

安全与发展并重——《数据安全法（草案）》要旨与解读

作者：潘永建 | 邓梓珊 | 沙莎 | 胡鑫超

2017 年 6 月,《网络安全法》的生效奠定了网络空间数据保护的基石。2018 年 9 月,十三届全国人大常委会立法规划中,《数据安全法》和《个人信息保护法》被列入第一类项目中条件比较成熟、任期内拟提请审议的法律草案。2020 年 7 月,在维护国家安全、抵御数据风险、发挥数据“新动能”的背景下,《数据安全法(草案)》(以下简称为“《草案》”)率先公布,旨在“以安全促发展、以发展促安全”。

《草案》围绕数据安全和数据开发利用,既明确数据是国家安全的重要组成部分,需通过立法提升国家数据安全保障能力,又强调数据作为新的生产要素,对社会经济发展具有引领作用。为帮助企业了解《草案》的实质及影响,笔者通过拙文梳理《草案》脉络,厘清《草案》相关法律体系与框架,并对《草案》条款进行重点详解。

一. 外解挑战、内促发展：数据安全治理的“中国方案”

自 2018 年以来,随着 GDPR 的生效,全球范围内掀起数据保护的浪潮。根据联合国贸发会的数据,截至 2020 年 4 月,已有 132 个国家出台隐私与数据保护法律。¹ 以“国家安全”为盾抵御数据跨境流通带来的风险似乎已成为备受青睐的有效举措,甚至成为各国政治、经济博弈的重要手段。

2020 年 6 月 29 日,印度电子与信息技术部以有损印度主权和完整、国防安全、国家安全和公共秩序为由封禁 59 款有中国背景的手机应用程序。该部门称其收到了来自各种渠道的投诉,Android 和 iOS 平台部分应用程序以未经授权的方式窃取和秘密传输用户数据到印度境外的服务器,若境外

.....
如您需要了解我们的出版物,
请联系:

Publication@llinkslaw.com

¹ Data Protection and Privacy Legislation Worldwide https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

机构将这些数据汇编集合，并对印度国家安全和国防数据进行挖掘分析，最终将影响印度的主权和领土完整，因此需采取紧急措施予以封禁。²2019年11月18日，美国参议员提议制定《2019年国家安全和个人数据保护法(草案)》，³该法拟禁止将数据存储或传输至威胁美国国家安全的关注国(a country of concern)，认为该等国家的隐私和数据安全规定会对美国国家安全构成重大威胁，并明确指出关注国包含中国和俄罗斯。2020年8月5日，美国国务卿宣布“清洁网络”计划，拟从电信服务商、应用程序、云存储等五个方面清除来自中国的技术和网络服务，以保护美国公民隐私和公司最敏感信息不受侵害。⁴8月6日，特朗普总统签署两项行政命令，其中指出TikTok“可能会被用于虚假信息活动”，微信“自动获取用户的大量信息”，并以国家安全之名禁止任何美国公司或个人与TikTok的中国母公司字节跳动及微信所属公司腾讯进行交易。⁵数据安全现已成为国家安全与权力博弈的重要内容，中国的数据立法已迫在眉睫。

除应对外界挑战外，《草案》的颁布也反映了国内对于数据开发与利用的现实需求。数字经济已不再是传统经济的补充，而成为经济的新动能和就业的蓄水池。数据的应用场景不断扩大，企业不仅能够将运营产生的数据进行收集整理分析，服务于自身经营决策、业务流程，还能将处理后的数据形成数据商品，例如芝麻信用和数据银行等。党的十九届四中全会首次将数据纳入可参与分配的生产要素之中。2020年4月和5月，中共中央、国务院先后发布《关于构建更加完善的要素市场化配置体制机制的意见》和《关于新时代加快完善社会主义市场经济体制的意见》，提出“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，加强数据资源整合和安全保护，发挥数据资源价值”等新要求。《草案》的颁布也将在法律层面为推动数据发展增添活力、指明方向。

二. 数据安全治理框架

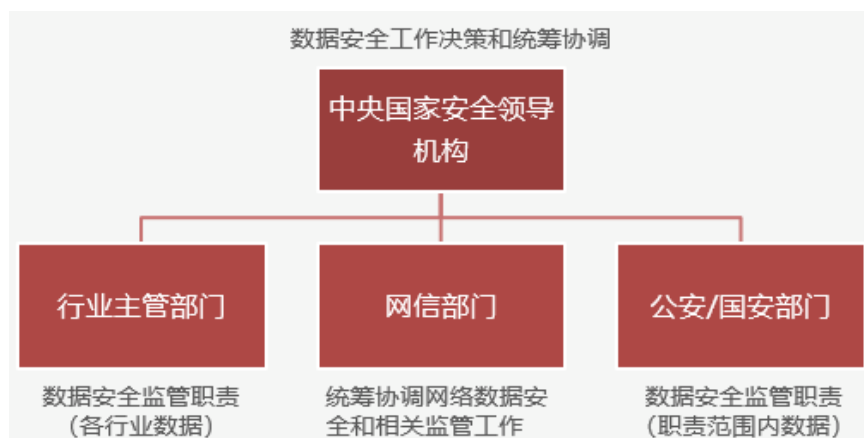
1. 监管体系

² Government Bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order
<https://pib.gov.in/PressReleaseDetailm.aspx?PRID=1635206>

³ National Security and Personal Data Protection Act of 2019
<https://www.congress.gov/bills/116/congress/senate/bills/2889>

⁴ Announcing the Expansion of the Clean Network to Safeguard America's Assets
<https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/>

⁵ Executive Order on Addressing the Threat Posed by TikTok
<https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/>
Executive Order on Addressing the Threat Posed by WeChat
<https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/>



《草案》的监管框架下，由中央国家安全领导机构负责数据安全工作的决策和统筹协调。作为《国家安全法》的下位法，中央国家安全领导机构应理解为中央国家安全委员会，而非中共中央网络信息化委员会。《草案》的规定是在数据安全领域秉承《国家安全法》第五条⁶的精神，由中央国家安全委员会整体负责数据安全工作，研究制定、指导实施国家数据安全战略和有关重大方针政策。

在具体实施层面，则由行业主管部门、公安和国家安全部门负责数据安全监管，由网信部门进行数据安全和相关监管工作的协调。尽管《草案》明确提到工业、电信、自然资源、卫生健康、教育、国防科技工业、金融业、公安机关、国家安全机关负责本领域或者本部门范围内的数据安全监管职责，但不排除实践中相关部门进行监管时职权出现交叉重叠。此外，《关键信息基础设施安全保护条例(征求意见稿)》规定，国家行业主管或监管部门按照关键信息基础设施识别指南，组织识别本行业、本领域的关键信息基础设施，此处的行业主管部门和监管部门可能也与《网络安全审查办法》中的关键信息基础设施保护工作部门相一致。因此，未来各行业主管部门、监管部门可能需要同时肩负数据安全监管职责与关键信息基础设施保护工作。

2. 基本制度和义务

作为数据安全领域的基础性法律，《草案》第九条要求建立数据安全协同治理体系。这意味着政府部门、行业组织、企业、个人应当共同参与数据安全保护工作。《草案》也明确了国家层面的数据安全基本制度与企业层面的数据安全保护义务：

国家层面：数据安全基本制度	企业层面：数据安全保护义务
第十九条：数据分级分类保护制度与重要数据保护制度	第二十五条：安全技术措施和管理制度
第二十条：数据安全管控制度	第二十六条：数据活动需符合社会公德和伦理
第二十一条：数据安全应急处置	第二十七条：数据安全缺陷和漏洞的补救及数据安全事

⁶ 《国家安全法》第五条规定，中央国家安全领导机构负责国家安全工作的决策和议事协调，研究制定、指导实施国家安全战略和有关重大方针政策，统筹协调国家安全重大事项和重要工作，推动国家安全法治建设。

机制	件的报告义务
第二十二條：数据安全审查制度	第二十八條：重要数据的数据活动风险评估及报告义务
第二十三條：数据出口管制制度	第二十九條：数据收集使用的规定
第二十四條：歧视性措施反制机制	第三十條、第三十一條：数据交易中介和在线数据处理服务商的相关义务
	第三十二條、第三十三條：配合国家机关调取数据及境外执法机构调取数据时的报告义务

3. 与其他法律法规的衔接

作为网络安全领域的奠基型法律,《网络安全法》生效已逾三年。《草案》与《网络安全法》一样,均为《国家安全法》的下位法,都属于国家安全体系的重要组成部分。《网络安全法》中不乏数据安全保护的相关规定,但该等规定侧重于数据自身安全,即网络数据的完整性、保密性、可用性;《草案》则更加侧重数据的宏观安全,即从维护国家主权安全的角度要求对数据进行有效保护,此外,《草案》还强调数据的合法利用,立法目的更加多元,在保障数据安全的同时发挥数据价值。

《数据安全管理办法(征求意见稿)》是《网络安全法》的下位法,其与《草案》都规定了网络运营者在数据处理活动中的安全保护措施。不同之处在于《草案》下的数据保护制度适用于所有数据,包括线下数据;而《数据安全管理办法(征求意见稿)》强调网络运营者应承担保护个人信息和重要数据的义务。

此外,《草案》设定的数据审查制度与《网络安全审查办法》《出口管制法》《外商投资法》等其他法律规定的网络安全审查、外商投资审查等可能存在重合,如何协调有待澄清。

三. 重点条款详解

1. 数据、数据要素与数据交易

《草案》开篇将数据定义为任何以电子或非电子形式对信息的记录,这一概念囊括了线下、非电子形式记录的信息;而数据活动包含收集、存储、加工、使用、提供、交易、公开等,几乎涵盖了数据生命全周期的进程。除了明确数据与数据活动的概念,《草案》第五条还提出数据是数字经济发展的关键要素,这与《关于构建更加完善的要素市场化配置体制机制的意见》相一致,即“加快培育数据市场,将数据作为与土地、劳动力、资本、技术等传统要素并列的要素之一”,从法律层面确立了数据的重要地位。

在数据安全与数据发展双轨并行的理念下,数据交易成为数据要素发挥作用的重要手段,只有数据流通才能挖掘数据价值,激发数据的生命力。具体而言,数据交易包括以货币交换数据商品

和以数据商品交换数据商品两种形式，其中数据商品涵盖了原始数据和加工处理后的数据衍生产品，即大数据。⁷由此看来，目前实践中常见的购买数据报告和企业间数据融合的行为都应纳入数据交易的范畴。《草案》针对越来越多的数据交易行为明确提出建立数据交易管理制度，一方面加强规范，另一方面则培育相关市场以进一步发挥数据价值。数据交易过程中，数据交易服务机构将发挥重要作用。《草案》第三十条和第三十一条专门针对数据交易中介服务机构和专门提供在线数据处理服务的经营者进行规定。

目前上海、浙江、贵州、吉林等地均已建立专门的数据交易中介服务机构，例如上海数据交易中心即为数据资源拥有方、数据技术开放方、数据应用方等大数据产业链各端提供市场化合作的平台，已发布数据流通安全合规、数据开放平台、中国企业画像服务、通用数据治理服务等产品。《草案》规定，数据交易中中介机构提供中介服务时，应要求数据提供方说明数据来源，审核交易双方的身份，留存审核、交易记录。如果中介服务商未履行相关义务，导致非法来源的数据进行交易，则会受到罚款、吊销营业执照等行政处罚。实际操作中，如果数据中介机构仅要求数据提供方说明来源，审核交易双方的身份，并不能有效预防非法来源的数据交易。与国家标准《信息安全技术 数据交易服务安全要求》(GB/T 37932—2019)相比，国家标准要求数据交易服务机构对数据提供方的数据来源合法性证明材料声明进行审核，即不仅需要数据供方说明数据来源，数据交易服务机构本身也对相关材料承担审核的义务。

对专门提供在线数据处理等服务的经营者而言，则应注意《草案》提出的经营资质要求，即取得经营业务许可或备案，具体办法应参照国务院电信主管部门出台的相关规定。目前工业和信息化部出台的《电信业务分类目录(2015年版)》B2 第二类增值电信业务中已经包括在线数据处理与交易处理业务(B21)，要求开展该等业务的经营者取得《增值电信业务经营许可证》，例如电商平台、物联网平台、车联网平台等专门提供在线数据处理等服务的经营者未来也可能需要根据自身业务情况取得相应资质，建议相关数据处理从业者予以持续关注。

就数据交易行为的规范，贵州、海南均已出台地方政府条例。例如，《海南省大数据开发应用条例》规定，可以交易的数据必须“依法获取、经处理无法识别特定数据提供者且不能复原，或者经过特定数据提供者明确授权”。深圳、安徽、山西、吉林、天津等地也颁布了大数据或数据开发相关的地方政府条例草案，目前正在征求意见阶段。此外，多地针对政务数据/公共数据或特定行业数据进行立法，其中也不乏数据交易相关规定。因此，数据交易的参与方除了关注《草案》的规定外，还应关注地方性规定的要求。

2. 数据分级分类与重要数据

《草案》第十九条要求对数据实行分级分类保护，并且由各地区、各部门制定本地区、本部门、本行业的重要数据保护目录，对列入目录的数据进行重点保护。在《草案》颁布之前，《网络安全法》规定了数据分类、重要数据备份和加密要求。但无论是《网络安全法》还是《草案》，其

⁷ 《信息安全技术 数据交易服务安全要求》第 3.1 条。

本身对于数据分级分类的规定尚属于原则性规定，对数据分类的标准、企业违反数据分级分类的法律后果均未明确。

目前，部分行业已经对数据分类分级进行立法尝试，如《科学数据管理办法》《工业数据分级分类指南(试行)》等，但几乎均未提到企业未能遵守数据分级分类要求，如未履行重要数据保护义务时需要承担何种责任，仅《证券基金经营机构信息技术管理办法》规定，证券基金经营机构违反该办法的规定(包括数据分级分类)，将受到中国证监会及其派出机构的行政监管措施，如责令改正、暂停业务、公开谴责等处罚。目前企业可根据自身业务中涉及的数据现状进行初步梳理并相应分类定级，尽早做好数据分类分级的准备，关注本行业监管部门出台具体要求，避免因无法及时履行数据分级分类的义务而受到处罚。

在重要数据的认定方面，《草案》并未给出具体定义，而是要求各部门、各地区制定相应规则，包括重要数据保护目录及相应保护措施。此前，《数据安全管理办法(征求意见稿)》和《信息安全技术 数据出境安全评估指南(征求意见稿)》采取了定义式或列举式的方法对重要数据进行界定。如《数据安全管理办法(征求意见稿)》将重要数据定义为“一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的的数据”，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。《信息安全技术 数据出境安全评估指南(征求意见稿)》则通过《重要数据识别指南》附则列举石油天然气、煤炭、石化等 27 类重要数据。我们理解，重要数据在不同行业应具有不同的识别标准，仅制定某些规定给出宽泛的定义或予以列举在实践中不具有可操作性，难以指导各行业进行重要数据识别和保护。在此背景下，全国信息安全标准化技术委员会已正式立项国家标准《信息安全技术 重要数据识别指南》。从目前的草案稿来看，该标准不再沿用行业分类的方式，而是从数据的作用、数据被破坏后可能带来的影响等角度，将重要数据分为国民经济运行类、安保类、自然资源与环境类、健康类、敏感技术类、用户类及政府工作秘密类，能够在很大程度上指导相关部门制定重要数据目录。而企业则应密切关注各地区和行业主管部门出具的重要数据目录，厘清自身业务所涉重要数据并按要求采取重点保护措施，例如境内存储数据、设立数据安全负责人和管理机构、对数据活动定期开展风险评估并向主管部门报告等。

3. 数据安全审查

《草案》第二十二条要求国家建立数据安全审查制度，对影响或可能影响国家安全的数据活动进行国家安全审查，且国家安全审查结果为最终结果。《草案》并未提出“影响或可能影响国家安全”的判断标准和判断依据，审查部门、流程与材料也需要后续配套法规出台后再进行确认。需要注意的是，与外商投资安全审查决定和不予延长拘留期限的决定一样，数据安全审查决定也属于行政机关的最终裁决，不能再通过行政复议或行政诉讼进行更改。

在《网络安全审查办法》中，关键信息基础设施运营者采购网络产品和服务，“影响或可能影响国家安全的”，需要进行网络安全审查，其中需要考虑的国家风险因素就包括重要数据被窃取和泄露带来的风险、产品和服务的提供者遵守法律法规的情况等，因此，笔者预判，与《网络安全审

查办法》相似，数据活动是否影响国家安全也需要通过多种维度进行考量，数据安全审查的启动需要相关经营者主动申请，有关机关认为必要的也会依职权启动安全审查。实际上，网络安全审查与数据安全审查在未来可能还会出现重合的情况。例如，关键信息基础设施运营者采购境外网络产品或服务，使用该产品或服务采集了某些重要数据，则可能同时需要申请网络安全审查和数据安全审查，而两种审查是否需要同时进行、是否能够合并、审查部门是否相同以及审查结果是否会出现冲突，还需要通过未来的实施细则和实践情况予以考察。

4. 跨境数据流动

在跨境数据流动方面，此前仅强调个人信息和重要数据出境的安全评估，以及特殊类型数据的本地存储和出境审批要求，例如人类遗传资源信息、人口健康信息和健康医疗大数据等。《草案》则在第二条域外效力的基础上，通过安全审查、出口管制、反制措施和数据调取审批实现数据跨境流动的全方位监管。笔者在前文已对数据安全审查展开论述，与安全审查制度一样，《草案》对数据跨境流通的制度设计仍基本立足于原则性规定，需要通过配合其他法规或国际条约、协定实现，如属于管制物项的数据有赖于之后出台的《出口管制法》进行判断。

《草案》第三十三条规定，境外执法机构调取我国境内存储的数据需要进行审批，该条被誉为应对外国政府机构“长臂管辖”的“封阻法令”。阻断别国的数据执法活动早有先例，美国《澄清境外数据合法使用法案》(CLOUD Act)的做法是与符合要求的国家签署跨境数据请求的双边或多边执行协定，该等国家在符合特定要求的情况下可以简化行政审批的程序。就我国目前的立法状况来看，短期内可能不会对来自不同国家的数据执法行动进行区分，企业应当履行相关报告义务，配合相关审批程序。

四. 结语

数据安全是捍卫国家安全的重器，数据发展则是激发经济活力的绚烂之花。作为保护数据安全的专门性法律，尽管《草案》中多为原则性规定，但其提出的数据与数据活动、域外效力、数据开发利用、数据分级分类、重要数据、数据交易、数据安全审查、数据出口管制、政务数据等概念或要求，在法律层面确立了数据保护与数据发展并行的基本方向，相关部门也必将出台配套法规政策具体执行《草案》的各项要求。因此，企业从事数据活动应当重视《草案》的相应规定，在数据处理的全生命周期做到合法合规。

如您希望就相关问题进一步交流, 请联系:



潘永建
+86 21 3135 8701
david.pan@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求, 请随时与我们联系: master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 16/19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市建国门北大街 8 号
华润大厦 4 楼
T: +86 10 8519 2266
F: +86 10 8519 2929

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环皇后大道中 5 号
衡怡大厦 27 楼
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: Llinkslaw

本土化资源 国际化视野

免责声明:

本出版物仅供一般性参考, 并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2020