汉坤法律评述

2020 年 7 月 3 日

HANKUN
汉 坤 律 师 事 务 所
Han Kun Law Offices

北京 | 上海 | 深圳 | 香港

简评《数据安全法》草案

作者：段志超 | 蔡克蒙 | 周莎莎 | 胡敏喆

2019 年 10 月至今，中共中央、国务院相继发文，明确了数据作为新的生产要素的地位，要求加快培育数据要素市场、推进政府数据开放共享、提升社会数据资源价值，而通过统一立法加强数据安全保护将是充分发挥数据产生要素价值的基础保障。与此同时，数字经济的不断发展也使得数据作为战略资源的地位愈加凸显，包括数据主权、数据跨境传输、数据相关贸易管制问题在内的数字时代下的特有问题尚需以数据为中心的基础性法律为在这一特定领域维护国家安全、确保国家利益提供依据。

有鉴于此，全国人大常委会于 6 月 28 日首次审议了备受瞩目的《数据安全法》（草案）（“**草案**”），并公布了草案全文。草案总结和提炼了近年来实践中的数据治理要求并将其上升到法律高度，勾勒出我国未来数据安全保护方面的主要制度框架。我们认为草案有以下值得关注的要点。

一、适用范围

草案明确在我国境内开展的数据活动，包括数据的收集、存储、加工、使用、提供、交易、公开等，均适用本法规定。此外，草案还规定了特定域外效力，中国境外的组织和个人开展数据活动损害中国国家安全、公共利益或公民组织和合法权益，依本法追究责任。

草案还规定，对于涉及国家秘密、个人信息等特殊类型的数据，适用《保守国家秘密法》或个人信息保护方面法律的特殊规定。

二、数据安全保护的职责分工

草案明确了中央和地方各部门在数据安全保护工作方面的责任和职责。

1. 中央层面：中央国家安全领导机构，即国家安全委员会将负责我国数据安全工作的决策和统筹协调；国家网信部门负责统筹协调网络数据安全和相关的监管工作；公安机关、国家安全机关则在各自职责范围内承担数据的安全监管职责；

2. 地方和各部门层面：各地方、各部门分别对各自工作中产生、汇总、加工的数据和数据安全负主体责任；

3. 行业层面：工业、电信、自然资源、卫生健康、教育、国防科技工业、金融业等行业主管部门统一负责本行业、本领域的数据安全监管工作。

上述管理体制既体现了集中领导，也兼顾到了各地各部门、各行各业的实践差异，有利于各地各部门、各行各业在国家统一的原则方针的指引下，开展有针对性的数据安全管理活动。

三、数据分级分类与重要数据保护

在数据的安全管理方面，草案提出了全面的数据分级分类保护要求，并在此基础上对重要数据予以重点保护。在草案出台之前，我国已经对金融、电力、卫生健康、关键基础设施等重点领域提出了数据分级分类保护的要求标准。草案则借鉴了网络安全等级保护中的分级标准，提出按照数据遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者公民、组织合法权益造成的危害程度，对数据实行分级分类保护。

在数据分级保护的基础上，草案进一步提出了重要数据的基本保护要求，包括：

1. 重要数据处理者应设立数据安全负责人和管理机构；落实数据安全保护责任；
2. 重要数据处理者应按照规定开展风险评估，并向有关主管部门报送风险评估报告。该报告应当包括本组织掌握的重要数据的种类、数量，收集、存储、加工、使用数据的情况，面临的数据安全风险及其应对措施等。

2019 年的《数据安全管理办法（征求意见稿）》曾将重要数据界定为“一旦泄露可能直接影响、经济安全、社会稳定、公共健康和安全的数据”，可能包括未公开的政府信息，大面积人口、基因健康、地理、矿产资源等，一般不包括企业生产经营和内部管理信息、个人信息等。或许是考虑到重要数据种类繁多，草案此次并未对重要数据的概念作出界定，而是授权各地区和行业主管部门制定本地区、本行业重要数据保护目录。实践中如何处理不同地区、部门划定的重要数据范围间的冲突有待进一步观察和明确。

四、数据交易制度

近年来，我国已在贵阳、上海、武汉、重庆等地建立数据交易所，数据交易合作已成为金融风控和征信、广告传媒、地图测绘、医药健康、环境气象等领域的市场主体重要的数据来源。草案的一项突破在于首次正式在立法层面承认数据交易及数据交易服务提供者的合法性[1]，这方面的主要规定包括：

1. 第 3 条将数据交易视为一项数据活动，为数据的交易活动赋予正当的法律地位；
2. 第 17 条规定国家建立和健全数据交易制度，规范数据交易行为，培育数据交易市场；
3. 第 30 条规定“从事数据交易中介服务的机构”应当要求数据提供方说明数据的来源，审核交易双方的身份，留存相应的审核和交易记录；
4. 第 43 条规定数据交易中介机构未履行第 30 条规定的，导致非法来源数据交易的，有关主管部门将责令改正，没收违法所得，并予以罚款、吊销相关业务许可证、吊销业务执照的行政处罚。相关责任人员也将被处以罚款。

由于数据交易的复杂性和多样性以及数据权属在法理层面仍存在诸多争议，草案并未对数据交易具体制度作出规定，而是留待实践中根据具体数据类型和应用场景探索。随着草案正式在法律层面承认数据交易的法律地位，我们可以期待数据交易制度未来将更好地为各个行业赋智赋能。

[1] 2017 年出台的《民法总则》承认数据作为财产保护的客体在一定程度上也为数据交易制度奠定了基础。

五、数据安全审查制度

草案第 22 条首次规定了我国的数据安全审查制度，旨在从国家安全角度出发，建立全方位的网络空间和数据安全保护制度，进一步维护我国的网络空间主权，避免事关国家安全的数据信息遭到泄露与破坏。草案并未对数据安全审查制度的内涵予以明确，而是原则性地要求影响或者影响国家安全的数据活动应接受国家安全审查。由于安全审查将覆盖我国境内的数据活动，因此受到社会广泛关注的数据出境安全审查制度未来亦可能被涵盖其中。此外，相应的安全审查决定可能将成为最终决定，进而排除现有行政复议或行政诉讼的救济渠道，凸显了行政机关在这一问题上的裁量性和专业性。

六、明确数据主权、推动数据跨境流动：

数据出境安全评估一直是社会各方关注的焦点问题。尽管本次发布的草案并未就此进行明确规定，但却提出了与数据跨境流转相关的出口管制、数据相关反制措施、跨境数据执法报批制度。这体现出了国家保障数据安全、鼓励数据自由流动的基本理念。一方面，数据是数字经济发展的关键要素，草案明确我国将积极参与国际交流、促进数据跨境流动；另一方面，数据也是国家基础性战略资源，出于国家安全等方面需要，我国将建立数据出口管制制度、数据利用反制措施及境外调取数据的报告批准制度，有效应对数据领域的国家安全风险与挑战。

（一）加强数据领域国际交流合作

作为世界第二大数字经济体，我国始终将数字经济视为国际交流合作新重点，而数据则是数字经济发展的关键要素。为进一步推动数据跨境流动，草案第 10 条明确，国家将积极开展数据领域国际交流与合作，参与数据安全相关国际规则和标准的制定，共同促进数据跨境安全、自由流动。

（二）确立数据出口管制制度

伴随着数据的跨境流动，数据主权和数据安全等问题也日益凸显。在此背景下，草案首次提出数据出口管制制度，对与履行国际义务和维护国家安全相关的属于管制物项的数据依法实施出口管制。数据的出口管制如何与国家安全审查及数据出境安全评估制度等制度相衔接值得我们进一步关注。

（三）明确针对数据、数据开发利用相关投资、贸易措施的反制措施

在近年来全球贸易和投资冲突加剧的背景下，草案明确规定任何国家或者地区在与数据开发利用技术等有关的投资、贸易方面对中国采取歧视性的禁止、限制或者其他类似措施的，中国可以根据实际情况对该国家或者地区采取相应的措施。

（四）明确跨境执法中的数据调取问题

就跨境执法中的数据调取问题，2018 年通过的《国际刑事司法协助法》和 2019 年修订的《证券法》已分别从刑事诉讼及证券业务角度，禁止境外机构在中国境内直接进行调查取证活动，并要求境内组织或个人未经同意不得向外国提供证据材料。作为数据领域的基本法，草案对境内组织及个人向境外执法机构提供数据的报批义务进行了进一步明确，原则上要求有关组织、个人应当向有关主管机关报告，获得批准后方可提供。

七、落实政务数据开放任务

为适应电子政务发展的需要，落实《促进大数据发展行动纲要》中的政府数据开放任务，草案就政务数

据安全与开放设置专章规定，进一步明确政务数据安全管理制度和开放利用规则，以推动政务数据资源开放和开发利用。

一方面，在基本原则层面，草案继续延续了《政府信息公开条例》中以公开为常态、不公开为例外的规定，要求国家机关遵循公正、公平、便民的原则及时、准确地公开政务数据。另一方面，具体实践中，草案规定国家将制定政务数据开放目录,构建统一规范、互联互通、安全可控的政务数据开放平台，以推动、落实政务数据开放利用。

事实上，目前我国各地已陆续出台了地方公共数据开放与安全管理规定，并不断规划完善数据开放平台：

1. 2016 年，贵阳政府率先启动建设数据开放平台，向社会免费开放数据资源，基本涵盖贵阳市级所有政府部门及相关直属事业单位。

2. 2018 年，上海市出台《上海市公共数据和一网通办管理办法》及《上海市公共数据开放暂行办法》，对包括政府数据在内的公共数据的开放流程、平台建设、安全保障等内容进行细化规定。

3. 2019 年，北京发布《关于通过公共数据开放促进人工智能产业发展的工作方案》，提出将在全国率先建成公共数据开放创新基地，通过特定方式向北京人工智能企业有条件开放医保、司法、交通等领域的一批特殊公共数据资源，为企业开发产品、创新应用提供无偿和精准的数据供给；同年出台的《交通出行数据开放管理办法（试行）》则通过向社会开放交通出行数据，致力于促进交通行业和互联网企业深度融合，优化和改善出行引导服务。

4. 2020 年，浙江推出全国首部省域公共数据开放立法《浙江省公共数据开放与安全管理暂行办法》，对开放数据、开放途径、数据安全进行了全方位规定，并细化明确了大数据管理局职责与专家委员会制度。

草案确立的政务数据公开制度将有助于充分利用政务数据这项公共资源，推动和深化各行业和领域的智能化和数字化转型，更好地服务于我国经济社会的发展。

八、结语

《数据安全法》（草案）的颁布对我国此前一个阶段的数据治理实践进行了初步总结，在综合考虑数字经济特点的前提下确立了数据安全和发展领域的多项基础性制度，是对《网络安全法》确立的网络空间治理规则的有益、必要的补充。以此为基础，后续随着《个人信息保护法》、重要数据确定规则、数据安全审查制度、以及数据跨境传输制度的落地，社会公众此前对众多现实问题的关注将得到回应，数据市场和数据行业的发展也将愈加有法可依，未来可期。

特别声明

汉坤律师事务所编写《汉坤法律评述》的目的仅为帮助客户及时了解中国或其他相关司法管辖区法律及实务的最新动态和发展，仅供参考，不应被视为任何意义上的法律意见或法律依据。

如您对本期《汉坤法律评述》内容有任何问题或建议，请与汉坤律师事务所以下人员联系：

段志超

电话： +86 10 8516 4123
Email： kevin.duan@hankunlaw.com