人工智能时代我国数据安全立法现状与影响研究

□ 文 | 林梓瀚　郭　丰

一、基于人工智能发展的数据安全困境

数据按照传统定义是事实或观察的结果，是对客观事物的逻辑归纳，是用于表示客观事物的未经加工的原始素材。与传统定义不同，《数据安全法（草案）》的规定更加简单明了，数据特指以电子或非电子形式对信息的记录。因此本文按照《数据安全法（草案）》定义，本文所指数据是在人工智能发展过程中所需的以电子或非电子形式对信息的记录，包括个人信息、商业信息、国防信息等。

数据、算法、算力三要素是人工智能发展的驱动力，其中数据是人工智能发展的核心。人工智能的创新发展主要靠深度学习实现，通过大量采集数据供深度学习进行模拟训练，从而促进人工智能知识与经验的积累，实现智能化。

在人工智能发展中，数据的生命周期尤其是数据安全保护重点关注的问题，按照《数据安全法（草案）》规定，数据的活动是指数据的收集、存储、加工、使用、提供、交易、公开等行为。在数据的生命周期中，每一个环节出现隐患都可能会危害数据的安全，如在数据收集时非法窃取与过度收集，数据在存储加工时被病毒攻击，数据使用时的关联分析与还原攻击。因此，在人工智能发展中数据生命周期的每一个环节都可能造成国家秘密、商业秘密、个人信息的泄露，从而危害个人隐私、社会安全与国家安全。

人工智能技术的发展给人类社会带来巨大的技术进步，人工智能技术被广泛运用到生活中的各个场景。由于疫情爆发，人工智能技术更是被大规模运用于防控疫情之中，如人脸识别技术、测温技术等。随着人工智能在生活各个场景的使用，数据安全问题凸显，我国加快立法，在法律层面在人工智能发展中对数据的安全进行保护。

二、我国现阶段的数据安全立法现状

2020年4月9日，《中共中央、国务院关于构建更加完善的要素市场化配置体制机制的意见》（简称《意见》）正式发布，《意见》明确提出数据作为五大生产要素之一，在人工智能时代，数据就是“石油”，数据赋能驱动技术与经济的发展，而数据的安全是核心。

此前，2019年发布的《新一代人工智能治理原则——发展负责任的人工智能》（简称《原则》）提出八项原则，其中第四项原则是尊重隐私，人工智能发展应尊重和保护个人隐私，充分保障个人的知情权和选择权。在个人信息的收集、存储、处理、使用等各环节应设置边界，建立规范。但是《原则》只是人工智能治理的框架和行动指南，缺乏一定的强制力。为了促进数据赋能，在人工智能发展的过程中保障数据安全，保证数据对数字经济发展的驱动作用，我国制定了相应的法律体系，《民

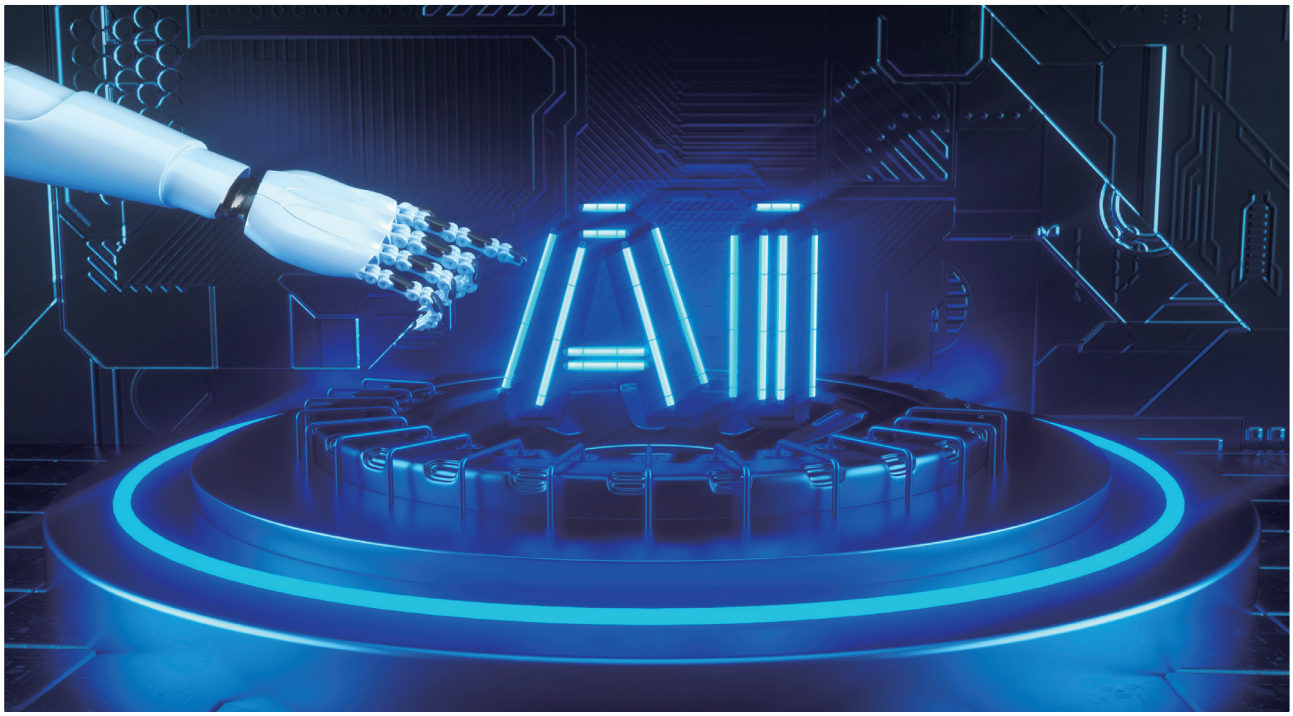
法典》第1032条至1038条明确个人隐私权，对个人信息保护进行定义，为纳入今年立法议程的《个人信息保护法》留下空间并确立方向。更具体可操作的数据安全立法体现在《电子商务法》《网络安全法》《数据安全法（草案）》以及即将发布的《个人信息保护法（草案）》中，这些法案在制度设计、保障措施、执法力度方面全面保障数据的安全与发展。

（一）《网络安全法》与《电子商务法》明确个人信息主体权利

《网络安全法》于2017年6月1日起正式施行，共7章79条。《网络安全法》对网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置、法律责任分别作出相应的规定，明确网络运营者的义务与网络用户的各项权利。其中第四章网络信息安全明确了网络经营者，包括网络所有者、网络管理者和网络服务提供者对收集的用户信息严格保密，并建立健全用户信息保护制度。《网络安全法》对个人信息的保护涵盖了人工智能运用个人信息数据的整个生命周期，包括个人信息的收集、存储、传输、使用、交易。

对于个人信息的收集，《网络安全法》规定被收集者同意是前提，网络经营者必须应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，明确了个人信息权利主体的知情权、许可权。同时，在收集的过程中确定了被收集者的“删除权”，亦既在若网络运营者违反法律法规或者约定非法收集、过度收集的情况下，被收集者可以要求其删除个人数据。

对于个人信息的存储与传输，《网络安全法》规定不得非法对个人信息进行传



输，未经被收集者同意，不得向他人提供个人信息。但是，有例外情况，在个人信息经过脱敏处理的情况下，已经无法识别特定个人且不能复原的除外。在存储的过程中法案进一步强调必须采取必要措施，确保其收集的个人信息安全。对于个人信息的使用与交易，《网络安全法》明确规定，不得非法出售或者非法向他人提供个人信息。《网络安全法》第64条同时对违反个人信息保护条款的网络经营者作出了处罚措施，相应设定了民事责任、行政责任与刑事责任。

在当前的电子商务发展中，电子商务经营者利用人工智能技术对收集到的个人信息数据进行“用户画像”，定点推送，对个人隐私造成了一定程度上的侵害。因此，2019年1月1日正式实施的《电子商务法》在《网络安全法》的基础上对个人信息保护做了进一步的强化与细化。《电子商务法》共7章89条，主要对电子商务经营者、电子商务合同的订立与履行、电子商务争议解决、电子商务促进和法律责任做出了相关的规定。纵观整个《电子商务法》，其对电子商务经营者在特定经营过程中涉及个人信息保护做出了一系列严格的规定，明确在不同场景中保护个人信息，赋予个人信息权利主体删除权，并对违反个人信息保护所应承担的法律责任也作出了清晰的规定。在《电子商务法》的第23条中明确提出保护个人信息，其规定规定电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定。

《电子商务法》同时明确个人信息权利主体的权利实现形式，赋予个人信息权利主体“删除权”。第24条要求电子商务经营者明示用户信息查询、更正、删除以及用户注销的方式、程序，不得对用户信息查询、更正、删除以及用户注销设置不合理条件，进一步加强了对个人信息权利主体权利的明示与个人信息的保护，这在《网络安全法》的基础上进一步强化了个人对信息的控制权。值得注意的是《电子商务法》在用户实现删除权方面未设置前提，这是在《网络安全法》基础上针对特定领域用户权

利加强了保护。

《电子商务法》对电子商务经营者违反个人信息保护及侵犯个人信息权利主体的权利做出了相应的处罚措施，进一步规范了电子商务经营者的经营活动，保障个人信息安全。《电子商务法》规定违反条款的，由市场监督管理部门责令限期改正，并对经营者与经营平台处相应的罚款。

（二）《数据安全法（草案）》定义数据内涵与安全保障

2020年6月28日，第十三届全国人大常委会第二十次会议初次审议《中华人民共和国数据安全法（草案）》（下称《草案》）。随后7月3日，该《草案》在中国人大网公布，面向社会各界征询意见。《草案》共51条，分七章，分别为总则、数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放、法律责任和附则。《草案》在《网络安全法》《电子商务法》《民法典》的基础上扩大了数据的范围，丰富了数据的内涵，把数据的定义从个人信息延展到记录的信息，从单纯保护个人权益扩展到维护社会、国家的安全。

《草案》的核心就是数据安全，纵观整个《草案》最重要的就是如何保障数据的安全。《草案》第三章数据安全制度为如何保障数据的安全，如何操作做了具体的规定，尤其体现在数据分级保护、安全机制设立（如预警、应急、审查等安全机制的设立）等国家监管手段。《草案》第四章数据安全保护义务明确了各数据活动主体在进行数据活动时的具体界限与义务，强化了数据活动主体的自我管理与数据保护意识。

此外，随着中美冲突的加剧，美国与其盟友加大在科技领域对中国的围堵。数据作为人工智能发展的核心，在新的国际关系背景下对我国数据在境外的安全保护以及数据跨境流动规则的明确尤为重要。《草案》规定在中华人民共和国境内开展数据活动，适用本法，这是典型的属地管辖权，但是除属地管辖外，《草案》延展管辖范围，也适用于我国境外的组织、个人。《法案》第2条规定中华人民共和国境外的组织、个人开展数据活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，亦将依法追究法律责任。《草案》对数据跨境流动也有相应的规定，《草案》第33条规定，境外执法机构要求调取存储于中华人民共和国境内的数据时，有关组织、个人应向有关主管机关报告，获得批准后方可提供。

三、我国立法的影响与存在的问题分析

（一）影响

（1）明确数据安全内涵与措施手段，保障了我国数据安全。《网络安全法》规定网络经营者对收集的用户信息严格保密，并建立健全用户信息保护制度。《电子商务法》对电子商务经营者在特定经营过程中涉及个人信息保护做出了一系列严格的规定，明确在不同场景中保护个人信息，并对违反个人信息保护所应承担的法律责任也作出了清晰的规定。《民法典》第1032条至1038条明确个人隐私权，对个人信息进行定义，确定了一系列保护个人信息的规则。《数据安全法（草案）》丰富了数据的内涵，把数据的定义从个人信息延展到记录的信息，从单纯保护个人权益扩展到维护社会、国家的安全。现有的立法体系通过明确对数据的保护，并进行制度设计，在制度层面进行预先与事后保护。同时，确定保护原则，设立相应的民事、行政、刑事责任，全方位保障我国数据安全。

（2）“赋权”数据主体，为未来立法确定方向。《网络安全法》以收集者同意为前提，明确了个人信息权利主体的知情权、许可权并在收集的过程中强调了被收集者的“删除权”。《电子商务法》进一步强化数据主体的权利，赋予主体查询权、更正权、删除权、注销权，并且这些权利的实现无设置前提。《民法典》中对个人信息进行了定义，同时强调个人隐私权利，确定了未来

个人信息保护立法的相关原则。现有的立法体系为数据主体进行“赋权”，为下一步确立“个人信息权”定下了基础，也为即将发布的《个人信息保护法（草案）》提供了权利“素材”与参考。

（3）维护我国数据主权。2018年美国实施《澄清域外合法使用数据法案》（Clarifying Lawful Overseas Use of Data Act, CLOUD Act），其规定“无论通信、记录或者其他信息是否存储在美国境内，服务提供者均应当按照本章所规定的义务要求保存、备份、披露通信内容、记录或其他信息，只要上述通信内容记录或其他信息为该服务提供者所拥有、监护或控制。”CLOUD法案明确采用“数据控制者标准”，由于全球互联网巨头大部分在美国，美国拥有巨大的优势，因此CLOUD法案实际上实现了美国的长臂管辖权。2018年欧盟实施的《通用数据保护条例》（General Data Protection Regulation, GDPR）也在一定程度上实现了欧盟的长期管辖，GDPR的适用范围不止适用于欧盟内，也适用于欧盟外的主体，其规定对欧盟内的数据主体的个人数据处理，即使控制者和处理者没有设立在欧盟内在满足条件的情况下也适用此法。《数据安全法（草案）》突破属地管辖，适用于我国境外主体是对欧美长臂管辖强有力的回应，维护了我国数据主权。同时，《数据安全法（草案）》第33条有关数据跨境流动规则对欧美主导的《布达佩斯网络犯罪公约》第32条b款进行了回应，强调“批准后方可提供”，设置了前提，进一步维护我国的数据安全与主权。

（二）立法存在的问题与不足

（1）宜粗不宜细的立法思想原则依然是主导。现有的数据安全立法依然秉持宜粗不宜细的立法原则进行立法，相关条款的规定比较模糊与抽象，依赖下位法的制定与司法解释进一步细化，灵活性比较大但是缺乏操作性与实效性，这加剧了我国的立法成本。我国现有数据安全立法与GDPR相关规定的对比，缺乏对特定场景的规定以及数据类别的区分，如缺乏在数据传输过程中对于发送者、接收者条件的具体规定等。

（2）数据权属问题尚未触及。现有的立法没有明确规定数据资产所有权的归属，数据主体与数据处理者或数据控制者对此认识存在争议。个人数据权包括财产权与人身权，数据所有权的归属决定着数据价值利益的分配以及读数据质量、安全责任的划分。现有的数据安全立法主要关注个人数据权利的人身权，明确保护个人信息安全与个人隐私，对于个人数据财产权尚未涉及。对于数据权属问题当前存在着争议，数据权益问题日益复杂化。有的观点认为，个人对数据财产权拥有绝对权，但是也存在相反意见，有的观点认为在人工智能或大数据时代，单个个人数据的价值有待商榷，数据控制者或者说平台利用收集的大量数据进而才利用数据创造出价值，因此所有权数据数据控制者。

个人数据权包括财产权与人身权，数据所有权的归属决定着数据价值利益的分配以及读数据质量、安全责任的划分。

四、结语

随着人工智能的发展，人工智能在赋能数字经济发展的地位越来越重要，数据作为人工智能发展核心，如何保障数据安全也引起各国的重视。各国纷纷立法保护本国的数据，如美国的《加州消费者隐私法》（CCPA）、印度的《个人数据保护法案》（PDPB）、巴西的《通用数据保护法》（LGPD）等。我国的《民法典》《电子商务法》《网络安全法》《数据安全法（草案）》以及即将发布的《个人信息保护法（草案）》构建了我国数据安全保护的整体法律体系，维护了数据安全，保障了数据要素赋能我国经济发展的重要作用。但是，目前我国数据安全立法宜粗不宜细的特点，数据安全立法仍然缺乏一定的操作性与实效性，有待后续下位法制定、司法解释以及后续实际运用来进行补充，未来将进一步细化与可操作化。同时，对于在人工智能时代，个人数据的财产权如何确定也将继续讨论。

随着互联网与通信技术的发展，5G时代已经到来，人类进入万物互联的时代。万物互联加速了数据的流动，因此做好数据本地化，确定数据跨境流动规则是我国数据安全立法接下来的立法方向，也是未来世界各国立法的发展方向。当前数据跨境流动规则主要是在世界贸易组织（WTO）的服务贸易总协定（GATS）有关条款的基础上制定的，GATS第14条一般例外规定了限制数据跨境流动的必要措施。无论是欧盟之间的隐私盾协议，或者美日、欧日之间基于亚太经济合作组织（APEC）的跨境隐私规则（Cross Border Privacy Rules System，CBPR）都没有突破GATS相关条款。随着欧盟与美国隐私盾协议的失效，如何确定数据跨境流动相关规则引起全球关注。我国《数据安全法（草案）》涉及了跨境数据流动的相关规定，如何在进行数据本地化的同时做好输出时合规，输入时安全，是我国下一步确定数据跨境流动规则重点的考虑。■

作者单位：中国信息通信研究院政策与经济研究所

参考文献：

[1]《数据安全法（草案）》总则第三条
[2] 郎为民等.大话物联网[M].人民邮电出版社，2020年4月，第265-267页。
[3]《数据安全法（草案）》总则第三条
[4] 上海赛博网络安全产业创新研究院、观安信息技术股份有限公司.人工智能数据安全治理报告[EB/OL]，第4-9页。
[5] 中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见[EB/OL].新华网，2020-04-09，网址：http://www.xinhuanet.com/politics/zywj/2020-04/09/c_1125834458.htm,引用时间：2020-07-27。
[6] 发展负责任的人工智能：新一代人工智能治理原则发布[EB/OL].中华人民共和国科技部，2019-06-17，网址：http://most.gov.cn/kjbgz/201906/t20190617_147107.htm,引用时间：2020-07-28。
[7]李媛.民法典为个人信息保护确立方向[EB/OL].中国社会科学网，网址： http://ex.cssn.cn/zx/bwyc/202007/t20200722_5158561.shtml,引用时间2020-07-28。
[8]《中华人民共和国网络安全法》第四十条
[9] 闵婉.《网络安全法》中的个人信息保护规则评析[J].法制博览，2018年01月（中），第69-70页。
[10] 袁泉.电子商务法视野下的个人信息保护[J].人民司法，2019第1期，第13-20页。
[11] 孟洁.《电子商务法》中的个人信息保护[EB/OL].中国监管市场新闻网，2018-11-26，网址：http://www.cicn.com.cn/zggsb/2018-11/26/cms112834article.shtml,引用时间:2020-07-29。
[12] 洪延青.美国快速通过CLOUD法案明确数据主权战略[J].中国信息安全，2018年第4期，第33-35页。
[13] 乔艺.“宜粗不宜细”立法的历史实践与法理反思[J].东南大学学报（哲学社会科学版），2019年6月第21卷，第83-87页。
[14] 丁道勤.基础数据与增值数据的二元划分[J].财经法学，2017年第2期。
[15] 京东法律研究院.欧盟数据宪章[M].法律出版社，2018年5月，第9-12页。