个人信息可携带权的实现路径研究

陈俊龙

山东科技大学　山东青岛

【摘要】我国《个人信息保护法》以赋权的方式确定了公民的个人信息可携带权，但因存在客体模糊、路径缺失、技术障碍等问题，导致权利难以落地。在属性层面，可携带权是一种“数据主导权”，旨在将个人信息的控制权从平台转移至用户，兼具人格权与财产权双重属性，并体现为公法对私法不足的必要补充。客体方面，以“包容化”思路重塑客体范围：除非平台能证明转移侵害其商业秘密或正当利益，否则用户账号内全部数据均应允许携转，单账户数据不构成商业秘密。在实现路径上，通过区块链技术的应用，既能解决个人信息转移过程中的安全问题，又能降低转移成本。

【关键词】个人信息可携带权；个人信息保护；数据主导权；区块链

【收稿日期】2026 年 1 月 4 日　　【出刊日期】2026 年 2 月 5 日　　【DOI】10.12208/j.ssr.20260051

Research on the realization path of the right to carry personal information

Junlong Chen

Shandong University of Science and Technology, Qingdao, Shandong

【**Abstract**】China's Personal Information Protection Law has determined citizens' right to carry their personal information through empowerment. However, due to issues such as ambiguous objects, missing paths, and technical obstacles, this right is difficult to be implemented. At the attribute level, the right of portability is a kind of "data dominance right", aiming to transfer the control of personal information from the platform to the user. It has dual attributes of personality rights and property rights and is reflected as a necessary supplement to the insufficiency of private law by public law. In terms of the object, the scope of the object should be reshaped with an "inclusive" approach: Unless the platform can prove that the transfer infringes upon its trade secrets or legitimate interests, all data within the user account should be allowed to be transferred, and the data of a single account does not constitute a trade secret. In terms of implementation, through the application of blockchain technology, not only can the security issues during the transfer of personal information be resolved, but also the transfer costs can be reduced.

【**Keywords**】Right to portability of personal information; Personal information protection; Data dominance; Blockchain

21 世纪以来，随着互联网时代的到来与大数据算法的兴起，数据已经成为与土地、劳动力、资本、技术并驾齐驱的第五大生产要素。数据对于各大网络平台的重要性不言而喻，甚至成为平台在与对手竞争中占据优势的根本原因，成为其最重要的生产力。个人信息作为数据的重要组成部分，兼具了两大属性，一方面作为普通数据的财产属性，可以为平台提供利益，例如某购物平台可以凭借其收集的用户购物偏好，通过算法向用户推荐个性化商品或服务以获取更多利益。而另一方面个人信息数据拥有比普通数据更为敏感的隐私属性，个人信息一旦不正当竞争中大量使用泄露将造成极大的危害性。

1 问题的提出

我国制定的法律中有多项关于个人信息保护的内容，其中首部专门针对个人信息保护的法律《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》）2021 年颁布实施。然而，与欧盟、美国、日本等国家和地区相比，我国在个人信息保护的理念、立法和实践经验等许多方面仍存在许多不足，在个人信息方面保护稍显落后。《个人信息保护法》第 45 条确立了个人信息的可携带权，“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。”这一规定使得个人信息保护从间接保护转向直接保护，并因此引发了学界广泛的理论研究。

然而，《个人信息保护法》第 45 条关于个人信息可携带权（以下简称“个人信息可携权”）的规定过于笼统。并且由于个人信息可携权这一权利在《个人信息保护法》草案第三次审议时才正式通过确立。由此可见，学界各方对此权利的争议极大。由于客体对象的模糊与行使权利路径的不确定使得该权利难以实现落地，本文将在讨论权利的属性和客体的基础上，从权利客体与个人信息转移路径为重点探析权利实现方式。

2 个人信息可携带权属性探析

个人信息可携权理论源自于“个人信息自决权”理论，该理论从私法的角度认为，个人数据作为人的虚拟数据空间的延伸，其在人权和自由涵摄范围之内，基于对人权和自由的保护，人应当自主掌握个人的信息[1]。信息权利则源自于宪法，我国《宪法》第三十三规定“国家尊重和保障人权”以及第三十八条规定“中华人民共和国公民的人格尊严不受侵犯”。在宪法的指导下，《民法典》关于个人信息保护的表述为第一百一十一条“个人信息受法律保护”，但并未将其确定为一项具体权利，因此有越来越多学者指出这一保护模式的不足，“个人信息的此种保护模式，必然使得个人信息保护在规范逻辑、制度功能等方面受到局限”。[2]由此来看，有必要将个人信息保护其扩展到公法领域，“个人信息保护是信息时代的一项全新挑战，个人信息控制权是通过个人信息保护法确立的一项新型公法权利”。[3]据此观点，个人信息可携权是私法上关于信息保护的难以被具体为权利的权益在公法上的扩展保护，这种保护以权利的具体化为核心，以宪法的法律规定为支撑。

对于数据产权的立法，立法者们一直处于一种“进退维谷”的境地。一方面，由于数据自身的主体多维性（即难以判断一段具体的数据的真正主体）和数据产生及管理过程中的复杂性使得数据产权难以用传统民法中物权的概念加以规制。另一方面，如果立法者们退一步，将个人信息保护仅局限于《民法典》 之“个人信息受法律保护”的表述范畴，则无法实现破除海量数据对个人的反向控制。换言之，面对庞大的个人数据几乎在网络虚拟空间形成了一个另外的自我的情况下，现实空间的自我应当取得对虚拟空间自我的控制权。对于数据这一并不以实物为表现形式的物质，谁控制的主导权，便在事实上控制了其所有权。其控制权要么在用户，要么在数据平台。在这一方面上来讲，个人信息可携权的本质便是在于将个人信息的控制权由数据平台企业转移至用户，使用户取得类似于“数据物权”的一种数据主导权。

3 个人信息可携权的客体界定

《个人信息保护法》并未对个人信息可携权的客体做出清晰规定，各个国家和地区法律对其客体的规定也不尽相同，造成了客体范围的模糊性。对于个人信息记录的形式表达较为宽泛，电子或者其他方式中的其他方式是否包括纸质记录，应当做限缩处理，即个人信息可携带权的范围并不包括以纸质介质记录的个人信息。这是因为首先转移纸质信息并不具有现实可操作性，其次纸质信息难以对个人信息造成实质侵害，无论是从人格权角度抑或是财产属性角度并没有对其保护的必要。

学界认为，存在于数据处理者的个人信息主要包括三种，一是直接数据，即用户直接上传的数据信息，包括用户资料、昵称、家庭住址等。二是观测数据，即用户在平台上活动所留下的数据痕迹，如浏览记录、收藏的视频歌单等。三是预测数据，即数据平台通过算法，基于以上两种数据加工形成的用户偏好，形成用户画像。通常此类数据是平台的核心数据。学界对三类数据是否是个人信息可携权的客体形成了三种主要观点。第一种观点认为仅有直接数据可以被个人信息可携权调整，观测数据和预测数据因其可识别性不足并且属于平台的正当利益而不宜转移[4]。第二种观点借鉴欧盟立法经验，认为可转移的数据包括直接数据和观测数据而不包括预测数据[5]。其主要理由在于预测数据包含了平台算法对其的加工，平台对其投入了创造性劳动，应当属于平台的正当利益[6]。第三种观点认为无论是直接数据、观测数据或者预测数据都应该纳入个人信息可携带权的调整范围之内，但通常都认为应当对预测数据的转移附加适当条件[7]。然而上述无论数据分类标准或者是数据是否可转移的判断依据都难以真正实现权利目的。

4 权利实现的完善建议

个人信息可携带权往往被认为是“软性”“具有宣誓性”的权利，但这样先入为主的概念通常为该权利的难以实现提供理由，使其沦为纸面上的权利而非事实上的权利。为确保该权利的实现，笔者提出以下几条建议。

4.1 个人信息模块化封装与场景化应用

个人信息的模块化封装指个人信息依照不同的功能维度被切分为不同的可独立调用的子模块，例如可

将个人信息的分割为偏好模块如算法标签、兴趣画像等，联系模块如手机号码、邮箱号等，行为模块如浏览、交易、社交记录等。以数据形式存在的个人信息不同于传统个人信息的特点在于其能通过算法以不特定的几条信息确定个人身份，这也是专门出台《个人信息保护法》保护个人信息之必要性所在。个人信息的模块化封装通过个人信息的切分能够有效降低因个人信息的泄露而识别个人的危险性，同时每个模块都遵循统一的数据模型与接口规范（如 OpenAPI），个人可一次性授权、跨平台复用，避免“格式转换—人工清洗—二次授权”的重复劳动。并且个人信息的模块化封装为场景化应用提供了基础。

个人信息的场景化应用包括两部分，首先对于不同的场景对个人信息可携带权的客体范围做出不同规定，例如在较为敏感的场景如涉及数据跨境流动或金融数据时采用较为严格的数据转移范围与审查，而对于日常化的商业场景如网络购物时采用较为宽松的标准。

4.2 区块链技术在权利实现上的应用

个人信息的转移可以概括为三件事：数据从 A 方“取出来”，路上“不走丢，不被改，不泄密”，数据到 B 方验真。区块链在这三件事上的优势可以概括为一句话：把“信任”从依赖机构变成依赖技术，把“控制”从平台还给个人。链上个人信息的转移安全性受到保障，对于数据接收方 B 方而言，哈希+数字签名保证“内容+时间戳”不可篡改，B 方一键链上核验即可确认来源和完整性。对于用户而言，一次授权可一键查看、随时撤销。通常个人信息的转移要满足 api 接口的互接与传输协议的签署，用户要实现个人信息的自由流动意味着每两家数据平台要重复上述过程，这无疑产生了巨大的对接成本。而区块链技术在个人信息转移仅需一条公共或联盟链即可当“信任总线”，A、B 只需遵循同一协议（如 DDTP），边际成本趋近于零。

4.3 客体的包容化与强化法律监管

现有无论数据分类标准或者是数据是否可转移的判断依据都难以真正实现权利目的。原因在于，首先，细分标准的做法不具备可操作性。在用户转移个人数据的过程中，情况往往是打包式转移，即通常为账号内所有数据的转移，对账号内所有数据进行数据区分并不现实且工作量巨大。其次，数据的计量单位难以确定，“单个”数据中“单”如果表示的是代表数据的 0 或者 1 的代码，则不具备可分类性。如果用单组数据表示，则一组数据往往可能包含多种属性既是观测数据又属于预测数据的组成部分而难以区分。因此，对于个别用户的数据转移而言，个人信息可携带权的客体不应拘泥于数据类型而应包括不侵犯他人隐私的所有用户数据，除非数据处理者能够证明数据的转移侵犯了其正当权益或者商业秘密，否则应当提供可供数据转移的途径。对于群体性数据转移，考虑到对平台的竞争利益，可以做出适当限制，并将举证责任转移至数据转移的发起者。

同时对于不履行信息转移义务的网络平台，应加强法律责任的追究。当前，《个人信息保护法》和《反不正当竞争法》均对信息处理者的违法行为规定了相应的法律责任。然而，这些规定在实际操作中仍存在一定的局限性。为此，应进一步完善相关法律法规，明确信息处理者的法律责任，确保个人信息可携带权的有效实现。

5 结语

尽管可携带权标志着从间接保护向直接保护的转变，但其规定过于笼统，存在客体模糊、路径缺失、技术障碍等问题，导致权利难以落地。在属性层面，个人信息可携带权是一种“数据主导权”，旨在将个人信息的控制权从平台转移至用户，兼具人格权与财产权双重属性，并体现为公法对私法不足的必要补充。针对客体界定难题，将数据细分为“直接—观测—预测”三类并分别判断是否可携的做法操作成本高、标准冲突、与“打包迁移”现实脱节。应以“包容化”思路重塑客体范围：除非平台能证明转移侵害其商业秘密或正当利益，否则用户账号内全部数据均应允许携转，单账户数据不构成商业秘密。在实现路径上，一是“模块化封装+场景化应用”，通过统一数据模型与接口，实现颗粒度可调、跨平台复用；二是引入区块链技术，以链上哈希、数字签名降低信任与对接成本，让用户私钥触发“转账式”数据迁移；三是强化平台义务与责任，禁止技术封锁，豁免小企业，合理费用由用户承担，并完善违法责任条款。个人信息可携带权的实现应以“流通”为核心价值，以“技术+法律”双轮驱动，力图破解可携带权“软性宣示”困境，为构建可操作的本土化方案提供系统性思路。

参考文献

[1] 程啸.论大数据时代的个人数据权利[J].中国社会科学,2018,(03):102-122+207-208.

[2] 王锡锌.个人信息国家保护义务及展开[J].中国法学,2021, (01):145-166.

[3] 周汉华.个人信息保护的法律定位[J].法商研究,2020,37(03):44-56.

[4] 孙跃元.数据可携权权利客体研究：结构、效果与中国化[J].河南财经政法大学学报,2022,37(03):78-90.

[5] 汤霞.数据携带权的适用困局、纾解之道及本土建构[J].行政法学研究,2023,(01):95-107.

[6] 李明明,孙佳雯,罗伟.数据可携带权的理论界定与实践模式[J].计算机学报,2020,43.

[7] 张哲.论个人信息可携带权的客体界定[J].地方立法研究,2024,9(03):39-56.

[8] 曾彩霞,朱雪忠.欧盟数据可携权在规制数据垄断中的作用、局限及其启示——以数据准入为研究进路[J].德国研究,2020,35(01):133-147+164.