

〔21〕［英］约翰·帕克：《全民监控：大数据时代的安全与隐私困境》，关立深译，金城出版社 2015 年版，第 24 页。

〔22〕 黄其松、俞洋、李昂等：《在技术与制度之间：大数据时代的权力监督》，经济管理出版社 2020 年版，第 107 页。

〔23〕 See Gary D. Bass, *Big Data and Government Accountability: An Agenda for the Future*, 11 ISJLP 19 (2015).

〔24〕 王燃：《大数据时代侦查模式的变革及其法律问题研究》，《法制与社会发展》2018 年第 5 期，第 114 页。

〔25〕 John Taschner, *Era of Accelerating Digital Convergence: Security, Surveillance, Data, Privacy, Big Tech, and Politics*, 36 Am. U. Int'l L. Rev. 833 (2021).

〔26〕 参见梅宏主编：《数据治理之论》，中国人民大学出版社 2020 年版，第 31 页以下。

〔27〕 参见王燃：《大数据侦查》，清华大学出版社 2017 年版，第 32 页以下。

二、纪检监察机关大数据监督的现有制度依据

有关纪检监察机关开展大数据监督的法律法规和党内法规制度中，既有赋权制度，也有限权制度，且这二者很难完全分开。

（一）对大数据监督的赋权制度

依照现行体制，纪律检查委员会的执纪和监察委员会的执法是贯通的，纪检监察工作既执纪又执法，并应当实现纪法协同。纪检监察机关开展大数据监督的现行制度依据主要是监察法、《监察法实施条例》等法律法规和《中国共产党党内监督条例》（以下简称《党内监督条例》）、《中国共产党纪律检查机关监督执纪工作规则》（以下简称《监督执纪工作规则》）等党内法规。

《党内监督条例》和《监督执纪工作规则》是纪检监察机关探索大数据监督最基本的党内法规依据。《党内监督条例》第3条规定，“党内监督没有禁区、没有例外”。该条例明确了纪检监察机关监督的对象、范围、内容等，既注重预防也注重惩戒严重的违法违纪行为。《监督执纪工作规则》主要对监督执纪的领导体制、监督检查、线索处置、谈话函询、初步核实、审查调查、审理、监督管理等问题作了规定。

监察法和《监察法实施条例》赋予了监察机关依法查询、共享、调取数据信息的权力。监察法第23条第1款规定，“监察机关调查涉嫌贪污贿赂、失职渎职等严重职务违法或者职务犯罪，根据工作需要，可以依照规定查询……涉案单位和个人的存款、汇款、债券、股票、基金份额等财产。有关单位和个人应当配合”；第25条第1款规定，“监察机关在调查过程中，可以调取……用以证明被调查人涉嫌违法犯罪的财物、文件和电子数据等信息”。《监察法实施条例》第9条规定，“监察机关开展监察工作……有关部门、单位应当根据监察机关的要求，依法协助采取有关措施、共享相关信息、提供相关资料和专业技术支持，配合开展监察工作”；第21条规定，“监察机关开展监察监督，应当……健全信息、资源、成果共享等机制”。从文义解释的角度来看，上述法条中的“监察工作”既包括一般监督，也包括个案监督；其中规定的调取“电子数据”、健全“信息、资源、成果共享机制”、依法协助“共享相关信息”等内容，为监察机关通过数据共享开展大数据监督提供了初步的、基本的制度依据。

监察机关办理案件时，可以将电子数据作为证据。可以作为监察机关办案证据的电子数据主要包括三类：一是行政机关执法或者查办案件中收集的电子数据。根据《监察法实施条例》第68条，行政机关或者根据法律、行政法规规定行使国家行政管理职权的组织，在行政执法和查办案件中收集的电子数据，经审查符合法定要求的，可以作为监察机关办理案件中的证据使用；二是人民法院、人民检察院、公安机关、国家安全机关等在刑事诉讼中收集的电子数据。根据《监察法实施条例》第69条，监察机关对人民法院、人民检察院、公安机关、国家安全机关等在刑事诉讼中收集的电子数据，经审查符合法定要求的，可以作为证据使用；三是监察机关自身依法收集、提取的电子证据。《监察法实施条例》第123条对监察机关收集、提取电子数据的程序作了明确规定。

（二）对大数据监督的限权路径

对纪检监察机关大数据监督的限权路径，主要包括五个方面。其一，纪检监察机关通过主动自我约束和加强内部控制限制大数据监督权力的行使。党中央高度重视纪检监察队伍建设，

要求“解决‘谁来监督纪委’问题，防止‘灯下黑’”，“把纪委的权力关进制度笼子”。〔28〕习近平总书记明确提出：“纪检监察机关要在强化自我监督、自我约束上作表率，牢固树立法治意识、程序意识、证据意识，严格按照权限、规则、程序开展工作，下更大气力把队伍建强、让干部过硬。”〔29〕纪检机关注重“强化自我约束，把监督执纪权力关进制度笼子”。〔30〕早在 2017 年，中央纪委就发布了《监督执纪工作规则（试行）》。自 2019 年 1 月 1 日起施行的《监督执纪工作规则》第 60 条规定，“纪检监察机关应当严格依照党内法规和国家法律，在行使权力上慎之又慎，在自我约束上严之又严，强化自我监督，健全内控机制，自觉接受党内监督、社会监督、群众监督，确保权力受到严格约束，坚决防止‘灯下黑’”。中国共产党第十九届中央纪律检查委员会第六次全体会议公报也提出，“完善监督执纪执法权力运行内控机制，坚决查处执纪违纪、执法违法、失职失责行为，切实解决‘灯下黑’问题，自觉做遵纪守法的标杆”。〔31〕

其二，通过外在监督限制大数据监督权力的行使。《党内监督条例》对纪检监察机关运用大数据监督权力的行为作了原则性限制，其第 34 条明确规定要“加强对纪律检查机关的监督”，“确保权力受到严格约束”。《党内监督条例》是依据《中国共产党章程》制定的。《中国共产党章程》在总纲部分指出，“党必须在宪法和法律的范围内活动”，其第 40 条第 3 款规定，“党内严格禁止用违反党章和国家法律的手段对待党员，严格禁止打击报复和诬告陷害”。这些规定实际上也构成了对监督手段的限制，即要求党内监督采取的“手段”必须符合党章和国家法律的各项规定。

其三，通过内部制度规范“调查措施权”的行使，通过“监督执法程序”限制纪检监察机关的权力。例如，2019 年 7 月中共中央纪律检查委员会、国家监察委员会印发《监察机关监督执法工作规定》，进一步提出纪检监察机关要自觉守法、规范和正确行使监察权、防止滥用权力。该规定对监察机关开展日常监督、谈话函询、初步核实、立案调查的审批程序作出具体规定，明确了各项调查措施的使用条件、报批程序和文书手续，明确了与司法机关、执法部门互涉案件的管辖原则，以及与检察机关在案件移送衔接、提前介入、退回补充调查等方面的协作机制。〔32〕

其四，以刑事诉讼审判制度、证据制度限制纪检监察机关的权力。党中央高度重视深化国家监察体制改革，明确提出要“强化法治思维，在措施使用、证据标准上主动对接以审判为中心的刑事诉讼制度改革”。〔33〕由于监察证据在进入刑事诉讼程序后转为刑事证据，故“监察证据的刑事司法审查判断应当遵循刑事证据审查程序，以刑事诉讼规则为司法依据”。〔34〕监察机关的调查取证，需满足刑事司法证据的关联性、合法性、真实性等要求，〔35〕尤其要确

〔28〕《十八届中央纪律检查委员会向中国共产党第十九次全国代表大会的工作报告》，载中共中央党史和文献研究院编：《十九大以来重要文献选编》上册，中央文献出版社 2019 年版，第 71 页以下。

〔29〕《一以贯之全面从严治党，强化对权力运行的制约和监督》，载《习近平谈治国理政》第 3 卷，外文出版社 2020 年版，第 550 页。

〔30〕《中国共产党第十八届中央纪律检查委员会第七次全体会议公报》，《中国纪检监察》2017 年第 2 期，第 16 页。

〔31〕《中国共产党第十九届中央纪律检查委员会第六次全体会议公报》，《人民日报》2022 年 1 月 21 日第 1 版。

〔32〕参见《中共中央纪委国家监察委员会印发〈监察机关监督执法工作规定〉》，https://www.ccdi.gov.cn/toutiao/201907/t20190715_197112.html，2022 年 3 月 10 日最后访问。

〔33〕刘一霖：《贯通规纪法，衔接纪法罪》，《中国纪检监察报》2022 年 2 月 23 日第 5 版。

〔34〕朱德宏：《监察证据的属性及其刑事司法判断》，《重庆大学学报（社会科学版）》2021 年第 6 期，第 1 页。

〔35〕参见纵博：《监察体制改革中的证据制度问题探讨》，《法学》2018 年第 2 期，第 123 页。

保取证程序合法，防止因程序不当致使证据资格受到损害。

其五，通过个人信息保护法等法律法规约束大数据监督权力的行使。个人信息保护法明确提出，其立法目的在于“保护个人信息权益，规范个人信息处理活动”，该法对国家机关处理个人信息作了特别规定，明确要求国家机关为履行法定职责处理个人信息“不得超出履行法定职责所必需的范围和限度”。此外，数据安全法、网络安全法等也对国家机关的数据共享、数据处理作了限制性规定。

三、完善纪检监察机关大数据监督制度的必要性

多地运用大数据技术开展的纪检监察监督，虽然取得了一些成效，但由于实践先于制度建构，当前的大数据监督既缺乏系统、统一、规范化的纪检监察数据来源，也缺乏统一的大数据监督规范、标准和操作程序，导致有限的数据、制度规范与不断增长的监督需求不相匹配，监督权力的行使也亟需更加完善的制度制约。

其一，在大数据共享方面，纪检监察机关需要获得更加具体明确的制度赋权，以化解监督数据来源的合法性难题。目前，大数据监督既缺乏统一的数据汇聚标准和高效的大数据平台支撑，也缺乏有关纪检监察机关共享、处理大数据的明确的制度赋权，纪检监察机关开展大数据监督的关联法律法规规定模糊、法律法规授权不充分。例如，依据《监察法实施条例》第 9 条，有关部门、单位应当根据监察机关的要求与其共享相关信息，但该条例并未明确规定纪检监察机关可以共享的信息的具体范围，也未明确信息共享的方式和程序等。再如，纪检监察机关可以将行政机关执法、查办案件中收集的电子数据或者人民法院等机关在刑事诉讼中收集的电子数据作为证据使用，也可以自己依法收集、提取电子证据。但是，《监察法实施条例》第 123 条仅规定监察机关可以收集、提取电子数据，对于其可以收集、提取哪些证据，并未作出明确规定或者限定。监督机关监督能力的大小，与其获取数据、信息的能力紧密相关。实践中，各地纪检监察机关的大数据监督，总体上是在数据碎片化的背景下推动的。纪检监察机关虽然能够获得一些数据，但所获数据的量与质、数据的类型以及获取数据的便捷程度等，尚无法满足大数据监督的实践需求。并且，大多纪检监察机关并未真正建立定向服务于大数据监督目标的、可以便捷使用的大数据监督平台。由于数据孤岛大量存在，大数据监督中数据不充分的情形十分普遍，监督者时常面临“信息不全、二手信息、信息滞后”的信息困境。〔36〕目前，不少省市的纪检监察机关正在尝试汇聚数据、建立高效的大数据监督平台，但其可以汇聚哪些数据，如何汇聚数据，按照何种规范标准汇聚数据，以及数据共享和数据处理应遵守什么准则，在总体上仍不清晰，缺乏制度规范的指引。当然，这一现状与大数据行业正处于快速发展期且在一定程度上呈“野蛮生长状态”有关，也与规范数据采集、流通、交易、应用等环节的法律法规尚不健全的现状密不可分。〔37〕

其二，需要进一步强化对纪检监察机关大数据监督权力的制约。纪检监察机关如何共享政务数据、政法平台数据，如何规范地处理互联网平台企业数据和公民个人信息，目前尚缺乏直接明确的法律法规或党内法规的指引。由于缺乏明确的制度制约，纪检监察机关容易借大数据监督之名行调查特定个人信息之实，模糊日常监督与案件调查的权力边界。按照规定，纪检监

〔36〕 白建军：《大数据助力法律监督》，《探索与争鸣》2015 年第 2 期，第 30 页。

〔37〕 参见何渊等：《大数据战争》，北京大学出版社 2019 年版，第 10 页。

察机关在案件调查中可以根据法律和党纪法规调取相关案件和当事人的数据，但其在日常监督中并不享有这一权力；即使是针对领导干部的日常大数据监督，也不能随意调取领导干部的个人信息数据。尽管从概括意义上讲，纪检监察机关的大数据监督行为具有正当性和法律依据，但在具体的操作环节中，大数据监督行为仍需更加具体、明确、合理的法律法规加以引导，以规范千差万别的数据汇聚行为，防止监督权力侵犯个体权利。

其三，数据共享和数据处理活动中的矛盾冲突，有待出台相应制度予以消解。使用大数据可能会提高监督效率，但也可能出现“结论不准确、侵犯隐私、非故意歧视”，以及大数据监督者权力的不当增加等消极后果。〔38〕如果缺乏必要的、合理的制度制约，监督数据共享和数据处理中的矛盾冲突就有可能加剧，进而引发数据滥用，强化社会偏见，形成算法歧视，导致个人信息泄露，加大社会伦理风险，乃至激化国家安全、个人信息保护、经济发展和技术创新之间的矛盾。总体来看，数据共享和数据处理活动中的矛盾冲突，主要包括两方面：（1）数据处理规则与监督规则的内在冲突。纪检监察机关推行的大数据监督，客观上需要打破数据孤岛的限制，以获取更多的数据，纪检监察规定及大数据监督实践更加倚重数据的开放、共享、获取、利用与处理。但是，数据安全法、网络安全法、个人信息保护法等法律法规，强调对国家安全、公共利益和个人信息的保护。（2）数据逻辑与法律逻辑的冲突。在将大数据技术运用于纪检监察案件监督时，容易产生一种简单的认知：数据就是客观准确的法律证据，大数据判断结论就是法律判断结论。但是，实际上，人们难以确保大数据是绝对真实和完整的。虽然大数据技术强调数据获取的“全数据”特性，但任何意义上的全数据，都只是在特定时空下和数据有限时的“全数据”。任何数据的公开、共享，本身也只具有相对性。由于数据孤岛、数据壁垒现象长期存在，许多数据无法被真正获取。数据被伪造和篡改、数据来源或者基础信息存在缺失或偏差、算法决策过程不透明、算法逻辑设计不合理等情形也时有发生。〔39〕因而，大数据算法的应用实践中，难免存在“偏见进，偏见出”的情形，“数据不准确、分析不准确或过度依赖分析结果”都极有可能导致结论错误。〔40〕即便是真实、及时、有效的数据，其本身也难以直接成为法律上的证据。证据不仅仅是一组数据、一条信息。数据、信息要成为法律上的证据，必须经受“真实性、合法性、关联性”方面的法律审查。大数据本身并不是法定的“证据类型”，大数据转化为证据通常要经过三个环节：汇总数据并进行数据清洗、建构分析模型或机器算法、进行运算并形成分析结论。〔41〕此外，大数据的获取、固定等，还必须符合刑事诉讼法的相关规定。

其四，大数据监督的理念有待更新。首先，大数据监督者在构想制度模式时，容易忽视算法偏见的存在。大数据的运用有先天的技术门槛，既需要有一套科学的数据分析软件，并辅之以自动化决策的科学算法，还需要通过大量的机器学习、模拟训练以改进算法。受制于认知局限、法律专业知识匮乏等因素，大数据算法模型的设计人员有可能将一些不合理的政策、价值需求编入数据算法中，形成潜在的算法价值偏见。〔42〕无论数据采集偏差还是数据分析偏差，

〔38〕 参见前引〔3〕，Mayer 文，第 1281 页。

〔39〕 参见苏宇：《算法规制的谱系》，《中国法学》2020 年第 3 期，第 165 页以下。

〔40〕 参见前引〔3〕，Mayer 文，第 1335 页；前引〔23〕，Bass 文，第 31 页以下。

〔41〕 参见刘品新：《论大数据证据》，《环球法律评论》2019 年第 1 期，第 25 页。

〔42〕 See Miller Kevin, *Total Surveillance, Big Data, and Predictive Crime Technology: Privacy's Perfect Storm*, 19 J. Tech. L. & Pol'y 119 (2014).

都可能导致数据分析结果错误。其次，大数据监督容易被误解为法律监督的“自动售货机”。“人类从依靠自身判断做决定到依靠数据做决定的转变，也是大数据作出的最大贡献之一。”〔43〕大数据推动了自动化执法和自动化行政。例如，监控器通过自动抓拍与数据比较，可以及时对机动车违章作出行政处罚决定；个人所得税 APP，可以自动且精确地计算出一个自然人在某一年度内应税所得和应税税额。不过，目前的大数据监督，更多只是运用数据检索工具在海量数据库中进行检索、比对，还远远谈不上依靠高效的算法进行“自动化决策”。法律裁断性工作需要通过人脑的复杂考量和法律价值衡量才能得出大致合理的结论，当前尚无证据表明算法能够做到这一点。大数据监督平台无法成为“自动售货机”，做不到一边输入数据、一边输出监督结果，其深层原因还在于，数据无法对法律逻辑、纪检监察机关的权力运行逻辑作出有效阐释。“大数据是一种资源，也是一种工具。它告知信息但不解释信息。”〔44〕权力监督行为本身是否合法、合规，需要结合事实、证据、规范及法律因果关系等进行复杂的综合判断，也常常涉及自由裁量、例外情形、情形变更、比例原则、对特定弱势群体的关照、国家政策的调整、执法者的价值判断等多重因素。对这些复杂情形的合理判断，需要更加科学合理的法律制度来引导。此外，中国正处于大规模的改革和制度变迁的通道中，需要在很多领域允许改革行为的试错，大数据监督也应把“纠错容错”的改革政策理念融入其中。最后，大数据监督的推进需要防止“泛在监控”理念的扩张。大数据监督有助于建立更加廉洁的权力运行机制，但这一美好的政治追求不应当以大幅度牺牲个人信息权利为代价。大数据监督的成本远低于物理监督的成本，如果有关机关不断加强对个人的密集监控，整个社会就有滑向“泛在监控”的可能。泛在监控相当于使监督者获得了“空白搜查令”，可以不受约束地在互联网上任意搜集数据或信息，其可能导致“违法圈”“违纪圈”不断扩大，只要监督者“决心去搜寻证据，任何人都可能被判违法”。〔45〕

其五，纪检监察机关大数据监督的程序正当性有待提升。从事大数据监督工作的人员是否需要经过专业的执纪、执法资格培训，当前的大数据监督是否存在将案件调查的启动时点不当前移的问题，大数据监督中的数据和结论如何转换为纪检监察机关使用的证据等，都是既有制度没有给出明确指引但现实中亟待破解的难题。一些模糊性规定也引发了关于程序正当性的疑问，如纪检监察机关可以共享“有关单位、有关部门”的数据信息，但相关制度尚未明确可以共享的数据信息的具体范围与方式；纪检监察机关可以自行收集和提取电子数据，但具体的收集范围和相关程序还未得到明确限定。国家法律和党内法规中的此类“开放结构”，为监督执纪者留下了“自我赋权”的空间，也为限制纪检监察机关的大数据监督权力、提升监督执纪的正当性提出了新课题。

四、纪检监察机关大数据监督的制度构建

当前，关于纪检监察机关大数据监督的规范化开展，最大的制度难题在于，如何对政务数据、网络信息企业数据、个人信息、政法机关和纪检监察机关的办案数据或管理数据等进行规

〔43〕［英］维克托·迈尔—舍恩伯格、肯尼思·库克耶：《大数据时代——生活、工作与思维的大变革》，盛杨燕、周涛译，浙江人民出版社 2013 年版，第 180 页。

〔44〕同上书，第 247 页。

〔45〕前引〔1〕，施奈尔书，第 139 页。

范化地共享、处理与使用。因此，本文对于纪检监察机关大数据监督制度构建的讨论，主要聚焦数据的共享、处理与使用等方面的问题。

（一）赋予纪检监察机关对政务数据的共享权力

数据和信息是存在区别但又相互关联的两个概念，“信息是数据的内容，数据是信息的形式”。〔46〕在此意义上，大致可以说，所谓政务数据，就是政府部门及法律法规授权具有行政职能的事业单位或社会组织，“在履行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表和数据等各类信息资源，包括政务部门直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的信息资源等”。〔47〕

由于数据来源广泛、汇聚主体多元、数据类型多样，不同领域、层面的政务大数据实际上掌握在不同政务主体的手中。对于大数据监督者来说，打破数据壁垒、实现监督数据的“全联通”，是最为理想的状态。然而，现实中数据孤岛化的情形严重，大量数据未被充分共享、难以有效集成、有待深度融合。〔48〕打破“数据孤岛”、促进数据共享，是政务数据管理的必然要求。参照国务院 2016 年印发的《政务信息资源共享管理暂行办法》第 9 条，政务数据按共享类型可以分为无条件共享的政务数据、有条件共享的政务数据、不予共享的政务数据三种类型。不同类型的政务数据，共享的自由度不同。具体来说：（1）无条件共享的政务数据，是可以提供给所有政务部门共享使用的政务数据，典型的如人口信息、法人单位信息、自然资源和空间地理信息、电子证照信息等基础信息。（2）有条件共享的政务数据，是可以提供给相关政务部门共享使用，或者仅能部分提供给所有政务部门共享使用的政务数据。至于共享条件，目前的法律法规中还找不到明确的规定。从法理上讲，针对政务数据的共享，可以设定的共享条件大致包括：主体条件，即限于部分政务部门共享；时间条件，即限于特定时间内共享；目的条件，即限于为特定目的而共享；保密条件，即只有签订了保密协议并能够履行保密义务者才可共享；管理条件，即需要采取特别管理措施才能够共享。当然，具体设定的共享条件可以是上述条件中的一个或多个。基于国家安全或者维护社会公共利益的目的，还可以设定其他的共享条件，并附加更多的管理义务和法律责任。（3）不予共享的政务数据，即不宜提供给其他政务部门共享使用的政务数据。2018 年国务院办公厅印发实施的《科学数据管理办法》第 25 条规定，“涉及国家秘密、国家安全、社会公共利益、商业秘密和个人隐私的科学数据，不得对外开放共享；确需对外开放的，要对利用目的、用户资质、保密条件等进行审查，并严格控制知悉范围”。除上述分类外，还可以将政务数据分为基础数据、主题数据、业务数据，并进行分类管理。不论什么类型的政务数据，其开放和共享都应当遵守一些共通性、前提性原则，如数据应当是及时的、可读取的、机器可处理的，数据的获取应是无歧视的，数据的格式必须是通用的而非专有的。〔49〕当然，确保数据的真实性和准确性，应是一条最基本的要求。

〔46〕 程啸：《论大数据时代的个人数据权利》，《中国社会科学》2018 年第 3 期，第 58 页。

〔47〕 参见《政务信息资源共享管理暂行办法》（国发〔2016〕51 号）第 2 条。《广东省公共数据管理办法》《浙江省公共数据条例》等法规中使用了“公共数据”的概念，其内涵与“政务数据”的内涵相同（参见《广东省公共数据管理办法》第 3 条、《浙江省公共数据条例》第 3 条）。本文所称“政务数据”，涵盖了“公共数据”。

〔48〕 数据融合是指，“将来自政府治理中不同数据源的同一实体（如企业、个人）的不同表象融合成单一表象，消除潜在的数据冲突”。参见金澈清、陈晋川、刘威、张召：《政府治理大数据的共享、集成与融合》，《大数据》2020 年第 6 期，第 33 页。

〔49〕 参见张海波：《大数据驱动社会治理》，《经济社会体制比较》2017 年第 3 期，第 65 页。

理论上，如果仅仅依据《政务信息资源共享管理暂行办法》等规定，即便是可以共享的政务数据，其共享主体也仅限于政务部门。纪律检查机关不属于政务机关，监察机关显然也不属于狭义的政务部门，而是“行使国家监察职能的专责机关”。纪检监察机关如欲获得明确的政务数据共享资格或权限，需通过修改相关党内法规或监察法来完成。较为合理的制度设计思路可以有两种：一是允许纪检监察机关准用相应的政务数据共享规则。按此思路，在政务数据的共享方面，纪检监察机关并不享有任何优于其他政务机关的数据共享权力。二是基于纪检监察工作的性质，以及纪检监察机关在国家监督体制中的独特作用，为纪检监察机关设置特定的数据共享前提和标准，赋予其比一般政务机关更大的政务数据共享权力。鉴于大数据监督尚处初步探索阶段，且有条件共享的政务数据和不予共享的政务数据本身都具有特殊性，如果要赋予纪检监察机关比一般政务机关更大的政务数据共享权力，则必须为其设定非常严格的共享条件和程序，如对其利用政务数据的目的、保密条件等进行严格审查，对其获取的政务数据的使用范围作出严格限制，并且“严格控制知悉范围”。

大数据的依法共享，有助于纪检监察机关构筑大数据监督数据网络，及时研判权力运行中存在的制度漏洞或短板、发现廉政风险点，进而通过监察建议等方式促进法律实施和党风廉政建设。〔50〕同时，大数据的便捷共享也能为违法违纪个案的查办提供有力保障，有助于形成“不敢腐”的制度环境和权力监督制约氛围。

（二）规范对政法类数据与法律监督类数据的调取和使用

目前，全国多地建有政法数据中心。据了解，纪检监察机关可以运用政法数据中心的数据初查或者核查案件。政法类数据包括政法管理类数据和办案机关办理具体案件的数据。〔51〕政法类数据的查询或调取，对纪检监察机关开展权力监督具有两大重要作用。一是有助于发现权力运行中的具体问题线索，洞察权力运行的宏观状况，总结权力行使的某些共性特征和突出问题，为纪检监察监督提供数据预测，以便于纪检监察机关随时调整监督工作重点。二是有助于促进纪法衔接。纪检监察机关从公安机关、人民检察院、人民法院调取职务犯罪类数据，以及党员领导干部的一般违法犯罪数据，有助于纪检监察机关准确掌握党员领导干部的违法犯罪事实，并在此基础上依据党规党纪及时作出纪律处分决定。由于纪检监察机关和公安机关、人民检察院、人民法院、司法行政机关、政法委等不同机关各有其法律职责、权限和分工，且不同机关办理案件的法律要求不完全相同，不宜采用数据接口等方式让纪检监察机关直接共享上述政法机关正在办理的案件数据，否则可能引发职责及责任体系的紊乱。例如，允许纪检监察机关直接共享公安机关或者人民检察院正在办理的案件数据，有可能加大数据信息泄露后的责任追究难度。考虑到不同机关的法律职责分工不同、相关数据规模庞大且内容敏感等因素，可采取纪检监察机关对政法机关统计数据共享，司法机关在办理刑事、民事、行政、执行案件中发现党员领导干部违法违纪问题时主动通报线索或移送，〔52〕纪检监察机关主动查询政法类数据三种方式，保障纪检监察机关在办案中对大数据的共享需要。纪检监察机关如果主动查询或者调取案件数据，原则上应针对公安机关、人民检察院、人民法院已经调查终结、审结的案件数

〔50〕 参见中国纪检监察报社评论部编：《党的十九大以来全面从严治党新观察》，人民出版社 2019 年版，第 83 页。

〔51〕 政法委员会是党委领导和管理政法工作的职能部门，其在管理政法工作时，会在推进政法改革、平安建设和社会综合治理等工作的过程中形成自有的管理数据，也会汇聚审判机关、检察机关、公安机关、国家安全机关、司法行政机关等政法单位定期分类报送的各类统计数据。本文所说的政法管理类数据，主要是指这些数据。

〔52〕 参见《监察与司法有效衔接工作指引》，中国方正出版社 2019 年版，第 15 页。

据，而不宜直接调取正在侦办中、没有侦办结论或尚未审结的案件数据，否则就可能构成对办案机关的不当干预。政法类数据的“敏感性、保密性和隐私性更强”，很多数据直接涉及当事人乃至案外第三人的个人身份信息、敏感个人信息乃至隐私等，未来可针对政法类数据查询的“主体条件、申请程序、申请理由、数据查询范围、数据使用范围、违法的法律责任等”设定更加严格的规则。〔53〕

纪检监察机关开展大数据监督的目标，主要是对公权力行使行为进行监督。纪检监察机关对法律监督类大数据的使用，应当主要围绕权力行使、权力监督环节汇聚数据。党的十九大报告提出，“构建党统一指挥、全面覆盖、权威高效的监督体系，把党内监督同国家机关监督、民主监督、司法监督、群众监督、舆论监督贯通起来，增强监督合力”。〔54〕法律监督中会涌现很多针对权力行使违规违法行为的投诉和举报，进而形成大量的法律监督类数据。信访举报是发现权力运行问题的主渠道，也是推进党内监督和群众监督相结合的重要方式。纪检监察机关大数据监督举报平台的建立，有助于“精准发现真信息、真线索、真问题”。〔55〕在自媒体高度发达的时代，舆论监督、群众监督有助于高效地反映违法违纪问题。村务监督委员会在民主监督中发现涉嫌贪腐谋私、侵害群众利益等违法违纪问题，并向纪检监察机关报告相关数据和信息，也有助于纪检监察机关对乡村基层予以精准监督。审计、巡视等专项法律监督工作，更是高效发现违法违纪问题的重要途径。纪检监察机关通过上述权力监督渠道汇聚数据，能够更具针对性地发现问题、开展监督。在此过程中，应注意做好两方面工作：一是依靠各类监督渠道汇聚的投诉、举报、信访等数据，不仅真假并存，且多涉及法律中的疑难问题。纪检监察机关在推进法律监督时，需要对数据和问题线索进行甄别、核实，甚至进一步调查。二是尊重宪法法律上的权力分工，尊重其他国家机关的法律监督权力或问题处理权力。例如，《信访条例》第 4 条规定，信访工作“坚持属地管理、分级负责，谁主管、谁负责，依法、及时、就地解决问题与疏导教育相结合的原则”。纪检监察机关如果过于主动、快速地将信访过程中反映的问题纳入纪检监察范围，有可能损及信访制度的功能。考虑到信访问题的复杂性及其独特的法律监督作用，监察机关可以将涉嫌职务违法和职务犯罪的问题纳入自己的特别监督范围，将问题线索分类处理。

（三）规范纪检监察机关对个人信息的处理权力

党员领导干部的个人信息是大数据监督的重要数据来源。纪检监察机关收集、存储、使用、加工、传输、提供、公开上述数据，必须严格按照法律法规和党内法规设定的职责、权限和程序，不能超越权限查询、使用数据；对在履职过程中知悉的个人隐私、个人信息、商业秘密等数据应当依法予以保密，不得泄露或者向他人非法提供；在大数据的采集、传输、存储、处理、交换、销毁、数据分级、去标识化、脱敏，以及数据运用过程中的安全运营和风险管理中，〔56〕必须保障公共安全和公共利益。案件调查结束时，包括查办案件过程中获取的个人信息在内的审查调查材料，应当“案结卷成、事毕归档”，以方便查找利用，并作为重要的历史

〔53〕 参见杨建军：《司法数据公开及其程序规制》，《广东社会科学》2019 年第 6 期，第 216 页以下。

〔54〕 习近平：《决胜全面建成小康社会，夺取新时代中国特色社会主义伟大胜利》，载前引〔28〕，中共中央党史和文献研究院编书，第 48 页。

〔55〕 中共中央纪律检查委员会、中华人民共和国国家监察委员会法规室编：《〈中国共产党纪律检查机关监督执纪工作规则〉释义》，中国方正出版社 2019 年版，第 83 页。

〔56〕 参见前引〔7〕，连玉明主编书，第 157 页以下。

凭证。〔57〕

我国个人信息保护法中既有针对个人信息保护的一般规定，也有针对国家机关处理个人信息的特别规定。该法第33条规定，“国家机关处理个人信息的活动，适用本法”；第34条规定，“为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度”。因此，纪检监察机关在大数据监督中负有遵守个人信息保护法相关规定的基本义务。为了加强对公民个人信息的保护，我国刑法第253条之一规定了侵犯公民个人信息罪，其第1款规定，“违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金”；第2款规定，违反国家有关规定，将在履行职责过程中获得的公民个人信息，出售或者提供给他人的，依照第1款的规定从重处罚。2017年发布的《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第4条，还明确将违反国家有关规定，在履行职责中收集公民个人信息的行为，认定为“以其他方法非法获取公民个人信息”。

手机、电脑和各种智能设备，源源不断地收集着使用者的各种信息。数据处理者在处理个人信息时，一般需要征得当事人的同意和授权。但是，基于法定义务的承担或法定职责的履行等原因而有必要对个人信息进行处理，就属于“同意和授权”原则的例外情形。因而，纪检监察机关在大数据监督过程中的数据处理，并不需要事先征得权利主体的同意，但必须遵守相关规定。纪检监察机关将国家法律允许的历史文件资料、公安交通管理部门的内部数据、互联网产生的官民互动信息，以及物联网产生的行政执法信息等作为数据予以采集和汇聚，应无太大疑问。但是，如果使用“数据铁笼”手机App等工具接入技术监督平台后自动生成数据信息，〔58〕则必须特别注意遵守数据调取规则。通信监控必须基于合法目的，其只在追求实现最重要的国家目标时才应被允许，且这种监控必须是为了实现合法目标而不得不采取的行动。由于通信监控被视为一种具有高度侵入性的行为，会对隐私权和言论自由权构成干预，监督者必须事先获得特别授权。〔59〕监察法第28条规定：“监察机关调查涉嫌重大贪污贿赂等职务犯罪，根据需要，经过严格的批准手续，可以采取技术调查措施，按照规定交有关机关执行。”按照该条及相关规定，采取电话监听、电子监控等“技术调查措施”的前提是，存在“涉嫌重大贪污贿赂等职务犯罪”，且相关技术调查应当以监察委员会的名义进行。〔60〕在此前提下，还应确保技术调查措施运用的对象特定、措施特定、实施主体特定。对象特定，即技术调查措施只能针对特定对象采取，不能够扩大到批准程序之外的其他任何第三人；措施特定是指，采取的技术调查措施仅限于经批准的特定措施，不能采取未经批准的技术调查措施；实施主体特定，即技术调查措施只能交由公安机关等有关机关执行，监察机关不能够自己执行，也不能够交由法律规定之外的主体执行。此外，技术调查措施的采取还必须严格依照规定的权限和程序报经批准。

针对领导干部个人事项数据的查询也必须遵守特定规则。依据2017年2月中共中央办公厅、国务院办公厅印发的《领导干部报告个人有关事项规定》第3条和第4条，领导干部应

〔57〕 参见《〈中国共产党纪律检查机关监督执纪工作规则〉学习问答》，中国方正出版社2019年版，第119页以下。
〔58〕 参见前引〔22〕，黄其松等书，第105页。
〔59〕 参见前引〔1〕，施奈尔书，第251页以下。
〔60〕 参见前引〔57〕，《〈中国共产党纪律检查机关监督执纪工作规则〉学习问答》，第96页以下。

报告的事项主要包括本人婚姻和配偶、子女移居国（境）外、从业以及收入、房产、投资等事项，由此形成了领导干部的个人信息。该规定第 10 条第 2 款规定，“纪检监察机关（机构）在履行职责时，按照干部管理权限，经本机关主要负责人批准，可以查阅有关领导干部报告个人有关事项的材料”；第 16 条对信息查询中的纪律作了具体规定，包括“严格遵守工作纪律和保密纪律，设专人妥善保管领导干部的个人有关事项报告和汇总综合、查核等材料”。为了更加严谨、规范地开展对领导干部个人事项的数据查询，应当对领导干部的个人事项数据作进一步的细化分类管理，如可区分为一般事项数据、敏感事项数据等类型，并针对不同类型的数据设计不同的数据查询、调取、使用和管理规则。

（四）严格纪检监察机关向网络信息企业调取个人信息的权力边界

大多数情形下，网络信息企业基于用户加入 APP 时勾选的知情同意协议，搜集和掌握着海量的个人信息，其基于推送商业广告等需要，还会持续搜集个人信息。网络信息企业对于个人的监控非常便利，容易发生基于特定目的对特定用户信息进行持续、定向、长期追踪的情形，如“四大互联网企业 GAFA——谷歌、苹果、脸书和亚马逊，通过十几年时间成功攫取了整个数据世界市场”，控制了海量的个人信息。〔61〕从理论上讲，运营商还可以“从信道上监听到各网站和 APP 的用户访问信息”。〔62〕

在数据开放、共享的背景下，企业的数据与政府的数据常常来回流动。〔63〕因而，网络信息企业的数据，构成了政府数据监控的网络通道。由于办案机关常常可以非接触性地获取数据，且“在秘密调查的方式中，执法人员不需要提醒搜索目标，因此政府调查人员可能更愿意从在线网站或云计算公司获得信息，而不是从个人获得信息”。〔64〕在“国家管平台、平台管用户”的数据治理模式下，〔65〕公权力机关对特定主体的监控，常常与企业数据紧密相连。根据网络安全法第 69 条的规定，网络运营者应受处罚的行为包括“拒不向公安机关、国家安全机关提供技术支持和协助”。这意味着，网络运营者对于自己掌握的数据，负有向纪检监察等有关机关依法提供的义务。实践中，由于技术和规则的便宜性，“刑事执法机关向网络信息业者调取数据”呈现出“扩张趋势”，对其规制极为必要。〔66〕传统的隐私保护主要由个人自主决定，是否处理、如何处理以及经由谁来处理他们的信息，相应的决定权掌控在个人手中。大数据时代的个人隐私保护，则需要实现“从个人许可到数据使用者承担责任”的规制模式转变。〔67〕考虑到纪检监察机关大数据监督权力不断扩张的内在特性，未来进行制度设计时，还需要强化对纪检监察机关通过网络信息企业调取个人信息的行为的规范和监督。这方面的核心问题在于，纪检监察机关可以向网络信息企业调取什么样的数据，其有权向网络信息企业提出什么样的数据调取指令，网络信息企业对包括纪检监察机关在内的有关机关的数据查询请求

〔61〕 参见［法］马尔克·杜甘、克里斯托夫·拉贝：《赤裸裸的人——大数据，隐私与窥视》，杜燕译，上海科学技术出版社 2017 年版，第 8 页。

〔62〕 陈本皓：《大数据与监视型资本主义》，《开放时代》2020 年第 1 期，第 180 页。

〔63〕 参见前引〔1〕，施奈尔书，第 121 页。

〔64〕 Daniel Rudofsky, *Modern State Action Doctrine in the Age of Big Data*, 71 N. Y. U. Ann. Surv. Am. L. 746 (2016).

〔65〕 参见单勇：《数字看门人与超大平台的犯罪治理》，《法律科学》2022 年第 2 期，第 74 页。

〔66〕 所谓技术便宜性，即“相较于侦查机关而言，网络信息业者在数据控制和处理能力方面有显著优势”。所谓规则便宜性，即“通过向网络信息业者调取证据可以规避其他取证方式中可能面临的法律障碍”。参见裴炜：《论个人信息的刑事调取——以网络信息业者协助刑事侦查为视角》，《法律科学》2021 年第 3 期，第 82 页以下。

〔67〕 参见前引〔43〕，舍恩伯格等书，第 220 页。

具体应当承担什么样的数据提供责任，以及提供数据的范围有多大。截至目前，上述问题尚未通过党内法规或者法律法规予以明确规定，为纪检监察机关自由调取数据留下了较大的制度空间。

依据网络安全法、个人信息保护法等相关规定，网络运营者、互联网企业，尤其是网络信息企业，在收集、使用个人信息时必须承担特定义务和责任，承担对个人信息全链条、全生命周期合规管理的法律责任，不得“超范围收集个人信息”或“以监听监视等非法方式获取个人信息”。〔68〕在美国也同样如此，微软2014年的透明度报告显示，“它拒绝了超过16%的美国政府的信息请求，并且在另外15%的请求中找不到数据。所以，它只在69%的请求中提供信息”；脸书（Facebook）也在2014年的报告中称，他们“收到了许多政府数据请求，但他们只在79%的时间里提供了数据”。〔69〕这些互联网企业的行动逻辑是，互联网服务提供商必须践行对用户的隐私承诺，不得侵犯用户的宪法权利。

网络信息企业不仅负有“信息存储、监控、披露”等协助执法的义务，也担负着“不随意进行监控、不向他人披露以及不做他途”等个人信息保护义务。同时，网络信息企业还有自身的经营目的。这就形成了网络信息企业协助执法、保护个人信息与实现经营目的之间的制度冲突。〔70〕基于我国宪法第40条所规定的“公民的通信自由和通信秘密受法律保护”，网络信息企业“不应当在普遍意义上承担通信权类信息的存储、审查和报告的协助执法义务”。〔71〕网络信息企业“协助执法的义务必须受到其所承担的保护公民基本权利之义务的限制”，其承担的义务应符合比例原则，符合“手段适当性、必要性、均衡性”的基本要求，且应在技术上具有可行性，不会“实质性地减损其经营利润”。〔72〕负担协助数据查询义务的网络信息企业，对作为公权力机关的数据查询和调取者难以享有对等制约能力，因而应将数据查询和调取中的守法义务更多交由公权力主体负担，同时还应明确设定网络信息企业协助查询数据的义务边界。若执法协助请求超出该义务边界，企业有权拒绝协助。

通常来说，公安机关等侦查机关对数据信息的调取范围和方式，应与数据的敏感程度相关联，“涉及个人隐私的大数据仅能在正式立案后向侦查人员提供，初查和预测警务阶段仅能针对一般个人信息进行调取和分析”。〔73〕不过，根据《监督执纪工作规则》第40条及纪检监察机关监督执纪相关规定，纪检监察机关案件审查调查组经批准可以“查询”被调查人或涉案人员的数据，且纪检监察机关“查询”数据的方式“可以在初步核实阶段使用”，“查询”并非立案后才可使用的措施。〔74〕这意味着，纪检监察机关即便在非立案情形下，也享有查询特定个人隐私数据的权力，也意味着纪检监察机关在开展一般性大数据监督时，也享有对特定企业或个人“数据”的查询权力。纪检监察机关有着独特的法律监督履职需要，赋予纪检监察机关查询数据的权力，有助于其准确发现案件线索并强化其监督效果。不过，对查询制度的进一步细化和改进依然是必要的。其一，应当明确纪检监察机关查询个人信息一般应以有问题线

〔68〕《广东省深圳市委网信办推动重点互联网企业公开承诺“保护个人信息”，压实主体责任》，http://www.cac.gov.cn/2021-11/15/c_1638574277375399.htm，2022年2月26日最后访问。

〔69〕前引〔64〕，Rudofsky文，第741页以下。

〔70〕参见裴炜：《数字正当程序——网络时代的刑事诉讼》，中国法制出版社2021年版，第36页以下。

〔71〕同上书，第68页。

〔72〕同上书，第33页以下。

〔73〕同上书，第98页。

〔74〕参见前引〔55〕，中共中央纪律检查委员会等编书，第139页。

索为前提。如果没有问题线索，通常不应行使针对个人信息的查询权力。其二，应当明确立案前的个人信息查询权力与立案后的个人信息查询权力的差异，立案前的信息查询权力应小于立案后的信息查询权力。其三，应当明确区分纪检监察机关监督执纪的信息日常查询权力和办理涉嫌刑事案件的信息查询权力的差异，前者的行使范围显然应当小于后者。其四，应当注意区分对个人基础信息的查询权力和对个人财产、通信信息等敏感个人信息的查询权力，具体可通过列举个人敏感信息清单的方式，明确不同查询权力的行使范围。

（五）完善纪检监察机关大数据监督的程序性制度

大数据监督应遵循正当程序原则。纪检监察机关调取的数据，原则上应当来源于公共数据库，而不能来自于暗网；〔75〕调取数据应当遵守严格的程序规则、数据存储规则和安全管理规则，采用“合法而有管制”的方式，〔76〕不宜采用“窃听”等方式或借助“感官增强技术”。〔77〕纪检监察机关不应根据可疑数据和数据库筛选结果形成“大数据黑名单”，这一做法实质上将被监督者推入了“有罪，直至证明无罪”的通道，侵害了公民在宪法上的权益。〔78〕

针对纪检监察机关办理一般违法违纪案件，目前已有比较完善的程序规定，例如，监督执纪工作的分级负责制度，请示报告制度，审批制度，案件调查与审理相分离，监督检查、审查调查、案件监督管理、案件审理之间相互协调、相互制约，案件管辖、回避、复议审查制度等。纪检监察机关在查办涉嫌刑事犯罪的案件时，在实体上应按照刑法的有关规定，围绕犯罪构成要件收集、固定、审查和运用证据。在程序上，监察法关于监察机关调查刑事案件的规定，在总体上与刑事诉讼法规定的程序要求和证据要求保持一致。纪检监察机关在采用大数据监督技术办理刑事案件时，应对标刑事证据规则和刑事诉讼证明标准，规范收集和调取证据。例如，侦办案件人员必须具备资格，且侦办应由 2 名以上人员进行；数据查询和调取不得超出批准的范围和权限；不得篡改、增加、删除、修改原始的电子数据；避免以威胁、引诱、欺骗等非法方式搜集证据等。

结 语

权力天然地具有扩张性，如果不对大数据监督作应有的、合理的规制，原本为了限制权力、保障权利的权力，就有可能演变成损及个人权利、社会秩序乃至社会长远发展的力量。监察法、《监察法实施条例》、《党内监督条例》、《监督执纪工作规则》等，为纪检监察机关开展大数据监督提供了基本的规范依据，但既有制度仍然存在赋权不足和限权不足的问题。在数据共享和数据处理活动中，存在着数据处理规则与大数据监督规则的冲突、数据逻辑与法律专业逻辑的冲突。大数据监督中的算法偏见、“自动售货机”理念、泛在监控观念等，也都需要通过制度的改进予以矫正或消除。面对大数据监督这一新事物，还要注意避免走入认知误区，不能简单地将大数据监督视为纪检监察人员与大数据平台的机械组合，或将大数据仅仅视为纪

〔75〕“暗网”是指那些存储在网络数据库里、不能通过超链接访问而需要通过动态网页技术访问的资源整合，不属于那些可以被标准搜索引擎索引的表面网络。参见前引〔37〕，何渊等书，第 4 页。

〔76〕参见前引〔21〕，帕克书，第 4 页。

〔77〕在凯洛诉美国案（Kyllo v. United States）中，美国联邦最高法院认为，使用感官增强技术的行为，构成了“法律上的搜查”。参见前引〔37〕，何渊等书，序言。

〔78〕See Margaret Hu, *Big Data Blacklisting*, 67 Fla. L. Rev. 1735 (2015).

检监察工作的工具或者手段。

纪检监察机关大数据监督制度的完善，可从厘清不同数据的获取和处理方式及其权力边界入手。例如，赋予纪检监察机关对政务大数据的共享权力；规范对政法类数据与法律监督类数据的调取和使用；合理限制纪检监察机关对个人信息的处理权力，尤其是采用技术调查手段获取数据的权力；规定网络信息企业不承担普遍意义上的数据查询协助义务，纪检监察机关要求其承担的协助执法义务应符合比例原则；对非立案情形下纪检监察机关享有的对个人信息的查询权力进行分级分类规制。此外，纪检监察机关在查办涉嫌刑事犯罪的案件时，在实体上应按照刑法上的犯罪构成要件收集、固定、审查和运用证据，在程序上应对标刑事诉讼法的程序规则、证据规则等搜集和调取证据。

纪检监察机关的大数据监督既涉及监督权力的行使，也涉及对监督权力的制约，更涉及对整个国家法治秩序的塑造。纪检监察工作与大数据技术相结合，不仅意味着监督方式发生了变化、部分监督规则需被重塑，也意味着如果缺少对权力的规制或者规制不当，监督权力就有可能被滥用甚至不当扩张。面对不断拓展的大数据监督实践，应及时更新理念，尽快制定、细化和完善相关制度规范，以进一步提升大数据监督的正当性，确保其在法治的轨道上行稳致远。

Abstract: The practical exploration of big data supervision by disciplinary inspection and supervision organs in many places has promoted the modernization of power supervision and restriction mechanisms, and give rise to questions about the legitimacy of big data supervision. The current practice of big data supervision lacks both standardized big data support and clear big data supervision criteria, and has problems of insufficient empowerment and limited competence at the institutional level. The improvement of the big data supervision system requires not only institutionally empowering disciplinary inspection and supervision organs to share big data, but also strengthening the restriction on the big data supervision power of disciplinary inspection and supervision organs, so as to resolve the conflicts between data rules and supervision rules, and between digital logic and legal professional logic. China should clarify the power of disciplinary inspection and supervision organs to share government big data and the rules for the acquirement and use of procuratorial, judicial, and public security data and legal supervision data, standardize the use of technical investigation means by disciplinary inspection and supervision organs, and improve the institution of data inquiry in non-case filing situations. When investigating cases involving suspected crimes, disciplinary inspection and supervision organs should collect, acquire and fix evidence in accordance with the rules of evidence in criminal procedure, so as to prevent such evidence from being excluded due to violation of legal procedures.

Key Words: disciplinary inspection and supervision, big data supervision, personal information protection, government data