

数据可携带权的构造与实现

权利客体、技术可行性与平台义务

赵跃

(安徽国运律师事务所, 安徽 合肥 230000)

摘要：个人信息保护法第四十五条第三款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。这一规定被称为数据可携带权，其规范目的在于打破平台的数据锁定、促进竞争、增强个人对其信息的控制。但条文的适用面临三重困难：其一，权利的客体范围不清，个人提供的原始数据、平台基于数据生成的衍生数据、以及与他人信息混合的数据，是否均可携带；其二，技术可行性未作界定，平台常以“格式不兼容”“系统不支持”为由拒绝；其三，义务的层次不明，平台是仅须提供导出，还是须直接转移至指定平台，抑或须持续同步。本文主张：客体范围以“个人提供”与“个人行为生成”为界，纯粹由平台投入形成的衍生数据不属于携带的范围，但平台不得以商业秘密为由拒绝传输原始数据；技术可行性以“现有技术条件下可实现”为标准，平台须以通用格式提供，不得设置专有格式的技术壁垒；义务分三层，第一层是提供副本，第二层是转移至指定平台，第三层是在合理期限内持续同步，三层的适用依请求的内容与平台的能力确定；拒绝的正当理由限于国家安全、公共利益、他人权益、技术不能四项，且须书面说明。

关键词：数据可携带权；个人信息；数据锁定；平台义务；技术可行性

中图分类号：D923 **文献标识码：**A **文稿编号：**WJLT(2020)05-0037-12

The Structure and Realization of the Right to Data Portability

ZHAO Yue

(Anhui Guoyun Law Firm, Hefei 230000, Anhui, China)

Abstract: Article 45(3) of the Personal Information Protection Law provides that where an individual requests the transfer of personal information to a designated processor and the conditions set by the national cyberspace authority are met, the processor shall provide a channel for transfer. This is the right to data portability, aimed at breaking data lock-in, promoting competition and enhancing individual control. Its application faces three difficulties: the scope of the object, namely whether raw data provided by the individual, derived data generated by the platform, and mixed data involving others may all be ported; technical feasibility, which platforms invoke to refuse on grounds of incompatible formats; and the layers of obligation, whether the platform need only offer an export, transfer directly to a designated platform, or synchronize continuously. This article argues that the object should be bounded by data provided or generated by individual behaviour, excluding derived data formed purely by platform investment, though trade secrets may not justify refusing raw data; that feasibility means what is achievable under existing technology, requiring common formats and prohibiting proprietary barriers; and that obligations fall into three layers, namely providing a copy, transferring to a designated platform, and continuous synchronization within a reasonable period. Refusal is limited to national security, public interest, third-party rights and technical impossibility, with written reasons.

Key words: data portability; personal information; data lock-in; platform obligations; technical feasibility

说明：（本文为作者个人研究观点，不代表所在单位意见）

作者简介：赵跃，安徽国运律师事务所执业律师，主要研究民商事诉讼与数据法。

一、问题的提出

用户在平台积累的数据，究竟属于谁？这一问题在数字经济时代日益突出。用户在社交平台发布的内容、在电商平台的交易记录、在音乐平台建立的歌单、在办公软件中保存的文档，均由用户创建或者由用户行为生成，但存储于平台的服务器，由平台的系统组织、由平台的算法推荐。用户离开平台时，这些数据能否带走？

平台的实践，多有限制。有的平台提供导出功能，但仅限部分数据，且格式专有；有的平台根本不提供导出，用户只能逐条复制；有的平台虽提供导出，但导出的数据不包含评论、互动记录、标签等“衍生信息”。用户想迁移到其他平台，往往须从头开始，既有的积累归零。这一现象，被称为数据锁定。

数据锁定有正反两面。正面的作用，是激励平台投入、保护用户数据安全、维持服务品质；负面的作用，是抬高用户的转换成本、阻碍市场竞争、削弱用户对其信息的控制。个人信息保护法第四十五条第三款的规定，正是针对负面作用而设：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。

条文的表述简略，留下三重困难。第一重是客体范围。条文说的是“个人信息”，但平台上的数据，既有用户提供的原始信息，也有平台基于用户行为生成的衍生信息，还有与其他用户混合的信息。三者是否均可携带，条文未作区分。

第二重是技术可行性。条文要求“提供转移的途径”，但未规定格式、接口、时限。平台常以“系统不支持”“格式不兼容”“涉及第三方技术”为由拒绝，用户无从主张。第三重是义务层次。平台是仅须提供导出，还是须直接转移至指定平台，抑或须持续同步，条文未予明确。

本文主张：客体范围以“个人提供”与“个人行为生成”为界，纯粹由平台投入形成的衍生数据不属于携带的范围；技术可行性以“现有技术条件下可实现”为标准，平台须以通用格式提供，不得设置专有格式的壁垒；义务分三层，依请求的内容与平台的能力确定；拒绝的正当理由限于四项，且须书面说明。

讨论之前，须先厘清一个前提：数据可携带权与爬虫抓取不同。可携带权是法定的、以个人同意为基础的数据获取通道，其对象是本人信息，其方式是平台配合；爬虫抓取是未经授权的数据获取，其对象是他人的数据，其方式绕过平台的技术措施。二者在合法性上截然不同。

未经授权爬取他人网站数据的合法性边界，实务中的判断标准可参见爬取别人网站的数据，违法吗一文所作的梳理。该文着眼于抓取的违法性，本文则着眼于合法携带的实现，两者构成数据获取的一体两面。

从产业背景看，数据锁定是平台经济的结构特征。平台通过用户规模、网络效应、数据积累形成壁垒，用户越多，数据越丰富，服务越精准，吸引力越强；后来者难以追赶，市场趋于集中。这一机制有其效率的一面，也有其排斥竞争的一面。可携带权的设置，正是对这一机制的法律校正。

校正的方式，不是拆解平台，而是降低转换成本。用户可以不失去既有数据而迁移，平台的锁定效应便减弱；平台为了留住用户，须在服务质量上竞争，而非在数据壁垒上设障。这一思路，与携号转网、账户迁移等制度一脉相承。

我国的数据要素政策，亦为可携带权提供了政策基础。数据作为生产要素，须流通才能发挥价值；流通的前提，是权属清晰、规则明确、通道畅通。可携带权是个人数据流通的通道之一，其完善程度，直接影响数据要素市场的发育。

争议的类型，亦值得梳理。实务中的纠纷，多因三种情形而起：其一是平台不提供导出，用户无从取得；其二是平台提供导出，但范围有限、格式专有，用户取得的数据无法使用；其三是平台提供导出，但要求用户结清欠款、放弃权利、接受新的授权。三种情形，分别对应客体范围、技术可行性、附条件履行三个问题。

纠纷的规模，尚难准确统计。此类纠纷标的额小、举证难，用户多不愿诉讼；公开的裁判文书数量有限，难以反映全貌。但从投诉的情况看，问题具有普遍性。这一点，恰恰说明可携带权的实现，不能只依靠个体的诉讼，还须有监管的介入与制度的配套。

二、规范基础与权利性质

数据可携带权的规范基础，主要在个人信息保护法第四十五条。该条第一款规定个人有权向个人信息处理者查阅、复制其个人信息；第二款规定个人请求查阅、复制个人信息的，个人信息处理者应当及时提供；第三款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。

三款之间，是递进关系。查阅是知情，复制是取得副本，转移是跨平台流动。查阅与复制的对象是本人的信息，转移的对象亦是本人的信息，但转移的后果是信息从一个处理者流向另一个处理者，涉及三方关系：个人、原处理者、新处理者。

民法典第一千零三十七条亦规定，自然人可以依法向信息处理者查阅或者复制其个人信息；发现信息有错误的，有权提出异议并请求及时采取更正等必要措施。该条未直接规定转移，但查阅、复制权可以视为转移权的基础。

比较法上，欧盟通用数据保护条例第二十条规定了数据可携带权，其内容有三：其一，个人有权以结构化、通用、机器可读的格式接收其提供的个人数据；其二，有权将这些数据传输给另一个控制者，不受阻碍；其三，在技术可行的情况下，有权要求直接传输。三项内容，构成完整的三层义务。

我国的规定，与欧盟的构造相近，但更为简略。相同之处，是都承认个人的转移请求权；不同之处，是我国将“符合国家网信部门规定条件”作为前提，而欧盟未设此前提。这一差异，反映了我国对数据流动的审慎态度：既承认权利，又保留监管的裁量。

权利的性质，学理上有三种学说。其一是人格权说，认为可携带权是个人信息权的权能，其基础是人格尊严与信息自决；其二是财产权说，认为数据是财产，可携带权是财产权的行使；其三是竞争法上的工具说，认为可携带权的功能是破除锁定、促进竞争，其性质是竞争政策的工具。

本文主张采人格权说为主、竞争法工具说为辅的复合构造。理由是：可携带权的直接

依据是个人信息保护法，其保护的法益是个人对其信息的控制，故以人格权为基础；但其实际效果是促进竞争，故在解释上应当兼顾竞争政策的考量。二者结合，可以使权利的行使既有私法的依据，又有公法的支撑。

权利的主体，是自然人，不包括法人。法人对其数据享有的权益，依反不正当竞争法、商业秘密的规定保护，不适用可携带权。个体工商户、农村承包经营户以自然人身份处理个人信息的，可以准用；但以组织名义处理的，不适用。

权利的对象，是“其个人信息”。此处的“其”，指的是请求人本人。请求人不得请求携带他人的信息，也不得请求携带与自己无关的平台的经营数据。这一限制，是可携带权与爬虫抓取的分水岭。

欧盟的经验，值得参考。通用数据保护条例第二十条的适用，限于“基于同意或者合同”处理的数据，且限于“个人提供”的数据；平台衍生数据不在其列。这一限制，与本文主张的三层区分相近。欧盟的实践亦表明，可携带权的实际效果有限，主要原因是格式不统一、接口不开放；故欧盟在数据法案中进一步规定了跨云服务的转换义务。

美国的路径不同。美国无统一的个人信息保护法，可携带权主要依行业监管与平台自律实现。金融、医疗领域有专门的携带规则；其他领域则依平台的自愿承诺。这一路径的优点是灵活，缺点是覆盖不全、执行力弱。我国的路径接近欧盟，采统一立法加监管细则的模式。

日本的路径，介于二者之间。个人信息保护法规定了本人的开示请求权，未直接规定可携带权；可携带的实现，依行业指南与竞争政策推进。这一路径的优点是循序渐进，缺点是权利基础不牢。三者的比较说明，可携带权的实现，既须有权利的宣示，也须有技术与产业的配套。

权利的限制，亦须讨论。可携带权的行使，不得侵害他人的权利，不得损害公共利益，不得滥用。滥用表现为：频繁请求、超范围请求、以携带为名获取他人信息、以携带为名实施不正当竞争。对滥用，平台可以拒绝，但须说明理由。

请求的频率，宜有限制。用户一年内请求携带的次数，不宜超过三次；超过的，平台可以要求说明理由，或者收取合理的成本费用。限制的目的是防止滥用，不是限制权利；用户有正当理由的，不受次数限制。

一个典型的争点，是用户在平台上的“创作内容”是否可携带。用户在社交平台发布文章、在短视频平台发布的视频，其著作权归用户，平台仅享有使用权；用户请求携带，平台应当提供。但平台往往以“内容已与平台的其他内容形成整体”为由拒绝，理由不成立。

另一个争点，是“关系链”是否可携带。用户的通讯录、好友列表、关注列表，既有用户本人的信息，也有他人的信息。本文主张，用户可以携带其自行添加的关系链，但不得携带他人未经同意提供的信息；平台可以提供关系链的摘要，例如好友数量、互动频

次，供用户参考。

三、客体范围：三层数据的区分

平台上的数据，可以按来源分为三层。第一层是用户提供的数据，包括注册时填写的信息、上传的内容、发布的文字图片视频。第二层是用户行为生成的数据，包括浏览记录、搜索记录、点击记录、购买记录、位置轨迹、设备信息。第三层是平台衍生数据，包括用户的画像标签、信用评分、推荐模型、聚合统计。

第一层与第二层，属于可携带的范围。理由是：这两层数据的形成，源于用户的提供或者用户的行为，用户对其有事实上的支配；平台的作用是存储与传输，未加入实质性的创造。故用户请求携带，平台应当提供。

第三层，原则上不属于可携带的范围。理由是：衍生数据是平台投入算法、算力、人力形成的，具有独立的财产价值；若允许用户携带，等于允许用户无偿取得平台的经营成果，与激励机制相悖。但衍生数据中涉及用户本人的部分，例如用户的画像标签，用户可以请求查阅、复制，但不得请求转移至其他平台用于商业目的。

三层之间的界限，并非绝对。以电商平台为例，用户的订单记录属于第二层，可以携带；平台基于订单生成的用户消费能力评分属于第三层，不可携带；但评分所依据的原始数据，即订单金额、频次、品类，属于第二层，可以携带。用户携带原始数据后，新平台可以自行计算评分，效果上与携带评分相近。

与他人信息混合的数据，处理须谨慎。例如社交平台的聊天记录，既有用户本人的信息，也有对方的信息；用户请求携带，可能侵害对方的个人信息权益。此时，应当区分：本人发送的内容，可以携带；对方发送的内容，须经对方同意；双方共同形成的内容，可以携带副本，但不得公开。

一个技术性问题，是数据的“可分离性”。若混合数据无法分离，平台可以拒绝携带，但应当提供替代方案，例如提供本人部分的摘要、提供去标识化后的数据。替代方案的合理性，由平台举证；不能举证的，应当承担不利后果。

匿名化数据，不属于个人信息，不受可携带权的约束。但匿名化的标准极高，须达到无法识别特定自然人且不能复原的程度；仅作去标识化处理的，仍属个人信息，仍可携带。实务中，平台常以“已匿名化”为由拒绝，法院应当审查匿名化的技术标准与实际效果。

数据的最小单位，亦须明确。携带的数据，应当以“条目”为单位，而非以“数据包”为单位。以条目为单位，用户可以自主选择携带的范围，避免全量导出带来的隐私风险；以数据包为单位，用户只能全有或者全无，不利于精细化控制。

元数据的携带，常被忽视。元数据是描述数据的数据，包括创建时间、修改时间、来源、标签、分类。元数据对于数据的可用性至关重要；若只携带内容而不携带元数据，新

平台难以还原数据的结构，迁移的效果大打折扣。本文主张，元数据应当随数据一并携带。

数据的完整性，须有保障。平台提供的数据，应当与平台内部存储的数据一致，不得删减、篡改、延迟。完整性的验证，可以由用户比对、由第三方审计、由监管抽查。验证发现不一致的，平台应当补正，并承担相应的责任。

数据的时效性，亦须考虑。平台提供的数据，应当是请求时的最新状态，而非某一历史时点的快照。若数据量巨大、难以实时提供，平台可以提供快照，但应当说明快照的时点，并在合理期限内补充增量。

四、技术可行性：标准、格式与接口

“技术可行”是可携带权适用的核心条件，也是最容易被滥用的抗辩。平台往往笼统主张技术不可行，却不说明不可行的具体原因，用户与监管机关均难以核查。本文主张，将技术可行性具体化为三项标准：格式的通用性、接口的开放性、时限的合理性。

格式的通用性，要求平台以结构化、通用、机器可读的格式提供数据。所谓结构化，是指数据以字段、表格、键值对的形式组织，而非以图片、扫描件、不可编辑的文档形式提供；所谓通用，是指格式为行业普遍支持，例如逗号分隔值、可扩展标记语言、数据交换脚本对象标记等；所谓机器可读，是指数据可以被程序自动解析，无须人工转录。

实务中的一种规避，是提供便携式文档格式的导出。此类格式虽然通用，但数据不可被程序直接解析，用户迁移到新平台仍需人工录入，实质上未实现携带。本文主张，此类导出不构成“提供转移的途径”；平台应当提供结构化格式，除非数据本身即为非结构化的内容。

接口的开放性，要求平台提供应用程序编程接口，供用户或者经用户授权的第三方调用。接口的开放，是可携带权从“导出”走向“转移”的关键。若平台仅提供导出，用户须自行下载、上传，转换成本仍然较高；若平台提供接口，新平台可以直接调用，实现一键迁移。

接口的开放，须有安全边界。平台可以要求调用方具备相应的资质、签署安全协议、接受审计；可以设置调用频率、数据量的限制；可以对敏感数据作脱敏处理。但安全边界不得成为拒绝开放的借口：平台以安全为由拒绝开放的，应当证明开放将导致具体的安全风险，而非抽象的担忧。

时限的合理性，要求平台在合理期限内完成转移。合理的期限，依数据的规模、复杂程度确定：一般情形下，不超过三十日；数据量巨大或者涉及多方处理的，可以延长，但不超过六十日。逾期未完成的，用户可以向监管部门投诉，或者提起诉讼。

技术不可行的举证责任，由平台承担。平台主张技术不可行的，应当提交技术说明、系统架构、改造方案的评估报告；仅以“系统不支持”为由的，不构成有效抗辩。监管机

关或者法院可以委托技术专家评估，评估的费用由平台承担。

技术可行性的判断时点，宜采请求提出时。平台在请求提出时不具备技术能力，但可以通过合理改造具备的，应当改造；改造的成本明显超过收益的，可以拒绝，但须说明。判断的标准，是成本与收益的比例，而非平台的主观意愿。

第一层义务的履行方式，可以是自助下载，也可以是人工处理。自助下载的，平台应当提供清晰的指引，说明可携带的数据范围、格式、限制；人工处理的，平台应当在合理期限内完成，并告知进度。两种方式，用户可以选择。

第二层义务的履行，须有新平台的配合。新平台应当具备接收的能力，包括接口的对接、格式的解析、安全的保障；不具备能力的，原平台可以提供导出，由用户自行上传。配合的方式，由双方协商；协商不成的，可以请求监管部门协调。

第三层义务的履行，涉及持续的技术投入。平台须维持接口的稳定、数据的同步、安全的监控；投入的成本，可以由用户或者新平台分担，但不得成为拒绝履行的理由。持续同步的期限，由用户与平台约定；未约定的，以一年为限。

义务的履行，须有记录。平台应当记录请求的时间、内容、处理的过程、结果，保存期限不少于三年；用户申请查询的，平台应当提供。记录的作用，是便于监管核查、便于争议解决。

小微企业的情况，须予考虑。小微企业技术能力有限，一并要求三层义务，可能超出其能力。本文主张，对小微企业可以设过渡期，过渡期内只要求履行第一层义务；过渡期的长短，依企业的规模、数据的类型确定。

五、平台义务的三层构造

平台义务的层次，是可携带权落地的关键。本文主张，义务分为三层，依请求的内容与平台的能力确定，层层递进，不得跳跃。

第一层是提供副本。用户请求查阅、复制其个人信息的，平台应当以通用格式提供副本。此层义务的依据是个人信息保护法第四十五条第一款、第二款，其内容明确，争议较小。副本的提供，可以即时下载，也可以在合理期限内以邮件、链接等方式交付。

第二层是转移至指定平台。用户请求将个人信息转移至其指定的处理者的，平台应当提供转移的途径。此层义务的依据是第四十五条第三款，其内容是提供“途径”，而非直接完成转移。途径包括接口、导出工具、授权机制。平台提供途径后，转移的实际完成由用户与新平台配合。

第三层是持续同步。用户请求在特定期限内持续同步其信息的，平台应当在技术可行的范围内提供。此层义务的依据，是第四十五条第三款的扩张解释，其正当性在于：数据是动态的，一次性的转移不足以实现真正的迁移；若用户在原平台继续产生数据，新平台的信息将不完整。

三层的适用，依请求的内容确定。用户仅请求副本的，适用第一层；请求迁移至新平台的，适用第二层；请求持续同步的，适用第三层。平台不得以第二层的义务未履行完毕为由拒绝第一层，也不得以第一层已履行为由拒绝第二层。

三层的关系，是递进而非替代。第一层是基础，第二层是第一层的延伸，第三层是第二层的延伸。平台的能力不足以履行第三层的，可以只履行前两层，但须说明；用户不接受说明的，可以请求监管部门处理。

义务的履行，不得附加不合理条件。平台不得要求用户支付高额费用、不得要求用户放弃其他权利、不得要求用户同意新的授权、不得以用户结清欠款为条件。合理的条件，限于身份验证、安全审查、费用分担，其标准由监管部门规定。

义务的免除，须有法定事由。个人信息保护法第五十条规定，个人信息处理者应当建立便捷的个人行使权利的申请受理和处理机制；拒绝个人行使权利的请求的，应当说明理由。据此，平台拒绝履行三层义务的，须说明理由，并告知用户投诉、诉讼的途径。

拒绝的通知，须及时。平台应当在收到请求后的合理期限内作出答复，一般不超过十五日；逾期未答复的，视为拒绝。答复的内容，包括是否同意、同意范围、履行时间、拒绝理由。

拒绝的救济告知，须明确。平台应当在答复中告知用户投诉的机关、诉讼的法院、起诉的期限；未告知的，用户起诉的期限从知道或者应当知道之日起算，不受短期限制。这一安排，可以防止平台以程序瑕疵逃避责任。

拒绝的复核，可以设置。用户对拒绝不服的，可以向平台申请复核；平台应当在收到复核申请后的十五日内作出复核决定。复核不是诉讼的前置程序，用户可以直接起诉；但复核可以过滤部分争议，减轻法院的负担。

六、拒绝的正当理由

平台拒绝携带的正当理由，本文主张限于四项：国家安全、公共利益、他人权益、技术不能。四项之外的理由，不构成正当拒绝。

国家安全，包括国家秘密、军事秘密、情报信息。平台主张涉密的，应当提交保密部门的认定；仅以“涉及国家安全”为由笼统拒绝的，不予支持。涉密数据的范围，应当严格限定，不得扩张至一般的经营数据。

公共利益，包括公共安全、公共卫生、应急管理。平台主张涉公共利益的，应当说明具体的公共利益内容、拒绝携带与公共利益之间的关联、拒绝的必要性。抽象地主张“影响公共利益”的，不构成正当理由。

他人权益，包括他人的个人信息、知识产权、商业秘密。平台主张涉他人权益的，应当区分：可以分离的，分离后提供；不能分离的，提供去标识化的版本；完全不能提供的，说明理由并提供替代方案。以他人权益为由一概拒绝的，不予支持。

技术不能，如前所述，须有技术说明与评估报告。技术不能是暂时的，平台应当在具备能力后履行；长期不能的，应当说明改造计划与时间表。以技术不能为由永久拒绝的，不予支持。

拒绝的形式，须采书面。书面说明应当载明拒绝的理由、依据、事实、救济途径；口头拒绝、系统提示、客服回复，不构成有效的拒绝。未书面说明的，视为未拒绝，用户可以直接起诉。

拒绝的审查，由监管部门或者法院进行。审查的标准，是理由是否真实、是否具体、是否必要。理由不成立的，责令履行；理由成立的，驳回请求。审查的过程中，平台应当提交证据，用户有权质证。

一个易被忽略的问题，是拒绝的部分性。平台对部分数据拒绝携带，对另一部分同意携带的，应当分别说明；不得以部分拒绝为由拒绝全部。部分拒绝的理由成立的，其余部分仍应履行。

平台间的数据迁移协议，是解决冲突的重要机制。原平台与新平台可以约定迁移的技术标准、安全要求、责任分担；协议的内容，不得损害用户的权益，不得排除可携带权的适用。协议的存在，可以作为平台已履行义务的证据。

行业标准的制定，亦须推进。可携带的格式、接口、安全要求，宜由行业协会牵头制定，报监管部门备案。标准的作用，是降低协商成本、统一技术口径、便于监管核查。标准应当是开放的，不得由个别平台主导。

七、与商业秘密、著作权的冲突

数据可携带权的行使，可能与平台或者第三人的权利发生冲突。冲突的类型有二：与平台的商业秘密、与第三人的著作权。两类冲突的处理，须在保护个人权益与保护投资之间寻求平衡。

与商业秘密的冲突，集中体现在衍生数据上。平台主张，用户画像、推荐模型、信用评分是其投入形成的商业秘密，用户无权携带。本文主张，商业秘密不能成为拒绝携带原始数据的理由；原始数据是用户提供或者生成的，不属于平台的商业秘密；平台对衍生数据主张商业秘密的，可以拒绝携带衍生数据本身，但不得拒绝携带其赖以形成的原始数据。

平台以商业秘密为由拒绝携带的，应当证明三项：其一，该数据符合商业秘密的构成要件；其二，携带将导致商业秘密的泄露；其三，泄露的损害超过用户的利益。三项具备的，可以拒绝；缺一的，不得拒绝。

与著作权的冲突，体现在用户上传的内容上。用户上传的图片、视频、文字，其著作权可能归用户，也可能归平台或者第三人。著作权归用户的，用户可以携带；归平台的，用户不能携带，但可以携带其使用的记录；归第三人的，须经第三人同意。

实务中的一种情形，是用户上传的内容包含他人的作品，例如翻唱、混剪、转载。此类内容的携带，可能构成对他人著作权的侵害。平台可以拒绝携带，但应当告知用户原因，并提供替代方案，例如携带原作品的链接、提供内容的摘要。

与数据库权利的冲突，亦须考虑。平台对其数据库享有汇编著作权的，用户可以携带其中的个人数据，但不得复制数据库的整体结构。判断的标准，是携带的数据是否构成对数据库的实质性利用；构成实质性利用的，须经平台许可。

冲突的解决，宜采比例原则。一方面，保护个人的信息自决，是可携带权的核心价值；另一方面，保护平台的投资，是数字经济发展的基础。二者冲突时，应当权衡：携带对个人利益的影响、拒绝对平台利益的影响、有无替代方案。权衡的结论，须在裁判文书中说明。

一个前置问题，是数据的权属。我国现行法未明确数据的权属，学理上有数据所有权说、数据用益权说、数据财产权说等多种主张。本文认为，在权属未明的情况下，可携带权的行使不以其为前提：无论数据归谁，个人对其个人信息享有查阅、复制、转移的权利；平台的权利，通过商业秘密、著作权、反不正当竞争等制度保护。

管辖的确定，须便于用户。用户与平台的纠纷，可以由被告住所地法院管辖，也可以由用户住所地法院管辖；用户住所地难以确定的，可以由合同履行地法院管辖。这一安排，可以降低用户的诉讼成本，避免用户因跨地域诉讼而放弃权利。

诉讼的费用，宜予减负。此类案件的标的额往往难以确定，可以按件收取；用户经济困难的，可以缓交、减交、免交。平台败诉的，诉讼费由平台负担，用户的合理费用亦由平台赔偿。

判决的执行，须有保障。平台拒不履行判决的，法院可以采取罚款、拘留、纳入失信名单等措施；情节严重的，可以追究拒不执行判决、裁定罪。执行的力度，是权利实现的最后保障。

八、救济与责任

平台无正当理由拒绝携带、拖延携带、以不合理条件阻碍携带的，用户可以寻求三条救济：向监管部门投诉、向法院提起诉讼、请求检察机关支持起诉。三条救济可以并用，也可以择一。

投诉的受理机关，是网信部门。用户应当提交身份证明、携带请求的记录、平台的拒绝说明；网信部门应当在受理后六十日内处理，情况复杂的可以延长三十日。处理的方式，包括责令改正、警告、罚款。

诉讼的类型，有两种。其一是个人信息保护纠纷，用户以平台侵害其个人信息权益为由，请求判令平台提供携带；其二是合同纠纷，用户以平台违反服务协议为由，请求判令履行。两种类型可以择一，也可以合并。

诉讼的请求，须具体。用户应当请求判令平台在特定期限内，以特定格式，提供特定范围的数据；请求泛泛的，法院可以释明。请求的具体化，是判决可执行的前提。

举证的责任，宜作有利于用户的分配。用户须证明：其向平台提出了携带请求、平台拒绝或者未在合理期限内履行。平台须证明：拒绝有正当理由、已提供合理的替代方案、技术不可行。这一分配，符合双方举证能力的差异。

损害赔偿的范围，包括实际损失与合理费用。实际损失难以计算的，可以依平台因拒绝而获得的利益确定；仍难以确定的，由法院酌定。合理费用包括律师费、公证费、技术鉴定费。精神损害一般不予支持，但平台恶意拒绝、造成严重后果的除外。

行政责任的配置，须与行为的性质相适应。个人信息保护法第六十六条规定，违法处理个人信息，情节严重的，处五千万元以下或者上一年度营业额百分之五以下罚款。拒绝携带是否属于“违法处理”，条文未明确；本文主张，经责令改正而拒不改正的，可以适用该条。

公益诉讼的空间，值得讨论。平台普遍拒绝携带，侵害众多用户的权益的，检察机关、消费者组织可以提起公益诉讼。公益诉讼的请求，可以是判令平台提供通用的携带接口、停止设置技术壁垒。这一路径，可以弥补个体诉讼的不足。

从审判的角度看，此类案件的审理须把握三点。其一，不要以“数据权属未明”为由拒绝裁判；权属未明不影响个人行使其信息权利。其二，不要以“技术不可行”为由轻易采信平台的抗辩；技术抗辩须有具体的说明与评估。其三，不要忽视判决的可执行性；请求应当具体，格式、范围、期限均须明确。

制度的成熟，须经实践的检验。可携带权在我国确立不久，适用的案例尚少，规则的细节有待明确。本文的讨论，是解释论上的尝试，不是立法论上的设计；其目的，是在现行法的框架内，为实践提供可操作的思路。随着案例的积累，规则自会细化。

最后须强调，可携带权不是万能的。它解决的是数据的迁移，不解决数据的定价；它降低了转换成本，不消除平台的规模优势。数据治理是一套组合拳，可携带权只是其中一招。指望一招制胜，既不现实，也不必要。

九、结语

数据可携带权是数字时代个人对其信息控制的重要制度。本文主张：客体范围以“个人提供”与“个人行为生成”为界，纯粹由平台投入形成的衍生数据不属于携带的范围，但平台不得以商业秘密为由拒绝传输原始数据；技术可行性以现有技术条件下可实现为标准，平台须以通用格式提供、开放接口、在合理期限内完成；义务分三层，提供副本、转移至指定平台、持续同步，依请求的内容与平台的能力确定；拒绝的正当理由限于国家安全、公共利益、他人权益、技术不能四项，且须书面说明。

这一构造的意义，在于为个人、平台、监管三方提供可预期的规则。个人知道可以携

带什么、以什么方式携带；平台知道应当履行什么、可以拒绝什么；监管知道审查什么、处罚什么。规则明确，数据流动才能有序。

当然，制度的落地须有配套。技术标准的制定、接口规范的统一、争议解决机制的建立，均须推进。立法层面，可以考虑在个人信息保护法中增加可携带权的专条，明确客体范围、义务层次、拒绝事由、法律责任；也可以由网信部门制定专门的规定，细化操作。

数据的价值在于流动，流动的前提在于可信。可携带权的功能，不是让数据无序流动，而是让个人在可信的规则下自主决定数据的去向。这一功能的实现，既需要权利的宣示，更需要义务的落实。权利的宣示易，义务的落实难；制度建设的重心，应当放在后者。

参考文献

- [1] 《中华人民共和国个人信息保护法》第四十五条、第四十七条、第五十条、第六十六条。
- [2] 《中华人民共和国民法典》第一千零三十七条、第一千零三十八条。
- [3] 《中华人民共和国反不正当竞争法》第九条、第十二条。
- [4] 《中华人民共和国数据安全法》第二十一条、第三十条。
- [5] 《网络数据安全管理条例》第二十四条、第二十五条、第三十条。
- [6] 丁晓东：《数据可携带权的性质与构造》，《中国法学》2022年第3期。
- [7] 张新宝：《个人信息权益的私法保护》，《法学研究》2021年第5期。
- [8] 周汉华：《数据要素市场化配置的法律框架》，《政法论坛》2023年第1期。
- [9] 胡凌：《平台数据锁定与可携带权》，《中外法学》2022年第6期。