法商研究 Studies in Law and Business
Vol. 40 No. 5(2023)

语音数据法律风险防范的本土制度构建

韩 文*

摘 要:伴随着智能语音助手的广泛运用,语音数据的重要性开始逐步显现,必须在语音数据独特性的基础上重新认识“语音”这一特殊的数字资源。单纯地借鉴《欧盟一般数据保护条例》的统一立法模式或者是美国目前的领域立法模式,均无法适应我国的数据治理现状。语音数据自身的特殊性使得其有可能触发的风险与规制都需要予以特别关注。语音的交互性是人工智能发展的重要条件,语音数据的画像性使得其所包含的个人信息更为多元,而语言的使用又让语音数据展现出一定的地域性和族群性特征。在我国强调构建数据基础制度的大背景下,可以从法律规则和监管规则上进行创新,以市场自律的方式建立最佳实践准则,同时以中国标准指导具体路径的实施,守护好我国的数字主权。

关键词:语音数据 交互式人工智能 数据安全 隐私保护

关于语音数据的概念,目前国内外尚无标准定义。① 要定义语音数据,首先需要厘清“语音”的概念。语音,是指人类的发音器官发出的能表示一定意义的声音。② 语音与自然界其他声音的区别在于其所具有的物理属性、生理属性与社会属性。③ 由此可见,语音是属于人的能够表达一定意义的自然语言。笔者认为,语音数据是在收集和处理个人自然语言信息的过程中所产生的一种数据形式。囿于语音数据存在和运用的多样性,需要在具象化的场景之中研究其可能带来的风险。因此,本文所限定的研究范围主要针对以智能化设备为载体的语音助手所收集和处理的人类语音数据。

* 江西财经大学法学院讲师

基金项目:江西省教育厅高校人文社科重点基地项目(JD22023)

① 以《大数据百科全书》中描述的语音数据(Voice Data)为例,自然语言处理研究、机器学习和海量数据的融合,使得新的交互方式成为可能,在交互式语音应答系统被开发出来以后产生了大量的自然语言数据。See Laurie A. Schintler, Connie L. McNeely eds., Encyclopedia of Big Data, Springer Press, 2022, pp.946－947.

② 参见李行健主编:《现代汉语规范词典》,外语教育与研究出版社、语文出版社 2004 年版,第 1601 页。

③ 参见邵敬敏主编:《现代汉语通论》(上),上海教育出版社 2017 年第 3 版,第 8～10 页。

自2011年苹果公司的语音助手西瑞正式亮相开始，语音助手[①]在我们的生活中出现的频率越来越高，也是人工智能在实践运用中较为成熟的领域。根据英国市场研究机构朱尼普研究公司的报告，到2024年，消费者将在超过84亿台设备上与语音助手进行交互。[②] 中国用户对搭载智能语音助手的智能家居产品接受程度也越来越高，此类产品的产值也逐步扩大。然而，智能化的生活并非全然没有代价，由此所产生的庞大语音数据的治理问题及衍生风险正在酝酿。以亚马逊公司旗下的产品所搭载的语音助手亚历克萨为例，其一直以来因“窃听”用户隐私而饱受争议。2018年，美国俄勒冈州波特兰市的一个家庭称他们在家中的私人谈话被搭载了亚历克萨的智能音箱所录制，并将该录制的音频随机发送给了通讯录中的一个号码。亚马逊公司回复称语音助手之所以被唤醒是因为听到了一个类似“亚历克萨”的唤醒词。如果说该起事件只是不当收集语音数据并造成恶劣影响的特例，那么香农·卡彭特于2021年4月在美国提起的诉讼则更具普遍性。香农·卡彭特称自2019年麦当劳公司在其得来速餐厅引入了智能语音助手，通过提取客户的声纹生物特征来确定他们声音的独特特征。这些特征包括音高、音量和持续时间，以及从声纹中识别信息，如年龄、性别和国籍。借助语音助手可以识别独特的客户，无论他们访问哪里的麦当劳餐厅，都可以为他们提供量身定制的菜单选项，但语音助手收集顾客的声纹信息均未征得顾客同意。[③]

我国也面临着同样的问题，2020年9月，国家网络安全宣传周组委会和移动互联网应用程序（App）违法违规收集使用个人信息专项治理工作组共同发布的《App安全意识公众调查问卷报告》显示，在32万名受访者中，有近三分之一的人表示很反感手机应用程序的精准推送广告行为，感觉遭到了窥探或偷听。[④] 而这其中很可能也包括在未经告知的情况下私自对用户语音信息所进行的“收集”，人们对此类现象不满的本质是对隐私及语音数据安全问题的担忧，而语音数据带来的法律风险亟待正视。有鉴于此，笔者尝试以语音数据的法律风险防范作为研究目标，探讨构建语音数据法律风险防范本土制度的可能进路。

一、语音数据的特殊性及法律风险

语音数据的治理既要考虑到数据治理的共性，也须认识到语音数据相较于其他数据类型在交互性、画像性、地域性与族群性等方面所展现出的特殊之处。

---

① 语音助手往往也被称为智能语音助手，其是人工智能技术的典型代表，在美国麻省理工学院科技评论网站列举出的目前比较重要的人工智能技术包括人脸识别、机器学习、机器人和语音助手。本文所指的智能语音助手与虚拟语音助手等称谓所指代的范围相同。国际知名的智能语音助手有谷歌公司的谷歌助手，苹果公司的西瑞和亚马逊公司的亚历克萨以及微软公司的小娜。智能语音（尤其是智能语音交互系统）也是我国大力发展的人工智能标志性产品。

② See Number of Voice Assistant Devices in Use to Overtake World Population by 2024, Reaching 8.4BN, Led by Smartphones, Juniper Research, 28 April, 2020.

③ See Anna Bradley－Smith, McDonald's Should Face Voice Data Privacy Lawsuit, Class Action Plaintiff Argues, Top Class Actions, 2021.

④ 参见刘硕、余俊杰：《调查显示：近九成受访者对App申请手机权限持谨慎态度》，https://baijiahao.baidu.com/s?id=1678409132616235057&wfr=spider&for=pc，2021－10－24。

(一)语音数据的特殊性

1.语音数据的交互性。交互性是语言的重要属性之一,也是语言区别于其他生物信息的显著特征。因现有的人工智能产品大都建立在语言或语音交互的基础之上,在交互过程中将不可避免地分析和使用语音数据,故语音数据同样具有交互性。也正是这种交互性使得语音数据成为交互式人工智能和生成式人工智能的重要基础,可以创建数字助理、自动客户服务系统和其他基于语音的应用程序。多数人工智能产品都极度依赖语言的交互性以实现技术设想与产品功能,这便使得数据如同能源一般,一旦语音数据"断供",人工智能技术的发展便有可能驻足不前。交互性催生出了庞大的数据需求,也造就了语音数据被违规利用的现状。与此同时,语音数据不仅仅可以用于创建语音识别系统进行身份识别和语音分析,其交互性也成为一种沟通的纽带,天然适用于语音合成和其他基于音频的应用程序。

2.语音数据的画像性。"画像"是基于特定人信息而形成的关于此人的某一方面或整体的印象,[①]而"数字画像"是建立在大数据技术上自动生成的数据组合,可以支撑某种决策。[②]《欧盟一般数据保护条例》(以下简称《条例》)第 4 条第 4 款也有对"画像"定义。这里所说的"画像性"源自于"画像"但又与"画像"不尽相同,可以视为对个人工作状况、经济状况、家庭状况、健康状况、个人偏好、位置行踪等多元化内容的信息集成与分析。这是由语音数据的使用场景和使用频次所决定的,语音数据中携带的不仅有声纹这类生物识别信息,还有其他诸多信息,而许多敏感信息[③]也被囊括其中。以面部数据作为对比,我们可以通过面部数据识别获取到个人的面部生物信息,与此同时,该主体的地理位置信息也将被捕捉,而面部数据本身无法带来更多的其他信息(虽然也有研究声称可以通过面部数据来判断健康状况等)。语音数据的特殊之处则在于,收集的语音数据越多,能够被捕捉和分析的个人信息也就越多,所呈现的数字形象也就越立体、画像性也就越强。

3.语音数据的地域性与族群性。因语音自身的社会属性使其本就具备民族和地域特征,[④]故语音数据也往往具有极强的地域性与族群性特征,其蕴含的信息中既有个体信息也有族群信息。民族本就是以语言作为纽带,与此相类似的还有语言与地域的关系,同一地域的人口往往也使用相同或类似的语言,有着类似的口音。因此,语音数据的分析过程同时也是针对固定族群和地域进行习惯、偏好与群体状况分析的过程,尤其是当语音数据所展现出的数据量足够大、信息足够丰富之时,该族群或地域所可能具有的共性特征就越明显,而族群特征也正是重要数据的识别要素。从这一角度而言,语音数据不仅仅涉及生物识别信息,同样与信息安全密切相关,这绝不是同一地域喜欢购买某种商品的数据价值这么简单,针对特定语种与口音的监控技术也仰赖语音数据的这一特性。

---

① 参见刘文杰:《被遗忘权:传统元素、新语境与利益衡量》,《法学研究》2018 年第 2 期。

② 参见陆青:《数字时代的身份构建及其法律保障:以个人信息保护为中心的思考》,《法学研究》2021 年第 5 期。

③ 《中华人民共和国个人信息保护法》第 28 条第 1 款对敏感个人信息进行了列举式规定,其中包括了生物识别、医疗健康、金融账户、行踪轨迹等信息。有学者认为,可以从泄露该信息是否会导致重大伤害、泄露该信息给信息主体带来伤害的几率、大多数人对某类信息的敏感度等 3 个方面来确定敏感信息。参见胡文涛:《我国个人敏感信息界定之构想》,《中国法学》2018 年第 5 期。

④ 参见邵敬敏主编:《现代汉语通论》(上),上海教育出版社 2017 年第 3 版,第 9~10 页。

（二）语音数据运用过程中的法律风险

1.语音数据产生的安全风险。首先，语音数据具有的交互性天然地会成为人工智能技术的结合对象，而交互性也催生出了源源不断的数据需求。公司本应为保护这些数据采取相应的安全保障措施，但若连收集数据都是通过打“擦边球”行为获得，则更难顾及数据分析、监管、存储等方面的安全，同时当该语音数据要与第三方机构共享时，公司若未尽到网络安全调查义务则也将助长风险的滋生。其次，利用语音数据进行的深度模仿或伪造而从事的行为，有可能演化为更为严重的安全问题。例如，2019 年，一家总部位于英国的能源公司的首席执行官被人工智能模仿的声音诈骗了 22 万欧元，接听电话的时候他认为正在与他的老板（该公司德国母公司的首席执行官）通电话并且表示听出了老板声音中微妙的德国口音。① 此类电话骗局曾经在我国也频繁发生，没有人知道未来不法分子会不会利用语音数据与人工智能技术卷土重来。与此同时，亚马逊公司透露了一项实验性的亚历克萨功能，该功能允许人工智能助手模仿用户死去亲属的声音，在其展示的视频中，一个孩子要求亚历克萨用他已故祖母的声音朗读睡前故事。虽然亚马逊公司目前并没有明确该功能是否会公开，但不可否认，“音频深度伪造”已经得到越来越普遍的运用，②这一切都是基于语音数据的交互性。一旦语音数据被别有用心之人利用就可能制造出更为严重的风险。最后，语音数据的画像性也会带来不可预知的风险。例如，精准定位用户推送某些具有成瘾性的产品，甚至可能出现人工智能基于用户性格分析而诱导用户作出某项决策的情况，此类安全问题的出现是语音数据画像性特征与交互性特征相结合的产物。

2.语音数据带来的隐私风险。语音数据对个人隐私形成的重大挑战首先体现为语音数据的易获得性将加剧违规收集、传输和处理语音数据的风险。收集语音数据的渠道范围十分广泛，可能是你正在驾驶的汽车，也可能是你的手机或智能音箱，甚至是扫地机器人。人们虽然在某些特定场景（如酒店）无法接受摄像头的存在，但是往往能接受语音助手控制的智能家居。这些搭载了语音助手的智能化设备对语音的采集一旦被不当利用就将产生严重的隐私风险。同时，你打给外卖、银行和理财顾问公司的电话都有可能在悄悄记录你的语音数据并准确分析出打电话的是谁，你曾经的购买经历与喜好、是否有投资的意愿等信息也可能随着你打出的电话而被捕获。总之，你开口说话的次数越多，你被获取的隐私信息也就越多。其次，语音数据的画像性决定了其所包含信息的复杂程度可能引发更大的隐私风险。据比利时媒体报道，有证据表明，谷歌正在通过谷歌助手来监听用户的私人谈话，在泄露出来的由谷歌助手录制的一千多个录音片段中，可以清楚地听到地址及其他敏感信息，且其中有 153 段没有触发词的对话本不应该被记录。③ 语音数据的复杂之处在于其所包含信息的丰富程度根本无法掌控。显然，我们不可能通过指纹或人脸识别数据而获得用户的银行卡密码、商业秘密和家庭关系的现状。

最有价值的数据往往来自真实环境，这也正是众多科技公司明知游走于法律的边缘地带却不惜铤而走险的真正原因。但若权利本身的边界模糊，则难以通过确定权利和规定他人不得干

① See Catherine Stupp, Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case, Wall Street Journal, 30 August, 2019.

② See James Vincent , Amazon Shows off Alexa Feature that Mimics the Voices of Your Dead Relatives, The Verge , Jun 23, 2022.

③ See Tim Verheyden et al., Google Employees are Eavesdropping, Even in Your Living Room, VRT NWS , 10 July, 2019.

涉的绝对义务达到规范保护的效果。① 现实中也存在将用户对“收集数据的同意”混淆为对“放弃隐私的同意”,语音数据的特殊性使得对相关数据的分析在与获取用户隐私之间似乎只隔着一层“纸”,而现在要做的是如何筑起保护数字隐私权的“墙”。

3.语音数据带来的数字主权与国家安全风险。海量的语音数据将推动其背后的科技公司在全球扩张的步伐,应当警惕的是因某一地域或者族群所使用的语言的独特性而导致的针对特定地域或者族群的数据分析成为一种以“暗线”形式存在的特殊需求。从商业的角度来看,某一族群对某种商品的独特偏好以及某一地域对某类产品的特殊需求都会成为数据处理者眼中极具商业价值的数字资源,与语音数据相挂钩的除了地域与族群,还可能囊括其他敏感信息,如声纹、精神状况、生理健康等高风险信息。如此一来,语音数据这种特殊数据形式将原本不具备关联性的信息联系在一起,从这个角度来看,语音数据可能产生的风险将上升到数字主权与国家安全的层面。

信息的公共性唤起了保护的社会决定性。② 个人数据所产生的信息是数字时代最宝贵的资源,而通过分析特定群体的语音数据得到的信息如果被不当利用便会上升为国家数字主权层面的问题。针对个人信息的国家保护义务更是一个“综合不同法律技术与制度工具的系统过程”。③ 一旦针对某一地域或者族群的语音数据被有预谋地利用,这都将构成对语音数据的重大风险。笔者以为对语音数据的规制已刻不容缓,在其风险防范的规则设计上必须做到数据共性规制与语音数据特性治理两者兼备。

二、语音数据的规制现状与治理原则

(一)语音数据的规制现状

关于数据的法律规制,欧盟的统一立法和美国式的领域法都极具代表性,因此域外法的比较主要以欧盟和美国为参照样本。本文所论及的语音数据,其法律风险不仅涉及数据的收集、存储以及隐私泄露等问题,还涉及人工智能对语音数据的分析,故笔者主要是从数据、隐私与人工智能立法等方面对规制现状进行阐述。

1.欧盟的规制现状。欧洲数据保护委员会 2021 年 7 月发布的《虚拟语音助手指南 2.0》(以下简称《指南》)第 3.1 条指出,相关的法律框架首先是《条例》,因为个人数据的处理是语音助手的核心功能,《条例》第 4(14)条虽然未直接表述声音为个人数据,但是,其规定生物性识别数据属于个人数据。声音也日益受到各国监管机构的关注,如法国国家信息自由委员会就直接规定对声音的记录属于个人数据。除了《条例》外,《欧盟电子隐私指令》(以下简称《指令》)也为数据存储或访问用户终端设备存储设定了特定的标准,当语音助手访问这些终端设备时,《指令》第 5(3)条的规定都适用。针对问责,《指南》第 3.10 条规定,依据《条例》第 7.1 条和第 7.3 条的规定,数据控制者有义务证明其对数据的处理是基于数据主体的同意,且数据主体有权随时撤回其同

① 参见龙卫球:《〈个人信息保护法〉的基本法定位与保护功能——基于新法体系形成及其展开的分析》,《现代法学》2021 年第 5 期。

② 参见高富平:《个人信息保护:从个人控制到社会控制》,《法学研究》2018 年第 3 期。

③ 参见王锡锌:《个人信息国家保护义务及展开》,《中国法学》2021 年第 1 期。

意，而撤回同意应与表达同意一样简单。语音数据的保留义务将由具体立法的问责要求来决定。《指南》第3.11条指出，语音数据主体依据《条例》享有访问、更正、删除和可携带等权利。不论是在数据层面还是在人工智能监管层面，欧盟都表现出了极大的立法热情。2021年4月发布的《欧盟人工智能法草案》（以下简称《草案》）将风险具体划分为不可接受风险、高风险、有限风险以及最小风险。其中，“不可接受风险”被彻底禁止。《草案》第6～51条主要规制“高风险”的人工智能系统，敏感或重要领域的人工智能将受到严格的监管。这种分类规制的方法看似合理，其实仍然面临巨大的挑战，其中之一便是针对“不可接受风险”和“高风险”的规制在实践中可能会被有意规避，因为这需要强大的监管和执行系统予以衔接。在《草案》“附件3”中所列举的8类高风险人工智能系统包括了“自然人的生物识别和分类”。

2.美国的规制现状。在数据隐私立法方面，美国虽然也曾多次有联邦层面的立法努力，但是没有获得如《条例》般显著的成果，然不宜武断地认为美国在此方面立法落后。[①] 美国联邦层面的隐私立法主要集中于某些特定领域。[②] 在州立法层面，美国各州也表现出了极高的立法热情。具有代表意义的地方立法有2008年《伊利诺伊州生物识别信息隐私法》（以下简称《伊州生物识别信息隐私法》）、2018年《加利福尼亚州消费者隐私法》（以下简称《加州消费者隐私法》）及2020年《加利福尼亚州隐私权法》（以下简称《加州隐私权法》）。从保护的典型意义而言，《伊州生物识别信息隐私法》率先界定了生物识别标识符，包括视网膜、虹膜、指纹、声纹、手部及脸部扫描。虽然没有单独对语音进行规制，但是《伊州生物识别信息隐私法》对生物识别信息的保留、收集、披露、销毁都有规定，且明确上述信息在收集之前，应当告知用户并取得其同意。加利福尼亚州的数据和隐私立法一向走在全美国前列，《加州消费者隐私法》规定了几项关于数据的关键性权利。[③] 相较于《加州消费者隐私法》，《加州隐私权法》则提供了更为细致的规则。[④] 这些具有代表性的州立法其实都是在数据、隐私、生物识别信息等层面进行的规制，对语音并未有单独规定。但是，加利福尼亚州立法并未止步于此，其正拟立法禁止在初始设置或安装期间未显著通知联网电视指定用户的个人或实体在州内提供联网电视的语音识别功能操作，包括条款范围内的智能扬声器设备；禁止制造商通过操作语音识别功能收集或保留任何实际录音或转录。[⑤]

3.我国的规制现状。在立法安排上，除《中华人民共和国民法典》（以下简称《民法典》）关于

---

① 以《国家生物识别信息隐私法案》为例，该法案于2020年8月3日在美国国会会议上提出，但未获得投票。实际上，虽然美国国会两党都支持制定国家层面的隐私法，但是每年都有大量关于数据和隐私的立法未通过表决，同时也有大量的法案等待表决，如2021年提出的《数据隐私法案》《促进数字隐私技术法案》此前就处于立法第一阶段，而备受瞩目的《数据隐私和保护法案》已于2022年6月由美国国会参众两院发布，这也是全面的隐私法案首次将在美国国会众议院和参议院进行表决。

② 典型如《电子通信隐私法》《儿童在线隐私保护法》。此外美国在联邦层面针对一些特殊行业或领域的立法也会规制隐私，如《金融服务现代化法》《驾驶员隐私保护法》《健康保险可携性与责任法》《家庭教育权利和隐私法》《公平信用报告法》等。

③ 这些权利包括：消费者的知情权（向消费者披露公司的数据收集和共享做法）；消费者的删除权；消费者的选择退出权（个人信息在加利福尼亚州可以成为商品，但消费者有权选择不出售其个人信息）。

④ 例如，扩展了数据最小化和目的限制。同时，其扩展了消费者的隐私权利，修改了删除权、可移植权的规定，增加了数据保留期限的知情权、禁止报复的规定。See California Civil Code §1798.100(a)(3), 1798.100(c), 1798.105, 1798.125, 1798.130(a)(3).

⑤ See 2022 Consumer Privacy Legislation, National Conference of State Legislatures, April 12,2022.

个人信息的规定外,我国还颁布了《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)、《中华人民共和国网络安全法》(以下简称《网络安全法》)、《中华人民共和国数据安全法》(以下简称《数据安全法》),在立法层面对可能存在的侵犯个人信息和隐私的行为进行指导性规范。以此为基础,我国构建起了以《民法典》为中心、以 3 部单行法为主干、以其他规范为补充的完整个人信息和数据保护体系。信息与数据虽然不能混为一谈,但是从保护的角度而言,都具有保护实质信息内容和数据形式完整的双重任务,两者无法分割。① 因此,数据的本质是信息。② 在信息自决方面,首先是对生物识别信息属于个人信息的确认(《民法典》第 1034 条)。而声纹是生物识别信息,属于个人信息的范畴,③可用于个人的身份认证。④ 对个人信息尤其是敏感个人信息采取严格保护措施,并且对生物识别、医疗健康、行踪轨迹等个人敏感信息也进行了界定,只有在具备特殊目的和充分必要的情况下,方可收集和处理(《个人信息保护法》第 28 条)。⑤ 其次,对个人在个人信息和数据处理活动中的权利进行了明确规定,如知情权、决定权、查阅权、复制权、更正权、补充权、删除权、要求解释说明权等权利(《个人信息保护法》第 44～48 条)。在信息(数据)处理者义务方面,首先规定了需要取得个人同意以及其他可以处理个人信息的情形。其次明确了不同种类信息在个人同意下收集、告知、使用和处理等规则。也明确了信息安全,我国境内收集和产生的个人信息原则上存储在境内(《个人信息保护法》第 40 条、《网络安全法》第 37 条)。加强数据风险监测,注重数据风险评估,新技术或功能应当开展安全评估(《数据安全法》第 29～30 条)。⑥ 最后明确了相关的义务和责任(《个人信息保护法》第 66～67 条、第 69～71 条,《数据安全法》第 44～48 条、第 51～52 条,《网络安全法》第 64 条和第 66 条)。虽然我国的规制体系已经十分成熟,但是现有的规制路径依旧较为单一,目前采取的是与《条例》类似的统一立法模式,这与美国侧重于领域法的立法模式有较大差异,但美国务实的立法观念仍值得重视,不同领域与场景下的风险差异也将导致规制差异。⑦ 语音数据的特殊性以及智能语音助手的蓬勃发展势必也影响到此类领域立法。以语音数据的交互性为例,单纯的数据监管显然比较乏力,需要结合人工智能技术进行综合监管。而画像性也体现出语音数据所蕴含信息的广泛性,其中的敏感个人信息和一般信息也不宜适用“一刀切”的处理模式。

(二)重新认识“语音”作为数字资源的价值

个人是数字时代的消费者,同时也是数字资源的创造者。《民法典》第 1023 条第 2 款规定:“对自然人声音的保护,参照适用肖像权保护的有关规定。”如果我们在认识层面仅将语音作为一

① 参见梅夏英:《信息和数据概念区分的法律意义》,《比较法研究》2020 年第 6 期。

② 参见季卫东:《数据保护权的多维视角》,《政治与法律》2021 年第 10 期。

③ 参见 2020 年 3 月全国信息安全标准化技术委员会发布的《信息安全技术 个人信息安全规范》第 5.4 c 条;2021 年 1 月最高人民检察院发布的《人民检察院办理网络犯罪案件规定》第 62 条第 6 款。

④ 参见 2021 年 6 月中国支付清算协会发布的《移动金融基于声纹识别的安全应用评估规范》第 4.1 条。

⑤ 其他规范对此也有规定,如国家互联网信息办公室等 5 部委发布的 2021 年 10 月 1 日开始施行的《汽车数据安全管理若干规定(试行)》第 9 条第 2 款规定:“汽车数据处理者具有增强行车安全的目的和充分的必要性,方可收集指纹、声纹、人脸、心律等生物识别特征信息”。

⑥ 其他规范也对此有规定,如 2019 年 11 月国家互联网信息办公室、文化和旅游部、国家广播电视总局发布的《网络音视频信息服务管理规定》第 10 条。

⑦ 参见丁晓东:《〈个人信息保护法〉的比较法重思:中国道路与解释原理》,《华东政法大学学报》2022 年第 2 期。

种可识别的个人信息，而完全忽略其作为数字资源所蕴含的更高层次价值，那么这种认知是片面且遗憾的。语音作为数字资源的利用已经远远超出我们的想象。例如，苹果公司正在尝试利用人工智能技术通过其智能语音助手西瑞来检测和测量一个人声音中的不同特征（称之为声音生物标志物），从而可以深入了解他们的健康或精神状态，尽管这目前还仅仅只是一种技术假设。[①] 在亚马逊公司公开申请的专利中，也有专门基于语音确定用户的身体和情绪特征的方法，它的另一项专利则是一个可以帮助商店销售人员破译购物者声音以探测其对产品有无购买意识反应的应用程序。谷歌公司的一项专利发明则是使用放置在家中的特殊麦克风实时跟踪家庭成员，根据语音签名的音高推断性别和年龄信息。[②] 与此同时，在数字化医疗领域，当可穿戴设备搭载了亚历克萨时，如果用户出现了心搏骤停的情况，只需用语音呼唤亚历克萨，它就可以背诵有关心肺复苏术的救生指令，这是美国心脏协会教给它的一项技能。我们现在正处于语音数据分析革命的初期，越来越强大的数据分析能力会将对语音数据的运用推上一个新的台阶。不过，由此产生的结果却并非单纯有益，这同时也意味着某一族群的声纹、健康数据正在被监测，这类数字资源甚至相较于语音数据本身而言更具价值。可见，作为生物信息和数字资源的“语音”一旦失控，将会带来极大的安全隐患。

（三）秉持技术发展与信息安全并重的治理原则

监管可能“扼杀”创新的论点由来已久，也备受质疑，因为监管的传统目标是使市场需求与个人和社会的偏好和价值观更好地保持一致。良好的监管可以使需求组合更接近实际的个人和社会偏好，而不受监管的需求组合有可能以牺牲其他社会价值为代价来激励过多的创新活动。因此，将监管描述为扼杀创新是不合理的。[③] 首先，我们需要打破的是在技术发展与信息安全之间二选一的价值选择悖论。破解之道就在于坚持发展趋势并专注于解决那些可能存在的风险，同时建立激励相容的治理型规则。[④] 也需要明白，数据权益主体是多元的，以信息为内容的数据可能存在多方主体的多元利益诉求，[⑤]所谓信息主体、信息处理者与国家利益的三方平衡其实是在保证核心利益的前提下，将非核心利益让渡给其他主体的共赢策略。[⑥] 其次，要想同时实现科技发展与信息安全的目标，就必须谨慎平衡两者之间的关系。以智能语音助手为代表的人工智能技术，无时无刻都需要新的语音数据以改进其算法和服务，故在此层面，平衡必须是动态的。最后，必须秉持数据收集与利用的最小必要原则，这将贯穿语音数据收集、存储、利用、传输和销毁的各个阶段。具体表现为：未经用户许可不得擅自收集、非必要不创建用户声纹信息、未经用户特殊许可不得扫描敏感信息词汇、未经用户特殊许可不得披露数据用途和高风险使用数据、不得与第三方共享语音数据、未经用户特殊许可不得传输语音数据、限定语音数据存储的时限等。这也是在发展的大前提下兼顾安全的必然选择。

---

① See Laura Tucker, Siri Can Help You Diagnose Coronavirus COVID－19, Iottechtrends, 23 March, 2020.

② See Joseph Turow, They're Listening－Inside the Coming Voice－Profiling Revolution, The Conversation, 28 April, 2021.

③ See Yafit Lev－Aretz & Katherine J. Strandburg, Regulation and Innovation: Approaching Market Failure from Both Sides, 38 the Yale Journal on Regulation Bulletin, 6－21(2020).

④ 参见周汉华：《探索激励相容的个人数据治理之道》，《法学研究》2018年第2期。

⑤ 参见王利明：《迈进数字时代的民法》，《比较法研究》2022年第4期。

⑥ 参见张新宝：《论个人信息权益的构造》，《中外法学》2021年第5期。

三、语音数据法律风险防范本土制度的构建路径

数字社会既要有全球治理的协同框架,[①]也要构建属于自己的本土制度,也即“认知开放、规范封闭”。[②] 因此,语音数据法律风险的防范应以中国标准构建具体的实施路径。

(一)语音数据治理的本土规则设计

1.完善语音数据相关基础制度。个人数据权利包括数据收集、存储、转让和使用的整个过程。[③] 对语音数据的规制首先需要完善相关的数据基础制度。(1)推进数据确权。我国目前已明确将统筹推进数据产权、流通交易、收益分配、安全治理等数据基础制度体系的建设。在数据产权方面,数据资源持有权、数据加工使用权、数据产品经营权等权利运行机制都将得到明确。[④]借助数据整体规制体系以完善语音数据的相关规则可以解决大部分共性问题,而对语音数据的特性问题则可能需要借助行业标准、技术标准进行统筹规范。(2)解决敏感信息的存储问题。除建立起规范的语音数据本地存储制度外,对上传到云端的语音数据需要建立审查和监管制度。由于声纹属于生物识别信息的一种,建议由政府部门牵头利用市场化的方式设立相关数据存储基础设施,对涉及敏感信息的数据进行特别管制,并由专门机构统一管理。(3)建立语音数据分级管理制度,对公共数据、企业数据和个人数据进行分类分级管理。对不同行业的语音数据设立差异化的数据合规标准。语音数据因其使用目的、录制频率、信息含量等因素,探索分级管理的模式势在必行。目前,我国正在着手建立统一的国家数据分类分级保护规则。[⑤] 同时,针对不同数据在国家安全、公共利益、主体权利上的差异,在数据跨境流动中进行分类管理。[⑥] (4)构建全国性规范的数据交易平台,制定数据交易和监管规则。有学者主张,数据交易应以撮合交易、提供安全认证的机构为模型。[⑦] 在市场经济的原则下探索有偿使用制度,这不仅便于语音数据的利用与保护,也可以成为语音数据对数据可携带权的示范性探索。

2.细化语音数据中个人信息的收集与处理规则。对如何收集和分析语音数据,需要细化操作规则。全国信息安全标准化技术委员会发布的《信息安全技术 移动互联网应用程序(App)收集个人信息基本要求》(以下简称《要求》)第6.1条和第6.4条规定:收集的个人信息应限于实现处理目的所必要的最小范围,对敏感个人隐私信息的收集要取得单独同意;用户有权拒绝或撤回同意,且不应强制退出或者关闭应用程序。《要求》附录第C.8.c条和C.8.d条针对“录音及拍摄录像信息”也提出了要求。这是对信息收集规则的一次细化尝试,同时也为个人信息的后续处理

① 参见马长山:《数字社会的治理逻辑及其法治化展开》,《法律科学》(西北政法大学学报)2020年第5期。

② 许可:《数据权利:范式统合与规范分殊》,《政法论坛》2021年第4期。

③ 参见程啸:《论大数据时代的个人数据权利》,《中国社会科学》2018年第3期。

④ 参见《习近平主持召开中央全面深化改革委员会第二十六次会议强调 加快构建数据基础制度 加强和改进行政区划工作》,http://china.cnr.cn/news/sz/20220623/t20220623_525878858.shtml,2022-06-24。

⑤ 全国信息安全标准化技术委员会起草的《信息安全技术 网络数据分类分级要求》(征求意见稿)已向社会发布并征求意见。

⑥ 参见马其家、李晓楠:《论我国数据跨境流动监管规则的构建》,《法治研究》2021年第1期。

⑦ 参见丁晓东:《数据交易如何破局——数据要素市场中的阿罗信息悖论与法律应对》,《东方法学》2022年第2期。

提供了规范基础，下一步则可以对语音数据中的哪些信息可以分析、哪些信息允许储存、哪些信息可以传输、哪些信息可以共享和交易进行国家标准的探索和规范管理。

（二）构建语音数据应用的综合监管框架

语音数据的行业监管，应以智能语音助手为抓手建立行业监管框架，一方面构建协同监管体系，另一方面不断地对监管场景与监管措施作出尝试。

1.协同监管体系的建立。作为收集与分析语音数据的主要应用，智能语音助手的规范显然需要一个协同监管的体系。（1）健全中央和地方协同监管，在中央层面明确监管规则，具体监管措施由地方政府落实。（2）完善政府、企业、社会多方协同监管，监管不仅仅是政府的职责，想达成完善的监管体系，必须让参与者加入监管体系之中，形成良性的监管反馈。（3）强化分业监管和跨行业协同监管，一方面根据语音数据的特性分业监管是必然，而另一方面，不同行业之间的协同监管又能保证监管体系的严密性，如智能音箱和可穿戴设备分属不同行业，却在对语音数据和隐私保护的方面存在协同监管的需要。

2.风险区分与场景监管的介入。同样的行为会因场景和环境的不同而使风险程度有所区别。语音数据提供的信息是复杂的，全部按照敏感信息或者全部按照普通信息进行监管均不可行。需要根据具体场景作出不同的数据保护方案。[①] 对此，场景一致理论提供了一种规制可能，坚持该理论的学者认为……焦虑的根源既不是数据可控性也非保密性，而是其合理性。具体而言，影响我们感受的是技术、系统和实践中不合理的个人信息流动。该理论模型中有3个关键参数：信息类型、参与者和传输原则。这3个参数在很大程度上是根据各自的社会场景而变化的。[②] 以智能语音助手收集用户的语音数据为例，不同场景下应当施以不同的监管义务。信息类型不同，监管措施也不相同，涉及生物信息识别和敏感关键词提取的技术使用应当予以特别监管；语音数据是否会被共享给第三方，面临的监管义务也不一样；本地存储与上传云端涉及同意的场景不同，监管程度也应有所区别。因此，可以根据不同的场景进行类似“高风险”或“普通风险”的区分，实现监管力量的有效分布。

（三）以市场方式型塑语音数据的运行规范

1.最佳实践准则的提出。市场主体为了让自己的商业行为合规化，必然会在实践中探索一种市场和监管都能接受的行为准则。以饱受诟病的“窃听”问题（语音数据的收集）为例，亚马逊公司针对性地提供了“选择退出”功能，[③]同时针对隐私设置也在实践中形成了日趋严格的标准。[④] “选择退出”模式并不是针对个人数据保护最严格的方式，但其在互联网企业中运用较为

① 参见安柯颖：《个人数据安全的法律保护模式——从数据确权的视角切入》，《法学论坛》2021年第2期。

② See Helen Nissenbaum, Respecting Context to Protect Privacy: Why Meaning Matters ,24 Science and Engineering Ethics,834－843 (2018).

③ 在手机上进入亚历克萨应用程序，然后单击“设置”，转到亚历克萨账户和亚历克萨隐私，可以在“管理智能家居设备历史记录”中删除数据，也可以在“管理数据如何改善亚历克萨”中选择退出使用录音和消息。

④ 以搭载了智能语音助手亚历克萨的亚马逊智能音箱为例，现在可以自动删除用户的录音，在亚历克萨应用程序管理数据，打开“自动删除录音”开关；也可以删除整个录音历史记录；也可以让亚马逊公司员工远离用户的谈话和录音，只需选择关闭使用录音。亚马逊的Halo（一种搭载“音频分析”功能的智能健康手环）表示，其用户的声音不会上传到任何服务器，其通过蓝牙将音频片段发送到用户的手机并利用手机进行分析。这些涉及声音的敏感信息仅储存在本地，应用程序会在分析用户的情绪状态后立即删除语音样本。

普遍,因为与“选择同意”模式相较,其更有利于释放数据价值。笔者以为,真正兼顾数据价值释放与信息安全保护的规则是需要企业在实践过程中不断摸索从而构建出来的最佳实践准则。鼓励市场自发建立最佳实践准则,以企业合规竞争的方式擢选出最优解,再由行业协会或相关主管部门总结成最佳实践准则,鼓励各市场主体参照适用。我国要想建立属于自己的语音数据运用的最佳实践准则,就必须依靠本土企业进行自律探索。当然,此类准则必须符合我国相关的法律规定和监管要求。

2.语音数据治理最佳实践的尝试。虽然最佳实践应交由各厂商来设计并执行,但是基于实践中所产生的问题,需要注重如下规则的设计:(1)语音数据收集和传输的明显提示,以便用户能够更好地采取行动来控制自己的隐私。(2)敏感信息和高风险用途的额外同意,对声纹等敏感信息,收集和存储都将触发额外的监管义务,非必要情况下应避免。为了某些高风险目的收集和使用语音数据所需的同意级别更高,不能事先一揽子同意。(3)明确语音数据的共享规则,与第三方共享语音数据需要额外的通知与同意。(4)明确语音数据的存储期限,如果想利用录音来提高智能语音助手的性能,则平台有可能无限期保留语音数据,如此必须设立限定平台使用时限、禁止外包等规则。(5)应在技术上尽量禁止使用设备的远程转换,避免在未经用户同意的情况下智能语音助手被“擅自”打开并进行语音录制。(6)尽可能在终端设备上而非云存储上储存语音数据,人工智能在硬件和软件上都会迎来巨大的进步,当我们终端设备上的微处理器可以完成所需要的人工智能技术时,理论上就不需要将语音数据再发送到云端来处理。这种被称为“边缘人工智能”的技术在带来便利的同时也能更好地保护隐私。① 同时当语音数据存储在终端设备上时还应提供加密。(7)承诺不扫描数据中的某些关键字和术语。② (8)数据隐私协议应便于用户阅读和理解并不附加不合理条件。不应当在数据隐私协议中设计相关的“陷阱条款”,利用复杂的协议条文来掩盖获取用户隐私的关键条款。(9)隐私政策如果存在虚假或误导性陈述,应当承担相应的责任。(10)用户个人语音数据要便于携带和处理。③

上述列举内容尚无法涵盖语音数据治理最佳实践的所有方面,随着技术的发展和实践的进步,我们还会发现更多隐藏的问题,而最佳实践准则相较于立法程序更具灵活性,可以迅速地弥补规则“真空”,实现精准且有效地规制。

(四)以中国标准守卫数据安全和数字主权

数字主权如今已然成为一个更为包容的概念,不仅解决了互联网通信与连接的问题,而且解决了更广泛的社会数字化转型问题,其核心要素是国家的数据自治和数字安全。④ 有数据安全

---

① See Worried About Privacy at Home? There's an AI for That, Wired, 21 January, 2020.

② See Anne Pfeifle, Comment, Alexa, What Should We Do About Privacy? Protecting Privacy for Users of Voice— Activated Devices, 93 Washington Law Review, 453—455(2018).

③ 例如,有的智能语音助手虽然提供本地录音的删除服务,但当用户选择收听其中的一个录音之后,如果点击后退按钮则会再次回到列表的最顶端。以这种方式一个接一个地删除数百条恶意录音将会花费大量时间。当然也可以一次删除所有内容,包括合法的录音,但语音助手会警告说,这会让它工作得不太好。See Rachel Metz, Yes, Alexa is Recording Mundane Details of Your Life, and It's Creepy as Hell, MIT Technology Review, 2018.

④ 此处需要说明的一点是,笔者赞同任正非先生的观点。在谈及数字主权时,他认为,信息安全的最终解决要靠法律,而不完全靠技术,数据是受制于所在主权国家的法律管理,以遵守这个国家法律的方式来保证信息的安全可靠。参见《任正非与外国专家对谈“数字主权”》,https://world.huanqiu.com/article/9CaKrnKnEG9,2021—10—19。

才有数字主权。当然,这并非要严格限制数据的跨境传输,而是构建数据自由与安全流动的制度,提供审慎包容、鼓励合作的中国方案。[①] 为此,须采取如下应对措施。

1.建设好本土数字基础设施。数字基础设施的建设,以数据为例,寻求将数据的存储、移动和处理限制在特定区域和司法管辖区,并且限制司法管辖区外的机构可能对特定的工业或个人数据的访问。[②] 伴随着移动支付、云存储和第五代移动通信技术的快速发展,我国在数字基础设施方面的建设成果斐然,一大批国内企业成为全国乃至世界的领先企业,这或许是我们的优势。但是如何保持优势,加大力度建设好属于我国自己的数字基础设施,不至于在未来的竞争中处于劣势,是一个需要长期思考的问题。

2.数据本地化与跨境传输许可。数字主权的重要内容之一便是数据的境内保存。关键信息基础设施的运营者在运营过程中收集和产生的全部个人信息和重要数据都应当存储在境内,同时,在个人信息和重要数据的跨境传输上,如向境外提供,应当通过安全评估。有学者认为我国的规定过于严苛,因为这似乎广泛适用于存储在我国境内的所有数据,而不论其敏感性和主题。[③] 笔者认为,这一问题的关键并非存储和传输而是数据安全。以语音数据为例,很多智能语音助手的运营者都是跨国公司,一旦此类数据不经许可便以数据分析的名义进行跨境传输,其后果不堪设想。我国国家互联网信息办公室于2022年9月开始施行的《数据出境安全评估办法》从国家层面为数据出境安全评估设定了具体要求。基于语音数据的地域性和族群性特征,防范此类数据跨境安全的风险也即是在构筑国家安全和数字主权。

3.构建技术运用的自主标准。语音数据与人工智能技术的结合还带来了一个不容忽视的问题,那就是需要建立交互式人工智能与生成式人工智能等技术运用的本土标准。因此,有必要对高风险人工智能应用设定明确要求,对其提供者确定具体义务,在投放市场前进行评估,投放市场后进行监管。考虑到未来人工智能行业与国际接轨,各国都有动力确保自己的国家标准能够影响国际标准的制订。新兴的人工智能标准战略还应当在技术和制度两个层面展开进一步研究。首先,应该发展和制定技术标准,主要在人工智能安全过程标准和系统能力标准上发力。其次,应该制定具体战略。如何大规模实施安全人工智能的过程需要与技术安全研究并进,建立相应的协调与执行机构。[④] 从历史上看,欧美等一直主导着技术和数据标准的制定,随着全球新技术中心的兴起,我国也应在今后的标准制定中占据一席之地。随着我国在数字经济和信息技术领域的持续发力,标准制定的参与权重也自然会增加。

四、结　语

正如美国联邦最高法院大法官索尼娅·索托马约尔在“卡彭特诉美国联邦案”[⑤]中所评论

① 参见许可:《自由与安全:数据跨境流动的中国方案》,《环球法律评论》2021年第1期。

② See Julia Pohle, Thorsten Thiel, Digital Sovereignty ,9 Internet Policy Review, 8－10(2020).

③ See Yi Bao, New Chinese Data Privacy Laws Further Complicates SEC Investigations, Columbia Business Law Review Online, 2021.

④ See Peter Cihon, Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development, Technical Report of Future of Humanity Institute ,29－31(2019).

⑤ See Carpenter v. United States, 138 S. Ct. 2206 (2018).

的:许多人甚至把手机带到床上和公共厕所,“现在,对于有些人来说,这是附属器官”。伴随着种类越来越多的智能化终端设备的普及,这些所谓的“智能助手”也将成为我们朝夕相伴的“附属器官”,他们会“倾听”着我们每一次的交谈,记录着我们一点一滴的信息,这些信息“水滴”将勾勒出用户画像的支流,最终汇集为数据的汪洋大海,而其所获取的所有信息甚至都有你亲自授予的权限,这似乎更接近奥地利作家茨威格所描述的那种“暗中标好了价格”的“馈赠”。这一切如果没有相应的监管与规制,未来将演化成一场不可预知的可怕灾难。重新认识语音数据有助于我们理解数据自身的复杂性,同时也有利于我们认识数据与人工智能之间的密切关系,从智能语音助手的运用现状入手,对法律风险和规制路径进行建设性的探索,有助于构建语音数据法律风险防范的本土制度。

Abstract: Along with the widespread use of intelligent voice assistants, the importance of voice data has gradually emerged, and it is necessary to re-understand the special digital resource of “voice” on the basis of examining the uniqueness of voice data. It is obvious that the unified legislative model of the EU GDPR or the current legislative model in the US cannot be adapted to the current situation of data governance in China. The special characteristics of voice data make it possible to trigger risks and regulations that require special attention. The interactive nature of voice is an important condition for the development of AI, profiling voice data will enable them to obtain more personal information, and the use of language makes voice data show certain regional and ethnic characteristics. In the context of China's emphasis on building a data foundation system, it is important to innovate in terms of legal and regulatory rules, establish best practice guidelines by way of market self-regulation, and at the same time guide the implementation of all specific paths with the construction of Chinese standards to guard our digital sovereignty.

Key Words: voice data, interactive AI, data security, privacy protection

责任编辑 翟中鞠