# 大数据时代下欧盟数据可携带权的风险和启示

吕思祺
（复旦大学　法学院，上海　200438）

**摘　要：**数据可携带权是欧盟于2018年生效的一项新兴权利，允许数据主体不受阻碍地将个人数据传输给另一个数据控制者。研究数据可携带权对我国个人数据保护体系的建构、国内互联网企业走向国际市场都将起到积极促进的作用。通过对欧盟《一般数据保护条例》中的立法规定及其实施现状进行分析，发现该条款实质上已沦为僵尸条款，并未发挥预期的功能。我国在《中华人民共和国个人信息保护法》中确立了此项权利，在后续相关制度规定时应当参考欧盟经验，对数据可携带权的客体范围进行限缩，加强政府部门分层级监管，实现数据可携带权的中国本土化。

**关键词：**数据可携带权；一般数据保护条例；数据保护；个人信息保护；数据安全治理
**中图分类号：**D913　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2023.08.001
**引用格式：**吕思祺. 大数据时代下欧盟数据可携带权的风险和启示［J］. 网络安全与数据治理，2023，42(8)：1-5，12.

# Risks and insights of EU data portability in the era of big data

Lv Siqi
（School of Law，Fudan University，Shanghai 200438，China）

**Abstract：**The right to data portability，introduced in the European Union in 2018，empowers data subjects to transfer personal data unimpeded to another data controller. An investigation into this emerging right contributes positively to the construction of China′s personal data protection system and propels domestic internet enterprises onto the global stage. By scrutinizing the legislative stipulations in the EU General Data Protection Regulation and examining the current status of its implementation，it is discerned that the provision essentially operates as a dormant clause，failing to deliver its intended function. As China has enshrined this right in the Personal Data Protection Law of the People′s Republic of China，it should draw upon the EU′s regulatory experiences. This includes limiting the scope of the right to data portability，strengthening hierarchical oversight by governmental departments，and actualizing the localization of data portability rights within China′s jurisdiction.

**Key words：**right to data portability；GDPR；data protection；personal data protection；data security governance

www.pcachina.com

## 0　引言

大数据时代改变了人类的生活和工作方式，同时也给个人数据和隐私的保护带来了更大的挑战。2016年，欧盟出台的“史上最严数据保护法律”——《一般数据保护条例》（General Data Protection Regulation，GDPR）中引入了名为“数据可携带权”的制度，使数据主体能够不受阻碍地将个人数据在不同数据控制者之间传输。这一权利旨在促进个人数据在欧盟内的自由流通，避免个人数据的“锁定”，让用户能在不同的数据控制者之间便捷自由地切换，以鼓励市场竞争[1]。然而，制度运行在具体实践中却出现了诸多问题：由于条文规定含糊、标准不统一、技术可操作性较差等问题，其实际上并没有给数据安全和市场公平竞争带来积极意义，而最终沦为僵尸条款。本文将针对以上问题展开论述，探讨该制度的缘起、发展及现实困境，以期为我国未来的立法实践提供参考。

## 1　理论缘起与制度设计

### 1.1　数据可携带权的缘起

作为欧洲数据战略的一部分，欧盟致力于构建“单一的数据市场”，确保其成为数字化和人工智能方面的全球领导者，并提出通过数据战略的实施，欧盟27国的数据经济总量将从2019年的3 250亿欧元（约占当年GDP的2.6%）提升至2025年的5 500亿欧元（约占当年GDP的4%）。因此，在数据经济时代的背景下，对数据控制和流转的监管显得愈发重要。

数据可携带权的诞生有迹可循。1980年，经济合作

与发展组织为了打破数据国别保护的非关税贸易壁垒、促进数据跨境流动，通过了《经合组织隐私保护和个人数据跨境流动准则》，成为倡导数据跨境流动的始祖。1981 年，欧洲理事会（The European Council）通过了《与个人数据自动化处理有关的个人保护公约》（European Treaty Series），旨在实现成员国之间的数据跨境共享。1995 年，欧盟出台的标志性法律——《欧盟个人数据保护指令》（EU Directive 95/46/EC）第 25 条规定：数据接收国只有达到欧盟所认可的条件才可以进行数据转移，从而建立了较高的数据保护标准。然而，随着互联网和物联网的兴起，碎片化的个人数据在传输时风险增大，原有的规定逐渐无法应对新时期信息安全的需要。由此，“数据可携带权”的概念应运而生。

这一概念最早由欧盟委员会于 2012 年 1 月在 GDPR 建议稿中提出，该稿第 18 条赋予用户将其个人数据传输给另一个数据控制者的权利。欧洲议会在审查后认为数据可携带权应当被视为是访问权的延伸，而不是单独的一项权利，因此其在 2014 年 3 月通过的 GDPR 修正案中将数据可携带权与访问权合并。但反对合并者认为两种权利之间存在明显不同：访问权的范围比数据可携带权的范围更广，且数据可携带权要求事先存在一个企业即时通信系统（Enterprise Instant Messaging，EIM）以便数据输出，访问权则不做此要求[2]。在双方激烈讨论后，考虑到数据可携带权旨在加强数据安全治理，确保个人数据在成员国之间自由流动，而访问权无法涵盖“数据转移”的权利内容，因此决定将前者作为一个单独的条款在 GDPR 中保留下来。

### 1.2 数据可携带权的应用

欧盟为推动数据可携带权的实施出台了配套规定。2016 年 4 月，欧盟委员会发布了一份名为“数字单一市场的 ICT 标准化优先事项”（ICT Standardization Priorities for the Digital Single Market）的公报，宣布将从 2016 年起，增加专门用于数据互操作性标准的研发和创新的投资，以实现跨部门的数据整合。欧盟第 29 条数据保护工作组（Article 29 Data Protection Working Party）曾在《数据保护官指南》（Guidelines on Data Proteciton Officers，以下简称《指南》）中指出，“如果没有互操作性的标准，数据可携带权注定是一个原则声明，而不会成为数据时代下个人自决的真正和有效的工具。”可见，互操作性标准的制定及其可行性是保证数据可携带权实施的前提。

《指南》强调，互操作性（Interoperability）不等于兼容性（Compatibility），后者实际上要求原数据控制者承担更加沉重的义务：数据发出方需要修改被转移数据的格式，以保证其符合接收方所使用的处理系统的要求。因此，相较于“兼容性”所包含的单方面责任，“互操作性”门槛较低，更强调双方共同的责任：发出方和接收方都有义务确保数据的顺利传输，前者发出的数据应当采用通用格式，而后者则需要将数据处理成其系统所采用的格式。为了满足“互操作性”的要求，数据控制者应当开发相应的下载工具和应用程序编程接口（Application Programming Interface，API），以确保其他系统或应用程序（Application，APP）能与其通畅连接并传输数据。这是因为 API 不同于一次性传输（One-off Exports）：一次性传输的工作原理是将用户作为中介，需要用户将其在一个 APP 中的数据下载下来，然后再上传至另一个 APP，这一过程类似于使用 U 盘进行数据传输，每次传输可能会花费数天甚至数周，效率很低。而在使用 API 的情形下，数据发出方与接收方保持持续连接，无论用户使用哪个 APP 添加或删除数据，其操作都会实时共享给另一个 APP，因而所需的传输时间更加短暂。文献［3］指出，API 允许用户在不放弃原有服务的情况下更换服务，可以帮助数据接收方节约储存成本，也可以提供更快更便捷的传输途径。

欧盟对数据可携带权三易其稿的立法过程以及出台《指南》进一步完善修正的行为，侧面反映出立法者在这一权利的权属和运用上依然处于摸索的阶段。正因如此，数据可携带权在实践中遇到了许多障碍。

## 2 制度中存在的问题与现状

### 2.1 条文存在矛盾与争议

GDPR 第 20 条从三个部分规定了数据可携带权的内容：第一，数据主体有接收、存储和使用个人数据的权利；第二，数据控制者有义务依照请求将个人数据传输给另一数据控制者；第三，该权利不适用于为公共利益执行职务或行使公权力的行为，同时不得对他人的权利和自由产生不利影响。此条规定正面罗列了数据主体及数据控制者的权利义务，同时又从反面规定了除外情形，从而构建了一套看似严密完整的逻辑框架。但实际上，条文自身的含糊性以及与其他条文之间的矛盾，使得对数据可携带权行使的理解伴随着很多争议，并因此引发了一系列问题。

首先，第 20 条第 1 款中将“数据可携带权”定义为：数据主体有权以结构化的（Structured）、通用的（Commonly Used）、机器可读的（Machine-readable）格式接收其提供给数据控制者的个人数据，并有权将其传输给其他数据控制者，而不受提供该个人数据的数据控制者的阻碍。其中，结构化要求将数据依照特定的结构进行组织并储存以便查阅和使用。通用化旨在促使数据控

www.pcachina.com

制者们使用相同的数据格式，或者至少应当使用便于数据开放的格式[4]。机器可读则被欧盟正式定义为“文件格式的结构化，使软件应用程序可以很容易地识别、确认和提取特定的数据，包括个别的事实陈述及其内部结构”，如逗号分隔值（Comma Separated Values，CSV）、可扩展标记语言（Extensible Markup Language，XML）、JavaScript 对象表示法（JavaScript Object Notation，JSON）等文件格式。这三个传输数据格式的“最低要求”，实质上即是对“互操作性”要求的细化。

尽管 GDPR 第 68 条明确提出“数据主体传输或接收有关其个人数据的权利不应对控制者产生采用或维护技术上兼容的处理系统的义务”，但上述格式要求实质上逼迫数据控制者在软件开发过程中添加额外的合规模块。对于企业来说，这实际上带来了巨大的成本支出：一方面，软件开发成本需要长期的资金注入，企业需持续投入技术成本；另一方面，GDPR 第 83 条第 5 款规定，未能遵守数据可携带权要求的数据控制者将被处以最高 2 000 万欧元的行政罚款。这不仅抬高了新企业的准入门槛，也加强了头部企业的垄断。

其次，定义所说的个人数据仅为数据主体提供的个人数据。这又内在地包含了两个方面的要求：第一，数据类型是个人数据，而不是企业数据或其他类型的数据，因此任何匿名化的数据都不属于数据可携带权的范畴，即数据主体在将数据以匿名化的方式存入服务器后就无权提出数据可携带权行使的请求。而 GDPR 第 32 条提出的增强安全级别的措施包括“个人数据匿名化和加密处理”，信息的保护与权利的使用之间形成了矛盾。第二，数据必须是由数据主体提供的。数据的范围通常可以分为四个层面，即接收的数据、观察到的数据、推断的数据以及预测的数据。那么该条规定中“由数据主体提供的数据”是否仅包括接收到的数据，而忽略了其他层面？对此，欧洲数据保护监督机构呼吁应当扩大数据的范围，而不是仅限于数据主体提供的数据[5]，这样有利于加强个人对数据的控制和治理。但也有学者认为，“提供”一词指的是数据主体做出的有意识的行为，所以应当对数据的类型进行限制，以保护商业数据处理者的商业秘密和战略[6]。此外，GDPR 第 20 条第 1 款中还规定了数据主体享有数据携带权需要基于其“以一种容易理解的形式”“在书面声明的情形下做出”的同意，这给数据处理者获取“同意”设置了重重关卡。但 GDPR 允许数据控制者在“处理对于控制者或者第三人所追求的合法利益是必要的”的情况下不经“同意”就获取个人数据。在此两种选项下，数据控制者大概率会偏向后一种更加容易的方式而忽略对数据主体“同意”之意思表示的获取，从而导致数据主体无法享有数据携带权[7]。

最后，GDPR 第 20 条第 3 款中规定：可携带权的行使“不影响第 17 条的规定”，即数据主体可以同时行使可携带权和被遗忘权，在撤回其对数据处理的同意时要求数据控制者删除这些数据。GDPR 第 68 条也明确指出，“数据可携带权不应损害数据主体要求删除个人数据的权利和本条例规定的该权利的限制”，对第 20 条第 3 款进行了确认。但是，当涉及第三人时，可携带权与被遗忘权之间就产生了矛盾[8]。倘若数据主体要求转移与第三人隐私有关的数据信息，而与此同时，第三人又主张被遗忘权，要求删除与其有关的数据，那么数据控制者就陷入了一个既不能转移又不能删除数据的两难境地。

### 2.2 实践中存在的风险与挑战

如前所述，欧盟创设数据可携带权主要为了实现三个目标：数据主体更好地实现对其个人数据的控制以保护个人信息及隐私，促进数据控制者之间的公平竞争以推动创新；以及实现欧盟内数据的自由流通，增强欧盟在数据安全治理领域的头部作用。但事实上，数据可携带权的发展可能正与其追求的目标背道而驰。

#### 2.2.1 无法更好地保护个人信息安全

早在 1999 年，数据可携带权还没有从访问权发展而来之时，联邦贸易委员会（Federal Trade Commission）下设的关于访问和安全的咨询委员会在其报告中就称，“访问和安全之间存在着非常真实的紧张关系。”而数据可携带权的发展，无疑增加了这种危险：在数据可以转移的情况下，一个人一生的数据都可能被一次性获取，而 GDPR 所要求的“不受阻碍”，或许也会在一定程度上影响数据控制者对用户身份核对的次数与验证方式，从而威胁用户个人信息的安全。事实上，在数据可一次性获取并移植的前提下，黑客可以更便捷地得到更多的个人数据，这对平台关于个人信息的保护措施提出了更高的要求。对此，本文认为，平台应当对申请数据转移的用户进行多重认证，包括一般的个人信息核验以及更保险的生物信息识别等。此外，还可以使用额外的认证信息，如一次性密码、密保问题等。

除了因身份欺诈造成的个人信息泄露外，数据传输过程中也存在许多被攻击的风险，如中间人攻击（Man-in-the-MiddleAttack，MITM）或分布式拒绝服务攻击（Distributed Denial of Service，DDoS）等。因此，本文认为，提高加密技术与水平是数据控制者应当采取的最低限度的安全措施，在此基础上还应使用更多授权认证方式。

www.pcachina.com

#### 2.2.2 不利于企业之间的公平竞争

从理论构想上分析，数据可携带权是打破垄断的利器，有助于削弱数据的“锁定效应”，实现不同数据控制者之间的数据流通，打破头部企业对数据资源的垄断。但在实践中，该权利并没有达到预期的效果。

头部互联网企业往往会提供多种在线服务，例如谷歌就同时提供搜索引擎、新闻、社交、购物、邮件等服务，用户注册一个账号就可以享受全部服务，这使用户形成了使用习惯，被“锁定”在这一数据控制者中。因此，即使出现了几次轰动全球的与网络安全相关的丑闻（例如“剑桥分析案”），用户依然不会选择其他替代服务。与此同时，头部企业还在继续开拓新市场，所占市场份额越来越大，从而造成了不公平的竞争环境。Stucke 和 Grunes 详细地描述了这一“良性循环”过程：“越多的人主动或被动地提供数据，公司就能进一步根据需求改善其产品，从而对潜在的用户更有吸引力。”[9] 例如，Zynga 在使用脸书（Facebook）的 API 的基础上开发了一个游戏平台，通过 Facebook 向用户及其好友投放广告、发送游戏邀请并发布游戏信息等，以吸引更多的玩家加入，两家公司形成了互利合作的关系。2011 年，Zynga 占 Facebook 收入的 19%，而 Facebook 占 Zynga 收入的 93%。然而，2012 年，Facebook 发布声明结束了与 Zynga 的合作关系，取消了两家企业之间的 API 对接，从而使得 Zynga 的估值从 150 亿美元下降到了 30 亿美元。从 Zynga 的失败案例可以看出，在 API 使用过程中，小企业对大企业存在着一定的依附性，如果监管机构试图通过强制执行 API 来促进竞争，其应当构建一个更加完善系统的法律框架，防止以大欺小。

在数据驱动型市场中，数据是经营者获得并维持竞争优势的重要保障，如国内发生的顺丰与菜鸟、腾讯与华为、京东与天天快递之间的纠纷从本质上来讲都是有关数据的争夺战[4]。为了收集更多的客户数据，新兴企业可能需要搭建一个更加便宜乃至免费的平台，而支撑该平台需要在技术、人工、宣传等方面付出大量的成本。然而，大部分的平台都只有在达到一定的规模或市场份额后才能盈利，前期需要企业自行承担风险成本，这会给新兴企业带来极大负担。尽管在资金有限的情况下，依然可以通过技术手段实现用户爆发式增长，但这也会产生潜在的风险。例如 2002 年，领英（LinkedIn）在其成立后不久就采用了一种名为“增长黑客”的手段扩大了用户规模，但这种方式背后带来的隐私、安全以及垃圾邮件等问题也使得领英被提起诉讼，并付出了 1 300 万美元和解金的代价[3]。此外，正如上一节所提到的，个人数据泄漏的风险不断上升，在这种情况下，用户通常会倾向于选择更加知名老牌的企业，变相地造成了大公司的数据垄断，不利于企业之间的公平竞争。

## 3 制度评估与法理启示

### 3.1 数据可携带权的现状

回顾 GDPR 颁布至今，有许多学者对其在欧盟各国实施的现状进行了实证研究，结果证明立法者本身期望赋予数据可携带权的意图与法律实施的现状之间存在较大差异。

2021 年，有学者针对德国部分互联网用户对 GDPR 权利的了解程度进行了调查[10]，其结果如图 1 所示。从图中可以看出，仅有不到 1/3 的参与者听说过数据可携带权，而 GDPR 中的其他权利均有超过半数的人知晓。这一结果表明，数据可携带权在互联网用户中鲜有人知，因而也缺少行使该权利的实践经验。同样，该团队也从数据控制者的角度对数据可携带权的实施现状进行了研究：参与调查的 182 家在线服务平台中，仅有 72.4%

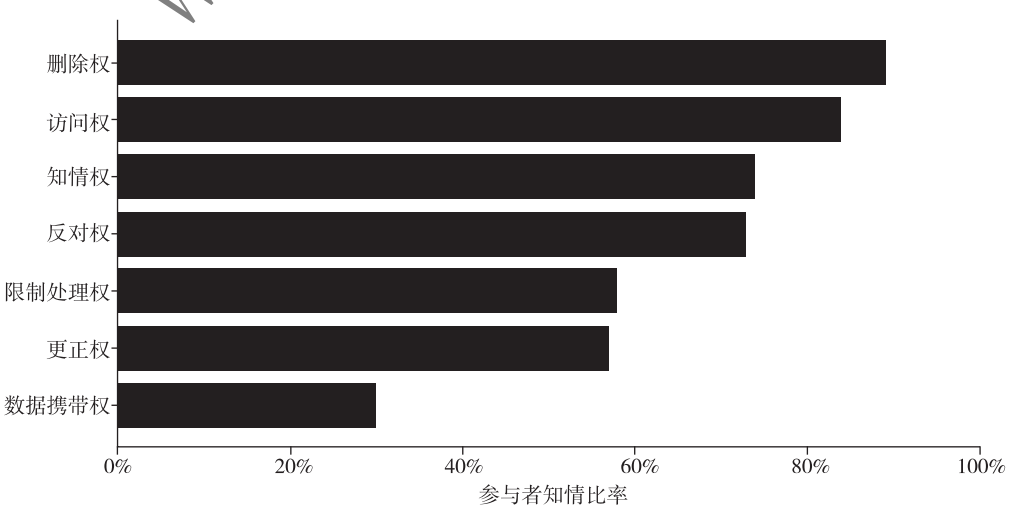


图 1 了解 GDPR 中相关权利的用户数据

www.pcachina.com

在法律允许的时间范围内提供数据传输，仅有 51.1% 的平台满足“结构化的、通用的、机器可读的”数据格式要求；而在导入数据方面，76.8% 的数据平台没有提供导入数据的选项，只有 24.2% 的平台提供了一部分的数据导入功能。文献［11］对“平台处理转移数据请求所需的时间”进行了实证研究，结果显示存在回复所需时间长（75% 的平台在一个月后才回复）、过程审核不严格、实践次数少（有 4 位数据控制者提出是第一次收到转移数据的要求）等问题，反映出该权利的行使在数据控制者层面也并没有得到很好的落实。

### 3.2 法理启示与借鉴意义

继欧盟于 2016 年提出数据可携带权概念后，美国、日本、瑞士等多个国家也引入了该权利。尽管欧盟的数据可携带权在条文本身以及后续的规范上都没有进行完善的规定，最终沦为了僵尸条款，但这对各国，特别是我国进行实际意义上的数据可携带权的实施或许可以提供一定程度上的借鉴意义。2021 年 8 月 20 日，《中华人民共和国个人信息保护法》颁布，该法第 45 条规定，个人有权从个人信息处理者处复制其个人信息以及要求个人信息处理者将其个人信息转移至其他处理者，这代表着数据可携带权在我国得以确立。我国将该权利规定在《个人信息保护法》中，意味着该权利的首要价值目标在于加强个人信息安全，增强数据主体对其数据信息的掌控能力，显示了我国立法机关对于个人信息保护权的开放与强化立场[12]。但该法并未明确规定该权利的范围、权利实现方式，因此，本文将立足权利保护，借鉴域外法提出一些建议，以期实现个人与数据处理者的双赢。

美国学者 Peter Swire 以美国 2002 年《电子政务法案》要求的隐私影响评估和 GDPR 要求的数据保护影响评估为蓝本，就如何避免或减少数据可携带权的实施带来的风险提出了一个名为 PORT-Ias 的框架。该框架提出对传输的数据根据其敏感性进行分类，对于一般的浏览数据、公开的个人信息等可以归为低风险数据，而诸如敏感信息、财务信息等则归入高风险数据；将科学家、政府工作人员、学者等影响力较大、更容易成为被窃取身份数据信息的人的数据归入高风险数据，而对于普通用户的数据可以进行稍低等级的保护。借鉴这一做法，本文认为，我国对于不同风险级别的数据应当制定不同的处理规则，以避免“一刀切”的情况。数据敏感级别的分类可以由单独的“隐私阈限分析”（Privacy Threshold Analysis）组织进行隐私影响评估和进一步的风险分析[13]，建立类似金融部门中的分层安全机制，对安全风险较高账户实施更高水平的保护。此外，政府部门应当积极推动与行业利益相关者以及行业协会合作，对关于数据控制者评估数据接受者的安全和数据主体提出请求时的安全性方面的责任和授权提出更加详细的指导，共同制定一套符合“互操作性”要求的最低标准和格式，确保绝大多数的企业都可以适用。

在监管上，可以设立一个专门监督数据可携带权的监管机构，对该权利的实现、监管等进行说明，并告知用户如何在数据控制者拒绝提供数据时进行投诉。为减轻监管机构的压力，同样可以对企业进行分级，根据企业的收入和控制的数据量级给予不同程度的监管。具体到分级标准上，可以参考美国的《加州消费者隐私法案》，其只适用于满足以下条件的营利性公司：总收入超过 2 500 万美元，每年购买或接受 5 万及以上的个人信息，或者每年 50% 及以上的收入来自出售个人信息。而我国正处于该权利施行的早期，可以适当对适用该权利的数据主体进行限缩，给中小型企业一定的缓冲和进步空间。

## 4 结束语

我国正处于数字经济发展的高速期，根据中国信息通信研究院发布的《中国数字经济发展白皮书（2022）》的数据显示，2012 年以来我国数字经济年均增速高达 15.9%。2022 年，我国数字经济规模达到 50.2 万亿元，数字产业化规模为 41 万亿元，数字经济已经成为稳增长的强大力量。而数字经济健康稳步发展的背后，离不开足够的法律规定与理论支撑。尽管有学者认为，在当前发展的初期，应当给数据企业和大数据产业的发展相对宽松的环境，不应当给其施加太多的限制和束缚，但是应当看到，在多国都对该权利进行了规定并出台了相关法规的背景下，我国企业在境外发展运行或进行跨境数据传输时不可避免会受到规制和影响，这有许多国际先例：2019 年 1 月 21 日，谷歌因违反 GDPR 被法国国家信息与自由委员会（National Commission on Informatics and Liberty，NCIL）罚款 500 万欧元；2022 年 8 月 5 日，NCIL 对法国营销科技公司 Criteo 涉嫌违反 GDPR 的行为罚款 6 500 万美元，且并未说明该公司存在何种数据使用不当的行为；2022 年 9 月 2 日，Facebook 母公司 Meta 因违反 GDPR 而被爱尔兰数据保护委员会（Data Protection Commission，DPC）罚款 4 亿美元。据此，为了维护我国企业在他国的利益，创造更加公平开放的营商环境，掌握数字经济时代个人数据保护的主导权和话语权，加强有关数据开放、传输、保护等方面的法律研究已经迫在眉睫。为此，有必要重视对欧盟数据可携带权立法及其实践方面的研究，为我国后续在该方向上的立法及相关法规的出台提供参考和借鉴，让这一权利中国化并服务于我国的数字经济发展。

（下转第 12 页）

www.bcachina.com

London：Routledge，2021.
[5] 张凌寒. 算法权力的兴起、异化及法律规制 [J]. 法商研究，2019，36（4）：63－75.
[6] 刘琳. 算法解释权与商业秘密保护的冲突化解 [J]. 行政法学研究，2023（2）：168－176.
[7] O'NEIL C. Weapons of math destruction：how big data increases inequality and threatens democracy [M]. New York：Crown Random House，2017.
[8] 戚聿东，肖旭. 数字经济时代的企业管理变革 [J]. 管理世界，2020，36（6）：135－152，250.
[9] 王怀勇，邓若翰. 算法时代金融公平的实现困境与法律应对 [J]. 中南大学学报（社会科学版），2021，27（3）：1－14.
[10] SEAVER N. Algorithms as culture：some tactics for the ethnography of algorithmic systems [J]. Big Data & Society，2017，4（2）：1－12.
[11] 张欣，宋雨鑫. 算法审计的制度逻辑和本土化构建 [J]. 郑州大学学报（哲学社会科学版），2022，55（6）：33－42.
[12] 丛颖男，王兆毓，朱金清. 论算法解释权的重构——全算法开发流治理与分级分类解释框架 [J]. 计算机科学，2023，50（7）：74－79.
[13] 刘峰，许菲. 风险导向型审计·法律风险·审计质量——兼论“五大”在我国审计市场的行为 [J]. 会计研究，2002（2）：21－27，65.
[14] LONGSDALE J，WILKINS P A，LING T. Performance auditing：contributing to accountability in democratic government [M]. Cheltenham：Edward Elgar Publishing，2011.
[15] BROWN S，DAVIDOVIC J，HASAN A. The algorithm audit：scoring the algorithms that score us [J]. Big Data & Society，2021，8（1）：1－8.
[16] RIBEIRO M T，SINGH S，GUESTRIN C. Anchors：high-precision model-agnostic explanations [C]//Proceedings of the AAAI Conference on Artificial Intelligence，2018，32（1）.
[17] 王光远，瞿曲. 公司治理中的内部审计——受托责任视角的内部治理机制观 [J]. 审计研究，2006（2）：29－37.
[18] 周中胜，陈汉文. 大股东资金占用与外部审计监督 [J]. 审计研究，2006（3）：73－81.
[19] 申卫星. 数字权利体系再造：迈向隐私、信息与数据的差序格局 [J]. 政法论坛，2022，40（3）：89－102.
[20] 王莹. 算法侵害责任框架刍议 [J]. 中国法学，2022（3）：165－184.

（收稿日期：2023－04－29）

**作者简介：**

王兆毓（2000－），男，硕士研究生，主要研究方向：算法治理、个人信息保护。

（上接第5页）

**参考文献**

[1] 李世刚，包丁裕睿，王峥. GDPR欧盟一般数据保护条例文本和实用工具 [M]. 北京：人民日报出版社，2008.
[2] SWIRE P，LAGOS Y. Why the right to data portability likely reduces consumer welfare：antitrust and privacy critique [J]. Maryland Law Review，2013，72（2）：335－380.
[3] NICHOLAS G. Taking it with you：platform barriers to entry and the limits of data portability [J]. Michigan Technology Law Review，2021，27（2）：263－298.
[4] 李伯轩. 数据携带权的反垄断效用：机理、反思与策略 [J]. 社会科学，2021（12）：105－116.
[5] European Data Protection Supervisor. Opinion 3/2015（with addendum）. Europe's big opportunity-EDPS recommendations on the EU's options for data protection reform [R]. 2015.
[6] QUINN P. Is the GDPR and its right to data portability a major enabler of citizen science [J]. Global Jurist，2018，18（2）：1－16.
[7] 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.
[8] SCUDIERO L. Bringing your data everywhere：a legal reading of the right to portability [J]. European Data Protection Law Review，2017，3（1）：119－127.
[9] STUCKE M E，GURNES A P. Big data and competition policy [M]. Oxford：Oxford University Press，2016.
[10] KUEBLER-WACHENDORFF S，LUZSA R，KRANZ J，et al. The right to data portability：conception，status quo，and future directions [J]. Informatik Spektrum，2021，44：264－272.
[11] WONG J，HENDERSON T. The right to data portability in practice：exploring the implications of the technologically neutral GDPR [J]. International Data Privacy Law，2019，9（3）：173－191.
[12] 王利明，丁晓东. 论《个人信息保护法》的亮点、特色与适用 [J]. 法学家，2021（6）：1－16，191.
[13] HONDAGNEU-MESSNER S. Data portability：a guide and a roadmap [J]. Rutgers Computer and Technology Law Journal，2021，47（2）：241－273.

（收稿日期：2023－05－09）

**作者简介：**

吕思祺（1999－），女，硕士研究生，主要研究方向：民商法、网络安全。

www.pcachina.com

# 版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com