数据交易平台安全保障义务的类型化研究

●李向阳

[摘要]《数据安全法》及各地出台的数据条例均明确指出了数据交易平台在推动交易活动的同时，要确保数据交易符合安全要件。然而，在具体操作层面，关于如何切实履行安全保障义务，尚缺乏详尽的规定。为此，本文首先从数据交易平台的特殊性出发，厘清数据交易的特点及数据交易平台安全保障义务的法理基础；其次，梳理了当前数据交易所面临的法律风险；最终提出以数据交易平台安全保障义务的类型化建构来应对当前出现的法律风险，以切实化解数据交易平台安全保障义务履行的系统性困境，构建安全、可信的数据交易环境。

[关键词] 数据交易平台；数据安全；保障义务

作为构建安全高效的可信数据流通体系的重要载体，数据交易平台不仅为数据交易双方提供可信的交易环境，同时也承担着数据安全保障的义务。数据交易平台作为数据流通的可信枢纽，能够提供数据全生命周期的安全保障义务。而当下关于数据交易平台的安全保障义务的相关规定，散见于《数据安全法》《个人信息保护法》《网络安全法》等相应规范中，且整体规定过于粗疏。此外，与传统交易不同的是，数据交易中的信任危机更甚。即使是交易量庞大的数据场外点对点交易，供需双方间也缺乏信任。这牵涉到数据供给方和数据需求方对双方资质查询、交易产品质量认定等方面成本的消耗，同时也是由于合规审查和监管体制不完善的市场忧虑。简而言之，数据交易市场呈现出了畸形化的交易结构。此时，数据交易平台如何构建明晰的数据安全保障义务，是提高数据交易合规效率、降低合规成本的重要考量，以实现数据动态合规的“正向激励”。

基于此，有必要阐明数据交易平台安全保障义务的本质意蕴，以及数据交易所面临的法律风险，并进一步明确数据交易平台履行数据安全保障义务的类型化构建。

Q 数据交易平台安全保障义务的理论基础

在对数据交易平台的安全保障义务进行研究前，首先，要明确数据交易的相关概念和特点。其次，应该指明数据安全保障义务的法理基础，为下文的研究奠定基础。

（一）数据交易的相关概念

在法规框架内，尽管我国现行法律体系尚未对数据交易的具体范畴进行明确界定，但我国在多个层面，包括国家推荐性标准、地方性立法及政府规章等，已积极展开了广泛而深入的探索与实践。具体到《信息安全技术数据交易服务安全要求》（GB/T37932-2019）这一国家层面的推荐标准中对其定义为：“数据供方和需方之间以数据商品作为交易对象，进行的以货币或货币等价物交换数据商品的行为”。

就数据交易平台而言，以数据交易的业务模式为区分视角，数据交易平台可分为第三方数据交易平台与混合数据交易平台。前者处于中立第三方，仅向数据供需双方提供交易通路，本身并不参与数据交易，业务属性为撮合交易。不同于前者的单一属性，混合型数据交易平台在提供中介服务的基础上，以数据供应商、服务商的角色参与数据交易开展业务。

（二）数据交易平台安全保障义务的法理基础

依循危险控制理论的核心逻辑，数据交易平台作为数据交易过程中的关键控制者，其对潜在危险源具有显著的控制力，因此应承担起相应的安全保障义务。概而言之，任何主体在掌管特定场所时，均须肩负起一系列特定的义务，这不仅是权责对等原则的体现，也是收益与风险共担的必然逻辑。一方面，作为控制者，数据交易平台凭借自身地位，在所控制的领域内开展经营活动以谋求利益，相应地其也必须承担起预防潜在危险、确保安全无虞的控制责任。这种责任源自他们对场所的直接管理和影响能力。另一方面，控制者身处其管理范围内，对潜在的风险源具备直接的控制力，这赋予了他们识别、评估并应对风险的能力与责任。作为在数据交易领域内拥有控制力的主体，数据交易平台需要承担起保障数据安全与交易顺畅的安全保障义务。

数据交易平台不仅为买卖双方搭建了交易桥梁，还负责数据的存储与交易资金的结算，其在交易流程中扮演着举足轻重的角色，因此自然而然地承担起了数据安全保障义务。这不仅是应对数据安全挑战、化解潜在风险的必要手段，也是提升场内交易模式信誉度、增强其市场吸引力的关键所在。

数据交易面临的法律风险和问题检视

尽管我国数据要素交易市场在政策引领下稳步发展，但在数据要素流通交易的实践中仍面临法律风险。信任缺失、数据非法采集、倒卖及滥用频发等这一系列违法违规行为，不仅对个人数据权益和企业数据权益造成了影响，也指引着人们进一步深入探索数据交易中数据交易平台应该承担何种安全保障义务。对此，下文以个人数据交易和企业数据交易的两个维度，对数据交易面临的法律风险进行检视。

（一）个人数据交易中的法律风险

个人数据交易中所面临的法律风险，在具体的交易实践中主要表现为非法收集与隐私泄露的问题。

隐私风险是信任危机的重要表现形式，也是个人信息被采集中的隐忧所在。尽管《个人信息保护法》中以“告知——同意”原则划定了数据收集的边界，但信任危机并未就此消除。企业加速对数据的攫取形成自己的技术壁垒，用户被迫用隐私换取服务的社会生态，“告知——同意”原则显然发生异化，企业的告知义务并不能与用户“知情同意”的权利对等，这实际上也违背了等价交换的基本原则。冗长晦涩的用户协议、隐私政策似乎成为企业规避法律的“避风港”，致使这种信任危机出现的根本原因在于用户和企业法律利益的背离。

交易流程中的个人信息泄露问题同样不容忽视。尽管《数据安全法》为数据交易中介服务机构设定了监管职责，各地数据交易平台也制定了相应的交易规则以强化监管，但数据的可无限复制特性、脱敏处理的不完善及交易后监管机制的薄弱，使得个人信息即便经过处理，仍可能保持一定的可识别性，进而面临被滥用和泄露的风险，这严重侵犯了自然人的隐私权和个人信息权益。此外，不可忽视的是，现实中还存在一部分数据交易绕过数据交易平台，以点对点的模式直接进行数据交易，即所谓的“场外交易”。这种交易模式完全游离于行业监管之外，为非法买卖个人信息提供了温床，使得难以对其进行合规监管，极易滋生灰黑数据交易。这对于数据交易市场的健康、有序发展构成了严重威胁。

（二）企业数据交易中的法律风险

目前，企业数据在进行交易时面临着市场失灵。这里主要以数据来源合法性和数据质量两个层面来说明其法律风险。

在数据交易的前置阶段，验证数据来源的合法性与合规性至关重要。在撮合交易的过程中，数据供应方通常会携带自有的数据信息进行展示，并邀请潜在买家进行报价与谈判，而需求方则基于自身需求提出询价，力求达成交易。然而，这一看似顺畅的流程背后，隐藏着一个不容忽视的难题：数据来源的合法性及卖方是否具备合法的处分权能。换言之，卖方数据权利是否完整无瑕，成了一个关乎交易安全性的法律隐患。

此外，随着数据交易市场的持续扩张，数据质量问题已跃升为不可忽视的挑战，其主要表现为数据质量评价难以实现。原因在于：首先，数据产品是一种“体验型”产品，只有经过长期的使用或者经过第三方加以验证才能明确其效用。其次，数据产品事前难以进行较为全面的信息披露。一方面，由于所交易的数据产品涉及数据供给方的商业秘密；另一方面，数据产品可能包含个人信息或者存在其他数据合规风险，导致数据交易当事人也很难预料。这种数据质量的非标准化不仅限制了数据的实际应用价值，也致使交易双方矛盾频发，不断滋生风险。

数据交易平台安全保障义务的类型化展开

事实上，透过上述问题，足可窥见数据动态安全的风险和挑战与数据要素价值创生这一复杂的交互过程相伴而生。数据交易平台在应对数据安全风险时如何履行安全保障义务正是下文的主要议题。

（一）实质审核义务

从责任基础来看，数据交易平台作为一种特殊中介人，应当依循《数据安全法》第33条和《民法典》第962条来划定其义务边界。一方面，有学者指出，应当按照数据交易平台的特性出发，对其所应承担的如实告知义务进行特殊设计，即履行实质审核和积极调查义务。另一方面，数据安全保障义务本质上是一种公法私法化的“转介”性义务，而安全保障义务为公法注入私法的转介渠道中就包括了主体身份核验这一内容。从体系性解释的视角，数据交易平台应当对数据交易主体资质进行实质审核。

主体身份验视（完成身份认证）属于数据交易（线上交易）信任的第一道闸石。“数据交易流通过程可追溯”首先就要求数据交易平台，在为数据交易双方提供交易通路前对双方主体资质进行核验，确保主体可追溯。目前，数据交易平台多采用注册会员制来把控数据交易主体的准入流程，并且一般否定个人成为数据交易主体。就现实状况而言，《上海市数据条例》第15条规定了自然人同样具有成为数据交易主体的资格。因此，数据交易平台对于个人用户的准入不应排斥，并采用差异化的交易资质审核要求应对不同主体。

其原因在于，当数据主体身份难以查明时，数据的使用目的和方式更加不得而知。故而，通过对数据交易双方主体资质加以核验时，能够进一步验证数据交易双方的交易权限以及数据需求方的数据使用方式与使用目的。

另外，值得注意的是，数据交易平台的实质审核义务兼具着对数据质量和来源加以验证的使命，其不能仅满足于“善意且尽到合理注意义务”的形式审查标准，因为这可能会严重侵蚀公众对数据交易平台的信任根基。因此，数据交易平台在其作为中介促进交易的角色之外，还需要清晰地界定信息处理的范畴、明确处理目的并划定行为界限，对数据来源也承担起更为严格的实质审核义务。

（二）记录保存义务

《数据安全法》第33条规定了数据交易平台留存、审核交易记录的义务。但对于如何具体履行并未明确交代，这里可以借鉴既有规范，进一步释明这一义务的真意。在产品交付阶段，需要对数据流转的历程加以记录，此处进行相关内容的记录是以交易合约为中心，对交易过程的记录。另外，交易完成后，为了促进数据产品的再利用与流通，部分数据可能会被存储在数据交易平台上。此时，数据交易平台应当履行数据安全保障义务，确保这些留存数据的完整性、保密性和可用性。实践中《深圳经济特区数据条例》第75条已经制定明确的规则，规定了数据交易平台必须保存交易记录，并设定合理的保存期限。这一做法不仅有助于数据的可追溯性，还能为解决潜在的交易纠纷提供有力的证据支持。

（三）数据报送义务和数据销毁义务

具体来说，数据交易平台需要进行信息披露，以回应《数据安全法》第29条所规定的“数据安全事件报告义务”及第30条规定“重要数据的数据处理者定期开展风险评估并报告的义务”。这就要求其应当对有关主管部门承担报送义务，在数据交易平台履行数据报送义务时应当以定期报送为主，临时报送更多应适用于突发性数据安全事件等例外情形。将交易磋商、产品交付阶段归档的数据交易记录日志报送主管部门，不仅能预防混合数据交易平台的自我优待，避免数据提供方与数据交易平台恶意串通，损害数据需方的合法权益。数据销毁义务与数据交易平台的报送义务联系密切，数据交易平台在交易结束后生成的交易日志不仅需要报送主管部门加以备份审计，同时也要对交易过程中缓存的各方数据加以清除，进行数据销毁。数据交易平台履行这一义务时，需要以“数据的彻底清除和不可复原”为基本原则，同时应当禁止数据交易平台未经交易双方授权或不存在法律规定的其他合理事项时对交易过程记录擅自更改、删除等。

结束语

综上，数据交易平台安全保障义务的类型化研究是数据治理范式转向下的重要子命题。本文以问题为导向呈现的领域法学思维与数据流通的治理范式高度契合。数据交易平台的业务类型和技术方案择定上的差异化呈现，为数据安全保障义务类型化的论证提供了现实可能。同时，通过义务类型化有助于进一步研究数据交易主体违反义务的责任承担，以实现《数据安全法》《个人信息保护法》等相关规范与《民法典》的衔接适应。

参考文献

[1]王青兰，王喆.数据交易动态合规：理论框架、范式创新与实践探索[J].改革，2023(08)：42-53.

[2]吴洁，张云.要素市场化配置视域下数据要素交易平台发展研究[J].征信，2021，39(01)：59-66.

[3]杨显滨.论场内数据交易的法律制度建构[J].政治与法律，2024(05)：159-176.

[4]倪楠.欧盟模式下个人数据共享的建构与借鉴——以数据中介机构为视角[J].法治研究，2023(02)：22-33.

[5]武腾.数据交易的合同法问题研究[M].北京：法律出版社，2023：231-232.

[6]杨显滨.数据交易所的合同法规制困境与出路[J].贵州社会科学，2023(11)：89-97.

[7]万方.公私法汇流的阀口转介视角下的网络经营者安全保障义务[J].中外法学，2020，32(02)：357-377.

[8]高艳东，李易.政府履行数据安全保障义务研究——以企业报送数据为视角[J].人民检察，2023(11)：20-24.

[9]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(02)：28-41.

基金项目：

青海民族大学创新项目，项目名称：数据交易平台安全保障义务的类型化研究，项目编号：04M2024142。

作者简介：

李向阳(1999－)，男，汉族，山西临汾人，硕士研究生，青海民族大学法学学院，研究方向：民商法。