论数据交易的法律结构文献研究

摘要：数据交易是数据价值实现的有效方式和途径，是动态的数据流动过程。以传统经济为基础所构建的法学理论与规则体系在调整数据交易法律问题过程中呈现出较多不适。因此，本文献研究试图对数据基础法学理论、数据交易相关私法理论、数据交易相关其他部门法理论的文献进行梳理与分析，总结提炼现有文献中发掘的数据交易过程中的主要制度困境和可能的突破路径。具体而言，构建数据交易制度理论应当以数据基础法律规范为基础前提，进而结合数据经济的自身特征进行数据交易规则的详细搭建。但法学理论与实践中对于数据基础法学理论的研究热烈而混乱。数据法律属性界定的观点众多且未成一致，虽然通过权利化路径对数据上的相关利益进行保护的路径较受推崇，但其应当如何形成逻辑缜密的权利结构则未见有较大突破，对于如何进行数据交易规则的制度构建也未见有较为体系和深入的思考。除此之外，对于数据主体、数据控制者及数据处理者的理论探讨与立法实践也值得仔细商榷。本文将通过细致的梳理分析，以期为数据交易法律问题研究提供科学严谨的文献参考。

关键词：数据；权利属性；数据交易；规制

现代信息技术及软硬件工具的产生和发展，为数据要素价值的实现提供了成熟可行的有效路径，让人类社会能发现和挖掘出其所蕴含的巨大财富。数据在企业商业模式构建、消费者行为分析、市场环境分析、个体画像等方面均发挥着基础要素的作用。总体上，以数据为生产要素的新经济模式已经成为现代经济社会的重要组成，新经济产业规模不断扩大，新经济产业形态不断变化，为人类社会蒙上科幻的面纱。但也正是这层面纱，影响了我们观察未来的视野，让我们对于经济社会走向的把控愈发无力。数据就好像流动的虚幻财富，财富价值显著但却又难以固定，让人贪恋而又难以捉摸。而数据的迷幻也同样使得法学研究和法律实践不知所往，法学家希望能够在法学理论和法律实践当中对数据加以明确，从而实现对这个新型生产要素的有效规范与保护，但现实却极为艰难。不过法学理论工作者和法律实践人员仍旧做着不懈的努力，试图拨开萦绕在数据之上的法学迷雾。就本文献综述而言，是笔者对在进行学位论文构思过程中所阅文献的整理与汇总，主要围绕着数据权属理论、数据交易理论、数据公法规制理论等展开，期望能够通过对这些文献的分析，能够总结和发现数据交易有效规范目的实现的主要理论困境，同时也为学位论文的写作提供具有科学性的理论基础，使得论证的过程更为规范与严谨，增强论证结论的有效性与可验证性。就既有文献本身而

言，主要集中于数据民法属性、数据相关公法规范理论的探讨，对于数据交易制度的详细展开与思考并不深入。以下笔者将结合论文构思的基本逻辑结构，对相应的文献进行针对性的梳理与评析。

一、数据主体及其数据法律属性的界定

（一）对于数据主体的既有规范与认识

数据主体及其相应权利义务配置的研究是数据交易实现的前提，只有当主体明确，并在明确的主体上进行权利义务体系的搭建，才能基于此进行有效的交易调整。

1. 国内外相关立法实践

我国《民法典》第 111 条规定：“自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”然后，《民法典》第 1034 条第 2 款对个人信息进行了界定，个人信息是以电子或者其他方式记录的能够多带带或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。我国《消费者权益保护法》明确规定，消费者享有个人信息依法得到保护的权利。《网络安全法》并没有提及“数据主体”的概念，只是规定了个人信息的定义，即以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息。虽然我国现行法律并没有对谁是数据主体作出明确规定，但一般认为数据主体就是通过个人数据已识别或可识别的自然人，具体是指通过姓名、身份证号、个人生物识别数据、住址、通信记录、财产数据、行踪轨迹、住宿数据、健康生理数据以及交易数据等能够被直接或间接识别到身份的自然人。

欧盟在其《通用数据保护条例》（GDPR）第 4 条则明确个人数据主体是一个已识别或可识别的自然人。美国《加州消费者隐私法案》（CPA）提及的“数据主体”不仅包括“特定消费者”，而且也包括“特定消费者的家庭”，甚至还包括数据经纪人（data broker）。

2. 数据主体之辩

姚佳曾在研究中探讨数据主体可不可以是企业呢？能不能是事业单位法人呢？对于这个问题，我们从既有研究中鲜有发现较为有说服力的、较为全面的论证分析，更多的研究是绕过了主体讨论，直接对数据的利用进行制度构建。[1]

[1] 参见姚佳：《企业数据的利用准则》，载《清华法学》2019 年第 3 期，第 115-118 页。

程啸认为，大数据时代的数据可分为个人数据和非个人数据两类，可以单独识别出特定自然人的数据或者与其他数据结合后能够识出自然人的数据为个人数据，反之则为非个人数据，数据的“可识别性”是区分两者的关键标准。[2]以可识别为基础划分个人数据与非个人数据很容易，但却很难为数据主体的细化分析提供有力的支撑，比如在非个人数据中有具体包括哪些数据主体类型呢？这种划分的依据或者标准又是什么呢？

综上，我们可以发现既有的个人与非个人的区分无益于数据交易相关法律问题的解决。当然数据主体问题的讨论也不可能单独进行，必然要与数据权利属性相结合，单独讨论数据主体的问题既不具有明显的理论意义，同时也不具有相应的实践意义。不能割裂数据主体与权属相互依存、相互验证的关系，在研究中要一体讨论分析。

（二）数据的权利属性与配置理论分析

数据权利属性的讨论可以说是整个数据法学理论研讨中核心要点，法学界与经济学界等相关理论学科在此问题上均有不少尝试。

1. 数据能否权利化保护之争

对此，当前法学界尚有较大争议。支持数据权利化保护和反对数据权利化保护的声音都很突出，虽然研究文献与成果都已经较为丰富，但始终未能形成较为统一或者说具有明显优势的理论结论。

梅夏英教授等数据权利否定论持有者就认为，数据缺乏民事权利客体的相关特征，因而也就无法通过民事权利加以保护，并且在分享经济的视野下，对于数据的控制应当需要合理的理由。[3]

龙卫球、沈卫星等支持以权利化方式对数据相关利益进行保护的学者则对此予以明确反对，并尝试在传统财产权理论内或者以传统财产权理论为基础进行创设性的权利架构。[4]

不过也有学者指出，数据权利化保护肯定论和否定论都具有不足之处，肖建华、柴芳墨就认为数据权利否定论忽视了数据的可支配性和财产性等特征，而数据权利肯定论就数据权利之概念、性质、主体、客体、内容等问题尚存分歧，没有一个清晰完整的定义。[5]

尽管两种理论都存在缺陷，但从当前的理论发展趋势和实践活动客观需求来看，数据权利化的保护路径更符合数据经济发展的实际。有学者也曾尝试对数据

---

[2] 参见程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018 年第 3 期，第 104-106 页。

[3] 参见梅夏英：《数据的法律属性及其民法定位》，载《中国社会科学）2016 年第 9 期；张阳：数据的权利化困境与契约式规制》，载《科技与法律》2016 年第 6 期，第 164-182 页。

[4] 参见龙卫球：《数据新型财产权构建及其体系研究》，载《政法论坛》2017 年第 4 期，第 63-77 页；申卫星：《论数据用益权》，载《中国社会科学》2020 年第 11 期，第 110-131 页。

[5] 参见肖建华、柴芳墨：《论数据权利与交易规制》，载（中国高校社会科学）2019 年第 1 期，第 85 页。

权利进行界定，如李爱君认为数据权利是指“主体以某种正当的、合法的理由要求或吁请承认主张者对数据的占有，或要求返还数据，或要求承认数据事实（行为）的法律效果”。[6]

本人在研究中发现，由于数据主体的权利对现有法律框架内的权益提出挑战，有关数据权利属于权利还是法益，是财产权范畴还是人格权范畴或者是其他利范畴尚无法确定，法理上存在争议，因而无法对其进行准确界定。这也是后续将尝试探索的问题之一。

2. 数据与信息的关系

肖建华、柴芳墨认为，数据外在形态虽表现为持续性海量增加的多结构类型数据集合，但其内在本质为信息。数据是信息的物理表达方式，而信息才是数据的心内涵，数据权利的本质是信息权。因此不妨借助信息权理论为数据权利作出抽象化定义：数据权利是数据在生产、收集、积累、储存、处理（加工）、传递、检索、使用、共享（传播）、消除等过程中在不同主体之间发生流转，从而产生不同性质内容的权利。在大数据交易中，无论是个人数据，抑或是匿名化的集合数据，其主体所享有的权利都可以统称为基于数据而产生的权利——数据权利，其本质是一种信息权。[7]

但上述数据与信息混淆讨论的研究路径并不可取，正如梅夏英教授指出的，数据与信息虽存有关联，但绝不能不加区分的合并讨论。信息和数据概念的区分具有法律意义，即可对现实中具体网络信息数据问题区分为两种基本问题类型：信息问题和数据问题，两种问题类型的区分标准在于当事人利益的侧重点、具体诉求的性质和救济的可能方式的不同上。[8]梅夏英教授亦指出，数据保护问题源于互联网的普及，只在数字技术语境中才有意义，故必须在区分信息问题和数据问题类型的背景下进行考察。[9]

3. 数据权利属性的界定与构成

王渊、黄道丽、杨松儒提出，关于数据权利的法律性质主要有财产权说、隐私权说、人格权说。[10]肖建华、柴芳墨在研究中对相关学说做了归纳提炼，财产权说认为数据权利具有财产权属性，主张将数据权利纳入财产权范畴。隐私权说为美国学界的主流观点，主张将数据权利纳入隐私权的范時。人格权说认为，数据权利体现了人格利益。[11]李晓阳则认为，个人数据权是一种多元权，其以个人

---

[6] 参见李爱君：《数据权利属性与法律特征》，载《东方法学》2018 年第 3 期，第 65 页。
[7] 参见肖建华、柴芳墨：《论数据权利与交易规制》，载《中国高校社会科学》2019 年第 1 期，第 85 页。
[8] 梅夏英：《信息和数据概念区分的法律意义》，载《比较法研究》2020 年第 6 期，第 153-155 页。
[9] 梅夏英：《企业数据权益原论：从财产到控制》，载《中外法学》2021 年第 5 期，第 1188-1207 页。
[10] 参见王渊、黄道丽、杨松儒：《数据权的权利性质及其归属研究》，载《科学管理研究》2017 年第 5 期，第 38-39 页。
[11] 参见肖建华、柴芳墨：《论数据权利与交易规制》，载《中国高校社会科学》2019 年第 1 期，第 84-86 页。

数据为权利客体，兼具人格权特性与财产权特性。[12]李爱君提出数据权利是一种具有财产权、人格权和国家主权属性的新型民事权利。[13]龙卫球甚至主张数据权利是种综合性的权利，其中包括数据经营产等不同的权能。[14]而从行业实践中，我们能发现仅就数据权利的转让来说，就是因为数据权利具有财产权属性，数据权利的转让才能够通过交易完成。[15]此外，也有很多观点主张，数据权利具有人格权属性，体现了人格尊严和自由意志。数据权利具有国家主权属性，国家保护公民个人数据安全，[16]防范和减少本国公民敏感数据受到外国政府和外国企业的侵害。

周永红等认为，尽管数据主体的权利最早涉及隐私权，与用户人格权属性相关的数据权利，同时要求相关机构在用户知情同意的情况下方能收集相关的个人信息。随着社会发展和大数据时代的要求，个人数据具有了财产权属性，且愈发受到重视。[17]程啸提出，自然人的个人数据的权利兼具人格权和财产权属性；数据企业的数据权利从性质上说属于独立于人格权、物权、债权、知识产权的新型财产权。[18]在我国的立法实践中，《民法典》第 127、1034-1039 条规定对数据提供保护，2019 年施行的《电子商务法》鼓励电子商务数据的开发应用，并明确国家保障电子商务数据依法有序自由流动，这为数据权利在我国作为一项人身性与财产性兼具的法律权利提供了法律依据。李晓阳基于个人数据、政府数据与商业数据在法律性质和数据功能上的巨大差别，提出对于以上三者的法律保护与规

---

12 参见李晓阳：《大数据背景下商业数据的财产性》，载《江苏社会科学》2019 年第 5 期。参见温：个人数据权利体系论》，载《甘肃政法学院学报》2019 年第 2 期，第 159-161 页。

13 参见李爱君：《数据权利属性与法律特征》，载《东方法学》2018 年第 3 期，第 67-71 页。

14 参见龙卫球：《数据新型财产权构建及其体系研究》，载《政法论坛》2017 年第 4 期，第 74-77 页。

15 2014 年 2 月以来，我国一些地方建立了大量数据交易所、数据交易中心等，主要有中关村数海大数据交易平台、贵阳大数据交易所、长江大数据交易所、武汉东湖大数据交易中心、徐州大数据交易中心、河北大数据交易中心、哈尔滨数据交易中心、江苏大数据交易中心、上海数据交易中心、陕西西咸新区大数据交易所、江苏大数据交易中心、安徽大数据交易中心等十余家大数据交易平台。另外，我国一些地方还布了大数据交易规则，如安徽大数据交易中心制定的《安徽大数据交易规则》、贵阳大数据交易所制定的《贵阳大数据交易所 702 公约》、哈尔滨大数据交易中心制定的《哈尔滨数据交易规则》、江苏大数据交易中心制定的《大数据交易用户协议》。参见李爱君：《数据权利属性与法律特征》，载《东方法学》2018 年第 3 期。

16 国家网信办出台的《个人信息和重要数据出境安全评估办法（征求意见稿）》第 8 条规定：“数据出境安全评估应重点评估以下内容：（一）数据出境的必要性；（二）涉及个人信息情况，包括个人信息的数量、范围、类型、敏感程度，以及个人信息主体是否同意其个人信息出境等；（三）涉及重要数据情况，包括重要数据的数量、范围、类型及其敏感程度等；（四）数据接收方的安全保护措施、能力和水平以及所在国家和地区的网络安全环境等；（五）数据出境及再转移后被露、毁损、改、用等风险；（六）数据出境及出境数据证聚可能对国家安全、社会公共利益、个人合法利益带来的风险；（七）其他需要评估的重要事项。”第 9 条规定：“出境数据存在以下情况之一的，网运营者应报请行业主管或监管部组织安全评估：（一）含有或计含有 50 万人以上的个人信息；（二）数据量超过 10000；（三）包含核设施、化学生物、国防军工、人健康等领域数据，大型工程活动、海洋环境以及敏感地理信息数据等；（四）包含关键信息基础设施的系统洞、安全防护等网络安全信息；（五）关键信息基础设施运营者向境外提供个人信息和重要数据；（六）其他可能影响国家安全和社会公共利益，行业主管或监管都认为应该评估。行业主管或管部门不明确的、由国家网信部门组织评估。”

17 参见周永红、赵维：《大数据交易背下用户个人数据权利的保护研究》，载《数字图书馆论坛》2019 年第 2 期，第 24-25 页。

18 参见程啸：《论大数据时代的个人数据权利》，载《（中国社会科学）2018 年第 3 期，第 106 页。

范路径应当予以区分。[19]相丽玲、高倩云、阮爽等学者在对各国及国际组织、区域性组织出台的与个人数据权利相关的法律法规的内容进行整理后，提出个人数据权包括个人数据知情同意权、被遗忘权、数据可携带权和个人数据财产权四种权利。[20]温昱提出，个人数据承载了数据主体的人格利益和财产利益，个人数据权利兼具人格权与财产权双重属性，个人数据权利体系分为个人数据人格权与个人数据财产权，其中，个人数据人格权包括自决权、同意权、修改权和被遗忘权，个人数据财产权包括使用权、收益权和数据可携权。[21]

这些观点都是从数据权利的人格权属性和财产权属性角度出发，本质上并无区别，但这些新提出的权利或法益对于丰富数据权利的内涵从而推进法律实践的相关探索很有裨益。

4. 延伸权利。

首先是知情同意权。石丹在研究中指出，传统法律构架如何对个人信息保护和数据利用主要是从用户角度出发，将个人信息限制于隐私权或者人格权之中，只在“知情同意”基础上，允许数据业者收集、加工和处理有限的用户数据。[22]例如，我国《民法典》第 1035 条第 1 款规定：“处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理，并符合下列条件：（一）征得该自然人或者其监护人同意但是法律、行政法规另有规定的除外；（二）公开处理信息的规则：（三）明示处理信息的目的、方式和范围；（四）不违反法律、行政法规的规定和双方的约定。”《网络安全法》第 4 条规定：“网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。”“个人数据知情权”是“知情权”的一种。阮爽在研究中介绍，欧盟 GDPR 确认了知情同意原则作为收集和处理个人数据合法性要件的重要地位，并在第 7 条规定了详尽的同意要件、同意的撤回及其效力、同意是否为自愿作出的判断标准，明确个人数据处理负责人必须承担获得同意的证明责任。[23]而个人数据知情权在各国或地区法律中主要体现在两个方面：一是个人被告知同意

---

[19] 参见李晓阳：《大数据背景下商业数据的财产性》，载江苏社会科学）2019 年第 5 期，第 166-167 页。

[20] 参见相丽玲、高倩云：《大数据时代个人数据权的特征、基本属性与内容探析》，载《情报理论与实践》2018 年第 9 期，第 47-50 页；阮爽：《<欧盟个人数据保护通用条例>及其在德国的调适评析》，载《德国研究》2018 年第 3 期，第 89-103 页。

[21] 参见温昱：《个人数据权利体系论纲》，载《甘肃政法学院学报》2019 年第 2 期，第 89-92 页。

[22] 参见石丹：《大数据时代数据权属及其保护路径研究》，载《西安交通大学学报（社会科学版）》2018 年第 3 期，第 79 页。

[23] 参见阮爽：《欧盟个人数据保护通用条例及其在德国的调适评析》，载《德国研究》2018 年第 3 期，第 95 页。

或拒绝的权利；二是查询权与修改权。[24]关于查询权和修改权的定义，相丽玲、高倩云介绍，查询权是指个人有权向个人数据持有者查询其个人数据的来源、类别、内容、加工状态及加工目的等的权利；修改权则是指个人有权向个人数据持有者就其个人数据的完整性、准确性和及时性进行补充或更改的权利，修改不准确或不正当的个人数据，确保用户人格画像不受歪曲。[25]如果用户不知情或不同意授权，那么任何个人、企业、交易平台对个人数据进行交易的行为都属于违法行为。周永红、赵维更进一步指出，对于收集到的用户数据及其使用目的，应确保数据所有权人拥有知情权和查询权，如用户应知道将要收集的数据范围和数据的用途等。[26]《民法典》第 1037 条规定：“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。自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除。”《网络安全法》第 43 条规定，用户发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息。2012 年《全国人大常委会关于加强网络信息保护的决定》第 2 条规定：“网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不得违反法律、法规的规定和双方的约定收集、使用信息。网络服务提供者和其他企业事业单位收集、使用公民个人电子信息，应当公开其收集、使用规则。”我国《信息安全技术公共及商用服务信息系统个人信息保护指南》第 4.2 条规定，个人信息管理者在使用信息系统对个人信息进行处理时应遵循以下基本原则：“…e）公开告知原则一对个人信息主体要尽到告知、说明和警示的义务。以明确、易懂和适宜的方式如实向个人信息主体告知处理个人信息的目的、个人信息的收集和使用范围、个人信息保护措施等信息。d）个人同意原则一一处理个人信息前要征得个人信息主体的同意。第 5.3.6 条规定：“个人信息主体发现其个人信息存在缺陷并要求修改时，个人信息管理者要根据个人信息主体的要求进行查验核对，在保证个人信息完整性的前提下，修改或补充相关信息。”第 5.3.7 条规定：“个人信息主体要求对其个人信息进行查询时，个人信息管理者要如实并免费告知是否拥有其个人信息、拥有其个人信息的内容、个人信息的加工状态等内容，除非告知成本或者请求频率超出合理的范围。”第 5.2.3 条规定：“处理个人信息前

[24] 《信息安全技术个人信息安全规范》第 81 条和第 82 条分别定了“个人信息查询”和个人信息更正”的权利。

[25] 参见相丽玲、高云：《大数据时代个人数据权的特征、基本属性与内容探析》，载《情报理论与实践》2018 年第 9 期，第 48 页。

[26] 参见周永红、赵维：《大数据交易背景下用户个人数据权利的保护研究》，载《数字图书馆论坛》2019 年第 2 期。

要征得个人信息主体的同意，包括默许同意或明示同意。”信息安全技术个人信息安全规范》第 3.6 条对“明示同意”作了详细解释，即“个人信息主体通过书面口头等方式主动作出纸质或电子形式的声明，或者自主作出肯定性动作，[27]对其个人信息进行特定处理作出明确授权的行为”。另外，该规范第 3.7 条还规定了“授权同意”，[28]即“个人信息主体对其个人信息进行特定处理作出明确授权的行为”；第 5.4 条还规定了收集个人信息时的授权同意的具体要求，[29]并在第 5.6 条规定了征得数据主体授权同意的例外。[30]

其次是被遗忘权。“被遗忘权”并不是一个新概念。郭小安、雷闪闪、丁晓东曾在发表中梳理，“被遗忘权”其形可上溯至 20 世纪七八十年代某些国家，如德国（1977 年）、法国（1978 年）、英国（1984 年）、荷兰（1989 年）出台的数据保护法中提到的删除权、忘却权、遗忘权、更正权、修改权等与“被遗忘权”相关的内容，“一个人犯错后一旦改过自新，应该使他的名声免于被过去的错误所累”是其背后的法理。欧盟在 2012 年《关于涉及个人数据处理的个人保护以及此类数据自由流动的第 2012/72、73 号草案》中首次提出了“被遗忘权”，欧盟法院在 2014 年西班牙谷歌案中确立了“被遗忘权”。[31]我国首例“被遗忘权”案件是 2015 年任甲玉诉北京百度网讯科技有限公司人格权纠纷案，法院认为我国没有认可“被遗忘权”，其并非我国民事权利体系中的法定权利，因而判决原告败诉。尽管 2013 年《信息安全技术公共及商用服务信息系统个人信息保护指南》第 5.5.1 条规定，“当个人信息主体有正当理由要求删除其个人信息时，及时删除个人信息”，但这一指南并非法律、行政法规或规章，[32]同时要求个人

---

[27] 肯定性动作包括个人信息主体主动勾选、主动点击“同意”“注册”“发送”及“投打”、主动填写或提供等。

[28] 授权同意包括通过积极的行为作出授权（即明示同意），或者通过消极的不作为而作出授权（如信息采集区域内的个人信息主体在被告知信息收集行为后没有离开该区域）。

[29] 收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得个人信息主体的授权同意；收集个人敏感信息前，应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意表示。收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意；收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意等。

[30] 具体包括：与个人信息控制者履行法律法规规定的义务相关的；与国家安全、国防安全直接相关的；与公共安全、公共卫生、重大公共利益直接相关的；与刑事侦查、起诉、审判和判决执行等直接相关的；出于维护个人信息主体或其他个人的生命、财产等重大合法权益但又很难得到本人授权同意的；所涉及的个人信息是个人信息主体自行向社会公众公开的；根据个人信息主体要求签订和履行合同所必需的；从合法公开披露的信息中收集个人信息的，如合法的新闻报道、政府信息公开等渠道维护所提供产品或服务的安全稳定运行所必需的，如发现、处置产品或服务的故障；个人信息控制者为新闻单位，且是其开展合法的新闻报道所必需的；个人信息控制者为学术研究机构，出于公共利益开展统计或学术研究所必要，且其对外提供学术研究或描述的结果时，对结果中所包含的个人信息进行去标识化处理的。

[31]参见郭小安、雷闪闪：《“数据被遗忘权”实施困境与我国的应对策略》，载《理论探索》2016 年第 6 期，第 109 页；丁晓东：《被遗忘权的基本原理与场景化界定》，载《清华法学》2018 年第 6 期，第 95-97 页。

[32] 《信息安全技术个人信息安全规范》与《信息安全技术公共及商用服务信息系统个人信息保护指南》的法律地位相同。其第 8.3 条对“个人信息除”作出如下规定：“对个人信息控制者的要求包括：a）符合以下情形，个人信息主体要求删除的，应及时删除个人信息：1）个人信息控制者违反法律法规规定，收集、

信息主体请求删除其个人信息时必须提供“正当理由”，并非赋数据主体被遗忘权。当然，个人数据权利保护应符合比例原则。金晶指出，当删除权可能与言论自由、信息自由、公共知情权等公共价值相冲突时，可能会受到限制。[33]例如，欧盟 CDPR 第 17 条第 3 款规定，五种情形下免除责任主体的删除义务：（1）行使言论自由权；（2）守法律义务或符合公共利益的职务执行或委托数据控制者行使公权力所必需；（3）为实现公共卫生领域的公共利益理由；（4）为实现公共利益、科学历史研究或统计目的；（5）为确立、行使或防御法律上请求时，应在必要范围内进一步保留个人数据合法。此外，一些学者对于被遗忘权提出了较多质疑，如梅夏英教授认为被遗忘权涉及多种价值的冲突，目前应对其保护范围进行严格限定，在最必要的情形下尝试引进，以逐步建立被遗忘权可能的法律地盘。[34]

再者是数据可携带权。相丽玲、高倩云在研究中指出，作为一种新型数据权利，数据可携带权是在 2016 年欧盟 GDPR 第 20 条首次正式提出并进行界定的。所谓“数据可携带权”，是指赋予数据主体从数据持有者处获取其个人数据以及将个人数据从一个数据持有者处无障碍地转移到另一个数据持有者处的权利。[35]邓刚宏提出，欧盟数据可携带权适用于基于数据主体同意或为履行合同而实施的自动化处理行为，其内容包括副本获取权和数据转移权前者为数据主体有权从数据控制者处下载自己的个人数据，后者为数据主体有权将其个人数据直接无障碍地从一个控制者处转移至另一个控制者处且无须事先下载。[36]金晶在研究中指出，数据可携带权是一项具有高度人身性的权利，不得移转给第三人，不得继承，但可代理行使，旨在平衡个人数据流动的自由和管制，使数据主体能以简明方式迁移数据并更好地控制个人数据。数据可携带权表明数据控制者对个人数据不具有控制权，仅负有配合义务，避免数据控制者争夺用户的个人数据，进而促进个人数据的流动，[37]这样能够很好地解决数据归属问题。

最后是个人数据财产权。虽然个人数据的确具有商业价值，但对于个人数据能否财产化和商品化，学界尚存争议，因而各国或地区个人数据保护法中主要解

使用个人信息的；2）个人信息控制者违反与个人信息主体的约定，收集、使用个人信息的。b）个人信息控制者违反法律法规定或违反与个人信息主体的约定向第三方共享、转让个人信息且个人信息主体要求副除的，个人信息控制者应立即停止共享、转让的行为，并通知第三方及时除。c）个人信息控制者违反法律法定或违反与个人信息主体的约定公开披露个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。”

[33] 参见金晶：《欧盟（一般数据保护条例）：演进、要点与疑义》，载《欧洲研究》2018 年第 4 期，第 17 页。

[34] 梅夏英：《论被遗忘权的法理定位与保护范围之限定》，载《法律适用（司法案例）》2017 年第 16 期，第 50-53 页。

[35] 参见相丽玲、高倩云：《大数据时代个人数据权的特征、基本属性与内容探析》，载《情报理论与实践》2018 年第 9 期，第 49 页。

[36] 参见邓刚宏：《大数据权利属性的法律逻辑分析》，载《江海学刊》2018 年第 6 期，第 149 页。

[37] 参见金晶：《〈欧盟一般数据保护条例〉：演进、要点与疑义》，载《欧洲研究》2018 年第 4 期，第 14 页。

决的是个人数据人格权的保护问题，如欧盟 DPR 和德国相关法律都没有提到个人数据财产权的保护问题。由于数据资源直接或间接体现出了一定的经济价值，个人数据人格权保护模式限制了数据产业发展的需求，为促进大数据时代下的数据大规模流通和交易，劳伦斯·莱斯格（ Lawrence Lessig）先提出了个人数据财产化相关理论，主张通过赋予个人数据财产化权利，从而突破个人数据的人格权保护限制。[38]正如石丹在研究中归纳的，作为平衡数据产业发展和个人数据保护的个人数据财产权逐步得到各方认可，在个人数据人格权保护和财产化法律路径上回应个人数据上的利益分配问题。[39]个人数据财产权实际上是在个人数据保护和利用之间寻找到的平衡点。正如相丽玲、高云在发表中分析的，个人有权合理使用、处理或交易其个人数据，并获取相应的利益——因此，所谓个人数据财产权，指的是个人享有对其个人数据的开发利用的处分与收益的权利或法益。[40]除了上述权利之外，还需注意的是，《信息安全技术个人信息安全规范》还规定个人信息主体有权“注销账户”，要求个人信息控制者应向个人信息主体提供简便易操作的注销账户方法；受理注销账户请求后，如需要人工处理的应在承诺时限内（不超过 15 个工作日）完成核查和处理；注销过程不应设置不合理的条件或提出额外要求增加个人信息主体的义务；个人信息主体注销账户后，应及时删除其个人信息或匿名化处理。“个人信息主体注销账户”这一权利值得我们在研究和司法实践中重视。其实，个人信息财产权还是要回到数据权利化理论中进行讨论，这也属于数据权利的组成部分。

[38] 参见（美）劳伦斯·莱斯格：《代码 2.0：网络空间中的法律》，李旭、沈伟伟译，清华大学出版社 2009 年版，第 20 页。转引自石丹：《大数据时代数据权属及其保护路径研究》，载《西安交通大学学报（社会科学版）》2018 年第 3 期，第 79 页。

[39] 参见石丹：《大数据时代数据权属及其保护路径研究》线《西安交通大学学报（社会科学版）》2018 年第 3 期，第 79 页。

[40] 参见相丽玲、高云：《大数据时代个人数据权的特征、基本属性与内容探析》，载《情报理论与实践》2018 年第 9 期，第 46-47 页。

二、数据控制者与数据处理者的权利义务配置

（一）数据控制者相关既有规范及理论认知

1. 既有规范中对于数据控制者的规定

对于数据权利体系中各主体的地位和作用，李勇坚旗帜鲜明的指出，数据主体、数据控制者、数据处理者等各主体在整个数据权利体系中都占有一定的地位。如何将权利与义务在这些主体之间进行平衡，对于数据权利体系的构建以及对个人数据的保护至关重要。[41]对于“数据控制者”的法律文本起源，高楚南在发表中指出，“数据控制者”是出现在经济合作与发展组织（OECD）于 1980 年发布的《隐私保护与个人数据跨境流动指南》（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data），其定义是：根据各国法律能够决定个人数据内容和用途的主体，无论该数据是由其本人还是由其代理人收集、存储、处理和传播的。”2013 年，OECD 颁布了修订后的《隐私保护与个人数据跨境流动指南》，但沿用了 1980 年版指南中关于数据控制者的定义。[42]周坤琳认为欧盟 GDPR 堪称全球个人数据保护法律体系的典范，以保护“个人数据”为重要内容，主要规范的义务主体是“数据控制者”和“数据处理者”。GDPR 第 4 条第 7 款规定，数据控制者是能单独或联合决定个人数据处理目的和处理方式的自然人、法人、公共机构、行政机关或其他非法人组织。个人数据处理目的和方式，以及控制者或可能成为数据控制者的具体标准由欧盟或其成员国的法律予以规定。成为数据控制者的关键，在于能够单独或联合决定个人数据处理的目的和方式。数据控制者的类型主要包括自然人、法人以及行政机关等。与 GDPR 同一天生效的德国《联邦数据保护法》指出，数据控制者是指任何为自身利益或委托他人（机构）收集、处理或使用个人数据的人或机构。英国《数据保护法》区分了数据控制者与数据处理者，并对数据控制者、数据处理者的义务进行了具体规定。[43]

不同于以往美国针对特定行业或者特定隐私权事项的法案，美国《加州消费者隐私法案》（CCPA）广泛适用于收集加州消费者个人信息的企业。CCPA 中提到的企业的概念类似于数据控制者与数据处理者，并从营业收入、信息规模、信息收入等维度对企业进行定义。根据 CCPA，企业是指为股东或其他所有人的

---

[41] 李勇坚：《个人数据权利体系的理论构建》，载《中国社会科学院研究生院学报》，2019 年第 5 期，第 96-97 页。

[42] 高楚南：《欧盟数据控制者的义务：源起、变迁及其缘由》，载《图书馆论坛》，2019 年第 3 期，第 141 页。

[43] 周坤琳：《互联网金融业信息控制者与信息处理者法律义务与责任研究——基于风险控制的探索》，载《海南金融》2019 年第 9 期，第 53-54 页。

利润或经济利益而组织或经营的独资企业、合伙企业、有限责任公司、协会或其他法律实体。这些实体收集消费者的个人信息或代表消费者收集了这些信息，并且单独或与他人共同确定处理消费者个人信息的目的和方法。这些实体在加州从事经营活动并且满足以下一个或多个条件：（1）根据 CCPA 第 1798.185 条（a）款第 5 项的规定调整后，年度总收入超过 2500 万美元；（2）为了商业目的，每年单独或组合购买、收集、出售或共享 50000 人甚至更多的消费者、家庭或设备的个人信息；（3）年营收的 50%或更多来自销售消费者个人信息。任何如前述所定义的、控制或受企业控制的和与企业共享共同品牌的任何实体也属于企业的范畴。“控制”或“被控制”是指对企业任何一类有投票权的股票中已发行股票有超过 50%的所有权或投票权；以任何方式控制大多董事的选举或行使类似职能的个人；或者有对公司管理层施加影响的权力“共同品牌”是指共享名称、服务标记或商标。通过这些规定可以看出 CCPA 试图将消费者隐私保护义务限定在规模较大、收集了较大数量消费者个人信息并以消费者个人信息为主要营利手段的企业，从而平衡产业发展与消费者个人信息保护之间的矛盾。[44]

我国《民法典》在第一编“总则”第五章“民事权利”中规定，自然人的个人信息受法律保护。我国《消费者权益保护法》也明确规定，消费者享有个人信息依法得到保护的权利。但这些分散的立法并未拟制特定的义务主体。在我国的立法中，仅有为数不多的几部法律规范对信息利用主体进行了界定。2012 年通过的《全国人大常委会关于加强网络信息保护的决定》中提及的义务主体是网络服务提供者和其他企业事业单位。《网络安全法》是我国第一部全面规范网络空间安全管理的基础性法律，其中并没有“数据控制者”的概念，其规范的主体有网络运营者、关键信息基础设施的运营者、网络产品或服务的提供者即电子信息发送服务提供者和应用软件下载服务提供者。“网络运营商”的概念与“数据控制者”并不能等同，网络运营商限于网络业务与服务的提供者，而数据控制者的范围更加广泛。《电子商务法》中有关个人信息保护的义务主体是电子商务经营者，是通过互联网等信息网络从事销售商品或者提供服务的经营活动的自然人、法人和非法人组织，包括电子商务平台经营者、平台内经营者以及通过自建网站、其他网络服务销售商品或者提供服务的电子商务经营者。2018 年实施的《网络安全等级保护测评机构管理办法》采用了“网络运营者”的概念。此外，《信息安全技术个人信息安全规范》规定，个人信息控制者是基于特定目的，经信息主体明确同意或认可进行个人信息的收集、处理、存储、利用的机构或个人。这一定义与欧盟法中对数据控制者的定义类似。在《民法典》第四编“人格权”第六章“隐私权和个人信息保护”中，也提到了信息收集者、信息控制者，并规定信

[44] CCPA 第 1798.140 条

息收集者、信息控制者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、墓改、丢失；发生或可能发生个人信息泄露、甚改、丢失的，应当及时采取补救措施，依照规定告知被收集者并向有关主管部门报告。同时规定国家机关及其工作人员对于履行职责过程中知悉的自然人的隐私和个人信息，应当予以保密，不得泄露或向他人非法提供。[45]

不同的学者也针对数据领域的主体提出过类似概念，黄震、蒋松成认为数据控制者是合法获取并实际控制数据，能够确定数据处理的目的、条件和手段，依照法律或合同约定对数据享有完整或部分财产权利，并承担相应义务的组织和个人。[46]另外，在个人信息保护法领域中存在的与普通信息主体对应的义务主体信息管理者。信息管理者是与数据控制者相类似的主体，同样是对个人数据进行收集、处理与利用的主体。

2. 对数据控制者范围的厘定

我们应根据数据主体类型化来探讨这个问题。

首先，是行政机关等公权力机构。黄震、蒋松成指出，行政机关是最早的数据控制者。20 世纪 60 年代，欧洲开始通过计算机自动处理技术积累个人数据，使个人数据的收集速度和范围发生质变，政府成为名副其实的数据控制者。由于国家强制力和公权力的存在，同时因为其行为主要是履行国家机关的职责，行政机关在收集和使用数据的过程中，一般无须征得对方的同意，且其掌握的除公开信息如公司登记信息、持股比例等之外，还有很多个人信息，如身份信息、婚姻状况与家庭住址等。[47]林红、沈健归纳行政机关收集个人信息的方式有以下几种：行政登记。这是行政机关获取个人信息最常见的方式，如户口登记、婚姻登记、税务登记、工商登记等；行政统计。这是行政机关为分析国家当前形势，预测未来发展方向所采取的一种重要手段；其他行政行为。这主要是指行政机关在日常履行职责时会获取一些个人信息，如交通管理部门为维护公共交通而安装设备采集照片、声音等信息，鉴定机构为侦破案件而采集指纹、DNA 等个人信息。[48]由于行政机关掌握着大量的企业数据信息，因而是重要的数据控制者。

其次，是法人与非法人组织。20 世纪 80 年代之后，信息网络发展迅猛，数据生成量成几何倍数增长，数据挖掘和分析技术的发展不断凸显数据的商业价值。郑令晗指出，在市场驱动下，数据控制者开始由公权力机构转向私人企业和社会机构，欧洲在立法上也出现新的化。大量的法人与非法人组织在提供服务的过程

---

[45] 潇湘晨报：《法学家王利明谈民法典编纂：互联网时代防隐私侵害成严峻挑战》，https://baijiahao.baidu.com/s?id=1666927132676932425&wfr=spider&for=pc，2021 年 10 月 6 日访问。

[46] 黄震、蒋松成：《数据控制者的权利与限制》，载《陕西师范大学学报（哲学社会科学版）》，2019 年第 6 期，第 36-37 页。

[47] 黄震、蒋松成：《数据控制者的权利与限制》，载《陕西师范大学学报（哲学社会科学版）》，2019 年第 6 期，第 37 页。

[48] 林红、沈健：《浅析行政机关与个人信息的保护问题》，载《科学大众》，2019 年第 4 期，第 46 页。

中必须先获取足够的个人信息，特别是各种互联网企业，如谷歌、Facebook、阿里巴巴、腾讯等，它们手中掌握了海量的个人信息，是最为典型的数据控制者。掌握着先进互联网技术的美国在数据竞争中占尽优势，并培育出 IT 界“八大金刚”（即思科、IBM、谷歌、高通、英特尔、苹果、甲骨文、微软），这些企业的产品涵盖教育、医疗、体育、金融、交通、军警等领域，小到智能手机，大到服务器集群，均有它们的身影，成为名副其实的数据控制者。[49]技术和市场的发展催生了数据制者形式的多样化和复杂化，我国相关立法就规定了如网络服务提供者、网络运营商、电子商务经营者、个人信息控制者等多种主体。[50]

最后是自然人。黄震、蒋松成认为互联网技术和数据技术的发展使自然人有成为数据控制者的可能。自然人在数据存储规模、数据分析与处理能力方面相较于其他形式的数据控制者而言有不小的差距，但个人形式的数据分析师和数据产业从业者正越来越多。[51]

在数据控制者当中还存在着种比较特殊的情形，那就是共同数据控制者。什么是共同数据控制者呢？GDPR 第 26 条规定：（1）两个或两个以上的数据控制者共同决定处理的目的和方式时，为共同数据控制者。共同数据控制者应以透明的方式，彼此安排时间，确定各自遵守本条例所规定的义务的责任，特别是关于数据主体行使其各自关于本条例第 13、14 条规定的提供信息的义务，对数据控制者生效的欧盟法律或欧盟成员国法律已对数据控制者各自的责任作出规定的除外。（2）第 1 款规定的安排应当适当反映共同数据控制者各自的职责及相对数据主体关系。数据主体应可得知该安排的实质内容。（3）不论第 1 款规定的安排条款为何，数据主体可以依据本条例向任何一个数据控制者行使权利。[52]我国《信息安全技术个人信息安全规范》规定，当个人信息控制者与第三方为共同个人信息控制者时（如服务平台与平台上的签约商家），个人信息控制者应通过合同等形式与第三方共同确定应满足的个人信息安全要求，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，并向个人信息主体明确告知。共同数据控制者是一个值得关注的法理领域，正如郑令晗在研究中指出的，无论行为主体是“单独”还是“共同”确定个人数据处理活动的目的和方式，并不影响被认定为数据控制者，只决定其是构成单独的数据控制者还是共同数据控制者。确定共同数据控制者之后，数据主体可以根据 GDPR 向任一共同数据控制者行使其权利或寻求侵权救济。[53]

---

[49] 郑令晗：《GDPR 中数据控制者的立法解读和经验探讨》，载《图书馆论坛》，2019 年第 3 期，第 148 页。

[50] http://www.64365.com/zs/1210142.aspx，2021 年 9 月 12 日访问。

[51] 黄震、蒋松成：《数据控制者的权利与限制》，载《陕西师范大学学报（哲学社会科学版）》，2019 年第 6 期，第 40 页。

[52] https://zhuanlan.zhihu.com/p/83200590，2021 年 1 月 20 日访问。

[53] 参见郑令晗：《GDPR 中数据控制者的立法解读和经验探讨》，载《图书馆论坛》2019 年第 3 期，第 149

3. 数据控制者的权利设置

数据控制者是否也可以享有数据权利呢？OECD 于 1980 年发布的《隐私保护与个人数据跨境流动指南》的解释备忘录指出，不论是否具备法人资格的商业企业、协会和团体的相关数据与个人数据都应受到保护，应将保护个人数据的规则扩张适用于前者。在 OECD 于 2010 年筹备修订《隐私保护与个人数据跨境流动指南》时，专家组明确建议将“洞察个人和团体的趋势、行动、利益和活动的条件下的数据分析范畴”作为修改内容之一。1981 年欧洲系列条约第 108 号《关于个人数据自动化处理的个人保护公约》第 3 条规定，“本公约也适用于团体、协会、基金会、公司、企业和其他直接或间接由个人组成的机构的信息保护，无论这些机构是否具有法律人格”，即将法人和非法人组织列为数据权利主体。另外，挪威《个人数据登记法》规定个人数据为“可追踪到可识别的个人、组织或机构的数据”，丹麦《数据保护法》规定该法也适用于法人数据。在我国，根据《网络安全法》第 1 条、[54]第 12 条第 1 款以及《电子商务法》第 25 条等法律规定，[55]数据权利主体主要包括自然人、法人、非法人组织等。所以，各国立法一般都认可上述两者的数据权利主体地位。个人数据因身份识别功能而具有强烈的人身性，其数据权利理应具有财产性和人身性。这个观点得到众多学者的支持。李晓阳认为，法人等团体组织也有相关的数据需要保护，比如公司的商业秘密；又如，对自然人等数据的匿名化使其去身份化且无法还原，这些被处理后的数据成了具有财产属性的商业数据。[56]邢会强老师也旗帜鲜明地支持自然人、法人和非法人组织拥有数据权利。[57]肖建华、柴芳墨则认为政府可以作为数据权利主体。[58]在司法实践中，我们能看到，各国的确通过立法对自然人和法人等团体组织以及政府的数据进行一体保护。石丹认为，数据控制者和处理者作为数据权利主体，对企业的相关数据享有一定的权利。此处的企业数据既包括反映企业基本状况的数据（如企业财务数据、运营数据和人力资源数据），也包括企业通过合同授权直接或间接采集的经过匿名化处理获得的个人数据集合，即无法识别出特定自然

页。

[54] 《网络安全法》第 1 条规定：“为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。”

[55] 《网络安全法》第 12 条第 1 款规定：“国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。”《电子商务法》第 25 条规定：“有关主管部门依照法律、行政法规的规定要求电子商务经营者提供有关电子商务数据信息的，电子商务经营者应当提供。有关主管部门应当采取必要措施保护电子商务经营者提供的数据信息的安全，对其中的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。”等相关法律规定，数据权利主体主要包括自然人、法人、非法人组织等。可见，尽管团体组织与自然人在各国立法上的保护程度有所区别，但一般都予以认可其数据权利的主体地位。

[56] 李晓阳：《大数据背景下商业数据的财产性》，载《江苏社会科学》，2019 年第 5 期，第 26 页。

[57] 邢会强：《大数据交易背景下个人信息财产权的分配与实现机制》，载《法学评论》2019 年第 6 期；王肃之：《大数据环境下法人信息权的法律保护》，载《当代经济管理》，2018 年第 8 期，第 89 页。

[58] 肖建华、柴芳墨：《论数据权利与交易规制》，载《中国高校社会科学》，2019 年第 1 期

人的数据（非个人信息的数据）。[59]而且，《网络安全法》第 42 条第 1 款规定：“网络运营者不得泄露、甚改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个信息。但是，经过处理无法识别特定个人且不能复原的除外。”可见，数据控制者和处理者对其合法收集的个人数据和非个人信息的数据享有应当受到法律保护的权利。但是，程啸提醒我们，个人数据的匿名化是相对的，在大数据时代，大量的匿名化数据重新整合有可能使特定个人的身份信息被识别从而导致泄露隐私。对这类个人数据的使用应受到限制。[60]此外，数据控制者和处理者的数据权利是否能够具有类似个人数据的数据知情权、数据可携带权等权利？对此，李扬、李晓宇的观点是，个人数据的上述权利源自个人的法定人格权，如无法律规定，不能将个人数据权直接适用于企业。企业数据权利有积极权能与消极权能两种类型。首先，企业数据权利具有积极权能，主要为存储数据权利、加工利用数据权利、交易处分数据并获取报酬权利等。其次，企业对企业数据权利具备排斥他人不当干涉的对世效力的消极权能，即权利人有权要求侵权人停止侵害、删除侵权数据、赔偿损失。例如，《网络安全法》第 43 条规定：“个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。”第 44 条规定：“任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。”[61]

4. 数据控制者的义务

李勇坚指出，在很多情况下，数据控制者收集数据被认为是一种交换，即这些控制者通过提供免费服务，来获得消费者的数据。如前所述，在数据权利体系中，必须承认数据控制者的权利。数据控制者的核心权利在于可以对非指向性数据进行开发和利用以及交易。[62]黄震、蒋松成等学者更一进步提出，出于对个人数据的保护及维护数据产业的有序发展，无论数据控制者依靠何种权利基础获得对数据的控制，在获得数据控制权的同时，必然要承担相应的责任和义务。[63]黄道丽、张敏明认为，我国互联网发展环境、运营特点、市场成熟度与国外存在差异，个人数据权的基础立法存在不足。他们提出，在新技术背景下，不仅应将告知义务、合法获得义务安全保障义务等纳入数据控制者的义务体系中，还应对风

---

[59] 石丹：《大数据时代数据权属及其保护路径研究》，载《西安交通大学学报（社会科学版）》2018 年第 3 期，第 80 页。

[60] 程啸：《论大数据时代的个人数据权利》，载《中国社会科学》，2018 年第 3 期，第 109-110 页。

[61] 李扬、李晓宇：《大数据时代企业数据权益的性质界定及其保护模式建构》，载《学海》，2019 年第 4 期，第 184 页。

[62] 李勇坚：《个人数据权利体系的理论构建》，载《中国社会科学院研究生院学报》，2019 年第 5 期，第 97 页。

[63] 黄震、蒋松成：《数据控制者的权利与限制》，载《陕西师范大学学报（哲学社会科学版）》，2019 年第 6 期，第 38 页。

险进行事先防御。例如，可在立法中设立激励机制，鼓励公私机构就拟建的数据处理系统或任何新的大数据项目进行数据安全影响评估，并定期向社会公布这些评估报告。另外，可鼓励高新技术企业将隐私强化技术应用至企业数据处理系统及产品的设计之中，增强企业对数据安全风险的防御能力。[64]丁晓东在研究中详细介绍了 GDPR 的相关做法。通过设置“数据主体的权利”和“数据控制者和处理者”两个章节，分别从数据主体权利要求、数据控制者义务承担两方面对数据控制者的义务进行详细规定，从而落实数据保护的责任。[65]GDPR 第四章第一节规定了数据控制者的基本义务，主要包括：设计的和默认的数据保护。GDPR 第 25 条规定，数据控制者必须承担“通过设计的数据保护和默认的数据保护”（data protection by design and default）的责任。所谓通过设计的数据保护，指的是数据控制者应当有一套固有的数据保护机制，而不只是采取一些临时性和个案性的保护措施。所谓默认的数据保护，是指在默认情况下仅处理那些为每个特定处理目所必需的个人数据。该义务适用于收集的个人数据的数量、数据处理的程度、数据的存储期限和数据的可访问性。特别的，这些措施应确保在未经个人干预的情况下，不向不确定数量的自然人提供个人数据；处理活动的记录。每一位数据控制者及特定情况下控制者的代理人，应当依其职责保存处理活动的记录。这些记录的内容具体包括控制者及相关员的姓名和联系方式、处理的目的、数据主体类别和个人数据类别的描述、个人数据已向或将向其披露的接收者的类别等；与监督机构合作。在执行任务的过程中，数据控制者、处理者以及特定情况下其代理人，应当根据要求与监督机构进行合作。GDPR 第四章第二节到第四节规定了数据控制者的特定义务：数据泄露的通知义务。在个人数据泄露的情况下，数据控制者应毫不延误地且在可行的情况下，至少在获知之时起 72 小时以内通知监督机构，除非个人数据泄露不会产生危及自然人权利和自由的风险；与数据主体的交流。当个人数据泄露可能对自然人权利和自由形成很高的风险时，数据控制者应当毫不延误地就个人数据泄露问题与数据主体行交流；数据保护影响评估。在进行数据处理之前，数据控制者应当对就个人数据保护所设想的处理操作方式的影响进行评估；事先咨询。数据保护影响评估的结果表明，如果数据控制者没有采取措施减少风险，那么处理过程将会是高风险的。因此，控制者应当在处理之前向监督机构进行咨询；指派数据保护专员。当需要对数据主体进行定期和系统的大规模监控时，数据控制者应当指派数据保护专员。[66]吴沈括曾在研究加州消费者隐私法案的文章中介绍 CCPA 的相关做法。CCPA 中数据保护的义务主体

---

[64] 黄道丽、张敏：《大数据背景下我国个人数据法律保护模式分析》，载《中国信息安全》，2015 年第 6 期，第 135-136 页。

[65] 丁晓东：《什么是数据权利？——从欧洲（一般数据保护条例）看数据隐私的保护》，载《华东政法大学学报》，2018 年第 4 期，第 43 页。

[66] GDPR 第 24-30 条。

主要是企业，相当于欧盟 GDPR 中的数据控制者。根据 CCPA 的规定，有关企业的义务主要有：根据消费者的要求披露收集信息的种类和目的以及共享数据的第三方；根据消费者的要求告知消费者所收集个人信息的类别及个人信息的使用目的；根据消费者的要求删除所收集的信息；根据消费者的要求不得出售该消费者的个人信息；尊重消费者选择不出售个人信息的权利，不得通过拒绝给消费者提供商品或服务、对商品或者服务收取不同的价格或费率等方式来歧视消费者行使该项权利；采取消费者可合理访问、合理获取的形式满足消费者的要求等。[67]

我国《电子商务法》第 23 条规定了电子商务经营者的义务，即收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定。第 79 条规定，电子商务经营者违反法律、行政法规有关个人信息保护的规定，或者不履行《电子商务法》第 30 条和有关法律、行政法规规定的网络安全保障义务的，依照《网络安全法》等法律、行政法规的规定处罚。另外，我国《信息安全技术个人信息安全规范》详细列举了个人信息控制者应遵守的各项义务，主要有：信息收集时应遵守的义务。如收集信息应具有合法性，满足最小必要原则，应获得信息主体的授权同意，不应强迫信息主体接受多项业务功能，应制定相应的隐私政策等；信息保存时应遵守的义务。如应实现保存时间最小化，应对信息去标识化处理，应对敏感信息的传输和储存采取加密等安全措施，在控制者停止运营时应对信息作出适当的处理等；信息使用时应遵守的义务。如应采取相应的访问控制措施，对个人信息的展示采取限制措施，对个人信息的使用目的进行限制，对用户画像的使用进行限制，应提供个性化展示及退出选项等；信息委托处理、共享、转让、公开披露时应遵守的义务。如委托处理时应征得信息主体的授权同意，共享、转让时应事先进行评估，公开披露时应进行评估并征得信息主体的同意等；发生个人信息安全事件时应遵守的义务。如应制定安全事件的应急预案，应履行告知义务等。[68]周坤琳等学者将数据控制者与处理者的义务分为三种类型：一是原则性义务，如知情同意义务、收集受限义务、目的特定义务等；二是一般性义务，如数据控制者“选择同意”、进行网络安全认证、遵守服务协议等的义务；三是具体的义务，如根据信息利用活动的不同采取匿名化或假名化技术，降低信息再识别的风险。对数据控制者与处理者的义务是有差异的，数据控制者的约定义务来源于与数据主体签订的服务合同，数据处理者的约定义务来源于与数据控制者之间的义务。但除此之外，因数据控制者与数据处理者在各信息利用活动中的角色不同，其承担的义务也就不同，如技术手段的选择及是否需要履行告知义

[67] 吴沈括：《2018 年加州消费者隐私法案中的个人信息保护》，载《信息安全与通信保密》，2018 年第 12 期，第 83 页。

[68] https://zhuanlan.zhihu.com/p/90546550，2021 年 5 月 6 日访问。

务的要求不同。[69]

综上，在尚未对个人数据形成体系化保护，事后救济途径匮乏，也没有完全将个人数据保护从民事侵权行为中区分开来的现状下，我国宜借鉴欧盟的立法经验，通过强化数据控制者的义务设定，构建个人数据事前保障措施，相信能够在避免个人数据的过度开发及泄露，促进数据产业朝着平衡利用、合理开发等方面取得进步。

5. 数据控制者与数据主体之关系

数据主体如何能够有效制约数据控制者？王雪乔一针见血指出，GDPR 积极主张数据控制者与处理者在个人数据保护中的参与性，导致在个人数据保护中数据主体的权利人地位被弱化，其要同时扮演将自己的个人数据向数据控制者与处理者开放的义务人。在数据主体作为义务人的情况下，数据控制者与处理者反过来会成为个人数据保护的权利人，数据主体的个人数据能否得到真正有效的保护受制于数据控制者与处理者，而不是受制于数据主体是否同意自己的个人数据被收集、控制与处理。在这种情况下，数据主体的“知情同意”的意义被削弱，而数据控制者与处理者的权利人地位相反则得到大幅度加强。[70]江波、张亚男建议个人参与和控制也是数据主体约束数据控制者使用数据的有效权利约束机制。赋予数据控制者权利，就应赋予数据主体参与和控制其个人数据处理的权利。权利与权利之间相互制约，才能达到对个人数据保护与利用之平衡状态。此外，赋予个人参与和控制的权利也能实现对个人数据风险评估的有效约束。[71]

（二）数据处理者相关既有规范与理论认知

1. 数据处理者相关立法例分析

在欧盟立法中，数据处理者是为数据控制者处理个人数据的自然人、法人公共机构、行政机关或其他非法人组织。为了确保数据处理符合 GDPR 的要求和保障数据主体的权利，数据控制者委托数据处理者具体处理数据时，应选择采取合适技术和组织措施的数据处理者。数据处理者应根据数据控制者明确的指示处理个人数据，履行相应的保密义务，在数据处理服务结束时，删除或返还所有的个人数据，并且要接受数据控制者的审计等。[72]金晶在对 GDPR 的研究里指出，欧盟立法对于“处理”的含义非常广泛，指对个人数据或个人数据集合所作的任何一项或一组操作，如收集、记录、组织、结构化、储存、修改、检索、查阅、

---

[69] 周坤琳：《互联网金融业信息控制者与信息处理者法律义务与责任研究——基于风险控制的探索》，载《海南金融》，2019 年第 9 期，第 55 页。

[70] 王雪乔：《论欧盟 GDPR 中个人数据保护与“同意”细分》，载《政法论丛》，2019 年第 4 期，第 143 页。

[71] 江波、张亚男：《大数据语境下的个人信息合理使用原则》，载《交大法学》，2018 年第 3 期，第 121 页。

[72] 全国信息安全标准化技术委员会：《网络安全实践指南——欧盟 GDPR 关注点》，https：//www.secrss.com/articles/2925，2021 年 9 月 5 日访问。

使用、传播或以其他方式利用、排列或组合、限制、删除或销毁。“处理”须具备合法性前提，包括数据主体明示同意、为履行合同所必需、为履行法定义务所必需，以及为了数据控制者的合法利益。欧洲法院通过判例进一步补充和明确了“处理”概念，例如，发布新闻稿、网页加载个人数据、在光盘上收集数据、传输或通过短信转发数据、响应访问文档请求传递数据、获取和存储指纹、通过ANAF 传输数据和 CNAS 的后续处理等都构成数据处理行为。[73]美国 CCPA 中虽然没有明示的数据处理者表述，但是提到“服务提供者”，其系指为其股东或其他所有权人的利润或经济利益而组织或经营的独资公司、合伙企业、有限责任公司、协会或其他法律实体，这一实体代表企业处理个人信息，企业则根据书面合同向这一实体披露消费者个人信息；但前提是，该合同禁止接收信息的实体保留、使用或披露个人信息以用于任何目的，除非为了履行合同规定的服务或本法允许的其他目的，包括保留、使用或披露个人信息用于提供合同规定的服务之外的商业目的。我们可以看出，这里的服务提供者与数据处理者是类似的。[74]

2. 数据处理者的义务

通过郑钧、高鼎的研究，我们能发现，欧盟对于数据处理处理者制约的认识经历过一个变化发展的历史进程。1995 年欧盟《数据保护指令》认为新数据处理者一般为数据控制者提供辅助服务，因此规制的对象是数据控制者，数据处理者为从属地位。而 GDPR 则认为数据处理者与数据控制者具有同等地位，因而予以同样规制。GDPR 第 28 条规定，数据处理者的处理应当受某类合同或其他欧盟法与欧盟成员国法的约束，这类合同或法律应当规定数据处理者相对于数据控制者的责任、主体事项、处理期限、处理性质与目的，以及个人数据的类型等。[75]GDPR 规定了数据处理者应当遵守的基本义务和特殊义务。部分义务与数据控制者的义务相同或相似，包括处理活动记录、与监督机构合作、数据泄露通知、特殊情况下指派数据保护专员和向第三国或国际组织传输个人数据。不同的是，数据处理者只能使用数据控制者实施的技术和组织措施，未经允许不能引入另一个处理者。此外，数据处理者的很大一部分义务是要依据合同项下的具体规定予以履行。[76]

3. 数据处理者与数据控制者的关系

通过德国学者库勒的相关研究，我们可以发现欧盟《数据保护指令》将参与个人数据的行为人划分为“数据控制者”和“数据处理者”。数据控制者是指单独或与他人共同确定个人数据处理的目的和方式的自然人和法人、公共机构、代

[73] 金晶：《欧盟<一般数据保护条例>：演进、要点与疑义》，载《欧洲研究》，2018 年第 4 期，第 10 页。
[74] https://docs.microsoft.com/zh-cn/compliance/regulatory/ccpa-faq?view=o365-worldwide，2021 年 9 月 29 日访问。
[75] 郑钧、高鼎新：《欧盟 CDPR 及其对金融业的影响》，载《中国金融》，2018 年第 12 期，第 52 页。
[76] https://www.sohu.com/a/341962728_442599，2021 年 9 月 7 日访问。

理机构或其他机构；如果数据处理的目的和方式由国内或共同体法律或规章确定，则控制者或其委任的具体标准可以由国内法或共同体法律制定。数据处理者是指代表数据控制者处理个人数据的自然人或法人、公共机构、代理机构或其他机构。[77]兰州大学 APUS 研究院明确指出欧盟对于此问题的立法取向，GDPR 第 4 条第 6 款规定，能够单独或与其他主体一起决定个人数据处理目的和方式的自然人、法人、公权力机构等，是个人数据的控制者。GDPR 第 4 条第 7 款规定，代表控制者处理个人数据的自然人、法人、公权力机构等，是个人数据的处理者。也就是说，数据控制者决定了个人数据处理的目的和方式，而数据处理者则替数据控制者处理个人数据。[78]综上，虽然角色不同，但数据控制者与数据处理者在数据保护的义务方面还是有很多共同点。正如 GDPR 规定，数据控制者和数据处理者同时适用的个人数据保护义务有：安全措施的采取、个人数据处理活动的记录、数据保护官的任命、对外传输时安保措施的采取、域内代表的任命、配合数据专门保护机关的工作等。

三、数据交易的性质判定与规则构建

从已有的文献来看，数据交易的性质判定与规则构建讨论的相对比较少，也没有很多体系性的成果。数据的共享、转让，可以直接通过文件发送的形式提供，如经移动存储设备拷贝、作为电子邮件附件发送、通过即时通信软件发送。但这样的数据共享、转让方式并不安全，数据的发送方也缺少对数据的控制，因此直接发送并不是唯一的方式。在数据共享的过程中，更多是通过开放权限、开放接口的形式实现。从语义理解上，数据交易是个动态的行为，有个活动的过程，它是数据共享和转让的主要表现形式，《安徽大数据交易中心交易规则》指出，数据交易是以货币换取数据的行为。该定义回避了数据所有权或使用权变更的问题，只是强调了货币与数据的对价。在数据交易中，提供方的交付实际上是对自己所控制的数据进行复制并传输给需求方的行为，在这个过程中限于数据传输技术本身，需求方无法确保提供方删除了交易的数据，所以数据交易的过程不存在所有权的转移，只能够通过有偿的方式让需求方获得新的权益。因此会存在多份相同的权益所共存的现象。[79]肖建华，柴芳墨从当前数据交易的实践分析，分析了各类数据交易平台模式。以电子商务营销模式来看，大数据平台交易的模式主要有三种。第一种是数据平台分销模式（Consumer to Business），即用户向信息业者

---

[77] （德）库勒：《欧洲数据保护法：公司遵守与管制（第二版）》，旷野、杨会水等译，法律出版社 2008 年版。

[78] APUS 研究院：《理清 GDPR 下的“控制者”和“处理者”有何不同》，http://www.mpaypass.com.cn/news/201810/11093704.html，2021 年 10 月 3 日访问。

[79] 参见何渊主编：《数据法学》，北京大学出版社 2020 年版，第 162 页。

提供数据，作为对价，信息业者以商品或者优惠反馈于用户；第二种是数据平台集中销售模式（Business to Business），即数据平台作为中间方撮合数据提供方和数据需求方通过平台进行交易，而交易平台按照交易金额的大小比例收取交易费用；第三种是分销与集销混合模式，即数据经纪商通过其他可公开来源渠道（包括数据经纪商之间的信息共享）获取数据，并按照属性将数据加工后予以销售。我国大数据交易平台如贵阳大数据交易中心、数据堂交易平台、中关村数海大数据交易中心等主要采用第二种商业模式，即交易双方通过平台进行数据交易，平台本身不作为信息收集的主体。当前，大数据交易市场规模不断扩大，交易方式不断创新，发展势头良好，但同时也存在不少问题。[80]从文献研究和实践来看，我们对于数据交易的关注实际上还是不是很全面，对于数据交易所之外的各种形式的数据交易并未能够给予充分的关注。那么数据交易行为从民法上应当如何定性呢？从工具论的视角审视我国当代《民法典》，关于市场交易的法律规制路径在承继潘德克顿法学体系的基础上发展出了两种不同的形式：一是权利规制路径，即通过构建一个客观存在的权利，使民事主体借助这一权利中所蕴含的各项权能实现对其他民事主体行为的限制。权利规制路径以某项民事权利为基轴，形成“权利主体-权利客体-权利内容-权利变动”的逻辑链条，《民法典》中的物权、人格权规则等即是这一路径的典型产物。二是行为规制路径，即关注民事法律纠纷中主体之间形成的关系，采用“条件-后果”式的方法表述在特定状态或条件下民事主体间的权利义务构造，合理分配主体间的“自由”与“强制”关系。行为规制路径下的民事主体间的权利义务配置是以特定民事纠纷为立足点，在相关规则的设计上 遵循“假定条件-行为模式-法律后果”的逻辑结构，其中《民法典》的合同、侵权责任规则等是这一路径下的产物。权利规制路径的数据要素市场制度建设是 以数据权利化为立足点，但当前数据权利化的相关理论基础未能完全提炼并澄清。因此，有必要同步转向数据要素市场的其他私法规制路径的研究，其中合同规制路径（属于行为规制路径）对于规范数据要素市场具有显著优势。[81]那么数据交易行为应当属于何种合同类型呢？或者我们要通过什么样的合同规则来对其加以限制呢？钟晓雯在其文章中认为，数据交易法律关系可以解构为“数据服务合同”，中介、委托合同以及“平台服务合同”。“数据服务合同”的双方当事人负有及时支付/接受对价之权利义务，以及及时提供/接受符合质量要求的数据服务的权利义务。中介、委托合同，“平台服务合同”的双方当事人除负有法定或约定的权利义务外，数据交易平台方对于数据源层方还负有数据安全存储与网络安全保障义务；对于数据用户方还负有服务说明、告知，形式审查

[80] 参见肖建华，柴芳墨：《论数据权利与交易规制》，载《中国高校社会科学》2019 年第 1 期，第 85 页。
[81] 钟晓雯：《数据交易的权利规制路径：窠臼、转向与展开》，载《科技与法律》2021 年第 5 期，第 38-42 页。

以及安全保障义务。但问题在于，即有文献当中对于数据交易行为的性质认定的思路有些的确是较为可取的，但并没有从更为宏观的全社会数据交易行为分析的角度加以思考，更没有深入细致的分析和研究数据交易合同认定之后，数据交易规则的具体设计的问题。总体上来说，完全针对于数据交易性质判定以及规则构建的文献非常少，缺少充分的参考价值，这对本文写作来说也是极具挑战的。

四、数据交易所涉其它法律问题

（一）数据跨境流动

数据跨境已经成为推动国际贸易中货物、服务、人、资金流动不可或缺的部分。随着数字经济的深入发展和数据作用的日益凸显，各国对数据跨境的含义和影响的认识日益深入，数据跨境相关立法和国际规则的制定也日新月异地呈现出新趋势和新特点。下文将对各学者关于全球范围内各国对数据跨境的促进和限制措施进行阐述，进而尝试分析对我国相关立法的启示与借鉴。娄鹤、陈国彧指出，“数据跨境”的定义可追溯至经合组织（OECD）的《隐私保护与个人数据跨境流动指南》。该指南将个人数据的跨境流动界定为跨越国境的个人数据移动。以此为基础，数据跨境即指数据从一个国家、地区、国际组织传输至另一国家、地区、国际组织。具体而言，数据跨境涉及许多现实场景，譬如从位于一国境内的服务器传输至位于另一国境内的服务器等。[82]为了后期写作需要，下文重点分析的是数据出境。按照欧盟 GDPR 第 44 条的规定，数据跨境转移是指对于正在处理或计划进行处理的个人数据，将其转移到第三国或国际组织，包括将个人数据从第三国或国际组织转移到其他国家或国际组织。2017 年 8 月 30 日，中国信息安全标准化技术委员会发布了《信息安全技术数据出境安全评估指南（征求意见稿）》，其中对数据出境作出定义，即网络运营商通过网络等方式，将其在中华人民共和国境内运营中收集和产生的个人信息和重要数据，通过直接提供或开展业务以及提供服务、产品等方式提供给境外的机构、组织或个人的一次性活动或连续活动。所谓“境内运营”，宜理解为网络运营者通过网络为中华人民共和国境内的主体提供了商品或服务的行为；所谓“向境外提供”，宜理解为网络运营者通过网络将在中华人民共和国境内运营中采集的信息传输并存储于其他信息控制者设在境外的服务器的行为。本人认为，从法律实践和产业发展的实际需求考虑，我们应对数据跨境的管理应采取广义理解，包含促进自由流动，本地化副本保留，有条件出境、本地化存储和处理等从完全开放到完全禁止的各种限制程度的跨境数据流动管理措施。

---

[82] 参见娄鹤、陈国彧：《中国企业个人数据跨境传输最佳法律实践探讨》，载《信息安全与通信保密》，2019 年第 8 期，第 53-54 页。

1. 数据跨境流动制度设计的立法例研究

随着国际经济全球化和区域一体化的不断发展，一些国家利用国际双边与多边自由贸易谈判、区域性规则、国内立法等多重方式，尝试在维护公共利益等原则的基础上，建立数据跨境流动生态圈，推动数据跨境自由流动，发挥数据跨境流动在降低企业经营成本、盘活线上跨境交易、支撑企业国际运营、促进国际执法合作等领域的积极作用，从而促进全球与区域经济发展。首先是国际多边贸易机制的构建问题。杨筱敏在研究中指出，2019 年 1 月，在 WTO 框架下，美国、日本、欧盟、加拿大、中国、巴西、韩国、新加坡等 75 个国家和地区签署了《关于电子商务的联合声明》。截至 2019 年 7 月，美国、日本、欧盟等国家和地区提出了 18 份概念文件或条文提案。其中，欧盟向 WTO 提交了电子商务提案（INF/ECOM/22），体现了在维护“个人数据保护”这个最高价值的基础上，最大限度地促进数据跨境流动。例如，该电子商务提案规定，禁止将“数据本地化存储和处理、设定数据本地化要求”等做法设定为数据跨境转移的前提条件。此外，欧盟并未对其他国家的公共政策或国家安全的目的予以考虑。但是，各方有权采取和维持其认为恰当的个人数据保护措施，包括制定和采用个人数据跨境转移规则，维护“个人数据保护”的价值，从而充分保障人权。[83]京东法律研究院的研究报告指出，2016 年联合国贸发会发布的《数据保护规则与数据全球流动：贸易与发展的影响》指出，运用专门的文件和促进一种或更多的机制是解决数据跨境流动问题的关键。数据保护立法应避免成为贸易和创新的新障碍。[84]其次是美国主导的国际贸易协定与监管合作机制问题。Dr. Clarisse Girot 在对美国的数据贸易政策分析中指出，鉴于美国在全球数字产业中占据优势地位，处于“全球数据高地”，鼓励数据自由跨境流动对美国而言利远大于弊。因此，无论是在美国主导的《跨太平洋伙伴关系协定》（TPP）中，还是在以该协定为蓝本的《全面与进步的跨太平洋伙伴关系协定》（CPTPP）、《美国一墨西哥一加拿大协定》（USMCA）里的数据保护条款中，都体现了“更加自由、市场驱动”的价值取向。[85]分别来看：亚太经合组织（APEC）下的隐私保护框架。“跨境隐私规则体系”［Cross-Border Privacy Rules（CBPR）System］是自愿性、基于责任的 APEC 经济体内部个人数据跨境流动机制，加入的企业遵守《APEC 隐私框架》中的个人数据保护原则。该机制不改变各国和地区自身的个人数据立法，但要求加入的经济体签署《跨境隐私执法协议》以便执法。CBPR 机制的保护水平等同

[83] 参见杨筱敏：《全球跨境数据流动国际规则及立法趋势观察和思考》，http://www.secss.com/ articles/1374，2019 年 11 月 26 日访问。

[84] 参见京东法律研究院：《欧盟数据宪章——<一般数据保护条例>GDPR 评述及实务指引》，法律出版社 2018 年版。

[85] See DR. CLARISSE GIROT, REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA 8 (2018).

于 1980 年 OECD 发布的《隐私保护与个人数据跨境流动指南》的水平。截至 2019 年 10 月，已有美国、日本、澳大利亚、加拿大、韩国、墨西哥、新加坡等 8 个国家和地区参与了 CBPR 框架机制。此外，美国试图推动 CBPR 与欧盟 GDPR 的制度对接，以促进跨境数据流动。但鉴于目前参与 CBPR 框架机制的 APEC 成员中仅有美国（仅限于《隐私盾协议》范围）、日本、加拿大（仅限于商业组织范围）通过了欧盟 GDPR 的充分性认定，因而参与 CBPR 框架机制的国家和地区与欧盟 GDPR 所管辖的欧洲经济区之间的数据自由流动尚待时日；《跨太平洋伙伴关系协定》。张衡、娄鹤、陈国彧都对 TPP 做过详细研究，TPP 的目标在于：在个人信息保护等合法公共政策目标得以保障的前提下，促进全球数据自由流动，从而驱动互联网和数字经济的发展。例如，TPP 在其“电子商务”一章当中加入“商业信息跨境自由传输”条款，限制缔约国关于“数据本地化存储”的规定。[86]此外，为了更好地促进数据跨境流动，TPP 不会设立“数据中心”（Internet Data Centre）作为允许 TPP 缔约方企业进入境外市场的前提条件，也不要求缔约方企业在数据跨境过程中转让或获取软件源代码；[87]《美国一墨西哥一加拿大协定》。2018 年 11 月，美国、墨西哥、加拿大签署了 USMCA。杨筱敏指出，其中包含开放水平最高的跨境数据流动条款，即 USMCA 中去除了 TPP 中“承认各国可以拥有自己的信息转移监管要求”的条款；USMCA 禁止一切“将计算设施放置于一国境内或使用一国境内计算设施”的本地化要求；[88]《全面与进步跨太平洋伙伴关系协定》。在 2018 年 3 月 8 日，澳大利亚、文莱、加拿大、智利、日本、马来西亚、墨西哥、新西兰、秘鲁、新加坡及越南等 11 国签署了 CPTPP。Dr. Clarisse Girot 认为 CPTPP 强调数据必须伴随商品和服务的自由贸易而自由流动。[89]杨筱敏认为，CPTPP 包含“通过电子方式跨境信息转移”条款，适用了 TPP 中的原则。相比于 USMCA 严格地推动数据自由流动的做法，CPTPP 在促进数据自由流动的同时保留了缔约国政府依照公共政策而采取一定限制措施、履行监管义务的灵活度。例如，CPTPP 保留了 TPP 中“承认各国可以拥有自己的信息转移监管要求”的条款；各国可因公共政策对数据跨境流动采取“必要的”限制措施。再如，CPTPP 虽承认“禁止数据本地化”是一般要求，但仍允许各国各自制定国内法规以保护国家机密与通信安全。典型例子是，越南作为 CPTPP 成员，在 2019 年 1 月实施的《网络安全法》中就针对特定情形提出了“数据本

[86] 参见娄鹤、陈国彧：《中国企业个人数据跨境传输最佳法律实践探讨》，载《信息安全与通信保密》，2019 年第 8 期，第 56 页。
[87] 参见张衡：《跨境数据流动的国际形势和中国路径》，载《信息安全与通信保密》，2018 年第 12 期，第 23 页。
[88] 杨筱敏：《全球跨境数据流动国际规则及立法趋势观察和思考》，http：//www.secss.com/ articles/1374，2019 年 11 月 26 日访问。
[89] See DR. CLARISSE GIROT, REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA 8 (2018).

地化”要求。与之类似，《美韩自由贸易协定》中对数据跨境流动亦采取柔性限制方式，灵活度较高；[90]电子数据相关的执法合作协议。2018 年 3 月，美国国会通过了《澄清域外合法使用数据法案》（Clarifying Lawful Overseas Use of Data Act，简称“CLOUD 法案”），Dr. Clarisse Girot 认为它允许美国与其他国家就执法部门电子数据跨境获取签订双边协议。2019 年 10 月 3 日，美国与英国就执法部门电子数据跨境获取达成协议，对 CLOUD 法案作了重要补充。根据该协议，在恐怖主义犯罪、儿童色情和其他网络犯罪情形下，特别是在涉及美国的死刑案件和英国的言论自由案件时，两国执法部门可在数据保护法的限制范围内，直接向有关实体跨境调取电子证据数据，而非通过主管部门调取。[91]再次，是欧盟主导的国际协议。一是双边自由贸易协定中的标准条款。欧盟委员会签署了拟在欧盟贸易协定中使用的数据流动和个人数据保护条款，并且用于与印度尼西亚等国的自由贸易协定谈判。杨筱敏特别指出，在以上条款中，欧盟禁止通过“数据本地化存储和处理”、设定“数据本地化要求”等条件限制数据跨境流动。此外，欧盟并未如 CPTPP 一样，明确考虑其他国家的公共政策或国家安全等“数据跨境自由流动”的限制性因素。然而，欧盟一贯将“个人数据保护”置于更高价值地位，因此允许贸易谈判各方采取和维持其认为恰当的个人数据保护措施，包括制定和采用个人数据跨境转移规则。[92]二是欧美双边协议：从《安全港框架协议》到《隐私盾框架协议》。2000 年，欧盟与美国签署《安全港框架协议》，对欧美之间的数据跨境流动进行规制。《安全港框架协议》参考了欧盟“95 指令”中的数据保护原则，由企业自愿加入该协议以获取数据跨境传输方面的便利，加入该协议的企业则必须遵守履行协议规定的原则和义务。2013 年“棱镜门事件”发生后，《安全港框架协议》因不能有效约束美国公共机构而遭到质疑。譬如，《安全港协议》明确规定了“国家安全及公共利益例外”。2015 年 10 月 6 日，在马克西米利·施雷姆斯诉数据保护专员（Maximillian Schrems v. Data Protection Com-missioner）一案中，欧洲法院正式废止了《安全港框架协议》。《安全港框架协议》被废止后，欧美经过多轮磋商，于 2016 年 7 月通过了《隐私盾框架协议》，[93]针对《安全港框架协议》的诸多漏洞进行了弥补。例如，《隐私盾框架协议》将以国家安全为目的的个人数据流动也纳入管辖范围，并且对欧盟公民的权利救济途径、欧盟委员会与美国商务部联合审查机制等作了细化规定。综上，我们发现欧盟的特点是，它在其主导的贸易协定谈判以及美欧《隐私盾框架协议》

---

[90] 参见杨筱敏：《全球跨境数据流动国际规则及立法趋势观察和思考》，http：//ww.secss.com/ articles/1374，2019 年 11 月 26 日访问。

[91] See DR. CLARISSE GIROT, REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA 10 (2018).

[92] 参见杨筱敏：《全球跨境数据流动国际规则及立法趋势观察和思考》，http：//ww.secss.com/ articles/1374，2019 年 11 月 26 日访问。

[93] http://curia.europa.ew/jcm/upload/doc/application/pdf/2015-10/epl50l17en.pdf，2019 年 11 月 26 日访问。

的起草过程中，同样将“促进数据跨境自由流动”作为基本原则。在此过程中，欧盟又表现出特定的价值取向，即将隐私权认定为“基本人权”，进而将“个人数据保护”置于较高价值位阶予以贯彻。

3. 数据跨境流动领域的区域性、国别性立法

先来看区域性立法。欧盟是以条例、指令的方式促进本区域内数据自由跨境流动的典型代表。早在 2000 年，欧洲议会和欧盟理事会即发布（EC）No45/2001 号条例，推动被欧盟公共机构处理的个人数据的自由流动。[94]在 2000 年 6 月 8 日欧洲议会和欧盟理事会发布的 2000/31/EC 号指令中，也提出应当保障社会服务数据在成员国之间自由流动，以促进区域内部市场良好运行。[95]2018 年 5 月正式生效的 GDPR 在正文第 1 条即阐明，“本条例就对与个人数据处理相关的…个人数据自由流动订立规则”；GDPR“鉴于条款”（Recital）第 3 条亦明确，欧盟“95 指令”致力于“保障成员国之间个人数据的自由流动”。2018 年 10 月，欧洲议会通过了《非个人数据在欧盟境内自由流动框架条例》，为非个人数据在欧盟境内的自由流动减轻障碍。2019 年的欧盟《电子证据条例（草案）》设置“域外管辖条款”，在欧盟司法执法机构调取电子证据数据时，不以数据存储位置作为确定管辖权的决定因素，只要满足如下两个条件，相关数据可被要求强制披露：（1）被要求提交的数据为刑事诉讼所需；（2）被要求提交的数据与服务提供商在欧盟境内提供的服务相关。除此之外，张衡还发现，2013 年版《OECD 隐私框架》亦是鼓励 OECD 各成员国在有足够保障措施，并且另一国也遵循 2013 年版《隐私保护与个人数据跨境流动指南》的情况下，[96]消除数据流动的障碍。[97]京东法律研究院的研究发现 2013 年版《隐私保护与个人数据跨境传输指南》建议成员国实施与数据隐私风险相适应的数据传输约束。[98]张衡进一步指出，2012 年，东盟部长会议通过的《东盟数据保护框架》为东盟国家制定个人数据保护法提供指南，同样鼓励成员国之间的合作与数据跨境流动，促进区域贸易发展。[99]2018 年 5 月 18 日，欧洲委员会部长委员会第 128 次会议通过

---

94 Regulation（EC）No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the Protection of Individuals with Regard to the Processing of Personal Data by the Community Institutions and Bodies and on the Free Movement of Such Data，https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/=CELEX：32001R0045＆from=EN, visited on 2019-11-26.

95 Directive2000/3l/EC of the European Parliament and of the Council of 8 June 2000 on Certain Le-gal Aspects of Information Society Services，in Particular Electronic Commerce, in the Internal Market (Directiveon Electronic Commerce), https://eurlex.Europa.eu/legal-content/EN/TXT/PDF/uri=CELEX:3200010031＆from=EN, visited on 2019-11-26.

96 OECD, The OECD Privacy Framework, Chapter 1Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (20l3), https：//www.oecd.org/sti/ieconomy/oecd_privacy._framework.pdf, visited on 2019-11-26.

97 张衡：《跨境数据流动的国际形势和中国路径》，载《信息安全与通信保密》，2018 年第 12 期，第 24 页。

98 京东法律研究院：《欧盟数据宪章——〈一般数据保护条例〉GDPR 评述及实务指引》，法律出版社 2018 年版，第 115 页。

99 张衡：《跨境数据流动的国际形势和中国路径》，载《信息安全与通信保密》，2018 年第 12 期，第 25

了欧洲委员会第108号公约附加议定书），并于2018年10月10日开放签署，缔约国包括欧洲委员会20多个成员国，以及俄罗斯、乌拉圭、突尼斯、毛里求斯等，同样强调数据输入国的“充分性保护”水平。此外，2019年《网络犯罪公约第二附加议定书》第32条对经同意或在公开场景跨境访问存储的计算机数据作出规定。即一方可在未经另一方授权的情况下：（1）公开访问（开源）存储的计算机数据、不管这些数据在地理上出于何处（2）通过其境内的计算机系统访问存储在另一国的数据，前提是获取数据披露方的合法和自愿同意。再就是国别性立法。典型例子为美国《加州消费者隐私法案》（CCPA）。杨筱敏指出，美国尤其是加州的互联网乃至整个信息产业领先于全球，因而从价值取向上更加鼓励数据的跨境流动，跨境流动越自由，美方在数据资产控制和利用方面就越主动。因此，与GDPR为数据跨境流动设置层层关卡相比，CCPA并未对数据跨境流动设置明显限制。此外，英国、瑞典的国内法也主张数据的跨境自由流动。[100]此外，美国CLOUD法案明确赋予美国执法机构跨境调取数据的权力。对于境外存储的数据，美国可出于公共安全等目的进行调取。可调取的数据范围不限于美国人的数据和美国企业的数据，只要符合一定条件，非美国人和非美国企业的境外数据也可被调取。

张衡认为，在以WTO为核心的多边机制中，虽然《服务贸易总协定》（GATS）中设置了“安全例外”和“个人信息保护例外”，但自多哈回合谈判以来，WTO项下的这两项例外并无显著发展。近年来，在美国主导下，以TPP模式为基础，通过双边、多边自由贸易协定谈判和监管合作，建立了以CBPR、CPTPP、USMCA为代表的数据跨境流动规制框架，并逐步构建了一个“数据跨境流动生态圈”，在上述各个协定成员国内部，各自建立起互信互认机制，从而促进“生态圈”内的数据自由流动，推动经济发展，同时也一定程度上兼顾了各国公共政策与监管执法等实际需要。[101]杨筱敏认为，欧盟通过严格的GDPR规范与监管寻求全球数据治理的更大话语权。欧盟为个人数据的处分权赋予“基本人权”的价值属性，因而与TPP模式下的条款相比，欧盟将对个人数据的保护置于优先位置，是不容谈判、磋商的，并且坚持其高要求。因此，不论是作为2013年版OECD隐私指南升级版的GDPR，还是向WTO提交的电子商务提案，又或是用于双边自由贸易谈判的数据保护条款，以及对《安全港框架协议》有效性的反思与《隐私盾框架协议》的设置，欧盟都努力寻求“个人数据跨境自由流动”与“个人数据保

页。

100 杨筱敏：《全球跨境数据流动国际规则及立法趋势观察和思考》，http：//ww。secss。com/ articles/1374，2019年11月26日访问。

101 张衡：《跨境数据流动的国际形势和中国路径》，载《信息安全与通信保密》2018年第12期，第25页。

护”之间的平衡。[102]

不过数据跨境自由流动仍受各项因素制约。Dr. Clarisse Girot 提出，在以 TPP 为蓝本的 CPTPP 中，在大力促进数据自由流动的同时保留了缔约国政府依照公共政策而采取一定限制措施、履行监管义务的灵活度。典型的例子是：越南作为 CPTPP 缔约国，在其国内法中仍可明确要求对数据进行本地化存储。同样是美国主导的 CBPR，虽原则上极力主张数据跨境自由流动，但也明确规定其并不强制改变各国国内个人数据立法。在 1980 年 OECD 发布的《隐私保护与个人数据跨境传输指南》中，虽以“数据自由流动”为原则，但在数据传输的目的国“尚未实质遵守准则要求”或“数据出境将损害本国隐私法律”的情况下，仍允许数据输出国对数据出境予以合法限制，以“达成各方利益平衡”。[103]京东法律研究院的研究表明，2013 年 OECD 发布《隐私保护与个人数据跨境传输指南》，同样建议成员国“实施与数据隐私风险相适应的数据传输约束”。此外，巴西和非洲集团在向 WTO 提交的电子商务提案当中，也出于国家安全、公共秩序、本地数字产业保护等考虑，对数据跨境自由流动提出了多项制约条件。[104]Dr. Clarisse Girot 还指出，数据隐私法与几乎所有部门的特定规则都存在交集——主要在医疗卫生、金融、信用记录、电子商务、消费者保护以及劳动关系等领域中，在法律法规层面进行必要的协调十分困难，且耗费时间成本，因而经常成为区域内不同法域数据流动规则相互融合的障碍。[105]Dr. Clarisse Girot 还提出我们必须要关注到的一点，那就是尽管诸如 APEC、东盟数据保护框架已为各国“制定数据保护法规提供粗略指南”，但“从对新制定的数据保护法律的理解，到执法和合规实践，因为各国自身法律体系的原生差别，各法域的数据保护法律产生了越来越多的分歧”。[106]

4. 数据跨境流动的限制

虽然如上文所述，全球范围内大多数司法管辖区原则上都允许数据跨境流动，然而，不同法域数据跨境流动的默认原则有所不同：有的以允许数据出境为原则，有的以禁止数据出境为原则，但两者都会规定一些例外情况，这些“例外情况”通常要综合考虑各项因素是否得以满足，包括但不限于“用户的同意”“行政许可”“资质认证”“有约束力的公司规则”（binding corporate rule，BCR）、“数

---

[102] 杨筱敏：《全球跨境数据流动国际规则及立法趋势观察和思考》，http：//ww.secss.com/ articles/1374，2019 年 11 月 26 日访问。

[103] See DR. CLARISSE GIROT, REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA 8 (2018).

[104] 京东法律研究院：《欧盟数据宪章——〈一般数据保护条例〉GDPR 评述及实务指引》，法律出版社 2018 年版，第 115 页。

[105] See DR. CLARISSE GIROT, REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA 5 (2018).

[106] See DR. CLARISSE GIROT, REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA 8 (2018).

据出境协议”等等。虽然形式上类似，但这些例外情形在不同国家发挥着不同的作用。例如，在韩国，“用户同意”是个人数据从韩国出境的所有方式的前提条件；而在其他大多数国家，“用户同意”仅为数据出境的若干合法依据之一。另外，针对“用户同意”这一概念本身，在有些法域（如韩国）被解释为必须“明示授权同意”，而在有些法域（如泰国）则被解释为“只要用户未选择退出（opt-out）即为默示同意”。[107]限制措施因法域不同存在上述差异，但各国对数据出境制定限制措施的出发点存在共性－多数国家是出于“保障国家安全”“保护本国产业”“个人隐私保护”等目标，针对特定行业数据、关键技术领域数据、个人敏感数据分别制定限制措施。Dr. Clarisse Girot 虽然并不反对各国的限制措施，但他还是提醒到，在制定具体国别性数据跨境流动限制措施时，各国必须考虑在“国家安全、网络主权、保护产业、数据保护”等目的与“促进数据流动、推动经济发展”的目标之间保持平衡，从而一方面有效行使数据主权，另一方面防止沦为“数据孤岛”，阻碍数据跨境流动，提高企业全球化经营成本。例如，外资并购国家安全审查，将使企业投资交易随时面临被撤销的巨大风险；数据本地化存储要求，将可能使本国企业利用云计算等新兴技术的能力受限，并且使内资、外资企业面临在当地建设数据中心等基础设施所产生的额外成本，从而可能阻碍数字经济及电信和互联网服务的发展。[108]此外，各国国内法中关于限制数据流动的零散规定以及不断变化的监管环境，也是提高企业经营成本的原因之一。“数据主体的利益并不必然通过改善监管就可得到明显提升”。[109]

5. 跨境数据流动规制的国内法现状

我国立法中主要规定了数据出境的限制性条件，主要表现形式为：针对重点行业中的重要数据、个人数据，采取以“本地化存储”为原则、“出境安全评估”为例外的方式进行规制，从而维护国家安全、保护个人数据、促进本国经济发展。从京东法律研究院的研究中，我们可以发现：我国个人信息保护相关规定，散见于《反恐怖主义法》《刑法》《网络安全法》《信息安全技术 个人信息安全规范》《征信业管理条例》《侵害消费者权益行为处罚办法》《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题解释》《电信和互联网用户个人信息保护规定》《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》《银行业金融机构数据治理指引》等规范性文件当中，其中仅零星涉及数据跨境流动的内容。例如，《征信业管理条例》第 24 条规定，征信机构在中国境内采集的信息的整理、保存、加工，应当在中国境内进行。征信机构向境外组织或者个人提供信息，应当遵守法律、行政法规和国务院

[107] Ibid，p.9.
[108] See DR. CLARISSE GIROT, REGULATION OF CROSS-BORDER TRANSFERS OF PERSONAL DATA IN ASIA 7 (2018).
[109] Ibid

征信业监督管理部门的有关规定。《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第 6 条规定，在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。[110]

对个人信息和重要数据的出境予以规制的体系化规定，主要见于《网络安全法》及网信办的部门规章当中。网信办的《个人信息和重要数据出境安全评估办法》和《信息安全技术数据出境安全评估指南》等规章都处于征求意见阶段。《网络安全法》第 37 条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估。《信息安全技术个人信息安全规范》作为推荐性国家标准，也作了类似规定。网信办公布的《个人信息和重要数据出境安全评估办法（征求意见稿）》，其中规定了安全评估的适用范围、评估内容、评估机构等基本规则。网信办立规目的在于，保障个人信息和重要数据安全，维护网络空间主权和国家安全、社会公共利益，促进网络信息依法有序自由流动。[111]2017 年的《个人信息和重要数据出境安全评估办法（征求意见稿）》将数据出境安全评估的责任主体由《网络安全法》中的“关键信息基础设施运营者”扩大到所有“网络运营者”，并根据具体情形规定了“自行评估”和“行业监管部门评估”两种安全评估形式。该评估办法规定，网络运营者在数据出境前，应自行组织对数据出境的安全评估。[112]除此之外，网络运营者每年还应对数据出境情况进行安全评估，并将评估情况报告给行业主管或监管部门。此外，数据接收方情况变化较大时，还应当重新进行安全评估。[113]针对大量或传输范围特别大或者特殊类型信息的跨境传输，网络运营者应当报请行业主管或监管部门组织安全评估。[114]网信办公布了《个人信息出境安全评估办法（征求意见稿）》，其借鉴 GDPR“数据跨境转移协议标准合同条款”的思路，规定了网络运营者与境外个人信息接收者签订数据合同的必要条款，并将该合同作为企业申请个人信息出境安全评估所必须提交的材料。同时，针对安全评估行政机构、安全评估的触发机制和具体流程、安全评估内容、出境记录保存义务、个人信息主体追偿等问题进行了细化规定。全国信息安全标准化技术委员会先后于 2017 年 5 月 27 日、2017 年 8 月 25 日发布了两版《信息安全技术 数据出境安全评估指南（征求意见稿）》，逐步确定了“境内运营”“加工处理”“数

---

[110] 京东法律研究院：《欧盟数据宪章——〈一般数据保护条例〉GDPR 评述及实务指引》，法律出版社 2018 年版，第 111 页。

[111] http：//www.cac.gov.cn/2017-04/11/c_1120785691.htm，2019 年 11 月 21 日访问。

[112] 参见《个人信息和重要数据出境安全评估办法（征求意见稿）》第 7 条。

[113] 参见《个人信息和重要数据出境安全评估办法（征求意见稿）》第 12 条。

[114] 参见《个人信息和重要数据出境安全评估办法（征求意见稿）》第 9 条。

据跨境”的含义与监管的具体流程，参照国际通行做法，增补了“个人同意”这一数据出境的重要条件之一。[115]

总体上就数据跨境流动来说。首先要鼓励和保护非个人敏感信息和公开数据自由流动。数据的价值在于信息，大数据发挥价值的前提在于算法分析，数据保持生命力的方式就是流动，这是数据承载信息的价值所决定的。除了可能涉及公民隐私的敏感信息应受宪法法律严格保护之外，对于非个人敏感信息、非重要数据以及公开数据等，立法宜鼓励并保障其跨境自由有序流动。本人认为，有必要在对数据进行分类和满足个人对其数据的自决权的前提下，确立非个人数据、非个人敏感数据和公开数据自由流动原则，在履行必要监管的同时，促进数据自由流动，立足于大数据驱动技术创新和经济发展的现实目标。目前我国倾向于采取“事前申报备案”的方式对个人数据出境进行规制，对豁免、例外情形规定较少。各国数据保护立法一般对数据出境规定诸多例外条件，从而在确保数据传输安全、维护公共利益及个人合法权益、尊重个人数据自决权、提高商业活动效率等情况下，促进数据跨境自由流动，推动经济发展。可供参考的豁免情况包括但不限于如下数据出境场景：（1）个人的授权同意；（2）个人出于私人或家庭活动需要主动公开（如拨打跨境私人电话、发送跨境私人邮件、进行跨境即时通信等）；（3）履行法律义务的需要（如配合执法机关调查、履行司法协助义务等）；（4）保障公共利益的需要；（5）司法与执法需要；（6）履行合同义务需要（如使用境外云盘、进行跨境电子商务交易等）；（7）出于内部管理目的在企业集团内部进行跨境数据传输（如雇员人力资源数据转移、雇员财务管理数据转移，以及客户常规数据梳理与转移等等）；（8）海关税务金融相关数据跨境传输；（9）数据输入地区数据保护水平与输出国相当（类似于“充分性认定白名单”）等；其次要明确数据跨境流动的监管要求及权责。数据跨境流动监管是网络治理的现实选择，建议从权力和责任两方面进行规定，对数据跨境传输、外企在华开展业务、民族企业走出去等可能涉及数据跨境流动的情形进行规范。例如，明确需本地化存储的特定关键数据范围；明确需开展出境评估的数据范围、评估流程、评估周期，以及对应主管部门等；再就是加强国际对话，形成双边或多边协作机制。无论是 CLOUD 法案的“适格外国政府”认定，还是 GDPR 的“充分性”认定，都体现出双边对话、平等互利的思路。我国的数据安全立法也应探索加强国际对话，通过双边或多边协作机制，扩大“数据自由流动生态圈”，提高司法协作效率，实现数据安全和合理的跨境流动。最后就我国而言，要借鉴国外有益的立法技术。我国数据出境安全评估类规范可统一将规范对象定义为“网络运营者”。同时，在大数据、云计算、平台经济迅猛发展的今天，宜寻求合适时机，将“网

[115] 京东法律研究院：《欧盟数据宪章——〈一般数据保护条例〉GDPR 评述及实务指引》，法律出版社 2018 年版，第 111 页。

络运营者”分为“数据控制者”和“数据处理者”两种角色，从而进一步明确不同数据输出主体的角色定位以及相应的权利、责任。建议可参考包括欧盟 GDPR 在内的境外法规与我国特殊情况予以考虑；在明确“数据控制者”和“数据处理者”权利和义务的基础上，主管部门可考虑出台“标准合同条款”，分别针对境内控制者与境外控制者、境内控制者与境外处理者之间的数据出境场景制定发布标准合同条款，从而更有针对性地确保不同场景下的数据跨境传输。

（二）数据交易中其他相关法律问题

在大数据精准营销时代，出现了“大数据杀熟”现象，在毫不知情的情况下，消费者自主判断和选择的能力因自主决定被操纵可能丧失，但消费者对此全然不知，李伦在著作中曾分析过这种现象，称其为“楚门效应”。[116]周永红、赵维在发表中也指出，大多数用户为了利用网络和信息服务，一般忽略个人隐私的自我保护，如注册时填满真实信息等。很多用户在自己的隐私数据泄露时，不知维权方式。因个人数据蕴含巨大价值，盗用、非法交易个人数据等侵权行为时有发生。为更好地进行大数据交易和大数据资源共享，个人数据权利应当受到法律保护。[117]例如，针对“大数据杀熟”现象，我国《电子商务法》第 18 条第 1 款规定：“电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益。李伦在分析并消除“楚门效应”的研究中进一步指出，伴随着个人数据保护的必要性或重要性，数据的收集和使用需征得用户的知情同意，要求尊重用户的数据权利和隐私权。机构或网站一般都制定了隐私条款，但这些条款出现了违背最少原则、扩大个人数据收集范围、违反知情同意原则、未经用户同意二次或多次使用用户数据等问题。因此，应对这些隐私条款进行审核与监督。37。从而让数据控制者或数据使用者等主体在对个人数据的处理中既要认识到数据的重要性，又要承担隐私保护的责任。

此外，通过对相关文献、资料的归纳，我们可以明显感受到国家日益重视通过加强对网络安全方面的立法和管理，以达到保护数据主体权利的目的。例如，我国《民法典》第 1038 条第 2 款规定：“信息处理者应当采取技术措施和其他必要措施，确保其收集、存储的个人信息安全，防止信息泄露、篡改、丢失；发生或者可能发生个人信息泄露、算改、丢失的，应当及时采取补救措施，按照规定告知自然人并向有关主管部门报告。”《网络安全法》第 12 条第 1 款规定：“国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提

---

[116] 参见李伦：《“楚门效应”：数据巨机器的“意识形态”一数据主义与基于权利的数据伦理》，载《探索与争鸣》2018 年第 5 期，第 29 页。

[117] 参见周永红、赵维：《大数据交易背景下用户个人数据权利的保护研究》，载《数字图书馆论坛》2019 年第 2 期，第 27 页。

升网络服务水平，为社会提供安全、便利的网络服务保障网络信息依法有序自由流动。”《网络安全法》第四章“网络信息安全”对个人信息的保护相对全面，如第 40 条规定：“网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。”第 42 条第 2 款规定：“网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。”第 49 条规定：“网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。”第 50 条规定：“国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。”同时，《数据安全法》也为数据交易过程当中可能涉及的数据安全问题提供了进一步的制度保障，促使数据交易经济活动实现健康有序运转。

从既有文献的梳理与分析结果来看，我们对于数据法律属性的探讨已经非常充分，只是在这些激烈的争辩之后，并没有能够互相充分说服的结论。但这种观点上的混沌状态显然难以满足数据经济发展对于制度供给的迫切需求，所以我们必须进行价值取舍与理论抉择。而数据交易行为的性质判定与数据法律属性的界定又紧密相连，在理论上存在前后延续性，所以也有部分文献对于该问题进行了相应思考，比如结合数据法律属性将数据交易行为定义为数据服务合同等。但总体上这种对于数据交易行为性质判定的理论研究是比较粗躁的，没有充分考虑数据交易的所有可能情形。而对于数据交易规则的具体构建的文献研究则更为鲜见，当然这也主要是受到数据基础法律问题研究进展缓慢的困扰。不过，对于数据交易中可能涉及的公法规制问题，既有的文献研究和立法实践还是有较多成果的，对于文章的写作也有较大的参考价值。从文献上来说，要实现对数据交易法律问题的全面剖解，并进而构建全面体系的数据交易法律制度还是极具挑战性的，笔者在后续写作中也会不断搜集整理最新的相关研究进展，以期为文章写作提供更好的助力，努力形成较为有说服力的理论说理。

参考文献

（一）中文著作

【1】弗吉尼亚·尤班克斯：《自动不平等》，商务印书馆 2021 年版。
【2】卡尔·拉伦茨：《法学方法论》，商务印书馆 2020 年版。
【3】劳伦斯·莱斯格：《代码 20》，清华大学出版社 2019 年版。
【4】罗伯特·P 莫杰思：《知识产权正当性解释》，商务印书馆 2019 年版。
克里斯托弗·米勒德：《云计算法律》，法律出版社 2018 年版。
【5】王汉生：《数据资产论》，中国人民大学出版社 2018 年版。
【6】张志安：《互联网与国家治理发展报告》，社会科学文献出版社 2018 年版。
【7】世界银行：《2016 世界发展报告》，清华大学出版社 2017 年版。
【8】黄志雄：《网络主权论》，社会科学文献出版社 2017 年版。
【9】姜浩：《数据化批判》，中国传媒大学出版社 2017 年版。
【10】刘珂：《贵州大数据兴起》，电子科技大学出版社 2017 年版。
【11】马科斯·卡泽尔：《罗马私法》，法律出版社 2017 年版。
【12】孙南翔：《互联网规制的国际贸易法律问题研究》，法律出版社 2017 年版。
【13】唐思慧：《大数据时代信息公平的保障研究》，中国政法大学出版社 2017 年版。
【14】福山：《信任》，广西师范大学出版社 2016 年版。
【15】佩德罗·多明戈斯：《终极算法》，中信出版社 2016 年版。
【16】李效东：《现代国际安全理论精要》，军事科学出版社 2015 年版。
【17】格林沃尔德：《无处可藏》，中信出版社 2014 年版。
【18】郑永年：《技术赋权-中国的互联网、国家与社会》，东方出版社 2014 年版。
【19】凯文·凯利：《新经济新规则》，电子工业出版社 2014 年版。
【20】徐晋：《大数据经济学》，上海交通大学出版社 2014 年版。
【21】徐子沛：《数据之巅》，中信出版社 2014 年版。
【22】沈逸：《美国国家网络安全战略》，时事出版社 2013 年版。
【23】陈威如：《平台战略》，中信出版社 2013 年版。
【24】迈耶-舍恩伯格：《大数据时代》，浙江人民出版社 2012 年版。
【25】(美)克里斯滕森：《创新者的解答》，中信出版社 2010 年版。
【26】胡晓军：《数据采集与分析技术》，西安电子科技大学出版社 2010 年版。

【27】(美)桑斯坦：《权利革命之后》，中国人民大学出版社 2008 年版。
【28】麻争旗：《媒介与主权》，中国传媒大学出版社 2008 年版。
【29】屠振宇：《宪法隐私权研究》，法律出版社 2008 年版。
【30】(美)劳伦斯·莱斯格（Lawrence Lessig）：《思想的未来》，中信出版社 2004 年版。
【31】高富平：《网络对社会的挑战与立法政策选择》，法律出版社 2004 年版。
【32】(美)托马斯·库恩（Thomas Kuhn）：《科学革命的结构》，北京大学出版社 2003 年版。
【33】(英)巴瑞·布赞（Barry Buzan）：《新安全论》，浙江人民出版社 2003 年版。
【34】理查德·A 波斯纳（Richard Posner）：《正义/司法的经济学》，中国政法大学出版社 2002 年版。
【35】孟勤国：《物权二元结构论》，人民法院出版社 2002 年版。
【36】张平著：《网络知识产权及相关法律问题透析》，广州出版社 2000 年版。
【37】(美)尼古拉·尼葛洛庞（Nicholas Negroponte）：《数字化生存》，海南出版社 1996 年版。
【38】江平、米健：《罗马法基础》，中国政法大学出版社 1987 年版。

（二）中文论文

【39】翟志勇：《论数据信托：一种数据治理的新方案》，载《东方法学》2021 年第 4 期。
【40】许可：《数据权利：范式统合与规范分殊》，载《政法论坛》2021 年第 4 期。
【41】丁晓东：《论数据垄断：大数据视野下反垄断的法理思考》，载《东方法学》2021 年第 3 期。
【42】李忠夏：《数字时代隐私权的宪法建构》，载《华东政法大学学报》2021 年第 3 期。
【43】兰磊：《论垄断行为分析模式的配置逻辑》，载《经贸法律评论》2021 年第 2 期。
【44】王利明：《和而不同:隐私权与个人信息的规则界分和适用》，载《法学评论》2021 年第 2 期。
【45】许可：《数据爬取的正当性及其边界》，载《中国法学》2021 年第 2 期。
【46】杰克·M 巴尔金、敖海静：《表达自由在数字时代的未来》，载《苏州大学学报（法学版）》2021 年第 1 期。

【47】莉娜·坎、大卫·博森、林少伟、林斯韦：《信息信义义务理论之批判》，载《交大法学》2021 年第 1 期。
【48】刘志强：《论“数字人权”不构成第四代人权》，载《法学研究》2021 年第 1 期。
【49】赵宏：《《民法典》时代个人信息权的国家保护义务》，载《经贸法律评论》2021 年第 1 期。
【50】申卫星：《论数据用益权》，载《中国社会科学》2020 年第 11 期。
【51】孔庆江、于华溢：《数据立法域外适用现象及中国因应策略》，载《法学杂志》2020 年第 8 期。
【52】杨旭东、高岭、王海、郭红波、郑杰：《一种面向直方图发布的均衡差分隐私保护方法》，载《计算机学报》2020 年第 8 期。
【53】支振锋：《贡献数据安全立法的中国方案》，载《信息安全与通信保密》2020 年第 8 期。
【54】刘欢、杨帅、刘皓：《零信任安全架构及应用研究》，载《通信技术》2020 年第 7 期。
【55】田杰棠、刘露瑶：《交易模式、权利界定与数据要素市场培育》，载《改革》2020 年第 7 期。
【56】高敏、张玉洁：《数据资源归国家所有的权利构造研究》，载《长江论坛》2020 年第 6 期。
【57】何伟：《激发数据要素价值的机制、问题和对策》，载《信息通信技术与政策》2020 年第 6 期。
【58】梅夏英：《信息和数据概念区分的法律意义》，载《比较法研究》2020 年第 6 期。
【59】韩瑞霞、徐剑：《网络主权视域下当前互联网治理的主要问题、成因及监管对策》，载《南京邮电大学学报（社会科学版）》2020 年第 5 期。
【60】苏道敬、夏小帆：《网络黑灰产的治理困境及法治应对探析》，载《法制与经济》2020 年第 5 期。
【61】王丹娜、周汉民：《推动中国数字经济安全、高质量发展》，载《中国信息安全》2020 年第 5 期。
【62】袁康、刘汉广：《公共数据治理中的政府角色与行为边界》，载《江汉论坛》2020 年第 5 期。
【63】唐彬彬：《跨境电子数据取证规则的反思与重构》，载《法学家》2020 年第 4 期。
【64】魏小强：《基于零信任的远程办公系统安全模型研究与实现》，载《信息

安全研究》2020 年第 4 期。
【65】冯果、薛亦飒：《从“权利规范模式”走向“行为控制模式”的数据信托——数据主体权利保护机制构建的另一种思路》，载《法学评论》2020 年第 3 期。
【66】胡凌：《网络法中的“网络”》，载《思想战线》2020 年第 3 期。
【67】李成熙、文庭孝：《我国大数据交易盈利模式研究》，载《情报杂志》2020 年第 3 期。
【68】李少卓、王娜、杜学绘：《按需披露的区块链隐私保护机制》，载《网络与信息安全学报》2020 年第 3 期。
【69】毛维准、刘一燊：《数据民族主义：驱动逻辑与政策影响》，载《国际展望》2020 年第 3 期。
【70】汪靖伟、郑臻哲、吴帆、陈贵海：《基于区块链的数据市场》，载《大数据》2020 年第 3 期。
【71】于施洋、王建冬、郭巧敏：《我国构建数据新型要素市场体系面临的挑战与对策》，载《电子政务》2020 年第 3 期。
【72】张丽娟、郭若楠：《国际贸易规则中的“国家安全例外”条款探析》，载《国际论坛》2020 年第 3 期。
【73】程啸：《区块链技术视野下的数据权属问题》，载《现代法学》2020 年第 2 期。
【74】丁晓东：《个人信息权利的反思与重塑论个人信息保护的适用前提与法益基础》，载《中外法学》2020 年第 2 期。
【75】石静霞：《数字经济背景下的 WTO 电子商务诸边谈判：最新发展及焦点问题》，载《东方法学》2020 年第 2 期。
【76】杨翱宇：《数据财产权益的私法规范路径》，载《法律科学（西北政法大学学报）》2020 年第 2 期。
【77】陈兴良：《网络犯罪的刑法应对》，载《中国法律评论》2020 年第 1 期。
【78】丁晓东：《论数据携带权的属性、影响与中国应用》，载《法商研究》2020 年第 1 期。
【79】韩旭至：《数据确权的困境及破解之道》，载《东方法学》2020 年第 1 期。
【80】华劼：《欧盟数据生产者权利质疑——以知识产权制度安排为视角》，载《知识产权》2020 年第 1 期。
【81】季卫东：《数据、隐私以及人工智能时代的宪法创新》，载《南大法学》2020 年第 1 期。

【82】李西明、陶汝裕、粟晨、黄琼、黄欣沂：《一种灵活的精度可控的可搜索对称加密方案》，载《计算机研究与发展》2020 年第 1 期。
【83】李政、周希禛：《数据作为生产要素参与分配的政治经济学分析》，载《学习与探索》2020 年第 1 期。
【84】张建文：《网络大数据产品的法律本质及其法律保护——兼评美景公司与淘宝公司不正当竞争纠纷案苏州大学学报（哲学社会科学版）》，载《》2020 年第 1 期。
【85】方元欣：《数据本地化政策的全球博弈分析》，载《中国信息化》2019 年第 12 期。
【86】罗原：《云计算环境下新型网络安全技术及解决方案》，载《电信工程技术与标准化》2019 年第 12 期。
【87】王文杰：《大数据时代网络信息安全及防护探讨》，载《中国管理信息化》2019 年第 12 期。
【88】罗王平、冯朝胜、秦志光、袁丁、廖娟平、刘霞：《一种面向公有云的密文共享方案》，载《软件学报》2019 年第 8 期。
【89】申卫星、杨旭：《中国民法典应如何规定居住权？》，载《比较法研究》2019 年第 6 期。
【90】邢会强：《大数据交易背景下个人信息财产权的分配与实现机制》，载《法学评论》2019 年第 6 期。
【91】崔国斌：《大数据有限排他权的基础理论》，载《法学研究》2019 年第 5 期。
【92】季卫东：《人工智能开发的理念、法律以及政策》，载《东方法学》2019 年第 5 期。
【93】廖继鹏：《计算机网络犯罪的防范措施探究》，载《法制与经济》2019 年第 5 期。
【94】马长山：《智慧社会背景下的“第四代人权”及其保障》，载《中国法学》2019 年第 5 期。
【95】张丽英、史沐慧：《电商平台对用户隐私数据承担的法律责任界定——以合同说、信托说为视角》，载《国际经济法学刊》2019 年第 4 期。
【96】朱程斌：《论人工智能电子人格》，载《天津大学学报（社会科学版）》2019 年第 4 期。
【97】许可：《数据安全法:定位、立场与制度构造》，载《经贸法律评论》2019 年第 3 期。
【98】姚佳：《企业数据的利用准则》，载《清华法学》2019 年第 3 期。

【99】梁坤：《基于数据主权的国家刑事取证管辖模式》，载《法学研究》2019年第2期。
【100】闫立东：《以“权利束”视角探究数据权利》，载《东方法学》2019年第2期。
【101】张敏：《大数据交易的双重监管》，载《法学杂志》2019年第2期。
【102】高秦伟：《个人信息概念之反思和重塑——立法与实践的理论起点》，载《人大法律评论》2019年第1期。
【103】肖建华、柴芳墨：《论数据权利与交易规制》，载《中国高校社会科学》2019年第1期。
【104】谢琳：《大数据时代个人信息使用的合法利益豁免》，载《政法论坛》2019年第1期。
【105】张新宝：《《民法总则》个人信息保护条文研究》，载《中外法学》2019年第1期。
【106】李雄一、熊励、孙文灿、王锟：《数据交易市场双边匹配模型与决策方法研究》，载《科技进步与对策》2018年第19期。
【107】李晓升：《大数据时代个人信息安全的刑法立法与完善》，载《中国市场》2018年第16期。
【108】许可：《数据权属:经济学与法学的双重视角》，载《电子知识产权》2018年第11期。
【109】雷震文：《以平台为中心的大数据交易监管制度构想》，载《现代管理科学》2018年第9期。
【110】吴超：《从原材料到资产——数据资产化的挑战和思考》，载《中国科学院院刊》2018年第8期。
【111】张敏、朱雪燕：《我国大数据交易的立法思考》，载《学习与实践》2018年第7期。
【112】纪海龙：《数据的私法定位与保护》，载《法学研究》2018年第6期。
【113】刘权、李东格：《网络黑产:从暗涌到奔流》，载《互联网经济》2018年第6期。
【114】丁晓东：《个人信息私法保护的困境与出路》，载《法学研究》2018年第6期。
【115】田野：《大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例》，载《法制与社会发展》2018年第6期。
【116】许可：《数字经济视野中的欧盟《一般数据保护条例》》，载《财经法学》2018年第6期。

【117】刘睿、张继成：《立法评价方法初探——立法过程中价值评价的理性分析》，载《法制与社会发展》2018 年第 6 期。
【118】叶名怡：《论个人信息权的基本范畴》，载《清华法学》2018 年第 5 期。
【119】周茂君、潘宁：《赋权与重构:区块链技术对数据孤岛的破解》，载《新闻与传播评论》2018 年第 5 期。
【120】茶洪旺、袁航：《中国大数据交易发展的问题及对策研究》，载《区域经济评论》2018 年第 4 期。
【121】丁晓东：《什么是数据权利?——从欧洲《一般数据保护条例》看数据隐私的保护》，载《华东政法大学学报》2018 年第 4 期。
【122】许可：《数据主权视野中的 CLOUD 法案》，载《中国信息安全》2018 年第 4 期。
【123】杨立新：《人工类人格:智能机器人的民法地位——兼论智能机器人致人损害的民事责任》，载《求是学刊》2018 年第 4 期。
【124】陈吉栋：《论机器人的法律人格——基于法释义学的讨论》，载《上海大学学报（社会科学版）》2018 年第 3 期。
【125】程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018 年第 3 期。
【126】高富平：《个人信息保护:从个人控制到社会控制》，载《法学研究》2018 年第 3 期。
【127】李爱君：《数据权利属性与法律特征》，载《东方法学》2018 年第 3 期。
【128】林洹民：《个人信息保护中知情同意原则的困境与出路》，载《北京航空航天大学学报（社会科学版）》2018 年第 3 期。
【129】龙卫球：《再论企业数据保护的财产权化路径》，载《东方法学》2018 年第 3 期。
【130】石丹：《大数据时代数据权属及其保护路径研究》，载《西安交通大学学报（社会科学版）》2018 年第 3 期。
【131】钱玉林、钱坤：《交易平台经营者的法律地位》，载《扬州大学学报（人文社会科学版）》2018 年第 3 期。
【132】黄宗智：《中国的正义体系的过去、现在与未来》，载《开放时代》2018 年第 2 期。
【133】武长海、常铮：《论我国数据权法律制度的构建与完善》，载《河北法学》2018 年第 2 期。
【134】闫铁鑫：《大数据背景下预测型警务的构建》，载《犯罪研究》2018 年第 2 期。

【135】周林彬、马恩斯：《大数据确权的法律经济学分析》，载《东北师大学报（哲学社会科学版）》2018 年第 2 期。
【136】胡凌：《超越代码:从赛博空间到物理世界的控制/生产机制》，载《华东政法大学学报》2018 年第 1 期。
【137】熊丙万：《实用主义能走多远?——美国财产法学引领的私法新思维》，载《清华法学》2018 年第 1 期。
【138】杨立新：《个人信息:法益抑或民事权利——对《民法总则》第 111 条规定的“个人信息”之解读》，载《法学论坛》2018 年第 1 期。
【139】叶媛博：《网络传销实证研究及打防对策》，载《北京警察学院学报》2018 年第 1 期。
【140】何波：《数据泄露通知法律制度研究》，载《中国信息安全》2017 年第 12 期。
【141】李春花、王桦、张彦哲、周可：《采用扩展公钥的云存储广播加密优化方法》，载《计算机研究与发展》2017 年第 12 期。
【142】刘金瑞：《关于《个人信息和重要数据出境安全评估办法（征求意见稿）》的意见建议》，载《信息安全与通信保密》2017 年第 6 期。
【143】胡凌：《商业模式视角下的“信息/数据”产权》，载《上海大学学报（社会科学版）》2017 年第 6 期。
【144】姚黎黎：《互联网平台免费服务提供者义务之设定》，载《重庆邮电大学学报（社会科学版）》2017 年第 6 期。
【145】许可：《数据保护的三重进路——评新浪微博诉脉脉不正当竞争案》，载《上海大学学报（社会科学版）》2017 年第 6 期。
【146】吕廷君：《数据权体系及其法治意义》，载《中共中央党校学报》2017 年第 5 期。
【147】梅夏英：《虚拟财产的范畴界定和民法保护模式》，载《华东政法大学学报》2017 年第 5 期。
【148】陈璐：《论《网络安全法》对个人信息刑法保护的新启示——以两高最新司法解释为视角》，载《法治研究》2017 年第 4 期。
【149】龙卫球：《数据新型财产权构建及其体系研究》，载《政法论坛》2017 年第 4 期。
【150】陈冉：《论大数据背景下隐私权的刑法保护》，载《中国刑事法杂志》2017 年第 3 期。
【151】丁道勤：《基础数据与增值数据的二元划分》，载《财经法学》2017 年第 2 期。

【152】王国成：《从 3V 到 5V:大数据助推经济行为的深化研究》，载《天津社会科学》2017 年第 2 期。
【153】张敏：《交易安全视域下我国大数据交易的法律监管》，载《情报杂志》2017 年第 2 期。
【154】祝振媛、李广建：《“数据—信息—知识”整体视角下的知识融合初探——数据融合、信息融合、知识融合的关联与比较》，载《情报理论与实践》2017 年第 2 期。
【155】祝振媛、李广建：《“数据—信息—知识”整体视角下的知识融合初探——数据融合、信息融合、知识融合的关联与比较》，载《》情报理论与实践年第期。
【156】苏今：《大数据时代信息集合上的财产性权利之赋权基础——以数据和信息在大数据生命周期中的“关系化”为出发点》，载《清华知识产权评论》2017 年第 0 期。
【157】孙冰：《黑色产业链暗流涌动个人数据“裸奔”如何防范》，载《中国经济周刊》2016 年第 49 期。
【158】王文平：《大数据交易定价策略研究》，载《软件》2016 年第 10 期。
【159】梅夏英：《数据的法律属性及其民法定位》，载《中国社会科学》2016 年第 9 期。
【160】陈天莹、陈剑锋：《大数据环境下的智能数据脱敏系统》，载《通信技术》2016 年第 7 期。
【161】吴伟光：《大数据技术下个人数据信息私权保护论批判》，载《政治与法律》2016 年第 7 期。
【162】张阳：《数据的权利化困境与契约式规制》，载《科技与法律》2016 年第 6 期。
【163】范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016 年第 5 期。
【164】王玉林：《信息服务风险规避视角下的大数据控制人财产权利与限制研究》，载《图书情报知识》2016 年第 5 期。
【165】张阳：《大数据交易的权利逻辑及制度构想》，载《太原理工大学学报（社会科学版）》2016 年第 5 期。
【166】华岗、顾德道、刘良华、田沄、许海燕、方丹丹：《城市大数据:内涵、服务架构与实施路径》，载《大数据》2016 年第 3 期。
【167】翟丽丽、王佳妮、何晓燕：《移动云计算联盟企业数据资产评估方法研究》，载《价格理论与实践》2016 年第 2 期。

【168】申晨：《虚拟财产规则的路径重构》，载《法学家》2016 年第 1 期。
【169】王玉林、高富平：《大数据的财产属性研究》，载《图书与情报》2016 年第 1 期。
【170】王贵松：《行政法上不确定法律概念的具体化》，载《政治与法律》2016 年第 1 期。
【171】刘洪玉、张晓玉、侯锡林：《基于讨价还价博弈模型的大数据交易价格研究》，载《中国冶金教育》2015 年第 6 期。
【172】芮文彪、李国泉、杨馥宇：《数据信息的知识产权保护模式探析》，载《电子知识产权》2015 年第 4 期。
【173】孙宝云：《论美国“敏感信息”管理过程的公开化及启示》，载《情报杂志》2015 年第 4 期。
【174】张新宝：《隐私到个人信息:利益再衡量的理论与制度安排》，载《中国法学》2015 年第 3 期。
【175】刘连泰：《信息技术与主权概念》，载《中外法学》2015 年第 2 期。
【176】王融：《关于大数据交易核心法律问题——数据所有权的探讨》，载《大数据》2015 年第 2 期。
【177】齐爱民、盘佳：《数据权、数据主权的确立与大数据保护的基本原则》，载《苏州大学学报（哲学社会科学版）》2015 年第 1 期。
【178】刘鹰：《浅析我国电商企业的大数据应用现状》，载《商业时代》2014 年第 25 期。
【179】何治乐、黄道丽：《欧盟《一般数据保护条例》的出台背景及影响》，载《信息安全与通信保密》2014 年第 10 期。
【180】梅夏英、杨晓娜：《网络服务提供者信息安全保障义务的公共性基础》，载《烟台大学学报（哲学社会科学版）》2014 年第 6 期。
【181】闫晓丽：《大数据分析与个人隐私保护》，载《中国信息安全》2014 年第 3 期。
【182】吕本富、陈健：《大数据预测研究及相关问题》，载《科技促进发展》2014 年第 1 期。
【183】肖秋会：《俄罗斯信息法研究综述》，载《中国图书馆学报》2013 年第 6 期。
【184】汪振林：《电子数据分类研究》，载《重庆邮电大学学报（社会科学版）》2013 年第 3 期。
【185】梅夏英、刘明：《网络侵权归责的现实制约及价值考量——以《侵权责任法》第 36 条为切入点》，载《法律科学（西北政法大学学报）》2013 年第 2

期。
【186】周奇：《云计算技术专利保护初探》，载《电子知识产权》2012 年第 12 期。
【187】李国杰、程学旗：《大数据研究:未来科技及经济社会发展的重大战略领域——大数据的研究现状与科学思考》，载《中国科学院院刊》2012 年第 6 期。
【188】宁红丽：《无偿合同:民法学与社会学之维》，载《政法论坛》2012 年第 1 期。
【189】郑彦宁、化柏林：《数据、信息、知识与情报转化关系的探讨》，载《情报理论与实践》2011 年第 7 期。
【190】齐爱民、周伟萌：《论计算机信息交易的法律性质》，载《法律科学（西北政法大学学报）》2010 年第 3 期。
【191】苏永钦：《现代民法典的体系定位与建构规则——为中国大陆的民法典工程进一言》，载《交大法学》2010 年第 1 期。
【192】梅夏英：《侵权法一般条款与纯粹经济损失的责任限制》，载《中州学刊》2009 年第 4 期。
【193】刘志刚：《公序良俗与基本权利》，载《法律科学（西北政法大学学报）》2009 年第 3 期。
【194】韩洪今：《网络交易平台提供商的法律定位》，载《当代法学》2009 年第 2 期。
【195】林旭霞：《虚拟财产权性质论》，载《中国法学》2009 年第 1 期。
【196】松下和夫、李佳：《论“人的安全”与“环境合作”》，载《浙江大学学报（人文社会科学版）》2008 年第 1 期。
【197】齐爱民：《论个人信息保护基本策略的政府选择》，载《苏州大学学报（哲学社会科学版）》2007 年第 4 期。
【198】刘德良：《个人信息的财产权保护》，载《法学研究》2007 年第 3 期。
【199】陈林林：《基于法律原则的裁判》，载《法学研究》2006 年第 3 期。
【200】彭礼堂、饶传平：《网络隐私权的属性:从传统人格权到资讯自决权》，载《法学评论》2006 年第 1 期。
【201】屈茂辉：《关于物权客体的两个基础性问题》，载《时代法学》2005 年第 2 期。
【202】杨立新、王中合：《论网络虚拟财产的物权属性及其基本规则》，载《国家检察官学院学报》2004 年第 6 期。
【203】傅鼎生：《义务的对价:双务合同之本质》，载《法学》2003 年第 12 期。
【204】徐洁：《论用益权的物权属性》，载《政治与法律》2003 年第 1 期。

【205】马俊驹、梅夏英：《财产权制度的历史评析和现实思考》，载《中国社会科学》1999 年第 1 期。

（三）学位论文

【206】陈旭琳：《个人信息协同保护的法经济学研究》，吉林大学 2021 年博士论文。
【207】姬蕾蕾：《数据权的民法保护研究》，西南政法大学 2019 年博士论文。
【208】刘新宇：《数据权利构建及其交易规则研究》，上海交通大学 2019 年博士论文。
【209】王磊：《个人数据商业化利用法律问题研究》，中央财经大学 2019 年博士论文。
【210】罗珍珍：《数据交易法律问题研究》，四川省社会科学院 2017 年博士论文。
【211】王秀秀：《个人数据权：社会利益视域下的法律保护模式》，华东政法大学 2016 年博士论文。
【212】郑光：《匿名通信系统的安全性分析与研究》，上海交通大学 2011 年博士论文。

（四）英文著作

【213】RICHTERICH ANNIKA, THE BIG DATA AGENDA: DATA ETHICS AND CRITICAL DATA STUDIES (2018).
【214】FEILER LUKAS, FORGÓ NIKOLAUS AND WEIGL MICHAELA, THE EU GENERAL DATA PROTECTION REGULATION (GDPR) : A COMMENTARY (2018).
【215】JAY ROSEMARY, MALCOLM WILLIAM, PARRY ELLIS, TOWNSEND LOUIS AND BAPAT ANITA, GUIDE TO THE GENERAL DATA PROTECTION REGULATION: A COMPANION TO DATA PROTECTION LAW AND PRACTICE (4TH EDITION)(2017).
【216】EZRACHI ARIEL AND STUCKE MAURICE E, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY (2016).
【217】PEITZ MARTIN AND WALDFOGEL JOEL, THE OXFORD HANDBOOK OF THE DIGITAL ECONOMY (2012).

（五）英文论文

【218】Khan Lina M and Pozen David , *A Skeptical View of Information Fiduciaries*, HARVARD LAW REVIEW(2019).

【219】Delacroix Sylvie and Lawrence Neil D, *Bottom-up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, INTERNATIONAL DATA PRIVACY LAW(2019).

【220】S Akila and U Srinivasulu Reddy, *Cost Sensitive Risk Induced Bayesian Inference Bagging （RIBIB） for Credit Card Fraud Detection,* JOURNAL OF COMPUTATIONAL SCIENCE (2018).

【221】Sen Nivedita, *Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?* . JOURNAL OF INTERNATIONAL ECONOMIC LAW (2018).

【222】Ruben Fernandez-Beltran and Filiberto Pla, *Prior-based Probabilistic Latent Semantic Analysis for Multimedia Retrieval,* MULTIMEDIA TOOLS AND APPLICATIONS (2018).

【223】Andreas Wiebe, *Protection of Industrial Data- A New Property Right for The Digital Economy?*. JOURNAL OF INTELLECTUAL PROPERTY LAW & PRACTICE (2017).

【224】Gary Anthes, *Data Brokers Are Watching You,* COMMUNICATIONS OF THE ACM (2014).

【225】Fennell Lee Anne, *Lumpy Property,* UNIVERSITY OF PENNSYLVANIA LAW REVIEW (2012).

【226】Nadezhda Purtova, *Property Rights in Personal Data: Learning from The American Discourse,* COMPUTER LAW AND SECURITY REVIEW: THE INTERNATIONAL JOURNAL OF TECHNOLOGY AND PRACTICE (2009).

【227】Mark A Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights,* STANFORD LAW REVIEW (2008).

【228】Henry E Smith, *Exclusion versus Governance: Two Strategies for Delineating Property Rights,* THE JOURNAL OF LEGAL STUDIES (2002).

【229】Graham Pearce and Nicholas Platten, *Achieving Personal Data Protection in the European Union,* JCMS: JOURNAL OF COMMON MARKET STUDIES (2002).

【230】Stephen J Kobrin, *Territoriality and the Governance of Cyberspace,* JOURNAL OF INTERNATIONAL BUSINESS STUDIES (2001).

【231】Stephen D Krasner, *Abiding Sovereignty,* INTERNATIONAL POLITICAL SCIENCE REVIEW (2001).