

数据可携带权的适用逻辑与完善进路

王 凡

青岛大学法学院, 山东 青岛

收稿日期: 2024年3月6日; 录用日期: 2024年3月14日; 发布日期: 2024年4月18日

摘 要

我国2021年出台的《个人信息保护法》第45条首次对个人数据可携带权作出了规定, 但关于数据可携带权的权利属性、适用范围、行使条件等并未作出详尽解释, 因此导致此项权利在实施过程中面临诸多困境。目前我国学术界围绕数据可携带权的概念、结构以及本土化改造等展开了诸多讨论, 但并未溯及《个人信息保护法》中规定这一权利的立法根源问题。目前我国立法体系日趋完善, 数据保护技术手段难题也逐渐克服, 从可行性视角来看, 我国具备数据可携带权的本土化条件。但是在具体适用过程中, 还面临着许多障碍, 需要立足这一制度, 结合立法目的等对数据可携带权的基本理论、必要性、可行性、实施障碍及完善进路展开更高层次的讨论。

关键词

数据可携带权, 欧盟GDPR, 《个人信息保护法》, 本土化

The Application Logic and Improvement Approach of Data Portability Rights

Fan Wang

Law School of Qingdao University, Qingdao Shandong

Received: Mar. 6th, 2024; accepted: Mar. 14th, 2024; published: Apr. 18th, 2024

Abstract

Article 45 of China's Personal Information Protection Law, which was promulgated in 2021, provides for the first time the right to personal data portability. However, there is no detailed explanation of the rights attributes, scope of application, and exercise conditions of the right to data portability, which has led to many difficulties in the implementation process of this right. At present, there have been many discussions in the academic community of our country regarding the con-

cept, structure, and localization of the right to carry data, but the legislative roots of this right stipulated in the Personal Information Protection Law have not been traced back. At present, China's legislative system is becoming increasingly perfect, and the difficulties in data protection technology are gradually being overcome. From a feasibility perspective, China has the localization conditions for data portability. However, in the specific application process, there are still many obstacles that need to be addressed. Based on this system, it is necessary to conduct a deeper discussion on the basic theory, necessity, feasibility, implementation obstacles, and improvement paths of data portability rights in combination with legislative purposes.

Keywords

Data Portability Rights, EU GDPR, Personal Information Protection Law, Act Localization

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 问题的提出

近年来,随着互联网技术对社会生活的全覆盖,网络上个人信息被泄露、平台不合理收集处理用户个人信息的事件频发,个人信息主体与个人信息处理者之间的关系以及个人信息权益成为常见议题。大数据时代个人信息不仅关乎个人信息主体的人格尊严和人格自由[1],也是个人信息处理者的发展基石,在保障个人信息安全的同时也应为个人信息流动创造便利可用的条件。个人信息可携带权即是在个人信息保护与流动平衡基础上设立的全新制度。

“可携带权”概念最初来源于欧盟。2016年,个人数据携带权被《通用数据保护条例》(以下简称“GDPR”)确立为个人数据主体的权利。从GDPR对个人数据携带权的规定以及第29条工作组发布的《个人数据携带权指南》(以下简称《指南》)中可以看出,欧盟的数据携带权立法基础实际上是赋予个人数据主体更多控制自己数据的权利,并在此基础上打破数据锁定效应,间接地促进竞争和创新,同时通过数据相互转移的方式实现欧盟数字单一市场的长期规划。可携带权作为法律创设的权益,发展至今一直受到争议。在数字经济和互联网高度发达的背景下,个人信息处理者收集的个人信息甚至可以成为企业优质的数据资产,但从《个保法》第45条的规定来看,可携带权并没有一个清晰的构成要件法律效果的法条结构,理论上的属性也不甚清晰,且在实践中,由于立法刚刚颁布施行,目前所有援引《个保法》中个人信息主体权利为依据的裁判都可能成为对后续有指导意义的判例。

研究我国《个保法》中的可携带权的意义具体为:首先,在可携带权的立法目的上,从《个保法》的体系中澄清可携带权的独立功能和定位是进一步分析可携带权的前提。可携带权多被认为可以打破“数据孤岛”和“锁定效应”的局面,其价值在于完善个人信息流动秩序,从而创造良好的数字市场竞争环境。其次,在《个保法》的私法层面上,分析可携带权的属性对个人信息主体行权有重要帮助。《个保法》是一部公私法交叉、具有开放性、应用性和整合性的领域法。明晰可携带权在个人信息权益体系中的具体权能,需结合人格权的防御性特征和我国《个保法》下个人信息控制性的范围和内容进行分析。在此立意和目标下,本文拟在我国个人信息保护法的视阙下探讨数据可携带权问题,探寻可携带权的功能定位,从个人信息主体对其信息的控制讨论可携带权作为人格权的防御性质,厘清可携带权的行权边界和方式,为规则的最终,落地提供理论支撑,并尝试探索可携带权的中国适用路径。

2. 引入数据可携带权的可行性及实施障碍预估

(一) 引入数据可携带权的可行性

在我国,互联网的发展在不断地发生着变化,在实际操作过程中,已经逐步地出现了与网络公司有关的数据可携带权的纠纷。因此,在实际操作中,数据可携带权的引进是一种迫切的需要,同时,权利本土化的现实条件也越来越成熟。

(1) 我国具有数据可携带权的法律基础

2005年《刑法修正案(五)》增加了“盗窃、收买、非法提供信用卡信息罪”,2009年《刑法修正案(七)》增加了“侵犯公民个人信息罪”,其中规定了“盗窃、收买、非法提供公民个人信息罪”,以及“盗窃、出卖、提供公民个人信息”等情节严重的,均为刑事犯罪。这就是我国刑法目前对个人信息保护的现状,从中可以看到,我国正在逐步强化对个人信息的保护。然而,仅仅从刑法的角度来考虑,显然并不能彻底解决大数据时代下的个人信息侵权问题[2]。

其中,《消费者权益保护法》于2013年进行了修改,将消费者信息纳入了法律保护范围,这也是第一次将个人信息作为一种民事权利来进行保护;2017年《网络安全法》中的“网络信息安全”一章,对收集、存储、保存、使用个人信息进行了详细的规定。这几部法律,都表明了我们国家对个人信息的私法保护,而且我们国家的立法也在进行着,《民法总则》在2017年10月开始生效,我们国家对个人信息的保护,已经有了很大的进展。《民法总则》第五章“民事权利”一节,明确规定了自然人的个人信息,可以看出,我国是把个人信息的保护定位在自然人的民事权利上的,这就为今后的个人信息的保护,提供了一个可以延伸和实现的空间,以及法律上的基础[3]。

《人格权编》于2018年8月在第十三届全国人大常委会第五次会议上正式通过,加强了对隐私、个人信息的保护,并在此基础上,进一步明确了个人信息的保护属于自然人的人格权益,尤其是在大数据环境下,对于人身权利、人格尊严的保护,更是具有十分重大的意义,这也为我国未来即将出台的《个人信息保护法》提供了可借鉴的空间[3]。

2018年9月,十三届全国人大常委会发布的近五年立法计划中,个人信息保护立法被排在了首位,而数据可携带权是个人数据权利体系中的一部分,在我国探讨个人信息保护立法时,对其进行考察和研究是合情合理的。我们需要结合自己的经济、法律、科技、政治等环境,以及欧美等国关于数据可携带权的立法经验,对我们的个人信息保护进行研究,并在此基础上,对数据可携带权的相关条款进行研究。

(2) 我国具有实施数据可携带权的市场空间

中国互联网信息中心公布了第39次《中国互联网络发展状况统计报告》,截至2016年12月底,中国互联网用户已达到7.31亿,数量庞大惊人。随着中国互联网用户的不断增加,互联网服务商的数量也在不断增加。中国物流业协会特邀研究员杨达卿认为,在当前的网络商务环境下,拥有对数据的掌控能力,才能在网络商务中占据一席之地。这其中有两个问题,其一,数据的取得;其二,数据的流通。数据的取得与数据的流通正是数据可携带权的内容。

目前在实务中所反映的,无非就是数据的获取和流通问题,或者说“数据可携”问题,但由于法律上没有明确的规定,所以法院在审理这类案件时,更多的是从公司之间的不公平竞争着手。但是,数据终究是用户的,数据的产生是建立在自然人在互联网上的活动基础上的,因此,它并不能被简单地定义为硬件厂商的,也不能被定义为服务提供商的,更不能被定义为物流公司等网络服务提供商的。国家对数据发展战略进行了重点关注,与此同时,也对个人信息的保护进行了重点关注。然而,随着数据的发展,不可避免地会产生大量的个人数据的获得和流动,这就产生了数据主体与数据控制者、数据控制者之间的矛盾,以及数据控制者与数据的冲突。这为我国引入数据可携权创造了市场空间,其重点在于自然人对个人数据的存储与转移,旨在增强对个人数据的控制能力,并促进市场竞争,因而也能起到一种

矛盾的调节作用[4]。

(3) 我国公民个人信息保护维权意识的提高

2015 年我国出现首例“被遗忘权”案：任某诉北京百度网讯科技有限公司人格权一案。这是第一次提起“被遗忘权”，虽然在二审中，法庭并没有支持，但是这起案例的重要性却是非同小可，此案引起了学术界对“被遗忘权”的广泛关注，也说明了我们国家的人民，正在逐渐意识到数据安全和数据权利的重要性。数据可携带权和“被遗忘权”均为欧洲联盟《一般数据保护条例》(General Data Private Act, 简称 GDPR)所确立的一种新的数据权，其实质是在“信息自决权”基础上，为适应大数据环境而产生的一种新的权利。

中国互联网协会公布了《中国网民权益调查报告 2016》，根据中国互联网协会 12321 网络不良和垃圾信息举报处理中心每日受理的投诉数据，《中国网民权益调查报告 2016》显示，中国庞大的网民群体中，用户的权益受到了严重的损害，大量的用户意识到了自己的隐私受到了侵犯，并且开始向社会求助[5]。由此可以看出，在大数据时代的背景下，人们对个人的信息危机有了更多的认识，并且对个人数据的保护也有了更多的认识。

(二) 引入数据可携带权的实施障碍预估

(1) 增加隐私与数据安全风险

数据可携带权的使用将增加数据使用者的隐私和数据安全风险。当数据控制者为履行其对数据可携带权的规定义务时，在满足其对数据可携带权的需求时，往往会将其隐私安全级别的门槛设定得很低，同时，因其不透明的传输过程，极易使其暴露在信息泄露的危险中，而信息主体又不能及时获取。数据主体作为自然人，在正常情况下，对其所要转移的个人数据的接收对象是否具备接受资格进行审查和核实。如果数据控制者向不应该获得数据权限的人提供了访问权限，那么数据就有可能被用于违法行为，进而给数据主体造成财产损失，甚至是人身伤害。换言之，数据可携带权必须以严格的认证和监管为前提，不然很可能会被恶意软件所利用，给数据使用者带来严重的数据安全隐患。

(2) 与企业各类权利产生冲突

数据控制者在对收集的数据进行加工处理之后，就会产生出财产价值。在这种情况下，如果数据主体将获得的副本直接有偿或无偿授予其他数据控制者，那么就会构成对数据控制者主动行为后所获得的商业秘密或知识产权的侵犯。相应地，知识产权和商业机密等方面的规定，又会对数据主体的个人信息进行限制，从而与基于可携带权的内容相抵触。

首先，数据可携带权与知识产权之间的矛盾集中体现在特殊数据库权利和著作权之上：著作权保护原创作品，具有排他性，比较容易从网络服务提供者的数据资产中分离出来，该权利防止未经授权的复制或传播，比如向公众或其他平台传播数据主体发布的影评、博客、照片、视频等；为了保护数据库的成果，才有了专门的数据库权，数据库是数据控制者对数据的收集、处理的投入的产物，这种权利阻止了对数据库的非法提取和使用。其次，数据可携带权与商业秘密权利之间的矛盾体现在：一是可携带权可以转让的信息，可能会涉及被数据控制者专享的商业秘密；二是数据可携带权会导致商业秘密拥有者的竞争优势被削弱，进而丧失创新的动力。个人数据同样能够成为知识产权与商业秘密权利形成的基础，因此，通过对个人数据进行分析，从而建立新型数字服务的商业模式的发展可能会因为数据可携带权的引入而受到影响。但是，《一般数据保护条例》第 68 条和第 20 条关于数据可携权的限制，并未清楚说明在数据可携带权的使用会对商业机密和知识产权造成负面影响时，应采取哪些措施加以限制[6]。

3. 数据可携带权本土化改造之构思

(一) 我国数据可携带权的确立路径

实现数据可携带权有个人数据保护法与反垄断法这两种路径，虽然上述两种路径之间存在着不同之处，但是这并不意味着这两种权利是完全相互排斥的，它们在很多方面都是相互关联的。首先，在某种程度上，这两个国家的目的是一致的。个人信息保护法以保护自然人权利为目的，而反垄断法以维护消费者合法权益为目的，两者在权利保护上有一定的交叉和重合；其次，因为数据可携带权的适用范围包含反垄断法所规定的范围，很多大型网络公司都会被《个人数据保护法》和《反垄断法》所限制；最后，二者各有优势，反垄断法可以对个人数据保护法下的数据可携带权予以适当补充。由于数据可携带权只适用于自然人，而反垄断法适用于法人、其他组织，因此，我国在数据可携带权方面存在着一定的不足。个人资料保护法的重点在于事先的预防，而反垄断法的重点在于事后的监督。基于此，我国应当以《个人信息/数据保护法》为基础，赋予数据可携带属性，并与反垄断法相结合，确保数据可携带权的实现。

(二) 我国数据可携带权的权利结构

(1) 权利义务主体的确定

《个人信息/数据保护法》对数据可携带权作出了明确的规定，其立法目标也是在大数据时代对个人数据的控制能力的基础上，因此，我国将数据可携带权的权利主体限制为非法人及其他组织的自然人。公司或其它组织在请求数据控制方提供或转让被控制方拒绝的情况下，公司或其它组织不能以数据可携带权为理由，只能依据《反垄断法》的规定来保护自己的利益^[7]。我国《反垄断法》第6条规定，具有市场支配地位的经营者，不得排除、限制竞争，不得滥用市场支配地位。《反垄断法》第十七条规定了7种滥用市场支配地位的行为，而第3种“无正当理由拒绝与对方交易”，则可以作为数据控制者拒绝公司的数据获取和转移要求的法律根据。如果具有市场支配地位的数据控制者不满足企业对数据可携带权的要求，则有可能被认定为滥用市场支配地位，依据《反垄断法》对其进行制裁。

数据可携带权的义务主体是对个人信息具有决定权的信息控制者，也就是信息主体要求提供存储、转移个人信息服务的对象。欧盟《一般数据保护条例》(GDPR)对数据控制者的规定过于笼统，尽管它对涉及公共利益的数据控制者进行了豁免，但却没有充分考虑到中小企业的合规负担和运营成本。所以，在我国建立数据可携带权制度时，应充分考虑到这一问题。笔者认为，应当对数据可携带权的责任主体范围进行适当的收缩和调整，以避免上述的执行障碍，因为数据可携带权会增加企业的遵从成本。在此基础上，可以根据所占的市场份额大小，分别对大、中、小三类企业的合规义务进行相应的审查；另外，在具体的执行上，也可以给予中小型企业足够的时间去达到遵守规定的要求，或适当地减少或取消其数据携带义务，从而降低其遵守规定的负担，降低其运营成本，并推动其竞争与创新。

(2) 数据可携带权的权利范围

信息主体请求获取或转移的个人信息，除必须满足“基于信息主体同意或履行合同的自动化处理”、“与信息主体有关并由信息主体提供”这两个条件以外，还“不得对他人的权利与自由造成不利影响”、“不得与商业秘密或知识产权等产生冲突”^[8]。

首先，在“以当事人同意为基础进行自动处理”的情形中，存在着两种情形：一是在不受人干扰的情况下，要求提供的信息是以当事人同意为基础进行的自动处理；二是在不考虑人为介入的情况下，将被请求的个人信息作为一项契约，由被请求方自动地进行处理。

其次，以“与受托人相关且由受托人提供”为前提，进一步限定了受托人的数据可携带权的范围。该条件有两个前提：第一，申请的个人信息必须与被申请的人有关，并且可以通过合理使用的对特定的自然人进行识别。在“匿名信息”和“假名信息”这两个概念中，“匿名信息”指的是自然人故意隐瞒自己的身份，通过一定的手段，无法确定其真实身份，因而不属于信息载体的权利；然而，“假名信息”能够借助其他信息来确定自然人的身份，将其“假名化”能够更好地保护个人隐私，增强数据传输的安全性，因而，“假名信息”应被纳入信息载体的权利范畴。除与被请求者有关外，还需要被请求

者的信息是被请求者所提供的。因此，数据控制者对数据主体所提供的个人数据进行了二次加工处理而得到的衍生数据，并不在数据可携带权的保护范围之内。

再次，“不得对他人的权利和自由造成负面影响”这一限制，是对信息主体所请求的个人信息涉及第三方的信息或权利时的处理。在我国的信息可携带权立法中，应该明确地规定，在信息主体所请求的个人信息中，包括了第三人的个人信息，而且是不能被分割出来的，那么信息主体就需要得到第三人的同意，不然的话，信息控制者就可以不履行自己的义务。为便利信息主体行使信息可携带权，我国法律可以在这里循序渐进地设定“第三人同意机制”，以简化在这种情形下的个人信息获取和转移。

最后，我国立法规定中必须明确信息可携带权需受到商业秘密与知识产权的限制。《一般数据保护条例》中并没有明确指出，数据可携带权是以商业机密和知识产权为限的。但是，在第二十九工作组发布的报告中，对数据可携带权和商业秘密、知识产权两者之间的平衡进行了指导规定：一方面，数据主体应当保证数据的转移和使用不会侵犯他人或企业的知识产权。另一方面，要对数据控制者以侵犯知识产权为由，拒绝向数据主体提供其相关的信息进行严格的控制，如果数据控制者以侵犯知识产权为由，拒绝提供相关的信息，则需提供相关的证据。侵犯商业秘密与知识产权，是一个很大的打击，特别是对那些以专业处理与分析个人信息为业务模式的公司，更是一个很大的打击[9]。所以，在我们的法律中，在数据可携带权的立法规定中，一定要对该权利的行使做出明确的规定，并对其实施细则进行详细的规定，尽量减少信息可携带权与商业秘密、知识产权之间的冲突，从而推动企业的创新发展和公平竞争。

4. 结论

个人信息流通与交易的两难境地，主要表现在个人信息权利的利益多元化与权利主体的错位。利益多元化指的是，经过挖掘、处理和分析后的数据，承载着三方甚至更多的人格和财产性权益。责任主体错位，即个人信息主要是由个人信息主体生成的，但在很多时候，还是需要依靠个人信息处理者来完成流转。可携性权利的建立，为各方利益的均衡创造了新的契机，然而，在信息拥有者与信息处理者这两个极端不均衡的环境下，其对于增强个人信息拥有者的控制能力所能起到的作用却是微乎其微，更谈不上改善网络平台上“积重难返”的不公平竞争与垄断现象[10]。可携带权已经被立法所确定，但在解释论中，必须对其本质及构成进行明确，以实现对个人权益的法律规范的理性期望。虽然可携带权具备了积极的行权条件，但是它的归属体系决定了它自身具有人格性利益的防御属性，这也决定了它的行权范围和内容都会受到社会公共利益和其他第三方主体权益的影响和限制。

在《个保法》背景下，构建数据可携带权制度，既要考虑一般制度，又要考虑不同行业的具体做法，要将个人信息保护主体视为可携带权的行使主体。在具体的实施细则中，可以将强制性义务和倡导性规范与行业标准结合起来，对可携带权的规则体系进行调整，对可携带权的个人信息的范围进行界定，探讨不同行业和场景下的可携带权的标准化适用，在保障个人信息主体的主导性、维护个人信息权益的同时，发挥出可携带权更多的工具性效能。

参考文献

- [1] 刘利平. 个人信息侵权法保护的价值与理据新论——基于大数据悖论的分析视角[J]. 重庆大学学报(社会科学版), 2022, 28(5): 221-234.
- [2] 王泽鉴. 人格权的具体化及其保护范围·隐私权篇(中)[J]. 比较法研究, 2009, 1(1): 1-20.
- [3] 李雨涵. 算法歧视法律规制研究[D]: [硕士学位论文]. 广州: 广州大学, 2020.
- [4] 周汉华. 探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向[J]. 法学研究, 2018(2): 3-23.
- [5] 姚佳. 企业数据的利用准则[J]. 清华法学, 2019, 13(3): 114-125.
- [6] 王利明. 论个人信息权在人格权法中的地位[J]. 苏州大学学报(哲学社会科学版), 2012, 33(6): 68-75.

-
- [7] 刁胜先, 李纯芬. 欧盟数据可携权的困境与本土化思考[J]. 重庆邮电大学学报(社会科学版), 2020, 32(2): 68-77.
- [8] 尚海涛. 论我国数据可携权的和缓化路径[J]. 科技与法律, 2020(1): 86-94.
- [9] 卓力雄. 数据携带权: 基本概念, 问题与中国应对[J]. 行政法学研究, 2019(6): 129-144.
- [10] 申卫星. 论个人信息权的构建及其体系化[J]. 比较法研究, 2021(5): 1-13.