

刑事诉讼数据处理的全流程监管

郑 曦^{*}

内容提要 数字时代的刑事诉讼越来越倚重于数据处理,而数据处理涉及重大法益,应对其进行全流程监管。为实现此种监管,应以数据处理活动为监管内容、以检察机关为监管主体、以具有公权力属性的数据处理者为监管对象,勾勒出刑事诉讼数据处理全流程监管的基本架构。刑事诉讼数据处理全流程监管应以权力行使与权利保障平衡为价值取向、以数据流动与数据安全兼顾为监管目标,采用“面”“线”“点”相结合的监管方式,为数据监管工作提供指引。在具体实施层面,应围绕数据的收集、使用与加工、存储与传输、删除与销毁四个数据处理的核心阶段展开监管,以保护公民权利,并保障数据的安全和有序流动。

关键词 刑事诉讼 数据处理 数据安全 数据流动 全流程监管

目 次

- 一、刑事诉讼数据处理全流程监管的现实之需
- 二、刑事诉讼数据处理全流程监管的架构
- 三、刑事诉讼数据处理全流程监管的要旨
- 四、刑事诉讼数据处理全流程监管的展开
- 五、结语

^{*} 北京外国语大学法学院教授。

一、刑事诉讼数据处理全流程监管的现实之需

数字时代下,数据已成为人类生产生活不可或缺的“原料”,在作为社会生活一部分的司法领域,刑事诉讼的运作也愈发依赖数据。从立案之初,到侦查、起诉、审判三大核心阶段,再到裁判的执行,刑事诉讼的进程时刻伴随着对数据的收集、使用、加工、存储、传输、删除等活动,甚至在刑事诉讼正式启动之前的“调查核实”即初查阶段就有对数据的收集使用。可见,数据处理已成为一类常见的诉讼活动,且其对于刑事诉讼的重要性日益增加。

刑事诉讼活动越来越倚重对数据的处理,其原因不难理解。一方面,数据处理活动是刑事诉讼应对犯罪“迭代升级”的必然手段。数字时代下刑事案件的样态发生了巨大变化,以计算机网络为工具的犯罪数量增加,呈现出传统犯罪网络化问题,甚至以数据为对象的新型犯罪形态随着个人数据捕捉、深度伪造等技术的运用而屡见不鲜。^①面对刑事案件样态的变化,以打击犯罪为重要任务的刑事诉讼显然不能无动于衷,尤其对于公安机关、检察机关等追诉机关而言,通过数据处理取得证据是应对新型犯罪的有效途径乃至必由之路。另一方面,刑事案件数量的增加也刺激着办案机关通过数据处理活动提高诉讼效率。近年来,刑事案件数量不断攀升,导致办案机关压力巨大。2018年至2022年,全国检察机关共办理各类案件1733.6万件(其中主要是刑事案件),比2013年至2017年上升40%;^②同期全国各级法院共审结一审刑事案件590.6万件,判处罪犯776.1万人^③。面对数量如此惊人的案件所带来的压力,办案机关通过构建数据库、数据上链存证、数据调取与共享等数据处理活动,在提高诉讼效率方面取得了积极成效。在这两方面因素的作用下,数据处理活动贯穿刑事诉讼的全流程。

数据处理活动贯穿刑事诉讼全流程的同时,也会带来诸多问题:一旦数据处理者未能以审慎之态度依法处理数据,则可能侵害公民合法权益,并带来数据安全方面的风险。一是刑事诉讼中的数据来源多样,既有公权力机关尤其是侦查机关主动获取的,也有从第三方处调取的,还有由诉讼参与人自愿提供的。来源复杂的数据使得刑事诉讼中的数据在真实性、合法性等方面可能出现纰漏,亦有外泄之风险。二是刑事诉讼领域各机关间数据“互联互通、共建共享”^④的目标与缺乏连通性而形成“数据孤岛”的现实之间的差距使得数据流通出现困难。在当前各机关数据处理系统处于各自为政状态的情形下,数据不同步、数据处理效率低的现象普遍存在;即便“互联互通”的数据共享机制建成后,亦可能因技术标准或保密要求不一致而导致数据失控。三是刑事诉讼中的部分数据处理工作需外包给相关科技企业。这是因为公安司法机关往往不具备进行大规模数据

① 参见刘艳红:《网络时代社会治理的消极刑法观之提倡》,载《清华法学》2022年第2期,第175-176页。

② 参见张军:《最高人民法院工作报告》,2023年3月7日在第十四届全国人民代表大会第一次会议上。

③ 参见周强:《最高人民法院工作报告》,2023年3月7日在第十四届全国人民代表大会第一次会议上。

④ 邵俊:《刑事诉讼信息共建共享问题研究》,载《浙江工商大学学报》2019年第1期,第38页。

处理的技术能力,在建设数据库、智能化办案平台时往往需要借助科技企业的力量。而这种数据处理工作的外包,扩大了刑事诉讼中数据处理者的范围,增加了数据被非法处理的风险。

鉴于数据处理活动贯穿于刑事诉讼全流程且可能带来上述问题或风险,有必要对刑事诉讼中的数据处理活动进行全流程监管。此种全流程监管至少有三个方面的意义:一是限制权力,防止数据处理过程中的权力滥用,特别是预防具有追诉倾向的侦查机关非法收集数据;二是保障权利,尤其是保障作为数据主体的公民个人(特别是被追诉人)的诉讼权利和数据权利;三是保护数据安全,预防刑事诉讼数据被篡改、破坏、泄露、非法获取和利用,或在出现此种数据安全事件时及时应对以降低损失。需要注意的是,刑事诉讼数据处理的全流程监管至少应当有两个向度:一是基于刑事诉讼程序的全流程监管,即从立案甚至立案之前到侦查、起诉、审判再到执行,对刑事诉讼各个阶段的数据处理活动进行监管;二是基于数据全生命周期的监管,数据具有与有形生物类似的生命周期特征,大体可以分为收集、存储、使用、加工、传输、销毁等阶段,^⑤对刑事诉讼中数据处理的监管也应当围绕这些阶段展开。

欧美对刑事诉讼中数据处理的监管问题关注较早,2016年欧盟即颁布了第2016/680号指令,较为系统地规定了刑事诉讼中的数据监管问题;^⑥2018年又颁布了《警察部门使用个人数据实务指南》,涉及警察刑事执法中的数据监管问题^⑦。学界也有相关的讨论,如研究刑事诉讼中第三方处理被告人数据时的义务、^⑧探讨欧盟法院在处理通讯公司保留个人数据并授权公共机构用于刑事调查方面的案例中所形成的先前案例法、^⑨分析刑事执法部门使用地理围栏授权访问私营公司位置数据的潜在影响及其监管^⑩。

目前我国尚无关于刑事诉讼数据处理监管的系统规定,《数据安全法》等法律中的相关规定较为零散。学界对刑事诉讼中的数据处理问题也关注较少,且主要研究对象为某一具体问题。例如,作为证据种类的电子数据在刑事诉讼中的运用问题;^⑪刑事诉讼中数据收集和传输及其监管问题,如数据远程或跨境调取、^⑫数据出境、^⑬从第三方处调取

⑤ 参见罗文华:《基于生命周期的数据跨境流动程序性与实质性监管》,载《中国政法大学学报》2021年第5期,第147页。

⑥ See Directive (EU) 2016/680, at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=EN> (Last visited on June 24, 2024).

⑦ See Practical Guide on the Use of Personal Data in the Police Sector, at <https://rm.coe.int/practical-guide-on-the-use-of-personal-data-in-the-police-sector-couv-/16807913b4> (Last visited on June 24, 2024).

⑧ See Mary Arden, *Privacy and Third Parties to Criminal Proceedings*, Cambridge Law Journal, Vol.76:469, p.469 (2017).

⑨ See Ioannis Revolidis, *H.K. v Prokuratuur: On Balancing Crime Investigation and Data Protection*, European Data Protection Law Review, Vol.6:319, p.324 (2020).

⑩ See Arianna Vettorel, *Geofence Warrants and the Fourth Amendment*, Harvard Law Review, Vol.134:2508, p.2512 (2021).

⑪ 参见喻海松:《刑事电子数据的规制路径与重点问题》,载《环球法律评论》2019年第1期;林喜芬:《大数据证据在刑事司法中的运用初探》,载《法学论坛》2021年第3期。

⑫ 参见裴炜:《刑事跨境取证中的数据安全风险及其应对》,载《国家检察官学院学报》2021年第6期。

⑬ 参见郑曦:《刑事数据出境规则研究》,载《法律科学》2022年第2期。

数据^⑭；数据合规与刑事诉讼的关系问题；^⑮等等。总的来看，当前研究主要有两方面的不足：一是对刑事诉讼中数据处理活动的监管重视不够，二是往往聚焦于某一具体的数据处理行为而缺乏对数据处理活动整体性、系统性的研究。

事实上，刑事诉讼中的数据处理监管具有“特殊监管+系统监管”的特征。一方面，刑事诉讼中数据处理活动常在一定程度上影响案件的最终结果，涉及“公平正义最后一道防线”，关系公民生命、自由、财产等重要法益。故此，在刑事诉讼中对数据处理活动进行监管，须在国家公权力运行与公民个人权利保障之间寻求平衡，相较于其他领域的数据处理监管具有特殊性。另一方面，在侦查、起诉、审判等不同阶段进行的数据处理活动具有程序上的递进性，前一个阶段的数据处理活动将对后一阶段的诉讼活动产生影响。相应地，对数据处理的监管亦须在各个阶段进行协调，这就对刑事诉讼中的数据监管提出了系统性、全局性的要求。鉴于此，有必要从数据处理的监管主体、监管内容、监管对象、监管的基本理念、具体的监管制度等方面研究刑事诉讼数据处理全流程监管问题，以从更为宏观的视角理解数字时代刑事诉讼面临的变革。

二、刑事诉讼数据处理全流程监管的架构

欲实现刑事诉讼数据处理的全流程监管，必须回答三个问题：一是监管什么，即监管的内容有哪些；二是谁来监管，即监管的主体是哪一机构；三是谁被监管，即监管的对象是何者。完成对这三个问题的回答，方能初步勾勒出刑事诉讼数据处理全流程监管的基本架构。

（一）监管什么：数据处理活动

所谓刑事诉讼数据处理的全流程监管，监管的内容即是《数据安全法》所言之数据处理者的数据处理活动。刑事诉讼中，数据处理活动涉及司法权力运作与公民权利保障以及重大法益，一旦发生数据泄露、破坏等数据安全事件，可能会对国家利益、公共利益和公民权利造成损害。其一，刑事诉讼数据包含大量能够识别到公民个人的数据，如各类定位数据、身份数据、生物识别数据等，这些数据与公民名誉、隐私、财产甚至人身安全等诸多法益密切相关，一旦处置不慎可能给公民个人带来巨大伤害，故针对这些数据处理活动的监管应当重视公民合法权益的保障，以使数据处理行为符合权利保护的要求。其二，刑事诉讼数据还包括对诉讼活动的记录，如办案人员分配、案件流转等，一旦被非法处理可能影响司法公正，甚至导致国家利益受损，因此针对这些数据处理活动的监管，应当更重视公权力行使合法性之约束，以保证数据的依法、安全处理。

由于刑事诉讼数据处理存在以上特点，对其进行全流程监管应当“轻其所轻、重其

^⑭ 参见李延舜：《刑事数据调取中网络服务提供者的角色定位及关联义务》，载《法学》2023年第1期；郑曦：《刑事诉讼中从第三方处调取生物识别数据行为的规制》，载《中国刑事法杂志》2023年第1期。

^⑮ 参见李玉华：《数据合规与刑事诉讼》，载《北京航空航天大学学报（社会科学版）》2022年第2期。

所重”地从数据全生命周期的视角展开,参考《数据安全法》的相关规定,可将监管重点聚焦于以下几个阶段:第一,数据的收集阶段。数据收集是数据处理的关键阶段,以何种方式收集数据在很大程度上决定了后续数据处理活动的合法性,因此对该阶段的监管向来受到重视。^{①⑥}在刑事诉讼领域,以国家强制力为后盾的公权力机关,特别是侦查机关收集数据时,通常都是以强制的方式进行。在这个阶段如何确保数据收集的程序符合刑事诉讼法关于取证的相关规定,对于保证数据处理的合法性具有至关重要的意义。第二,数据的使用和加工阶段。刑事诉讼中数据收集完成后通常会被使用或加工,例如,将数据用于对案件事实的查证或推动诉讼进程,或将数据进行格式、体例等的转化,或将数据与其他材料结合使用。无论何种方式,此阶段的数据处理关系到数据在案件办理中发挥何种以及多大作用,在一定程度上将决定案件的走向和最终结果,故而应当慎重对待。第三,数据的存储和传输阶段。数据处理者对数据的存储和传输在刑事诉讼中十分常见,尤其在数字司法、智慧司法的建设过程中,数据连通与共享对于提升办案效率与质量具有重要意义。然而在存储和传输数据的过程中可能发生诸多问题,如存储时间过长以致缺乏合理性、传输过程出现数据泄露破坏等风险,因而在此阶段的监管有利于维护数据安全、保障数据权利。第四,数据的删除和销毁阶段。当不再有合法或合理使用数据之需时,应当将数据予以删除或销毁。有学者认为删除并非数据处理的最后环节,销毁才是数据归于消灭的处理流程末端,从而将删除与销毁的概念进行了分离,^{①⑦}此种认识符合数据全生命周期流转的实际状况。在刑事诉讼领域,当刑事诉讼的目的已然达到或不复存在时,应当删除甚至销毁数据,其间亦有必要监管,以保证此种删除或销毁及时、全面和彻底。

(二) 谁来监管: 监管主体

在对刑事诉讼数据处理进行全流程监管中,确定由哪一主体来行使监管职能应当考虑三方面因素:

一是专业性。对刑事诉讼中的数据处理活动开展监管需要具有高度的专业性,盖因一方面刑事诉讼事关被追诉人生命、自由、财产等最重要法益,本身就是一项高度专业的司法活动,故公安司法机关的办案人员需具备专业资格并经过专门培训,另一方面数据处理活动也有高度的专业性,其中常有科技手段的运用,非专业人员往往难以理解。基于上述两方面因素的考虑,履行刑事诉讼数据处理全流程监管职能之机构需兼具刑事司法和数据处理方面的专业能力。

二是独立性。数据监管主体具有一定程度的独立性,这是确保其履行监管职责的必要前提。此种独立性是数据监管主体排除干扰、履行职责的基本要求,亦是其针对数据处理活动作出专业判断之地位保障,甚至在某种意义上,无独立性之监管主体即无实质监管之可能。为确保监管的独立性,一些国家和地区的数据立法中设置了专门的数据监

^{①⑥} See Salomé Viljoen, *A Relational Theory of Data Governance*, Yale Law Journal, Vol.131:573, p.578 (2021).

^{①⑦} 参见赵精武:《从保密到安全:数据销毁义务的理论逻辑与制度建构》,载《交大法学》2022年第2期,第28-30页。

管机构,如欧盟《一般数据保护条例》(GDPR)第六章详细规定了独立监管机构的地位和权责,^⑮欧盟第2016/680号指令第42条也对刑事司法领域数据监管机构的独立性作出了明确要求,^⑯日本设置了个人信息保护委员会作为专门监管机构^⑰。针对我国刑事诉讼中数据处理活动开展全流程监管,亦须确保监管机构具有一定的独立性,以保证其监管职责的履行。

三是全程参与性。如前所述,刑事诉讼有立案、侦查、起诉、审判与执行阶段,数据处理活动贯穿此五大阶段,甚至在刑事立案之前也有以犯罪控制为目的的数据处理活动。基于此,欲实现对刑事诉讼数据处理的全流程监管,监管主体应对刑事诉讼程序的各个阶段有全程参与,方有可能令其监管工作贯穿刑事诉讼活动始终。

根据我国《数据安全法》《网络安全法》《个人信息保护法》等法律的规定,国家网信部门有统筹协调网络数据安全和相关监管工作的职责,但考虑到不同地区、不同部门的特殊性和专业性,《数据安全法》第6条又规定“各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责”,其中公安机关、国家安全机关等“在各自职责范围内承担数据安全监管职责”。这样的规定,似乎将刑事诉讼中数据处理的监管职责交托于公安机关和国家安全机关,然而从上文所述的三方面因素来看,无论是公安机关还是国家安全机关,都在独立性和全程参与性方面存在明显缺陷。公安机关和国家安全机关作为刑事诉讼中的侦查机关,天然带有追诉倾向,很难以一种客观中立的态度开展监管活动,且二者对审查起诉、审判等侦查之后的核心诉讼阶段少有参与,缺乏进行全流程监管的基础条件,故将其作为刑事诉讼数据处理的监管机构并不适宜。

相对于公安机关、国家安全机关和国家网信部门,笔者认为检察机关更适合作为刑事诉讼数据处理的监管主体。

首先,在专业性方面,刑事检察是检察机关的核心业务,检察机关在刑事司法方面的专业性毋庸置疑;在数据处理方面,随着数字检察改革的推进,“数字检察人才”培养和数字检察队伍建设愈发受到检察机关的重视,^⑱检察机关已经初步具有刑事诉讼数据处理方面的专业能力,未来还可以通过人员招录、机构调整、辅助性工作外包等方式进一步补强该能力。

其次,在独立性方面,《刑事诉讼法》第5条明确规定“人民检察院依照法律规定独立行使检察权,不受行政机关、社会团体和个人的干涉”,确定了其在刑事诉讼中的独立地位。而且大陆法系检察机关被认为是“世界上最客观之官署”^⑲,我国受大陆法系影响,亦对检察机关的客观中立性作出要求,要求检察官“秉持客观公正的立场”^⑳办理案

^⑮ See General Data Protection Regulation, at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> (Last visited on June 24, 2024).

^⑯ See *supra* note 6, Directive (EU) 2016/680.

^⑰ 参见《日本个人信息保护法》,刘颖译,载《北外法学》2021年第2期,第249页。

^⑱ 参见贾宇:《论数字检察》,载《中国法学》2023年第1期,第22页。

^⑲ 林钰雄:《检察官论》,法律出版社2008年版,第25页。

^⑳ 《中华人民共和国检察官法》第5条。

件,使得检察机关独立行使权力时具有相对客观中立性。

最后,在全程参与性方面,检察机关依据刑事诉讼法的规定对刑事诉讼活动进行从立案到执行的全程法律监督,是仅有的全程参与刑事诉讼全部五个阶段的机关,即便对于普通刑事案件的立案、执行等,检察机关也可以法律监督机关的身份实施监督。由其承担数据处理监管职责,不但具有全局的视角而且能够深入各个具体程序。

综上,由于检察机关是唯一符合专业性、独立性和全程参与性三方面要求的机关,由其作为刑事诉讼数据处理的监管机构,既有合理性,又有可行性。同时,刑事诉讼中的数据处理是以办理刑事案件为目的、附随着案件办理而进行的,因此具有显著的司法属性,这种具有司法属性的数据处理行为的监管,亦属于刑事司法的范畴,而检察机关是刑事司法领域的专门监督机关,由其作为刑事诉讼数据处理的监管机构名正言顺。司法实践中,检察机关在数字检察建设中已然开展的大数据法律监督、^{②④}在线诉讼监督^{②⑤}等工作,也为检察机关对刑事诉讼数据处理进行全流程监管打下了实践基础。

(三) 谁被监管: 数据处理者

相对于作为监管主体的检察机关,刑事诉讼数据处理全流程监管的对象是各类数据处理者。我国《数据安全法》第3条对数据处理进行了宽泛的界定,由此,刑事诉讼中的数据处理者是指所有实施数据处理活动的主体,具体而言可以分为两大类。

一类是具有公权力属性的数据处理者,具体包括刑事诉讼中的专门机关和获得专门机关授权处理数据的机构。其中公安机关是刑事诉讼中最主要的数据处理者,其在侦查过程中有大量主动收集数据以及从第三方处调取数据的工作,^{②⑥}并有存储、使用、传输数据的活动;检察机关在自侦、审查批捕、审查起诉、抗诉等刑事检察工作中既可以因“互相配合”而从其他专门机关处获取数据,亦有依职权主动收集或调取数据的权力;法院作为审判机关不仅在审判阶段有处理数据的权限,在审判完成交付执行和后续公开裁判文书等工作也有传输、公开数据的行为;此外,其他侦查机关如国家安全机关和执行机关如监狱或社区矫正机构,亦是刑事诉讼中的数据处理者。除了刑事诉讼中的专门机关之外,获得专门机关授权处理数据的机构或个人亦因此种授权而应被视为具有公权力属性的数据处理者,如智慧法院建设中因法院将司法辅助职能外包而处理相关数据的科技企业,以及受到公安司法机关指派或聘请的鉴定机构等。

另一类是具有私属性的数据处理者,最为典型的是从事刑事辩护业务的律师和律师事务所。这些律师和律师事务所通过刑事辩护业务可能收集、存储大量数据,也有可能将相关数据向其分支机构或合作机构传输,甚至可能有数据出境的需要,故而亦可成为刑事诉讼中的数据处理者。但需要注意的是,因刑事诉讼中的个人或家庭事务少量处理数据的诉讼参与人,如当事人、法定代理人、证人等,不应被视为数据处理者。

针对这两类数据处理者,检察机关作为监管机构所监管的对象应是前者即具有公权

^{②④} 参见前注^{②①},贾宇文,第13页。

^{②⑤} 参见高景峰:《数字检察的价值目标与实践路径》,载《中国法律评论》2022年第6期,第43页。

^{②⑥} 参见前注^{②④},李延舜文,第151页。

力属性的数据处理者。至于具有私属性的数据处理者的数据处理行为,无需纳入刑事诉讼数据监管的范畴,而可以通过国家网信部门的监管予以解决。理由如下:

第一,刑事诉讼中公权力机关等具有公权力属性的数据处理者是最主要的数据处理者,其处理的数据从数量上看远非律师、律师事务所等能够比拟。例如,法院系统2022年司法区块链统一平台完成超过28.9亿条数据上链存证固证。^⑦从处理数据的数量上看,将具有公权力属性的数据处理者(如公安司法机关)作为全流程监管的主要对象,符合刑事诉讼数据监管的实践需要。

第二,随着智慧法院、数字检察、智慧警务等改革的推进,数据在公权力机关之间的流转愈加高速、频繁,其间发生数据安全风险的几率也同时增大。数据从侦查机关向检察机关再向审判机关的传输对于推动刑事诉讼进程至关重要,但这一方面导致接触和处理数据的人员数量增加,另一方面由于各个机关的数据处理平台往往因由不同的科技企业开发而采用不同的技术标准,可能出现兼容性或保密技术方面的冲突,从而增加数据被非法处理的风险。

第三,以具有公权力属性的数据处理者为监管对象,体现了刑事诉讼监督公权力、保障公民权利的基本价值取向。数字时代下,国家机关作为数据权力主体大规模地集聚并利用个人数据来塑造与调整个人的行为,已成为公民权利最主要的侵害风险源之一。^⑧此种情况在刑事诉讼领域亦不例外,公安司法机关通过数据处理活动有意或无意地侵害公民权利,特别是侵害被追诉人诉讼权利和数据权利的情形时有发生。在此种情况下,通过全流程监管规范公权力机关的权力行使、保障公民权利,符合《刑事诉讼法》第2条“尊重和保障人权”的要求。

第四,对律师等具有私属性的数据处理者的数据处理行为,应主要以行政的方式予以监管,无需由检察机关在刑事诉讼中进行监管。原因在于:一方面,私属性的数据处理者在刑事诉讼中处理的数据,无论在数量还是范围上都受到严格限制,且此种数据处理行为主要针对个案,不具有系统性、普遍性,可能导致的数据安全风险亦相对有限;另一方面,我国《数据安全法》《个人信息保护法》等相关法律法规已对监管私属性数据处理者的数据处理行为作出了规定,依据这些法律法规足以满足此种数据处理行为的监管需求。

此间还有个问题值得讨论,即检察机关如何既作为监管主体又作为被监管的对象、既做裁判员又做运动员的问题。从应然的视角看,此种制度设计确实存在不足之处,但从实然的角度看,这却可能是相对合理的选择。为确保监管的独立性、专业性和有效性,根据检察机关在刑事诉讼中行使职权的方式以及其内设机构划分机制,应当考虑在检察机关内部将具体办理案件的部门与履行数据监管职责的部门进行必要的区分,以尽可能实现职司之分离。

^⑦ 参见前注③,《最高人民法院工作报告》。

^⑧ 参见王锡锌:《个人信息国家保护义务及展开》,载《中国法学》2021年第1期,第154页。

三、刑事诉讼数据处理全流程监管的要旨

构建刑事诉讼数据处理全流程监管制度,先需确定其核心价值取向,再设定此种监管欲实现的基本目标,从而为全流程监管制度设计奠定基础。在此基础上,还需合理设计监管的工作方式,以促进全流程监管价值取向和基本目标的实现。

(一) 价值取向: 权力行使与权利保障平衡

刑事诉讼向来重视预防和打击犯罪,但随着法治的进步,保护公民权利的重要意义逐步得到普遍认同,“尊重和保障人权”被视为刑事诉讼的任务,^{②⑨}从而使得人权保障也成为刑事诉讼的基本价值追求。为保证预防和打击犯罪的效果,便需使刑事诉讼程序成为社会安全秩序的捍卫者,并赋予国家公权力机关更加积极的权力和手段以控制犯罪;^{③①}而为保证权利保障价值得以实现,就要对可能对公民权利造成侵害的国家权力抱有充分警惕,防止公权力的过度扩张和滥用侵犯公民权利。为使打击犯罪和保障人权的价值均得到尊重,刑事诉讼在对为打击犯罪而进行的赋权和为保障权利而进行的限权之间应进行平衡,此种理念毫无疑问也应当适用于刑事诉讼数据处理的全流程监管之中。

一方面,刑事诉讼数据处理全流程监管的直接目的在于制约公权力。如前所述,刑事诉讼数据处理的监管应以公安司法机关等具有公权力属性的数据处理者为监管对象,其根本原因在于此类数据处理者以国家权力为依靠,一旦有故意或疏忽而非法处理数据之行为,其后果远甚于私属性数据处理者的同类行为。因此,通过监管防止公权力机关在数据处理活动中的权力滥用,意义重大且刻不容缓。为实现对公权力行使的监督和制约,刑事诉讼中的数据监管应着重从三个角度展开。一是针对数据处理的关联性进行监管。所谓关联性是指数据处理活动应当与刑事诉讼的案件办理相关,且有助于刑事诉讼目的的实现。此种关联性的要求,得以否定办案人员基于职务竞争、个人利益、窥私欲等刑事诉讼之外的原因而处理数据,防止刑事诉讼成为掩盖非法数据处理的“挡箭牌”。但需要注意的是,在尊重办案规律的基础上,此种关联性要求也允许办案人员基于个体的经验、认识等在具体办案过程中有一定的裁量空间。二是针对数据处理的合法性进行监管。所谓数据处理的合法性,即数据处理的主体、方式、程序等符合法律要求,这不但要求数据处理符合法律的具体规定,也要求其符合数据处理的基本原则。因此,就合法性展开的监管,除审查刑事诉讼中的数据处理行为是否合乎规范外,还应重视对其是否遵循比例原则下目的正当性、适当性、必要性和均衡性四项子原则要求的审查。^{③②}三是针对数据处理的真实性进行监管。数据处理的真实性有两个层面:其一是要求数据处理活

^{②⑨} 参见《刑事诉讼法》第2条。

^{③①} See Herbert L. Packer, *Two Models of the Criminal Process*, University of Pennsylvania Law Review, Vol.113:1, p.10 (1964).

^{③②} 传统的“三阶”比例原则仅包含对公权力行使的适当性、必要性和均衡性的考量,但由于目的正当是公权力正当行使的前提,目的正当性审查已为许多国家的立法与司法实践所接受。参见刘权:《比例原则》,清华大学出版社2022年版,第20-24页。

动真实,即此种活动在刑事诉讼过程中真实存在,而非捏造、虚构或后补的;其二是要求所处理的数据具有真实性,如数据的形式及其内容应是客观存在的、是伴随案件诉讼进程客观产生的。针对数据处理真实性的监管也应从这两个层面展开。

另一方面,刑事诉讼数据处理全流程监管应重视对公民权利的保障,此种保障的重点在于关注公民的数据权利。如前所述,刑事诉讼处理的数据中包含大量个人数据,直接涉及公民的人身、财产安全和隐私等重大法益,为此欧盟第2016/680号指令第三章专章规定了数据主体的权利,赋予公民数据访问权、更正权、删除权、限制处理权等一系列权利。我国《刑事诉讼法》虽未规定公民在刑事诉讼中享有的数据权利,但参考《数据安全法》《个人信息保护法》等相关法律的规定,有必要在既有刑事诉讼法律规范的基础上确认公民的数据权利,如知情同意权、数据访问权、更正权、被遗忘权、限制处理权等,并在数据处理的全流程监管中予以足够重视,保障这些数据权利的行使。除关注数据权利本身外,也需要关注公权力机关的数据处理活动对公民诉讼权利的影响。例如,控方可能以“数据倾倒”的方式将海量数据向辩方开示,但实际的效果是令辩方迷失在数据海洋中,^{③②}从本质上架空辩方的阅卷权。再如,侦查机关以从第三方处调取数据为掩饰,阻碍辩方申请非法证据排除之权利的行使。对于此种通过数据处理损害公民诉讼权利的行为,在监管过程中应有充分关注并予以纠正或向当事人提供救济。

(二) 基本目标: 数据流动与数据安全兼顾

数据流动和数据安全是数据监管的双重目标。一方面,自由流动是数据的天然属性,也是数据在生产生活中发挥价值的关键。数据流动是以数据为关键要素的数字经济得以发展的根本前提,只有流动起来的数据才是有意义的数据,而静止的数据则将濒临“死亡”。正是基于对数据流动重要性的充分认识,各国的数据立法多明确将保障数据流动作为其主旨。例如,欧盟GDPR第1条即指明,该条例保护个人数据的自由流动,且不得以保护公民个人数据为由,限制或禁止欧盟的个人数据自由流动;我国《数据安全法》第1条亦指出该法以“促进数据开发利用”为立法目的。但另一方面,数据流动会带来数据安全方面的风险,且这种安全风险可能出现在数据流动的各个环节,一旦数据遭到篡改、破坏、泄露或者非法获取、非法利用,不但公民的隐私、财产、人身安全可能遭遇威胁,企业或其他商业主体的商业利益也可能受到侵害,甚至国家安全、主权等亦可能遭受损害,例如某些国家就凭借其数据技术优势实施秘密监控活动收集他国数据。^{③③}在此种情形下,在强调数据流动的同时,也应当充分重视数据安全。我国就将数据安全纳入总体国家安全观这一基本方略的体系中,^{③④}以期实现数据流动与数据安全的兼顾。

刑事诉讼领域的数据处理活动与其他领域并无本质区别,因而兼顾数据流动与数据安全的基本理念也同样应当被贯彻于刑事诉讼数据处理的全流程监管中。

^{③②} See *S.E.C. v. Collins & Aikman Corp.*, 256 F.R.D. 403 (S.D.N.Y.2009); *Stevens v. U.S.*, 955 A.2d 200 (2008).

^{③③} 参见刘云:《中美欧数据跨境流动政策比较分析与国际趋势》,载《中国信息安全》2020年第11期,第75页。

^{③④} 参见陈文清:《牢固树立和践行总体国家安全观 谱写新时代国家安全新篇章》,载《中国信息安全》2022年第4期,第14页。

从直接目标上看,刑事诉讼领域数据处理全流程监管是为了确保刑事诉讼领域的数据安全。其一,刑事诉讼领域一旦发生数据安全事件,不但可能影响案件办理,还将损害司法公信力。例如 2019 年英国就发生过司法信息化系统的重大数据安全事件,导致案件办理系统崩溃、案件审理和相关工作停滞、数据库损坏、数据丢失,使人们对刑事司法的公正性产生了疑问,也令司法机关的形象备受打击。^⑤ 刑事诉讼领域的数据安全事件将影响人民群众在刑事司法案件中“感受到公平正义”,辜负人民群众对司法公正的期许,因此为保证刑事案件的顺利办理、维护司法的公信力,我国应当从数据安全保障的角度切入对刑事诉讼领域的数据处理进行全流程监管,将保护数据安全确立为监管的直接目标。其二,与其他领域相同,刑事诉讼领域的数据同样对国家、商业机构、公民个人的安全有重大影响。例如,在办理《刑法》第一章危害国家安全罪、第二章危害公共安全罪、第七章危害国防利益罪、第十章军人违反职责罪以及第八章和第九章职务犯罪等案件时,均可能涉及对事关国家安全的国家核心数据的处理;在办理《刑法》第三章破坏社会主义市场经济秩序罪、第六章妨害社会管理秩序罪等案件时亦可能涉及商业机构的商业秘密。至于刑事诉讼中非法处理数据给公民个人带来人身或财产等方面危害的情况就更为常见了,湖南省张家界慈利县就出现过公安机关办案人员非法使用服刑罪犯支付宝账户密码等数据而盗取 25 万余元的案件;^⑥ 江苏省苏州市虎丘区也发生过办案人员泄露报警人个人数据,引发相关人员发生冲突并导致一人重伤的案件^⑦。因此在对刑事诉讼数据处理进行全流程监管时,应当从保障数据安全的目标出发,保护国家、商业机构、公民个人的安全。

从最终目标上看,刑事诉讼数据处理全流程监管是为了促进数据在刑事诉讼领域的依法、有序、安全流动。刑事司法数字化建设以提升司法效率为内在驱动力,而提升司法效率的要点在于发挥数据在办案机关间流转带来的红利,因此尽管刑事诉讼数据处理的全流程监管是以保障数据安全为直接目标,但从根本上看最终仍应以促进数据在刑事诉讼领域的流动为目标,从而实现数据的“互联互通、共建共享”。鉴于此,在进行数据处理全流程监管时应当注意两个方面的问题:一是对于监管工作应当有全局的视角和宏观的设计,作为监管主体的检察机关应当以促进数据流动为最终目标,制定出刑事诉讼数据处理的一般规则;二是监管不能满足或终止于对数据处理活动的否定,而应具有建设性,检察机关在认定某项数据处理活动违法之后,应当以检察建议等方式指明应然的数据处理方式,使相关主体在未来的数据处理活动中依法行事,促进数据在刑事诉讼领域的有序流动。

^⑤ See Owen Bowcott, *Justice Ministry Knew Court IT Systems were 'Obsolete', Papers Reveal*, at <https://www.theguardian.com/law/2019/jan/28/justice-ministry-knew-court-it-systems-were-obsolete-papers-reveal> (Last visited on June 24, 2024).

^⑥ 参见肖鹏:《盗取当事人支付宝 25 万元,慈利县公安局辅警唐虎涉贪污罪被批捕》,载上游新闻, https://www.cqcb.com/xindiaocha/redian/2020-10-19/3141672_pc.html, 2024 年 6 月 24 日访问。

^⑦ 参见江苏省苏州市虎丘区人民法院(2017)苏 0505 刑初 332 号刑事判决书。

（三）工作方式：“面”“线”“点”监管结合

强调对数据处理活动进行全流程监管,在实践中容易出现因求“全”而平均用力、重点不突出的情况,影响监管的效果。刑事诉讼中的数据监管亦有此种可能,为此应当以“面”“线”“点”监管相结合的方式,提升监管工作的质效。

所谓“面”上的监管,是指刑事诉讼数据处理的全流程监管应有足够的覆盖性,须涵摄数据全生命周期。为实现“面”上的监管,作为刑事诉讼中数据监管主体的检察机关应重视三个方面的工作。一是制定刑事诉讼领域数据处理的一般通用规则。如前所述,欲使监管具有全局性和宏观性、实现全面覆盖,就应当重视制定数据处理规则,从而提供刑事诉讼数据处理监管的规范性依据。例如,应当确定刑事诉讼领域的重要数据目录、确立相关数据出境的安全评估和程序性规则、制定数据安全事件发生后的应急方案等,以使相关数据处理活动有据可依。二是建立刑事诉讼领域数据处理的考核评价体系。考核评价制度对于公权力机关的工作人员有“指挥棒”式的作用,^⑳甚至在一定程度上塑造了工作人员的行为方式,这点在数据处理上亦不例外。倘若能针对数据处理活动建立起一套科学的考核评价体系,则对于监管效果的实现自然大有裨益。三是构建刑事诉讼领域数据处理的教育培训机制。相较于其他领域的数据处理者(如互联网平台等),刑事诉讼领域的主要数据处理者(公安司法机关办案人员)在数据处理方面的专业知识明显不足,其行为失范的部分原因正在于相关专业知识的缺失,因此有必要构建常态化的数据处理教育培训机制,以利于实现数据监管的目的。

所谓“线”上的监管,是指刑事诉讼数据处理的全流程监管应伴随具体数据处理行为的全程,即从事前、事中、事后三个维度对有重要意义的数据处理行为展开全程监管。事前监管的价值在于提前预防非法处理数据行为,检察机关对特定数据处理行为进行事前监管亦有此种效果,例如对于国家核心数据的收集和处理可以考虑交由检察机关进行事先审批、基于国际司法协助目的的数据出境应经过检察机关事前的安全评估,均有防范风险之意义。事中监管强调对具体数据处理行为合法性的关注,检察机关在刑事诉讼中进行全程的法律监督为数据处理的事中监管提供了可能。例如,检察机关可以根据2019年《人民检察院刑事诉讼规则》第256条的规定提前介入侦查,^㉑从而对侦查程序中的数据处理行为进行同步监管。事后监管是检察机关开展数据监管的主要途径,检察机关对在刑事诉讼中主动发现或在实施诉讼监督时发现或因投诉举报等而发现数据处理者的非法数据处理行为,应予以及时处理,纠正错误行为、实施必要惩戒并向有关公民提供救济途径。

所谓“点”上的监管,是指刑事诉讼数据处理的全流程监管应聚焦数据处理过程中的关键环节,并对其间的风险点、争议点、纠纷点予以充分关注。其一,检察机关应主动

^⑳ 参见杨铜铜:《法官绩效考核制度的非司法化困境及其调试》,载《法制与社会发展》2022年第3期,第102页。

^㉑ 《人民检察院刑事诉讼规则》第256条规定:“经公安机关商请或者人民检察院认为确有必要时,可以派员适时介入重大、疑难、复杂案件的侦查活动,参加公安机关对于重大案件的讨论,对案件性质、收集证据、适用法律等提出意见,监督侦查活动是否合法。”

对刑事诉讼领域数据处理的重要风险点进行提示,引导相关数据处理者规避风险。例如,针对各个机关为办理刑事案件而传输数据的关键节点(如内外网的数据交互环节),提出技术协调性、保密层级匹配性等提示,将有助于降低办案系统遭遇攻击或数据泄露等方面的风险。其二,针对易出现非法处理数据、发生数据安全事件的风险点,检察机关应以常态化巡查和专项巡查相结合的方式,及早发现问题并加以处理。例如,就相关问题对办案机关进行约谈并提出纠正整改的建议,在能力所及时主动排除问题,在力有不逮时也可通过司法辅助性工作外包,引入科技企业等第三方的技术支持完成病毒查杀、防火墙维护、系统更新等技术性工作。其三,“点”上的监管还要求检察机关解决与数据处理活动相关的争议和纠纷。根据《数据安全法》第12条、《个人信息保护法》第65条等规定,作为监管机构的检察机关有权基于数据主体等的投诉举报及时处理与刑事诉讼中数据处理相关的争议与纠纷,从而实现通过数据监管定分止争、保障权利的效果。

四、刑事诉讼数据处理全流程监管的展开

全流程监管固然需针对数据全生命周期的各个阶段展开,不过在刑事诉讼中最容易发生数据非法处理行为、进而侵害公民权利、带来数据安全风险的当属数据的收集、使用与加工、存储与传输、删除与销毁四个阶段,故此四阶段应成为监管的重点。

(一) 数据收集阶段的监管

刑事诉讼中的数据收集是公权力机关等数据处理者的刻意行为,对数据收集的监管可以参考对证据的审查,从关联性、真实性、合法性三个方面展开,而这恰是检察机关熟悉的工作领域和工作方式,因此其监管工作的展开有扎实的实践基础。

首先,针对数据收集关联性的监管。参考证据法的关联性规则,针对数据收集关联性的监管,关注要点在于数据处理者所收集的数据与案件之间是否存在逻辑上的联系,即收集到的数据是否会使得案件办理者对待证事实产生更有可能为真或更有可能为伪的认识。但需要注意的是,对于数据收集关联性的监管不宜过度严苛,因为一方面关联性的判断取决于具体办案人员的个人经验和案件的具体情况,应当允许办案人员有一定的裁量空间;另一方面关联性的判断还需要符合诉讼认识规律,即对某一数据是否具有关联性的理解存在逐步发展的可能性,不宜一刀切。此外,在考虑数据收集的关联性问题时,还应当参考数据最小化原则,审查数据收集是否与刑事诉讼目的充分相关。数据最小化原则要求仅在服务特定目的时进行数据处理,据此,刑事诉讼中收集数据应从诉讼目的出发、以足以实现诉讼目的为标准、且不得超出实现目的所需的数量和内容,就此可以通过审查数据收集记录等方式,将收集的数据与诉讼目的相对照,以验证是否依据数据最小化原则收集数据。

其次,针对数据收集真实性的监管。如前所述,关于数据处理真实性的监管包含两个层面的内容,一是数据处理活动的真实性,二是所处理的数据的真实性。在数据收集阶段,对其真实性的监管也应包括这两个方面。相对而言,数据收集活动本身的真实性

较易审查,监管的重点应集中于所收集数据的真实性上。具体应从以下几个方面着手:第一,若是通过处理原始存储介质而收集数据的,应审查从原始存储介质中提取数据的流程是否符合规范,如是否将犯罪嫌疑人或其他人员与原始存储介质隔离、对于具备无线通信功能的原始存储介质是否采取信号屏蔽等方式阻断干扰、是否在原始存储介质中安装可能导致数据失真的程序、有无提取数据的笔录等。第二,若是以网络在线的方式提取数据的,应着重审查是否计算数据的完整性校验值,是否提取电子签名认证证书、数字签名、注册信息等关联性信息,对无法重复提取或可能发生变化的数据是否以录像、拍照、截屏等方式记录相关信息,笔录中是否包含对数据提取过程的完整记录等。^{④①}第三,对于从商业机构或社会管理机构等第三方处调取数据的,还应审查该第三方的数据收集过程和公权力机关从第三方处调取数据过程中是否存在增加、删减、修改数据的情形。第四,对于所有收集的数据均应进行同一性审查即数据鉴真,交叉运用完整性校验、可信时间戳、数字签名、区块链存证等技术性鉴真方法和保管链证明、独特性确认等传统鉴真方法,确保数据的真实性。^{④②}

最后,针对数据收集合法性的监管。合法性监管主要指向公权力机关的数据收集行为,即监管重点在于审查数据收集行为是否依法进行。此种对行为合法性的审查对公权力机关未来的数据收集活动有重要的“震慑”意义。为此,作为刑事诉讼数据处理监管机构的检察机关应当从以下几个方面进行:其一,审查收集数据是否取得数据主体的同意。刑事侦查有强制侦查与任意侦查之区分,^{④③}刑事诉讼中的数据收集以强制为主,但也有任意的空间,在任意情形下应当审查数据收集是否充分告知并取得数据主体的合法同意,以符合任意收集时的“知情—同意”规则要求。其二,审查收集过程是否遵循法定程序和相关技术标准,如收集数据是否办理相应的审批手续、收集数据的人员是否具有专业资质和能力、收集数据的人员数量是否为二人以上、有无数据提供者的签章、是否对数据的类别或文件格式等注明清楚、是否邀请见证人参与数据收集活动、有无录像等。^{④④}其三,对于不具有合法性的数据,应当参照刑事诉讼中的非法证据排除规则和瑕疵证据补正规则,根据收集数据时的违法程度是否足以影响所收集的数据具备对案件事实进行证明之资质而进行审查判断。^{④⑤}对于收集行为严重违法取得的数据,根据《刑事诉讼法》第56条的规定,属于收集行为不符合法定程序、可能严重影响司法公正、不能补正或作出合理解释的,应当依法予以排除,禁止将其用于证明案件事实并作为定案依据;对于收集行为轻微违法、存在瑕疵而得到的数据,允许补正或作出合理解释,并在完成补正或作出合理解释之后许可其在刑事诉讼中使用。

④① 参见《公安机关办理刑事案件电子数据取证规则》第二章第四节“网络在线提取电子数据”。

④② 参见谢登科:《电子数据的技术性鉴真》,载《法学研究》2022年第2期,第209-210页。

④③ 参见〔日〕田口守一:《刑事诉讼法》(第7版),张凌、于秀峰译,法律出版社2019年版,第53页。

④④ 参见《最高人民法院、最高人民检察院、公安部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》第24条。

④⑤ 参见李学军、刘静:《瑕疵证据及其补正规则的适用》,载《清华法学》2020年第5期,第115页。

（二）数据使用与加工阶段的监管

所谓数据使用是指在不实质改变数据集合的前提下对数据进行的访问、复制、研究、审查、分析、评估、计算；而数据加工是指以数据清洗、抽取、转换、分析以及其他模型化处理的方式，改变原数据集合的性质、内容，生成新数据集合。^④二者的本质区别在于是否对数据集合作实质性改变。刑事诉讼中，公权力机关等数据处理者处理数据时，既有对数据的使用，也有对数据的加工。数据的使用与加工不但是数据处理的核心阶段，也对刑事案件的最终结果有重大影响，因此应对其进行充分监管。

第一，数据使用与加工阶段的监管应以数据的区分为基础。“从区分出发进行解释”^⑤对于理清数据使用与加工阶段的基本监管思路有参考意义，此阶段的监管应从数据的层级区分展开。刑事诉讼领域所处理的数据，根据其所承载法益的重要程度以及被非法处理后可能导致的危害后果的大小，可以参照《数据安全法》第21条区分为国家核心数据、重要数据和一般数据。对于刑事诉讼中不同层级数据的使用与加工，应有不同的监管策略。其一，对于事关国家安全、国民经济命脉、重要民生、重大公共利益等重大法益的国家核心数据，原则上不允许加工，对其的使用也应当经由最严格的审批并采取最强有力的数据安全保护措施。其二，对于关系司法公正、公民人身安全等重要法益、一旦被非法处理将对国家和公共利益或公民合法权益造成严重损害的重要数据，如案件分配方案、匿名证人名录、合议庭评议记录或被追诉人生物识别数据等，对其进行使用和加工亦须格外慎重，监管机构应审查数据处理者使用此类数据是否符合法定条件、是否采取必要的保密方式等。其三，对于其他重要性相对较低、一旦被非法处理造成的危害也相对较小的一般数据，应当允许数据处理者在法定权限内进行使用或加工，但仍须监管此种使用或加工是否超出刑事案件办理的目的、是否确保安全等。

第二，数据使用与加工阶段的监管应以程序性审查为主。刑事诉讼中数据的使用与加工，是以刑事案件的办理为指向的，对此种数据使用与加工的监管，应主要采取程序性审查的方式，尊重具体办案人员的裁量权限和在当时阶段的认知，尤其不宜在事后以“全知视角”“上帝视角”^⑥进行实质性审查。此种程序性审查应重视以下几个方面：一是制定数据使用与加工的指引性规范。检察机关制定相关指引性规范，符合前述“面上”监管的工作方式要求，可以为数据处理者的数据使用与加工行为提供指引，预先防范数据的非法处理。二是把握数据使用与加工中的关键问题，如数据使用与加工的事由、具体实施使用与加工行为的工作人员及其专业资质、使用与加工过程的合法性、有无相应的笔录或记录、是否有签名或盖章等。对这些关键事项进行审查，能够大大降低数据使用与加工阶段违法处理数据的可能性。三是采取多种形式的程序性审查手段。面对不同的数据使用与加工的场景，检察机关应采取更为灵活多变的多元化审查手段，通过全面审查与抽样审查互补、定期检查与不定期检查相结合等方式，应对不同场景下的程

^④ 参见许可：《从权利束迈向权利块：数据三权分置的反思与重构》，载《中国法律评论》2023年第2期，第27页。

^⑤ [德] 卢曼：《社会的法律》，郑伊倩译，人民出版社2009年版，第10页。

^⑥ 田松：《何以知其然也——上帝视角与相对主义》，载《科学与社会》2015年第4期，第63页。

序性审查需求。

第三,对于因司法辅助工作外包而由科技企业使用与加工数据的场景,应加大监管力度。首先,应审查此种数据使用与加工的必要性。由于数据处理具有较强的专业性,公安司法机关常常缺乏此方面的专业能力,因此有司法辅助工作外包之必要,由科技企业代为使用与加工数据,以助力刑事案件的办理。这种情况下,就应当严格审查在具体的个案中是否存在此种外包的必要性,防止无必要外包带来靡费国帑、数据外泄等方面的可能。其次,应审查数据的使用与加工有无超越外包之目的。公权力机关将数据使用与加工外包,应基于刑事诉讼之目的,即或为办理具体刑事案件中处理大量复杂数据、或为建设办案系统或数据库等数据平台以利后续案件办理。检察机关应审查科技企业在数据使用与加工的过程中有无超越此种目的而将数据用于其他事项,如商业经营、个人窥私等。最后,应审查此种数据的使用与加工是否会导致对司法公正的干扰。科技企业可能因商业利益或个人观念而对数据进行有倾向性、甚至是故意歪曲的使用与加工,如此就可能产生“科技的介入不是有助于减少司法的不确定性,而是增加了司法的不确定性”^{④8},从而影响司法公正。对于这方面的可能性,监管机构应有充分的认识和重视,并通过资质审查、结果核查等方式进行监管,以降低此种风险。

(三) 数据存储与传输阶段的监管

刑事诉讼中的数据处理者在收集数据后,必然需要对相关数据进行存储;而基于刑事案件办理流程推进之需,数据也会在不同数据处理者之间进行传输。此种存储和传输过程亦有数据安全风险发生之可能,应进行充分监管。

对于数据存储的监管,应着重关注以下三个方面:一是数据存储的地点。关于刑事诉讼中数据存储地点的监管,首要的审查点在于是否符合数据本地化的存储要求。所谓数据本地化即要求数据、特别是重要数据须存储于本国,并对其出境进行限制。数据本地化是数据主权理论的产物,已被绝大多数国家所接受,即便主张数据自由的美国也对关键部门的数据提出了本地化的要求。^{④9}我国《网络安全法》第37条规定关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储,《个人信息保护法》第40条将数据本地化的要求扩张到处理个人信息达到国家网信部门规定数量的个人信息处理者。刑事司法领域的案件办理系统关系国家主权、司法公正,一旦遭到破坏、丧失功能或者数据泄露,可能严重危害国家安全、国计民生、公共利益,因此可以被认定为国务院2021年发布的《关键信息基础设施安全保护条例》第2条所指之关键信息基础设施。因此,在国内办理刑事案件中收集或产生的数据应当存储于境内,对此应予以严格监管以维护数据主权。此外,基于数据安全的考虑,监管机构还需要监督办案机关将刑事诉讼中收集的数据在内部网络系统进行存储,除非有特殊情形并经严格审批和充分的安全保障,不得将数据存储于公共网络系统。

^{④8} Niklas Luhmann, *Legal Argumentation: An Analysis of Its Form*, Modern Law Review, Vol.58:285, p.294 (1995).

^{④9} 参见唐彬彬:《数据本地化法律规制的反思与完善》,载《情报杂志》2022年第5期,第163页。

二是数据存储的方式。传统上数据需使用电子设备、硬盘、光盘、优盘、记忆棒、存储芯片等介质予以存储,但随着技术的发展,云存储这一新型存储方式的出现使得数据存储的方式更为多样化。相较于传统的、“天然依附于计算机硬件设备”^{⑤0}的数据存储方式,云存储借助互联网技术呈现出存储虚拟化的特征,对于数据存储而言,存储设备借由虚拟网络而变得无法触及。这样的存储方式固然方便快捷,但存储设备与数据存储方的分离导致数据存储方对存储设备失去控制,进而对其所存储的数据失去控制,增加了数据泄露、篡改等安全风险。如前所述,刑事诉讼数据中包含大量国家核心数据、重要数据,为保障数据安全,原则上应禁止以云存储方式进行数据存储,对此监管机构应予以重点审查。

三是数据存储的时长。数据的存储时长应契合数据处理的目的,并在能完成目的的前提下尽可能缩短存储时长。我国《个人信息保护法》第19条就要求,“除法律、行政法规另有规定外,个人信息的保存期限应当为实现处理目的所必要的最短时间”。在刑事诉讼中,尽可能缩短数据存储时长,无论对于公民个人的权利保障还是整体的数据安全而言都是有益的,因此当刑事诉讼目的完成或无处理数据之需时,应当停止对数据的存储。考虑到刑事司法领域尚有建立指纹、声音、面容识别等数据库并长期保存相关数据以实现预防和打击犯罪的需要,监管机构在针对数据存储时长开展监管时应当区分不同情形,原则上要求在刑事诉讼目的完成后尽可能短的时间内(如6个月至1年)^{⑤1}删除或销毁相关数据,但在经过严格审批并有强有力的安全保障之下,亦可允许长期存储某些特定数据。

对于数据传输的监管,按照上文所述的“面”“线”“点”结合的工作方式的要求,既要审查数据传输的整体安全性,更要关注传输过程中的关键风险节点。数据传输整体安全性审查的内容包括数据传输的目的和必要性,数据传输方和接收方的管理和技术能力,双方为传输数据采取的技术措施和安全保障措施,传输过程中发生数据泄露、丢失、篡改、破坏或被非法获取和利用的风险,接收方是否将再向其他数据处理者传输数据等。而对传输过程中风险节点的关注,体现了“点”上监管突出重点的特征,具体表现为对传输过程中数据交换的关键环节进行更为严格的安全审查,例如检查不同数据处理者在数据交互的节点是否存在遭受攻击的技术漏洞、基于不同技术逻辑设计的案件办理平台在数据传输方面是否具有协调性、不同办案机关之间因保密规定的区别是否存在安全疏漏等,从而确保这些数据传输的关键节点的安全性。

(四) 数据删除与销毁阶段的监管

数据处理应基于合法之目的,当此种目的完成或不复存在时,应使数据走向其生命周期的终结环节。欧盟GDPR第17条规定了数据主体的删除权(被遗忘权),我国《民法典》第1037条、《网络安全法》第43条、《个人信息保护法》第47条等亦有关于数

^{⑤0} 郭烁:《云存储的数据主权维护——以阻断法案规制“长臂管辖”为例》,载《中国法律评论》2022年第6期,第74页。

^{⑤1} 参见《网络安全法》第21条;《信息安全技术 人脸识别数据安全要求》(GB/T41819-2022)第11条。

据主体删除权或数据处理者删除义务的规定。相对于数据删除,将销毁作为数据全生命周期终点的观点逐步得到认可,例如工信部《工业和信息化领域数据安全管理办法(试行)》第20条要求工业和信息化领域数据处理者建立数据销毁制度,并禁止对被销毁的重要数据和核心数据进行恢复。由此可见,数据销毁相较于数据删除的本质区别在于强调令数据实现永久的、不可逆的“死亡”。

在刑事诉讼领域,数据的删除与销毁在一些国家已得到立法的肯认,如《法国刑事诉讼法》第770条规定未成年人犯罪记录登记信息可在符合条件时被销毁。^{⑤2}在刑事司法中,数据的删除与销毁应成为数据处理的最后阶段,当刑事诉讼目的已然完成或者不复存在时,继续存储数据已不再符合目的正当性的要求,应当促使此类数据尽快走向终结。无论是对于保护刑事诉讼领域的公民权利,还是对于维护数据安全而言,数据的删除与销毁均有终局性的保障价值,因此作为监管机构的检察机关应对此环节进行严格监管。

针对数据删除,监管的重点在于保障公民删除权的行使并为其提供权利救济的途径。数据删除的常规方式是“请求—回应”或“主动删除”,即当删除数据的条件成就时,由数据主体向数据处理者提出删除数据的请求、数据处理者进行审查后作出删除的回应,或由数据处理者依职权主动删除相关数据。然而此种常规模式下时常发生争议,如数据处理者接到数据主体的请求后发现不符合删除条件而拒绝删除。参考《个人信息保护法》第65条关于公民有权就违法个人信息处理活动向履行个人信息保护职责的部门进行投诉举报、由该部门依法及时处理的规定,应由作为监管机关的检察机关按照“投诉—指令”模式,审查数据主体与数据处理者之间关于数据删除的纠纷。如检察机关认为已满足删除的条件,则可直接指令数据处理者删除数据。

针对数据销毁,监管的关注点在于确保数据永久性地不可恢复。倘若刑事诉讼中处理的数据关系到国家安全、公民人身安全等国家、社会、公民的重大利益,如国防军事方面的涉密数据、涉恐案件中的匿名证人身份数据等,一旦发生泄露等数据安全事件的后果难以承受,非彻底销毁不足以确保安全,则应在刑事诉讼目的完成后予以销毁并不得以任何理由或任何方式恢复。为此,作为监管机构的检察机关可以通过提出销毁建议或指令、提供销毁的程序或技术指引、监督销毁过程、实施事后检查等方式,监督数据销毁工作并确保数据不被恢复。

五、结 语

数字时代下,刑事诉讼制度不得不或主动或被动地转型,将数据处理作为推进诉讼、查明事实的必要或重要手段。然而刑事诉讼本就有公私力量的悬殊对比,数据处理又进一步带来了持续不平等的数据关系,^{⑤3}不但有权利保障和数据安全方面的风险,亦可能

^{⑤2} 参见《法国刑事诉讼法典》,罗结珍译,中国法制出版社2006年版,第612页。

^{⑤3} 参见丁晓东:《个人信息保护原理与实践》,法律出版社2021年版,第26页。

阻碍司法公正的实现,为此必须对刑事诉讼中的数据处理予以充分的、全流程的监管。检察机关以法律监督机关的身份在刑事诉讼中履行数据监管职责,将公权力机关的数据处理活动“关进制度的笼子”,有利于促进刑事诉讼打击犯罪和保障人权的价值目标的实现,也有利于实现刑事司法领域数据流动与数据安全的平衡,是当前制度框架下的较优选项。但随着技术和制度的进步,刑事诉讼数据处理全流程监管的制度革新亦有可能,例如创设专门、独立的数据监管机构以解决检察机关之数据处理与监管角色混同的问题。对于此种监管制度革新之可能性,我们应当如同法律对待技术的姿态一般,对其抱有既审慎又开放的态度,在理论反思和实践探索中不断寻求更优方案,以确保刑事诉讼数据处理活动始终在法治轨道上进行,并以此促进刑事司法现代化的实现。

Abstract: In the digital age, criminal procedure increasingly relies on data processing, which involves significant legal interests and thus requires full-process supervision. To achieve this kind of supervision, data processing activities should be the focus of supervision, procuratorates should serve as the supervisor, and data processors with public power attributes should be the subject of supervision, thus outlining the basic framework for the full-process supervision of data processing in criminal procedure. The value orientation of balancing power exercise and rights protection should be determined first, and the supervision objectives of both data flow and data security should be set, followed by the supervision method with a combination of ‘surface’, ‘line’, and ‘point’ to provide guidance for data supervision work. At the practical level, the full-process supervision of data processing in criminal procedure should focus on the four core stages of data collection, usage and processing, storage and transmission, and deletion and destruction, to achieve the regulatory objectives of protecting citizens’ rights and ensuring data security.

(责任编辑:王 楷)