数据交易安全港白皮书

Safe Harbor for Data Exchange White Paper

北京大学法学院

上海数据交易所

版权声明

编写组（排名不分先后）

吴蔽余、戴昕、朱恬逸、吴峻

编写单位（排名不分先后）

北京大学法学院

上海数据交易所

目录
Contents

报告要点

“安全港规则”（译自英文“safe harbor rules”，也常被译作“避风港规则”）。目前在我国，包括《个人信息保护法》《数据安全法》《网络安全法》等在内的数据领域基础性法律，已建构出一个强调风险预防、损害问责的原则性制度框架。但由于法律中的许多规定较为笼统，市场主体对更高法律确定性和责任可预期性的需求尚待满足。

安全港规则旨在为数据交易市场主体提供一个清晰、明确的合规路径，在提升数据交易活动自身安全性的同时，也为交易提供相应的法律保障，从而促进交易规模的扩大、体量的释放和活跃度的提升。具体而言，安全港规则将以数据交易所场内交易的安全保障和技术服务条件为基础，设置更为明确的市场主体合规路径，为后者提供可操作的合规要求和合规方案，从而既降低交易自身带来的数据风险，又为交易主体带来更为确定的合规预期。根据目前的设想，数据交易安全港规则包含“2+2”框架。首先，“合规技术”与“法律规则”相结合，不仅将使用区块链存证、AI 智能检测、隐私计算等合规技术手段确保数据交易安全可信，也将引入合规、透明、可操作的法律规则，明确安全港的适用条件、免责后果。其次，“主动投入”与“预期免责”相结合，安全港要求企业满足特定的资质、合规条件，并进行可信披露，主动投入相关成本进行“驶入”安全港的动作，从而获得免责预期：在监管部门的授权下、在数据交易场所建构的可信空间内开展交易，可以避免因为事先未曾预料的风险而事后被追责。

安全港规则并不意味着放任市场自由。对于“驶入”安全港的数据交易活动，权威机关仍然有责任和权力对其进行监管。权威机关还可以通过定期审核、随机抽查等方式，确保市场主体真正遵循安全港规则，从而确保数据交易的合规性、透明性和公正性。安全港规则在交易所以集中、透明的方式施行，会更有助于规则倡导的合规交易模式产生溢出效应。相对规范、安全的场内数据交易模式，基于披露机制，可对场外交易产生引导作用，成为更大范围内市场主体在进行数据交易活动时协调行为的聚焦点。即使市场主体因种种原因，不选择或无法选择进行场内交易，也可参照场内交易所适用的安全港规则的要求规划自身行为。这种参照不仅对自行探索合规的企业有价值，对整体层面的风险控制也有价值。

上海数据交易所针对案例中展示的市场需求和痛点，建构了包含下列具体措施的数据交易安全港：其一，智能接入，基于企业主动申请和特定场景（特别是创新容错场景）主动接入，对流通交易数据进行智能分类分级、按需接入安全港。其二，可信交易，在合规技术保障下，在监管部门授权、监管、验收等流程下按照特殊规则在港内交易。其三，风险响应，在安全港港内交易，如果存在侵权投诉、情势变更等风险警示情形，及时启动中止交易、信息披露等响应机制，并保障市场主体取得与前期合规投入、创新容错政策相适应的责任豁免。其四，反馈迭代，成立数据交易合规委员会，对安全港规则进行动态调整，并与行业主管部门、监管部门、司法部门进行定期沟通反馈，根据安全港运行情况和需求情况迭代完善相应规则。

《数据交易安全港白皮书》（“《白皮书》”）开创性地提出应运用“安全港规则”这一制度工具，提升交易主体参与数据交易活动的积极性，释放数据交易动能，并更为高效、平衡地推动数据要素配置过程中安全保障和价值创造两大政策目标的实现。在数据交易的场景中，安全港规则以一套“2+2”框架为主要内容，即“合规技术”与“法律规则”相结合，“主动投入”与“预期免责”相结合。将数据交易所等专业、可信、高效的中介交易场景探索打造成为安全港规则的核心制度适用场景，不但有助于提升数据交易活动的整体安全性，而且有助于市场主体有效管理其在参与创新性、具有高价值产出的数据交易活动时面临的法律风险，降低其不确定性，从而提升市场主体参与交易的积极性和整体交易活跃度。

《白皮书》将在检视当前国内和国际数据交易市场现状的基础上，分析数据交易市场进一步发展所面临的与竞争环境和法律环境有关的核心障碍与挑战。在各方积极寻求数据交易进一步破局的大背景下，应当看到，以上海数据交易所为代表的数据交易中介平台类机构，其提出和开展的多项数据交易安全合规探索，均体现出交易所场内交易在兼顾安全性和效率性方面所具有的独特优势。据此，结合对安全港规则一般制度原理的阐释，《白皮书》提出，安全港规则是将数据交易实践向前推进的一种可行思路，而数据交易所应被建设成为安全港规则的核心制度适用场景。对于具备相应技术和服务条件，有能力高效保障场内交易相对场外交易安全优势的数据交易所，有关部门应考虑在政策层面为其中的场内交易活动提供基于安全港规则的合规效力，从而促进更大规模的数据交易活动以更安全的方式开展，使得数据要素在流通中获得更高的整体配置效率。

一、国内外数据交易实践简介

1.1 国外数据交易实践简介

数据交易并非互联网时代的独有现象，它的根源追溯到远早于数字化浪潮的时代。实际上，数据的交换和利用在商业活动中一直占据着核心地位，无论是古代商人通过手稿记录和交换贸易信息，还是工业时代通过统计数据优化生产流程，[1]数据交易始终是推动知识发展和经济增长的重要力量。然而，互联网时代的到来加速了数据交易的速度与规模，使其成为日常商业活动中不可或缺的一部分。

随着科技的不断发展，数据交易的概念和实践也经历了深刻的变革。特别是在 1970 年代左右，随着电子技术的普及，海外特别是美国的数据交易开始步入电子化时代，这一变化使得数据交易的模式和效率都发生了质的飞跃。具体来看，美国的数据交易模式主要分为三种类型，各自有着不同的运作机制和参与主体。

[1] 由于商业需求的存在，即便当时还没有如今这般便利的数字技术，美国也已经开始了实质意义上的数据交易。伴随着独立战争与南北战争，美国近代工业初步形成，工厂产值在 1810 至 1860 年间增长了 10 倍；在这一过程中，美国企业在商业活动中越发需要更准确的信息以帮助自己完成商业决策，这便促生了纽约布鲁克林在 1860 年出现了第一家信用局，开启了美国数据经济市场的时代并在 1956 年促成了基于数据的 FICO 信用分的诞生。数据经纪人（data broker）在这个过程中起到了重要作用。数据经纪人通过与各类数据提供方的合作，负责收集、整合和维护大量的个人和企业数据。他们的职责涵盖数据的获取、处理和管理，以确保数据的完整性和准确性。同时，数据经纪人还与数据需求方合作，如金融机构和保险公司，为他们提供可靠的数据资源。通过数据交易的方式，数据经纪人将数据提供给 FICO 体系，用于信用评分和风险分析。

第一种是 C2B 分销模式，这种模式下的数据平台直接与消费者打交道，用户主动向平台提供自己的个人数据。而作为交换，平台会提供商品、服务、现金回报，或者是优惠、折扣和积分等形式的利益，从而吸引用户分享自己的数据。

第二种是 B2B 集中销售模式，这里的数据平台起到连接数据提供方和数据购买方的桥梁作用。这一模式更接近于数据市场的概念，类似于中国对数据交易所的构想。在这个模式中，平台为双方提供撮合服务，确保交易的正规化和合规化。参与方必须通过平台的审核，他们可以自主定价，设定销售期限和使用条件，而平台则负责确保交易的顺畅和安全。

第三种数字经纪人模式是对前一模式的扩展。中介性数据平台在这里充当数据经纪的角色，它们从个人用户那里收集数据，并将这些数据转让给其他企业使用。这种模式的运作涉及复杂的数据流转和处理过程，要求平台在确保数据质量、保护个人隐私以及遵守相关法律法规等方面有着更高的标准和能力。

通过这三种模式，不难看出，数据平台在美国数据交易中扮演着极为重要的角色。他们不仅是数据交易的促成者，更是维护交易安全、保护交易主体数据相关利益、公民个体数据隐私权益乃至国家安全等一般社会利益的关键力量。随着数字经济的不断发展，这些模式的创新和完善将对全球的数据交易实践产生深远的影响。

在美国的数据交易实践中，虽然也有学者曾经主张建立全国的数据交易市场来进行个人数据的公开交易，[2]但是美国的数据交易实践的主流，仍然是数据经纪人（data broker）模式。这一模式的核心在于数据经纪公司的运作，这些公司精于从各种途径搜集和加工用户数据，并将其转化为商业智能或营销工具出售给企业。美国联邦贸易委员会对数据经纪人的定义凸显了这些机构在现代商业中的角色——它们是搭建企业与消费者之间桥梁的专家，但同时也引发了一系列隐私与监管的问题。[3]

在美国，政府对数据经纪人的监管相对宽松，他们在处理消费者数据时的不透明做法常常让消费者在交易中感到处于劣势，且在事后很难找到保护自己利益的有效途径。而在中国，以广东省 2022 年 5 月的试点为代表，虽然数据经纪人的概念和实践也在蓬勃发展，但在市场规模和成熟度方面与美国仍有一段距离。[4]

综上所述，数据经纪人模式在美国已经成为数据交易的一个标志性实践，而这一模式的影响力和问题也引起了全球的关注和思考。对于中国来说，借鉴和适应这一模式，同时考虑本土的法律、文化和市场特点，对于建立更加成熟和规范的数据交易市场至关重要。

[2] See Kenneth C. Laudon, *Markets and Privacy*, 39(9) communication of the ACM 92, 99-100 (1996).

[3] See Justin Sherman, *Data Broker Registries in Bills: the ADPPA and the DELETE Act*, Lawfare, Jun. 6, 2023, <https://www.lawfaremedia.org/article/data-broker-registries-in-bills-the-adppa-and-the-delete-act> accessed Nov. 17, 2023.

[4] 参见刘珊：《全国首批“数据经纪人”在广州海珠诞生 3 家企业入选，涉及电力行业、电子商务、金融等领域》，载《南方日报》2020 年 5 月 28 日，第 4 版。

在全球范围内，数据交易的模式和理念正处在快速演变之中。除了美国所倡导的数据经纪人模式，欧盟也在探索一条不同的路径，那就是创建一个欧洲共同数据空间。这一宏伟的构想意在打造一个跨领域、统一的欧洲数据市场，其宗旨与数据交易所有着异曲同工之妙。[5]

欧盟委员会不仅在理念上提出了这一计划，更通过了一系列的立法措施以支持其实施。例如，欧盟《数据治理法》（European Data Governance Act）于 2022 年 6 月 23 日通过，于 2023 年 9 月 24 日适用于欧盟各成员国；而后，欧洲议会于 2023 年 11 月 9 日通过《数字法案》（EU Data Act），该法案将在完成余下程序后生效。上述立法行动，均体现了欧盟对于包括数据交易在内的数据领域的重视，或将在后续进一步影响数据交易市场的经营。尽管欧洲共同数据空间还处于起步阶段，还未展现出明确的成果，但其目标十分明确：促进数据共享和流通，以此加快欧洲数字经济的发展，为企业和创新者开拓更广阔的市场和提供更多的机遇。

在这一框架下，欧洲共同数据空间计划为各行各业的数据使用者提供一个安全、可信的平台，从而更有效地管理和利用数据资源。这一平台将成为加速跨国合作、激发技术革新的重要力量，并为欧洲的数字化转型铺平道路。

当然，这个雄心勃勃的计划并非没有挑战。在推进过程中，欧盟必须应对众多复杂的法律、隐私以及安全问题。实现这一计划需要欧盟委员会、各成员国以及企业和其他利益相关者之间的紧密合作，共同确保数据的安全和个人隐私得到严格保护。

虽然欧洲共同数据空间的实际成果还有待观察，但这一进程无疑彰显了欧盟对于数据经济的高度重视和对未来发展的明确愿景。随着技术的不断创新和全球数字化转型的加速，欧洲共同数据空间不仅有潜力为欧洲数字经济带来新的活力，也为全球数据交易模式的多样化和发展提供了新的视角和可能性。

在审视全球数据交易的不同模式时，可以注意到美国和欧盟各自的做法提供了有益的参考。美国的数据经纪人模式强调了市场的自由流动和效率，而欧盟的共同数据空间则侧重于打造安全、规范的跨国数据交易环境。这两种做法都在各自的法律和文化背景下发挥了作用，并为世界其他国家，包括中国，提供了值得借鉴的经验。

然而，这些国际经验并不能简单地移植到中国。中国在数据交易方面的发展必须立足于本国的经济结构、法律体系和市场环境。中国需要根据自己的国情，借鉴国外的先进做法，同时结合本土的实际情况，来构建适合自己的数据交易模式。

---

[5] 具体到数据市场/平台，境外市场的主要参与者包括 Dawex、Datarade 等公司。Dawex 是一家于 2015 年成立的科技公司，其总部位于法国，业务拓展至欧洲、亚洲、北美和中东。Dawex 的主要业务是为各个公司/集团构建自己的数据交换平台（Data Exchange Platform）提供技术支持，例如 Dawex 在 2023 年 9 月 25 日推出的企业数据中心解决方案（Corporate Data Hub solution）即是旨在帮助集团公司内部数据孤岛、促进组织内数据流通。[5]在 Dawex 积极运营的日本，也由私营部门牵头成立了依托于 Dawex 数据交换技术的日本数据交换公司（JDEX），该日本公司旨在创建一个跨越行业、学术界和政府的大型数据交易社区，为促进跨行业和跨境数据交换环境作出贡献。[5]Datarade 则并非单纯的技术提供者，其市场平台整合了超过 2000 家数据提供商，是全球最大的数据交易平台；Datarade 的多样化交易环境促进了全球的数据交易，买家有机会找到更合适的数据，数据商则可以通过 Datarade 的平台将数据交易到全球各地。[5]在这个意义上 Datarade 类似于淘宝等 B2C 的交易平台，只是其交易标的从日常用品变成了数据——Datarade 给了买家与卖家交互的场所，并同时提供了买家对卖家的评价机制，致力于打破数据交易市场的不透明。

对于中国来说，重要的是要找到一个既能保护个人隐私和数据安全，又能促进数据流通和经济创新的平衡点。这可能意味着需要制定更加创新性的法律规范，确立更加严格的数据管理框架，并建设透明、可信的数据交易场所。

1.2 我国数据交易实践简介

追溯我国过去二十余年中不同种类的数据和信息使用方式，也能看到和海外数据交易实践相似的发展路径——数据和信息交换行为一直存在于平台企业构建的市场中，但直到近些年才凝结为“数据交易”这一观念。

当前，数据已经成为数字经济时代的基础性资源、重要生产力和关键生产要素。总书记强调，数据基础制度建设事关国家发展和安全大局，要统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系。[6]其中，建立合规高效、场内外结合的数据要素流通和交易制度成为了主要的关切。深入理解国家关于要素市场化配置的政策就不难发现，该政策的目标是培育和建立数据要素市场，且对相关举措有比较明确的看法和指引：首先是利用公共机关的地位解决数据供给侧问题（即开放共享），其次是通过标准化等措施提升数据价值，最后是加强资源流通和整合，加强市场基础设施（如数据资产评估、登记结算、交易撮合、争议仲裁）。[7]

可见，若要释放数据的全部价值，就需要让数据在全社会流动起来。目前无论是学术界还是实务界，基本能够对数据需要自由流通、扩大共享达成共识。人们已经逐渐认识到，不同于传统的生产要素，数据具有非排他性、非竞争性的特点，而数据实现价值又要以大规模聚合（aggregation）为前提。例如，亚马逊在进行产品销售预测时，随着积累的数据周数增加，预测的准确性也随之提升，而在机器学习领域，以提高汽车安全性的算法为例，当算法训练所用的数据量更大时，它能够执行更复杂的任务（如自动驾驶），这说明在数据量大的情况下，技术解决方案的质量和效能会显著提高。总的来说，无论是在商业预测、技术创新还是企业发展等方面，数据的大规模聚合都是实现其最大价值的关键。[8]

由此，如果能让数据在全社会的范围内流动起来，就可以让数据在不同主体的开发下，被激发各个维度的价值潜力。[9]因此，建立成熟的数据要素市场，被认为是刻不容缓的要事，[10]不仅因为我国的数据产量从

[6] 陆娅楠：《构建数据基础制度　更好发挥数据要素作用——国家发展改革委负责同志答记者问》，http://cpc.people.com.cn/n1/2022/1220/c64387-32590046.html

[7] 见国务院发布的《要素市场化配置综合改革试点总体方案》，载中央人民政府网 http://www.gov.cn/zhengce/content/2022-01/06/content_5666681.htm。

[8] See Charles I. Jones and Christopher Tonetti, *“Nonrivalry and the Economics of Data”*, American Economic Review, Vol.110, No.9, 2020, p.2821.

[9] 唐郡：《数据基础制度奠基：淡化所有权，优先流通》，载微信公众号“财经五月花”，2022 年 10 月 8 日。

[10] 比如《广东省数据要素市场化配置改革白皮书》中指出，广东抢占发展先机，前瞻性、全局性、整体性推进数据要素市场化配置改革。参见广东省政务服务数据管理局网站，http://zfsg.gd.gov.cn/gkmlpt/content/4/4042/post_4042842.html#2589。也有学者明确提出这一观点。参见黄朝椿：《论基于供给侧的数据要素市场建设》，载《中国科学院院刊》2022 年第 10 期，第 1402-1409 页。

2017 年的 2.3ZB 增长至 2022 年的 8.1ZB，以占比 10.5%的规模位居世界第二，也是因为数据被视为深刻改变生产和生活的新型生产要素，是我国未来经济发展超越主要竞争对手的战略制高点。[11]

然而，即便数据的流动、共享、开放依然成为了热议的话题，但“专网林立”“信息孤岛”“数据烟囱”[12]才更能揭示真正的现实情况：尽管人人都知道数据只有流通起来才能被释放尽可能多的价值，但是企业或其他组织为了维持自己的竞争优势，并不会主动地拥抱数据共享和数据流动，反而是控制数据的获取和流动，甚至在特定数据产品市场实施的排除限制竞争。这是因为企业或其他组织可以利用数据优势提高产品质量或服务水平，从而保持较高的客户粘性并不断扩大市场规模，而规模效应的提升又会反向增强企业的数据优势，有利于形成市场进入壁垒，[13]因此，初创企业进入数据驱动型产品市场可能会面临较高的进入障碍，比如在搜索引擎与社交产品市场。[14]

观察当前的数据产业格局，可以发现无论是企业还是其他组织，都在积极地“圈地”，以牢固地控制自己的数据资源。“划地为王”的现象普遍存在，组织倾向于保护和内部利用其数据，而非轻易地分享或出售。因此，一个合理的推论是，如果政府能够在外部建立一个数据要素交易市场，并且这个市场能够提供足够的激励机制，那么它可能会吸引那些控制数据的企业和组织参与进来。如果这个市场能够确保数据出售方得到合理的报酬，同时也满足数据购买方的需求，那么它可能会促成一种互利共赢的局面。

因此，在2020 年3 月中共中央、国务院发布的《关于构建更加完善的要素市场化配置体制机制的意见》（以下简称“数据二十条”）首次提出了要加快培育数据要素市场之后，[15]通过建立数据要素市场来解决数据封闭的逻辑成为了主流。在实践中，全国各地迅速开启了一轮数据要素市场的建设，并将数据交易所或数据交易中心作为发展模式；在理论上，也有不少学者畅想数据交易市场也能像证券交易市场一样，发展出登记、尽调、评估、挂牌、交易、结算、交割、审计等一系列流程。[16]

尽管我国政府在政策和财政上都对数据交易所的建设投入了巨大的支持，期望通过数据交易所刺激企业在场内开展交易，但实际成效却并不如人意。尽管政策上的激励措施不断，交易所内的项目仍然难以聚集成有效的交易量。[17]近年来，虽然全国各地纷纷推动数据交易所或交易平台的建设，但那些已经投入使用的交

[11] 参见于施洋、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，第 2-12 页。

[12] 唐郡：《数据基础制度奠基：淡化所有权，优先流通》，载微信公众号“财经五月花”，2022 年 10 月 8 日。

[13] 参见梅夏英、王剑《“数据垄断”命题真伪争议的理论回应》，载《法学论坛》2021 年第 5 期，第 99-101 页。

[14] See Kerber,Wolfgang."Digital Markets,Data,and Privacy:Competition Law,Consumer Law and Data Protection",Journal of Intellectual Property Law & Practice 11.11 (2016):856-66.;Argenton,Cédric,and Jens Prüfer."Search Engine Competition With Network Externalities",Journal of Competition Law and Economics 8.1 (2012):73-105.

[15]《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》提出土地、劳动、资本、技术、数据五个要素领域的改革方向，其中针对数据要素,第一次明确了加快培育要素市场的发展方向,要求加强数据资源整合和安全保护。

[16] 参见范文仲：《完善数据要素基本制度 加快数据要素市场建设》，载《中国金融》2022 年第 1 期，第 14-17 页。

[17] 据统计，2020 年，交易所场内数据交易只占我国数据交易市场总规模的 4%。参见中国网络空间协会、温州市委网信办及南都大数据研究院：《布局与破局——2022 年中国数据交易实践趋势报告》，第 31 页，载道客巴巴网站 https://www.doc88.com/p-94087802708426.html，2023 年 1 月 2 日访问。

易所普遍面临着交易活跃度不高的窘境。这反映出，在数据交易所的建设上，还需更深入的市场研究和制度创新，以实现真正有益于企业和整个经济生态的发展。

尽管政府试图通过数据交易所提供一个正规化的交易环境，但实际上交易所的交易量和活跃度却远未达到预期。与此形成鲜明对比的是，场外交易正在如火如荼地进行着，它几乎已成为数据交易领域的主流方式。

数据交易所的最初设想，是希望将地下或黑市的非正式数据交易引入光明、规范的交易环境中，以实现数据流通的合法化和标准化。但现实情况却是，许多场外交易的参与者并没有太大的动力去适应交易所更为严格的标准和流程，特别是对于那些通常只涉及一次性交易的数据。[18]

这种现状反映出，尽管数据交易所在理论上提供了一个更加安全和透明的交易平台，但若不能提供足够的激励或降低交易成本，它们难以吸引那些已经习惯于场外交易的市场参与者。因此，如果数据交易所想要在未来的数据经济中扮演更重要的角色，就必须创新其服务方式和制度，提供真正能够吸引并满足市场参与者需求的解决方案。

在当前关于如何优化数据交易所的讨论中，一个关键的问题往往被忽视：交易主体为何持续对场内交易保持着谨慎甚至是回避的态度？讨论如何完善交易所的各种机制——包括定价、流通、信用和支付等[19]——固然重要，但这些讨论之前，必须首先理解交易主体的真实顾虑和需求。

事实上，仅仅通过建立一个数据交易平台，并不能自动地满足交易参与者的所有需求。如果要真正吸引交易主体走入交易所，更需要做的是站在交易主体的角度，深入挖掘交易主体的真实担忧，从而提供更为切实的解决方案。

因此，要想激活场内交易，需要重新定位数据交易所的角色和功能可能是更好的处理——这不仅仅是简单地复制互联网平台早期的逻辑和行为模式，而是基于对交易主体深层次需求的洞察，设计出更为精准的策略和规则。目前可能最需要先做的，是构建一个真正能激发交易热情的环境，这样交易主体才会被吸引进场，积极参与交易，从而让数据交易所真正发挥其应有的作用。

[18] 参见胡凌：《数据要素财产权的形成：从法律结构到市场结构》，载《东方法学》2022 年第 2 期，第 120-131 页。

[19] 有学者提出，数据交易所的重点在于思考如何通过公共机构的外部力量重新规制市场各类核心机制。参见陈越峰：《超越数据界权：数据处理的双重公法构造》，载《华东政法大学学报》，2022 年第 1 期，第 18-31 页。

二、数据交易现状解析：竞争挑战与法律风险

2.1 数据交易主体面临的竞争性风险

数据，这个在数字化时代日益被提及的词汇，往往被轻率地比作现代的“石油”或“黄金”。然而，这一比喻忽略了数据本身的复杂性和多样性。数据并不仅仅是一串串数字的堆砌，更不是简单的电子表格可以囊括的。[20]真正的价值产生于数据的原始性和其与买方产品结合时所展现的潜力。

原始数据是对现实世界中的人、物、事件的直接记录——它们是未经加工的数字化信息，它们的价值在于能够准确反映被记录对象的状态。[21]这些数据集在被整合、清洗或分类后，才能够作为分析的基础。[22]然而，仅仅拥有这些原始数据集，并不能自动转化为商业智慧，它们必须被妥善利用。

数据转化为商业价值的过程可以概括为以下四个主要模式。[23]第一种是数据的聚合，这一过程涉及将来自不同来源的原始数据集中于一点，以便于用户访问和利用，就像“天眼查”或“万德”所做的那样。

第二种是数据的应用化，这是指将数据以用户友好的形式，如 App，直观呈现给用户，降低他们获得和理解数据的门槛，正如“车来了”或“飞常准”所展现的。

第三种是数据的变现，这经常体现在咨询公司、智库或企业战略团队的工作中，他们通过分析数据产生的深层次信息和知识，创造出新的商业模式和价值。

第四种是数据的赋能，这在算法优化和机器学习领域表现得尤为明显，大量多维度的数据集对于精炼算法和预测模型至关重要，从而推动企业在未来的商业实践中获得成功。

总而言之，数据的真实价值并非仅仅在于其原始形态，而是在于这些原始数据如何被加工、分析并最终被应用，它们在与买方产品的融合中，才能释放出巨大的商业潜力。

在我国的数据交易所中，尽管众多数据产品已经被列出以供交易，但这些产品往往并未能满足市场的实际需求。关键的问题在于，这些所谓的“数据产品”通常缺乏可机读性，不符合原始数据的要求，从而未能吸引到那些真正需要数据来推动商业创新的买方。

许多在交易所挂牌的所谓数据产品，实际上是对原始数据进行了某种程度的加工处理，转变为了带有特定解释或结论的“知识产品”。购买者获得的可能只是一个指标、一个趋势或者一项结论，而这些成果往往缺乏用于进一步分析或整合的潜力，难以与其他数据产生协同效应，创造新的价值。

[20] 例如，很多政府认为发布 pdf 格式的数据文件也属于开放数据的表现形式。参见郑磊：《开放不等于公开、共享和交易：政府数据开放与相近概念的界定与辨析》，载《南京社会科学》2018 年第 9 期，第 83-89 页。

[21] 参见高富平：《数据经济的制度基础——数据全面开放利用模式的构想》，载《广东社会科学》2019 年第 5 期，第 5 页。

[22] 参见高富平：《数据流通理论——数据资源权利配置的基础》，载《中外法学》2019 年第 6 期，第 1405 页。

[23] 笔者参照 Andrew Stott 撰写的《为了经济增长的数据开放》(Open Data For Economic Growth)报告，作了文中的分类。See Andrew Stott, Open Data for Economic Growth (Jun 25, 2014), at https://openknowledge.worldbank.org/handle/10986/19997.

“数据一旦转化为具有特定含义的信息或知识，原始数据的生命就此结束。”[24]原始数据的真正价值在于其未经加工的、原生态的状态，它们能够被购买者自由地分析和探索，以挖掘出更深层次的商业机会。一旦数据被固化为特定的信息或知识，它就失去了作为数据的活力和多样性。

因此，对于数据交易所而言，想要迅速吸引并聚集买方的关键在于提供能够直接被商业界利用、具备创新潜力的真正的数据产品。只有那些能够被灵活运用、并能够促进新模式商业价值转化的原始、机读数据，才是买方真正期待和愿意为之支付的产品。只有当数据交易所把握住这一核心需求，并据此调整其产品供给策略时，才可能在数据经济的大潮中占据一席之地。

市场对于原始数据的渴望几乎无处不在，但数据持有者对于出售这些原始数据却显得异常谨慎，这种现象背后的逻辑值得深入探讨。

在信息时代，数据的潜在价值是难以预测的，且未来可能呈现指数级增长，正是由于这种潜在价值的不确定性，数据持有者对于原始数据的保护态度尤为慎重。

数据虽然不具备物理意义上的排他性，理论上它的分享和开发能够最大化其价值。然而，在现实的商业竞争环境中，数据的拥有者往往选择保护自己的数据资产，以避免潜在的竞争挑战。数据一旦公开，就相当于将企业的策略和知识财产暴露给可能的竞争对手。

企业之所以谨慎出售原始数据，是因为数据的真正价值在于其预测能力——通过解析用户偏好、揭示模式并构建连接，数据能够对用户的决策产生影响。[25]这种预测能力并非固有，而是需要与企业内部的数据分析结构和用户账户体系紧密结合，通过个性化推送等手段实现，才能确保数据的价值与现实世界紧密相连，而不是虚构的泡沫。[26]

综上所述，原始数据的出售与保留之间的平衡，需要每个数据持有者根据自己的业务目标和市场策略来权衡。

在数据价值的转化过程中，人类行为的复杂性不容忽视。即使拥有大量关于某个用户的行为数据，算法也不能完全预测其未来的选择，[27]因为行为背后是错综复杂的偏好和权重。[28]数据算法的智慧在于，它不是去穷尽每一个偏好的缘由，而是通过模式的识别，将分散的数据点连接起来，从而得出大概率的行为预测。[29]

---

[24] 高富平、冉高苒：《数据要素市场形成论——一种数据要素治理的机制框架》，载《上海经济研究》2022 年第 9 期，第 70-86 页。

[25] 参见胡凌：《论赛博空间的架构及其法律意蕴》，载《东方法学》2018 年第 3 期，第 87-91 页。

[26] See Katerina Pistor, “Rule by Data: The End of Markets?”, Law and Contemporary Problems, Vol.83, No.2, 2020, p.110-112.

[27] 人的行为远比想象得复杂，一个行为的背后不仅存在多个偏好，而且不同偏好之间还存在权重高低——即便算法“知道”一个顾客一年买了 50 次草莓口味的雪糕，也不能预测该顾客会不会买草莓口味的蛋糕。算法在一定程度上也和人脑一样，不会去追问究竟为什么该顾客会买 50 次草莓口味的冰淇淋，而是当“知道”该顾客一年吃了 50 次草莓口味的雪糕，喝了 40 次草莓口味的奶昔，买了 30 罐草莓口味的曲奇，才能大致“推断”出一个行为模式：该顾客在选择甜食的时候尤其偏好草莓味，所以该顾客大概率会选草莓口味的蛋糕。

[28] See Viktor Mayer-Schönberger and Kenneth N. Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think, Houghton Mifflin Harcourt, 2013, Chapter 1-3.

[29] See Ethem Alpaydin, Machine Learning, MIT Press, 2016, Chapter 4.

由此可知，“数据+算法”能输出精准预测的前提，不仅是被输入大量数据，而且还被输入多个维度的数据[30]：比如电商平台不是仅从用户购买的商品中，就直接捕捉到了用户的偏好，而是收集了用户在电商平台有关的所有网站的数据，从买的衣服、吃的外卖、看的视频、玩的游戏、住的酒店这些数据中，提取到了用户的偏好。[31]

在现实中，各家企业或其他组织都已在自家的赛道中深耕多年，已经积累了大量的同维度数据，但真正能发挥最大潜力的，是多个维度的数据。或许可以设想，以往一个电商平台可能需要 10 年的积累，才能从用户浏览、购买商品的数据里，大致推测出用户的消费偏好，但如今一个短视频平台若想发展电商业务，可能只需要拿到用户近半年的商品购买数据，再结合上用户已经在短视频平台留下的大量视频观看、点赞、下载数据，就能大致定位用户的消费偏好。

企业对原始数据的保护态度之严格，源于其深知数据的潜在价值和竞争优势。在企业看来，原始数据是宝贵的资产，通常会首先自行挖掘开发，希望从中获得创新和增长的动力。仅当内部开发遇到瓶颈，无法进一步挖掘其价值时，企业才可能将这些数据出售，但这样的决策通常伴随着高度的谨慎，因为一旦原始数据落入竞争对手之手，潜在的竞争风险巨大。

这种风险不仅仅在于数据的匿名化程度，即便是去标识化的数据，在精心地分析和对特定群体的细致研究下，也能够产生强大的预测力，为竞争对手带来意料之外的市场洞察。原始数据在不同企业手中的价值可能天差地别，一个数据点的加入，可能使得竞争对手的数据分析得到质的飞跃，从而在市场上获得巨大的优势。

同时，由于算法和机器学习的发展日新月异，每一次迭代都可能带来颠覆性的变化，这使得数据价值的估算变得极其复杂。[32]企业难以预测，自己出售的数据在他人手中的应用和价值转化能力，因此在不确定性如此高的情况下，售出原始数据带来的直接现金流入，可能与潜在的商业损失相比显得微不足道。

在这样的背景下，出售原始数据不仅可能削弱企业自身的创新能力和市场地位，还可能无形中增强了竞争对手的力量。因此，对于许多企业而言，保留并内部开发原始数据，而非将其贸易于市场，更是一种长远的战略选择。

这一逻辑同样能在国外企业中得到验证：即便是谷歌“高调宣传”将会开放数据和代码，但从来没有开放过它收集的原始数据和算法；亚马逊虽然向程序开发者开放了编程接口，但一向严格控制接口深入原始数据。[33]

---

[30] See Rostek and Nathan Yoder, *“Matching with Multilateral Contracts”* (July 2, 2017), at https://ssrn.com/abstract=2997223.

[31] 例如，阿里巴巴集团旗下有淘宝、饿了么、优酷土豆、阿里游戏、飞猪等公司，几乎涵盖了各种领域。

[32] 例如，计算机领域著名的莱斯定理(Rice’s Theorem),就证明了某类算法的不可知属性，算法复杂化模块化,会令各个部分算法之间的相互反应变得更加不可预测。参见沈伟伟《算法透明原则的迷思——算法规制理论的批判》，载《环球法律评论》2019 年第 6 期，第 20-39 页。

[33] See Julie E.Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism, Oxford University Press, 2019, p.45.

实际上，企业或其他组织，尤其是互联网企业不倾向于出售自己的原始数据，是由其生产方式本身所决定的。互联网作为一种新型生产方式，不断连接线上与线下各类生产性资源，在社会范围内调动匹配，从而创造性地产生有效利用资源的新方法，并对既有行业的利益格局和秩序产生破坏性影响。[34]这意味着，“原始数据”是企业或其他组织在互联网这一赛道最大的竞争力，原始数据既可以创造性地从物理世界和传统行业中“非法”获取尚未数字化的资源（比如百度文库针对文化产业的侵权和盗版），也可以“搭便车”从其他竞争者那里获取已经数字化的资源（通过爬虫抓取竞争对手的信息内容，如图片[35]、用户创作文字[36]、数据[37]）。

但无论是以何种方式获取原始数据，互联网作为一种新经济，相对于传统经济而言，它的运转逻辑是从何处以低成本获得原始数据，同时使用算法进行匹配。新经济的兴起要求数据保持流动和低成本非法获取，动态地积累更多用户活动和数据，但同时希望它们在自己的不断扩展的架构内流动，而非跨平台流动，从而通过架构的微观机制不断监控追踪；对外则要求架构不受非法入侵。[38]

在当今的竞争格局下，数据交易市场的特征可以概括为“需求大于供给”。企业在争夺市场份额和拓展业务的同时，对数据的需求日益增长，数据已经变成了他们发展的关键推动力。然而，正是因为这种强烈的需求，企业对自己掌握的原始数据变得更加保护性，他们宁愿自己尝试开发，也不愿轻易将数据让渡给潜在的竞争者。

在我国，上文所提到的涉及数据、流量和社会资本等的一系列不正当竞争案例，反映出司法机关逐渐承认原始数据对企业而言是一项重要的竞争优势。尤其是在反爬虫案件的判决中，看到了互联网行业潜在的竞争秩序：平台企业可以排他性地利用用户授权的行为数据，而抵制其他竞争者的访问和使用。即便是在允许第三方使用的情况下，也必须遵循平台制定的严格规则。

有学者将这种平台企业的“自主圈地”现象称为“非法兴起 2.0”。在这个阶段，平台企业不再是简单地以低成本搭便车获取数据，而是更加积极地通过合法渠道确立其在数字经济中的地位。这种“非法兴起”展现了新经济的双面性：一方面，它需要不断扩张、吸收新的资源来建立新的市场；另一方面，则需筑起防线，抵御其他竞争者对其资源的侵蚀。[39]一旦扩张的步伐放缓，互联网创新和发展便可能受阻；然而，如果不加以控制地让不正当竞争行为泛滥，那么市场和生产秩序就会陷入混乱，导致逆向选择的现象。

因此，数据交易市场的本质是一种供不应求的状态。广泛且持续地对原始数据的需求显而易见，它是企业及组织增长和扩张的驱动力。但是，与此同时，这些组织为了保持自己的竞争边缘——正如厨师愿意出售烹饪出的佳肴而保留食谱一样——并不倾向于向外界出售他们的原始数据。这一矛盾性是数据交易市场独特的经济动态。

[34] 参见胡凌：《互联网“非法兴起”2.0——以数据财产权为例》，载《地方立法研究》2021 年第 6 期，第 21-36 页。
[35] 大众点评诉百度不正当竞争案(2016 年)。
[36] 大众点评诉爱帮网不正当竞争案(2011 年)
[37] 新浪诉脉脉不正当竞争案(2016 年)
[38] 参见胡凌：《互联网“非法兴起”2.0——以数据财产权为例》，载《地方立法研究》2021 年第 6 期，第 21-36 页。
[39] 参见胡凌：《互联网“非法兴起”2.0——以数据财产权为例》，载《地方立法研究》2021 年第 6 期，第 21-36 页。

2.2 数据交易主体面临的法律风险

在数据交易的复杂环境中，除了面临激烈的竞争挑战，数据交易主体还需应对一系列的法律风险。这些法律风险不仅对交易流程产生影响，也对交易双方的决策造成深远的影响。

尽管在数据交易的实践中，交易双方约定的合同可以有效地分配多数风险，确保交易流程顺畅——合同通常清晰界定权利、责任，对侵权等普遍风险作出具体规定——但仍有关键风险无法完全由合同涵盖。

比如，当涉及国家安全或个人信息保护时，合同在交易中能发挥的效力就变得有限。首先，国家安全风险由于其敏感性和可能导致的重大后果，往往超出合同双方的风险承担能力，难以在合同中明确规定。

其次，个人信息保护风险更加复杂，因其相关法律条款模糊、执法态度不一致，导致交易双方面临极大不确定性。此外，合同无法预设或规避行政责任，使得即便双方在合同中达成共识，也可能面临执法机构不可预测的行政措施。同时，个人信息的泄露或不当使用还可能引发公众不满和舆论压力，在这种情况下，公众的关注往往不涉及合同细节，而是将责任泛化到所有相关方。这种外部性的影响意味着，即使风险在合同中有所体现，也无法阻止由此引发的公共谴责。

总的来说，与国家安全和个人信息保护相关的法律风险，由于其不确定性极高，甚至在一些情况下具有系统性特征，因此往往超越了交易方私人合同能够完全内化、妥善安排的范畴。相关法律制度本身的复杂性和适用的不确定性，使得合同在这些领域内的风险分配变得困难。

2.2.1 数据交易与国家安全风险

数据流动和交易可能看似日常和普通，但在某些情境下，它们有可能带来巨大的安全风险。数据的广泛流通和易于访问性虽然为社会发展提供了巨大推动力，但也暴露了潜在的安全漏洞，特别是在关键国家基础设施和敏感领域。然而，不仅仅是保密数据，就连公开和众所周知的信息，也可能在某些情况下变得“敏感”对公开数据的不当管理和使用也会引发对国家安全的严重担忧。以下几个著名案例充分展示了数据流动可能引起的安全问题。

首先，是著名的美国“Strava 事件”，该软件支持数百万的用户发布自己的运动位置，通过汇总所有用户的运动位置后，会在平台上发布运动“热图”，供所有用户在地图上查看运动人群最集中的区域。这些“热图”无意中揭示了美国在世界各地的秘密军事基地，特别是在撒哈拉沙漠和阿富汗城市郊区的集中活动——毕竟，在撒哈拉沙漠和阿富汗城市郊区居然集中着大量运动的美国人[40]——这突显了即使是为了娱乐或健康目的收集的数据，也可能被用作不当用途。

其次，是我国的滴滴“大数据揭秘事件”，这一事件不仅引起了社会的广泛讨论，更重要的是，它强调了数据使用和公开的风险。2015 年，滴滴作为我国领先的出行平台，发布了一篇名为《大数据揭秘：高温天部委加班大比拼》的文章。该文章基于滴滴的实时移动出行数据进行分析，展示了在高温天气下，哪些国家部委的员工加班最为勤奋，其中，国土资源部和公安部被点名加班“最狠”。[41]这篇文章可能本意为展示大数据分析的威力和为公众提供有趣的数据视角，但是，它的发布引发了广泛关注和争议。问题的核心在于，

[40] See Omri Ben-Shahar, “Data Pollution”, Journal of Legal Analysis, Vol.11, No.1, 2019, pp.112-115.

[41] 参见《高温天部委加班大比拼 国土资源部“最狠”》，载人民网，http://politics.people.com.cn/n/2015/0719/c1001-27325279.html。

通过结合部委的公开活动和社会事件，外界可能会对部委的日常工作进行大致的推断，这为恶意行为者提供了可能的利用空间。

最后一个例子是 2022 年 4 月的央视《焦点访谈》报道一起典型案例“高铁数据泄露事件”，这一事件生动体现了即使是公开数据，也可能对国家安全构成潜在威胁。在这一事件中，上海的一家公司与境外的公司进行了所谓的“正常开展工程技术服务”。然而，这一合作被认为涉及非法向境外提供我国的高铁数据，而且导致法定代表人、销售总监和销售人员在 2021 年 12 月 31 日被上海市国家安全局逮捕。

值得注意的是，涉案的“高铁信号数据”并不是国家的保密数据，其采集行为本身似乎也不会影响高铁无线通信的正常进行，更不会威胁列车的安全运行。然而，这并不意味着其对国家安全没有潜在的威胁。高铁信号可能承载着关于高铁运行管理、指挥调度等各种指令，如果这些数据被非法利用，例如被用于故意干扰或恶意攻击，可能会对我国的铁路运营构成严重的威胁，例如导致高铁通信无线中断，进而影响高铁的正常运行。

值得注意的是，上海这家公司并不是一个小规模或不知名的组织。相反，它有着完善的组织架构和功能岗位，包括法务、技术总监、网络安全总监等，并拥有专门的网络安全子公司。此外，与其合作的境外的公司也是一个专业的国际通信服务公司，其客户遍及各国政府、军队及大型企业。[42]

数据交易，尤其在如今全球化、数字化的时代，具有双刃剑的特性。一方面，数据的共享与交易能够为企业带来经济效益和新的市场机会；另一方面，数据的交易可能意味着它被无法预测或控制的对方或第三方用于不明目的，从而带来潜在风险。如上文中的高铁数据泄露事件所展示的，即便是看似普通的公开数据，也可能承载着关键信息，如若被恶意利用后，可能会对国家安全造成威胁。

这些潜在的风险由于其难以预测和难以预知的特性，给企业带来了巨大的担忧。为了规避可能的法律纠纷、声誉损失，甚至是对国家安全的潜在危害，许多企业选择谨慎行事，避免出售或共享其拥有的数据。这种风险意识，使得数据交易的行为被覆盖上一层阴影，尤其是在涉及关键数据或涉及国家利益的情况下。

实际上，数据的重要性已经远远超出了经济价值的范畴，它已成为国家经济安全和主权的关键要素。随着数据价值的不断提升，各国对数据跨境交易的关注也日益增强。这种关注不仅源于数据的经济潜力，更因为数据交易可能对国家安全构成影响。因此，数据跨境交易在国家安全层面上面临着日益严峻的法律和监管挑战。2022 年 1 月，最高人民法院、最高人民检察院根据十三届全国人大常委会第二十四次会议通过的《中华人民共和国刑法修正案（十一）》新增设“为境外窃取、刺探、收买、非法提供商业秘密罪”，对应刑法第二百一十九条之一的罪状表述，即“为境外的机构、组织、人员窃取、刺探、收买、非法提供商业秘密的，处五年以下有期徒刑，并处或者单处罚金；情节严重的，处五年以上有期徒刑，并处罚金”。与属于情节犯的其他七项知识产权刑事犯罪不同，该罪系行为犯，一经实施即构成犯罪；“情节严重”则是加重处罚的依据。

新增的罪名为数据跨境交易划定了刑事红线，强调了数据交易不仅是经济行为，更是与国家安全紧密相连的活动。这种法律环境的变化使得数据交易主体在面对跨境数据交易时变得非常谨慎，担心触犯法律，即使没有直接的危害结果。因此，这种担忧不仅抑制了数据交易的活跃度，也反映出当前数据交易环境中的法

[42] http://www.legaldaily.com.cn/zt/content/2022-04/14/content_8703750.htm

律挑战。在这样的背景下，数据交易主体在进行交易时必须展现出极高的警惕性，以避免潜在的法律风险。这种风险意识不仅限制了数据的交易和流通，也揭示了当前数据交易环境中与国家安全相关的合规压力。

然而，法律设计层面的这种担忧并非空穴来风，而是基于过去一些数据泄露事件。“力拓案”是此类事件中的经典案例，该案清晰地展现了数据跨境对国家经济安全的影响——当时我国在铁矿石贸易中处于被动地位，而澳大利亚力拓公司通过非法手段收集到了我国钢铁企业的商业数据，最终导致我国企业巨额预付款的经济损失，更让我国在铁矿石价格谈判中处于极其不利的地位。

根据人民法院报文章，发生在 2010 年的“力拓案”间接地推动了两高在 2021 年新增了这一罪名“本罪侵害的法益不局限于权利人的商业秘密，更涉及国家经济安全”。[43]“力拓案”的发生背景是我国处于铁矿石贸易中的劣势地位。从世界范围看，我国是最大的铁矿石进口国之一，但铁矿石的定价权一直掌握在澳大利亚力拓公司等三家公司手中，使得我国在铁矿石采购一直处于被动地位。

根据判决书公开的信息，2003 年至 2009 年间澳大利亚力拓公司驻上海代表处首席代表胡士泰等 4 人，为澳大利亚力拓公司在中国铁矿石贸易中获取更多的销售利润，采取利诱等不正当手段，通过多家钢铁企业的工作人员，非法搜集了中国钢铁企业的多项商业数据——四人涉嫌将所在中国钢铁企业的原料库存的周转天数、进口矿的平均成本等财务数据，以及生产安排、炼钢配比、采购计划等内部资料透露给了澳大利亚力拓公司，并致 2009 年中国钢铁企业与力拓公司铁矿石价格谈判突然中止，造成 2009 年中国 20 余家企业多支出铁矿石预付款 10.18 亿元。

2009 年 7 月，胡士泰等四名力拓员工先是被上海市国家安全局以“为境外窃取国家秘密罪”刑事拘留，但是最终法院定罪时是以“侵犯商业秘密罪、非国家工作人员受贿罪”这两项罪名进行定罪。

涉嫌的罪名由原来的“为境外窃取、刺探、收买、非法提供国家秘密、情报罪”，变为“侵犯商业秘密罪”，学界较为一致的观点是：涉案罪名上的降格反映出我国在经济安全的立法方面有很大的缺陷与漏洞，我国在侵犯商业秘密犯罪方面的立法落后于形势，不区分一般侵犯商业秘密的犯罪行为与为境外利益而侵犯商业秘密的犯罪行为，这将不利于对本国企业的保护，以至于我国无法有力惩治这类为境外组织、机构、人员利益而进行的商业间谍行为。

“为境外窃取、刺探、收买、非法提供国家秘密、情报罪”基本犯的法定刑被设定为“五年以下有期徒刑或者拘役，并处或者单处罚金”，其加重犯的法定刑被设定为“五年以上有期徒刑，并处罚金。”而刑法第 219 条规定的“侵犯商业秘密罪”，基本犯的法定刑是“三年以下有期徒刑或者拘役，并处或者单处罚金”，加重犯的法定刑是“三年以上七年以下有期徒刑，并处罚金”。相比之下，“为境外窃取、刺探、收买、非法提供国家秘密、情报罪”的法定刑显然更重。尽管没有无期徒刑，但在整体上达到了与刑法分则第一章“侵犯国家安全罪”中“为境外窃取、刺探、收买、非法提供国家秘密、情报罪”之法定刑的严厉程度。

除此之外，还需特别注意的是，“为境外窃取、刺探、收买、非法提供国家秘密、情报罪”和“侵犯商业秘密罪”还有一个显著的区别：“为境外窃取、刺探、收买、非法提供国家秘密、情报罪”是行为犯，而“侵犯

[43] 唐震：《为境外窃取、刺探、收买、非法提供商业秘密罪“情节严重”的考量因素》，https://www.chinacourt.org/article/detail/2022/01/id/6494323.shtml

商业秘密罪”是情节犯。这意味着，行为人只要实施了为境外的机构、组织、人员窃取、刺探、收买、非法提供商业秘密的行为，即可构成，不要求有危害结果的发生，也不要求发生具体危险。

这意味着，只要涉及为境外实体提供数据的行为被认定为是提供商业秘密的行为，即使没有直接的危害结果，也可构成罪名。可以说，两高在 2021 年新增的“为境外窃取、刺探、收买、非法提供商业秘密罪”为数据跨境交易画上了刑事红线，反映了国家对于数据安全的严肃态度，意味着数据跨境交易不再只是经济行为，它已经与国家安全紧密相连。这一罪名为行为犯的特性使得任何企业和个人在数据交易中都需倍加小心，因为单纯的行为就可能触犯法律，而无需等到其产生实质性的危害结果。因此，数据交易主体在面对跨境数据交易时变得非常谨慎，担心自身可能承担的法律风险。这种担忧无疑抑制了数据交易的活跃度，也反映出当前数据交易环境中的法律挑战。

正因为上述案例和法律环境，现在的数据交易主体在面临数据交易时都展现出极高的警惕性。担心潜在的法律风险，许多企业选择避免或限制数据的交易和流通。这种风险意识抑制了数据交易的活跃度，同时也揭示了当前数据交易环境中的与国家安全相关的合规压力。

2.2.2 个人信息保护制度对数据交易的挑战

在数据交易的过程中，企业在面对个人信息保护法的要求时经常遭遇多重挑战。首先，个人信息保护法律本身存在一定的模糊性，这使得企业在处理个人数据时，往往难以准确判断自己的行为是否完全合规。例如，关于数据的收集、存储和使用的具体限制可能不够明确，导致企业在实际操作中不得不在合法性和商业利益之间进行微妙地平衡。对数据交易主体而言，法律的模糊和不确定，会增加交易的成本。[44]

虽然政府发布了一系列政策来鼓励数据流通和交易，建立数据交易所欢迎数据交易，但这与数据保护“三驾马车”《网络安全法》《数据安全法》和《个人信息保护法》的核心宗旨——保护个人隐私权和数据安全——存在明显的冲突。而在实践中，数据交易所往往要求数据出售者通过第三方机构提供符合《数据安全法》《个人信息保护法》等保护规则的资质安全证明，在合规高标准背景下，囿于成本，数据出售者很难有动力进入政府提供的数据要素市场。[45]

这些冲突不仅导致了法律实施的困难，还使得数据交易者在进行交易时感到担忧，因为他们不确定自己的行为是否会违反现行的法律法规。《个人信息保护法》对于数据的保护偏重，似乎与鼓励数据流通的政策背道而驰。这种矛盾使得数据交易市场的潜在参与者对于进入市场感到犹豫，因为他们担心自己会因为违反个人信息保护规定而受到法律的制裁。

无论是在《个人信息保护法》《网络安全法》还是《数据安全法》中，都通过“告知－同意”的机制，将数据流通与否的决定权交到了用户个人手中。即便是为了促进数据交易的《重庆市数据条例》《上海市数据条例》等地方性法规，也明确指出，未经合法权利人授权同意的数据交易活动不得进行。法律如此设计的后果是，数据出售者在进行数据交易之前，需要对数据的每一个维度，向每一个用户取得同意。

[44] See Hirsch, Werner Z, “Reducing Law's Uncertainty and Complexity.”, UCLA Law Review, vol. 21, no. 5, June 1974, pp. 1233-1236.

[45] 参见胡凌：《数据要素财产权的形成：从法律结构到市场结构》，载《东方法学》2022 年第 2 期，第 120 页。

其次，执法机构在个人信息保护方面的态度和实践存在变化，这给企业带来了额外的不确定性。今天可能被视为合法和可接受的数据处理方式，明天可能因为政策变动或执法态度的改变而成为违法行为。这种不稳定性让企业在进行数据交易时必须承担更高的风险，因为他们无法准确预测未来的法律环境和执法趋势。

在数据流通的实际操作中，为了绕过法律的规制并且降低成本，公司确实可以“花点小心思”在用户协议中对数据的收集和使用进行“一刀切”的授权——公司可以将所有需要“告知－同意”的数据一次性打包，写在《用户协议》中“强取”用户的同意。[46]然而，这种做法很容易被认为是“过度收集”个人信息，尤其是在数据收集与实际业务功能之间没有明确的关联时。这种情况下，用户的“告知-同意”很可能只是形式上的，没有实质性的同意。

在政府层面，众多执法机构已经开始加大对于违反个人信息保护规定的企业的打击力度，强调收集数据应当以“必要性”为原则，并对收集范围进行明确的限制。这无疑给那些想通过数据交易获利的企业带来了巨大的压力。比如网信办、工信部等多部门印发的《App 违法违规收集使用个人信息行为认定方法》第 4 条规定，不得仅以改善服务质量、提升用户体验或定向推送信息等为由强制要求用户同意收集个人信息，个人信息收集的范围被限于实现具体业务功能需要，而《常见类型移动互联网应用程序必要个人信息范围》将收集的必要个人信息的范围限定为最小值。2022 年 11 月，国家网信办依法查处了 135 款违法违规 App，原因是其中 55 款 App 存在强制索要非必要权限，80 款 App 存在频繁索要非必要权限。[47]

实践中，在完善个人信息保护和实现数据充分流通利用之间追求平衡确实存在困难，其对制度设计者和政策实施者的权衡决策能力都提出了较高要求。而在实际的数据交易中，一种看似能够平衡数据使用和隐私保护之间关系的方式，即“匿名化”处理，也受到了广泛的关注。

有学者仍认为，“匿名化”可以成为破解之道——匿名处理后的数据，因无法识别到个人而不再承载主体权利，由此数据交易行为就可以根据《个人信息保护法》第 4 条“个人信息不包括匿名化处理后的信息”，跳出《个人信息保护法》的规制范围，数据交易者也自然被免去了法律风险。[48]

然而，对数据匿名化处理的期待也不应脱离实际，因为从技术原理上来说，所谓的“匿名化”，很多时候只是剔除了“姓名”“IP 地址”这样的直接标识符，却没有消除数据之间的可链接性，这意味着只要数据保持可计算、分析的原始状态，就具备被识别分析的可能性。[49]比如，学者 Sweeney 大量实验后发现，即便是匿名处理过的医疗、财务和教育数据，都能被重新定位到个人，更糟糕的是，个人无法阻止“去匿名化”的数据被进一步扩散和滥用。[50]

[46] 实践中，用户为了使用企业提供的产品或服务，必须同意所有条款。See Marotta-Wurgler, Florencia, “Self-Regulation and Competition in Privacy Policies”, Journal of Legal Studies, vol. 45, no. 2 Supplement, June 2016, p. S13-S40.

[47] 《国家网信办依法集中查处一批侵犯个人信息合法权益的违法违规 App》，载中国网信网，http://www.cac.gov.cn/2022-11/03/c_1669106604621340.htm。

[48] 参见姚佳：《数据要素市场化的法律制度配置》，载《郑州大学学报(哲学社会科学版)》2022 年第 6 期，第 6-7 页。

[49] See Ohm, Paul, “Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization.” UCLA Law Review, vol. 57, no. 6, August 2010, p. 1701-1778.

[50] See Sweeney L, Von Loewenfeldt M, Perry M, Saying it’s Anonymous Doesn't Make It So: Re-identifications of “anonymized” law school data (November 12, 2018), at https://techscience.org/a/2018111301/.

Sweeney 曾通过美国 1990 年的人口普查数据发现，美国有 87.1%的人可以被邮政编码、出生日期和性别这三组数据精准定位，53%的人可以被城市、出生日期和性别定位。[51]2012 年，Sweeney 又做了一个实验，她用 50 美元买了一个华盛顿州公开的住院病例数据集，数据集里包含了每个病人的诊断信息、手术信息、主治医生信息、所在医院信息、费用信息，但没有公开病人的姓名和住址，仅仅是公开了邮政编码，通过搜集公共信息的方式，Sweeney 发现 43.2%的病人可以被精准定位。[52]

即便是和身份关联度不大的数据，也可以被实现“反匿名”，由此企业更难把好“匿名化”这一关。大型互联网公司和技术企业为了研发和改进算法，有时会发布数据集供研究者使用，如 AOL 和 Netflix。网络服务商美国在线（AOL），曾在网站上开放了 65 万用户的 2000 万次搜索数据，尽管数据被剔除了用户名和 IP 地址，但是一名《纽约时报》的记者很快从数据集中找到了一位用户的身份线索，最后实现了对用户的精准定位。[53]流媒体平台“奈飞”（Netflix）为了增强自己的算法推荐机制而公开举办了算法大赛，在大赛中开放了所有用户的评分数据集。虽然数据集经过匿名化处理后，仅剩下被评电影、电影评分和评分日期这三个维度的数据，但有计算机科学家很快发现，只要知道一个用户在一段时间内给哪 6 部电影评过分，“反匿名化”的成功率高达 99%。[54]随后有用户指控奈飞侵犯隐私，而对奈飞提起了集体诉讼。[55]

因此，即使这些数据经过匿名处理，仍有可能被重新关联到个体。这不仅侵犯了用户的隐私，还可能导致企业面临法律诉讼和巨额赔偿。即便是已经进行了匿名化处理的数据，也不意味着企业可以毫无顾忌地进行数据交易。因为在《个人信息保护法》的规定下，一旦数据被重新关联并导致个人信息泄露，企业仍然需要承担相应的法律责任。

因此，《个人信息保护法》第 4 条并不是免责条款，匿名化处理后的数据如若还是发生了泄露的危机，企业仍然会因为《个人信息保护法》承担法律责任。匿名化处理并非万能的，它并不能完全消除数据泄露的风险。正如 Sweeney 的研究显示，通过邮政编码、出生日期和性别这些表面上并不直接与个人身份相关的数据，已经能够精确定位到绝大多数的人。这意味着，只要有足够的数据和分析工具，即便是被“匿名化”的数据也能被“去匿名化”并关联到特定的个体。

最后，公众对个人数据的敏感性和对隐私保护的高度关注也为企业带来了挑战。一旦发生个人信息泄露或被不当使用的事件，即使企业在法律上可能无责，也可能面临公众的强烈谴责和负面舆论。这种情况下，公众可能不会去考虑企业与数据主体之间的具体合同条款和责任分配，而是倾向于将所有责任归咎于企业。

个人信息的处理在当今的数据交易市场中显得尤为敏感和复杂。一旦个人信息被泄露或不当使用，不仅可能引发用户个人的法律诉讼，还可能对企业的声誉造成严重损害。用户的数据直接关联到他们的隐私和个

[51] See Latanya Sweeney, Simple Demographics Often Identify People Uniquely, at https://dataprivacylab.org/projects/identifiability/paperl.

[52] See Sweeney L, Only You, Your Doctor, and Many Others May Know (September 29, 2015), at http://techscience.org/a/2015092903.

[53] See Michael Barbaro & Tom Zeller, Jr., A Face Is Exposed for AOL Searcher No. 4417749, N.Y. TIMES, Aug. 9, 2006.

[54] See Arvind Narayanan & Vitaly Shmatikov, How to Break the Anonymity of the Netflix Prize Dataset(October 18, 2006), at https://arxiv.org/abs/cs/0610105.

[55] See supra note [39], pp.1717-1730.

人权益，数据的任何不当处理都可能对用户造成重大的隐私侵犯和经济损失。因此，如果用户发现他们的信息被未经授权使用或泄露，他们很可能采取法律行动，追求赔偿或追究责任。一旦大量用户集体行动，企业可能面临庞大的赔偿压力，这不仅在经济上是一笔巨大开销，更在管理和声誉上构成严重挑战。

除了直接的法律风险，个人信息的不当处理还可能对企业的公众形象和市场地位产生长期的负面影响。在信息泄露或滥用的事件中，即使企业在法律上可能无责，公众的舆论也可能不利于企业，导致信誉受损。这种情况下，公众往往不会深入了解事件的具体细节，而是倾向于将责任归咎于企业，从而加剧企业面临的社会压力。

鉴于这些风险，企业在进行数据交易时只能非常谨慎。考虑到潜在的法律诉讼、赔偿金、声誉损害以及客户信任的丧失，许多企业开始重新考虑其数据交易策略。在很多情况下，确保交易活动不涉及法律风险，比简单追求短期的经济利益更为重要。

三、数据交易所的未来定位：独特服务优势探索

基于对数据交易现状的分析，数据交易机构需要思考整体上的数据要素市场结构，找准自身在数字经济和相关产业链中的定位，寻求和场外交易相比存在差异化的竞争优势。场外交易之所以受到市场主体的青睐，可能归功于灵活性、快速反应能力和较低的交易成本等特点。这种交易方式能够迅速适应市场需求的变化，为交易双方提供了便利和高效率的交易环境。

场内目前面临的挑战是，当场外交易的优势无法全部在场内复制时，应如何塑造自身独特的竞争优势。这要求数据交易所在设计和运营机制上进行创新，找到与场外交易不同的吸引点。目前，数据交易所已经通过提供更高级别的数据安全保障、更严格的合规审查，以及更广泛的市场对接机会，来吸引那些对安全性和合规性有更高要求的交易主体。

然而，仅仅提供基本服务并不足以赋予数据交易所强大的竞争优势。为了真正在市场上占据一席之地，数据交易所需要开发出更加有竞争力的独特优势，尤其是针对那些场外交易无法满足的市场需求，提出切实可行的解决方案，这才能让数据交易所在数据交易中真正破局。

3.1 点对点交易：场外交易的核心优势分析

在数据交易市场，实际情况往往是数据出售方比数据购买方拥有更大的话语权。这一现象源于数据本身的独特性和稀缺价值，使得数据卖方在交易中占据了主导地位。他们不仅可以决定交易是否发生，还可以主导交易的内容、定价，甚至决定责任分配的方式。这种状况在场外的点对点交易中尤为明显，数据出售方利用其独特优势，掌控了交易的基本面。

然而，在政府搭建的数据交易所环境中，这种主导地位却受到了挑战。数据交易所在设计时，力图确保交易双方平等，强调合法性、公正性、透明度等原则，数据出售方往往需要遵循一系列的规范和要求，包括数据出售者需要遵循“合法、正当、必要、诚信的原则”，数据出售者被要求不能差别待遇，尽量定价统一，而最终定价可能还会受到政府的影响。[56]

这种做法旨在创造一个公平的交易环境，但却与数据交易市场的实际运作情况相悖。由于数据出售方通常享有较大的议价权，他们往往倾向于在那些能够充分发挥自身优势的场外交易中寻求更大利益，而不是受到严格规则约束的数据交易所。

这种情况导致数据交易所难以吸引数据出售方参与，因为在场内他们将无法像在场外交易中那样享受更大的议价权和控制权。数据交易所所倡导的平等原则，对于那些有能力控制市场的关键数据卖家吸引力不足，并由此会在整体上削弱了交易所的吸引力和交易活跃度。

溯源买卖双方权力结构不对等的原因，数据出售方之所以占据更高的地位，主要在于当前数字经济的市场格局总体上趋向于集中，而这种集中状况直接影响了有价值数据的可获取性。随着各大平台企业的发展壮大，他们在特定领域中积累的用户数据和行为分析变得越来越难以替代，这不仅是因为这些数据的数量庞大，更因为它们涵盖了广泛且深入的用户行为和偏好。

[56] 例如，《上海数据条例》第 24 条规定：“利用个人信息进行自动化决策，应当遵循合法、正当、必要、诚信的原则，保证决策的透明度和结果的公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。”

在这种格局下，数据的非替代性变得尤为明显。数据作为生产和生活的伴生品，随着平台企业的扩张和影响力增强，它们所掌握的数据集涵盖了用户的各个层面。例如，在短视频行业，抖音和快手这样的平台因其巨大的用户基数和深入的用户行为理解，所积累的数据在广告投放、市场研究等方面具有独特且不可替代的价值。这种情况在其他领域也有类似的体现，如电商、社交媒体等。

正因如此，这些拥有独特数据的平台企业在数据交易市场中占据了主导地位。他们不仅能够控制自身数据的出售条件和价格，还能决定数据的使用方式和范围。为了巩固数据交易的主导地位和自身的竞争优势，数据出售者虽然拥有大量独特且价值高的原始数据，但他们通常不选择直接出售原始数据。相反，他们倾向于将数据加工、分析后转化为信息或知识产品，再将这些产品出售给数据购买者。因此，所谓的“点对点交易”的交易标的很多时候交易的内容并非原始数据，而是已被二手处理过的“信息、知识”。

例如，一个掌握大量消费者购买行为数据的电商平台，可能不会直接出售这些原始数据。相反，成熟的数据出售者可能会开发出基于这些数据的市场趋势分析报告，或是为其他企业提供定制化的市场研究服务。通过这种方式，数据出售者不仅能够保持对其数据的控制权，还能通过转化为知识或信息产品来创造新的价值和收益。

此外，这种做法也有助于数据出售者规避法律风险。由于涉及到个人信息保护法、数据安全法等法律法规的约束，直接出售原始数据可能会使数据出售者面临各种法律责任。而通过转化为信息或知识产品，数据出售者能够更好地控制数据的使用方式和范围，从而减少法律上的风险。

出售咨询服务而不是原始数据，对数据出售者来说是避免了风险，对于购买者而言，也不失为一个好的选择。数据购买方有时倾向于购买经过加工和分析的数据服务而不是原始数据本身，是因为这些服务更能直接地为其带来商业价值，同时降低了技术和风险挑战。首先，原始数据的价值往往在于其与特定算法的结合使用，但原始数据本身可能是杂乱无章且非结构化的，不易与现有的技术或算法相融合。因此，在质量不一和难以保证的情况下，从技术和操作层面考虑，选择已经加工和分析过的商业咨询服务，往往是更稳妥且风险更低的选择。

其次，由于缺乏清晰的数据估价机制，数据的价值可能在不同购买者眼中差异巨大。例如，对于饮料企业而言，茶饮消费数据可能极具价值，而对于游戏企业则可能价值有限。在这种情况下，拥有市场上已经形成的相对清晰和统一定价的商业咨询服务，对于买卖双方而言都是更为明智的选择。商业咨询服务的定价通常更加透明和明确，这有助于在数据交易过程中减少误解和谈判难度，从而促进交易的顺利进行。

总的来说，选择商业咨询服务而不是直接购买原始数据，对于数据出售者来说可以减少潜在的法律和商业风险，而对于数据购买者而言，则提供了更明确、更可操作的商业价值，这使得商业咨询服务也成为数据市场中的一种较受欢迎的交易形式。

在数据交易的复杂格局中，有学者曾提议将数据交易所转型为中间的撮合者，专注于为交易双方提供磋商服务，类似于华东江苏大数据交易中心的做法，即通过专家团队为数据购买者定制解决方案，而不是直接交易原始数据。[57]然而，这种模式在现实中的实施面临重大挑战，关键原因在于许多平台企业已经具备完善的数据处理和分析能力，它们可以自行实现点对点交易，不依赖数据交易所的介入，同时还能规避政府监管。

[57] 参见丁晓东：《数据交易如何破局——数据要素市场中的阿罗信息悖论与法律应对》，载《东方法学》2022 年第 2 期，第 144 页。

此外，这种模式导致数据购买者对数据出售方的依赖性增强。由于无法直接获取原始数据，购买者必须频繁向出售者购买服务以满足其数据需求。这不仅增加了交易频率，也使数据出售方在交易中的主导地位得到巩固。

综上所述，数据出售方由于掌握稀缺且独特的数据资源，在数据交易市场中占据了主导地位。他们倾向于通过出售经过加工或分析后的数据服务而不是原始数据，以此来控制交易过程、降低法律风险，并保持自身的竞争优势。这种做法虽然为双方带来了价值，但同时也加剧了购买者对卖方的依赖，进一步加强了数据出售方在市场上的主导地位。因此，对于数据交易所而言，仅仅充当中间撮合者的角色可能难以满足市场需求。更重要的是，数据交易所需要寻找和开发独特的优势和功能，以满足市场上尚未被点对点交易满足的需求，从而在数据交易市场中扮演更加核心和有影响力的角色。

3.2 场内交易的优越之处：与场外交易的对比分析

场外点对点交易模式在数据交易中独树一帜，为数据出售者带来了不小的商业优势。在这种交易模式下，由于交易的双方直接沟通，数据出售者可以根据自身的情况和买家的需求，灵活制定交易策略。更重要的是，点对点交易为数据出售者提供了极大的价格和内容控制权，从而确保其核心数据资产的价值不会被稀释。而且，由于交易过程中的信息不公开，数据出售者可以有效避免与其他竞争对手的直接竞争，确保自身的市场地位。

但是，这种模式并不是没有缺陷的。最明显的问题就是法律风险。尽管数据出售者可以避免与竞争对手的竞争，但在点对点的交易模式下，交易的合规性、透明性都可能受到挑战。数据的收集、存储、处理和传输，都涉及诸如隐私权、知识产权等法律问题。而在点对点的交易模式中，缺乏有效的第三方监管和审核机制，很容易导致合规性问题。

这也正是数据交易所的价值所在。通过制度建设和服务创新，数据交易所不仅可以降低交易双方的法律风险，还可以为交易双方提供更多的支持和服务。例如，交易所可以为交易双方提供标准合同模板、第三方审核服务、法律咨询等，确保交易的合规性。此外，交易所还可以建立纠纷解决机制，为交易双方提供公正、及时的争议解决服务。

近年来在国内各地纷纷推动建设数据交易所或交易平台，但已落地的项目普遍面临场内交易难以形成规模的困境。[58]有论者指出，数据交易所需重新定位其功能，不能只是提供集中交易场所，而应更多致力于交易撮合，甚至主动发掘交易需求，并提供符合数据交易特殊需要的交易服务（例如数据清洗等）。[59]提高服务水平当然有助于提升交易所对市场主体的吸引力。但在练好内功之外，如果政策层面的确属意靠交易所带动数据要素流通，特别是希望提升场内交易相对于平台流通和灰黑市交易的吸引力，那么将交易所场内交易设定为安全港规则适用的首要场景，或是一条捷径。

[58] 据一些统计，截止 2022 年 3 月底，全国各省已经设立 53 家数据交易场所，包括交易平台、交易中心和交易所等不同形式；而目前，甚至有此前挂牌的数据交易中心因无实际业务而已被撤销。https://mp.weixin.qq.com/s/tQRwTQKw1nEjMoYo9vVX8A。

[59] 参见丁晓东：《数据交易如何破局--数据要素市场中的阿罗信息悖论与法律应对》，《东方法学》2022 年第 2 期，第 144 页。

换言之，若交易所为场内交易设置的主体资格要求和交易行为规范，同时可获得权威效力背书，成为安全港规则，那么选择在交易所场内开展数据交易，就可使交易主体获得较场外交易更明确的免责预期。这一思路在当前有关数据交易制度配套的讨论中获得初步关注，但并不充分，[60]然而免责预期明显可以成为交易所和场内交易的竞争优势。[61]类似科斯所说，法律提供的免责预期本身就构成生产要素。[62]

从历史经验看，互联网的“非法兴起”过程就是这样一种安全港思维方式的实践，即法律不断确认信息内容的数字化演进过程，减少对传统要素的保护力度。具体而言，“非法兴起”是学者对网络经济特别是互联网企业发展模式的一种解释性描述——以网络经济为代表的新经济模式具有一种本质特点，即通过低成本获取免费内容或劳动力，例如，互联网企业为了吸引用户，早期曾通过有侵权嫌疑的方式以低廉成本将内容放到互联网上。[63]这种新经济特征与传统的规范和思维方式产生了冲突，但基于发展产业的战略需求，政策制定者和执法者都选择了在一定程度上容忍新经济成本的外部化，避免过于严苛的法律责任导致相关创新活动规模受到过度抑制。

及时解决新型生产方式的合法性同样重要，随着新型市场要素的不断增加，市场规模扩大，成为有影响力的生产组织，就需要适时通过立法确认既有稳定的商业模式，以进一步吸引社会资源的投入。[64]

“安全港规则”（译自英文“safe harbor rules”，也常被译作“避风港规则”[65]）。虽然目前包括《个人信息保护法》《数据安全法》《网络安全法》等在内的信息数据领域基础性法律，已建构出一个强调风险预防、损害问责的原则性制度框架，但是其笼统和模糊的形式难以满足市场主体对更高法律确定性和可预期性的需求。而安全港规则旨在为数据交易市场主体提供一个清晰、明确的合规路径，同时为其提供相应的法律保障。这一机制是为了平衡市场效率和法律责任之间的关系，确保在鼓励数据交易的同时，保障数据隐私、数据安全和网络安全。安全港规则的实施为数据交易市场主体提供了明确的操作指南。在数据交易领域，尤其是跨境数据交易中，存在许多不确定性，包括如何收集、处理和使用数据的法律责任、如何确保数据的隐私和安

[60] 提及这一思路的，见胡凌：《数据要素财产权的形成：从法律结构到市场结构》，《东方法学》2022 年第 2 期，第 120 页；杨力：《论数据交易的立法倾斜性》，《政治与法律》2021 年第 12 期，第 3 页。

[61] 目前的讨论主要角度是法律如何规范数据交易，而不是法律如何赋能数据交易。丁晓东，155-157.

[62] See R. H. Coase, *The Problem of Social Cost*, The Journal of Law and Economics, Vol.3, 1960, p.44.

[63] 参见胡凌：《互联网“非法兴起”2.0——以数据财产权为例》，载《地方立法研究》2021 年第 6 期，第 21-36 页。

[64] 参见胡凌：《数据要素财产权的形成：从法律结构到市场结构》，载《东方法学》2022 年第 2 期，第 120-131 页。

[65] 本文将统一使用“安全港”的译法。需要说明，我国法律界专业人士在探讨网络侵权语境中的“safe harbor rules”时，更常将其译为“避风港”。例如，单甜甜：《互联网平台适用避风港规则免责的条件》，《人民司法（案例）》2020 年第 5 期；陈昶屹：《“避风港规则”扩张适用网络人格权保护之困境与消解——兼论侵权责任法第三十六条之完善》，《人民司法（应用）》2012 年第 1 期。而在证券法、反垄断法和税法等经济法领域中，“安全港”的译名更常用。例如，冯果、洪治纲：《论美国破产法之金融合约安全港规则》，《当代法学》2009 年第 3 期；沈朝晖：《上市公司私有化退市的“安全港”制度研究》，《法学家》2018 年第 4 期，第 66 页；范晓娟：《论有限合伙基金的“安全港”规则的突破》，《政治与法律》2013 年第 5 期，第 128 页；陈洁：《“利用自身信息交易”作为内幕交易抗辩规则的建构--兼论我国内幕交易安全港规则的基本框架》，《现代法学》2021 年第 5 期，第 145 页。网络法研究者偶尔也有将“通知—删除规则”译为“安全港”的。例如，最高人民法院发布互联网十大典型案例（2021）“天津市嘉瑞宝金属制品有限公司诉徐桂珍、邓艳辉、赵振全、天津多维斯地毯有限公司、天津欧豪雅地毯有限公司、第三人浙江天猫网络有限公司不正当竞争纠纷案[（2019）]”（周汉华的评论）。选用译名不同，或许是导致不同领域研究者未留意其他领域中也有“安全港规则”的一个原因。

全等。安全港规则通过明确规定合规路径，为市场主体提供了一个明确、可操作的框架，从而减少了交易的不确定性和风险。

此外，安全港规则还鼓励了数据交易市场主体的自律和自我管理。在安全港机制下，只有满足特定要求的交易主体，才能享受到法律上的免责预期。这意味着，市场主体不仅需要具备相应的合规资质和合规记录，还需要在交易过程中遵循特定的合规要求，例如数据来源的披露、数据用途的描述等。这样，不仅保证了交易的合规性，也提升了市场主体的自律意识和自我管理能力。

然而，安全港规则并不意味着放任市场自由。对于“驶入”安全港的数据交易活动，权威机关仍然有责任和权利对其进行监管。例如，对于不满足安全港要求的交易主体，权威机关可以采取相应的法律措施，确保其对数据处理活动导致的损害承担法律责任。此外，权威机关还可以通过定期审核、随机抽查等方式，确保市场主体真正遵循安全港规则，从而确保数据交易的合规性、透明性和公正性。

安全港规则为数据交易市场主体提供了一个合规、透明、可操作的框架，从而促进了数据交易的健康、稳定和有序发展。同时，通过鼓励市场主体的自律和自我管理，确保了数据的隐私、安全和网络安全。在数据日益成为关键生产要素的今天，安全港规则的实施和完善，对于推动数据交易的公正性、透明性和安全性，具有十分重要的意义。

在此基础上，交易所还可以引入数据估价机制，为交易双方提供数据的市场价值参考；或者引入数据保险机制，为交易双方提供数据损失的风险保障。通过这些制度创新，数据交易所不仅可以保障交易的公正性、透明性和安全性，还可以为交易双方提供更多的价值。与此同时，数据交易所还可以与其他市场主体合作，形成数据交易的生态圈。例如，交易所可以与数据处理和分析公司合作，为数据买家提供数据加工和分析服务；或者与金融机构合作，为交易双方提供数据融资和保险服务。通过这种生态圈合作，数据交易所不仅可以提升自身的市场地位，还可以为交易双方提供更多的价值和服务。

正是在这样的背景下，安全港规则的设计成为数据交易领域的关键议题。虽然场外点对点交易在灵活性和控制权方面拥有显著优势，但随之而来的法律风险和合规挑战，使得安全港规则在数据交易所中的应用显得尤为重要。安全港规则不仅提供了一条明确的合规路径，还为交易主体创造了一个相对安全的法律环境，有效平衡了市场效率和法律责任之间的关系。这一机制对于促进数据交易的合规性、透明性和公正性，提供了一种新的可能性。

下文将重点探讨安全港规则的具体设计和实施方式。将分析如何通过明确的规则和标准，为数据交易市场主体提供清晰的操作指南和法律保护。同时，也将探讨安全港规则在实际应用中可能面临的挑战，以及如何通过制度创新来提升数据交易的整体效率和安全性。通过深入探讨这些问题，旨在为数据交易市场的健康发展提供新的思路和解决方案。

四、上海数据交易所“安全港规则”的理论构建

在数字经济时代，数据交易已成为推动经济增长和技术进步的关键因素。然而，如何确保数据交易的安全与合规性，一直是行业内外都深感关切的话题。特别地，上海数据交易所，在其业务的深化和拓展中，逐步展现出了对这一议题的深入思考和探索。

“安全”这一词汇在此背景下呈现出其双重的含义：

第一重含义的“安全”，是技术与实务角度的“安全”。对比不受监管的黑市数据交易与数据交易所提供的服务，后者显著地提高了交易的安全性和合规性，为交易双方构建了一个更为稳固和可靠的交易环境。数据交易所的存在不仅仅是作为一个交易的场所，更重要的是，它为数据的买卖提供了一系列的合规服务，从而在客观上降低了交易风险。这是因为数据交易所通过严格的审核和持续的监管，确保了交易数据的合法来源和透明流通。与黑市交易中常见的来源不明和质量无保障的数据相比，交易所内的数据都经过了严格的审核，这不仅保护了数据出售方的合法权益，也为数据购买方提供了一个可信赖的数据来源。

然而，仅有技术上的保障还远远不够消除交易主体对交易的担忧。这引出了安全的第二重含义——法律上的安全。对于交易主体来说，他们需要确信其交易行为在法律框架内是被允许的，且不会带来潜在的法律风险。因此，除了技术保障，上海数据交易所还积极寻求在法律层面的支持和认可，以期为交易者提供一个更为全面的“安全港”。

事实上，上海数据交易所的追求并不仅限于简单的客观安全。更深远的愿景是在数据安全风险和数据交易规模之间寻找一种平衡。这种平衡不仅仅是技术层面的实现，更是要通过深入的制度建设来达成。

如此看来，数据交易安全港规则的实现是一个两阶段的过程：

在第一阶段，上海数据交易所将探索通过提供一系列创新和先进的服务，来降低交易的客观风险。这意味着交易所在技术层面的服务，应做到确实比其他没有这些服务的平台更具优势，从而确保交易在客观层面的风险更低。

第二阶段的重点，是使数据交易所在其通过自身努力已经能够取得的服务能力和优势的基础上，进一步获得政府和行政部门的支持。这种支持可以视为对数据交易所的努力和成效的认可，也是激励其持续发展和创新的重要动力。这种待遇不仅是对数据交易所技术和客观努力的肯定，更是对其在推动数据交易市场健康发展中所发挥作用的认可。

目前，数据交易所持续致力于整合自身研发资源和外部合作力量，探索、开发一系列合规服务，以有效降低数据交易的各类安全风险。相关探索和实践的潜力和价值，未来将有待在政策层面获得进一步肯定和激励。上海数据交易所相信，这样的安全港建设是必要且重要的。安全港机制不仅提供了一个明确的合规框架，还为交易者提供了更多的法律保障，从而增强了市场主体对交易所的信任和依赖。因此，数据交易所将继续推动安全港的建设和完善，同时积极争取更多的政策支持，以确保其在数据交易市场中的关键角色和地位。

在未来的发展中，上海数据交易所将继续在客观和技术层面做出努力，不断提高服务水平和交易安全性。同时，它也期待政府和行政部门能够给予更多的支持和激励，以促进数据交易市场的健康发展，实现数据交易的更广泛应用和价值挖掘。通过这样的双向努力，数据交易所有信心在未来构建一个更加公平、透明和安全的数据交易环境。

正因为此，尽管目前安全港规则尚未全面落地，但对其进行深入的理论研究和规划显得尤为重要。这不仅是因为安全港规则是数据交易所未来发展蓝图中的关键一环，也是因为它对于确保数据交易市场的健康和有序发展具有重要意义。

下文将重点分析上海数据交易所在合规技术层面上的安全港规则设计，以及在法律规则层面上的相关措施。这种双重保障的设想旨在为数据交易市场的参与者提供更全面的法律和技术保障，确保交易过程的安全性、合规性和效率。

详细探讨安全港规则，意味着将深入分析如何在数据交易中平衡效率和安全性，如何确保数据交易所能在保护数据隐私和促进数据流通的同时，有效管理法律风险。通过对这些关键问题的解答，上海数据交易所希望能为整个数据交易市场的健康发展奠定坚实的基础。

因此，尽管安全港规则的具体细节和实施可能仍需时日，但对其原理和框架的理论探索绝非早熟。相反，这种前瞻性的思考和规划是确保数据交易所能够顺应数据经济时代潮流、引领市场发展的关键所在。

4.1 合规技术层面的安全港规则

上海数据交易所作为国内领先的数据交易平台，在数据交易合规性方面有丰富的探索，积累了诸多实践经验。上海数据交易所不仅制定了一系列的交易规范和指引，更重要的是，其正在积极引入创新技术，致力于全面降低数据交易的客观风险。

上海数据交易所不仅寻求建立一套完善的数据交易合规体系，确保数据交易的合法性、公平性和安全性，也致力于推动利用人工智能（AI）技术破解数据合规难题，为数据交易的合规问题提供有效解决方案，为安全港规则提供支撑。

4.1.1 合规服务

（1）打造数据要素流通交易规则

上海数据交易所在推动数据交易领域的规范化和合规化方面发挥着关键作用。2022 年 8 月，上海数据交易所首次发布了一系列关于数据交易的规范和指引，紧接着在 2023 年 10 月，进一步发布了《上海数据交易所数据交易安全合规指引》。这一系列规范和指引旨在构建健康的数据要素市场，同时注重交易安全和合规性，并提出创新制度，其中明确了交易规范、合规规范、安全规范、交易流程和数商规范，以下将详细介绍五大核心规范的内涵和重要性。

交易规范的明确性与深化

上海数据交易所对交易规范的制定与明确，展现了对整个数据交易过程的精细管理和高度重视。交易规范不仅是数据交易的基石，更是确保交易公平、透明和安全的关键。

首先，交易的基本原则为所有参与方提供了一个公平交易的平台，确保每一方在交易中的权益都得到了保障。这些原则涵盖了交易的公正性、透明性和诚信性，为数据交易的各方提供了明确的行为指导。

其次，交易的主体、对象和方式的明确，确保了交易的专业性和高效性。上海数据交易所对交易主体的资质、交易对象的合规性、交易方式的安全性都作出了明确的要求。

再者，违规处罚与监督管理保障的制定，是为了维护交易的公正性和公平性。任何违反交易规范的行为，都将受到相应的处罚，确保交易的公信力。

合规规范的明确性与深化

上海数据交易所对合规规范的制定与明确，体现了对数据交易合法性的高度重视。合规规范是确保数据交易各方权益的关键，也是数据交易健康、稳定和可持续发展的基石。

首先，主体的资质与责任的明确，确保了数据交易的专业性和合法性。

其次，数据交易标的的合规要求与风险控制，确保了数据的质量、安全性和合规性。这包括数据的来源、数据的处理和数据的使用等各个环节的合规要求。

安全规范的明确性与深化

上海数据交易所对安全规范的制定与明确，展现了对数据交易安全的高度重视。安全规范不仅是数据交易的基石，更是确保数据交易的可靠性和稳定性的关键。

首先，数据的加密、备份与恢复的要求，确保了数据在交易过程中的安全。

其次，第三方的合规评估，确保了数据交易的公正性和客观性。上海数据交易所引入了第三方机构进行合规评估，确保评估的公正性和客观性。

数据交易流程的明确性与深化

明确数据交易流程是实现数据价值的关键。上海数据交易所已经制定了明确的数据交易规则、交易标的、违规的处罚方式以及监管理保障等事项。

首先，主体认证、产品登记、产品挂牌等环节的明确，确保了交易的专业性和高效性。上海数据交易所对这些环节进行了严格的管理，确保交易的顺利进行。

其次，交易签约与结算的流程，确保了交易的公正性和公平性。上海数据交易所采用了先进的技术手段和管理手段，确保交易的公信力。

数商规范的明确性与深化

首先，数商资格标准的制定是为了确保参与数据交易的数商都具备一定的专业能力和信誉度。这包括对数商的基本资质、技术能力、经营历史等进行综合评估。只有满足一定标准的数商，才能在上海数据交易所进行数据交易，这样可以有效地减少交易风险，提高交易的公信力。

其次，管理规范的制定是为了规范数商的日常经营活动，确保其行为与上海数据交易所的总体目标和原则相一致。这包括数商的数据采集、数据处理、数据销售等各个环节的管理规范，确保数据的质量、安全性和合规性。

再者，责任义务的明确是为了确保数商在数据交易中的行为是负责任的。这不仅包括对数据的真实性、完整性和安全性的责任，还包括对数据交易合同的履行责任、对客户的服务责任等。任何违反规范的行为，都将受到相应的处罚。

最后，退出机制的制定是为了确保数商在无法满足上海数据交易所的规范要求时，可以有序、安全地退出数据交易市场。这既保障了数商的权益，也确保了数据交易市场的稳定性和公信力。

上海数据交易所对数商规范的制定与明确，体现了对数据商业活动的高度重视和规范化管理。上海数据交易所对数商规范的明确与深化，旨在建立一个公平、透明、安全的数据交易环境，促进数据经济的健康发展。

（2）推动数据产品合规评估服务

上海数据交易所在数据交易合规性方面的实践和经验为国内外的数据交易所提供了宝贵的参考，通过建立完善的合规评估体系，上海数据交易所确保了数据交易的合法性、公平性和安全性。这为数据交易的参与者提供了一个公平、透明和安全的交易环境。

除此之外，上海数据交易所还面向数据合规评估商，围绕数据产品合规评估业务组织培训专场，包括不同行业的合规审查标准、合规审查清单指引培育数据合规评估商评估能力、规范评估方式，促进合规高效流通，让市场对数据交易合规标准达成统一共识。

随着一系列的合规培训及沙龙讲座的宣导，数据合规评估商及企业已逐步适应合规评估的标准及全流程要求，对数据产品、数据交易合规有了更清晰的认知。上海数据交易所还针对中小企业对数据合规问题的认知缺失、描述不清等问题，提供有针对性的指导，旨在解决中小企业难以向市场表达合规的痛点问题。目前，上海数据交易所已经为近 50 家中小企业助力解决产品合规问题（这些合规问题主要集中在数据来源，数据安全能力等方面），帮助中小企业完成产品合规要求，为其向市场证明符合法律法规的合规标准提供支撑。

4.1.2 合规科技

（1）探索人工智能工具解决合规痛点

上海数据交易所致力于通过引进先进技术的方式，为数据交易的合规问题提供成熟的解决方案。随着人工智能的迅猛发展，通过人工智能赋能数据合规，全面提升合规管理质效已成为破解数据合规难题的重要抓手。基于 AI 的智能评估工具，能够自动化处理一些复杂的合规流程，如自动扫描企业合规材料、辅助识别数据风险等功能，有效减少了人工检查工作量，提升合规工作的效率

数据交易归根结底会落实到双方的合同。不同于常规的货物买卖合同，数据交易合同较为新颖且专业化更强，需要更为综合性的合规指引方才能够为交易的顺利进行保驾护航。通过自然语言处理、机器学习等人工智能前沿技术，人工智能可以根据语义识别比对关键条款，自动审核数据交易合同是否符合法律法规要求，快速识别合同中存在的风险点并提供相应的修改建议。

（2）建立合规知识库助力市场主体智能检索

数据交易对于市场主体的一大痛点便是规则的复杂性，以及由此产生的高昂合规成本。数据交易领域的法律架构非常复杂，需要极为专业化的知识支持，这是因为数据交易涉及到许多法律法规、合同和隐私保护等方面的问题。为了确保交易的合法性和合规性，必须符合《网络安全法》《个人信息保护法》《数据安全法》等诸多法律及其细则的复杂规定，市场主体需要详尽的合规指南以及专业化的法律检索数据库，这些服务对法律专业能力要求极高。为此，上海数据交易所正在根据市场需求引进专业的合规知识库，以求大规模降低市场主体进行场内交易的合规成本，希望能在未来促进数据交易市场的进一步发展。

在数据交易领域，法律架构的复杂性主要体现在以下几个方面。首先，跨境数据交易可能涉及到多个国家和地区的法律法规，而不同国家和地区对于数据的使用、存储和传输可能有不同的规定。因此，在进行复

杂的跨境数据交易时，需要考虑各个国家和地区的法律要求，并确保交易符合各方的法律规定。其次，数据交易还涉及到知识产权保护的问题。在数据交易过程中，可能涉及到他人的知识产权，如专利、商标和著作权等。因此，必须确保在数据交易中不侵犯他人的知识产权，并遵守相关的法律规定。此外，数据交易还需要考虑数据隐私的保护。随着数据泄露和滥用的风险不断增加，保护用户的数据隐私成为一项重要任务。因此，在数据交易中必须遵守相关的隐私保护法律，并采取相应的技术措施来保护用户的隐私。

上海数据交易所认识到市场主体面临的上述痛点，通过积极培育数商生态、引入专业服务机构解决数据合规专业知识上的难点与堵点。上海数据交易所正在与知识行业的头部机构展开合作，为市场主体提供一站式数据合规知识服务。数据合规知识平台以成为数据价值实现全生命周期知识服务专家为愿景，以上海数据交易所合规规范指引为基础，全面整合数据合规各领域、各区域的法律规范与案例，为市场主体提供客观标准，并关联知识要点，为决策提供支撑与参考；嵌入审查系统，依据数据类型、场景为审查/自评者提供流程化、导引式服务，提高数据合规服务的能力与效率。通过数据合规知识平台，市场主体可以快速了解进行数据交易的具体要求，帮助其在面对海量的法律法规时，能迅速定位到相关要求及实践案例；在进行数据交易时，可以精准检索支撑数据交易的合规知识，降低企业合规成本。

（3）检测关键条款保护双方合法权益

数据交易归根结底会落实到双方的合同。不同于常规的货物买卖合同，数据交易合同较为新颖且专业化更强，需要更为综合性的合规指引方才能够为交易的顺利进行保驾护航。在数据交易的商业场景中，交易的本质是围绕数据使用权等核心权利的转让，同时因为数据的来源也会涉及到一般合同之外的第三方，因此一个符合法律规定的合同文本便是交易的核心，也是交易双方关于本次交易的权利义务约定书，能够尽可能减少日后因为交易发生争议的风险。

上海数据交易所致力于开发合规科技，结合具体的交易场景专门化合同审查流程与重点。作为国内领先的数据交易平台，上海数据交易所一直致力于引入科技力量解决目前数据交易合规性的痛点问题，以提高交易合规性和效率。在合同审查方面，上海数据交易所结合具体的交易场景，专门化合同审查流程与重点。此外，上海数据交易所正在积极开发利用人工智能技术开发智能合约检查工具，该工具可以对合约进行自动化检查，以提高审查效率和准确性。

4.2 作为数据交易制度支撑的安全港规则

在中国的法律实践中，“安全港规则”尽管是一个常被提及的术语，但其确切含义往往模糊不清，不同领域的使用者对其理解各异，甚至对彼此之间的用法和定义缺乏足够的认知。许多法律专业人士，虽然经常使用此术语，却未能全面而深入地理解其作为一种法律技术的精髓。这一法律术语的泛用和多样性，使其在不同法律领域中的具体应用和原理探讨成为一个有待深入研究的领域。当前，安全港规则在法律领域的确切应用和界限尚不明晰，这就迫切需要从理论上对其进行深入的阐释和明确界定。

因此，在探讨上海数据交易所如何设计具体的安全港规则之前，了解安全港规则基础的理论架构显得尤为重要。安全港规则作为一种法律技术（legal technology），不仅是简单的法律条文或规则，而是一套更加复杂和细致的制度设计，旨在为受法律约束的主体提供明确、有条件的合规路径。这种技术的核心在于在一般

法律原则和行为限制之下，通过具体规则为社会行为主体指明安全的行动范围，以便在遵循规则的前提下获得法律上的免责预期。

在此基础上，下文将尝试为安全港规则提出一般性的学理解释，探讨其作为法律技术的核心特征、功能优势和设计难点，并将其与其他类似的法律技术进行必要的比较和辨析力图为这一概念提供更为清晰和全面的理解。希望通过这种方式，能够凝练出安全港设计的原则，在未来为数据交易场景下的安全港规则的具体设计和应用，提供更为坚实的理论基础。

4.2.1 安全港规则的学理解释

中文语境里人们最熟悉的安全港规则，恐怕要属已进入《民法典》的网络服务提供者侵权责任规则：当用户利用网络服务实施侵权时，网络服务提供者接到受害人通知，应及时采取删除、屏蔽、断开链接等必要措施，否则需对损害的扩大部分承担连带责任。[66]这种经常被笼统简称为“通知—删除”[67]的规则，之所以也叫“安全港”[68]，是因为其源自更早时我国网络著作权保护制度对美国《数字千禧年版权法》（Digital Millennium Copyright Act，以下简称“DMCA”）中“安全港规则”的借鉴。[69]1998 年 DMCA 出台之前，网络服务提供者原则上要为用户实施的版权侵权行为承担责任。[70]这种责任体制下，以提供免费内容为核心商业模式的早期互联网产业要面对极大的版权诉讼风浪，甚至有“翻船”之虞。作为版权与互联网两大利益集团妥协的结果，[71]DMCA 为网络服务提供者设定了可使其免于为侵权担责的路径，特别是要建立并运行一套简称为“通知—删除”（notice and takedown）、但其实包含十余项流程要素的应对机制。[72]DMCA 的安全港规则影响了多国立法。[73]我国在 2006 年制定《信息网络传播权保护条例》时将类似规则引入，[74]并在 2009 年

[66] 参见《民法典》第 1195、1196 条。

[67] 严格来说，在此类规则下，法律要求网络服务提供者接到“通知”后应采取的“必要措施”不只是删除，还有屏蔽、断开链接等。参见《民法典》第 1195 条。

[68] 或更准确地说，在这一语境中通常被翻译为“避风港”。

[69] 刘家瑞：《论我国网络服务商的避风港规则——兼评“十一大唱片公司诉雅虎案”》，《知识产权》2009 年第 2 期，第 13 页；王迁：《《信息网络传播权保护条例》中“避风港”规则的效力》，《法学》2010 年第 6 期，第 128，133 页。

[70] 参见刘家瑞：《论我国网络服务商的避风港规则——兼评“十一大唱片公司诉雅虎案”》，《知识产权》2009 年第 2 期，第 14 页；王迁文，第 129-133 页。

[71] 朱开鑫：《从“通知移除规则”到“通知屏蔽规则”——《数字千年版权法》“避风港制度”现代化路径分析》，《电子知识产权》2020 年第 5 期，第 42 页。

[72] 有关“通知—删除”所要求流程的一个简明梳理，见 Eric Goldman, Internet Law: Cases & Materials, E-version, 2021, p.159。需说明，一般认为，DMCA 第 512 条共为网络服务提供者创设了四项安全港，分别针对提供（1）传输（2）缓存（3）存储（4）信息查询检索这四类网络信息服务的服务商，而后三项安全港的使用以服务商建立通知—删除机制为前提。Pamela Samuelson, Pushing Back on Stricter Copyright ISP Liability Rules, 27 Michigan Technology Law Review 299, 306 (2021).

[73] 但 DCMA 的安全港思路也非美国原创，是受当时已出现的国际规范（WIPO Copyright Treaty）影响。See Pamela Samuelson, Pushing Back on Stricter Copyright ISP Liability Rules, 27 Michigan Technology Law Review 299, 305-307 (2021).

[74] 参见王迁：《《信息网络传播权保护条例》中“避风港”规则的效力》，《法学》2010 年第 6 期，第 128，133 页。

制定《侵权责任法》时将“通知—删除”的适用范围扩张到版权侵权之外，作为包括人格侵权在内各类场景中界定网络服务提供者责任的一般规则。[75]

或许由于网络侵权问题一向受到极高关注，“安全港规则”如今几乎被视为网络法专用术语。[76]但事实并非如此。法律界另一个常与“安全港规则”打交道的群体，是证券法领域的研究者和从业者。该领域中“安全港”之说同样来自对美国法的比较研究和译介。[77]美国证券法的核心特点是覆盖范围极广。例如，除非符合法定豁免，否则地球上任何一个角落发生的售卖证券行为，都要以根据美国 1933 年《证券法》第 5 条依法注册为前提。但在此原则下，立法不但本身已包含一系列豁免特定类型证券和交易注册要求的规定，而且还赋予美国证监会（SEC）制定更多豁免规则的行政立法权。[78]由于有关豁免规则的司法判例无法为市场主体提供足够确定性，SEC 在当代通过制定一系列更为具体明确的安全港规则，为发行人等市场主体指出可选用的豁免注册要求的交易方案。[79]又如，证券发行人所做信息披露如被认定存在虚假陈述或重大遗漏，构成欺诈，依法会面临极为严重的责任后果。但像与财务前景预测、经营战略规划等有关的所谓“前瞻性信息”（forward-looking statements），对投资者很有价值，但其准确性没人能打包票，而企业可能因担忧责任风险而披露不足。为缓解这种“寒蝉效应”，1995 年《私人证券诉讼改革法》特别为披露前瞻性信息的企业设立了一个安全港，使其可通过主动满足法定条件（如使用特定警示语言）的方式，避免被事后追责。[80]在前瞻性信息披露责任等问题上，我国已引入类似安全港规则。[81]而证券法实务界由于开展跨境业务的需求，长期系统研究并操作美国证券法，这使得他们很早就对“安全港规则”之说耳熟能详。[82]

[75] 参见《侵权责任法》第 36 条。参见陈昶屹：《“避风港规则”扩张适用网络人格权保护之困境与消解——兼论侵权责任法第三十六条之完善》，第 80 页。

[76] 笔者在写作本文过程中随机询问过几位法律学者（包括境外学者）和律师，后者均表示只在网络侵权语境中听说过“避风港”或“安全港”规则。而有关网络侵权安全港规则的中文论文则未见有提及其他领域中安全港规则的。

[77] 例如，参见冯果、洪治纲：《论美国破产法之金融合约安全港规则》，《当代法学》2009 年第 3 期；沈朝晖：《上市公司私有化退市的“安全港”制度研究》，《法学家》2018 年第 4 期，第 66 页；范晓娟：《论有限合伙基金的“安全港”规则的突破》，《政治与法律》2013 年第 5 期，第 128 页；陈洁：《“利用自身信息交易”作为内幕交易抗辩规则的建构--兼论我国内幕交易安全港规则的基本框架》，《现代法学》2021 年第 5 期，第 145 页。网络法研究者偶尔也有将“通知—删除规则”译为“安全港”的。。

[78] Thomas Lee Hazen, Principles of Securities Regulation, 3d Edition, St.Paul, Minnesota: West, 2009, pp.95-96.

79 中国法律界熟悉的如涉及向美国境外投资人或机构投资人发行证券的若干安全港规则（特别是 Regulation S 和 Rule 144A 下的安全港），可使得主要在美国市场之外开展的证券发行（例如在伦敦、香港或新加坡等主要市场发售股票或债券）免去注册负担。See Thomas Lee Hazen, Principles of Securities Regulation, 3d Edition, St.Paul, Minnesota: West, 2009, pp. 132-135.

[80] Thomas Lee Hazen, Principles of Securities Regulation, 3d Edition, St.Paul, Minnesota: West, 2009, pp.204.

[81] 《最高人民法院关于审理证券市场虚假陈述侵权民事赔偿案件的若干规定》第 6 条。

[82] 较早的系统梳理，如郭雳：《美国《证券法》注册豁免规定研究》，《金融法苑》2003 年第 6 期，第 173 页。

证券法之外，我国企业组织法、破产法、反垄断法、税法等领域的研究者，也都关注到各自领域中美国法上的安全港规则。[83]目前可查到的最早介绍美国安全港规则的文献是以国际税法为主题的。[84]而在反垄断领域，不但业界始终将修订前后的《反垄断法》中豁免纵向垄断协议的制度称为“安全港”，[85]甚至在正式规定中也已明确使用了“安全港规则”这一术语。[86]不过，上述各领域研究者也往往未能有意识地将本领域与其他领域中的安全港规则作横向联系、比较，[87]更不用说探讨安全港规则作为一种法律技术的一般制度原理。

可见，在中文法律语境中，“安全港规则”一词被应用于多个不同的法律领域，但其核心原理和特征在各领域间却往往缺乏足够的交流和比较，更未能深入探讨其作为一种法律技术的一般制度原理。鉴于此，为“安全港规则”提出一种一般性的学理解说是有必要的。

不过，美国学界就该法律技术所作的一般学理探讨同样不多见。[88]如前所述，安全港规则虽然在美国法上的应用极为广泛，[89]在收入权威的《布莱克法律词典》（Black’s Law Dictionary）时，“安全港规则”如今

[83] 例如，参见冯果、洪治纲：《论美国破产法之金融合约安全港规则》，《当代法学》2009 年第 3 期；沈朝晖：《上市公司私有化退市的“安全港”制度研究》，《法学家》2018 年第 4 期，第 66 页；范晓娟：《论有限合伙基金的“安全港”规则的突破》，《政治与法律》2013 年第 5 期，第 128 页；陈洁：《“利用自身信息交易”作为内幕交易抗辩规则的建构--兼论我国内幕交易安全港规则的基本框架》，《现代法学》2021 年第 5 期，第 145 页。网络法研究者偶尔也有将“通知—删除规则”译为“安全港”的。

[84] 参见赵金旗：《跨国公司避税行为分析及法律对策》，《河北法学》1989 年第 6 期。

[85] 例如，时建中：新《反垄断法》全面解读，《中国法律评论》2022 年第 4 期。

[86] 例如《国务院反垄断委员会关于知识产权领域的反垄断指南》第 13 条，就明确列出涉知识产权协议可不认定为垄断协议的条件，并将此称为“安全港规则”。又见市场监管总局《企业境外反垄断合规指引》（2021 年）。

[87] 一个例外，魏俊：《证券法上的安全港及其制度价值--以前瞻性信息披露为例》，《证券法苑》2014 年第 3 期。

[88] 仅有的两篇，见前引 Susan C. Morse, Safe Harbors, Sure Shipwrecks,49 UC Davis Law Review 1385,1392 (2016)，以及 Andrew Stumpff Morrison, *Case Law, Systematic Law, and a Very Modest Suggestion*, 35 Statute Law Review 159, 173 (2013). 思路相近的理论讨论，见见 Gideon Parchomovsky & Alex Stein, *Catalogs*, 115 Columbia Law Review 165 (2015).

[89] 除了前文提到的各经济法领域外，环境法、刑法等领域中也不少见。例如，在反海外腐败刑事执法体制中，跨国企业常面临本国和所在国法律差异造成的复杂合规风险，而安全港是其可借助的重要合规工具。https://www.gibsondunn.com/wp-content/uploads/2022/01/Stokes-Partridge-Michaels-Safe-Harbors-and-Other-Strategies-for-Life-Sciences-and-Healthcare-Companies-in-the-International-Anti-Corruption-Storm-ABA-The-Health-Lawyer-December-2021.pdf. 在宪法领域，美国最高法院也曾在第四修正案相关案件裁判中，为警察执法人员划出诸多可在无搜查令时开展搜查的情形，警察按要求去做，就不必担心事后被认定因搜查“不合理”（unreasonable）而违宪。See Susan R. Klein, *Identifying and (Re)formulating Prophylactic Rules, Safe Harbors, and Incidental Rights in Constitutional Criminal Procedure*, 99 Michigan Law Review 1030, 1044–45 (2001); Susan C. Morse, *Safe Harbors, Sure Shipwrecks*,49 UC Davis Law Review 1385,1392 (2016). 而联邦行政法规汇编（Federal Register）中据称每月都会出现 15 次甚至更多次“安全港”字样。Morse, pp.1391-1392

也被作为通用、而非某领域专用的法律术语。[90]或许正由于使用范围很广，这个概念在美国语境中也出现了一定程度的“泛化”，有时被论者与其他近似的法律责任豁免技术混淆起来。[91]

有鉴于此，这里首先要明确限定：下文讨论的“安全港规则”，仅指权威机关在相对原则、一般的行为限制和追责体制下，以相对具体的规则形式，为受法律约束的社会行为主体指明有限、有条件合规路径的一种法律技术；当行为主体选择在安全港范围内开展相关活动时，便可获得较为确定的免于被追究违法责任的预期。[92]

下文将进一步指明安全港规则的核心特征，并将其与近似法律技术作必要辨析。

4.2.2 安全港规则的核心特征：“有限”“有条件”的“安全”

权威的《布莱克法律词典》（以下简称“《词典》”）将安全港规则定义为“成文法或行政规章中的规则，其赋予特定对象免于赔偿责任（liability）或处罚（penalty）后果的保护”，并以前文提到的证券法上“前瞻性陈述安全港”作为示例。[93]这定义固然“权威”，但其实并不确切、充分：美国法上的安全港规则不只出自成文法和行政法规，也有由司法创设的情形；[94]更重要的是，如果只是让特定主体免于赔偿或处罚责任，那么“豁免”“除罪”之类的规范在法律中古已有之，晚近才出现的“安全港”，又有何特别？

要真正理解安全港规则的制度内涵，需要结合其产生和作用于其中的制度结构。尽管以“免责”为适用结果，但安全港规则并非追求在全面、普遍的意义上为行为主体提供其欲求的免责预期。正如这一术语在修辞层面暗示的，安全港提供的是“有限”“有条件”的安全。首先，之所以要开辟港湾，让行船人在其中感到“安全”，是因为开放海域上常有惊涛骇浪。而在提供港内安全的同时，安全港并做不到、也不追求使港

---

[90] “1. An area or means of protection. 2. A provision (as in a statute or regulation) that affords protection from liability or penalty. · SEC regulations, for example, provide a safe harbor for an issuer's business forecasts that are made in good faith. — Also termed safe-harbor clause; safe-harbor provision.” SAFE HARBOR, Black's Law Dictionary (11th ed. 2019)

[91] 例如，Morrison 曾举例，在税法上，存在以所谓“安全港”的名目，去对原本已足够清晰具体的规则作出修改的情况。见 Andrew Stumpff Morrison, *Case Law, Systematic Law, and a Very Modest Suggestion*, 35 Statute Law Review 159, 173 (2013), 第 173 页脚注 34。

[92] See Andrew Stumpff Morrison, *Case Law, Systematic Law, and a Very Modest Suggestion*, 35 Statute Law Review 159, 173 (2013); Peter Swire, *Reply: Safe Harbors and a Proposal to Improve the Community Reinvestment Act*, 79 Virginia Law Review 349, 350 (1993).

[93] “1. An area or means of protection. 2. A provision (as in a statute or regulation) that affords protection from liability or penalty. · SEC regulations, for example, provide a safe harbor for an issuer's business forecasts that are made in good faith. — Also termed safe-harbor clause; safe-harbor provision.” SAFE HARBOR, Black's Law Dictionary (11th ed. 2019)

[93] 仅有的两篇，见 Susan C. Morse, *Safe Harbors, Sure Shipwrecks*,49 UC Davis Law Review 1385,1392 (2016)，以及 Andrew Stumpff Morrison, *Case Law, Systematic Law, and a Very Modest Suggestion*, 35 Statute Law Review 159, 173 (2013). 思路相近的理论讨论，见见 Gideon Parchomovsky & Alex Stein, *Catalogs*, 115 Columbia Law Review 165 (2015).

[94] See Susan R. Klein, *Identifying and (Re)formulating Prophylactic Rules, Safe Harbors, and Incidental Rights in Constitutional Criminal Procedure*, 99 Michigan Law Review 1030, 1044–45 (2001)

外洋面的风浪一概平息。其次，获得港湾内的安全并非无需代价，而以行为人满足特定条件为前提。很多安全港往往只对符合特定资格、条件的船只开放，甚或要求驶入者支付“入场费”。不仅如此，选择进入安全港还意味着航行者付出了机会成本：进入安全港固可求得安全、定心，但也将自己束缚在相对逼仄的腾挪空间内，放弃了在更广阔天地中另行探索。

就本文讨论的安全港规则而言，“有限性”和“有条件性”是其核心特征。这两项特征同时意味着安全港规则是选用性而非强制性的——是否要借助安全港管控自身法律风险，行为人需要抉择，也保有一定选择空间。仍以被《词典》选为范例的前瞻性陈述安全港为例。这一安全港既是“有限”的，也是“有条件”的。首先，在证券法严惩信息披露欺诈的整体责任制度下，行为人因作出前瞻性信息披露而原本可能面临的法律不确定性较高。而安全港规则的有限性，体现在其仅指出前瞻性陈述可免于追责的特定情形（particular rule），因此并非免除前瞻性陈述责任的一般规则（general rule）。[95]第二，为了使用前瞻性陈述安全港，披露人必须在进行相关信息披露时配用特定警示语，提示预测可能因种种原因落空。[96]尽管这种警示语随着市场实践的发展，逐渐变得越来越标准化甚至形式化，但其仍在事实上为有意运用安全港的市场主体增加了沟通负担。近十年来，随着网络社交媒体平台的兴起，越来越多的企业开始尝试运用新兴媒介开展投资者沟通，而这类操作常可能导致前瞻性陈述落到安全港之外。最常见的情形，就是企业或高管通过社交账号发布经营计划或财务预测时，不同时搭配传统信息披露中包含的预警提示——这既可能是社交网站发帖的字数限制所致，也可能是发言者不希望啰里啰嗦的提示语影响“短频快”“造热点”“带节奏”的传播效果。由于前瞻性披露安全港的有限性和有条件性，上述行为会面临额外的法律风险。[97]但值得注意的是，在变化了的媒体条件下，会有企业为追求效率更高、效果更好的投资沟通，宁愿选择走出安全港，去承受更大的法律风险。

4.2.3 近似法律技术辨析

安全港规则是一种现代法律术语，用于减少法律责任的不确定性，为行为主体提供一定程度的免责预期。这种法律技术并不新鲜，但通过与其他技术比较，可以更好地理解其原理和特点。

1.规则细化：为了提高法律的确定性，权威机关可以将原则性规定细化为具体的规则。例如，中国在社会信用建设中使用清单和目录来细化失信惩戒制度。[98]安全港规则也是一种规则细化的形式，但它只提供有限的免责范围，而不是全面的合规或免责预期。

---

[95] 关于有限/特定（particular rule）规则和一般规则（general rule）的差别，可参看 Duncan Kennedy, Form and Substance in Private Law Adjudication, 88 Harvard Law Review 1685, 1689-1690 (1976).

[96] 当前美国上市公司年度财报通常包含长达一整页的有关前瞻性陈述有可能无法落实的提示。See Alibaba Group Holding Limited, Form 20-F (fiscal year ended March 31, 2021) , pg. x, https://www.sec.gov/ix?doc=/Archives/edgar/data/1577552/000110465921096092/baba-20210331x20f.htm#FORWARDLOOKINGSTATEMENTS_253837.

[97] 而像特斯拉公司创始人埃隆．马斯克这样常年用推特造势的明星企业家，更是曾直接“翻车”，因有关企业私有化计划的推文内容不实而被美国证监会发动执法调查。*See* SEC Settles with Elon Musk and Tesla: Time to Review Your Disclosure Controls and Procedure.

[98] 《国务院办公厅关于进一步完善失信约束制度 构建诚信建设长效机制的指导意见》（2020 年）；《全国公共信用信息基础目录（2021 年版）》；《全国失信惩戒措施基础清单（2021 年版）》。

2.模糊无效（void for vagueness）：这是一种公法领域的法律技术，用于处理法律规范含糊不清的情况。[99]当法律规范包含太多模糊之处（vagueness），人们难以判断行为是否合法，可能导致寒蝉效应（chilling effect），即人们为避免被追责而过度谨慎，连很多实际上正当合理的活动都不敢从事、开展。[100]为应对上述问题，法院可以基于模糊无效的理由否定这类规定的法律效力。[101]与此相比，安全港规则提供的是有限、有条件的免责例外。

3.完整免责（full immunity）：这是立法者通过制定明确的免责条款来消除责任不确定性的方法。例如，美国《通讯风化法》中的网络服务商免责规定，提供了与安全港规则不同的免责预期。[102]与此相比，安全港规则提供有限、有条件的免责，而《通讯风化法》则提供了更广泛的免责。

4.有限豁免：与安全港规则相比，有限豁免规则在法律中很常见，如基于年龄或精神状况的刑事责任豁免。[103]这些规则的适用条件通常是客观事实，如年龄或疾病状态，而安全港规则则要求行为人主动满足某些条件。

5.监管沙盒（regulatory sandbox）：监管沙盒，源自金融监管领域，是政府划定的一个实验区域，允许金融科技企业在此测试创新产品和服务。这种制度最早在英国出现，后来扩散到全球多个国家和地区。[104]监管沙盒的实施流程包括提交测试申请、沟通协商、正式测试和测试结束后退出，企业需向监管部门提交申请，说明其金融科技的创新性和安全性，监管部门评估后，与企业协商确定测试的具体内容、时间安排和风险管理，测试期间企业自主测试，同时报告进展和风险，接受监管，测试结束后监管部门评估总结，为未来政策提供参考。[105]监管沙盒的设计初衷是为金融科技创新提供测试空间，重点在于特定场景下的创新测试，而非普遍适用的交易规则框架。相比之下，安全港规则所追求的是更普遍、常态化的交易环境。

总结来说，安全港规则作为一种普遍适用的法律技术，旨在减少法律责任不确定性。它通过为行为主体提供有限、有条件的免责预期，与其他法律技术如规则细化、模糊无效、完整免责、有限豁免和监管沙盒相区别。

4.2.4 安全港规则的功能优势

既然安全港规则并非权威机关为行为主体提供免责预期的唯一可用法律技术，那么选择使用安全港规则，可以并应当以其所具有的何种比较优势为依据？

---

[99] *See* United States v. Williams, 553 U.S. 285, 304 (2008); Cass R. Sunstein, *Problems with Rules*, 83 California Law Review 953 (1995).

[100] *See* Reno v. American Civil Liberties Union, 521 U.S. 844, 870-871 (1997).

[101] 例如，根据美国宪法判例法，政府若制定规制某些言论表达的法令，即使相关表达就其性质（如属于色情或商业言论）落在宪法保护范围之外，但若法令对规制对象的界定过于模糊、宽泛，法院仍然可据此宣告其违宪。*See* Reno v. American Civil Liberties Union, 521 U.S. 844, 870-871 (1997).

[102] See Anupam Chander, *How Law Made Silicon Valley*, 63 Emory Law Journal 639, 652(2014).

[103] 《刑法》第 17 条、18 条。

[104] 参见胡滨、杨楷：《监管沙盒的应用与启示》，载《中国金融》2017 年第 2 期，第 68 页。

[105] 参见张景智：《“监管沙盒”制度设计和实施特点：经验及启示》，载《国际金融研究》2018 年第 1 期，第 58 页。

预期与安全

由笼统的责任或处罚规定导致的不确定性，理论上都是可以借助“模糊无效”或“完整豁免”这类策略全面消除的。但不难想见，若觉得合法和违法行为之间的界线很难足够合理确切地划定，便一概不追责，这种做法必然导致涵盖不足（under-inclusiveness），即部分应被问责、处罚的行为会逃脱责任后果。在宪法和刑法等公法领域中，权威机关通常明知前述涵盖不足的存在，并有意识地选择接受对应成本，将其作为必要代价，以求避免涵盖过宽（over-inclusiveness）——正当合理的行为被过宽地划入有责、应罚范畴——以及由此导致的寒蝉效应。

之所以在公法领域中，权威机关取舍两类偏差时立场鲜明，是因为相关问题常涉基本权利保护，后者在当代法治语境中获得较为明确的价值偏向。然而在其他更多领域，决策者权衡两类偏差时未必能参照有广泛共识的价值立场。以网络侵权责任体制为例，如前所述，美国立法者在二十多年前选择以完整豁免的策略，寻求全面消除企业面临的责任不确定性。但随着网络活动伴生的社会风险日益加剧，这种一刀切的免责体制近年来受到越来越多批评和反思，被认为其在降低经营者法律风险与保护社会免遭侵害之间，过度倾向了前者。[106]

当然，“既要又要”总是困难的。但如何妥善应对包括数据技术、人工智能、基因科技等在内的既蕴含潜在风险又具有创新价值的活动，对当代规制政策而言，其实是常见挑战，也没法都靠一刀切方式解决。若决策者寻求在两类错误间做更精细权衡，兼顾制度的一般性和客观预期，那么安全港规则是一个有吸引力的方案。[107]相较于完整免责或模糊无效，安全港规则提供的免责预期是有限的，其能够克服的涵盖过宽在规模上也更有限。[108]但至少对于愿意选择进入安全港开展相关活动的主体而言，宽泛或模糊责任规则产生过度威慑和寒蝉效应的担忧，都会变得可控。与此同时，安全港规则相对完整免责类规则的优势在于，其使用不会彻底废除或颠覆具有原则性的问责或处罚体制。当责任或处罚规定的原则性和一般性（generality）够强时，其威慑效果才能更完整地覆盖各类行为主体及其活动，避免有太多或太明显的“漏网之鱼”。[109]不仅如此，原则性责任规定的确立和保存，还可一般性地向社会提示相关活动的风险属性，并明确地宣示法律对安全这一底线价值的关切和坚持。这种表达功能（expressive function）常常是决策者实际关注、也有理由通过责任规定追求的。[110]

激励安全投入

[106] See Danielle Keats Citron,*How To Fix Section 230*, Virginia Public Law and Legal Theory Research Paper No. 2022-18,2022, available at SSRN: https://ssrn.com/abstract=4054906.

[107] See Andrew Stumpff Morrison, *Case Law, Systematic Law, and a Very Modest Suggestion*, 35 Statute Law Review 159, 173 (2013), p174 页.

[108] 参见。See Susan C. Morse, *Safe Harbors, Sure Shipwrecks*,49 UC Davis Law Review 1385,1392 (2016), p1420 页.

[109] See Duncan Kennedy, Form and Substance in Private Law Adjudication, 88 Harvard Law Review 1685, 1689-1690 (1976), p1690.

[110] Cass R. Sunstein, *On the Expressive Function of Law*, 144 University of Pennsylvania Law Review 2021, 2034-2036 (1996)

有限性之外，安全港规则的另一结构性特征是有条件性，即其适用以行为主体采取法律指明的积极合规作为为前提。正因如此，安全港规则的一个比较优势，是其具有其他免责或豁免规则所不具备的行为激励和引导功能。一个人无法为了免票或免责改变自己的身高或年龄，但一个网站可以为了免于在用户侵权时承担连带责任，而根据安全港规则的要求建立适当的“通知—删除”机制。而网站投入成本建立能够实际运转的“通知—删除”机制，至少可使得侵权风险预防和纠纷化解有一个看得见摸得着的抓手。换言之，经营者在法律规则的激励下作出的这种投资，是具有安全价值的。一个更加极端但也可能更容易理解的例子，则是包括我国在内许多法域都曾尝试施行的弃婴安全港法律（“safe haven laws”）。弃婴行为在所有国家几乎都构成刑事犯罪，但因各种社会经济文化因素（如贫穷、医疗水平落后乃至歧视等）而无法根除禁绝。在这种无奈现实面前，一些法域选择在刑事处罚的原则之下设立安全港，有意弃婴者只要在规定时间期限内将婴儿送到指定接收地点（主要为医院、福利院等机构），即可不被追究法律责任。[111]不难想见，弃婴者按照法律指定的方式交付婴儿，比自行随意丢弃要更“费事”——但这多付出的“心力”对提升弃婴人身安全的边际价值很大，以至于权威机关宁愿为此付出不究刑责的“价码”。

此外，安全港规则产生行为激励或引导作用，不仅因其可提供免责预期，还因其便利了社会和市场中行为主体发送有关自身合规意愿的信号。通过作出积极投入、选择满足安全港适用条件的行为方式，行为主体可以向监管者与其他利益相关方发送信号，表明其具有注重安全、追求合规的属性，从而可使自身与其他偏好冒险、不选择适用安全港的主体区别开来。在日益强调企业社会责任的市场环境中，许多企业都会关注这种信号机制。也正因如此，安全港规则还会创造有利于大量诚信主体协调行动的聚焦点（focal point），[112]从而在群体层面促成追求安全的行为人与不安全行为人之间的分离均衡。[113]

正因为安全港规则具有行为激励功能，因此权威机关在设计特定安全港规则的适用条件时，应考虑相关风险活动以何种方式开展，会产生防范风险、降低损害的安全收益，并由此值得法律以提供免责预期的方式予以激励。不过，从原理上讲，之所以权威机关会选择采用安全港，本身就是因其无法系统、细致地区分危险和安全行为。但安全港规则的有限性，又意味着决策者只需要能正面识别出少量甚至个别值得激励的安全活动模式即可——这大大降低了规则制定的难度。

规则生产的边际模式

实体效果之外，安全港规则在生产过程这一维度也有优势。通常而言，若法律规范在订立时采取相对粗疏、原则性的标准（standard）形式，则立法环节权威机关所需信息不多，但守法和执法环节相应主体要承担较高信息成本，才能搞清楚规范如何适用于具体情形。反过来，如果法律规范在订立时就追求清晰明白、界定精准（而非粗暴一刀切）的规则（rule）形式，那么立法者需要处理的信息就相当可观，守法和执法环

[111] Carol Sanger, *Infant Safe Haven Laws: Legislating in the Culture of Life*, 106 Columbia Law Review 753, 762-772 (2006).

[112] See Susan C. Morse, Safe Harbors, Sure Shipwrecks,49 UC Davis Law Review 1385,1392 (2016), p.1397.

[113] T. Randolph Beard et. al., *Safe Harbors and the Evolution of Online Platform Markets: An Economic Analysis*, 36 Cardozo Arts & Ent. L.J. 309, 312 (2018).

节的信息成本却可大幅降低。[114]结合这一视角观察可知，法律生成和运行的全过程中，信息成本不可能完全消除，而提高制度效率的思路，无非是结合具体语境，考虑在哪个环节投入信息处理成本的产出更高。[115]

但值得强调的是，特别是在行政国家（administrative state）语境中，制定具有一般适用效力的法律规范的动态过程，并非在狭义的“立法”完成后告终。狭义立法之后，行政机关和司法机关通常还会继续为生产规则投入资源，例如行政机关在宽泛立法文件之下出台细则，或法院在裁判案件时通过“解释”的方法填充立法规范中的间隙甚至空洞。这些狭义立法环节后的投入，同样应被理解为规则生产这一动态过程的必要组成部分。而由于信息在这一过程中是不断积累、增加的，这使得后续的立法投入往往比最初在狭义立法环节的投入具有更高产出效率。[116]

而安全港规则正是一种典型的借助信息动态累积的原理提高规则产出效率的技术。有学者曾分析指出，安全港规则虽常由立法机关和行政机关制定，但其逻辑有判例法的味道：判例法体制下，逐次形成的司法先例，每一个都可以理解为是向背景中的宏观规范增加了事实信息后获得的具体规则。[117]而在安全港规则的动态制定过程中，立法机关即使最初面临过高不确定性，无法掌握足够信息实现精准立法，也可以出于防范风险的审慎态度，先订立原则性责任规范，并授权行政机关在后续信息条件积累的动态过程中，以设置一个又一个安全港的方式，逐步划出更为清晰的边界，为社会提供其需要的免责预期。甚至，如果在更大尺度的坐标中审视这种动态过程，可以认为，安全港规则的逐个、边际积累，最终能为全局性变革提供条件：某种意义上，中国改革进程中常用的“特区”“试验区”“自贸区”等策略，可以被理解为“大号”的安全港；一旦旨在为具有创新价值和政策风险的活动提供宽松责任环境的特区遍地开花，便自然会打开整体改革的局面。

4.2.5 安全港规则设计的难点

安全港规则虽是在防范社会风险与稳定个体预期之间寻求平衡的一种可行策略，但“可行”不等于效果有保障。说到底，之所以要诉诸这样的技术，恰是因为法律的制定和运行都不处在“理想”环境之中：权威机关在现实条件下不仅面临严重信息约束，也深嵌在纠缠的利益格局之中。这意味着任何具体安全港规则，其设计和实效都可能偏离最优。

“过宽”“过窄”“过低”“过高”

基于安全港规则有限和有条件的特性，可预见其最容易出现的偏差，主要应是有限的免责范围被划定得过宽或过窄，和/或适用的条件门槛被设置得过低或过高。

具体来看，一方面，既然安全港规则的比较优势在于保留原则性责任规定及其威慑效力，那么安全港覆盖的活动开展方式在范围上应是有限的——至少要比背景中的一般责任规范覆盖更窄。在此前提下，究竟设

[114] See generally Louis Kaplow, Rules versus Standards: An Economic Analysis, 42 Duke Law Journal 557(1992), pp579-584.

[115] See generally Louis Kaplow, Rules versus Standards: An Economic Analysis, 42 Duke Law Journal 557(1992), pp621-622.

[116] Gideon Parchomovsky & Alex Stein, Catalogs, 115 Columbia Law Review 165 (2015), pp.171-172, pp.188-190.

[117] See Andrew Stumpff Morrison, Case Law, Systematic Law, and a Very Modest Suggestion, 35 Statute Law Review 159, 173 (2013), p169, pp173-174.

置多少个安全港，涵盖多少种被认为相对安全的活动方式，取决于权威机关的认知和判断。过于保守的机关设定的安全港，其范围可能极为有限：在安全港外，还有其他可被识别、界定的值得获得免责预期的活动方式。例如，DMCA 的“通知—删除”避风港，就曾被批评为“过窄”，只覆盖其制定当时存在的主流网络中介，却未能有效保护其后迅速出现并流行的新型网络传播平台（如 P2P）。[118]而过于激进的决策者则可能急于设立过宽的安全港，导致某些风险不低的活动方式也能获得安全港庇护。在刑事程序领域，美国执法机关曾在一系列有影响力的案件中主张法院应以安全港规则的形式，为警察调查执法活动的合宪性提供更高确定性，但法院往往犹豫，担忧如此一来警察的过度执法行为就会缺乏足够约束。[119]安全港过窄时，相关活动会被抑制在过低水平。安全港过宽时，原则性责任规定则会变得千疮百孔，甚至遭到虚化，导致风险在安全港范围内以相对隐蔽的方式累积、增加。

另一方面，设置安全港规则的适用条件或门槛时，把握“刚刚好”的分寸同样不容易。门槛若设得太低，甚至无需行为主体付出足够努力即可迈过，则安全港会变得与完整豁免差异不大，激励、引导安全行为的作用也会不足。即便相关条件需要选择使用安全港的主体付出成本，这些投入也可能缺乏风险防范和控制方面的实际产出，属于“表演合规”般的表面功夫，甚至沦为以形式合法掩盖实质规避的套路。[120]前文提及的证券法上前瞻性披露安全港，一度曾面临的批评就是相关要求被做过于形式化的理解和适用，以至于有些明知披露信息不真实的发行人都可以通过使用警示而免于追责。[121]而曾用于为美国企业提供明确的欧洲数据法合规路径的隐私安全港框架，也被批评为其包含的实质性合规要求不够高，乃至被欧洲法院判定无效。[122]反过来，如果安全港规则设定的适用门槛过高，以至于绝大多数行为主体都无法在成本合理的前提下寻求满足安全港适用条件，这种过于昂贵的安全港规则会被“绕行”。例如，DMCA 安全港，实际上并不像“通知—删除”这个名称听上去那样简单；按要求建成并持续运行全部机制，对大平台而言成本可以接受，对小网站来说却过于昂贵，因此实际上严格照办者不多。[123]此外，更微妙的是，如果安全港要求行为主体投入的成本对

[118] See Mark A. Lemley,Rationalizing Internet Safe Harbors, 6 Journal Telecommunication & High Technology Law 101, 112 (2007), p.113.

[119] See Susan R. Klein, Identifying and (Re)formulating Prophylactic Rules, Safe Harbors, and Incidental Rights in Constitutional Criminal Procedure, 99 Michigan Law Review 1030, 1044–45 (2001), p.1046.

[120] See Duncan Kennedy, Form and Substance in Private Law Adjudication, 88 Harvard Law Review 1685, 1689-1690 (1976), p.1696.

[121] Adding Meaning to "Meaningful Cautionary Statements": Protecting Investors with A Narrow Reading of the PSLRA's Safe Harbor for Forward-Looking Statements, 84 Temple Law Review 481, 499-501 (2012).

[122] Dr. Nora Ni Loidean, The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law, 19 J. Internet L. 1, 10 (2016)

[123] Sarah E. Jelsema, How Websites Can Reduce Their Copyright Infringement Liability for What Users Post, Utah B.J., November/December 2014, at 14. 甚至，由于通知删除安全港适用的条件复杂，即使网站力求选用，也常免不了被拖入诉讼、由法院确认其已符合安全港要求，这更使得选用安全港对许多中小网络服务提供者而言不足够划算。See Eric Goldman, Internet Law: Cases & Materials, E-version, 2021, p.179 页.为了降低 ISP 适用安全港的门槛,有些国家的安全港比 DMCA 的通知删除要求更低,只需要“通知—通知”。See Pamela Samuelson, Pushing Back on Stricter Copyright ISP Liability Rules, 27 Michigan Technology Law Review 299, 306 (2021), p.308.

其自身而言可以接受，能够带来足够高的免责预期，但这种投入产出的社会安全收益却低于投入本身——即“私人收益>私人成本>社会收益”——此时安全港门槛也可被认为设置得“过高”了，但其后果与前述门槛“过低”时类似，即导致了无效率的合规投入。

规则制定的政治经济学

为什么安全港规则会出现范围“过宽”“过窄”、门槛“过高”“过低”的偏差？如前所述，安全港规则本身是权威机关在信息条件不完美的现实面前做出的妥协；既然条件有限，无法克服“高迪洛克规制难题”（Goldilocks Regulatory Challenge）[124]自然不令人意外。此外，由于同一个原则性责任体制下的诸多安全港规则，可能是由不同的后续规则制定者分散、逐步制定出来的，这也使得它们叠加在一起时，会出现相互冲突，由此可能反而会提高行为主体的合规难度。[125]

但值得注意的是，除了客观条件约束，偏差背后也可能存在利益冲突因素。真实世界中的规则制定不必然以追求公共利益为宗旨。具有规则制定职权的机关被规制对象及其背后的特殊利益集团“俘获”（capture），[126]“下不了手”或“网开一面”，都不是新鲜事。有足够影响力的特殊利益集团，完全可以推动权威机关在制定一般性责任规范的同时，借安全港之名给自己单独开个“口子”，留条“出路”。在此背景下设定的安全港，范围自然可能过宽，门槛也可能过低，从而满足相应主体以最低成本获得免责预期的需求。

相对不那么直观的是，范围过窄、门槛过高的安全港规则，同样可能是特殊利益影响的结果。在模糊、原则性的责任或处罚规定导致各类社会行为主体均面临较高不确定性的情况下，少数群体获取最大竞争优势的策略，未必是推动设立范围宽、门槛低并因此具有“普惠性”的安全港，而是谋求规则制定者为其“量身定制”：对特殊利益集团而言，最理想的安全港，应恰好窄到仅覆盖他们偏好的活动模式，并设置只有他们才能跨过的高门槛。换言之，过窄、门槛过高的安全港规则，本身可能是利益集团为排斥竞争设置的壁垒。

还需指出，偏离最优的安全港规则，除了可能是初始设计时便已有利益驱动甚至操控所致，也完全可能是路径依赖的结果。基于特定时期信息条件及对应认知设立的安全港，即使在设立时合理、适当，也可能随着时间推移和情势变化而逐渐不合时宜。但由于既有安全港被相关领域中的合规主体反复使用，后者不但得了甜头，还可能已做出为使用该项安全港的专属投资（specific investment），由此有动力祭出“保护稳定预期”的名目，反对决策者对既有安全港作适时调整、变更乃至废止。这种局面对决策者的判断和魄力无疑都是很大考验。

4.2.6 安全港规则设计的原则

认识到安全港规则可能出现偏差，有助于为这种法律技术找到恰如其分的制度定位。说到底，用或不用，以及怎样设计使用，取决于权威机关如何考量多重制度目标并对其加以取舍。决策者需要清楚地意识到，若

[124] Orly Lobel, *The Law of the Platform*, 101 Minnesota Law Review 87,156-157 (2016).

[125] *See* Mark A. Lemley,*Rationalizing Internet Safe Harbors*, 6 Journal Telecommunication & High Technology Law 101, 112 (2007), p.108.

[126] See Susan C. Morse, Safe Harbors, Sure Shipwrecks,49 UC Davis Law Review 1385,1392 (2016), pp. 1427-1428.

要追求何种目标，不得不承受哪些代价甚至牺牲。而基于对可能出现的制度偏差的认知，此处还可初步提出若干有助于优化安全港规则设计和适用的基本思路或原则。

首先，安全港规则在设立和适用层面，均应确保公开透明。权威机关旨在通过安全港规则为行为主体提供的免责预期，不应是以隐蔽方式传授少数“关系户”的窍门或秘诀。而除了有助于避免安全港沦为照顾特殊利益的法律漏洞，公开透明也是其有可能激励、引导行为主体有效安全投入的前提。如果缺乏公开性，或者要求不够清晰透明，这类安全港本身也不会好用，无法真正为行为主体提供需要的免责预期。[127]

其次，安全港规则设置的适用条件，既要有可操作性，也应确保行为主体需要付出足够成本和努力。如前所述，安全港为行为主体提供的免责确定性不应是免费的，行为主体为此需要向社会付出的对价，是其根据要求采取的行为具有风险控制或安全价值。[128]同时，如前所述，愿意为使用安全港付出成本，也是行为主体发送的表明合规意愿的信号。只有不过于廉价、投资可观察验证的安全港，才能发挥信号功能，进而促成分离均衡。

第三，安全港规则在设置时应考虑配备动态评估和调整机制，例如规定由特定权威机关在一定周期内评估安全港规则的适用情况和效果，了解其是否被广泛使用，是否起到了提高法律确定性和引导防范风险行为等积极效果，以及是否应根据客观社会经济或技术条件的变化而在未来周期内不继续沿用、需加以调整甚至废止。安全港规则本意在充斥不确定性的宏观环境中为人们提供有限的确定预期，因此不宜朝令夕改，否则便背离初衷。但话虽如此，安全港规则提供的确定预期毕竟是有限的。“有限性”其实还意味着安全港难免“权宜之计”的属性，是开放而非封闭的法律系统[129]动态应对风险的策略，没必要被单独固化下来，否则反可能与特殊利益绑定。尽管设计具体的动态调整机制有其复杂之处，但总体而言，若要兼顾预期保护和与时俱进，安全港规则应就调整周期、内部检讨和外部评估程序、过渡安排和溯及力等事项，做出明确规定。

最后，安全港规则的设置权限，除了由立法机关享有外，也应基于立法明确授予处在相关领域监管一线的行政机关。[130]相对于立法机关，行政机关设计安全港规则的核心优势在于其有更充分的信息条件，可结合现实因素，指引更具可操作性和风控实效的合规行为模式，并适时予以调整。从信息角度来看，行政机关比立法机关更有能力避免安全港规则出现“过宽”“过窄”“过高”“过低”的问题。当然，对行政机关做出立法授权，会对应由此产生的代理成本，例如立法机关需要被行政监管机关遭特殊利益俘获的风险予以关注，并保留问责可能。但即便如此，行政机关获得明确的充分授权，对于安全港规则实际创设免责预期是必要的——如果没有授权，行政机关提供的免责例外，可能沦为前文所说的“不太安全港”，无法为行为主体提供充足信心，也难以避免寒蝉效应。

---

[127] See Susan C. Morse, Safe Harbors, Sure Shipwrecks,49 UC Davis Law Review 1385,1392 (2016), pp.1394-1395.

[128] 参见吴伟光：《视频网站在用户版权侵权中的责任承担--有限的安全港与动态中的平衡》,《知识产权》2008 年第 4 期，第 62 页。

[129] See Andrew Stumpff Morrison, *Case Law, Systematic Law, and a Very Modest Suggestion*, 35 Statute Law Review 159, 173 (2013), p172.

[130] 我国法院理论上完全可以用司法解释的形式订立可一般适用的安全港规则的情况，而这与行政机关制定安全港机制有类似之处，却与英美语境中法院以判例法形式创设安全港不同。限于篇幅，本文暂不讨论基于司法解释创设安全港可能存在的与司法机关制度定位有关的一些特殊问题。

五、探索之路：安全港规则在上海数据交易所的应用

推动数据交易只需订立责任承担规则，不需建构财产权属规则，并不意味着前者轻而易举。数据交易及其促生的新型数据处理活动有何种致害风险，在当下和未来本身不确定，这使得法律无法为数据交易活动一揽子划定合法/不合法、有责/不担责的边界。目前来看，包括《个人信息保护法》《数据安全法》《网络安全法》等在内的信息数据领域基础性法律，已建构出一个强调风险预防、损害问责的原则性制度框架。这一框架的基础规范内容，就是任何主体在从事包括数据交易在内的数据处理活动时，应对风险和损害后果有概括性认知，由此以负责任的态度开展相关活动。[131]

这种体现风险防范共识的制度框架不可或缺，但其笼统和模糊的形式当然难以满足市场主体对更高法律确定性和可预期性的需求。而设计并施行范围有限、条件合理并动态调整的安全港规则，应是当前条件下有助于推动交易起步的一种务实方案。类似方案在域外已有落地的先例[132]，而此前国内研究者也提出过建立“数据安全合规的责任豁免”制度，以体现包容审慎的监管思路。[133]这与安全港规则的方案思路相通。具体而言，法律可设定原则规范，要求市场主体在交易前、中、后就数据隐私、数据安全和网络安全承担保障责任。在此基础上，立法机关和/或监管部门可考虑为市场主体指明至少一条供其选择的合规路径，并为选择以相应方式开展数据交易活动的主体提供合规确认或免责预期——即赋予该合规路径以安全港规则的法律地位。

具体而言，在规则层面，对于“驶入”安全港的数据交易活动，权威机关应就参与交易主体划定范围，并对交易活动开展方式提出特定要求。例如，交易主体应具备特定合规资质（包括一般经营资质和数据领域安全资质等）和合规记录（包括一般公共信用记录和信息数据领域违法记录等）；数据提供方应就数据来源作出合规披露和保证（如已取得授权、已完成脱敏等）；数据获取方应就数据用途作出合规披露和保证（如对主要用途的描述和对特定高风险用途的排除），并承担持续经营信息报备义务等。而交易主体在满足上述要求的前提下开展的交易，即可基于安全港的效力，对与交易相关的数据处理活动导致的损害，享有免责预期。

上述各类规定，初看似乎只是常见数据合规要求，但将其明确组合适用时，就可以开辟出有实质且鲜明效力边界的安全港，其既不对所有数据交易开放，也不会让有意驶入的交易参与方都感到合规不费吹灰之力。例如，尽管提供方和获取方的合规保证，其内容可靠性很难在做出当时审查，但在需要为虚假披露承担事后责任的前提下，交易方敢于做出细致披露和具体保证的前提，是其在专业人员指导下，建立、执行内部合规制度与流程——而这些投入本身具有降低交易活动数据风险的价值。数据交易安全港的范围宽窄和门槛高低，取决于决策者有关数据交易风险和收益的偏好、认知与权衡。如前所述，由于技术环境快速变动，要求决策者通盘权衡并全面规范各类数据交易活动的风险与收益，难度极大。但结合已有信息，在有限范围内识别出一些风险可控的交易主体和交易方式，在此基础上设立安全港，可行性更高。

[131] 例如《个人信息保护法》第 9 条规定：“个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。”

[132] See 27.04[6][H]Ohio's Data Security Safe Harbor Law, 3 E-Commerce and Internet Law 27.04[6][H] (2020 update).

[133] 参见杨力：《论数据交易的立法倾斜性》，《政治与法律》2021 年第 12 期，第 9 页。

不过，相比证券交易等实践较为成熟、信息积累较为充分的市场活动，数据交易的风险仍处于被市场、社会和监管者充分理解的过程中，因此即使是设计和运行安全港，也有相对更高的难度。合理性不足的安全港规则，其过宽、过窄、过高、过低的问题，可能在施行后才会显露出来。这意味着数据交易安全港需要相对更灵活的动态调整机制——但这又会对规则可预期性和制度可信赖性提出挑战。基于此，数据交易安全港规则的设置和运行，在当前需要借助可信中介，以实现安全性和灵活性的优化组合。这种结构性的制度需求是数据交易所探索发展前路的契机。

总结而言，虽然安全港规则在数据交易领域的具体实施存在挑战，但具体讨论它的设计和应用却是十分必要的。在对安全港规则的核心特征有深入的了解之后，接下来将进入到更具体的领域——安全港规则与监管沙盒制度的区别、创新容错机制的具体应用以及法律经济学对数据交易的影响。这些详细讨论将让数据交易所更精确落地这一法律技术。

在探讨这些细节之前，重要的是要认识到，安全港规则不仅是理论上的构想，而是有望通过中央政府鼓励的创新容错机制，在实践中找到落地的可能性。这不仅需要对安全港规则的法律框架有深入的理解，也需要将其与现实中的数据交易实践结合起来，寻找最佳的实施路径。

5.1 落地路径：创新容错机制与安全港规则

讨论安全港规则在数据交易所的应用和落地前，必须先关注中央对创新容错机制的重视。正是这种机制的推广和实施，使得安全港规则成为现实可能，而非单纯的理念探讨。因此，在探讨安全港规则如何在数据交易场景中落地之前，有必要先理解中央对创新容错机制的重视，这为安全港规则的成功实施提供了坚实的政策基础。在此基础上，上海数据交易所等机构可以在符合国家大政方针的前提下，勇于创新，探索符合中国特色的数据交易模式。

《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》（“《数据二十条》”）第 19 条规定，“采用‘揭榜挂帅’方式，支持有条件的部门、行业加快突破数据可信流通、安全治理等关键技术，建立创新容错机制，探索完善数据要素产权、定价、流通、交易、使用、分配、治理、安全的政策标准和体制机制，更好发挥数据要素的积极作用。”该条在数据交易的场景下，确立了创新容错机制，“鼓励各参与主体创新开展数据流通交易工作。”[134]这一政策不仅鼓励数据流通交易的创新尝试，还为数据交易所等机构提供了探索和实验新模式的空间。

回顾中国改革开放的历程，创新容错机制一直是改革的重要组成部分。自党的第十八届三中全会强调“鼓励地方、基层和群众大胆探索，加强重大改革试点工作，及时总结经验，宽容改革失误”以来，总书记多次强调建立和完善“容错机制”，旨在为改革提供更大的灵活性和试错空间。2013 年 11 月，党的第十八届三中全会发布《中共中央关于全面深化改革若干重大问题的决定》，强调要“鼓励地方、基层和群众大胆探索，加强重大改革试点工作，及时总结经验，宽容改革失误”。[135]随后，总书记又在多个场合都提到类似主题，

[134] 周民：《完善数据要素治理制度，保障数据流通交易安全<数据二十条>解读》，中华人民共和国国家发展和改革委员会，2022 年 12 月 20 日，https://www.ndrc.gov.cn/xxgk/jd/jd/202212/t20221219_1343659.html。

[135] 《中共中央关于全面深化改革若干重大问题的决定》，载《人民日报》2013 年 11 月 16 日，第 1 版。

从最初的“宽容改革失误”到倡导建立“容错机制”并要求完善“容错纠错机制”，体现了中央对于改革事物的重视。[136]

这种政策背景下，上海数据交易所得以在合适框架内，对安全港规则进行创新性实践。安全港规则不仅可以有效保障数据交易的安全性和隐私性，还能够吸引更多的市场参与者，推动数据要素市场的发展。创新容错机制对于数据交易场景而言是一项有力的政策支持，其使得上海数据交易所在不违背党和国家大政方针的前提下进行一些具有开创性的尝试，从实践的角度切实解决数据交易过程中遇到的具体问题。

通过创新容错机制，上海数据交易所有机会在中国特色的数据交易领域内开展开创性的实践，探索适合国内市场的最佳实践。由于数据在生产、流通、使用等过程中，个人、企业、社会、国家等相关主体对数据有着不同利益诉求，并且呈现复杂共生、相互依存、动态变化等特点，当前的具体法律法规并不能完美一一对应实践中出现的具体问题，因此需要具体的行动者在具体的场景中进行具体的判断。在多次实践证明相应的行为模式整体来说有利于行业的进一步发展后，便有可能将上海数据交易所的实践上升为在更广大范围内推进的规则。

正如下文将要提及的，创新容错机制有助于上海数据交易所为数据场内交易实践安全港规则。安全港规则是一种保护数据交易安全和隐私的政策措施，可以吸引更多的数据交易参与者。然而，要实施这样的规则，需要各部门的密切配合和协同努力。只有在多个部门的支持下，才能探索出最符合中国特色数据交易的最佳实践。在推进安全港规则的过程中，需要与数据保护部门、技术专家、法律机构等合作，确保数据交易的合规性和安全性。同时，还需要与相关部门共同制定和完善数据要素产权、定价、流通、交易、使用、分配、治理、安全的政策标准和体制机制，以确保数据交易的顺利进行。通过创新容错机制，上海数据交易所可以积极探索和试验各种政策和机制，以找到最适合中国特色数据交易的路径。这将为数据交易市场的发展提供更多机遇和可能性，并促进数据要素的积极作用在经济和社会发展中的充分发挥。

5.2 安全港规则激活数据交易的制度价值

在探讨数据交易和安全港规则时，首先需要理解经济学和法律的基本逻辑。经典法律经济学理论指出法律责任会影响个体的行为模式，例如，当人们开车时，他们会考虑自己是否应该承担责任，是否有过失，以及这些责任如何影响他们的驾驶注意力和行为。[137]法律责任除了会影响行为人的注意力之外，法律责任也会影响行为的活跃度，即“行为水平”。

在过失责任下，人们被要求采取合理的注意力，但在严格责任下，人们可能仅限于合理的注意力范围，因为超出合理范围的额外注意力带来的收益逐渐减少。Shavell 的研究进一步表明，严格责任可能会降低行为人的行为意愿。[138]将这一理论应用于数据交易领域，安全港规则的目的是在确保交易安全的同时提高交易主

[136] 参见李蕊：《容错机制的建构及完善——基于政策文本的分析》，载《社会主义研究》2017 年第 2 期，第 90-91 页。

[137] See Shavell, Steven. "Strict liability versus negligence." In *Economics and Liability for Environmental Problems*, pp. 89-113. Routledge, 2018.

[138] Shavell, Steven. "Strict liability versus negligence." In *Economics and Liability for Environmental Problems*, pp. 89-113. Routledge, 2018.

体的活跃程度。如果交易主体承担的责任过重，可能会导致他们在交易活动上的参与度下降，从而抑制整体交易活动的发展。安全港规则通过明确的制度设计，旨在提升交易主体的行为水平，实现数据交易的安全性与规模的有效平衡，这与 Shavell 的观点相呼应，即责任规则应激励更高效和安全的行为模式。

此外，提升注意水平同样重要，意味着诸如上海数据交易所等机构需要提供数据合规审查等服务，以降低数据交易风险。安全港规则追求的不仅是数据的客观安全，更重要的是找到数据交易安全风险与交易规模之间的平衡。这种平衡可能通过制度设计而非仅仅技术手段来实现。

综上所述，引入安全港的目的是促进数据交易行为的边际变化。在其他条件不变的情况下，这样的制度变化可带动交易规模增长。制度变化旨在确保交易所在承担适当责任的同时，能够维持甚至提升交易主体的活动，从而最大化经济效益和社会福利。

然而，即使在政府暂时无法完全实施法律意义上的安全港规则的情况下，选择在正规交易所进行数据交易对企业而言仍具有重要的声誉价值。这是因为，正规交易所的严格安全措施和审查机制不仅保障交易透明和公正，也体现了企业对数据安全和隐私保护的承诺。在公众对数据安全高度关注的当今社会，企业的数据处理方式直接关系到其声誉。

因此，即使在安全港规则未完全落地的情况下，企业通过选择正规交易所进行数据交易，本身就是对市场的一种积极信号——这表明企业不仅重视数据安全，而且愿意承担超越法律基本要求的社会责任。当今商业环境中，企业社会责任（ESG）已成为企业长期成功的关键，ESG 涵盖环境、社会和治理三大领域，其中数据安全和隐私保护是企业社会责任的重要组成部分。在这一背景下，企业的剩余责任意识成为关键因素。

数据交易作为现代商业活动的常态，具有其固有的复杂性和风险性。企业在从事数据交易时不仅需遵循法律法规，以规避法律纠纷和罚款，还需要展现出对社会责任的承担，超越法律的基本要求。选择在正规交易所而非黑市进行数据交易，本身就是企业对数据安全和隐私保护的一种承诺。正规交易所通常配备更严格的安全措施和审查机制，保障数据交易的透明性和公正性，而黑市交易则可能涉及非法、不道德或有害的行为。

通过公开支持并积极参与正规数据交易，企业向公众展示了其承担社会责任的决心。这种积极的形象塑造对于赢得消费者、合作伙伴乃至投资者的信任至关重要。在市场竞争激烈的今天，这种信任是企业宝贵的无形资产，对于现代企业而言，数据交易不仅是一项商业行为，更是承载着深刻社会责任的活动。

综上所述，安全港规则的引入，旨在提高企业在数据交易中的行为水平，同时减轻过于严格的责任带来的潜在威慑效果。这种制度设计旨在实现数据交易安全性与规模的平衡，鼓励企业在遵循法规的同时，积极参与数据经济。即便在安全港规则未完全实施的情况下，场内交易仍是企业展现对数据安全和社会责任重视的有效途径，进而提升其在消费者、合作伙伴和投资者心目中的信誉。

5.3 数据交易所的蓝图规划：安全港规则的愿景

在下文中，将深入探讨安全港规则在数据交易所领域的具体应用。这包括考虑安全港规则如何与数据交易所的日常运营相结合，以及如何在确保数据安全和交易合规的前提下，促进数据流通和利用。通过这一讨论，希望为数据交易所提供一个明确的行动框架，以便能够有效地利用安全港规则，实现其在数据交易领域的目标和愿景。

权威机关若以设定安全港的方式赋予交易所此种竞争优势，当然不能仅以扶持交易所本身作为理由，而需要充分的公共利益依据。一般而言，运用安全港规则这一法律技术，有助于撬动数据交易活动形成规模化价值。但是有反对意见认为，将安全港规则设立在数据交易所不太合适，原因在于数据交易所对数据开发和利用过程的专业性理解不足，反对者认为安全港规则更应建立在数据持有方端，因为这可以确保数据的安全性和合理利用。

然而，这一观点可能忽略了数据交易所在集中监管和数据安全监管方面的规模优势。数据交易所通过统一的交易平台，为政府提供了监管的窗口，使得每一笔数据交易都能够被有效追溯和监控。这种集中化的监管模式不仅提高了监管效率，还增强了数据交易过程的透明度和可信度。此外，数据交易所可以通过严格的数据审核和处理流程，确保数据的合法性和安全性，为市场参与者提供额外的保障。因此，尽管有反对意见，但在实际操作中，数据交易所仍然是实施安全港规则的有效平台。

而基于以下理由，与交易所结合的数据交易安全港规则，更可能符合优化设计原则，发挥功能优势，防范制度偏差。

首先，场内交易更有助于保证安全港规则及其适用的公开、透明。与证券发行和交易领域安全港规则适用的实践类似，数据交易安全港规则在施行过程中，将主要借助法律和数据合规等领域专业中介机构开发的合规文书体系。但基于安全港发行、交易的证券，只是免于在证券监管机构注册，不会完全处于黑暗之中，且通常追求在特定期间（如锁定期）结束后进入公开市场。相比之下，获得安全港庇护的数据交易，如不从一开始便在公开监督机制下开展，很容易为灰黑交易洗白提供掩护：例如，交易方完全可以到出现合规疑问时，再临时补做甚至伪造文书，号称交易时已满足安全港适用条件。要求安全港规则仅适用于场内交易，便可借助交易所的集中、公开审查保障安全港规则的执行，并降低监管机构和社会公众进行外部监督——不仅针对场内交易活动，也针对交易所运营行为——的难度。

其次，将安全港规则的适用限定在场内交易，固然是制度赋予交易所的红利，但也可为此名正言顺地要求后者提供对价——尤其是要求交易所承担较当前更高的数据保护和数据安全保障责任。一直以来，尽管尝试通过服务外包等方法为场内交易主体提供有限的数据脱敏和清洗等工作，但数据交易所总体上坚持豁免交易相关风险的监管责任。[139]实际上，借助安全港规则发展、扩大数据交易规模，无法避免带来新增风险，因此需要解决的制度问题无非是将这种风险或应对风险的成本配置给何种主体。尽管交易主体和交易所都将获益于交易规模的扩大，但将额外的风险应对责任全部配置给交易主体，无疑只会导致安全港规则的政策追求落空。在新的制度和市场结构中，交易所可以也适合承担应对至少部分新增风险责任的主体。例如，作为法律背书场内交易安全港效力的明确对价，交易所可以被要求投入足够资源，开发并运行包括交易行为追踪和数据致害保险在内的风控机制。

再次，与场内交易绑定的安全港规则，更易于随交易实践发展持续获得调整、校正。数据交易的类型和场景千差万别，任何一种主体资质和行为要求都无法保证能有效降低所有场景中的风险。交易所以及监管部门可借助场内交易的披露和记录机制，稳定积累信息，并通过只有场内交易才能实现的备案、报告和追踪制

[139] 参见杨力：《论数据交易的立法倾斜性》，《政治与法律》2021 年第 12 期，第 4 页。

度，了解、验证不同类型交易的实际风险。借助安全港规则将更多交易吸引到场内，有助于为决策者建立稳定、可靠的政策制定信息来源，形成“政策订立—实践验证—制度调整”之间的正向循环。

最后，安全港规则在交易所以集中、透明的方式施行，会更有助于规则倡导的合规交易模式产生溢出效应。相对规范、安全的场内数据交易模式，基于披露机制，可对场外交易产生引导作用，成为更大范围内市场主体在进行数据交易活动时协调行为的聚焦点。即使市场主体因种种原因，不选择或无法选择进行场内交易，也可参照场内交易所适用的安全港规则的要求规划自身行为。[140]这种参照不仅对自行探索合规的企业有价值，对整体层面的风险控制也有价值。

[140] 一个可参照的情形时，即使在欧盟—美国隐私盾框架协议被欧洲法院认定无效的情况下，美国执法机关仍然建议美国企业继续基于隐私盾框架包含的要求开展数据合规。https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

六、安全港适用前景：案例分析与规则应用

在探讨安全港规则的实际应用和有效性时，将其置于具体案例分析中显得尤为重要。通过将安全港规则应用于具体案例的分析，能更好地理解其在解决数据交易中现实担忧方面的潜力。而这些担忧，如合规性的不确定性和法律责任的风险，正是场外点对点交易无法有效解决的问题。因此，数据交易所推行安全港规则不仅是为了自身发展的需要，更是为了整个数据交易市场的健康和可持续发展。

在现实的数据交易过程中，企业普遍面临着法律责任的不确定性，为应对这些挑战，许多企业依赖于合同机制来明确各方的权利和义务，并尽可能确保交易的合规性。然而，这种基于合同的解决方案在处理更复杂的交易场景时仍然存在局限性。

在此背景下，数据交易所的角色变得尤为关键。作为一个中立的第三方平台，数据交易所不仅提供了一个规范化的交易环境，更重要的是，它通过集中多个行业和企业的数据交易活动，提供了规模效应。这种规模效应的优势在于，交易所能够整合各行业的最佳实践，持续优化和标准化这些操作，从而有效降低所有参与者的交易成本。

安全港规则作为一种制度创新，提供了解决这些法律风险的新途径。通过为数据交易者提供明确的合规路径和法律保护，安全港规则不仅能够降低企业面临的法律风险，还能够提升整体交易的效率和安全性。尽管目前安全港规则还处于设想阶段，但对其进行理论探索和应用实验是至关重要的。这不仅能够验证其在实践中的有效性，更能够指导交易所在未来的蓝图规划中找到自己的独特优势。

下文拟制了一家省级公共数据授权运营公司（某公司），并设计其相应数据流通交易中的痛点、需求，以及安全港规则的可能适用。需要说明的是，这家公司都是为了说明一般性原理、普遍性问题的“拟制”，请读者不要对号入座。

6.1 某公司及其业务简介

某公司在省级公共数据处理和管理方面拥有独特的地位，也被赋予了处理和管理公共数据的重要任务。某公司的业务特点不仅展示了其在数据治理领域的专业能力，也反映出其在面对政策和市场变化时的应变能力。然而，某公司的业务发展也受到一系列政策和法规的限制，这对其商业模式和长期发展策略产生了深远的影响。

某公司的主要业务有以下四方面：

1.公共数据授权处理：某公司作为某省公共数据处理的授权实体，享有在该领域的专有地位和数据访问权，这为公司提供了显著的市场优势。

2. 数据治理：某公司专注于基础数据治理工作，组建了专业团队来负责数据的汇集、整合及质量提升工作，保障了数据的准确性和可靠性。

3. 数据集成：某公司负责整合全省各部门业务系统数据，提供全面的数据集成服务，增强了数据的综合应用能力。

4. 原始数据加工：某公司专注于原始数据的基础加工和提纯，而非转化为其他形式的知识产品，确保数据质量的同时避免破坏数据生态。

虽然某公司在公共数据处理领域具有独特优势，但同时面临由政府政策、业务范围及技术资源分配等因素带来的多重挑战。首先，某公司的活动受限于仅进行数据的初级开发，即基本数据加工，无法进行深度的数据开发或创造更复杂的数据产品，公司不得从事超出初级开发活动范围的任何经营活动，限制了其业务的多样性和扩展性。其次，作为一家公益性企业，某公司的所有定价，包括技术服务费用，都需受到政府的审批和控制。

6.2 某公司在数据交易中的问题与安全港规则的适用

作为一家公共数据授权公司，某公司在数据交易领域面临着一系列复杂且棘手的挑战，这些挑战根植于数据权属的不明确性、定价难题，以及数据滥用带来的潜在风险。这些因素交织在一起，形成了一道难以逾越的障碍，使得某公司在数据交易上显得异常谨慎，甚至不敢轻易涉足。

首先，数据权属的模糊性是某公司面临的一大问题。作为一个被授权运营公共数据的公司，某公司在数据的收集、管理和使用方面扮演着关键角色。然而，这些数据的所有权和使用权却并非完全归某公司所有。公共数据，尤其是医疗数据，涉及到多方利益主体，如个人、医院、卫健委等，每一方都可能对数据主张一定的权利。这种权属的不明确性导致某公司在考虑数据交易时不得不非常谨慎，担心一旦交易可能会触及法律红线，或引发利益相关方的反对。

其次，数据交易的定价问题对某公司来说是另一个难题，公共数据的性质决定了数据并不能像普通商品那样随意定价。某公司作为国有资产管理者，对公共数据的定价必须遵守政府的指导和相关法律法规。然而，这些指导往往缺乏具体的定价标准，留给某公司的操作空间非常有限。对于不同的数据，如何定价，以及定价的合理性，一直是某公司难以解决的问题。尤其是当数据交易涉及到公益性使用和产业发展时，如何在确保公平性的同时，又不失去数据的市场价值，是一个需要精心平衡的问题。

最后，数据滥用的风险是某公司在数据交易中必须认真考虑的一个重要因素，这是因为数据的敏感性和多样性意味着数据的使用方式可能存在极大的变数。尤其是在医疗数据领域，不当的数据使用不仅可能违反伦理和法律，还可能对个人隐私造成严重侵害。某公司担忧一旦数据流入市场，就难以有效监控其使用情况，特别是在缺乏严格监管机制的情况下。数据被滥用后，作为数据出售方的某公司可能需要承担相应的管理责任，甚至面临法律诉讼和社会舆论的双重压力。这种风险的不可预测性和潜在的严重后果，使某公司在数据交易上变得更加谨慎。

综上所述，某公司在数据交易上的谨慎态度，源自于数据权属的不明确性、定价难题和数据滥用的潜在风险。这些问题不仅是技术性的，更是法律和伦理层面的深层次挑战。只有通过系统性的法律和政策创新，明确数据的权属和使用规则，合理定价，严格监管，才能为某公司等数据管理者提供一个更清晰、可行的数据交易路径。

而安全港规则作为一种法律技术，则提供了一种系统性的解决方案，有望有效解决某公司在数据交易过程中所面临的一系列问题。在安全港规则的框架下，某公司可以在一个更加明确和可预期的法律环境中进行数据交易，同时减少与数据交易相关的各种法律风险和社会压力。

首先，安全港规则为解决数据权属的模糊性提供了一个实用的路径。通过明确的法律指引和标准，安全港规则可以为数据交易的各方主体提供明确的操作框架。在这种框架下，某公司可以更加明确地知道哪些数

据可以交易，哪些数据需要保留，并且能够清楚地理解在数据交易过程中的法律责任和义务。这不仅有助于减少法律争议，也增加了某公司进行数据交易的信心和依据。

其次，安全港规则对于数据交易定价问题的解决同样至关重要。在数据交易所专业人员的指导下，可以建立起一套更加合理和透明的数据定价机制。这种机制可以根据数据的种类、用途、价值等因素来确定价格，同时考虑到公共利益和市场规律。这样，某公司在数据交易时可以依据这一机制进行合理定价，减少定价的随意性和不确定性，同时安全港规则使交易主体可以避免因价格问题引起的争议和法律风险。

最后，安全港规则在防止数据滥用方面也发挥着重要作用。通过明确的法律规定和指导，数据交易所可以设定数据使用的边界和条件，明确哪些数据使用方式是允许的，哪些是禁止的。同时，数据交易所还可以为数据交易提供必要的监管和审查机制，确保数据交易的合法性和合规性。这样一来，某公司在交易数据时，可以更加有信心地保证数据不会被滥用，同时有安全港规则在法律层面的加持，可以减少某公司数据滥用而带来的法律责任和社会风险。

综上所述，安全港规则作为一种法律技术，可以为某公司在数据交易中遇到的权属不明确、定价难题和数据滥用风险等问题提供可能的解决方案。通过这些解决方案，某公司可以在一个更加安全、明确和可预期的法律环境中进行数据交易，从而有效促进数据的合理利用和健康发展。

七、结论

本报告系统建构了“安全港规则”的理论及其通过数据交易所的实现机制。安全港规则旨在为数据交易市场主体提供一个清晰、明确的合规路径，在提升数据交易活动自身安全性的同时，也为交易提供相应的法律保障，从而促进交易规模的扩大、体量的释放和活跃度的提升。当前，阻碍数据交易发展的一个重要因素，是市场主体开展数据交易时，面临与数据交易相关数据处理活动有关的各类法律责任方面的不确定性。而这种法律责任的不确定性，本身又与数据交易相关数据处理活动可能涉及较为复杂的安全风险有关。安全港规则及其对应的相关制度机制寻求更为有效地平衡效率和安全，确保在鼓励、促进数据交易的同时，保障数据隐私、数据安全和网络安全。

数据交易安全港规则包含“2+2”框架。首先，“合规技术”与“法律规则”相结合，不仅将使用区块链存证、AI 智能检测、隐私计算等合规技术手段确保数据交易安全可信，也将引入合规、透明、可操作的法律规则，明确安全港的适用条件、免责后果。其次，“主动投入”与“预期免责”相结合，安全港要求企业满足特定的资质、合规条件，并进行可信披露，主动投入相关成本进行“驶入” 安全港的动作，从而获得免责预期：在监管部门的授权下、在数据交易场所建构的可信空间内开展交易，可以避免因为事先未曾预料的风险而事后被追责。

上海数据交易所针对案例中展示的市场需求和痛点，初步建构了包含下列具体措施的数据交易安全港：

（一）智能接入，基于企业主动申请和特定场景（特别是创新容错场景）主动接入，对流通交易数据进行智能分类分级、按需接入安全港。

（二）可信交易，在合规技术保障下，在监管部门授权、监管、验收等流程下按照特殊规则在港内交易。

（三）风险响应，在安全港港内交易，如果存在侵权投诉、情势变更等风险警示情形，及时启动中止交易、信息披露等响应机制，并保障市场主体取得与前期合规投入、创新容错政策相适应的责任豁免。

（四）反馈迭代，成立数据交易合规委员会，对安全港规则进行动态调整，并与行业主管部门、监管部门、司法部门进行定期沟通反馈，根据安全港运行情况和需求情况迭代完善相应规则。

参考文献

[1] 陈昶屹：《“避风港规则”扩张适用网络人格权保护之困境与消解——兼论侵权责任法第三十六条之完善》，《人民司法（应用）》2012 年第 1 期。

[2] 陈洁：《“利用自身信息交易”作为内幕交易抗辩规则的建构--兼论我国内幕交易安全港规则的基本框架》，《现代法学》2021 年第 5 期，第 145 页。

[3] 陈越峰：《超越数据界权：数据处理的双重公法构造》，载《华东政法大学学报》，2022 年第 1 期，第 18-31 页。

[4] 单甜甜：《互联网平台适用避风港规则免责的条件》，《人民司法（案例）》2020 年第 5 期。

[5] 丁晓东：《数据交易如何破局--数据要素市场中的阿罗信息悖论与法律应对》，《东方法学》2022 年第 2 期，第 144 页。

[6] 范文仲：《完善数据要素基本制度 加快数据要素市场建设》，载《中国金融》2022 年第 1 期，第 14-17 页。

[7] 范晓娟：《论有限合伙基金的“安全港”规则的突破》，《政治与法律》2013 年第 5 期，第 128 页。

[8] 冯果、洪治纲：《论美国破产法之金融合约安全港规则》，《当代法学》2009 年第 3 期。

[9] 高富平、冉高苒：《数据要素市场形成论——一种数据要素治理的机制框架》，载《上海经济研究》2022 年第 9 期，第 70-86 页。

[10]高富平：《数据经济的制度基础——数据全面开放利用模式的构想》，载《广东社会科学》2019 年第 5 期，第 5 页。

[11]高富平：《数据流通理论——数据资源权利配置的基础》，载《中外法学》2019 年第 6 期，第 1405 页。

[12]胡滨、杨楷：《监管沙盒的应用与启示》，载《中国金融》2017 年第 2 期，第 68 页。

[13]胡凌：《互联网“非法兴起”2.0——以数据财产权为例》，载《地方立法研究》2021 年第 6 期，第 21-36 页。

[14]胡凌：《论赛博空间的架构及其法律意蕴》，载《东方法学》2018 年第 3 期，第 87-91 页。

[15]胡凌：《数据要素财产权的形成：从法律结构到市场结构》，载《东方法学》2022 年第 2 期，第 120-131 页。

[16]黄朝椿：《论基于供给侧的数据要素市场建设》，载《中国科学院院刊》2022 年第 10 期，第 1402-1409 页。

[17]刘家瑞：《论我国网络服务商的避风港规则——兼评“十一大唱片公司诉雅虎案”》，《知识产权》2009 年第 2 期，第 13 页。

[18]刘珊：《全国首批“数据经纪人”在广州海珠诞生 3 家企业入选，涉及电力行业、电子商务、金融等领域》，载《南方日报》2020 年 5 月 28 日，第 4 版。

[19]陆娅楠：《构建数据基础制度 更好发挥数据要素作用——国家发展改革委负责同志答记者问》，http://cpc.people.com.cn/n1/2022/1220/c64387-32590046.html

[20]梅夏英、王剑《“数据垄断”命题真伪争议的理论回应》，载《法学论坛》2021 年第 5 期，第 99-101 页。

[21]沈朝晖：《上市公司私有化退市的“安全港”制度研究》，《法学家》2018 年第 4 期，第 66 页。

[22]沈伟伟《算法透明原则的迷思——算法规制理论的批判》，载《环球法律评论》2019 年第 6 期，第 20-39 页。

[23]唐郡：《数据基础制度奠基：淡化所有权，优先流通》，载微信公众号“财经五月花”，2022 年 10 月 8 日。

[24]王迁：《《信息网络传播权保护条例》中“避风港”规则的效力》，《法学》2010 年第 6 期，第 128，133 页。

[25]杨力：《论数据交易的立法倾斜性》，《政治与法律》2021 年第 12 期，第 3 页。

[26]姚佳：《数据要素市场化的法律制度配置》，载《郑州大学学报(哲学社会科学版)》2022 年第 6 期，第 6-7 页。

[27]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，第 2-12 页。

[28]张景智：《“监管沙盒”制度设计和实施特点：经验及启示》，载《国际金融研究》2018 年第 1 期，第 58 页。

[29]郑磊：《开放不等于公开、共享和交易：政府数据开放与相近概念的界定与辨析》，载《南京社会科学》2018 年第 9 期，第 83-89 页。

[30]朱开鑫：《从“通知移除规则”到“通知屏蔽规则”——《数字千年版权法》“避风港制度”现代化路径分析》，《电子知识产权》2020 年第 5 期，第 42 页。

[31] Andrew Stumpff Morrison, Case Law, Systematic Law, and a Very Modest Suggestion, 35 Statute Law Review 159, 173 (2013), p169, pp173-174.

[32]Anupam Chander, How Law Made Silicon Valley, 63 Emory Law Journal 639, 652(2014).

[33]Argenton,Cédric,and Jens Prüfer."Search Engine Competition With Network Externalities",Journal of Competition Law and Economics 8.1 (2012):73-105.

[34]Carol Sanger, Infant Safe Haven Laws: Legislating in the Culture of Life, 106 Columbia Law Review 753, 762-772 (2006).

[35]Cass R. Sunstein, On the Expressive Function of Law, 144 University of Pennsylvania Law Review 2021, 2034-2036 (1996)

[36]Charles I. Jones and Christopher Tonetti, “Nonrivalry and the Economics of Data”, American Economic Review, Vol.110, No.9, 2020, p.2821.

[37]Danielle Keats Citron,How To Fix Section 230, Virginia Public Law and Legal Theory Research Paper No. 2022-18,2022，available at SSRN: https://ssrn.com/abstract=4054906.

[38]Duncan Kennedy, Form and Substance in Private Law Adjudication, 88 Harvard Law Review 1685, 1689-1690 (1976), p.1696.

[39]Eric Goldman, Internet Law: Cases & Materials, E-version, 2021, p.159.

[40]Ethem Alpaydin, Machine Learning, MIT Press, 2016, Chapter 4.

[41] Gideon Parchomovsky & Alex Stein, Catalogs, 115 Columbia Law Review 165 (2015), pp.171-172, pp.188-190.

[42]Hirsch, Werner Z, "Reducing Law's Uncertainty and Complexity.", UCLA Law Review, vol. 21, no. 5, June 1974, pp. 1233-1236.

[43]Julie E.Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism, Oxford University Press, 2019, p.45.

[44]Katerina Pistor, "Rule by Data: The End of Markets?", Law and Contemporary Problems, Vol.83, No.2, 2020, p.110-112.

[45]Kerber,Wolfgang."Digital Markets,Data,and Privacy:Competition Law,Consumer Law and Data Protection",Journal of Intellectual Property Law & Practice 11.11 (2016):856-66.

[46]Louis Kaplow, Rules versus Standards: An Economic Analysis, 42 Duke Law Journal 557(1992), pp579-584.

[47]Mark A. Lemley,Rationalizing Internet Safe Harbors, 6 Journal Telecommunication & High Technology Law 101, 112 (2007), p.113.

[48]Marotta-Wurgler, Florencia, "Self-Regulation and Competition in Privacy Policies", Journal of Legal Studies, vol. 45, no. 2 Supplement, June 2016, p. S13-S40.

[49]Michael Barbaro & Tom Zeller, Jr., A Face Is Exposed for AOL Searcher No. 4417749, N.Y. TIMES, Aug. 9, 2006.

[50]Ohm, Paul, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." UCLA Law Review, vol. 57, no. 6, August 2010, p. 1701-1778.

[51] Omri Ben-Shahar, "Data Pollution", Journal of Legal Analysis, Vol.11, No.1, 2019, pp.112-115.

[52]Pamela Samuelson, Pushing Back on Stricter Copyright ISP Liability Rules, 27 Michigan Technology Law Review 299, 305-307 (2021).

[53]R. H. Coase, The Problem of Social Cost, The Journal of Law and Economics, Vol.3, 1960, p.44.

[54]Susan C. Morse, Safe Harbors, Sure Shipwrecks,49 UC Davis Law Review 1385,1392 (2016), p.1397.

[55]Susan R. Klein, Identifying and (Re)formulating Prophylactic Rules, Safe Harbors, and Incidental Rights in Constitutional Criminal Procedure, 99 Michigan Law Review 1030, 1044–45 (2001), p.1046.

[56]T. Randolph Beard et. al., Safe Harbors and the Evolution of Online Platform Markets: An Economic Analysis, 36 Cardozo Arts & Ent. L.J. 309, 312 (2018).