# 数据可携带情形下的权利冲突与规则调适

王欣辰[1]，沈廖佳[2]
（1. 中国科学技术大学 知识产权研究院，安徽 合肥 230026；
2. 东南大学 法学院，江苏 南京 211189）

**摘 要**：能否有效化解数据可携带情形下的权利冲突问题，既是各国布局可携带权的考量要点，亦是影响制度成败的关键所在。从权利本质上看，可携带权既是实现多元主体利益平衡的工具，又因其权利内涵的积极性和实体性在个人信息权利束中扮演着极为特殊的角色。以司法实践为镜，唯有摆脱“三重授权原则”与《反不正当竞争法》的窠臼，直面可携带情形下的各类权利冲突，才能打破个人介入数据流转与分配的桎梏。由典型场景入手，可携带情形下的权利冲突主要体现为对个人信息的贬损、对知识产权的袭扰和对数据安全的威胁。应从立法理念、客体范围、法律互动和安全保障四个方面进行冲突调试，进而实现我国可携带权制度的“完美闭环”。

**关键词**：数据可携带权；个人信息保护；权利冲突；数据安全
**中图分类号**：D923.8 **文献标识码**：A **DOI**：10.19358/j.issn.2097-1788.2023.04.007
**引用格式**：王欣辰，沈廖佳. 数据可携带情形下的权利冲突与规则调适［J］. 网络安全与数据治理，2023，42(4)：39-44.

## Rights conflict and coordination in situation of data portability

Wang Xinchen[1], Shen Liaojia[2]
(1. Intellectual Property Research Institute, University of Science and Technology of China, Hefei 230026, China;
2. School of Law, Southeast University, Nanjing 211189, China)

**Abstract**: Whether it can effectively address the collision of the right to data portability is not only the key aspects for the right to portability strategy in countries, but also the core of the success or failure of the system. From the perspective of the essence of rights, the right of portability emerges as a tool to achieve a balance of interests of multiple subjects, it also plays an extremely special role in the bundle of personal information rights due to the positive impacts and the substance of being human. Taking judicial practice as a mirror, the only way to break the shackles of data transfer and distribution of data interests is to get rid of the “Triple Authorization Principle” and the Anti-Unfair Competition Law and face up to the various types of the collision of the right to data portability. Starting from a typical scenario, the collision of the right to data portability is mainly reflected in the derogation of personal information, the infringement of intellectual property rights as well as the threat to data security. It is advised to establish a resolution mechanism of collision of right under the various situation, designing from the four aspects of the legislative concept, object boundary, legal interaction, and security guarantee, so as to achieve a “perfect closed loop ” of the right to data portability system in China.

**Key words**: the right to data portability; personal information protection; collision of rights; data security

## 0 引言

数据可携带权（以下简称可携带权）是由我国《个人信息保护法》第45条第3款确立的新兴权利，其含义为个人作为数据的源头有权请求数据处理者将特定个人信息转移至其他的数据处理者，而数据控制者应当予以必要的协助[1]。可携带权起源于欧盟的《通用数据保护条例》（General Data Protection Regulations，GDPR），又陆续被美国、巴西和印度等国家引入。一般认为，可携带权是用户制衡数据控制者和数据处理者的策略性工具，肩负着塑造数字人格、消解锁定效应、抑制数据垄断和激发创新活力的制度理想。近年来，除了《个人信息保护法》，相关部门又相继在《中国人民银行金融消费者权

益保护实施办法（征求意见稿）》《信息安全技术 个人信息安全规范》（GB/T 35273－2020）《网络数据安全管理条例（征求意见稿）》等文件对数据携带问题进行了回应，所涉条文覆盖了可携带权的定义、可携带情形和数据处理者风险提示义务等内容。

然而，自诞生之日起，可携带权便伴随着大量的争议。在国际社会中，不论是权利的具体内容和范围，抑或是可携带权对市场创新、公平竞争和数据安全的具体影响，理论界均未达成共识。即使是那些明确引入可携带权的国家和地区，也往往对其实践保持着审慎、保守的态度。在我国，立法者对是否引进该权利的态度亦经历了权衡与反复，直至《个人信息保护法》，可携带权的权利地位才最终得以确认。如表 1 所示为我国法律对数据携带问题的相关规定。不过，在一系列围绕可携带权的研究中，我国学者虽在基础理论、域外对比和制度本土化等方面取得了不俗的成果，但对可携带权与相关权利的冲突与化解，学界并未给予足够的关注。据此，本文将在澄清可携带权本质的基础上，考察数据可携带情形下权利冲突的典型场景和司法实践，为我国可携带权规则的细化和深入提供参照。

表 1　我国法律对数据携带问题的规定

| 颁布时间 | 法律文件 | 主要内容 |
| --- | --- | --- |
| 2019 年 12 月 | 《中国人民银行金融消费者权益保护实施办法（征求意见稿）》 | 第 36 条对数据可携带权作出了前瞻性规定，即鼓励金融机构在技术可行的前提下，对金融消费者转移信息的请求予以配合 |
| 2020 年 3 月 | 《信息安全技术 个人信息安全规范》（GB/T 35273－2020） | 第 8. 6 条规定根据个人信息主体的请求，数据控制者应在技术可行的前提下直接将个人信息的副本转移至指定第三方，但将可携带数据限定为本人的基本资料、身份信息、健康生理信息、教育工作信息 |
| 2021 年 8 月 | 《个人信息保护法》 | 第 45 条第 3 款规定个人请求将个人信息转移至其指定的数据处理者，符合国家网信部门规定条件的，数据控制者应当提供转移的途径 |
| 2021 年 11 月 | 《网络数据安全管理条例（征求意见稿）》 | 第 24 条尝试平衡各方利益，既细化了数据可携带的条件，又规定了数据处理者的风险提示义务和收取合理费用的权利 |

## 1　数据可携带权本质之澄清

### 1. 1　立法目的：作为利益平衡工具的可携带权

在竞争法视野下，可携带权的主要意义在于塑造公平的数字市场环境。近年来，随着数字市场的发展壮大，部分数字巨头借助技术手段和经营模式竭力巩固其市场领先地位，并衍生出诸如算法滥用、数字垄断、数据爬虫等竞争失序现象，而个人却在数据生产、利用和分配的环节中逐渐“失语”。为了缓解个人与数字企业间的不平等现象，欧盟首先在 GDPR 中规定了数据可携带权，使用户有权通过结构化、通用化的方式实现数据转移。简言之，在市场竞争的环境下，可携带权是对数据处理者实际控制力的适当削弱，以及对用户选择路径的理性扩张，降低了用户跨平台操作的成本。

除此之外，可携带权还具有私权层面的独立价值。一方面，适时引入可携带权是厘清数据权属的必然要求。近年来，数据日益成为个体权益的应然构成、企业竞争的战略资源和国家发展的重要引擎，但究竟应该怎样设计数据财产权和数据人身权，如何平衡用户、数据处理者和数据控制者等多元主体间的利益，仍然是理论界久拖不决的难题。而以引入域外相对成熟的可携带权为契机，逐步搭建我国的个人信息权利体系，将为澄清各数据权利间的边界提供契机。另一方面，可携带权的存在为数字人格的保护提供了有效工具。唯有当用户可以按照自身意愿进行复制、转移个人信息，才能真正拥有数字化环境下的“人身自由”，安然往返于各类数字平台之间。

### 1. 2　体系定位：可携带权在个人信息权利束中的位置

可携带权与其他个人信息权存在千丝万缕的联系。一方面，在个人信息权利束的体系中，知情权与决定权是基础性权能，而可携带权则属于工具性权能的一种。其中，基础性权能乃是立法者对个人信息权利内核的描述，而可携带权等工具性权能是为了实现知情权与决定权所采取的技术配置。另一方面，我国立法者将数据可携带权与访问权、复制权一同规定于《个人信息保护法》第 45 条，也是有其原因的。从权利实现的角度看，访问权是可携带权的前置条件，倘若用户无法得知个人信息的收集、处理与利用情况，也就无从对信息的转移作出理性判断；从权利性质的角度看，可携带权又构成了复制权的积极延伸，即用户不仅可以从数据控制者那里获取个人信息的副本，还可以进一步将该类信息转移至其他数据接收者。

与此同时，可携带权又在个人信息权利束中扮演着极为特殊的角色，无法被传统的个人信息权利完满容纳。

一方面，可携带权蕴含了一种积极的权利表达，这在个人信息权利中是极为少见的。例如，查阅权和复制权为用户了解个人信息处理情况并索取备份创造了制度条件，删除权使用户能够在《个人信息保护法》第47条规定的情形下，要求处理者删除特定数据。但这些权利都具有显著的防御性，对应的实现途径往往是被动的、消极的。而可携带权却试图引导用户积极、主动地参与数据的转移与共享，从纯粹的数据来源进阶为数据流通的参与者和受益人。另一方面，可携带权指向实体利益的分配，属于分配正义的范畴[2]。不论是《个人信息保护法》第44条规定的知情权、决定权，抑或是第48条确立的要求解释和说明权，均象征着数据处理、利用中的程序正义，而与数据权益的实质归属无涉。反观可携带权，其在实现数据跨平台流动的同时，也深刻影响着数字平台间的经营利益和竞争格局。

## 2 数据可携带情形下权利冲突的典型场景

### 2.1 个体层面：对个人信息的贬损

可携带权“粘连”的数据，可能包含第三方用户的个人信息。以微信中的数据为例，朋友圈中发送的每一张照片、产生的每一次评论和点赞，都是在“仅共同好友可见”的前提下进行的，互动的相关方并未就相关数据的公开达成任何合意；不论是好友列表的信息和排序，抑或私人的聊天记录，几乎都是由用户和好友共同完成的，理应免受非法个人信息处理活动的侵害。进言之，在数据转移的过程中，许多看似专属于个人的数据，实际上都包含了其他自然人的参与和协同。参照《个人信息保护法》第4条之规定，鉴于我国对个人信息的定义已完成了从“识别说”到“关联说”的转向[3]，相关数据只须具备基本的关联性，即可纳入个人信息的范畴。

具体而言，数据可携带权的不当行使可能会损害其他用户对个人信息享有的知情权、决定权和删除权。一方面，如果数据转移行为未征得关联主体的知情同意，将对他人的知情权和决定权构成威胁。《个人信息保护法》相继在第13条、第17条中规定了个人信息处理的合法性基础和数据处理者的告知义务。前者将“取得个人的同意”作为信息处理活动主要的合法性来源；后者则要求数据处理者应以显著的方式、清晰易懂的语言“真实、准确、完整”地告知相关内容。另一方面，用户单方面进行数据转移，可能会在事实上克减他人的删除权。从价值位阶上看，具有隐私保护意义的删除权应在取舍上优先于可携带权，即可携带权不应为删除权的行使创设障碍。而如果某项包含个人信息的数据已率先被其他用户转移至第三方平台，权利人对删除权的行使将面临实质障碍，很难实现真正意义上的“全面删除”。

### 2.2 企业层面：对知识产权的袭扰

一方面，可携带权裹挟的数据，可能涉及数据发送者的商业秘密。从理论上讲，数据的无体性、非竞争性和价值性，使其成为天然的知识产权客体；在实践中看，当下企业经营形成的很大一部分无形财产，都凝聚在商业数据中。基于此，如果数字企业对数据采取了必要的管理和保密措施，所涉数据便有可能构成商业秘密。相应地，用户借助可携带权将数据转移到第三方的行为，一旦导致接收者直接获取或间接破译了数据背后的技术信息或经营信息，便涉嫌构成对数据发送者商业秘密权益的侵犯，将面临《反不正当竞争法》的处罚。

另一方面，可携带权牵掣的数据，可能涉及数据发送者的著作权。依据《著作权法》第15条的规定，如果对作品、数据或其他材料的选取和编排体现了足够的独创性，该数据集合就可以纳入著作权法的客体范畴。因此，如果数字企业对个人信息进行了程度较深的加工、处理、分类和汇总，并进一步产生了蕴含智慧性、创造性的数据集合，则该集合完全能够满足汇编作品的构成要件[4]。在司法实践中，亦不乏通过汇编作品条款，对企业数据库进行保护的先例。如在佛山鼎容软件科技有限公司诉济南白兔信息有限公司著作权权属、侵权纠纷案[5]中，法院就以被告通过反向破解获取、复制原告公司数据库并进行盈利的行为，裁判其承担著作权侵权责任。故用户在行使可携带权的过程中，仅仅是数据转移行为本身，就可能侵犯数据控制者作为著作权人享有的复制权。

### 2.3 社会层面：对数据安全的威胁

数据可携带权引发的安全隐患，根本上源自数据互操作性与安全性之间的异质性。为了实现数据的跨平台转移、实现可携带权的落地，就必然要求数据处理者提供更多的访问接口，并实现数据传输的标准化。然而，随着数据分布的碎片化和数据主体的多元化，用户数据被侵入、泄露甚至丢失的风险亦将呈指数级上升。甚至可以说，为了实现可携带权在破除数字垄断、促进平台融通上的制度初衷，承担更高的数据安全隐患几乎是必然的。遗憾的是，即使在欧盟的《通用数据保护条例》、美国的《加州消费者隐私法》等现有的域外规范中，也并没有为可携带场景下的数据安全风险提出可行的解决方案[6]。

具体而言，可携带权造成安全隐患的情形大体可以分为两类：其一，用户身份被他人盗用或冒用，进而做出与权利人本人意志相悖的数据转移行为，如将个人信

息转移至带有推销乃至欺诈属性的违法平台。其二，相关企业存放个人信息的数据库遭受黑客入侵，发挥安全保障功能的算法和技术措施陷入失控，进而导致数据泄露。可以预想，倘若数据的泄露和丢失上升为普遍性的风险，作为个体的用户基于理性的判断，一定会优先将个人数据存放在相对可靠的大型数字平台中，而不愿意借助可携带权将数据转移至尚不成熟的新兴企业，可携带权对竞争效益的促进作用将大打折扣。因此，妥善应对数据安全层面的问题，是塑造制度信任、培植权利认同的必经之路。

## 3　数据携带情形下权利冲突的司法实践

我国在司法实践中虽屡次遭遇个人信息的携带问题，但截至2023年2月1日，在裁判文书网上进行检索，“可携带权”这一正式称谓仅见于腾讯诉搜道不正当竞争纠纷案[7]。其原因大致有二：其一，确立可携带权的《个人信息保护法》于2021年11月生效，自然无法对先前的案件产生拘束；其二，多数案件的纠纷集中在数据控制者与数据处理者之间，并不涉及个人这一可携带权的权利主体。然而，从可携带权的视角出发，对非法爬取他人数据的相关案件进行考察仍具有现实意义，不但有助于确定数据携带行为的合法性边界，还将为实现数据控制者与数据处理者之间的利益平衡提供启示。

### 3.1　现状梳理

纵观近年来与爬取个人信息/数据有关的案例，法院在裁判中体现出如下倾向：其一，法院的论证紧密围绕着“是否构成反不正当行为”这一核心展开，而在《反不正当竞争法》中又尤其依赖一般条款和第12条之规定。其二，在法无明文规定的情况下，法院并没有赋予个人类似“可携带权”的权利，而仅是将个人作为“三重授权原则”中的一环，即数据的跨平台流动需要先后取得用户对数据转出的同意、数据控制者对数据转出的同意和用户在知晓数据用途后的再次同意。其三，为了在数据保护与数据流动之间、数据权益与竞争秩序之间寻求平衡，法院在说理中引入了大量模糊的法律概念，如公共利益、商业道德、消费者权益等。

如果不加节制地允许市场主体任意地使用或利用他人通过巨大投入所获取的信息，将不利于鼓励商业投入、产业创新和诚实经营，最终损害健康的竞争机制。故在具体识别某行为是否构成反不正当竞争时，法院时常会综合考虑如下因素：其一，原告是否为数据的收集与整合负担了相应成本，针对后台运营数据、用户评论等获取难度较大的信息，更容易受到《反不正当竞争法》的保护。其二，擅自抓取的数据是否超过了必要限度，即使是公开的数据，也不必然意味着可以被随意获取和使用。其三，被告是否存在恶意破坏或绕开原告技术保护措施的行为，甚至影响平台的正常运行。其四，被告行为在多大程度上违反了或突破了以robots协议为代表的诚实信用原则和公认的商业道德。其五，被告行为是否对市场竞争秩序和消费者权益等抽象利益造成了负面影响。

### 3.2　成因与反思

撇开当时可携带权的立法空白不谈，法院选择绕开《民法典》之下侵权责任编的规定转向《反不正当竞争法》，有其内在的动因。第一，反不正当竞争法保护的是权益而非权利，并为孵化性、补充性的法益提供兜底保护[8]。故其本就具备在搁置数据权益归属问题的情况下，优先为数据控制者利益提供保护的先天优势。第二，由于个人信息案件往往属于大规模的侵权案件，相较于竞争法下的“三重授权原则”，传统侵权责任法的规制模式貌似不经济，也不实用。如果法院选择侵权责任的分析路径，则必须要直面下列诘问：如何证明被侵权人因个人信息遭受的财产或精神损失？如果无法确定是否造成实际损害，又该如何确定原告资格？与其采取零星、分散的个人诉讼，为什么不能通过数字企业间的诉讼寻求救济？第三，在个人与数据处理者的纠纷中，借助公权力介入更充分的反不正当竞争法，能在现实意义上填补二者的地位差距。在遵循比例原则的前提下，市场监管部门按照《反不正当竞争法》的规定，有权对数据携带进行事前监管和事后惩罚，甚至采取行政制裁；面对个人在可携带权诉讼中实际损害不明、举证困难的窘境，从《反不正当竞争法》亦能更快地建立起政府部门代为诉讼和举证责任倒置的规则。

应当对法院向《反不正当竞争法》“逃逸”的现象保持警惕。第一，盲目适用一般性条款加剧了法律适用的不确定性和不同部门法间的矛盾，也存在法官造法的嫌疑。例如，依据《个人信息保护法》，公开个人信息意味着信息主体已作出同意处理的表示，但新浪微博诉脉脉案以《反不正当竞争法》一般性条款为由强加数据处理者寻求信息主体同意的额外义务。第二，在数字经济发展初期，应当秉持“竞争行为中心主义”[9]，要求企业对市场中的损害行为保持一定程度的容忍。当无法借助著作权、商业秘密等权利（权益）保护数据控制者的利益时，意味着请求权基础的缺乏，轻易以《反不正当竞争法》赋予额外的保护可能导致权利范围的不当扩张。第三，法院“重反法而轻侵权”的态度，相当于在反不正当竞争法与侵权责任法之间设立了本不存在的障碍。但所谓的竞争法规则，不过是侵权法规范体系中一种具体的筛选工具，不可能具备侵权法之外的价值体系与论证

模式[10]。是故对不正当竞争行为的认定，只能在侵权法的价值定位、教义学框架和推理模式下展开，而不应忽视《反不正当竞争法》与民事规范的客观链接。

## 4 数据可携带情形下权利冲突的调适路径

### 4.1 采取开放的立法理念

为尽量减少可携带权与其他权利的冲突，首先要在其构造上保持充分的开放性与灵活性，这是由可携带权在个人信息权利束中的特殊定位决定的。一方面，可携带权是用户对数据所做的积极的、涉及实体利益的干预，与防御性的、程序性的个人信息权利存在本质差异。应对传统个人信息权利和可携带权采取两种截然不同的立法框架，前者是静态的、消极的、相对确定的，后者是互动的、积极的、充分灵活的。另一方面，由于可携带权兼具竞争属性和私权价值，在相当长的一段时间内，我国的可携带权制度大概率会采取“权利化模式”与“行为规制模式”并行的双轨方案。因此，在数据权益分配尚未形成共识的当下，不宜过早形成明确、详尽的立法，为可携带权的诸多细节盖棺定论。

### 4.2 设定合理的客体范围

过宽和过窄的客体范围都会影响可携带权的效益，前者可能会为数据控制者增添不必要的成本，而后者又会阻碍个体数据权益的实现。我国虽未在《个人信息保护法》《网络数据安全管理条例（征求意见稿）》等规范中对可携带权的客体进行明确，但参考域外立法，对可携带权客体的限制主要基于三个方面：其一，可携带权原则上仅针对直接来源于用户的“原始数据”，如年龄、性别、位置数据、浏览痕迹、消费记录等，而不包括经过加工和处理形成的“衍生数据”和“观测数据”，如用户画像、行为习惯、消费动机等。该限制主要是为了弥补数据处理者此前投入的智慧和劳动，因此若支付合理的对价，也可以将客体延伸至其他两类数据。其二，可携带权划定的客体范围不应对公共利益构成妨碍。即如果具有公共管理职能的行政部门出于国家安全、应急管理、社会道德的需要进行数据获取和转移时，可携带权应进行合理的避让。其三，可携带权涉及的客体不应侵犯他人在先的民事权益。若一段数据上同时存在第三方的删除权或隐私权，在未达成合意的情况下，作为数据来源的自然人亦无权决定个人信息的去留；同时，为了避免行使可携带权时侵犯他人的知识产权，在进行转移决定前，应由数据控制者证明携带数据具备基本的“清洁性”，即所涉数据不存在明显侵犯他人商业秘密或汇编作品的情况。

### 4.3 实现部门法间的良性互动

建议法院在审判过程中，将《个人信息保护法》《民法典》和《反不正当竞争法》等多个部门法视为有机的整体，以体系化目光促进部门法间的良性互动，对行为违法性作出更精准判断，杜绝根本性冲突。一方面，判定数据携转行为违法性的过程中，应综合适用《反不正当竞争法》第2条与《民法典》第1165条之规定，倘若穷尽请求权基础仍无法对原告的权益进行救济，相关诉讼请求就不应获得法院的支持。另一方面，应缓解《个人信息保护法》与《反不正当竞争法》之间的紧张关系，既要规避绝对意义上的数据可携带权，又要防止落入严格的三重授权原则当中。具体而言，一来要承认数据控制者对数据的持有付出劳动，借助数据盗用理论牵制可携带权的功用，一旦具有直接竞争关系的数据处理者窃取或盗用该数据，即便取得个人同意，也并非意味着行为的正当性[11]。二来要防范数据控制者权益的任意扩张，数据控制者付出的成本和劳动完全可以通过付费获得补偿，而不必为每次数据携转捆上控制者同意的枷锁。

### 4.4 提供数据携转的安全保障

随着立法的进步与技术的迭代，我国完全有可能将数据携带中的安全风险控制在合理区间内。一方面，应为数据携转提供全生命周期的风控方案：在数据存储阶段，应充分利用区块链、云计算等数字加密手段，尽可能降低数据入侵及泄露的风险，并做好数据的标记、脱敏和溯源工作；在数据转移阶段，应落实严格的身份验证制度，通过密码确认、短信验证和人脸识别等多重技术手段，确保数据携转的决定由权利人本人做出，在传输金融、医疗等敏感数据时，更应通过电话、短信或电子邮件进行风险提示；而一旦数据主体对数据库失去控制、无法保障个人信息处于安全状态，应果断启动自毁程序，最大程度上降低数据泄露和非法复原的可能性[12]。另一方面，有必要进一步明确数据处理者的安全保障义务。其一，应当依据数据处理者的地位、所处市场的竞争程度和行业性质，设定差异化的安全保障义务和场景化的责任水平[13]；其二，建议逐步完善数据审查制度和数据安全认证制度，由国家相关部门制定“可信赖接收者”标准，并将审查或认证的结论作为评判数据处理者过错程度的主要问责点；其三，有必要健全数字企业内部的合规管理体系，厘清个人与数据处理者在数据携转过程中的义务边界，防止责任混同。

## 5 结论

随着《个人信息保护法》的落地，继续在我国讨论可携带权的必要性和可行性已不再具有现实意义。以欧美等地的法律实践为参照，唯有直面并尝试化解数据可携带情形下的各类权利冲突，才能使可携带权这项颇具

争议的新兴权利真正服务于数字经济和社会发展的远景目标。同时，由于可携带权在个人信息权利束中的特殊定位，在构建民事权益平衡机制的过程中，应当秉持谦抑、保守的姿态，审慎处理制度的本土化问题，切忌盲目革新。

2022 年 12 月 19 日，由中共中央和国务院联合发布的《关于构建数据基础制度更好发挥数据要素作用的意见》明确指出，应“建立健全个人信息数据确权授权机制”，加快实现个人信息的合理使用；在 2023 年 2 月印发的《数字中国建设整体布局规划》中，亦将“畅通数据资源大循环”作为数字中国建设基础的重要内容。相信在此背景下，我国的可携带权终将从“纸面”走进“现实”，成为打通个人介入数据流转与分配的重要契机。

**参考文献**


[1] 程啸. 论个人信息权益 [J]. 华东政法大学学报，2023，26（1）：6 - 21.

[2] 王锡锌. 个人信息可携权与数据治理的分配正义 [J]. 环球法律评论，2021，43（6）：5 - 22.

[3] 丁晓东. 论个人信息概念的不确定性及其法律应对 [J]. 比较法研究，2022（5）：46 - 60.

[4] 刁云芸. 涉互联网平台作品数据集合的反不正当竞争法保护 [J]. 中国出版，2021（9）：24 - 28.

[5] 中国裁判文书网. 广东省佛山市中级人民法院（2016）粤 06 民终 9055 号判决书 [EB/OL]. [2023 - 04 - 09]. https://wenshu. court. gov. cn/website/wenshu/181107ANFZ0BXSK4/index. html.

[6] 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（1）：1 - 13.

[7] 中国裁判文书网. 杭州铁路运输法院（2019）浙 8601 民初 1987 号民事判决书 [EB/OL]. [2023 - 04 - 09]. https://wenshu. court. gov. cn/website/wenshu/181107ANFZ0BXSK4/index. html.

[8] 孔祥俊. 论反不正当竞争法的二元法益保护谱系——基于新业态新模式新成果的观察 [J]. 政法论丛，2021（2）：3 - 18.

[9] 王磊. 法律未列举的竞争行为的正当性如何评定——一种利益衡量的新进路 [J]. 法学论坛，2018，33（5）：126 - 136.

[10] 杨芳. 个人公开信息爬取中侵权法与竞争法的互动 [J]. 中国法律评论，2022（6）：143 - 157.

[11] 刘辉. 个人数据携带权与企业数据获取“三重授权原则”的冲突与调适 [J]. 政治与法律，2022（7）：114 - 131.

[12] 赵精武. 从保密到安全：数据销毁义务的理论逻辑与制度建构 [J]. 交大法学，2022（2）：28 - 41.

[13] 张凌寒. 数据生产论下的平台数据安全保障义务 [J]. 法学论坛，2021，36（2）：46 - 57.


（收稿日期：2023 - 04 - 10）


**作者简介：**

王欣辰（2000 - ），男，硕士研究生，主要研究方向：数据法学、知识产权法学。

沈廖佳（2001 - ），女，硕士研究生，主要研究方向：数据法学、互联网法学。


2023 年 4 月 8 日，中国（大湾区）工业互联网发展与安全峰会在深圳成功召开，来自产学研用各领域专家学者及工程技术人员 200 余人现场与会。北京航空航天大学网络空间安全学院副教授、博士生导师洪晟带来题目为《新时期工业互联网基础设施建设的内涵与发展机遇》的演讲，同时受邀担任专刊《工业互联网技术与应用》（本刊 2023 年第 3 期）的特约主编。专家简介如下：

洪晟　北京航空航天大学网络空间安全学院副教授、博士生导师，北京市安全学科带头人，北京市科委技术专家，北京航空航天大学“青年拔尖人才”，担任北京市安全科学与工程学会理事、中国系统工程学会系统可靠性工程委员会理事，从事网络信息安全、工业互联网安全、复杂系统通用质量特性技术等方向的教学和科研工作。他主持和参与 973 课题，国家重点研发课题，技术基础课题和国家自然科学基金等，跟该领域的国际专家有深入的合作，担任多个国际期刊和会议的编委，发表论文 60 余篇，其中 SCI 检索 30 余篇，授权国家发明专利 14 项，获国防科技进步一等奖 1 项。

# 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