中国应用软件中数据可携带权的实证分析

刘　春　奉其其　祝嘉悦

摘要：欧盟《通用数据保护条例》第 20 条引入了数据可携带权，规定数据主体有权以结构化、常用且机器可读的格式获取其提供给数据控制者的个人数据，并可以不受阻碍地将这些数据传输给其他数据控制者。我国《个人信息保护法》也引入了个人数据的可携带权。为探讨数据可携带权在中国的实施情况，本研究检视了中国市场上 405 款应用软件的隐私政策，向其中 95 款提及数据可携带权的应用软件发起了数据转移请求，并对数据处理流程及返回数据的质量进行评估。研究结果表明，企业的数据请求回复率总体较低，处理流程复杂，部门职能划分不明。本研究共收集到 40 份数据副本，这些数据主要以 txt、HTML/pdf 和 xls/xlsx 等格式呈现，未完全满足“结构化、常用且机器可读”的格式要求。在数据转移方面，企业成功完成转移数据的比例仅为 4.2%。本研究从流程优化与规范、数据安全与隐私保护以及数据转移成效与技术互操作性三个方面为各利益相关者提出了改进数据可携带权实践的建议。

关键词：数据可携带权　个人信息保护　数据隐私　数据转移

一、引　言

数据是数智时代推动经济和社会发展的核心驱动力。2018 年 5 月 25 日，欧盟正式实施《通用数据保护条例》（*General Data Protection Regulation*，GDPR），其中第 20 条引入了数据可携带权，即数据主体有权以结构化、常用且机器可读的格式获取其提供给数据控制者的个人数据，并可以不受阻碍地将这些数据传输至其他数据控制者。随后，美国的《消费者隐私法案》、印度的《个人数据保护法》、澳大利亚的《消费者数据权利法案》、韩国的《信用信息法》和新加坡的《个人数据保护法》等也

［作者简介］刘　春，电子科技大学公共管理学院教授、博士生导师，研究方向：数字信息管理与政策、农村信息化、数字鸿沟；
奉其其，电子科技大学公共管理学院博士研究生，研究方向：数字信息管理与政策；
祝嘉悦，电子科技大学公共管理学院硕士研究生，研究方向：数字鸿沟。
四川成都　611731

［收稿日期］2024-12-11
［基金项目］四川省哲学社会科学基金“中国式现代化引领四川高质量发展研究”重大专项课题（编号：SCJJ24ZD27）

相继对数据可携带权进行了规定。[①] 我国《个人信息保护法》于2021年11月1日正式实施，其中第45条第3款明确规定："个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。"该条款表明我国也引入了个人信息可携带权。

作为一项新兴的数字权利，数据可携带权的实施情况尚未得到全面的研究。特纳（Turner）等人在检视160家物联网供应商的隐私政策后指出，数据可携带权在物联网领域的实际应用仍面临诸多障碍。[②] 黄简妮斯（Janis. Wong）和亨德森（Henderson）等人对230个数据控制者进行了数据可携带性测试后发现，尽管74.8%的请求得到成功处理，但数据副本的格式没有全部符合GDPR的要求。[③] 西尔穆迪斯（Syrmoudis）等人分析了182款应用软件的数据导出与导入功能，指出严格的监管有助于推动数据可携带的实现。[④] 在我国，关于数据可携带权的研究还处于理论层面，涵盖了基本概念[⑤]、权利客体界定[⑥]、权利属性[⑦]及实践路径[⑧⑨]等议题。然而，从实践角度评估中国应用软件中数据可携带权实施情况的研究仍较为匮乏。本研究检视了405款应用软件的隐私政策，向其中95款提及数据可携带权的应用软件发起数据转移请求，对其回复情况及数据格式的合规性进行评估。本研究旨在揭示我国数据主体在行使数据可携带权过程中面临的挑战，为监管机构制定具体且有效的数据可携带权实施细则提供依据。

二、研究设计

（一）理论基础

数据可携带权的理论基础可以追溯到20世纪70年代德国法学家施泰姆勒（Steinmüller）在《个人信息保护法草案》中提出的个人信息自决理论。该理论指出，数据主体有权自主决定并合理利用与其自身相关的数据信息，而不应受到不必要的干扰或限制。由此，数据主体能够在法律允许的范围内，根据个人需求和合法目的，自主决定其个人数据在网络空间中的流动与传播，并选择数据传输的中介平台及第三方数据接收者。[⑩]

（二）研究流程

在研究流程上，本研究借鉴了平斯（Pins）等人[⑪]和特纳等人[⑫]的框架，结合中国市场的具体情况，设计了数据请求流程，详见图1。首先，研究人员审查各应用程序的隐私政策，筛选出支持数据可携带权的企业。其次，通过在这些应用程序中注册账户，并在研究期间正常使用这些软件，确保研

① P. De Hert, V. Papakonstantinou, G. Malgieri, et al., "The Right to Data Portability in the GDPR: Towards User-centric Interoperability of Digital Services," *Computer Law & Security Review*, Vol. 34, No. 2, 2018.

②⑫ S. Turner, J. Galindo Quintero, S. Turner, et al., "The Exercisability of the Right to Data Portability in the Emerging Internet of Things (IoT) Environment," *New Media & Society*, Vol. 23, No. 10, 2021.

③ J. Wong, T. Henderson, "The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR," *International Data Privacy Law*, Vol. 9, No. 3, 2019.

④ E. Syrmoudis, S. Mager, S. Kuebler-Wachendorff, et al., "Data Portability Between Online Services: An Empirical Analysis on the Effectiveness of GDPR Art. 20," *Proceedings on Privacy Enhancing Technologies*, No. 3, 2021.

⑤ 蔡培如：《个人信息可携带权的规范释义及制度建构》，《交大法学》2023年第2期。

⑥ 罗英：《个人信息可携带权在国家机关间的实现》，《政法论坛》2023年第6期。

⑦ 李婕：《个人信息可携带权的权利属性及实现路径》，《东北师大学报（哲学社会科学版）》2023年第1期。

⑧ 宋歌：《数据可携带权的解读与践行路径研究》，《大连理工大学学报（社会科学版）》2024年第2期。

⑨ 郑磊、侯铖铖：《信息传递、价值适配与降本协调：公共数据资源开发利用中的供需鸿沟研究》，《电子政务》2024年第10期。

⑩ 杨芳：《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》，《比较法研究》2015年第6期。

⑪ D. Pins, T. Jakobi, G. Stevens, et al., "Finding, Getting and Understanding: The User Journey for the GDPR's Right to Access," *Behaviour & Information Technology*, Vol. 41, No. 10, 2022.

究环境与用户的实际使用场景高度一致。最后，研究人员依据隐私政策中的联系方式（如电子邮件、电话、在线客服等）向这些企业提出个人数据转移请求。在请求回复阶段，本研究参照全国网络安全标准化技术委员会发布的《信息安全技术基于个人请求的个人信息转移要求（征求意见稿）》，将企业的回复时限设定为两轮（共 30 天）。若企业在规定期限内回复，流程进入身份验证阶段，研究人员将配合企业完成身份核验。待身份验证通过后，数据控制方对个人数据进行提取、整理和加密等处理。根据企业支持的不同数据转移模式（包括以数据接收方为中心、以数据主体为中心以及以第三方代理为中心的模式），数据主体将个人数据转移至目标企业。若数据成功转移至目标企业，视为数据转移成功，否则视为转移失败。

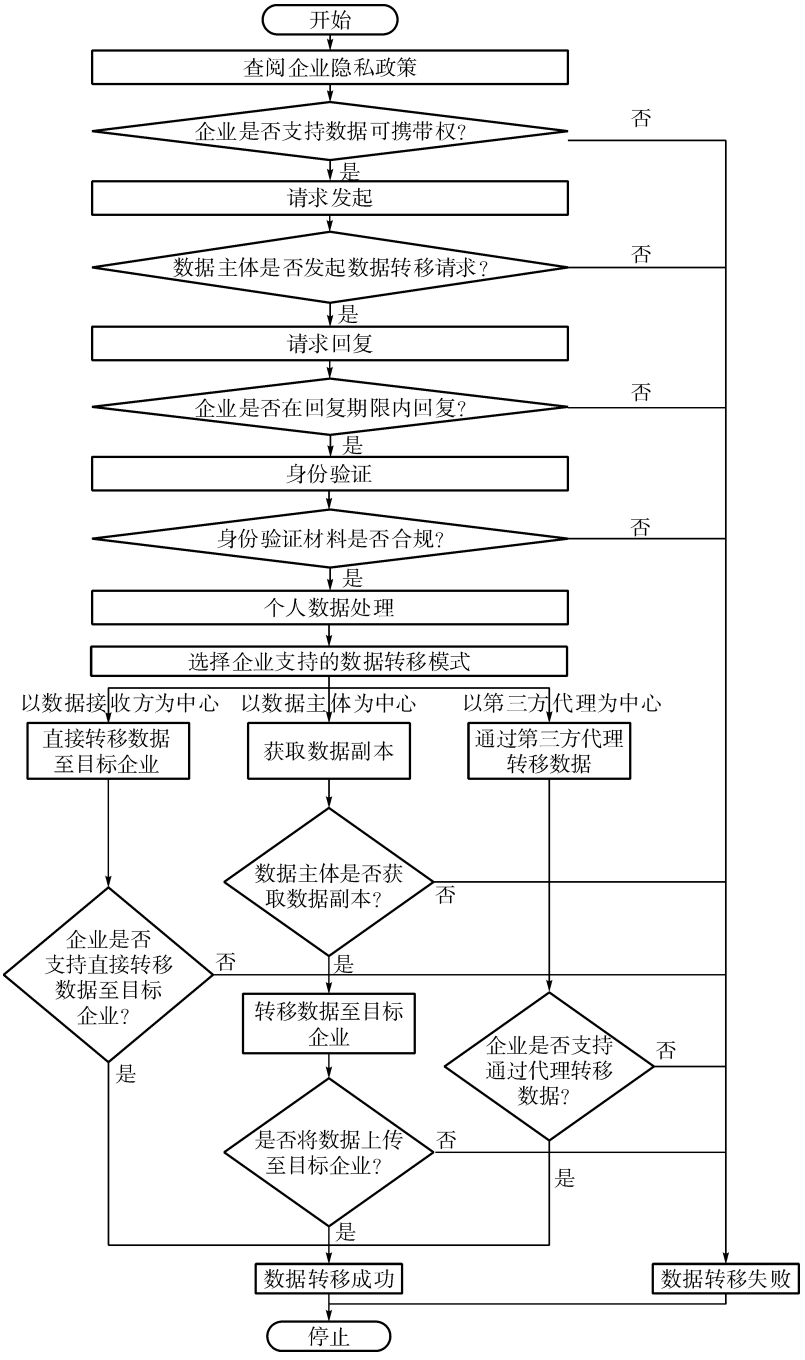

图 1　数据可携带权请求流程图

（三）数据来源与样本选择

本文的数据收集工作于2024年2月至5月期间进行，通过考察腾讯应用宝、华为应用市场及苹果应用商店（App Store）的应用软件排行榜，研究了涵盖购物、视频、社交、生活、工具、系统、理财、美食、汽车、阅读、音乐、游戏、教育、交通出行、摄影、办公、健康、母婴及旅游出行在内的19个大类及其下81个子类别的应用软件。为了确保样本的代表性，本研究综合考量了应用下载量、用户活跃度、中国互联网络信息中心与各大在线平台发布的年度总结报告中的相关数据，从每个子类别中挑选出综合排名前5位的应用程序作为研究对象。最终，总计405款应用软件被纳入本研究的样本范围。

本课题组对这405款应用软件的隐私政策进行了审读，评估其是否明确规定了与数据可携带权相关的条款。结果表明，只有95款应用软件在其隐私政策中清楚载明用户享有此项权利。基于此，本研究将这95款应用软件作为分析的样本。

三、研究结果

（一）请求发起

为了确保研究人员能够提出规范且正式的数据可携带权请求，本研究借鉴了鲍耶（Bowyer）等人[①]的方法，并参考了英国信息专员办公室（Information Commissioner's Office，ICO）提供的数据可携带权模板，进行了适当修改，形成了本研究的标准化电子邮件模板，见图2。为了对每封电子邮件进行个性化处理，该模板包括以下关键要素：（1）法律依据；（2）数据发送者与接收者信息；（3）请求的具体内容；（4）请求的目的；（5）所需数据的范围。在与企业沟通过程中，尽管本课题组未告知企业正在进行学术研究，但在每封邮件的末尾均披露了研究人员的真实姓名，以确保沟通的透明性。

尊敬的[工作人员名称]：

根据《中华人民共和国个人信息保护法》第45条第3款的规定，个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。贵单位在[隐私政策名称]中明确指出，[与数据可携带权相关的条款]。基于此，我正式提出如下请求：第一，请提供[数据发送者名称]所持有的与本人相关的所有数据；第二，请协助将上述数据转移至[数据接收者名称]。如贵单位能够提供此服务，请告知具体的数据转移途径；如无法提供，请明确说明具体原因；第三，[附加信息]。

我期待能在提出请求后的[回复期限]收到您的回复，感谢您的配合与支持。

此致

敬礼！

[姓名]

[日期]

图2　数据可携带权请求电子邮件模板

① A. Bowyer, J. Holt, J. Go Jefferies, et al., *Human-GDPR Interaction: Practical Experiences of Accessing Personal Data*, Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, 2022.

（二）请求回复

1. 回复方式

截至研究结束[①]，对于获取数据副本予以回复的企业共有 64 家，对于数据转移请求予以回复的企业共有 70 家。其中，对于获取数据副本的请求，44 家企业采取了纯人工回复，由客服团队或专人负责提供个性化服务；2 家企业采用了自动回复，通过预设算法或系统自动生成标准化的回复内容；18 家企业采用了人工回复与自动回复相结合的混合回复模式。对于数据转移请求，70 家企业均使用了人工回复。

2. 回复时效

在回复时效方面，尽管大多数企业在其隐私政策中声称将在 15 日内回复数据请求，但实际按时回应获取数据副本请求的企业仅有 38 家。而对于数据转移请求，按时回复的企业数量更为有限，仅有 28 家。Moon 月球、189 邮箱和翼支付 3 家企业，虽然设定了较短的回复时限，分别为 14 个工作日、7 个工作日和 72 小时，但仅有 189 邮箱按时回复了请求。

3. 回复部门

在隐私政策中，68 家企业表示已设立个人信息保护部门。然而，在实际处理数据请求时，只有 40 家企业明确指出了具体负责处理此类请求的部门。在这 40 家企业中，32 家企业将回复责任归属于客户服务部，4 家企业将回复责任分别归属于法律部、隐私部、安全与数据部以及信息安全部，而仅有 4 家企业将回复责任归属于个人信息保护部门。

4. 回复媒介

在响应数据请求时，53 家企业通过电子邮件回复数据主体，9 家企业通过电话联系，5 家企业使用在线客服。此外，3 家企业采用了多元化沟通渠道，同时使用电子邮件、电话和在线客服。也有应用软件在不同沟通渠道之间存在回复矛盾问题。具体而言，客服在电话中明确表示无法提供数据副本，但随后却通过邮件成功提供了个人数据副本。

（三）身份验证

在回应数据主体数据携带请求的 70 款应用软件中，32 款要求用户通过用户名和密码登录，另外 22 款支持使用手机验证码替代密码进行登录。其中，20 款应用软件在密码或手机验证码验证的基础上，进一步要求用户验证电子邮箱。对于涉及购物、汽车、交通出行和旅游出行类软件的企业，共有 16 款应用软件要求用户验证身份证号码或提供身份证照片。同时，2 款应用软件还要求用户提交个人中心页面的截图或手机号码的清晰录屏，以确保数据请求确实由本人发出。

（四）个人数据处理

1. 导出频率

在个人数据副本的导出服务中，38 款应用软件未对导出频率施加限制，其余 2 款应用软件则设定了相关限制。例如，曹操出行规定用户每日仅能申请一次导出，百度地图的个人数据副本链接仅支持导出一次。

2. 数据交付方式

在数据交付方式方面，34 家企业通过电子邮件发送下载链接或以附件形式直接交付数据，3 家企业则将数据内容直接嵌入邮件正文。3 款软件采取了不同的交付策略。例如，游拍将个人数据副本以

① 本文中出现的截至研究结束，指的是研究人员向企业提出数据转移申请，企业回复的限定时间为 30 天。下同。

图片形式存储至用户相册，麻豆约拍通过微信客服发送个人信息表格，腾讯地图仅允许用户在平台内复制数据，无法直接下载保存。

3. 接收数据副本的安全保障措施

为保障数据主体能安全接收数据副本，11 家企业为数据下载设定了时间限制，其中 8 家企业要求在 7 日内完成下载，2 家企业将下载时间限定在 72 小时内，而曹操出行将时限缩短至 30 分钟。此外，4 家企业要求用户输入正确的密码才能解压并查看数据内容；2 家企业采取了多重安全措施，如结合扫码验证、72 小时内下载限制及解压密码等。然而，23 家企业未采取安全保障措施，数据主体可直接查看数据。

（五）企业支持的数据转移模式

有 28 家企业在其隐私政策中表明能够提供数据转移服务，但未说明数据转移方式。

（六）获取个人数据副本

在获取个人数据副本的过程中，57 家企业提供了清晰的导航流程，例如通过应用软件内的详细步骤指引（如“我的”→“设置”→“隐私设置”→“个人信息导出”），引导用户获取数据。截至研究结束，本研究共成功收集了 40 份个人数据副本。对于能提供个人数据副本的 67 家企业，实际成功获取的副本数量为 33 份，其中 19 份由数据控制者主动发送，14 份由数据主体自行下载。此外，对于仅提供数据转移服务，而不提供数据副本的 28 家企业，经与其沟通后，8 家企业表示可以提供个人信息副本，最终成功获取了 7 份。其中，6 份由数据控制者发送，1 份由数据主体自行下载。详见表 1。

表 1　个人数据副本获取的成功情况

方式	具体情况	数量	小计	总计
数据控制者发送数据副本	数据控制者在隐私政策中表明能为数据主体提供数据副本，并按照规定为数据主体提供了数据副本。	19	25	40
	尽管隐私政策未表明能提供数据副本，但数据控制者主动为数据主体提供了数据副本。	6		
数据主体自行下载数据副本	隐私政策赋予数据主体自助下载权限，数据主体成功下载了数据副本。	14	15	
	尽管隐私政策未表明能提供数据副本，但数据控制者特别授权数据主体自助下载数据副本。	1		

对于未能成功获取的 34 份数据副本，11 份因数据主体与数据控制者沟通不畅导致失败，表现为企业未回复或未及时处理数据主体的请求，部分客服人员态度冷淡或缺乏合作意愿等；9 份请求因数据控制者的技术限制而被拒绝，包括数据控制者因技术原因无法提供数据副本，或请求范围超出了企业当前的处理能力，需进一步协商或调整；14 份由于数据主体自身条件的限制而未能完成，例如数据主体账户信息不完整，不满足获取数据副本的前提，或因提交请求时未提供完整的身份验证信息，请求处理暂停。详见表 2。

表 2　个人数据副本获取的失败情况

原因	具体情况	数量	小计	总计
数据控制者的技术限制	数据控制者因技术条件限制，无法提供获取数据副本的服务。	21	30	55
	数据主体请求的数据范围超出了应用软件的当前处理能力，需进一步协商或调整请求范围。	9		
数据主体与数据控制者沟通不畅	研究人员多次联系应用软件，软件均未回复数据主体的请求。	4	11	
	数据控制者因审核流程冗长，未能及时回应获取数据副本的请求。	2		
	数据控制者的邮箱拒绝接收邮件，导致邮件被退回。	2		
	用户发起的请求与应用软件回复的内容不匹配。	1		
	应用软件的不同客服人员对同一请求的回复内容不一致。	1		
	客服人员态度冷漠，缺乏合作意愿。	1		
数据主体自身条件的限制	数据主体账户信息不完整，不满足获取数据副本的前提。	8	14	
	数据主体未能提供完整的身份验证信息，导致请求处理暂停。	6		

1. 数据副本格式

在收集的 40 份个人数据副本中，文本格式（txt）最为常见，共计 16 份；其次为文件（HTML/pdf）格式，共计 8 份；其他还有表格格式（xls/xlsx）7 份，图片格式（jepg/img/png）3 份，字词格式（doc/docx）3 份，数据格式（xml）2 份，电子邮件（EML）格式 1 份。详见图 3。其中，2 款软件允许用户选择数据导出的格式。例如，迅雷支持用户选择 HTML 或 pdf 格式下载，爱彼迎提供 HTML、JSON 和 excel 三种下载选项。其余 38 家企业并未提供数据导出格式。

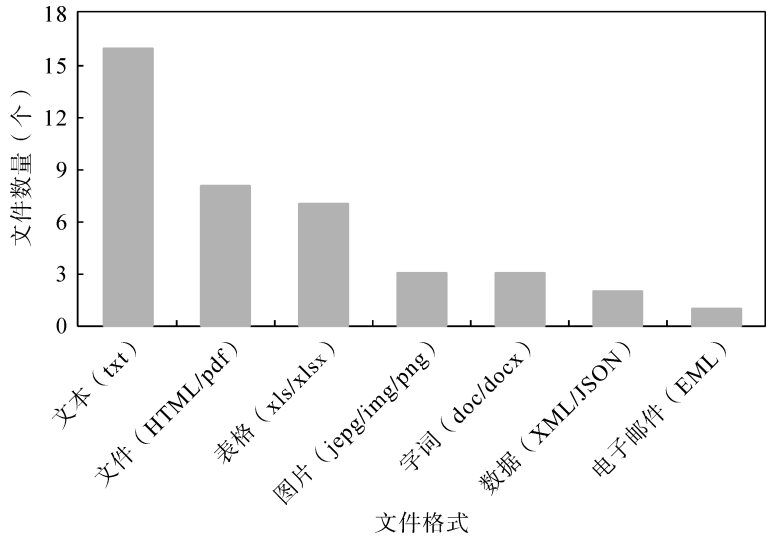

图 3　数据副本的文件格式分布

2. 数据类型

本研究将数据副本分为人类可读与机器可读两类①。结果显示，在收集的 40 份个人数据副本中，

① 人类可读类，指以易于理解的形式呈现的数据，通常采用标准化的文本格式，有助于非专业人员或数据分析人员能够直接访问并清晰理解数据内容；机器可读类，则指以结构化或标识化格式存储的数据，通常采用标准的机器语言格式，便于计算机程序进行自动化处理与分析。

38 家企业提供了直观且易于理解的人类可读数据副本，2 家企业提供了未经处理的机器可读数据副本。

3. 数据内容

个人数据副本主要包含以下四类信息：用户身份信息（如姓名、性别、生日、手机号码及身份证件等）、账户信息（如昵称、ID、邮箱、注册日期及头像等）、使用过程信息（如订单详情、发布内容及搜索历史等）以及设备信息（如 IP 地址、登录设备型号及客户端版本等）。

不同类别的应用软件在个人信息采集内容方面存在差异。视频、社交、购物类软件广泛收集用户的身份信息、账户信息和使用过程信息。交通出行和旅游出行类软件还侧重于采集用户的手机号码、地址、身份证件等信息，以及订单详情、居住地址和出行轨迹等动态数据。相比之下，系统、教育、母婴、汽车类软件提供的个人数据内容相对较少，而理财、美食和音乐类软件未提供相关数据。

（七）转移个人数据

在探讨转移个人数据的实践时，本研究向 95 家数据控制者发起了数据转移请求，但仅有 4 家企业（虎牙直播、中国国航、189 邮箱和爱彼迎）成功实现了数据转移，占比仅为 4.2%。值得注意的是，这些成功案例均依赖于数据主体在获取个人数据副本后主动将其上传到目标企业，目前尚未设立可协助数据主体完成数据转移的第三方代理机构，也缺乏将数据直接转移至第三方的有效渠道。具体见图 4。

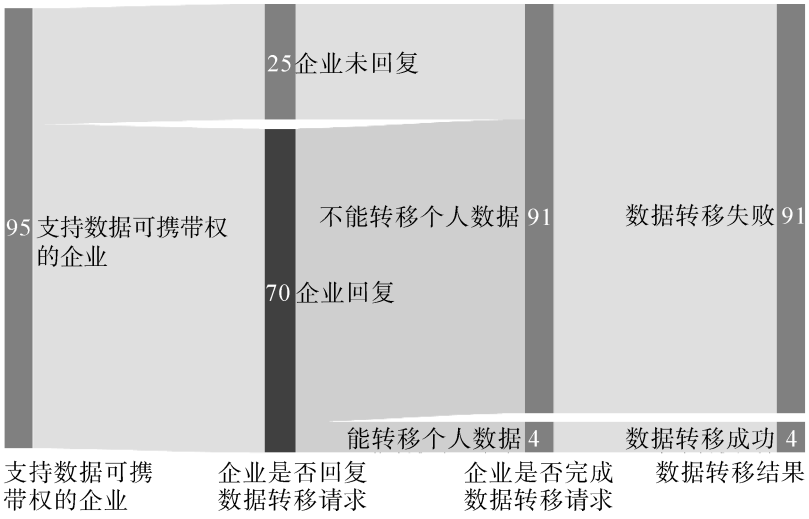

图 4　数据可携带权冲击图

在其余 91 家企业中，数据转移尝试均以失败告终，原因见表 3。失败的原因包括数据控制者在沟通过程中的障碍、技术方面的局限以及数据主体自身条件的限制。其中，25 家企业因沟通不畅导致请求失败。例如，研究人员多次提交请求，企业回复迟缓，数据主体因此面临长时间等待或不明确的信息。35 家企业因技术限制未能完成数据转移，包括发送方因技术条件不足无法提供转移服务，或接收方因技术能力不足无法导入数据。此外，一些企业和目标平台之间未建立合作关系或存在接口缺失，导致不同平台间的数据无法互通。另外，1 起数据转移请求因数据主体账户信息不完整而失败，研究人员未持有有效的企业账户，致使企业无法获取或转移个人数据。面对这些问题，多数应用软件提供的解决方案是建议用户在目标平台上直接注册新账户，而不是采用数据转移的方式。

表 3　个人数据转移的失败情况

原因	具体情况	数量	小计	总计
数据控制者的技术限制	数据发送者的技术条件不足，无法提供数据转移服务。	26	35	91
	数据发送者与数据接收者尚未建立合作关系，或缺乏接口导致不同平台的数据无法互通。	5		
	数据发送者能转出数据，但数据接收者的技术条件不足，数据无法导入。	4		
数据主体与数据控制者沟通不畅	研究人员多次提交请求，企业均未回复。	25	55	
	企业沟通渠道单一，部分企业仅提供在线客服，无法有效转至人工服务。	12		
	回复迟缓，数据主体面临长时间等待或信息不明确的情况。	8		
	部门间推诿责任，且回复内容不一致。	6		
	客服态度冷漠，或直接拒绝数据主体的请求。	1		
	企业只回复获取个人数据副本的内容，忽视数据转移的请求。	2		
	数据专员提供的操作指引与实际操作不符。	1		
数据主体自身条件的限制	研究人员未持有企业账户，企业无法转移个人数据。	1	1	

四、讨　论

随着部分国家在数据可携带权实践方面的发展以及我国《个人信息保护法》的正式颁布，我国的数据可携带权实践也在快速发展。为了方便数据主体行使该权利，未来的重点应聚焦以下三个方面。

（一）流程优化与规范

目前，我国在数据可携带权的操作流程中仍存在规范性不足的问题。为提高操作效率，需制定覆盖全流程的标准化操作规范，涵盖数据请求的发起、回复、身份验证、数据处理、数据副本的获取和转移等环节。

第一，数据请求的发起方式存在多样性，缺乏统一的操作标准。研究表明，许多企业尚未提供在线申请渠道，导致数据请求在内容和形式上存在不确定性。为此，建议数据控制者提供标准化的申请模板，以降低数据主体提交请求的难度。例如，使用个人信息数据查看、编辑、修改平台（如 Privacy Inzage Machine、Access My Info 等）工具[①]，以及本研究借鉴的标准化电子邮件模板，能够帮助用户生成规范的请求信。此外，企业还可以在其应用软件中设计直观且容易使用的交互功能，例如“一键申请数据携带权”按钮，从而简化用户发起数据请求的流程。

第二，数据请求回复流程中的时效性、回复部门和回复媒介仍需引起重视。欧洲数据保护委员会发布的《数据可携带权指南》为企业设定了相对宽松的回复期限，通常要求在一个月内完成处理，对于复杂情况则可延长至三个月。因此，建议我国涉及数据可携带权的平台和应用软件借鉴这一规定，合理设定回复期限，为响应请求提供充裕的缓冲时间。此外，数据请求处理经常面临部门职责不明确的困境。尽管企业普遍声称已设立专门负责个人信息的部门，但在实际操作中，大部分数据可携

① A. Galetta, P. De Hert, *A European Perspective on Data Protection and the Right of Access*, The Unaccountable State of Surveillance: Exercising Access Rights in Europe, Springer International Publishing, 2017, pp. 21-43.

带请求并未分配到隐私或法律部门，而是交由客户服务部门处理。马休（Mahieu）等人[①]的研究也证实了这一现象，客户服务部门回复率最高，而隐私部门和法律部门的参与度较低。为此，企业应加强部门间的协作，提升回复的专业性。同时，在企业与数据主体的沟通中，方式较为单一，电子邮件是常用的回复数据请求的方式之一。[②] 奥斯卢斯（Ausloos）和德维特（Dewitte）[③]、黄简妮斯[④]等的研究也发现，绝大多数请求依赖电子邮件作为沟通渠道，用户体验欠佳。因此，建议企业采用多元化的沟通渠道，如电子邮件、电话、在线客服等，以优化沟通方式，提高沟通效率。

在数据处理环节，应针对数据导出频率和交付方式等关键节点做出明确的规定。例如，《加州消费者隐私法案》（*California Consumer Privacy Act*，CCPA）规定，消费者在 12 个月内最多可向数据控制者申请两次个人信息导出。尽管这一要求在一定程度上限制了数据获取的便捷性，但它可以避免数据主体频繁请求而增加企业运营负担。企业在选择数据交付方式时，不仅应考虑数据的可访问性，还应考虑数据主体是否能够管理和处理这些数据。一些企业将个人数据直接嵌入邮件正文，导出不便，以图片形式传递个人数据会带来格式转换的困难，降低数据的可读性和可编辑性。

在获取和转移数据副本的过程中，有必要制定统一标准，以规范个人数据副本的格式、类型和内容。克兰兹（Kranz）等人提出了五种直接数据可移植性技术架构，包括手动导出与导入、开放授权与应用程序编程接口、数据可移植性平台、开放协议与服务网关、自托管及个人数据存储，这些架构为制定统一标准提供了重要参考。[⑤]

（二）数据安全与隐私保护

在数据可携带权的实践中，安全与隐私保护具有重要地位。首先，在身份验证环节，为防止冒名顶替者或黑客通过虚假身份窃取数据，数据控制者应实施多重身份验证，如密码、生物识别、动态验证码和安全令牌等，以预防身份盗窃行为。平斯等人的研究探讨了当前身份验证方法的多样性，指出数字验证手段如用户登录和短信验证，在实际应用中的广泛使用。[⑥] 而斯怀尔（Swire）和拉戈斯（Lagos）强调，若身份验证的流程过于复杂，可能引发“可见性悖论”，即数据主体在行使权利时，可能被迫披露更多个人信息，反而增加了隐私泄露的风险，并引发用户抵触的情绪。[⑦] 因此，企业在设计身份验证机制时，应遵循最小必要原则，要求数据主体提供合理且适当的验证材料，以确保验证过程既高效又安全。

其次，在数据交付过程中，为保障数据主体能够安全接收数据副本，数据控制者采取了多样化的安全措施，包括设定下载时限、扫码验证、软件授权及设置文件下载密码等。设定下载时限有助于减

① R. L. P. Mahieu, H. Asghari, M. van Eeten, “Collectively Exercising the Right of Access: Individual Effort, Societal Effect,” *Internet Policy Review*, Vol. 7, No. 3, 2018.

② J. Gantner, L. Demetz, R. Maier, “All You Need is Trust: An Analysis of Trust Measures Communicated by Cloud Providers,” *On the Move to Meaningful Internet Systems: OTM* 2015 *Conferences*, *Springer International Publishing*, 2015, pp. 557-574.

③ J. Ausloos, P. Dewitte, “Shattering One-way Mirrors: Data Subject Access Rights in Practice,” *International Data Privacy Law*, Vol. 8, No. 1, 2018.

④ J. Wong, T. Henderson, “The Right to Data Portability in Practice: Exploring the Implications of the Technologically Neutral GDPR,” *International Data Privacy Law*, Vol. 9, No. 3, 2019.

⑤ J. Kranz, S. Kuebler-Wachendorff, E. Syrmoudis, et al., “Data Portability,” *Business & Information Systems Engineering*, Vol. 65, No. 5, 2023.

⑥ D. Pins, T. Jakobi, G. Stevens, et al., “Finding, Getting and Understanding: The User Journey for the GDPR′s Right to Access,” *Behaviour & Information Technology*, Vol. 41, No. 10, 2022.

⑦ P. Swire, Y. Lagos, “Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique,” *Computer Law & Security Review*, Vol. 72, No. 2, 2013.

少文件长时间暴露的风险，但过短的时限将会给用户造成不便。扫码验证、软件授权和下载密码增加了数据接收方身份验证的复杂性，从而降低了未经授权访问的可能性。此外，利用同态加密、安全多方计算、匿名化和数据脱敏等隐私保护技术，并加大对边缘计算和差分隐私等新兴技术的投资，可以进一步强化隐私保护力度。

最后，为了确保数据传输阶段的安全，避免数据在不同平台之间传输时遭受中间人攻击、拦截或篡改，可以采用 TLS/SSL 等标准加密协议，使用 RSA 和 AES-256 等加密算法，并引入区块链、可验证凭证、分散式标识符等数据保护技术，帮助企业构建去中心化的身份系统①，从而减少数据伪造和市场失灵的风险。

（三）数据转移成效与技术互操作性

第一，在数据格式多样化方面，根据《通用数据保护条例》，数据控制者应以“结构化、常用和机器可读的格式”提供数据。然而，在实际操作中实现这种数据格式往往困难重重。例如，尽管文本（txt）格式简单直观，但难以满足复杂大数据分析的需求。文件（HTML/pdf）和表格（xls/xlsx）格式虽在一定程度上兼顾了数据的可读性与结构化需求，但在大规模自动化数据处理中存在局限性。为应对上述问题，企业应同时提供人类可读的信息摘要与机器可读的数据文件，便于数据主体能在常见操作系统（如 Linux、MacOS 和 Windows）上查看。此外，考虑到目前仅少数企业支持数据格式的选择，企业应积极研发和采用能够支持多种数据格式转换的技术工具，如 Apache NiFi、Pentaho Data Integration 或 Talend 等，以克服数据格式差异带来的重用障碍，推动数据的无障碍流通与高效利用。

第二，企业提供的数据副本中包含的内容太少，本研究中大部分企业仅提供用户身份信息、账户信息和设备信息等用户主动提交的直接数据，仅有一小部分企业提供通过观察用户的行为痕迹获得的观测数据。所有企业均未提供基于直接数据和观测数据通过算法生成的衍生数据。国外研究也有类似情况，西尔穆迪斯等人对 182 个应用软件的数据导出实践进行研究，发现 36%的应用软件只提供直接数据，55%的应用软件包括观测数据，9%的应用软件还涵盖衍生数据。② 鲍耶（Bowyer）等人指出，企业可以将直接数据和部分观测数据纳入可携带数据的范畴，同时对衍生数据赋予有限的携带权。③在不侵犯第三方合法权益的前提下，数据可携带权可以涵盖涉及第三方的数据（如电话、合照、聊天记录等），并建议企业提供获取第三方同意将其数据进行传输的渠道。对于公共部门收集和存储的个人数据，只要不涉及国家安全、公共利益及第三方权益，应允许数据主体获取并转移这些数据，以打破政府部门间的数据壁垒。

第三，在数据跨平台转移层面，尽管 GDPR 提出了“无障碍”和“技术可行”的要求，但在实践中，企业间的数据互操作性仍然有较大提升空间。具体表现为：企业均不支持以数据接收方为中心或以第三方代理为中心的方式，只能依赖于数据主体自行转移，即数据主体在获取个人数据副本后，主动将其上传至目标企业。为此，企业应升级其数据管理系统，解决数据格式标准化、接口兼容性及系统适配等核心问题，确保数据在不同系统间的顺畅迁移。④ 麦考恩（McCown）和纳尔逊（Nelson）提出的开放 API、浏览器扩展和归档框架以及第三方 Web 归档程序等机制，可以为有效提取个人数

① F. Banterle，“Data Ownership in the Data Economy：A European Dilemma，”*EU Internet Law in the Digital Era：Regulation and Enforcement*，Springer International Publishing，2020，pp. 199-225.

② E. Syrmoudis，S. Mager，S. Kuebler-Wachendorff，et al.，“Data Portability Between Online Services：An Empirical Analysis on the Effectiveness of GDPR Art. 20，”*Proceedings on Privacy Enhancing Technologies*，No. 3，2021.

③ A. Bowyer，J. Holt，J. Go Jefferies，et al.，“Human-GDPR Interaction：Practical Experiences of Accessing Personal Data，”*Proceedings of the* 2022 *CHI Conference on Human Factors in Computing Systems*，2022.

④ 姜宇：《数据要素市场化的一种方案：基于数据信托的数据交易所机制重构》，《电子政务》2023 年第 7 期。

据提供借鉴。[①] 佩特库（Petcu）等人强调了 REST API 函数与库的应用，能够支持跨设备、跨应用的个人数据读写，实现更广泛的互联互通。[②] 企业应积极采纳这些方案，并借鉴苹果（Apple）、谷歌（Google）等科技巨头的成功经验，通过参与数据传输项目（DTP），推动数据在不同系统中的自由流通，进而解决数字市场成熟度不足、数据控制者技术能力差异及验证流程复杂等难题。此外，随着数据可携带权的落地，未来相关企业将面临海量的数据导出和传输需求，企业应提前优化服务器及基础设施，以应对数据迁移过程中可能产生的网络负载及可靠性挑战。

五、结　论

本研究旨在探讨我国应用软件中数据可携带权的实践现状，通过向 95 款支持数据可携带权的应用软件发起数据转移请求，对数据处理流程和返回数据的质量进行评估。研究结果表明，企业的数据请求回复率总体较低，处理流程复杂，部门职能划分不明。本研究共收集到 40 份数据副本，这些数据主要以 txt、HTML/pdf 和 xls/xlsx 等格式呈现，未完全满足“结构化、常用且机器可读”的格式要求。在数据转移方面，企业成功完成转移数据的比例仅为 4.2%，尚未设立可协助数据主体完成数据转移的第三方代理机构，也缺乏将数据直接转移至第三方的有效渠道，而是依赖于数据主体在获取数据副本后手动上传。为此，本研究从流程优化与规范、数据安全与隐私保护以及数据转移成效与技术互操作性三个层面提出了改善数据可携带权实践的建议。

本研究仍然存在一定的局限性。首先，尽管本研究覆盖了中国市场上广受欢迎的应用程序，但由于研究范围仅限于每个类别中综合排名前五位的热门软件，许多潜在的数据控制者未被纳入。后续的研究应致力于拓宽样本的边界，增强评估的广泛性。其次，本研究的时间跨度仅限于 30 天，对于长期趋势的捕捉尚显不足，未来研究应探索更长时间维度下的动态变化，以验证结果的稳定性。最后，关于数据携带对用户行为的具体影响，尤其是用户在行使数据携带权及提出相关请求过程中的主观体验与感受，尚需深入探究。

（责任编辑：武素迁）

① F. McCown, M. L. Nelson, “What Happens when Facebook Is Gone?” *Proceedings of the 9th ACM/IEEE-CS Joint Conference on Digital Libraries*, 2009.

② D. Petcu, A. V. Vasilakos, “Portability in Clouds: Approaches and Research Opportunities,” *Scalable Computing: Practice and Experience*, Vol. 15, No. 3, 2014.