E-Commerce Letters 电子商务评论, **2025, 14(12), 2305-2310**
Published Online December 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14124116

Hans汉斯

电子商务中侵犯公民个人信息犯罪的法律规制

余　漫

贵州大学法学院，贵州 贵阳

收稿日期：2025年10月31日；录用日期：2025年11月14日；发布日期：2025年12月16日

摘　要

在电子商务深度渗透日常生活的背景下，侵犯公民个人信息犯罪呈现链条化、技术化、隐蔽化特征，已形成“信息获取－解密倒卖－精准利用”的黑产生态，严重威胁公民财产安全与数字市场秩序。本文结合《刑法》及相关司法解释实施实践，通过分析电商领域此类犯罪的典型形态与司法认定难点，揭示现行规制体系在前置法衔接、责任主体界定、证据标准适用等方面的现实困境。相较于现有研究侧重单一维度的规制建议，本文基于“两高”司法解释与近年典型案例，提出“立法补位－司法适配－执法闭环”的三维协同规制路径，突出“平台责任梯度化认定”“电子证据链标准化”“跨部门协同机制实体化”三大创新要点，为破解电商场景下个人信息刑事保护难题提供更具实操性的理论支撑与实践指引。

关键词

电子商务，公民个人信息，侵犯公民个人信息罪，法律规制，平台责任

Legal Regulation of Crimes Involving the Infringement of Citizen’s Personal Information in E-Commence

Man Yu

Law School of GuiZhou University, Guiyang Guizhou

Received: October 31, 2025; accepted: November 14, 2025; published: December 16, 2025

Abstract

Against the backdrop of e-commerce deeply permeating daily life, crimes involving the infringement of citizens’ personal information exhibit characteristics of chain-based operations, technological sophistication, and concealment. These offenses have formed a black-market ecosystem encompassing “information acquisition-decryption and resale-targeted exploitation”, posing a severe threat to

文章引用：余漫．电子商务中侵犯公民个人信息犯罪的法律规制[J]．电子商务评论, 2025, 14(12): 2305-2310.
DOI: 10.12677/ecl.2025.14124116

citizens' property security and the order of the digital marketplace. This paper examines the implementation of the Criminal Law and relevant judicial interpretations, analyzing typical patterns of such crimes in the e-commerce sector and challenges in judicial adjudication. It reveals practical difficulties within the current regulatory framework regarding pre-trial coordination, liability attribution, and evidence standards. Compared to existing research focusing on single-dimensional regulatory recommendations, this paper proposes a three-dimensional collaborative regulatory approach—"legislative supplementation, judicial adaptation, and enforcement closure"—based on the judicial interpretations of the Supreme People's Court and Supreme People's Procuratorate, as well as recent landmark cases. It highlights three key innovations: "graded determination of platform liability", "standardization of electronic evidence chains", and "institutionalization of cross-departmental coordination mechanisms". These innovations provide more practical theoretical support and operational guidance for addressing challenges in criminal protection of personal information within e-commerce contexts.

Keywords

E-Commerce, Personal Information of Citizens, Crime of Infringing on Citizens' Personal Information, Legal Regulation, Platform Liability

1. 引言

随着数字经济的蓬勃发展，电子商务已成为社会经济运行的核心载体，而公民个人信息则是电商平台精准营销、服务优化的核心资源。电商交易全流程中产生的姓名、手机号、收货地址、支付记录等信息，既承载着个体隐私权益，也蕴含着巨大商业价值。然而，信息价值的凸显催生了黑色产业链，2024年公安机关侦破的电商领域侵犯公民个人信息案件达 1.2 万起，涉案金额超 30 亿元，其中“订单解密”“内鬼倒卖”等新型犯罪占比达 68% [1]。

此类犯罪的社会危害性具有复合性：不仅通过精准诈骗、敲诈勒索等下游犯罪直接侵害公民财产权，更是破坏电商市场的信任根基。某电商“订单解密”案中，18 名犯罪嫌疑人勾结平台商户与快递“内鬼”，非法获取百万条用户信息并用于诈骗，导致数千名消费者累计损失超千万元，凸显了现有规制体系的短板。尽管《刑法》第 253 条之一及“两高”司法解释构建了基本刑事规制框架[2]，但电商场景的技术复杂性与利益链条多元性，使法律适用面临诸多挑战。因此，系统研究电子商务中侵犯公民个人信息犯罪的法律规制，既是回应《数字中国建设整体布局规划》的安全需求，也是保障数字经济健康发展的必然选择。

2. 电子商务中侵犯公民个人信息犯罪的典型形态

电子商务的交易流程特性与技术架构，使侵犯公民个人信息犯罪形成了独具行业特征的行为模式，结合司法实践可归纳为以下四类典型形态。

2.1. “订单解密”型：加密机制下的信息窃取

为响应《个人信息保护法》要求，主流电商平台与快递企业对订单信息采取“部分脱敏”处理，将手机号、地址等关键字段替换为“*”号，但这一防护措施被犯罪团伙利用形成“解密黑产”。其运作模

式为：电商商户通过打单软件批量导出加密订单，交由“解密中介”处理；中介勾结快递公司内部人员或利用平台漏洞，调用解密接口还原完整信息，再以每条 0.5~2 元的价格售予商户。

此类犯罪的技术隐蔽性极强，表面上依托平台合法功能(如订单导出)，实则突破数据保护边界。2025 年侦破的某跨境电商解密案中，犯罪团伙利用平台“商户售后服务”权限漏洞，将解密范围从“售后订单”扩展至全部订单，半年内非法获取 80 万条用户信息，涉案金额达 300 余万元[3]。从法律性质看，该行为既符合“以其他方法非法获取公民个人信息”的构成要件，若解密后转售则同时触犯“出售公民个人信息”罪名，属于想象竞合犯[4]。

2.2. “内鬼泄密”型：数据管理环节的监守自盗

电商平台员工、第三方服务商人员等“内部人员”利用职务便利窃取信息，已成为犯罪链条的重要源头。此类行为主要有三种表现：一是核心岗位人员直接下载用户数据库，如某电商数据分析师利用权限导出 50 万条支付记录转卖牟利；二是技术人员植入木马程序，如教培行业内鬼鲁某某通过优盘植入恶意软件，窃取 50 余家企业客户信息；三是客服人员泄露特定用户信息，如应第三方要求查询并提供消费者订单详情。

“内鬼泄密”的社会危害性尤为突出，因其获取的信息具有完整性与精准性，且往往引发连锁侵权。最高检数据显示，2023 年此类案件占电商信息犯罪总数 34%，且 80%的案件下游关联电信诈骗[5]。从犯罪构成看，内部人员利用履职便利获取信息的行为，符合司法解释中“履行职责或者提供服务过程中获得的公民个人信息”的加重情节，量刑时需适用“数量或数额减半入罪”标准[2]。

2.3. “算法滥用”型：数据挖掘中的权益侵害

部分电商平台或第三方服务商以“数据分析”为名，通过算法技术对合法收集的信息进行深度挖掘，突破授权范围获取敏感信息并用于商业变现。典型表现包括：通过浏览记录、消费频次等数据推定用户收入水平、健康状况等敏感信息；将脱敏的聚合数据还原为可识别个人的具体信息；利用“Cookie 跟踪”技术收集用户跨平台行为数据并出售。

算法的隐蔽性使此类行为难以被察觉。某母婴电商平台通过算法分析用户购买记录、咨询内容，构建“孕期阶段画像”，将包含精准预产期的信息售予奶粉品牌商，涉案信息达 20 万条[6]。根据司法解释，算法还原的个人信息若符合“能够单独或结合识别特定自然人”标准，即属于刑法保护对象，此类行为已构成“非法提供公民个人信息罪”。

2.4. “黑产协作”型：产业链条的分工犯罪

电子商务的跨环节特性催生了分工明确的犯罪链条，通常分为上游(信息获取)、中游(信息倒卖)、下游(信息利用)三个环节。上游由平台内鬼、黑客等组成，负责非法获取原始信息；中游由专业中介负责分类整理、层级转卖，形成“信息超市”；下游则对接诈骗、推销等非法使用者。

2024 年侦破的全国性电商信息黑产案中，上游人员通过植入木马获取订单数据，中游中介按“超敏感(行踪轨迹)－敏感(交易记录)－普通(姓名电话)”分类定价，下游诈骗团伙利用这些信息实施“退款诈骗”，全链条涉及 23 个省份、120 余名犯罪嫌疑人。此类共同犯罪中，各环节人员虽未直接接触，但通过网络工具形成犯意联络，应根据其在链条中的作用认定主从犯[7]。

3. 电子商务中侵犯公民个人信息犯罪的规制困境

尽管刑事立法与司法解释不断完善，但电商场景的特殊性使司法实践仍面临多重障碍，集中体现在法律适用、责任认定与证据采信三个层面。

3.1. 法律适用困境：前置法衔接与认定标准模糊

1) 刑民行衔接机制不畅。现有研究已普遍认可刑民行衔接存在脱节问题，具体在电商场景中则表现为：个人信息保护相关法律涵盖收集、存储、使用等全流程，而刑法仅规制“非法获取、出售或提供”行为。实践中，对于平台过度收集信息后未出售但用于算法牟利的行为，因刑法未明确规制，难以纳入刑事打击范围，形成“行政违法易认定、刑事犯罪难追究”的现象[8]。

2) 信息性质界定存在争议。现有研究已梳理公开信息、脱敏信息、必要信息的认定分歧，但在电商场景中仍存在特殊性争议：一是公开信息的转卖边界，电商平台公示的商家联系人信息转卖是否侵害权益，缺乏统一裁判标准；二是算法还原脱敏数据的定性，能否直接认定为“公民个人信息”，各地法院裁判尺度不一；三是超必要收集信息的刑法评价，平台超出服务需求收集的非敏感信息，是否一律纳入保护范围存在分歧[9]。

3) 入罪标准适用难题。司法解释以“信息数量+违法所得”为核心入罪标准，但电商场景下的特殊适用问题尚未形成共识：一是重复信息的扣除，批量数据中包含的重复手机号、无效地址如何剔除，缺乏操作规范；二是虚假信息折算困境，查获的“信息包”中大量虚假数据如何认定有效数量；三是违法所得计算差异，“购买后转卖”案件中成本是否核减，导致量刑不一致[10]。

3.2. 责任认定困境：平台与多方主体的责任边界不清

1) 平台刑事责任认定模糊。这是现有研究的核心争议点，电商场景下的特殊难题主要包括：一是不作为责任的前置条件模糊，平台未履行安全管理义务导致信息泄露，“经监管部门责令改正而拒不改正”的认定标准与时限不明确；二是作为责任的主观认定困难，平台员工或第三方服务商侵权时，“明知或应知”的判断缺乏具体依据；三是单位犯罪规避问题，平台以“独立第三方运营”为由抗辩，司法机关难以举证其主观故意[11]。

2) 上下游犯罪的责任划分困难。现有研究已经关注到共同犯罪认定中的争议，但电商黑产的跨环节特性加剧了这一问题：上下游人员通过匿名网络工具联络，缺乏直接犯意沟通，中游中介向不明身份者出售信息时，“是否明知下游用于犯罪”的主观证明难度极大[9]。

3) 技术服务商的责任空白。为电商平台提供数据存储、算法服务的技术公司，若明知平台存在信息侵权行为仍提供技术支持，其刑事责任认定缺乏明确依据。现有司法解释未将技术服务商单独列为责任主体，导致此类“帮助犯”往往以“技术中立”为由逃避处罚[12]。

3.3. 证据采信困境：数据特性导致的证明障碍

1) 电子证据的固定与认定困难。电商信息犯罪的电子证据具有易篡改、易灭失特性：一是数据存储分散，涉及平台服务器、第三方工具、犯罪嫌疑人设备等多源载体，取证难度大；二是加密技术阻碍取证，部分犯罪团伙使用“暗网”交易、端到端加密通讯，导致交易记录难以获取；三是电子证据的真实性认定，缺乏统一的存证标准与鉴定规范，部分法院因证据链不完整不予采信[10]。

2) 主观明知的证明乏力。侵犯公民个人信息罪的主观故意证明是司法共性难题，电商场景下的抗辩理由更具隐蔽性：一是平台以“合规审查”为由抗辩，主张对员工泄密或第三方侵权不知情；二是中介以“信息用途不明”否认明知，辩称不知下游用于犯罪；三是内部人员以“履行职务”为由辩解，主张信息获取具有合法性[13]。

3) 被害人举证能力不足。此类犯罪的被害人往往人数众多且分散，难以单独提供被侵权的直接证据。实践中，被害人多仅能证明遭受诈骗等下游损害，无法证明信息泄露源头与具体侵权人，导致“立案难、

追责难”。

4. 电子商务中侵犯公民个人信息犯罪的规制路径

针对上述困境，结合电商行业特性与现有研究不足，本文从立法完善、司法精准、执法协同三个维度，提出具有创新性的系统性规制路径。

4.1. 立法完善：明确规制边界与责任标准

1) 构建刑民行衔接的规范体系。相较于现有研究的原则性建议，以下具体措施更有利于保护电商平台中公民的个人信息：一是细化刑事入罪标准，将电商场景下“收集后非法利用”“脱敏后还原使用”等情节严重的行为纳入刑法规制；二是出台电商专项司法解释，增设“信息数量折算规则”，明确重复信息、虚假信息的扣除标准，统一“全额认定违法所得，不核减成本”的裁判规则；三是扩大刑法保护范围，明确算法可还原的脱敏数据、跨平台聚合数据均属于“公民个人信息”。

2) 明确平台刑事责任的认定规则。通过构建梯度化认定体系，明确平台刑事责任：一是优化不作为责任标准，通过司法解释明确“监管责令改正”的具体情形(如信息泄露预警、用户投诉集中等)，降低入罪门槛；二是建立“客观义务违反－主观故意推定”的逻辑链条，平台未履行数据加密、权限最小化管理等基本义务，且存在用户投诉未处理、漏洞未修复等情形的，推定其对侵权行为具有“概括故意”，可追究共犯责任；三是细化单位犯罪认定标准，以“行为以平台名义实施、违法所得归平台所有”为核心要件，防止责任规避[14]。

3) 增设技术服务商的责任条款。参照“帮助信息网络犯罪活动罪”的规定，明确数据存储、算法服务等技术服务商的刑事责任：若明知电商平台存在信息犯罪行为仍提供技术支持，或未履行安全审查义务导致信息泄露，可单独定罪处罚；情节严重的，与平台构成共同犯罪。

4.2. 司法精准：优化认定规则与证据体系

1) 统一司法认定标准。针对电商平台中的责任认定分歧，提出专项规则：一是明确公开信息保护边界，非敏感公开信息转卖未侵害权益的排除犯罪性，敏感公开信息转卖仍可入罪；二是确立“授权范围限制”规则，平台超出合同必要范围使用收集的信息，即认定非法性，无需以“未经同意”为唯一标准；三是推定中游中介的明知故意，若出售对象要求批量购买行踪轨迹、支付记录等敏感信息，直接推定其“明知他人用于犯罪”[9]。

2) 完善电子证据规则。一是建立“电商数据存证平台”，由监管部门强制平台实时上传用户信息处理日志，实现电子证据的溯源与固定；二是确立电子证据采信标准，明确区块链存证、第三方鉴定等方式的法律效力，简化取证流程；三是推行“举证责任倒置”，对于平台信息泄露案件，由平台举证证明已履行安全义务，无法证明则推定存在过错[8]。

3) 强化被害人权利救济。一是建立集体诉讼与公益诉讼衔接机制，允许检察机关或消费者协会代表众多被害人提起刑事附带民事诉讼，降低个体举证难度；二是设立“信息犯罪案件快速立案通道”，以平台数据、第三方检测报告等间接证据作为立案依据；三是完善量刑情节，将“退赃退赔”“修复信息安全”等作为法定从宽情节，激励犯罪嫌疑人主动弥补损害。

4.3. 执法协同：构建全链条监管与打击机制

1) 强化源头监管。一是开展电商平台“信息安全专项检查”，重点核查数据加密、访问权限、第三方管理等制度落实情况，对存在漏洞的责令限期整改；二是建立“内鬼防范”机制，要求平台对核心岗位人员实行“权限最小化+操作留痕”管理，定期开展背景审查与法律培训；三是规范第三方合作，要求

平台与服务商签订保密协议，明确信息泄露的违约责任与刑事责任。

2) 推进跨部门协同执法。一是建立公安、网信、市场监管等部门的信息共享机制，实现犯罪线索、监管数据、司法裁判的实时互通；二是开展“全链条打击行动”，针对电商信息黑产的上游获取、中游倒卖、下游利用环节同步发力，摧毁犯罪网络；三是加强国际执法合作，对跨境电商信息犯罪，与相关国家建立证据交换与罪犯引渡机制。

3) 深化行业自律与技术赋能。一是推动电商行业协会制定《信息安全自律公约》，建立违法企业“黑名单”制度，实现行业内联合惩戒；二是鼓励平台运用隐私计算、联邦学习等技术，在保护信息安全的前提下实现数据价值利用；三是开展“法律进企业”活动，通过典型案例宣讲、合规培训等方式，提升平台及从业人员的法律意识。

5. 结语

电子商务中侵犯公民个人信息犯罪的法律规制，是数字时代刑法应对技术变革的重要命题。此类犯罪的链条化与技术化特征，对传统刑事规制体系提出了严峻挑战，亟需通过立法、司法、执法的协同发力实现规制升级。本文相较于现有研究，在规制逻辑上突出“问题导向－创新回应”，在具体路径上强调“电商场景适配性”，在实施机制上注重“多主体协同”。

未来的规制路径应立足于：以立法完善明确责任边界与入罪标准，破解法律适用模糊难题；以司法精准优化证据规则与认定逻辑，提升案件办理质效；以执法协同构建源头防控与全链条打击机制，遏制犯罪蔓延态势。这一过程需要立法者兼顾惩治犯罪与保障数字经济发展，司法者强化技术认知与裁判创新，执法者提升技术执法能力与协同水平，更需要电商平台主动履行信息保护义务。唯有如此，才能实现公民个人信息权益保护与电子商务健康发展的良性互动，为数字中国建设筑牢安全法治屏障。

参考文献

[1] 公安部网络安全保卫局. 2024 年打击整治网络侵犯公民个人信息犯罪工作通报[R]. 公安部, 2025.
[2] 最高人民法院, 最高人民检察院. 关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释[Z]. 2017.
[3] 王莹. 电商平台“订单解密”型犯罪的司法认定[J]. 政法论坛, 2024, 42(4): 112-127.
[4] 张明楷. 侵犯公民个人信息罪的司法认定[J]. 政治与法律, 2023(2): 45-62.
[5] 最高人民检察院. 检察机关办理侵犯公民个人信息犯罪典型案例[R]. 北京: 最高人民检察院, 2024.
[6] 丁晓东. 数据治理中的刑民分界——以电商信息利用为例[J]. 法学家, 2022(6): 54-68.
[7] 周光权. 数字时代侵犯公民个人信息罪的教义学分析[J]. 法学研究, 2022, 44(4): 132-150.
[8] 刘艳红. 个人信息保护法与刑法的衔接困境及解决路径[J]. 中国法学, 2023(1): 78-95.
[9] 赵秉志. 侵犯公民个人信息罪的立法完善与司法适用[J]. 现代法学, 2023, 45(1): 23-39.
[10] 李兰英. 侵犯公民个人信息罪的电子证据采信问题研究[J]. 法律科学(西北政法大学学报), 2023, 41(2): 145-160.
[11] 王秀梅. 网络服务提供者的刑事责任边界——以电商平台信息泄露为例[J]. 法商研究, 2024, 41(3): 89-103.
[12] 刘品新. 数字时代刑事证据的变革与应对[J]. 中国刑事法杂志, 2022(5): 3-20.
[13] 陈兴良. 刑法谦抑性与个人信息犯罪的规制边界[J]. 中外法学, 2023, 35(3): 678-695.
[14] 张军. 刑事司法视野下的个人信息保护[M]. 北京: 法律出版社, 2023.