数据可携权的建构与隐私保护

高宁宁

（西南政法大学， 重庆 401120）

摘要：数据可携权有助于打破用户“锁定效应”和增强个人数据控制。数据主体行使数据可携权的过程中可能会因为服务提供商的管理不当而导致数据主体的隐私遭受侵犯，在保护隐私的方式下强化数据转移实体、数据接收实体、请求数据可携的数据主体三方义务，并明确违反义务时承担的责任，保障数据主体行使数据可携权，有利于促进数据可携权在隐私保护下的持续发展与完善。在保护隐私的同时构建数据可携权，为人们提供前所未有的信息控制可能性，并且有效支持服务提供商充满活力的持续创新和在线竞争。

关键词：数据可携权；数据转移权；个人信息；隐私；

Construction of Data Portability under Privacy Protection

GaoNingNing

Abstract:Data portability helps to break user “lock-in effects” and enhance personal data control. In the process of exercising data portability of the data subject, the privacy of the data subject may be violated due to improper management of the service provider. In the manner of protecting privacy, strengthen the data transfer entity, the data receiving entity, and the data subject requesting data portability The three parties' obligations, and clarifying the responsibilities they assume when violating their obligations, guaranteeing the data subject to exercise the right of data portability, is conducive to promoting the continuous development and improvement of relevant laws and regulations related to the right of data portability. While protecting privacy, building data portability, providing people with unprecedented information control possibilities, and effectively supporting service providers' dynamic, continuous innovation and online competition.

Key words: Data portability　Right to data transfer　Personal data　Privacy protection

（责任编辑：侯净雯）

引言

在信息化浪潮席卷之下，国与国之间的竞争将取决于对信息的占有程度，谁占据了信息优势，谁就占领了政治、经济、军事、文化的制高点”。在互联网产业迅猛发展期间，为了构建欧洲数字化单一市场并促进欧盟数字经济发展，欧盟地区需要通过法律手段来削弱境外企业已有的优势，力求打造一个更加公平竞争的市场环境，从而促进本土互联网企业的发展。设置数据可携权实际上是欧盟为了减少垄断力量和改善市场竞争，促进本土产业的发展。落后的企业发展，成为数据可携权产生的动力之一。

数据可携权是建立在保护基本人权和隐私的基础之上的。在欧盟范围内的法律，数据可携权的一个重要理由是实施与隐私相关的人权。数据自由流通和交易会极大的促进经济社会的发展，数据可携权便是增强数据流通和数据利用的一种方式。允许数据可移植性可以使企业和数据主体能够最大限度地利用平衡和透明的方式进行数据处理，从而减少不公平或歧视性做法，降低将不准确的数据用于决策目的的风险，实现企业和数据主体的共赢。2005 年欧盟实施一项针对 28000 名欧洲民众的调查显示，超过三分之二的民众更希望在个人数据的存储和转移上有更高的便捷性，欧洲民众认为其个人数据的控制力仍有待加强。个人数据高水准保护的社会要求，成为数据可携权产生的又一动力。

数据可携权一直都在处于规划和演变过程，其被作为一种法定权利是势不可挡的趋势。1995 年《欧盟数据保护指令》没有规定数据可携权，但是 12 条规定了数据访问权是数据可携权诞生的前提性权利。欧盟委员会在 2012 发布的《个人数据保护指令》建议稿第十五条中首次引入了“数据可携权”，标志着数据可携权正式进入欧盟立法进程。2013 年欧洲议会下设的公民自由、司法和内政事务委员会提出将数据可携权作为数据访问权的具体内容并入第 15 条规定之中。2014 年 3 月，欧洲议会通过 GDPR 草案修改稿，采用该建议，也是将其作为数据访问权的具体内容予以规定。2015 年确定将该权利作为独立的一项权利规定于 18 条。2016 年 5 月 4 日 GDPR 将数据可携权规定于第 20 条正式公布。

之所以成为一种权利，赋予其法定性，以权利形式在法律中规定并设置相应的配套措施。为了数据控制者侵犯数据主体的数据可携权时，司法机构可直接予以法律保护。如果未规定为一种法定权利，则须满足侵犯行为的违法性，也即证明保护该项利益的正当性才有可能获得司法救济。在欧盟数据体系中，赋予数据主体一种积极主动地支配权利数据可携权是符合当时欧洲民众对个人数据保护的要求。

一、数据可携权的提出

（一）数据可携权的概念

为了加强对个人数据的控制，欧盟将数据可携权作为一种新型权利引入，在GDPR第20条予以规定。数据可携权指当数据控制者基于数据主体的同意或者基于合同的约定，以自动化的方式处理个人数据时，数据主体有权获取其提供给数据控制者的数据副本（副本获取权）;同时有权不受原数据控制者阻碍地将个人数据转移至另一个数据控制者(数据转移权)。欧盟GDPR规定的数据可携权是以“信息自决”为理论基础的个人信息保护模式。“信息自决”源自于德国的“人口普查法案”的判决中，由于该案在立法、司法以及学术研究上的重大影响，其也因此被德国国内学者、法院和国外比较法学者反复参引。信息自决权的精髓在于信息主体对自身信息的控制与选择，即自我决定的权利。GDPR设置数据可携权这一新型权利，一方面强化了数据主体对个人数据的控制，降低数据主体在选择服务提供商时获取数据及转移数据的成本;另一方面在赋予数据主体数据可携权下施加给数据控制者和数据处理者更严格的数据保护义务。

（二）数据可携权的权利架构

1、数据可携权的主体 （1）数据可携权的权利主体。 GDPR第一条第二款“该条例保护自然人的基本权利和自由，尤其是他们个人数据受到保护的权利”。欧盟制定的条例GDPR中所规定的数据可携权，欧盟境内的自然人均可成为数据便携权的主体。关于欧盟境外的适用主体，GDPR第三条规定如果欧盟境内企业为境外的用户提供商品或者服务，那么由于这些企业受欧盟成员国法律的约束，负有满足法定条件时进行数据处理的义务，此时即使是在欧盟之外使用欧盟境内企业提供的商品和服务的自然人而言，也同样可能成为数据可携权的主体。（2）数据可携权的义务主体。 欧盟《一般数据保护条例》适用整个欧盟地区，所以欧盟境内的数据控制者当然成为数据可携权的义务主体，对于欧盟境外的数据控制者在以下两种情况同样受到条例的约束。第一种情况：数据控制者在欧盟境外领域但其在欧盟境内存在设立机构。欧盟境内设立机构的数据处理行为不仅要受到该条例的约束，该设立机构的数据控制者和处理者所实施的数据处理行为同样受到该条例的约束。第二种情况：欧盟境外数据控制者或者处理者在欧盟境内不存在设立机构，但是对欧盟境内数据主体提供有偿或者无偿的商品或者服务；或者涉及对数据主体在欧盟境内发生行为的监控，其所实施的数据处理行为要受到GDPR的约束，该数据控制者和数据处理者均为数据可携权的义务主体。

2、数据可携权的客体。 根据GDPR第二十条的规定，可以得知数据可携权的权利客体是以个人数据为核心。从来源上进行限定是数据主体主动提供的个人数据，也就是说将数据控制者基于合法授权而获得的个人数据以及数据控制者基于该服务的使用用途而推断出的数据排除在数据可携权的范围外，比如服务提供商基于监视和分析用户行为过程中而形成的数据。界定个人数据范围的核心标准就是“已识别或者可识别”，判断一个人是否可识别，需要考虑“所有合理可能的方法”。这就意味着对个人数据可识别性的判断是一个动态的过

程，包括直接识别方式和间接识别方式。个人数据的范围虽然极其广泛，但是并不是所有个人数据都具有可携性，也不应将所有个人数据都纳入可携性的范围内。针对涉及使用服务的个人数据，将那些技术上容易获得但是又很快被删除的数据，纳入数据可携权的范围内对于数据控制者来说具有一定的挑战。而对于数据控制者或者数据处理者仅仅为方便可携而保留的个人数据，不属于数据可携权的权利客体。

3、数据可携权的行使条件。 GDPR 指出数据主体获取并转移个人数据的处理行为其前提是基于数据主体的同意或者合同等合法理由，其方式必须采取自动化处理实施的。这两个条件必须同时满足。根据 GDPR 规定数据可携权仅适用自动化处理的信息。数据主体有权无障碍地将这些数据传输给另一个数据控制者，狭义解释认为无障碍是指数据控制者的消极义务，即不得设置障碍以阻止用户将数据传输给另一个控制者。除此之外，还规定了一种在技术可行的情况下直接传输的特殊数据转移权。这种情况下，数据主体无须从一方数据控制者处先下载再传输至另一数据控制者，而是通过控制者所提供的技术接口直接实现数据转移，使得数据转移更加便捷。数据可携权在内容上类似于所有权人基于自由意志而做出的物权转移过程，个人数据的转移与物的空间位置移动二者在法律性质方面并无大异。

二、数据可携权与隐私保护的冲突困境

数据可携权包括两方面的内容：副本获取权和数据转移权。副本获取权是指从数据控制者处得到个人数据复制件并将其存储在私密的设备中以备再度使用的权利。数据可携权与数据访问权之间最核心的区别就在于数据转移权。即无障碍地将数据主体的个人数据一个控制者处转移至另一控制者处。数据可携权将副本获取和数据转移的权利回归于数据主体本身，加强用户对数据控制权利的同时进一步降低数据主体更换数据服务商的成本。数据可携权在一定程度上有助于澄清数据权属，即数据控制者对个人数据不具有控制权，仅具有配合义务，由此避免控制者争夺用户数据，促进数据流动。

对隐私的保护需求作为一种人类的自然情感，来源于人类的羞耻本能。社交网络和通讯方式的更新变革使得个人与社会的关系愈发紧张，公共领域、数据服务平台、周围人窥视欲望对于个人私生活领域的干扰和侵入，人们对于避免其私生活遭受公开的权利诉求日渐高涨。这对个人隐私法律保护提出了要求。在我国民事立法中，《中华人民共和国民法典》第一千零三十二条规定隐私权，第一千零三十四条规定个人信息的保护，形成了隐私保护与个人信息保护平行并立的结构，有将隐私权和个人信息保护相互独立的倾向。但司法裁判中，法院倾向于将二者相结合，放在隐私权的框架内去保护个人信息。这种情况有点类似于在将原本只具有消极权利特征的传统隐私权设计为具有积极权利特征的现代隐私权。有的法院将个人信息等同于隐私，有的法院认为个人信息的保护是隐私权保护范围不断扩大的结果，也有法院认为保护路径的差异并不影响对个人信息在个案中进行的具体保护。王利明教授认为个人信息与隐私之间属于交叉关系，涉及个人私密生活的信息属于隐私，个人信息因为高度公开就当然不列入隐私的保护范围。笔者也赞同该观点。

数据可携权增加了控制和处理个人数据的复杂性，个人数据在数据控制者之间传输的过程隐私安全设置较低，且传输过程的不透明使数据主体无法有效掌控个人数据的泄露风险。数据可携权虽然并未禁止数据主体转移有关他人的数据，但是被转移的信息可能关涉第三人。数据可携权下无论是自然人获取数据还是数据控制者之间的数据转移都是十分便捷，对个人信息以及涉及相关隐私造成一定的威胁。二者的冲突集中体现在涉他数据的转移，与搜索、购物等以满足用户自我需求为目的的服务不同，社交网络具有天然的涉他性。涉他数据多集中于社交网络，比如用户 A 想要将自己的微信账号中的通讯录或者好友的联系方式，日志等个人数据转移至 QQ 中，A 是否可以未经通讯录好友的同意将其在微信中的个人数据转移至 QQ,如果 A 将涉他数据转移至另一数据控制者，与该数据有利益关系的第三方认为其隐私被侵犯，可否请求相关机构认定数据接收者构成“非法收集信息”。因为在涉他数据的转移过程中，A 并未取得该涉他数据直接利害关系第三人的同意，即违反 GDPR 中规定的个人信息收集的基本原则——同意。知情同意原则是信息管理者在收集个人信息时，应当对信息主体就有关个人信息被收集、处理和利用的情况进行充分告知，并征得信息主体明确同意的原则。社交网络中的涉他数据在 Facebook 白皮书中称为“社交图谱”，即可携的数据中数据所有者与该数据中其他人和实体之间的联系。社交网络的核心功能就是允许用户与他人联系并创造共享体验。但是在社交图谱可携的过程中伴随着重要的隐私问题。

三、数据可携权与隐私保护冲突下的三方实体义务分配

（一）数据转移实体

数据转移实体在保护隐私的前提下进行数据可携，主要负有以下义务。第一数据泄露报告义务。数据控制者在发生数据泄露事故时及时向有权监管机构报告，并在某些必要情形下告知涉事数据主体。第二数据系统保护和默认保护。数据控制者在设计新型处理技术、产品或服务的过程中和正式处理过程中都要考虑到数据保护问题并且对其可能带来的风险进行评估以确保该处理符合 GDPR 的规定，保障数据主体的基本权利与自由。第三审查义务。数据转移实体基于其与数据接收实体相当的地位，其有能力和资源为数据主体审查数据接收实体的真实性和安全性，是否有适当的隐私策略，施加这种审查义务于数据转移实体并不会给其带来难以实现和承受的负担。服务提供商可能会探索工具来帮助用户了解下载数据的安全风险和协议。

（二）数据接收实体

数据主体要求转移个人数据时，数据接收实体必须确保他们只接收与其向请求用户所提供的的服务中必需和相关的数据。在数据可携过程中，数据转移方不能够切实审查所有潜在的接收方，为了保护数据转移的安全降低滥用数据的风险，需施加给数据接收方证明义务：1 证明在数据可携性请求下接收个人数据的目的和用途的正当性和合理性;2 证明按照适用的法律和数据保护要求处理数据[①]。在数据传输后，数据接收实体必须根据 GDPR 规定处理和保护其接收到的个人数据。保护数据的责任仅由接收方承担，而数据转移实体不负责数据

主体或者个人数据的其他潜在接收者处理的数据。有关数据可携权产生的数据准确性和质量责任，数据传输之前和过程中由数据转移实体负责，传输后由数据接收实体负责安全性及风险分担。数据传输方不应对与所移植数据的准确性和质量有关的索赔负责，除非证明数据是在传输方的控制下被损坏。

（三）请求数据可携的数据主体

数据主体作出知情同意是实现数据可携的前提，转移实体应当采取适当的措施确保个人数据转移过程的安全，但是传输实体仍应使数据主体“了解”，使其能够采取适当步骤的措施。对于未请求数据可携而被传输的个人数据，存在着复杂的责任问题。数据可携权的数据主体请求涉他数据可携的过程中可能会将未请求数据可携的第三人的数据共同传输，而对数据主体行使数据可携权施加过多的义务会大大降低对数据可携权的兴趣，尤其是在社交网络中对社交图谱的可携权。因此在只涉及真正不合理或者鲁莽情况的行为对该数据中的第三方造成不可恢复的情况，请求用户才需要承担相应的责任，更有利于数据可携权的构建。例如故意将联系人的数据传输给明知有数据滥用或者数据保护措施不力的一方，数据主体应承担数据保护的责任。

四、隐私保护方式下构建数据可携权困境之破解

个人自决权和控制个人数据的权利特别源于隐私权和人格尊严。为了保护个人隐私和人格尊严，个人数据不应视为纯粹意义上的物而采取相同或相似的措施，在处理个人数据时采取必要的安全保障措施，以确保个人数据的安全转移至正确的目的地，但安全保障措施的实施不得妨碍用户行使其权利。

（一）设置身份认证模式

数据便携权可以增强数据控制者对数据的控制，但是另一方面可能会增加控制和处理个人数据的复杂性，增加数据主体的隐私和数据安全风险，对审查方面提出更高的要求，提出实施身份认证和程序确保隐私和数据安全。WP29（欧洲数据保护委员会前身）在指南中指出，在任何情况下，数据控制者必须执行身份验证程序，可以要求数据主体提供合法身份证明，但指南并未详细说明评估身份认证的标准。数据控制者有责任采取全部必要的安全措施，不仅要确保个人数据被安全地传输（采用点对点传输方式或者数据加密方式）至正确目的地（利用强认证措施），还要继续保护存储在其系统内部的其他个人数据，并且还需采取透明程序应对数据泄露潜在风险，数据控制者认证数据主体的身份，采取风险缓解措施。但是，这些安全措施不得具有阻碍性，不得妨碍用户行使其权利。

（二）强化技术保障措施

在处理个人数据过程中要采取适当的、必要的技术和组织措施来实现处理行为的合理合法化，同时还要确保数据主体的基本权利与自由尤其是隐私得到保障。涉他数据的转移对第三人的隐私将构成极大的威胁，这种特殊数据主要存在于社交网络上，社交平台建立了“社交图谱”，涉及众多用户相关信息的数据。最有希望使社交图谱数据实现可携性的途径，可

以向接收实体隐藏数据主体的 ID，个人数据转移至数据接收实体后，仍然提供给数据主体重建其社交图谱的能力，即将之前加密模糊处理的数据进行恢复，从而避免不必要地暴露个人信息，侵犯数据主体和第三人的隐私。但是这项举措需要强大的合作性技术措施，应建立易于使用的数据处理技术，以促进应该遵守适用的法律。尽可能向数据主体提供对自己的个人数据安全的在线访问，在设置默认的技术要求时，应选择隐私友好的标准配置。无论是匿名化处理、假名化处理，均是通过采取特定的技术手段来消除或代替个人数据中的敏感属性（数据中的敏感属性），是一种隐私增强技术。

（三）规定数据留存期

数据可携权并未规定数据控制者有义务将个人数据保留的时间必要或者超过任何指定的保留期限。重要的是，除仅为了满足未来任何潜在的数据可携请求之外，不需要额外的将数据保留超过所适用的期限。个人数据中包括个人敏感信息和一般个人信息时，数据转移实体可采取区分原则，区分个人敏感信息和一般个人信息的数据留存措施，设置不同的数据留存期。由于个人敏感信息的处理可能为数据主体的利益、权利和基本自由带来风险，所以针对个人敏感信息的保障措施应多加防范。数据转移方在数据主体要求行使数据可携权，进行数据转移，此时如果数据主体没有主张删除权，要求数据转移实体删除数据，数据转移实体可以保存该数据一定期限。为防止数据丢失以及不可恢复，原有数据转移实体留存数据是很有必要的，但是其留存数据的目的与手段需符合比例原则，防止数据被过度使用。尽可能采取向数据主体提供对自己数据的安全在线访问，使得数据主体能够将自己的数据带向自己选择的另一个数据提供者，或者保留数据本身。数据控制者、数据处理者所留存的数据应保持已传输的数据同等质量，并得到同等程度的安全保护。

五、数据可携权本土化：基于隐私保护的再思考

欧盟 GDPR 所规定的数据可携权本身存在的问题：欧盟数据可携权不具有完备的法律体系和执法规范、模糊的概念分析、对知识产权和公平竞争的破坏以及对数据安全的威胁。欧盟提出数据可携权的目的之一就是削弱以美国为首的互联网巨头的数据垄断带来的优势，促进欧盟本土企业的发展从而减少互联网产业之间的发展差距。我国互联网企业的发展正处于上升趋势，如果贸然引入数据可携权，可能会施加给企业过多的负担，数据可携权的成本远远高于给我国互联网领域带来的福利。加之我国的数据保护法律体系不健全，数据主体的保护意识薄弱，更应该以审慎的态度对待。GDPR 的数据可携权意义在于数据主体权利的增强，促进市场竞争，具有极为重要的意义。但是其在具体操作层面，该条款还有待进一步具体细化的部分，比如关于涉他数据的获取，GDPR 序言（68）仅宣示性地指出获取涉及第三人的数据时应当无差别地保护他人的权利和自由，但对于具体的解决机制并未明确。

我国目前关于数据、个人信息保护相关法律尚未形成完整统一规范的法律体系，对个人信息和个人数据的保护仍以刑法、各类法规、规章规定为主。数据可携权属于个人信息权的一部分，应将其认定为个人信息权的子权利。用隐私换便利的说法虽然引起很多人反对，但

是切实反映我国大众数据保护意识相对薄弱，比如大多数 APP 功能的使用都要经过手机用户的授权，勾选同意用户协议与隐私条款，如果不同意网络服务提供商的隐私条款，用户则无法继续使用该 APP。“被授权”“被同意”的情况比比皆是。在这种运营模式下，大多数用户都选择同意条款，或许是出于用户的知情同意，也或许是面对强大网络服务提供商的被迫同意。这背后反应的是我国的个人数据保护在实践层面的缺失以及我国数据保护意识相对薄弱，欧盟通过大量的数据保护法律将数据保护意识进行提高，GDPR 对个人数据权利的监管以数据主体投诉为主，数据监管部门辅助的模式。贸然引入适用基础优于我国的欧盟数据可携权，不仅可能无法加强数据主体对个人数据的控制，还可能会造成恶性市场竞争，威胁数据安全。

结语

数据可携权自问世以来，对个人数据安全和互联网产业发展的影响尚未稳定。笔者认为，欧美国家在其社会经济背景之上创制的数据可携权相关法律法规和司法实践不能直接成为数据可携权本土化的正当依据。我国可以在充分了解数据可携权制度的基础上，结合当前立法实际，在将来的立法与司法实践中充分吸收其精神，并加以改进，以加强对个人信息的保护和促进数据市场的良性竞争。

参考文献：

[1]. 齐爱民.信息法原论[M].武汉: 武汉大学出版社.2010:55.

[2]. 苗振林.欧盟数据可携权立法评析[J].许昌学院学报,2018,37(05):83-87.

[3]. 张建文.新兴权利保护的基本权利路径[J].河北法学, 2019, 37(02):18-30.

[4]. 张哲.探微与启示:欧盟个人数据保护法上的数据可携权研究[J].广西政法管理干部学院学报.2016,31(06):43-48.

[5]. 闫静.信息自决权理论下的档案隐私保护路径探析[J].档案学研究.2016(01):80-85.

[6]. 张哲. 欧盟个人数据保护法上的数据可携权研究 [D].西南政法大学,2017.

[7].齐爱民, 张哲.识别与再识别:个人信息的概念界定与立法选择[J].重庆大学学报:社会科学版.2018,24(02):119-131.

[8]. 陆青.个人信息保护中“同意”规则的规范构造[J].武汉大学学报:哲学社会科学版.2019,72(05):119-129.

[9]. 金晶.欧盟《一般数据保护条例》:演进、要点与疑义[J].欧洲研究.2018,36(04):1-26.

[10].张新宝.从隐私到个人信息:利益再衡量的理论与制度安排[J].互联网金融法律评论.2015(02):16-21.

[11].李永军.论《民法总则》中个人隐私与信息的“二元制”保护及请求权基础[J].浙江工商大学学报.2017(03):10-21.

[12].张建文,高悦.从隐私权的立法与司法实践看新兴权利保护的综合方式[J].求是学刊.2019,46(06):102-111.

[13].王利明.论个人信息权的法律保护——以个人信息权与隐私权的界分为中心[J].现代法学.2013,35(04):62-72.

[14].张才琴, 齐爱民, 李仪. 大数据时代个人信息开发利用法律制度研究[M]. 北京:法律出版社,2015:142.

[15].程海玲.108 号公约现代化与个人信息收集合法性依据的重构[J].时代法学.2019,17(06):107-115.

[16].周杰.比例原则下电子通信数据留存之限度——《欧盟 2006/24 号指令》无效案[J].苏州大学学报(法学版).2018,5(03):150-160.

[17].冉从敬, 张沫.欧盟 GDPR 中数据可携权对中国的借鉴研究[J].信息资源管理学报.2019,9(02):25-33.

[18].谢琳, 曾俊森.数据可携权之审视[J].电子知识产权.2019(01):28-39.