

个人数据交易中的互联网企业交易行为规制研究

李子煦

(山东理工大学法学院, 山东 淄博 255049)

摘要: 个人数据是数据中最有价值的部分之一,也是企业创造经济价值最重要的资源,个人数据流通起来才能发挥巨大的作用。互联网企业在个人数据交易中容易出现过度采集个人数据、对数据脱敏不到位,以及背离公平、诚信的合同原则和形式化知情同意规则的不当交易行为。应通过制定用户许可协议范本、完善数据脱敏规则、明确互联网企业的保护义务,建立行业自律机制和加强知情同意规则的遵守等方式对交易行为进行规制。

关键词: 个人数据交易; 互联网企业; 交易行为

中图分类号: F49; F724.6; F273.1 **文献标志码:** A **文章编号:** 1671-1807(2025)13-0229-06

数据作为新型生产要素,是数字经济生态圈中最重要的战略资产。国家高度关注数据发展战略并出台一系列政策性文件,以此对数据交易进行指引。2022年12月,《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》(以下简称“数据二十条”)明确提出促进数据使用价值复用与充分利用。2024年的《政府工作报告》再次强调大力推动数据开发开放和流通使用,并将之视为发展新质生产力的前提与基础。个人数据构成了信息社会的核心基础资源,而个人数据交易则是数据实现资产化与市场化的直接体现。从参与主体的角度出发,个人数据交易可被划分为初级交易与次级交易两大类。初级交易涉及数据处理者直接从个人那里获取数据,个人通过让渡数据使用权以换取数据处理者提供的网络服务或产品;次级交易则发生在数据处理者与第三方之间,即不同数据处理主体间的个人数据流转^[1]。当前,尽管一些数据公司或大数据交易中心承载着大量的数据交易活动,但这些交易量远未全面映射出中国个人数据交易的实际需求。更为严峻的是,在数据交易过程中频繁出现尖锐的矛盾与冲突,个人数据泄露、滥用及侵害事件屡见不鲜。鉴于此,亟待探讨个人数据交易中的作为数据处理者的互联网企业在与个人进行交易时对个人信息权益可能造成的风险,进而应当采取哪些措施对企业的交易行为进行规制,以期维护数据市场的稳定并促进其发展。

当前,互联网企业在个人数据交易中的种种行

为问题,已成为当前学术界与政策制定者共同瞩目的焦点,吸引了众多学者深入探究,旨在为规范互联网企业行为提供坚实的理论与实践支撑。李森^[2]认为在个人数据交易过程中,只有通过对个人数据进行相对保护,才能有效缓解数据领域中个人与企业之间的矛盾与紧张态势。中国对于企业收集个人数据的行为,秉持着附条件允许的立法立场,明确规定数据处理主体唯有在获取“个人同意”或符合其他法定条件的前提下,方可进行个人信息的收集工作。但现实中,大型互联网平台企业的强大影响力使得个人的谈判议价能力微乎其微,用户通常只能选择点击同意,缺乏选择权。阳雪雅^[3]指出互联网企业作为数据的主要处理者,其在交易中的行为既关系到自身的经济利益,更紧密联系着数据主体的权益保障以及整个数据市场的繁荣稳定。因此,清晰界定并规范互联网企业在数据交易中的权利与义务,对于推动个人数据交易领域的良性发展具有举足轻重的作用。针对当前个人数据在收集与处理环节所面临的制度性挑战,如知情同意原则流于形式,阳雪雅进一步提议,可以引入区块链技术作为解决方案。这一技术的应用将赋能个人数据主体,使其能够实时、准确地掌握自身数据的使用动态,从而有效缓解信息不对称的问题,显著提升数据交易过程中的透明度与公平性。为加强知情同意规则在个人数据交易中的适用,尹博文^[4]则主张摒弃“个人利益优先”这一单一立场,倡导运用多重主体规制模式,构建涵盖多个责任主体的数

收稿日期: 2025-01-17

作者简介: 李子煦(1998—),女,山东淄博人,硕士研究生,研究方向为民商法学。

据保护机制,将“形式知情”与“实际知情”相结合,并引入“弱同意”模型,以此调和个人数据交易与个人权益保障之间的关系。在常规情境下,互联网企业唯有在用户给予明确许可的条件下,方可进行个人信息的收集与处理。然而,孙小雨和关伟杰^[5]发现,不少互联网公司往往在网站首页设置相关协议或采用弹窗的形式征求用户的同意,以期完成合规的信息公开要求,但实际成效与预期相差甚远。互联网企业凭借其优势地位,对披露内容进行“价值筛选或导向”,这往往使用户处于相对劣势。为此,企业需明确界定个人数据使用的合理边界,在平衡企业数据利用需求与个人数据保护的过程中,确立一个恰当的平衡准则,保护与用户密切相关的个人数据权益,这样才可以增强用户对企业的信任。综上所述,互联网企业在个人数据交易中的交易行为规范问题,涉及数据保护、企业责任、用户权益等多个层面。现有的研究揭示了个人数据交易中的多个法律与实践问题,并提出了一系列理论与技术性解决方案,为未来在数据交易领域加强互联网企业行为的法律规制提供了有益的参考。

1 个人数据交易中的互联网企业交易行为类型与规制必要性

1.1 个人数据交易中的互联网企业交易行为类型

互联网企业可以以不同形式进行个人数据的交易,目前最常见的数据交易形式主要为3种:数据包交易、API(应用程序编程接口)数据交易以及数据定制化交易。

1.1.1 数据包交易形式

在数据包交易流程中,互联网企业作为数据交易的卖方,会先将待交易的数据上传或拷贝至指定的数据交易中心。一旦交易达成,买方(可能是另一家互联网企业或个人)将在数据交易中心获得数据的下载权限。交易确认无误后,卖方互联网企业有权要求交易中心从平台上下架该交易数据,以确保数据的流转符合双方约定。在这种模式下,买方获得的是对数据的使用权,而非所有权。这意味着买方互联网企业不能禁止或妨碍卖方对数据包的后继使用,也不能阻止卖方将数据再次交易给其他方。

1.1.2 API数据交易形式

API数据交易,作为一种在线交易形式,特指互联网企业通过应用程序接口(API)向数据需求方提供动态数据访问服务的行为。这种模式类似于知网等数据访问平台,但核心在于利用API接口进行

数据交互。在这种业务模式下,互联网企业不仅拥有权限来指定哪些对象可以访问其开放的数据,还能精确控制开放数据的范围和内容。个人则可根据自身需要调用数据,并按照访问的频次付费。

1.1.3 数据定制化交易形式

这一交易模式起始于数据买方(可能是另一家互联网企业、研究机构或个人)向数据卖方明确提出其所需数据的具体要求。随后,卖方互联网企业根据这些需求,进行数据的收集、整合与最终交付。该形式具有动态性,因为只有卖方互联网企业不断更新数据,才能满足定制人对数据质量的要求^[6]。数据定制交易的最大优势在于其能够满足客户高度个性化的数据需求,提供量身定制的数据解决方案。对于互联网企业而言,通过参与定制数据交易,不仅可以更加精准地获取所需数据,还能促进数据的高效采集与整理,从而为数据的充分利用和价值的最大化创造有利条件。

1.2 个人数据交易中的互联网企业交易行为规制必要性

在数字经济时代,数据作为核心资源与基础要素,其商品化特性愈发显著。个人数据,作为数据版图中的关键一环,其深度挖掘与有效利用已成为众多互联网企业获取利润的重要途径。然而,这一趋势也伴随着个人与互联网企业之间关系的日益紧张,这在数字经济发展进程中尤为明显。从国际法律框架的演变中不难发现,欧盟对数据权利的保护力度正不断加强。美国要求数据从业者在收集和使用的行为必须遵循“合理信息实践”原则,包括收集和储存个人信息的系统不得秘密运行、个人须事先被告知哪种类型的信息将被记录或使用等^[7]。世界范围内,企业普遍被视为政府和个人需高度警惕与防范的对象,其商业利益往往被视为与国家安全及个人人格权益相冲突的。因此,为了捍卫国家安全及保障个人权利,制定法律法规以约束企业的数据收集等商业活动显得尤为重要。在实际操作中,各国和地区针对互联网企业侵犯个人数据权利的集体诉讼案例层出不穷,进一步印证了这一利益矛盾的普遍性。例如,2022年9月,韩国个人信息保护委员会对谷歌和Meta未经用户同意收集个人信息、用于个性化推荐广告的违法行为进行审议,并对谷歌、Meta处以罚款。个人与互联网企业间的紧张态势不仅制约了互联网企业的蓬勃发展,也损害了用户体验,影响了其享受互联网服务的质量。理想的解决之道在于,企业与个人应

由对立转向合作,建立在个人充分知情并自愿授权的基础上,实现数据的合法交易。然而,现实情况中,大型互联网企业凭借其市场垄断地位,不仅掌控了大量数据资源,还可能滥用这种优势以维持或扩大竞争优势。相比之下,中小互联网企业为在竞争中脱颖而出,面对数据资源的匮乏,有时会采取非法手段如数据窃取、参与地下数据交易,这些行为不仅严重侵犯了个人隐私权,也扰乱了数据市场的正常秩序。“数据二十条”强调了培育数据市场的重要性,其中个人数据交易被视为关键一环。对于互联网企业而言,参与个人数据的合法有序交易,不仅有助于提升对个人数据的保护水平,也是推动数字经济健康发展的关键所在。因此,构建企业与个人间的和谐数据交易生态,对于平衡各方利益、促进数字经济繁荣具有深远意义。

2 个人数据交易中互联网企业的失范交易行为

随着大数据技术的发展,个人数据海量积累,互联网企业在对数据的收集、处理再到分析、交易过程中都将获得巨大的市场利益。中国对于个人数据的保护无论是在立法还是司法层面,均存在一定程度的不足。综合分析、整合中国个人数据交易中互联网企业存在的失范交易行为,才能针对性地提出规范互联网企业交易行为的建议。

2.1 过度采集个人数据

个人数据交易作为一种以营利为导向的商业活动,其核心在于将原始数据作为交易标的基础。数据的资产性和价值性激励着数据收集者力求全面收集数据,以期获取更多的数据资源从而在数据市场中占据优势,攫取更大的经济利益。然而,尽管欧盟的《通用数据保护条例》以及中国的《数据安全法》均明文规定数据收集应遵循最小必要原则,即在满足特定目的的前提下,仅收集和处理实现该目的所必需的最少量个人信息,但在巨大经济利益的驱使下,部分原始数据收集者在实际操作中往往难以坚守这一原则。这些收集者可能采用强制许可、信息不透明、默认同意等多种手段,过度收集包含个人信息的原始数据,导致个人信息收集范围无节制地扩大,严重侵犯了个人信息主体的合法权益。此外,当用户在注册网络账号或享受平台服务时,常被要求提供电子邮件等与服务相关的个人信息。部分平台在获取这些信息后,会运用数据处理技术进行深入分析,并将分析结果与有需求的网络运营商进行交易,其中不乏未进行脱敏处理

的个人信息。这种做法的直接后果是,用户频繁收到各类广告邮件,一部分邮件是推销产品、传播色情内容或包含诈骗链接的垃圾邮件。例如,2024年11月,多位用户发文称,准爸爸注册美柚等母婴类App后,频繁接到涉黄短信。在此之前,工信部组织过第三方检测机构对违规推送弹窗信息、App过度索取权限等问题进行重点抽测后,共发现38款App存在问题,包括欺骗诱导用户提供个人信息、强制用户使用定向推送功能、超范围收集个人信息等,其中就包含美柚和宝宝树孕育。

2.2 对数据脱敏不到位

数据脱敏旨在不改变数据原始格式和属性特征的基础上,依据敏感信息规则对涉及个人隐私、商业秘密和技术秘密等敏感数据进行变形处理,从而确保这些敏感隐私数据得到安全可靠的保护^[8],这既体现了法律层面的严格要求,也反映了技术实施上的必要性。对于互联网企业而言,个人敏感数据的脱敏处理是保护用户数据隐私的关键环节。在数据交易过程中,互联网企业作为数据卖方,有责任对数据进行彻底的敏感数据清洗,并通过匿名化处理确保数据与具体个人之间的关联被彻底切断,从而避免数据接收方通过技术手段识别出个体身份。特别是在保险、信贷等风险定价敏感领域,互联网企业作为个人数据处理者,能够轻易获取用户的敏感信息。如果不加以妥善处理,这些企业可能会基于敏感数据的分析结果做出具有歧视性的决策,如个人遗传数据的泄露就可能让用户在就业、保险、教育及社会生活等多个方面遭遇不公平待遇^[9]。《个人信息保护法》第28条第1款通过抽象概括结合非穷尽式列举的方式,对敏感个人数据进行了界定,似乎表明敏感性与特定的数据类型之间存在着客观联系。然而,这种理解具有一定的片面性,因为它忽略了敏感性与具体应用场景之间的复杂关系。随着敏感个人数据形式的不断多样化,互联网企业如果忽视了非敏感数据与敏感数据之间的潜在联系,就可能在法律条款的实际应用中遭遇障碍,这不仅会损害敏感数据主体的个人权益,还会阻碍信息化技术的创新与迭代发展^[10]。鉴于大数据的交互特性和网络信息的复杂性,机器学习算法具备突破限制的能力,能够挖掘海量数据中潜在的相关性,从而经常能够克服因缺乏直接联系而产生的局限^[11]。在数据交易的情境中,即便数据卖方已经对个人数据进行了一次性的脱敏处理,但这些数据在庞大的数据集中仍有可能被重新组合,进

而形成与个人身份相关联的、更为详尽的数据信息,从而引发个人信息及隐私泄露的风险。互联网企业应当意识到,数据脱敏并非一种简单的“非黑即白”的处理方式。诚然,脱敏处理会降低数据的识别能力,但当这些脱敏后的数据与其他碎片化的个人数据相结合时,它们可能会相互补充,增强识别个体的可能性。

2.3 背离公平、诚信的合同原则

数据的生产与商品化过程显著地体现了资本密集和技术密集的特点,而在数据交易市场中,数据的提供方往往是大规模甚至具备垄断地位的企业,它们拥有远超普通市场主体的资金和技术优势^[12]。在此背景下,许多互联网企业作为数据提供方,在数据交易过程中占据了明显的优势地位,能够主导交易流程并决定交易价格。这种优势地位实质上造成了数据交易主体间的不平等,极大地损害了交易双方身份上的公正性^[13]。此外,在合同订立时,数据处理者利用免费机制承诺个人无须缴纳费用即可使用网络产品与服务,使个人误认为未与数据处理者发生交易而同意其收集个人数据^[14]。事实上,个人与数据处理者之间的数据换取服务行为是典型的个人数据交易行为。当个人错误地认为自己获得免费服务时,就极有可能忍受数据处理者采取的过度攫取个人数据行为,由此被迫承受个人数据交易的不公正结果。处于相对优势地位的互联网经营者应当诚信经营,在黄某诉某科技(深圳)公司等侵害个人信息、隐私权纠纷案中,虽然社交软件和阅读软件均由深圳某计算公司运营,但社交平台 and 阅读平台属于两个平台,仍需个人信息主体的明确同意。读书信息中可能包括用户不愿意公开的信息,仅以用户概括性地同意用户协议,不能认定充分履行告知和获得同意的义务。这体现出企业滥用其相对优势地位,未能秉持诚信原则对待自身所处优势地位。

2.4 形式化知情同意规则

个人对自己个人数据的处理拥有不可或缺的知情权和决定权,这对于捍卫个人的人格尊严与自由至关重要。根据知情同意原则,互联网企业在进行个人数据的收集与处理时,必须清晰地向数据主体说明相关目的及情况,并获取其明确的同意。这一原则在实践中通常体现为要求个人通过勾选格式条款来表达同意。然而,尽管知情同意原则旨在保障个人在数据交易中的权益,互联网企业却常常将其作为一种“保护伞”,甚至在某些情况下变相剥

夺了个人的决定权。以“谷歌案”为例,用户若要使用 Google 账户,就必须先接受 Google 的格式条款,这其中包括了对 Google 收集和处理个人数据的同意。只有在用户“同意”这些条款后,才能进一步去调整个性化广告的设置。这种做法实际上是在对用户进行变相的强制同意,使个人难以真正行使自己的知情权和决定权^[15]。虽然个人数据交易中的知情同意看似遵循了私法中意思自治的基本原则,但实际上,这并未实现与个人数据主体之间的信息充分共享,因此难以保证真正体现了数据主体的真实意愿^[16]。同时,由于个人数据具有低价值密度的特点,单个用户在与互联网企业的交易中往往缺乏议价能力。尽管在法律上双方的地位是平等的,但在实际的谈判力量上,双方存在着显著的差异。服务商虽然表面上提供了多种选择,但实际上,用户往往只能被动接受这些条件,否则就无法享受其提供的产品或服务。这种现象揭示了个人在数据交易所处的弱势地位,以及知情同意规则在实践中的局限性。

3 个人数据交易中的互联网企业交易行为规制路径

在当前个人数据交易日益频繁的实践中,中国法律体系尚缺乏一套成熟、完整且与这一领域相匹配的制度架构,难以对互联网企业的交易行为实施全面、系统的规制。鉴于此,以下将着重探讨并阐述针对互联网企业交易行为进行规制的有效路径。

3.1 制定用户许可协议范本

用户许可协议是用户与互联网平台之间的一种法律协议,它规定了用户在使用互联网平台服务时需要遵守的条款和条件,以及互联网平台对用户数据和隐私的处理方式。协议的内容通常包括使用许可、知识产权归属、用户行为规范、法律责任与免责、协议修改与终止等条款。不同的互联网平台会根据自身的业务特点、服务内容以及法律法规的要求,制定各自的用户许可协议。这些协议在内容、格式和条款上可能存在较大的差异。目前互联网平台并没有统一的用户许可协议,有些互联网企业与个人进行数据交易时,就会通过自己制定的用户许可协议,获取不符合该平台业务特点、服务内容的数据。因此有必要制定统一的用户许可协议,为互联网企业提供不同类型的范本,详细规定何种情况下企业可以收集超过范围的数据,防止企业为一己私利而损害个人合法权益。对于普通个人数据的收集,可以采用统一且简洁的格式化规则来高

效获取。然而,当数据收集具有特定目的且需要扩大范围时,就必须进行更加具体和针对性的“告知”与“同意”流程。这种做法既可以有效防止数据收集范围的过度宽泛,又能促进数据处理器与数据提供者之间关系的和谐。此外,还应明确规定,互联网企业不得擅自利用技术手段对通过合法途径获得的个人数据进行深入分析。若数据分析对于企业经营确属必要,企业应以醒目的方式(如加大字体、使用不同颜色等)来引起用户的注意,并获取用户的明确同意。在用户对此表示疑惑时,企业有责任进行充分的解释和说明,方可进行后续的技术分析。

3.2 完善数据脱敏规则

为了优化数据交易中的敏感数据处理流程,必须清晰界定敏感数据清洗的责任主体及其执行标准。互联网企业在进行次级数据交易之前,负有对个人数据进行匿名化处理的法律义务,这要求它们运用专业技术手段对个人数据进行有效清洗。鉴于个人通常不具备数据脱敏所需的技术能力和条件,因此,作为数据初次交易的接收方和后续扩散的起点,互联网企业承担着在数据流转初期就进行敏感数据清洗的重任。对清洗后的数据进行脱敏合格性的严格审查同样不可或缺,且清洗标准应由法律明文规定。具体而言,脱敏后的可交易数据必须确保无法直接关联到具体个人或企业,同时,这些数据应难以通过现有技术手段轻易复原,以维护数据的安全流通。随着技术的不断进步,数据脱敏技术也应与时俱进,法律需鼓励并规范技术的持续升级,以适应时代发展的需要,确保数据交易在保护个人隐私的同时,促进数据的合法合规流通。此外,若在交易过程中发生个人数据泄露、隐私权侵权行为,应明确各主体的责任承担。笔者认为,互联网企业在数据交易中处于优势地位,应当对数据流通和数据产业的健康发展承担更多责任,因此对互联网企业适用过错推定责任,即企业应当承担赔偿责任,除非企业能证明已对数据进行脱敏处理,并且达到无法轻易复原的程度。

3.3 明确互联网企业的保护义务,建立行业自律机制

互联网企业既能参与与个人进行的初级数据交易,也能参与与其他互联网企业(第三方数据处理器)的次级数据交易。而处于次级数据交易阶段的互联网企业,由于法律没有规定这些处理器对个人数据的保护义务,就有可能在对个人数据进行最

大化利用时造成对个人权益的损害,因此,初级数据交易合同的效力应当及于第三方,促使第三方数据处理器遵守初级数据交易合同中对其使用、转让等处理个人数据行为的限制规定。这是对合同相对性的突破,正如著作权人在部分转让著作财产权的同时,始终保留不可剥夺的署名权一样,数据主体在进行个人数据交易时,也不会因此完全丧失其对个人数据的所有权利。这一特性确保了个人数据具有一种法律约束力,能够要求那些与数据主体无直接法律关联的第三方尊重并维护数据主体对个人数据的各项权益。除此之外,要建立行业自律机制,相关监管部门应积极督促各行业协会和组织制定本领域内数据流转的自律性、指导性规范,针对交易中的不公正、不诚信行为进行罚款或者禁止其一定期限内进行数据交易。企业应针对存在安全隐患的数据实施标准化的管理流程,详细记录数据的访问历史,确保这些记录可追溯、可验证、责任可追究,从而最大限度地消除信息泄露的风险^[17]。

3.4 加强知情同意规则的遵守

《个人信息保护法》第十三条明确指出,获取个人信息需事先征得个人同意。鉴于个人数据交易本质上涉及个人信息的转让,个人信息保护法的相关规定同样适用于个人数据交易活动,以维护意思自治在契约型治理中的核心地位^[18]。然而,实践中,网络服务商往往出于自身利益最大化,采取多种策略诱导个人“同意”提供更多个人数据,导致个人难以在充分知情的情况下做出真正的同意决定^[19]。因此互联网企业应当采取更加清晰、直接的告知方式。例如,利用醒目的弹出窗口或加粗字体的形式,来引起数据提供者的注意。同时,信息的表述应当力求简洁明了,避免冗长和复杂的措辞,以便数据提供者在有限的时间内能够迅速抓住重点,并基于充分的理解做出是否同意的决定。企业应定期开展内部培训,提高员工对知情同意规则的认识。例如,安排法务人员讲解相关法律法规,结合实际案例分析违规行为可能导致的后果。同时,在新员工入职培训中加入这部分内容,确保所有员工从入职起就树立正确的合规意识。政府也应不断细化和完善关于数据隐私和知情同意的法律法规。以欧盟的《通用数据保护条例》为例,该条例详尽地规定了企业在收集、使用及存储个人数据时,必须获取用户清晰明确的同意,并且对于同意的具体形式、内容构成以及撤回机制等方面均设定了严格的标准。这样的详细法律条文不仅为企业明确

了其应承担的责任范围,也为企业在实际操作中遵循这些规定提供了坚实的法律支撑。

4 结论

数据交易作为信息社会必不可少的一环,对于驱动经济增长和促进社会进步具有重要作用。规范互联网企业在个人数据交易中的行为,不仅能够有效保障数据安全和个人隐私权,还为数据交易市场的长远健康发展奠定了坚实基础。诚然,通过制定用户许可协议的标准模板等措施,可以在一定程度上提升治理效能。然而,要进一步推动个人数据交易的繁荣发展,实现个人与互联网企业之间的互利共赢,还需在理论与实践层面的进一步探索。

参考文献

- [1] 夏庆锋. 个人数据交易的私法制度构造研究[J]. 中国法学, 2024(5): 144-164.
- [2] 李森. 数据立法核心问题的类型化展开[J]. 中国科技论坛, 2024(8): 83-93.
- [3] 阳雪雅. 数据要素市场下个人数据交易的证成与实现[J]. 上海政法学院学报(法治论丛), 2023(5): 91-105.
- [4] 尹博文. 个人数据交易中知情同意规则的破局与重构[J]. 科技与法律(中英文), 2022(5): 85-94.
- [5] 孙小雨, 关伟杰. 平台经济数据隐私保护与合规之协调[J]. 海峡法学, 2024(4): 29-42.
- [6] 林涸民. 个人数据交易的双重法律构造[J]. 法学研究, 2022(5): 37-53.
- [7] 李晔. 我国数据交易监管制度研究[D]. 南昌: 江西财经大学, 2022.
- [8] 徐双, 刘文斌, 李佳龙, 等. 大数据背景下的数据安全治理研究进展[J]. 太原理工大学学报, 2024(1): 127-141.
- [9] 莫琳. 公共卫生安全视角下医疗健康个人信息的保护与限制[J]. 电子知识产权, 2022(5): 88-98.
- [10] 莫琳. 数字经济背景下的数据交易及其法律制度构建[J]. 华侨大学学报(哲学社会科学版), 2024(1): 117-127.
- [11] COHEN J E. Turning privacy inside out[J]. Theoretical Inquiries in Law, 2019, 20: 1-31.
- [12] 王茜. 商法意义上的数据交易基本原则[J]. 政法论丛, 2022(3): 120-131.
- [13] 杨旭. 个人信息处理中履行合同必需规则的限制适用[J]. 法学, 2023(6): 85-98.
- [14] 张新宝. “普遍免费+个别付费”: 个人信息保护的一个新思维[J]. 比较法研究, 2018(5): 1-15.
- [15] 张敏. 数据交易中的伦理问题及其法律规制[J]. 上海政法学院学报(法治论丛), 2023(6): 122-132.
- [16] 刘斌. 个人数据交易领域数据信托的私法建构[J]. 学习与实践, 2024(6): 83-92.
- [17] 汪浩, 张俊妮. 连带责任、数据交易与信息权益保护[J]. 经济研究, 2024(9): 118-135.
- [18] 黄文艺. 民法典与社会治理现代化[J]. 法制与社会发展, 2020(5): 21-37.
- [19] 程啸. 论个人信息处理中的个人同意[J]. 环球法律评论, 2021(6): 40-55.

Research on the Regulation of Internet Companies' Trading Behaviors in Personal Data Transactions

LI Zixu

(School of Law, Shandong University of Technology, Zibo 255049, Shandong, China)

Abstract: Personal data is one of the most valuable segments of data and is also the most crucial resource for enterprises to create economic value. The circulation of personal data can unleash its immense potential. However, internet companies are prone to improper trading behaviors in personal data transactions, such as over-collecting personal data, inadequate data desensitization, deviation from the principles of fairness and integrity in contracts, and formalistic informed consent rules. To address these issues, regulatory measures should be implemented through the formulation of model user license agreements, the improvement of data desensitization rules, the clarification of protection obligations for internet companies, the establishment of industry self-regulatory mechanisms, and the enhancement of compliance with informed consent rules.

Keywords: personal data transactions; internet companies; trading behaviors