公安机关数据安全监管职责的法治化路径探究

■ 唐致远

摘　要　目前，公安机关数据安全监管职责面临数据监管边界不明晰、跨部门协作机制不健全与新兴技术发展带来的挑战等现实困境。公安机关数据监管职责体系的优化应当遵循权责统一、法治保障和协同治理三大原则，以实现维护国家数据主权、保障公民个人信息权益和促进社会公共安全秩序稳定作为价值目标，对数据进行分类管理。应当通过建立权责清单制度、细化执法裁量基准、完善跨部门协同机制和构建新技术监管体系等方面对公安机关数据安全监管职责进行完善，促进公安机关数据安全监管职责的法治化。

关键词　数据安全　监管职责　权责清单　跨部门协同　技术监管

数据安全问题不仅关涉公民的个人信息保护，还关乎国家的经济利益、社会稳定以及国家安全。因此，如何构建起科学全面的数据安全法治保障体系已然成为我国社会治理的新课题。作为国家重要的执法机构，公安机关在数据安全监管中的角色和职能愈加重要和复杂。然而，由于数据监管涉及的领域和主体较多，公安机关的数据安全监管职责与其他行政执法部门之间的职责边界尚不明晰，亟需相关法律和制度进一步厘定。本文首先明确了公安机关数据安全监管的法律基础与职责范畴，进而对公安机关数据安全监管职责的现实困境进行分析，在此基础上，结合公安机关数据监管职责体系优化的总体要求，提出构建及完善公安机关数据安全监管职责体系的具体路径，提升数据安全治理的有效性，促进公安机关数据安全监管职责的法治化。

一、公安机关数据安全监管职责的法律定位

（一）公安机关数据安全监管的法律依据

1．既有法律架构

公安机关作为国家的执法主体之一，其数据安全监管职责的合法性与合理性首先源

作者：上海公安学院法律教研部讲师

于既有涉数据相关立法的明确授权。随着《中华人民共和国数据安全法》（以下简称《数据安全法》）《网络安全法》《个人信息保护法》等多部重要法律的相继施行，我国数据安全法律制度体系日趋完善，为公安机关的数据安全监管提供了基础法律依据。

具体而言，《数据安全法》第六条第三款的规定，公安机关应当依法在其职责范围内承担数据安全监管职责。2025 年 1 月 1 日颁布施行的《网络数据安全管理条例》第七章延续《数据安全法》规定，再次明确公安机关的网络数据安全监督管理职责。同时新增“依法防范和打击危害网络数据安全违法犯罪活动职责”。《网络安全法》第六十四条第二款规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚未构成犯罪的，由公安机关进行处罚。又如，《个人信息保护法》第六十条规定，国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。此外，工信部在 2022 年发布的《工业和信息化领域数据安全管理办法（试行）》中明确了其仅在工业数据、电信数据和无线电数据等本行业领域开展数据安全监管。

综合目前的法律规范性文件来看，我国数据安全监管体系总体上形成了“统筹协调、行业监管、专门执法”的三层架构体系。国家网信部门统筹协调全国范围内的网络数据安全和监管工作；工业和信息化等行业主管部门承担本行业、本领域的数据安全监管职责；而公安机关、国安机关则在各自职责范围内相应的履行数据安全监管职能。

2．立法目的探析

就我国数据安全领域相关立法实践来看，比较明显的特点是突出数字化时代下国家对公民权利保护和国家公共利益的重视。在《个人信息保护法》第一条和第十一条阐述了其立法目的主要在于规范个人信息处理活动，预防和惩治侵害个人信息权益的行为，保护个人信息权益。根据《数据安全法》第一条规定，主要目的是为了规范数据的处理活动，保护个人、组织的合法权益的同时维护国家主权、安全和发展利益。

此外，立法者通过“授权 + 限权”的双重逻辑，既赋予公安机关对数据违法行为的行政执法权限，也对权力进行了一定限制。具体体现在《网络安全法》第六十四条对非法获取个人信息的处罚权，同时在该法第八条中又通过“职责范围内”的表述划定权力边界。这种设计既回应了现代社会公权力主动积极保障私主体权利的要求，又通过一定程度的保留防止了权力滥用，呼应了“法定职责必须为、法无授权不可为”的现代法治精神。

综合前述相关规定，不难发现其深层的立法逻辑在于：以公安机关监管权力法定化方式推动依法行政理念的深入，同时实现治理范式从原先的“事后惩戒”向“事前、事中防控”的转型，最终服务于国家数据主权空间构建和公民基本权利保障的整体目标。

（二）公安机关数据监管职责的厘定

就目前的现状来说，公安机关的数据监管职责主要集中在行政执法、刑事司法以及维护社会安全三个方面。在信息化时代，强化公安机关在数据安全保障方面的职能，是维护网络秩序、打击数据犯罪和完善社会治理能力、维护公共安全的重要方面。

1．刑事司法维度

公安机关作为刑事司法机关，在打击数据安全相关犯罪上应当承担相应职责。对于

从事非法侵入他人计算机系统、干扰他人计算机系统正常运行、窃取计算机系统数据等危害计算机系统安全的行为，如符合刑事犯罪，公安机关应依法予以立案侦查。同时也要充分利用自身优势，通过技术手段追溯数据黑产的源头，打击网络犯罪行为以形成震慑效应。在此过程中需以保障公民权利为数据安全保护的重要价值取向，严格遵守刑事诉讼程序，保障取证过程的合法性，提升案件的办理质量和效率。

2．行政执法维度

在行政执法方面，公安机关的职责主要集中于维护网络安全秩序、查处数据违法行为、网络安全等级保护和关键信息基础设施安全保护的监督与管理等工作。例如，对于网络运营者违反数据安全保护义务，即有关企业或个人未落实安全技术方面措施、防护手段未达到网络安全等级保护的标准、违规存储和传输敏感数据、未履行数据安全事件报告义务导致发生重大网络安全案事件等违法违规行为依法进行处理；此外针对窃取或者以其他方式非法获取公民个人信息，出售或是非法提供公民个人信息等违法但还未构成犯罪的行为可以予以行政处罚。公安机关还可通过常态化巡查、开展专项治理等督促关键基础设施运营者履行数据安全主体责任，加强数据安全合规管理。

3. 维护社会安全维度

在维护社会安全方面，公安机关需要构建起数据安全风险的社会面风险防控体系。例如，针对由于数据泄露引发的群体性事件、人工智能伪造传播的虚假信息、基于关键基础设施的数据遭篡改导致的公共基础服务瘫痪等新型社会风险。公安机关应协同网信、工信等部门开展安全性评估，合作建立起一套高效的数据风险防范预案体系。依据《突发事件应对法》第四十二条规定，县级人民政府及其有关部门应当组织开展面向社会公众的应急知识宣传普及活动和必要的应急演练。公安机关作为最深入基层的政府主体之一，应当承担起数据安全的宣传教育职能。在此要求下，公安机关需通过多形式的普法宣传活动，增强公众对数据安全意识，从而规避数据安全事件的发生。

二、公安机关数据安全监管职责的现实困境

虽然公安机关在数据安全监管领域拥有相应的职责，但在实际操作过程中，仍面临着一系列亟待解决的挑战与问题，对公安机关开展数据安全监管工作构成了一定的考验。

（一）数据监管边界不明晰

在数据安全监管领域，现行法律法规对于相关部门监管边界的规定不够明晰，导致执法过程中存在一些模糊地带。例如，在《网络安全法》和《数据安全法》中，立法者虽肯定了公安机关在履职范围内的数据安全监管职责和数据安全保护义务，但该规定过于原则，缺乏细化的规则，使得公安机关在实践中进行数据安全监管的难度增大。又如，《数据安全法》第十二条规定，针对公民的投诉举报，要求“有关主管部门”保护相关人员的合法权益，但是有关主管部门具体为谁并不明晰，此种模糊表述还存在于《数据安全法》第三十、四十四条等多处。可以说，现行法律对各部门的监管范围及程序规范等方面缺乏清晰界定，导致行政部门实际执法过程中可能会面临“无法可依”与“选择性执法”的双重困境。

监管边界的不明晰对公安机关在数据安

全违法行为的执法方面会产生消极影响，可能损害其在司法领域的职能发挥。在面对新型数据安全犯罪行为时，公安机关在确定监管范围时可能因法律规定模糊而产生争议，导致执法过程中出现权责不清、推诿扯皮现象，进而影响案件的及时侦破和处理效率。

（二）跨部门协作机制不健全

在数据安全治理体系中，各部门之间信息沟通不畅、共享机制缺失成为影响整体行政效率与治理效能的重要因素。在目前的监管工作中，各部门所掌握的数据安全监管信息范围有限，多为本部门执法过程中的内部数据。因为数据的共享机制的缺失，部门间未能形成执法监管的合力。一般情况下，公安机关在侦办数据犯罪案件时能够从企业获取数据安全记录等内部档案信息。但由于缺乏与网信、工信部门的共享渠道，这使得其他业务部门在日常对企业开展数据安全监管工作时不能及时获得上述信息，从而也就无法进行有针对性的督促整改，降低了监管效率。此外，重大数据安全突发事件发生后，因为缺乏统一的指挥协调机制，部门之间未形成合力，使得处置的效率大大降低。

数据安全监管还存在不同部门资源分配差异较大的问题，主要表现在技术资源上。现实中，各部门之间所掌握的技术手段和检测设备并不完全相同，各自优势也不尽相同。若仅仅从数据犯罪侦查的角度来说，公安机关具有强大的取证技术和先进的侦查设备，但是在数据安全防护和检测方面的能力又有待提升；若是从技术标准制定和安全检测方面的角度来看，网信、工信部门具有先天的优势，但他们又缺乏刑事侦查和执法经验。如果有条件实现不同部门间技术资源整合，实现各部门在侦查取证、风险评估、标准制定等技术手段上的共享与互补，则可有效提升数据安全监管整体效率。

（三）新兴技术发展带来的挑战

随着云计算、大数据、物联网等技术的不断成熟，虽然这给现代社会带来了很多新的发展机遇，不过相关技术的滥用、误用、谬用对个人信息和财产安全、社会安全、国家安全也一定程度上构成了潜在威胁。

一方面，由于大数据技术促进了海量数据在不同系统、平台、机构之间的流动，其来源和去向更加复杂，这使得以传统地域为界限的管辖标准发生变化。在信息化背景下，数据存储与传输变得更加模糊不清，这会在确定案件管辖范围上带来挑战，即具体哪个公安机关有案件的管辖权将会更难判断。

另一方面借助着现代化的技术手段，黑客攻击、数据倒卖等行为呈现出隐蔽化、产业化的趋势，进而给公安机关的日常监督执法造成一定挑战。网络违法行为已然从原来的高级持续性威胁（APT 攻击）发展至人工智能驱动阶段，即借由生成式人工智能技术制造出海量虚假访问请求，以此来实现攻击网络的目的。可以说犯罪治理日益脱离了沉重的物质羁绊，抽身进入数据世界。所以新技术的发展也是一把双刃剑，对其如何合理的使用和监管是有关部门面临的一个重要课课题。

三、公安机关数据监管职责体系优化的总体要求

（一）遵循三大原则

在构建公安机关数据安全监管职责体系时，应当遵循权责统一、法治保障和协同治理三大原则，以确保监管体系的科学性和合理性。

首先是权责统一原则。在有权必有责，

失责必追究的要求下，公安机关在数据安全监管上的责任范围应该明确，真正做到权责匹配。一方面，公安机关需在制度框架内明确自身的监管权限，确保执法行为符合相关规定。避免公安机关因职能泛化所导致的多头监管和执法真空现象，导致监管效能受到影响。另一方面，还需要设置合理追责体系，保证各级公安机关履行自身监管职责时有据可查、有理可依，提升整体监督的效果。

其次是法治保障原则。数据安全监管中的所有执法行为都要严格按照法律法规的相关规定进行，这不仅需要监管行为符合实体法律的规定，在处理流程上还需要符合程序上的规定。具体而言，公安机关在监管时不仅要以《数据安全法》《网络安全法》《个人信息保护法》等法律规定作为依据，整个过程中还要遵循正当程序原则，平衡好执法手段与相对人合法权益保障的关系，尽量避免不必要的侵害。

最后是协同治理原则。数据安全监管涉及多个职能部门与监管主体，单纯依靠公安机关的力量还难以应对海量数据的监管需要。在此意义上需要各部门之间加强联动协作，即公安机关要加强与网信、工信等部门的合作，建立起信息互通、联动执法的协同机制，形成数据安全监管合力。

（二）实行分类管理

在公安数据监管工作中整体数据可以大体归为执法办案数据、基础业务数据和社会协作数据三种类别，对不同类型的数据也应依据各自特点制定不同的合规标准和安全管理方案，以实现高效监管和风险防控的要求。

1. 执法办案数据

此类数据涵盖诸如刑事案件侦查过程中所形成的现场勘验数据、讯问笔录、视听资料等证据材料，还有治安行政案件办理过程中形成的执法记录类数据。因为警务数据与国家安全和公共安全关联度高、数据内容涉密性强以及涵盖个人敏感信息等多种特殊属性。所以对于此类数据的处理务必谨慎，对于数据的调取要精确到人，做好相关记录留存。管理过程应当与《个人信息保护法》《公安机关执法公开规定》等法律规范性文件的规定相符，以满足数据的保密性和合法性。

2. 基础业务数据

此类数据为公安机关内部的基础数据，具体而言包括人口信息管理数据、违法犯罪数据、交通管理数据等。这些数据中敏感性等级存在一定差异，比如相较于车辆违法信息，涉及公民身份信息和犯罪记录等数据隐私程度等级会更高一些。实际中可以根据数据价值和敏感程度的高低实施分层次、差异化的安全防护策略进行防护，兼顾行政效率与数据安全。

3. 社会协作数据

此类数据为执法过程中通过工商、民政等行业主管部门政务共享的方式获得，因为其涉及多机构、跨行业和多方协同共享的因素，在数据监管上应秉承“谁提供，谁负责”的原则，要明晰数据提供者、接受者、使用者的权责界限，强化数据流转过程中的安全技术防护手段，避免带来数据的滥用和不当关联分析的风险。

（三）明确监管目标

公安数据安全治理是一个体系化、动态化的过程，应对数字化背景下的诸多安全威胁，需围绕国家数据安全的维护、公民个人信息权益的有效保护及维护社会公共安全秩序稳定这三大目标构建整个数据监管体系。

首先，以维护国家安全为根本。数据安全事关国家的数据主权，同时也是影响国家安全的直接因素。公安机关作为数据安全监

管的主体，应重点关注涉及国家安全数据、关键信息基础设施、核心技术等重要数据的监管，同时防范来自境外的非法数据获取和网络攻击行为。公安可配合有关部门完善国家安全审查监管制度，针对威胁国家安全的重点数据进行重点监管。

其次，以保障社会安全为基础。社会公共安全秩序稳定的总体目标要求公安机关通过数据监管防控社会面风险，提升治安管理效能。在此过程中要针对敏感数据信息保持高度的警惕性，避免网络数据的不当传播或使用引发群体性事件或社会信任危机发生。

最后，兼顾公民基本权利的保护。公安机关在监管过程中应当禁止非法收集、利用和披露公民个人隐私的违法行为，切实维护公民的隐私权和人格尊严。要进一步加强针对电信诈骗、非法公开公民个人信息的违法犯罪行为的打击力度，保障公民合法权益不受侵害。

四、公安机关数据安全监管职责完善的具体路径

公安机关数据安全监管体系的构建应坚持法治化、协同化和技术驱动原则，通过健全权责清单、规范执法裁量尺度、强化跨部门协作机制、提升技术支撑等措施，确保监管体系的系统性与可操作性，以有效维护国家安全、社会秩序和公民数据权益。

（一）建立权责清单制度

职能划分的合理性有利于优化监管层级与部门协作。在公安机关内部的职能配置上，建议公安部制定《数据安全监管权力清单》，将分散在《数据安全法》《网络安全法》《个人信息保护法》中涉及公安机关的数据监管职责（如数据出境安全评估、等级保护制度等）系统整合，形成“权力名称、法律依据、适用场景、执法手段”四维清单框架。

对于公安机关内部上下级之间、横向各部门警种之间的职责权限做出明确规定。纵向方面如公安部负责制定全国公安系统内数据安全执法办案细则；省级公安机关承担区域性重要数据风险评估、省内重点企业数据合规审查；市县级公安机关履行日常执法检查、违法线索受理等基础职能。横向方面可由网安部门主责数据安全技术监管、经侦部门负责数据犯罪侦查、法制部门承担执法监督的三位一体架构。

同时，公安、网信、工信等部门在外部职能划分上，应充分考虑各部门特点和优势的情况下优化职能配置。公安侧重数据安全案件侦办及执法检查，网信、工信部门侧重标准制定。对于涉及其他监管部门专业领域的数据事项，应建立“非请勿入”的负面清单，确保公安机关的执法活动不越权、不缺位，促进多部门职责的合理分工与协作，提升数据监管效率。

（二）细化执法裁量基准

就公安机关数据安全监管问题，目前整体的法律规定过于宏观，具有较高的概括性和原则性。此外有关数据监管的规则零星分布于多部法律法规之中，一些规则之间出现重叠甚至冲突的现象。标准不明增加了规则识别难度，在一定程度上影响了数据效益的充分发挥。对此可以制定专门的政处罚裁量基准，细化数据泄露、非法交易等违法行为的处罚标准，建立阶梯式处罚体系。

山东省2024年修订的《行政处罚裁量基准》已尝试将网络安全违法行为按“轻微、一般、较重、严重”划分层次，并明确数据违法行为的具体处罚标准。如将初次违法，情节轻微认定为轻微情形；将经公安机

关责令改正后拒不改正认定为一般情形；将因拒不改正被公安机关给予行政处罚，仍拒不改正但尚未造成严后果的认定为较重的情形；将因拒不改正被公安机关行政处罚仍拒不改正且造成严重后果认定为严重情形。此外可结合数据敏感性差异、数据量级、影响范围、主观上故意与过失差异进一步细化处罚规定。可将山东的这种尝试进一步推广，提升数据监管的合理性。

（三）完善跨部门协同机制

公安机关数据安全监管职能的发挥关系到国家安全与社会稳定，为了能够有效应对数据安全风险，公安机关在数据安全监管方面亟需完善跨部门协同监管机制。具体而言，需要进一步加强与工信、市场监管、网信等部门的协同配合，建立健全跨部门协同监管机制，确保在数据安全事件发生时，能够迅速响应、高效处置，共同筑牢数据安全防线，保障国家和人民群众的切身利益。

当重大数据安全事件涉及网信、工信、公安等多部门监管职责时，可以由国家网信部门牵头启动“三级联动响应机制”：组建由分管领导组成的应急指挥中心，在 24 小时内完成涉案系统风险等级评估；协调层召集相关部门召开联席会议，制定跨部门调查方案；执行层搭建跨系统数据共享平台。这种协同监管机制能够将多部门协同原则转化为具体可操作的制度实践，有助于提升我国数据安全事件的应对能力，为维护国家数据安全提供有力的保障。

（四）构建新技术监管体系

数据管辖权的确立与行使，不仅只是关乎数据的归属、使用和保护，还涉及到数据主权、数据跨境流动等更加复杂的问题，对于国家安全和个人隐私有着十分重要的意义。针对大数据云计算环境下的数据存储碎片化和管辖难以确立的问题，可以尝试运用区块链技术构建全国统一的云服务器节点登记平台，要求相关主体实时上传服务器地理坐标与数据存储分布图，实现数据存储位置的动态追踪。公安机关可接入该平台电子取证接口，实现“物理位置穿透式监管”，破解属地管辖盲区。同时也可以探索建立数据流通安全审计和溯源机制，应用区块链、数字水印、电子签名等技术手段，高效支撑数据流通过程中的取证和定责。

另一方面，对于人工智能也需要合理利用，开发挖掘其背后蕴含的巨大潜力。通过深度学习让人工智能识别异常流量和恶意代码，在对网络空间海量信息进行比对筛选基础上再由人工介入进一步核实。这样不仅节约了警力资源，同时也提升了对恶意攻击、勒索病毒等网络违法行为的拦截效率和准确率，切实以科技手段助力公安机关新质战斗力的提升。

随着数据安全越来越受到重视，公安机关在数据安全监管中的重要作用也日益凸显。然而现实中还存在着诸如具体职责划分不够清晰、跨部门协作机制仍需完善和管辖边界需进一步明确等问题。通过完善公安机关的数据安全监管职责体系，不仅有助于提升数据安全的治理能力，还能更好地维护国家安全、社会稳定和保障公民的合法权益，促进公安机关数据安全监管职责的法治化。接下来公安机关应进一步加强数据执法能力的建设，提升数据安全和公民个人信息保护水平，为我国的数据安全事业保驾护航。

责任编辑 尚钰涛