Open Journal of Legal Science 法学, 2025, 13(5), 884-890
Published Online May 2025 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2025.135126

Hans汉斯

数据交易场所监管义务及归责分析

侯林宝

南京信息工程大学法学与公共管理学院，江苏 南京

收稿日期：2025年4月2日；录用日期：2025年4月11日；发布日期：2025年5月16日

摘　要

本文旨在探究数据交易场所监管义务的刑法介入正当性及归责路径，以解决当前数据交易市场快速发展与刑事规制滞后间的制度张力。通过比较法分析国外“看门人”责任制度演进，结合我国《数据安全法》《刑法修正案之(九)》等规范体系，系统论证数据交易场所监管义务的法理基础与实践逻辑。数据交易场所的监管义务源于“看门人”理论的发展完善、数据交易场所的职能定位及内部技术控制力；在归责路径上，根据不作为形态差异构建“单独责任－共同责任－帮助行为正犯化”的层次化刑事归责体系。同时，在数据交易场所不履行监管义务的刑事责任认定上，需要以“功能性法秩序统一”原理整合行刑责任边界，坚持“动态平衡与刑行协同”的原则，为数据要素市场化改革提供刑事法治保障。

关键词

数据交易场所，义务，刑事责任

Analysis of Regulatory Obligations and Liability in Data Trading Venues

Linbao Hou

School of Law and Public Administration, Nanjing University of Information Science and Technology, Nanjing Jiangsu

Received: Apr. 2nd, 2025; accepted: Apr. 11th, 2025; published: May 16th, 2025

Abstract

This paper aims to explore the legitimacy of criminal law intervention in the regulatory obligations of data trading venues and the imputation path, so as to address the institutional tension between the rapid development of the current data trading market and the lagging criminal regulation. Through a comparative legal analysis of the evolution of the “gatekeeper” liability system abroad and in combination with China’s legal norm system, this paper systematically demonstrates the jurisprudential basis and practical logic of the regulatory obligations of data trading venues. The

文章引用: 侯林宝. 数据交易场所监管义务及归责分析[J]. 法学, 2025, 13(5): 884-890.
DOI: 10.12677/ojls.2025.135126

regulatory obligations of data trading venues stem from the development and improvement of the "gatekeeper" theory, the functional positioning of data trading venues, and their internal technical control capabilities. In terms of the imputation path, a hierarchical criminal imputation system of "individual liability-joint liability-principal offenderization of assisting acts" is constructed based on the differences in the forms of omission. At the same time, in the determination of the criminal liability of data trading venues for failing to fulfill their regulatory obligations, it is believed that the principle of "functional legal order unity" is needed to integrate the boundaries of administrative and criminal responsibilities, and the principles of "dynamic balance and coordination between criminal and administrative actions" should be adhered to, so as to provide criminal legal protection for the market-oriented reform of data factors.

Keywords

Data Trading Venues, Obligations, Criminal Liability

1. 引言

当前，我国数据交易市场正处于蓬勃发展的关键时期，市场规模与政策环境、技术驱动与交易模式创新共同推动着行业发展壮大。2022 年 3 月，中共中央、国务院发布《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：要“加快培育统一的技术和数据市场”[1]，随后，全国各地纷纷加快了数据交易场所的建设，各级行政法规陆续颁布实施。截止 2024 年 12 月，全国主要数据交易场所已超 65 家，全国数据市场交易规模超 1600 亿元，同比增长 30%以上，其中场内市场数据交易(含备案交易)规模预计超 300 亿元，同比实现翻番[2]。

随着数据交易规模的不断扩大，数据交易场所的监管问题也日益严峻。数据泄露、非法交易等事件频发，给国家、企业和个人带来了巨大损失。在此背景下，我国积极推进数据安全相关立法工作。《中华人民共和国数据安全法》(以下简称《数据安全法》)《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)相继出台，确立了数据交易场所的监管地位。《数据安全法》第 33 条规定，“从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录”，《个人信息保护法》也对数据交易场所在个人信息保护方面的责任提出了更高要求。然而，这些法律法规仅原则性地规定了数据交易场所的监管义务，对于其刑事责任的边界并未明确界定。在司法实践中，对于数据交易场所的某些违规行为，行政部门往往采取严厉的行政处罚措施，而刑事追责却相对缺位。中国司法大数据研究院《2020~2022 年网络与数据犯罪司法统计报告》显示：2020~2022 年数据安全刑事案件年均立案数：487 件；同期数据安全行政处罚案件年均数：8236 件；行刑案件转化率：5.9%，凸显二元标准导致的治理断层。这不仅影响了法律的权威性和公正性，也不利于数据交易市场的健康有序发展。基于此，本文通过对数据交易场所的监管义务和刑事责任分析，为刑法介入规制交易场所不履行监管义务的行为奠定基础。

2. 数据交易场所监管义务的正当性

2.1. “看门人”理论发展的具体体现

早期比较法实践中，网络服务平台的法律地位长期受“技术通道理论”支配，主张其仅承担信息传

输的中介职能，对用户行为保持技术中立立场[3]。该理论契合互联网初期平台自动化处理交易、不干预具体内容的运营特征，深刻影响欧美立法，典型如美国确立的避风港规则体系——平台在收到侵权通知后及时采取删除、屏蔽等措施即可免责，侵权发现与举证责任由权利人承担[4]。例外情形限于“红旗规则”适用，即当侵权行为如“飘扬的红旗”般显著时(如盗版影视资源批量传播)，平台不得以不知情为由推诿责任[5]。

随着算法推荐、数据画像等技术的深度应用，网络服务平台的功能发生根本性转变。其通过内容审核算法、用户行为分析系统等技术手段实质控制信息流动，已突破单纯技术通道的被动角色，演变为网络空间的“架构管理者”。这种技术控制力的强化催生了责任范式的革新：克拉克曼(Kraakman)提出的“守门人责任理论”被引入网络治理领域，主张平台因掌握风险防控的技术优势与信息特权，应当承担主动审查违法内容的义务[6]。

立法实践呈现三大转向：其一，德国 2017 年《网络执行法》要求社交平台 24 小时内处理显见违法信息，否则面临高额罚款[7]；其二，澳大利亚 2019 年立法规定平台对暴力内容未履行及时报告义务将承担刑事责任[8]；其三，欧盟《数字服务法》创设“看门人”制度，要求超大型平台建立非法内容主动监测机制并发布年度合规报告[9]。此类规则突破避风港框架，将平台责任从被动响应升级为主动防控。

我国刑事立法同步回应此趋势，《刑法修正案(九)》增设的拒不履行信息网络安全管理义务罪，将平台未建立内容审核机制、未处置违法信息等行为纳入规制范畴。该罪名的设立体现“义务犯”理论内核——平台因占据网络生态治理的关键节点，需承担与其技术能力相匹配的作为义务。这种责任扩张既源于平台对信息流动的实质控制力，也反映数字经济时代风险分配机制的重构需求。

2.2. 数据交易场所职能定位的应然要求

数据交易场所作为数据要素流通的核心枢纽，已初步形成兼具“准公权力”属性与市场化功能的运行架构，承担维护交易秩序、防范系统性风险的公共职能[10]。

《数据二十条》中明确要求：“突出国家级数据交易场所合规监管和基础服务功能，强化其公共属性和公益定位”。其虽非数据危险源的直接开启者，但作为场内交易的“中继站”与“仓库”，凭借技术优势(如隐私计算、区块链存证)、组织能力(如合规团队配置)及规模化数据沉淀，成为风险防控的第一接触者与最佳控制主体，背负着“数据安全看门人”的社会期待[11]。依循危险控制理论，数据交易场所具有防控系统性风险的技术能力与信息优势，理应担负起监管义务。《数据二十条》通过“所商分离”制度设计，将数据交易场所职能限定为交易场所服务(如信息披露、资金结算)，而数据清洗、合规评估等衍生服务剥离至专业服务商，避免其因“既当运动员又当裁判员”弱化监管中立性[12]。与此同时，数据交易场所兼具监督保证人(审核数据来源合法性)与保护保证人(保障交易安全与隐私)双重身份，其公益服务机构定位为承担第三方监管义务提供了合法性基础，形成政府监管与市场自治协同的风险治理格局[13]。

2.3. 数据交易场所内部控制力的现实可能

控制力的本质溯源在于数据交易场所作为“风险第一接触者”的时空优先性。相较于政府监管的后端追责，交易所可在数据脱离存储介质的初始阶段即介入风险处置(实证研究表明其响应效率较传统监管提升 87% [14])。这种控制力源自技术路径的迭代升级与组织资源的协同配置，最终形成“以控制力界定责任边界”的新型交易风险防范逻辑。

一方面，通过技术架构的底层治理权来实现。数据交易场所通过代码规则对数据流通秩序进行系统性重塑，印证了莱斯格(Lessig)提出的“代码即法律”理论范式在数字治理领域的延展性[15]。基于隐私计算(联邦学习、多方安全计算)、区块链分布式账本及 AI 动态监测等技术集成，构建起多维风险防控体系，

例如：通过实时数据流分析识别异常交易行为(如非法跨境传输、敏感字段泄露)，依托智能合约自动执行风险处置协议(如交易熔断、权限冻结)。典型案例可见北京国际大数据交易场所自主研发的 IDeX 系统，其通过隐私计算与区块链技术耦合，构建“数据可用不可见”的精细化管控机制，实现数据流动利用与风险管控的平衡[16]。

另一方面，通过结构化制度创新来实现。具体表现为：在交易规则层面确立“不合规不挂牌”原则，通过《数据资产合规入表手册》等标准填补法律真空[17]，在合规工具层面设计多层级审核机制，运用联邦学习沙箱等技术将合规要求嵌入交易流程[18]。贵阳大数据交易场所试点的数据“三权分置”制度即体现此逻辑，其通过确权规则创新实现数据持有权、使用权与收益权的结构性分离[19]。同时，数据交易场所对存储数据的访问权限设置也体现了其控制权，只有经过数据交易场所授权的程序或人员才能访问特定数据。

当且仅当特定主体同时具备技术防控的物质基础与组织规范的制度能力时，法律设定的监管义务方可能从“规范应然”转化为“实践实然”，数据交易场所基于上述技术和规则，体现了对数据的深度控制，被赋予监管义务也就在情理之中。

3. 数据交易场所监管义务的来源

数据交易场所的监管义务来源具有法秩序统一性下的多维构造：刑法层面，其义务根植于“实质作为义务说”所主张的危险源控制责任，即数据交易场所因技术支配地位对数据交易风险具有排他性管控能力，产生防止违法交易的保证人义务；行政法层面，《数据安全法》第 33 条设定合规基准，要求履行数据来源审查、身份核验等强制性义务；行业规则与内控机制则构成社会期待的具体化，通过《数据交易服务安全要求》[20]与 ISO 合规管理体系将技术伦理转化为可归责的注意义务。周光权教授提出的“功能性法秩序统一”[21]原理为此提供整合框架：刑事责任的认定需以行政义务违反为前提，并以行业自治水平与内控实效为归责梯度，实现规范协同与责任限度的动态平衡。

3.1. 法律规范的强制性义务

数据交易场所的监管义务首先源于国家立法的直接规定。在行政法层面，《数据安全法》第 33 条明确要求数据交易中介机构审核数据来源合法性并留存交易记录；《网络安全法》第 37 条对关键信息基础设施运营者的数据跨境传输义务作出限制；设定数据分类分级与加密去标识化等合规基线。在刑法层面，《刑法修正案(九)》增设的拒不履行信息网络安全管理义务罪(第 286 条之一)，将交易所未履行网络安全管控等义务导致严重后果的行为纳入刑事追责范围；帮助信息网络犯罪活动罪(第 287 条之二)则对交易所明知数据用途非法仍提供技术支持的行为施以刑罚威慑。

3.2. 行业主管部门的行政监管要求

国家网信办、工信部及地方数据管理局通过规范性文件细化监管要求。例如，国家发改委《数据要素市场化配置改革方案》要求省级数据交易场所完成备案登记，并定期提交跨境数据流通风险评估报告[22]。地方实践中，上海数据交易场所依据上海市经信委《数据交易场所管理办法》，实施数商分级认证制度，未通过年审的机构将限制交易权限[23]。此类行政规制通过许可、备案、检查等手段，将法律原则转化为可操作的合规要求。贵州省 2024 年实施的《数据流通交易促进条例》创新性地赋予“违规交易熔断机制”，要求其对涉敏数据交易实施实时阻断[24]。

3.3. 行业标准与内部合规规则的技术性约束

行业技术标准与交易所内部规则构成监管义务的第三重来源。《数据交易服务安全要求》规定交易

所需采用区块链存证等技术确保交易可追溯[20]；国家标准《数据分类分级指南》细化数据敏感等级判定规则，要求交易所建立差异化管控策略[25]。例如，深圳数据交易场所在其《交易规则》中明确规定，对参与交易的数据进行合法性、合规性审查，确保数据来源合法、交易目的正当[26]。

4. 数据交易场所不履行监管义务的归责路径

数据交易场所不履行监管义务的刑事可罚性认定，须以犯罪类型的精准界分为前置条件。其正当性基础在于，判断交易所是否构成不作为犯罪时，需综合考量义务来源类型(如刑法义务和内部交易规则)、技术架构特性(如中心化存储系统与分布式账本的功能差异)以及危害关联强度(如对非法交易行为的直接促成或间接放任)等变量因素的差异性影响，才能做到对数据交易场所的不作为行为合理入罪，并实现妥当归责。

4.1. 不同参与形态下的规责路径

按照犯罪参与的不同形态分为独立归责和共同归责模式；按照主观通谋和参与程度，共同责任模式可被进一步区分为共同犯罪模式和帮助行为正犯化模式。

4.1.1. 单独责任模式下的不履行监管义务犯罪

数据交易场所作为独立责任主体未履行法定监管义务，直接导致法益侵害结果的，构成单独不作为犯罪。其归责逻辑需满足三重要件：义务来源法定性(如《数据安全法》第 33 条规定的义务)、履行能力客观性(如是否部署符合国家标准的技术措施)、因果关系直接性(如未审核数据来源导致非法交易扩散)。具体罪名判定需涵摄于犯罪构成要件：

从危害的法益类型来看，既包括网络秩序等抽象内容，也涉及网络安全、个人信息安全以及公民财产安全等具象法益；从可能构罪的罪名看，单独责任模式下，数据交易场所成立的不作为犯罪具有一般化特征，刑事归责路径多指向拒不履行网络安全管理义务罪、帮助信息网络犯罪活动罪等定型化罪刑规范。

4.1.2. 共同责任模式下的不履行监管义务犯罪

当数据交易场所与数据卖方、买方等主体存在明示或默示通谋，以不作为形式参与犯罪活动的，可能成立共同犯罪。从分工角度看，数据交易场所一般起到帮助作用，这是典型的共同犯罪模式。例如，交易所明知某企业通过 API (Application Programming Interface)接口非法爬取公民信息，却未关闭其接入权限，构成侵犯公民个人信息罪的帮助犯。但是，在犯罪成立与科处刑罚方面，共同犯罪的认定需遵循“共犯从属性原则”——正犯行为需满足构成要件该当性。日本学者西田典之强调：“不作为帮助犯的成立需以作为义务与正犯行为的高度关联为前提”，即交易所的不作为须实质促进正犯目的实现[27]。

4.1.3. 帮助行为正犯化模式下的不履行监管义务犯罪

数据交易场所的不履行监管义务与数据犯罪产业化、链条化趋势深度嵌合，其不作为的技术特征呈现多对多关联性(单一监管漏洞被多个犯罪团伙利用)、技术中立性掩盖犯意(交易所与具体犯罪人无直接意思联络)等特性。依据传统共犯理论，此类行为的违法性与有责性难以有效评价，故需通过“帮助行为正犯化”模式实现独立归责。基于帮助行为理论的归责独立性原理，技术辅助主体的刑事可罚性判定突破传统共犯从属性框架，形成帮助行为正犯化归责范式。具象化于数据交易场景，当场所存在主观认知可能性时，未通过技术介入阻断违法数据流动，在技术性中立表象下实质构成犯罪行为的协同促进要件，从而引发法益侵害的构成要件该当性评价。

在此模式下，数据交易场所的定罪与量刑独立于具体犯罪实施者，体现“技术控制者责任优先”的

刑事政策导向。

4.2. 义务模式区分后的归责路径

根据监管义务的来源不同(法定义务、实质义务)，可以将数据交易场所不履行监管义务的违法行为区分为纯正的不作为犯和不纯正的不作为犯。

4.2.1. 纯正不作为犯

以法定监管义务为核心构成要件，义务来源于其前置法《数据安全法》《网络安全法》《个人信息保护法》中关于数据交易场所各类监管义务，典型如《刑法》第 286 条之一“拒不履行信息网络安全管理义务罪”。必须同时满足四重要件：比如，数据交易场所违反《数据安全法》第 33 条“审核交易双方的身份，并留存审核、交易记录”的规定，客观上造成重大法益侵害后果(如导致核心数据泄露或引发系统性风险)，主观上存在明知且放任的故意，如经监管部门程序上的责令改正后仍不履行监管义务，将严格依据《刑法》第 286 条之一归责。陈兴良教授主张，此类犯罪的认定须恪守形式解释论，避免通过实质解释扩张义务范围，以维护罪刑法定原则的刚性约束[28]。

4.2.2. 不纯正不作为犯

其实质监管义务为核心构成要件，其监管义务来源超越成文法的形式规定，涵盖技术控制能力、业务风险关联等实质要素。数据交易场所犯罪成立需通过“等价性原则”验证不作为与作为犯的法益侵害相当性[29]：若数据交易场所对危险源是否具有排他性支配地位(如独占数据流通的技术控制权)，其未履行匿名化、风险监测等义务导致危害结果，则被认为与积极实施犯罪具有等价的可罚性。张明楷教授强调，等价性判断应聚焦于不作为对结果的因果贡献强度，如交易所未屏蔽非法 API 接口致使千人级信息泄露，其不作为的辐射性危害等同于直接提供犯罪工具。

5. 结语

本文针对当前刑法规制数据交易场所的情况，论述了数据交易场所监管义务的正当性基础、监管义务的来源及不履行监管义务的归责路径，为司法实践中准确做到合理入罪，并实现妥当归责提高了理论研究的方向。数字时代的刑事法治演进中，各国立法与司法实践对数据交易场所的不作为刑事责任需要秉持审慎立场。这种克制源于对技术中立原则的尊重与数字经济发展规律的深刻认知——过度扩张数据交易场所责任将抑制技术创新活力，动摇数据交易产业的根基。刑法作为社会治理的最后手段，其介入需严格遵循“法益保护必要性与手段相当性”的双重检验：一方面，数据交易场所的监管责任范围应与其技术控制能力、风险预见可能性相匹配；另一方面，刑事归责须以实质化标准界定主观罪过，即对违法性认知的“明确知道”或“应知而放任”。此种限制性解释路径既符合期待可能性理论对责任主体的合理期待，亦彰显现代刑法在数字治理中的谦抑品格，为技术创新与公共安全的价值平衡提供制度保障。

参考文献

[1] 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[J]. 中华人民共和国国务院公报, 2023(1): 28-33.

[2] 严赋憬. 2024 年全国数据市场交易规模预计超 1600 亿元[EB/OL]. 中国政府网, 2025-01-11. https://www.gov.cn/lianbo/bumen/202501/content_6997834.htm, 2025-03-15.

[3] 中国司法大数据研究院. 2020-2022 年网络与数据犯罪司法统计报告[R]. 北京: 中国司法大数据研究院, 2023: 12.

[4] United States District Court Cubby, Inc. v CompuServe Inc. (1991) 776 F Supp 135 (S D N Y 1991). https://lawjustiacom/cases/federal/district-courts/FSupp/776/135/1445354/

[5] US Government Publishing Office (2020) U S Copyright Office Section 512 of Title 17: A Report of the Register of

Copyrights. 45.

[6] 王迁. 网络服务提供者版权责任的守成与创新[J]. 法学研究, 2021(2): 89.

[7] Krakman, R.L. (1986) Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy. *Journal of Law & Economics*, **34**, 53-60.

[8] 德国联邦司法部. 网络执行法(NetzDG) [Z]. 柏林: 联邦法律公报, 2017: 3.

[9] 澳大利亚议会. 分享重大暴力内容刑法修正案[Z]. 堪培拉: 联邦立法登记处, 2019: 第 5 条.

[10] European Commission Digital Services Act: 2022/0295(COD) [Z]. 布鲁塞尔: 欧盟官方公报, 2022: Art. 13.

[11] 洪学军 关于加强数字法治建设的若干思考——以算法、数据、平台治理法治化为视角[J]. 法律适用, 2022(5): 140-148.

[12] 单勇. 数字看门人与超大平台的犯罪治理[J]. 法律科学(西北政法大学学报), 2022, 40(2): 74-88.

[13] 陈兵, 郭光坤. 国家级数据交易平台建设的法治方向及架构——以《数据二十条》为中心的解读[J]. 法治现代化研究, 2023, 7(6): 71-86.

[14] 熊丙万, 何娟. 论数据要素市场的基础制度体系[J]. 学术月刊, 2024, 56(1): 102-114.

[15] 中国信息通信研究院. 隐私计算技术与应用研究报告(2023) [J]. 数字经济研究, 2023, 4: 23.

[16] Lessig, L. (1999) Code: And Other Laws of Cyberspace. Basic Books, 89-112.

[17] 隐私计算: 让数据“可用不可见” [EB/OL]. 2023-04-10. https://www.zjwx.gov.cn/art/2023/4/10/art_1673571_58873053.html, 2024-10-15.

[18] 北京国际大数据交易场所. 数据资产合规入表操作手册(2024 版) [R]. 北京: 北京国际大数据交易场所, 2024: 15-18.

[19] 贵阳大数据交易场所. 数据产品定价机制研究报告[M]. 贵阳: 贵州科技出版社, 2023: 7.

[20] 全国信息安全标准化技术委员会(SAC/TC 260). 信息安全技术 数据交易服务安全要求: GB/T 37932-2 [EB/OL]. https://www.ictbda.com/upload/default/20231214/f66b1ce21db2c8b8ee5aff79e2a271bf.pdf, 2025-02-01.

[21] 周光权. 法秩序统一性原理的实践展开[J]. 清华法学, 2021(4): 15.

[22] 国家发展和改革委员会. 数据要素市场化配置改革方案[Z]. 2022-06-22: 第 15 条.

[23] 上海市经济和信息化委员会. 上海市数据交易场所管理办法[Z]. 2023-03-01: 第 12 条.

[24] 贵州省数据流通交易促进条例[N]. 贵州日报, 2024-08-05(008).

[25] 全国网络安全标准化技术委员会. GB/T 43697-2024 数据安全技术 数据分类分级规则[S]. 北京: 中国标准出版社, 2024.

[26] 北京市市场监督管理局. 数据分类分级指南: DB11/T 1948-2021 [S]. 北京: 中国标准出版社, 2021.

[27] 西田典之. 刑法总论[M]. 刘明祥, 王昭武, 译. 北京: 中国人民大学出版社, 2020: 189.

[28] 陈兴良. 教义刑法学[M]. 北京: 中国人民大学出版社, 2017: 809.

[29] 黎宏. 排他支配设定: 不真正不作为犯论的困境与出路[J]. 中外法学, 2014, 26(6): 1573-1595.