欧洲“数字服务法”（DSA）：重塑跨境内容审核格局的引擎与挑战

摘要:欧洲《数字服务法案》（DSA）旨在确保用户在线权利，加强平台责任，对跨境内容审核影响深远。TEMU 上线欧洲市场后，重视商品安全和消费者保护，2024 年 5 月 31 日被列为超大型在线平台（VLOP），依据 DSA 要求发布透明度报告。报告期内，TEMU 投入资源进行内容审核，采用集成先进自动化系统、主动措施和人工监督的全面策略，遵循清晰透明且定期更新的政策，实施贸易商验证等主动性预防措施，以维护安全的线上购物环境，确保平台内容、产品和互动合法合规。

关键词:欧洲“数字服务法”（DSA）、平台内容审核

1.引言

在数字技术迅猛发展、全球信息交流日益频繁的当下，互联网的无边界特性使得跨境内容传播变得愈发便捷，同时也给内容监管带来了前所未有的挑战。数字平台上的内容种类繁多、来源广泛，其中不乏有害信息，对社会秩序、用户权益等造成潜在威胁。在此背景下，各国纷纷寻求有效的监管措施来规范数字空间，而欧洲“数字服务法”（DSA）的出台则成为这一领域的重要里程碑。

欧洲“数字服务法”（DSA）作为一套全面且具有开创性的法规，旨在应对数字时代复杂的内容审核问题，重塑数字服务领域的责任体系与监管框架。该

法案不仅对欧洲内部的数字服务提供商提出严格要求，更因其广泛的域外效力，对全球范围内的跨境内容审核产生深远影响。众多国际数字平台，无论总部是否位于欧洲，只要在欧洲市场提供服务，都需遵循 DSA 的规定（图 1），这无疑打破了以往跨境内容审核相对宽松和模糊的局面。



图 1. DSA 涉及内容

通过深入分析欧洲“数字服务法”（DSA）对跨境内容审核的影响，本案例分析旨在揭示数字时代内容监管面临的复杂现实，探讨不同利益主体在新法规环境下的应对策略及其背后的逻辑，剖析 DSA 实施过程中出现的问题与挑战，并从中汲取经验教训，为全球数字治理的未来发展提供有益参考，推动建立更加合理、有效的跨境内容审核机制和数字治理体系。

2.内容策略与创新

首先，明确非法内容界定与清除责任。DSA 要求科技公司对平台上出现的

内容承担更大责任，需更快地删除非法内容和商品。明确规定“在线下违法的内容在线上也是违法的”原则，为内容审核提供清晰的法律基准。这意味着跨境平台在面对欧盟用户时，必须依据欧盟法律标准，对各类非法内容进行严格排查和及时清除，如虚假信息、有害信息、侵权内容等。例如，若出现侵犯知识产权的商品信息，平台有责任立即下架处理。

其次，强调算法透明度。科技公司需要向用户和外部研究员解释他们的算法如何工作。这一要求使得跨境平台的算法不再是“黑箱”。通过公开算法原理和运行机制，有助于外界了解平台内容的推荐逻辑，也便于监管机构和公众监督算法是否存在对非法或不良内容的不当推送，促使平台在算法设计上更加注重内容质量筛选，减少有害内容的传播。

第三，聚焦保护未成年人。完全禁止根据个人资料或个人数据对未成年人定向投放广告，同时向用户提供广告信息，包括为何展示广告以及谁为广告付费等。这一策略旨在从广告投放源头保护未成年人免受不适当内容影响，跨境平台在涉及欧盟未成年人用户时，需严格遵守该规定，重新审视和调整广告投放策略，保障未成年人的网络安全和健康成长。

另外，完善用户反馈与审核流程透明化。向受任何内容审核决定影响的用户提供原因声明，例如内容删除、账户暂停等，并将原因声明上传到 DSA 透明度数据库；为用户提供投诉机制，以质疑内容审核决定；每年至少发布一次

内容审核程序报告。这些措施既保障了用户的知情权和申诉权，也让跨境平台的内容审核流程更加透明公开，接受用户和社会监督。

在创新方面上，其一，建立“可信标记者”合作机制。在线平台必须与“可信标记者”合作，这些专门实体的通知必须优先受到平台关注。“可信标记者”作为独立的第三方，具备专业的审核能力和资源，能够协助平台更高效地识别非法内容。对于跨境平台而言，可借助“可信标记者”对不同来源的海量内容进行快速标记筛选，提高内容审核的准确性和及时性，这是一种全新的审核合作模式。

其二，设立严格的超大型平台监管。DSA 授权欧盟委员会监督非常大的平台（图 **2**），对违规科技公司可处以高达全球营业额 6%的罚款，甚至在屡次严重违规的情况下禁止在欧盟单一市场运营。这一创新举措对超大型跨境平台形成强大威慑力，促使这些平台主动投入更多资源用于内容审核体系建设，加强内部管理，以避免巨额罚款和市场禁入风险，从而提升整个跨境内容审核的标准和水平。



图 2. 数字服务平台遍及全球

3.欧洲“数字服务法”（**DSA**）对跨境内容审核的影响

其一，内容审核责任体系的重构。DSA 通过分层监管框架将平台划分为超大型在线平台（VLOPs）、在线平台及中介服务商三类，针对不同规模主体设定差异化义务。以 TEMU、Shein 等被列为 VLOPs 的企业为例，其需建立包含自动化系统（AI 过滤技术）、人工审核团队（多语言支持）及第三方验证机制的三级审核体系。根据合规要求，此类平台需每季度提交内容审核效能报告，详细披露非法商品拦截率、知识产权侵权处理时效等关键指标。

其二，跨境治理规则的刚性约束。DSA 首创“线上违法即线下违法”原则，要求平台建立覆盖欧盟 27 国的统一合规框架。具体表现为：商品安全标准需同时满足欧盟通用指令（如 CE 认证）与成员国特殊要求（如德国包装法）；用户举报系统必须支持 24 种官方语言服务；审核决策需在 72 小时内响应，较非 VLOPs 平台缩短了处理时限。违规企业面临最高全球营业额 6%的罚款，对

于屡次严重违规的企业，DSA 授权欧盟委员会实施全欧盟域禁令，禁止其在欧盟市场运营，并可能被实施全欧盟域禁令。

其三，算法透明度的强制披露。平台需向监管机构报备内容推荐机制的核心参数，包括但不限于商品排序权重设置、用户画像构建维度、广告投放逻辑等关键技术细节。TikTok 等企业已调整推荐算法，取消基于宗教、政治倾向等敏感标签的定向推送。同时要求为欧盟用户提供"无算法推荐"浏览模式，这对依赖个性化推荐的跨境电商转化率构成直接影响。

其四，供应链追溯能力的强化。针对跨境电商业态，DSA 要求建立全链条可追溯系统。以 Shein 为例，其需实现从中国供应商资质审核（工商登记验证）、物流信息追踪（包裹电子标签）到终端消费者反馈（产品评价监测）的数字化闭环。平台必须保存供应商 KYC 资料至少 5 年，并配合欧盟海关进行商品溯源调查，违规供应商将面临即时清退及跨境黑名单联动处罚。

这些变革正在重塑全球数字贸易规则体系，促使企业构建覆盖合规审计、技术升级、流程再造的跨境治理新范式。

4.跨文化适配

DSA 要求超大型平台（VLOPs）针对欧盟成员国语言配备相应规模的内容审核团队，确保对多语言环境的精准覆盖。例如，平台需按成员国语言要求部署审核资源，避免因语言障碍导致有害内容漏筛。同时，法案限制利用种族、性别等敏感标签进行定向广告投放，间接推动平台在内容策略中嵌入文化敏感

性。

VLOPs 需定期评估平台内容对欧盟民主进程、公共安全及基本权利的影响，DSA 要求 VLOPs 评估系统性风险，包括虚假信息、非法内容等。例如，不同成员国对仇恨言论的定义存在差异，平台需建立动态审核标准以适配多元文化背景。

DSA 通过制度设计提高了平台透明度和用户保护，但其效能取决于执行中资源投入与技术创新的协同，以及欧盟内部文化共识的持续凝聚。

5.从可供性理论视角的评估

5.1 技术可供性重构

DSA 强制要求超大型平台建立多层级审核体系（自动化系统+人工监督），例如通过部署 AI 内容识别算法与人工复核的双轨机制，平台能够显著提高非法商品的识别率，但具体识别率取决于平台的技术能力和资源投入。这种技术架构的升级使平台具备即时阻断跨境违禁品传播的能力，同时算法透明度条款要求平台向监管机构公开推荐机制参数，通过提高算法透明度，DSA 旨在增强用户对推荐机制的理解和选择权，减少算法对用户信息获取路径的不透明影响。

5.2 制度可供性强化

法案创设的“分层追责框架”建立了差异化义务体系。例如，Shein 被列为 VLOP 后需每年提交系统性风险评估报告，涵盖商品溯源数据与知识产权保护

措施等内容。这种制度设计迫使跨境平台将欧盟合规标准内化为全球运营基准，形成“布鲁塞尔效应”。例如，TikTok 为符合 DSA 要求的年龄验证系统进行了技术升级，并将其同步应用于全球市场，进一步推动了全球合规标准的统一。

5.3 认知可供性转变

DSA 赋予用户“内容审核异议权”与“算法拒绝权”，重塑了用户-平台权力关系。法案生效后，欧盟用户对平台内容删除决定的申诉量显著增加，平台回应时效也有所缩短。这种双向互动机制的建立，使内容审核从单向管控转变为多方参与的协商治理。例如，用户可以对内容审核决定提出申诉，并要求平台提供明确的理由；同时，用户可以选择拒绝个性化推荐算法，要求平台提供非个性化内容推荐选项。

5.4 风险可供性控制

法案创设的“系统性风险评估”机制要求 VLOPs 建立风险预测模型，例如 Twitter 为应对 DSA 审查可能增加了仇恨言论监测节点，使跨境虚假信息扩散速度显著降低。但过度合规也产生了技术排斥效应，独立研究机构 EU DisinfoLab 发现中小型平台因无法承担合规成本，其内容多样性指数同比下降。评估表明，DSA 通过重构技术、制度、认知三重可供性维度，使跨境内容审核从被动响应转向主动防御。但需警惕监管壁垒对数字公共领域生态的挤压，最新数据显示 VLOPs 内容审核支出占营收比显著上升，可能加剧数字市

场垄断格局。

6. 启示与挑战

欧盟《数字服务法》（DSA）通过“规则输出型监管”范式驱动跨国企业重构内容治理体系，标志着数字主权博弈进入深水区。其以“看门人制度”和“算法透明性义务”为支点，迫使全球平台将欧盟标准内化为技术基座，形成“布鲁塞尔效应 2.0”下的合规辐射网络，典型如 TikTok 分割全球审核架构、Meta 开发地理围栏系统等实践。这一进程催生“防御-预防”双轨技术革新，企业通过联邦学习模型平衡数据本地化与算法效能，运用区块链存证链满足追溯审计，但算法参数强制披露亦削弱平台核心竞争力。跨文化适配成为深层挑战，东欧历史叙事差异与西欧言论自由传统的冲突，要求构建动态文化敏感度数据库与区域性争议调解机制，而 DSA 对中小企业的合规成本挤压则凸显“技术民主化”缺失。未来数字治理需在“监管刚性”与“创新弹性”间寻求平衡——既通过开源工具包降低中小企业准入门槛，也需设立独立仲裁机制防范过度审查，最终在欧盟规则输出的“制度引力”与全球文化多样性之间构筑可持续的治理生态。