E-Commerce Letters 电子商务评论, 2025, 14(10), 2207-2215
Published Online October 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14103386

Hans汉斯

网络“薅羊毛”行为的法律定性

施章耀

贵州大学法学院，贵州 贵阳

收稿日期：2025年9月15日；录用日期：2025年9月28日；发布日期：2025年10月30日

摘 要

本文针对网络“薅羊毛”行为的法律定性，围绕“羊毛”法律属性、盗窃与诈骗界分、“预设同意”判定展开研究。明确具备管理可能性、转移可能性与价值性的“羊毛”属刑法意义上的财物；提出“机器智能类型化区分”标准，利用弱智能机器漏洞取财构成盗窃罪，利用强智能机器虚构事实取财构成诈骗罪；重构“预设同意”判定规则，以行为发生时平台规则文义为基础，结合行业惯例与普通理性用户认知，仅严重背离商业逻辑的行为超出同意范围。据此，对利用系统漏洞、规则漏洞、恶意注册账号等三类行为分别定性，并建议司法机关明确裁判标准、平台强化风控。

关键词

虚拟财产，盗窃罪，诈骗罪，数字经济

On the Legal Qualification of Online “Wool-Gathering” Behavior

Zhangyao Shi

School of Law, Guizhou University, Guiyang Guizhou

Received: September 15, 2025; accepted: September 28, 2025; published: October 30, 2025

Abstract

This paper focuses on the disputes over the criminal characterization of online “wool-pulling” behaviors in judicial practice, exploring three key issues: the legal attribute of “wool”, the distinction between theft and fraud, and the determination of “presumed consent”. It defines “wool” as property under criminal law with “manageability, transferability, and value”. A “typed distinction” standard

文章引用: 施章耀. 网络“薅羊毛”行为的法律定性[J]. 电子商务评论, 2025, 14(10): 2207-2215.
DOI: 10.12677/ecl.2025.14103386

for machines is proposed: exploiting vulnerabilities of "weak-intelligent machines" constitutes theft, while deceiving "strong-intelligent machines" via fabricating facts constitutes fraud. For "presumed consent", judgment relies on the literal interpretation of platform rules at the time of the act, combined with industry practices and ordinary users' cognition—only acts seriously deviating from commercial logic exceed "presumed consent". Based on this, the three types of behaviors—exploiting system vulnerabilities, exploiting rule loopholes, and malicious account registration—should be respectively characterized. It is also recommended that judicial authorities clarify adjudication standards and platforms strengthen risk control.

Keywords

Virtual Property, Theft Crime, Fraud Crime, Digital Economy

1. 问题的提出

在数字化浪潮席卷全球的当下，网络购物与线上交易已深度融入社会经济生活，成为民众日常消费的主要方式之一。据中国互联网络信息中心(CNNIC)发布的第 52 次《中国互联网络发展状况统计报告》显示，截至 2023 年 6 月，我国网络购物用户规模达 8.80 亿，占网民整体的 84.8%。在此背景下，电商平台、金融机构、生活服务平台为吸引用户流量、拓展市场份额，纷纷推出以电子优惠券、积分兑换、红包返现、专属折扣为核心的优惠活动，这些本意为让利消费者、激活市场活力的举措，却被部分不法分子异化为“牟利工具”，催生出网络“薅羊毛”行为。

起初，“薅羊毛”的概念最开始是由 1999 年央视春晚小品《昨天 • 今天 • 明天》让该说法流传开来，此后人们把在网络平台有选择性参与活动，低成本或零成本获物质实惠行为称作“薅羊毛”[1]。但随着互联网技术的迭代与黑灰产业链的渗透，“薅羊毛”逐渐偏离合法轨道：部分行为人通过技术爬虫抓取平台优惠信息、利用系统漏洞批量套取优惠券、伪造身份信息注册海量账号刷单套利，甚至形成“上游技术开发、中游批量操作、下游利益变现”的完整黑产链条。例如，2022 年某电商平台“618”大促期间，有团伙利用平台支付结算漏洞，以 0.1 元的价格购买原价数千元的电子产品，涉案金额超千万元；2023 年某金融 APP 推出“新用户注册送 10 元红包”活动，不法分子通过“接码平台”获取海量虚拟手机号，注册 20 余万个虚假账号，套取红包资金 200 余万元。

此类行为不仅直接损害平台与商户的经济利益——据行业统计，2023 年我国电商平台因“恶意薅羊毛”造成的损失超 500 亿元，更破坏了公平竞争的市场秩序：一方面，恶意“薅羊毛”挤占了正常消费者的优惠资源，导致合法用户无法享受应有的权益；另一方面，平台为弥补损失可能提高商品定价或缩减优惠力度，最终形成“平台受损—消费者买单”的恶性循环。此外，部分“薅羊毛”行为还伴随侵犯公民个人信息、破坏计算机信息系统等违法犯罪活动，对网络安全与公民权益构成双重威胁。

然而，司法实践中对网络“薅羊毛”行为的定性却存在显著分歧：同样是“利用漏洞套取优惠券”，部分法院以“盗窃罪”定罪处罚，部分法院认定为“诈骗罪”，还有法院认为行为未达到刑事处罚标准，仅作行政处罚。这种“同案不同判”的现象，既不利于保护当事人的合法权益，也削弱了刑法的指引与规制功能。因此，如何准确界定网络“薅羊毛”行为的法律属性、厘清其刑法定性的争议焦点、构建科学的定性规则，成为法学界与实务界亟待解决的重要课题。

2. 网络“薅羊毛”行为的界定与表现形式

2.1. “羊毛”的概念与属性

2.1.1. “羊毛”的概念界定

在网络“薅羊毛”的语境中，“羊毛”并非传统意义上的自然物，而是指网络平台为吸引用户、促进交易而创设的，能够为用户带来经济利益或消费权益的各类虚拟权益载体。结合司法实践与平台运营规则，“羊毛”的具体形态可分为以下四类：

电子优惠券：包括满减券、折扣券、品类券等，通常有使用门槛、有效期与适用范围限制，可在用户购物结算时直接抵扣价款。

积分与虚拟货币：积分如淘宝淘气值、京东京豆、美团成长值等，用户可通过消费、签到、评价等行为获取，积分达到一定数量可兑换商品、抵扣现金或升级会员权益；虚拟货币如平台专属代币，可通过充值或任务获取，用于购买平台内服务。

现金红包与补贴：包括平台直接发放的现金红包、消费返现、专项补贴等，通常可直接提现或用于平台内消费。

专属权益：如会员资格、优先购买权、服务折扣等，虽不直接体现为现金价值，但能为用户节省消费成本或带来额外便利。

2.1.2. “羊毛”的法律属性争议

“羊毛”的法律属性直接关系到网络“薅羊毛”行为的刑法定性——若“羊毛”属于刑法意义上的“财物”，则行为可能构成盗窃罪、诈骗罪等侵犯财产罪；若仅属于“计算机信息系统数据”，则可能构成非法获取计算机信息系统数据罪或不构成犯罪。学界对此存在两种对立观点：

观点一：“羊毛”属于计算机信息系统数据，而非财物

持该观点的学者刘明祥认为，“羊毛”缺乏传统财物的“有体性”与“价值稳定性”，不应纳入刑法“财物”范畴[2]。具体理由包括：其一，“羊毛”以电子数据形式存在于网络空间，无物理形态，无法像货币、商品一样被实际占有与控制，不符合“财物需具备客观实在性”的传统认知；其二，“羊毛”的价值依赖平台规则设定，具有极强的不确定性——平台可通过修改规则(如取消积分兑换功能、调整优惠券使用门槛)随时剥夺其价值，且不同平台的“羊毛”无法跨平台流通，缺乏统一的价值评估标准；其三，部分“羊毛”仅具有“使用价值”而无“交换价值”，如免费会员资格、专属折扣等，无法在市场上自由交易，不符合财物“可流通性”的核心特征。例如，某游戏平台的“虚拟金币”虽可在游戏内购买道具，但无法兑换为法定货币，其价值仅存在于平台封闭生态中，不应认定为财物。

观点二：“羊毛”具备财产属性，属于刑法意义上的财物

以张明楷、陈兴良为代表的学者主张，随着数字经济的发展，刑法对“财物”的认定应突破“有体性”限制，以“管理可能性、转移可能性、价值性”为核心判断标准，“羊毛”完全符合这三项要件，应认定为财物[3]。具体论证如下：其一，“羊毛”具有管理可能性——用户可通过账号密码控制“羊毛”的使用，平台也可通过技术手段对“羊毛”的发放、使用、核销进行全程管理，二者均具备对“羊毛”的支配权；其二，“羊毛”具有转移可能性——用户可通过赠送、转售等方式将“羊毛”转移给他人，部分“羊毛”甚至可直接提现为法定货币，具备明确的转移路径；其三，“羊毛”具有客观价值——一方面，“羊毛”可直接降低用户消费成本，其价值等同于等额法定货币；另一方面，“羊毛”可通过市场交易转化为经济利益，具备可衡量的交换价值[4]。例如，淘宝淘气值积分达到1000分可兑换“88VIP会员”，该会员每年可节省购物成本超千元，其价值已远超部分传统财物，若仅将其认定为计算机数据，将无法有效保护用户与平台的财产权益。

笔者认为，对“羊毛”属性的认定应采用“实质判断”标准，而非拘泥于形式特征。从司法实践来看，2017 年最高人民法院、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》已将“支付结算、证券交易、期货交易等网络金融服务的账号密码、数字证书”纳入“公民个人信息”保护范畴，间接承认了虚拟权益的法律价值；2022 年《关于办理危害计算机信息系统安全刑事案件应用法律若干问题的解释》进一步明确，“非法获取计算机信息系统数据或者非法控制计算机信息系统，违法所得五千元以上或者造成经济损失一万元以上的”应追究刑事责任，其中“违法所得”既包括法定货币，也包括“羊毛”变现后的利益。

2.2. 网络“薅羊毛”行为的特征与类型

2.2.1. 网络“薅羊毛”行为的核心特征

网络“薅羊毛”行为区别于传统侵犯财产行为的显著特征，主要体现在以下三方面：

行为动机的逐利性：无论是合法“薅羊毛”还是恶意“薅羊毛”，行为人的核心目的均为获取经济利益。合法“薅羊毛”是消费者利用平台规则最大化自身权益，而恶意“薅羊毛”则是通过非法手段追求超出正常消费范畴的利益，二者的区别仅在于手段的合法性，而非动机的本质。

行为手段的隐蔽性与技术性：网络“薅羊毛”行为依托虚拟网络空间实施，行为人无需与平台直接接触，可通过匿名账号、虚拟 IP、技术工具隐藏真实身份。尤其是恶意“薅羊毛”，往往伴随技术手段的滥用，如使用爬虫软件抓取优惠信息、利用“接码平台”获取虚拟手机号注册账号、通过群控设备批量操作账号等，这些手段不仅难以被平台实时监测，也给案件侦查取证带来极大困难。

行为后果的扩散性：传统侵犯财产行为的危害对象通常具有特定性，而网络“薅羊毛”行为的危害对象具有扩散性——一方面，恶意“薅羊毛”会挤占大量优惠资源，导致合法用户无法享受应有的权益；另一方面，平台为弥补损失可能调整运营策略，如提高商品定价、缩减优惠力度，最终损害全体用户的利益，形成“个体违法、群体受损”的扩散效应。

2.2.2. 网络“薅羊毛”行为的类型划分

结合行为手段与平台规则的关系，可将网络“薅羊毛”行为分为以下三类：

利用平台漏洞类行为：指行为人发现平台在技术代码或规则设置中存在的缺陷，通过该缺陷获取“羊毛”的行为。其中，“漏洞”可进一步分为“系统漏洞”与“规则漏洞”：系统漏洞是平台技术层面的缺陷，如代码编写错误导致的价格计算异常、支付接口漏洞导致的资金抵扣错误；规则漏洞是平台运营规则的缺陷，如未明确“新用户”的定义、未设置优惠使用的数量限制、未完善风控机制等。

借助技术手段刷单类行为：指行为人通过技术工具伪造交易记录或消费数据，以满足平台优惠活动条件，进而获取“羊毛”的行为。常见的刷单手段包括：使用脚本软件自动生成虚假交易订单、利用群控设备控制多账号互刷交易、伪造消费场景等。

恶意注册账号类行为：指行为人通过伪造身份信息、使用虚拟账号，注册海量平台账号，以获取“新用户专属羊毛”的行为。此类行为的核心是利用平台对“新用户”的优惠政策，通过多账号重复享受新用户权益牟利。常见的手段包括：利用“接码平台”获取虚拟手机号接收验证码，注册账号；购买他人身份证信息，伪造实名认证账号；使用虚拟机、模拟器等工具，模拟不同设备环境注册账号等。例如，2023 年某生活服务平台推出“新用户首次打车立减 20 元”活动，不法分子通过上述手段注册 10 余万个虚假账号，累计套取补贴 200 余万元。

3. 网络“薅羊毛”行为刑法定性的争议

网络“薅羊毛”行为的刑法定性争议，本质是对行为侵犯的法益、行为手段的法律属性、平台意志

的认定存在分歧，其中最核心的争议集中在“盗窃与诈骗的界分”以及“预设同意的判定”两大问题。

3.1. 盗窃与诈骗的争议：“机器能否被骗”

在网络“薅羊毛”案件中，行为人获取“羊毛”的对象通常是平台的智能系统，而非平台的工作人员，因此“机器能否被骗”成为区分盗窃罪与诈骗罪的关键——若机器能被骗，则行为可能构成诈骗罪；若机器不能被骗，则行为可能构成盗窃罪。学界对此存在两种对立观点。

3.1.1. “机器不能被骗”说

学者主张，诈骗罪的成立以“被害人产生认识错误”为核心要件，而机器不具备人类的认知能力，无法产生“认识错误”，因此“机器不能被骗”[5]。具体理由包括：其一，诈骗罪是针对“人”的犯罪，其本质是行为人通过欺骗手段使“人”陷入错误认识，并基于该错误认识处分财物，而机器仅能按照预设的程序执行指令，无自主判断能力，无法理解行为人的欺骗内容，更不可能陷入“认识错误”；其二，机器对行为人的指令仅能进行“形式审查”，而非“实质审查”——例如，平台优惠发放系统仅能审查用户账号是否符合“新用户”的形式条件，无法审查用户身份的真实性，这种“形式审查”的结果并非“认识错误”，而是程序执行的必然结果；其三，若承认“机器能被骗”，将扩大诈骗罪的适用范围，导致盗窃罪与诈骗罪的界限模糊。例如，行为人利用 ATM 机故障取走超额现金，若认为“ATM 机能被骗”，则应定诈骗罪，但实际上该行为属于“秘密窃取”，应定盗窃罪。

在网络“薅羊毛”案件中，持“机器不能被骗”说的学者认为，行为人获取“羊毛”的过程中，平台智能系统仅是按照预设程序执行指令，并未产生“认识错误”，因此行为不构成诈骗罪。若行为人通过秘密手段获取“羊毛”，且“羊毛”属于财物，则应定盗窃罪；若“羊毛”属于计算机信息系统数据，则可能构成非法获取计算机信息系统数据罪。例如，行为人利用平台系统漏洞，以 0.1 元的价格购买原价 1000 元的商品，系统仅是按照错误的价格代码执行结算指令，并未产生“认识错误”，行为人通过该手段秘密获取商品利益，应定盗窃罪。

3.1.2. “机器背后的人能被骗”说

以刘宪权教授为代表的学者主张，虽然机器本身不具备认知能力，但机器是按照人的意志运行的，机器的判断结果本质是“机器背后的人”的意志体现，因此“机器背后的人能被骗”[6]。具体理由包括：其一，随着人工智能技术的发展，现代平台的智能系统已具备“类人决策能力”，能够根据实时数据调整行为(如风控系统可识别“异常交易”并暂停优惠发放)，这种决策能力并非单纯的程序执行，而是“机器背后的人”的意志的延伸；其二，平台在设计智能系统时，会预设“对合法用户的信任”，即相信用户会遵守规则、提供真实信息，若行为人通过欺骗手段破坏这种信任，本质是对“机器背后的人”的欺骗，使平台基于错误认识处分“羊毛”[7]；其三，司法解释已间接承认“机器背后的人能被骗”——2004 年最高人民法院《关于审理诈骗案件具体应用法律的若干问题的解释》规定，“冒用他人信用卡在自动柜员机(ATM 机)上取款的，属于信用卡诈骗罪中的‘冒用他人信用卡’”，而信用卡诈骗罪是诈骗罪的特殊类型，该规定本质是承认“ATM 机背后的银行能被骗”。

在网络“薅羊毛”案件中，持“机器背后的人能被骗”说的学者认为，若行为人通过虚构事实、隐瞒真相的手段，使平台智能系统基于错误认识处分“羊毛”，则行为构成诈骗罪。例如，行为人伪造“新用户”身份信息注册账号，领取平台“新用户红包”，系统基于错误的身份识别结果发放红包，本质是“机器背后的平台”陷入了认识错误，因此行为构成诈骗罪。

3.1.3. 争议的核心与笔者观点

上述争议的核心，在于对“机器认知能力”与“平台意志载体”的理解差异：“机器不能被骗”说聚

焦机器的“工具属性”，认为其无独立认知能力，仅能机械执行程序；“机器背后的人能被骗”说则关注机器的“意志延伸属性”，认为其是平台意志的数字化体现。笔者认为，应结合数字时代智能系统的功能演变，采用“类型化判断”标准，而非绝对化的“能”或“不能”。

一方面，对于“弱智能机器”，其仅能执行单一预设程序，无异常识别、动态调整功能，如仅能根据“投币金额是否达标”决定是否出货，无法识别“假币”或“异常投币行为”，此类机器无“类人决策能力”，仅为纯粹工具，不存在“认识错误”的可能，利用其漏洞取财，应认定为盗窃罪。

另一方面，对于“强智能机器”，其具备“多维度判断”“异常行为预警”“动态规则调整”等功能，已超出“机械执行程序”的范畴，成为平台意志的有效载体。例如，某电商平台的优惠发放系统会综合“用户注册时间、登录设备、消费记录、收货地址”等 10 余项数据，判断用户是否为“真实新用户”，若发现“同一设备登录多账号”“收货地址高度相似”等异常情况，会自动暂停优惠发放——这种基于多维度数据的决策，本质是平台对“用户合法性”的判断，与人工审核的逻辑一致。此时，行为人通过虚构数据使系统误判为“真实用户”，本质是对“机器背后的平台意志”的欺骗，系统的错误决策即平台的“认识错误”，符合诈骗罪的构成逻辑。

在网络“薅羊毛”案件中，绝大多数行为针对的是“强智能机器”，因此需结合机器的智能程度区分定性：若机器为“强智能”，且行为人通过虚构事实、隐瞒真相使机器产生错误认识，定诈骗罪；若机器为“弱智能”，或行为人通过技术手段直接突破机器控制，定盗窃罪。

3.2. 预设同意的判定

“预设同意”是指平台在制定规则时，预先对“符合条件的用户获取‘羊毛’”的行为表示同意，其核心是“平台对财物转移的预先意志”。在网络“薅羊毛”案件中，若行为人获取“羊毛”的行为在平台“预设同意”范围内，则属于合法行为；若超出该范围，则可能构成犯罪。但司法实践中，“预设同意”的边界极难界定，核心争议集中在以下两方面：

3.2.1. 争议焦点：“规则漏洞是否属于预设同意范围”

部分观点认为，平台制定规则时应预见可能存在的漏洞，若未及时修正，应视为对“利用漏洞取财”的预设同意[8]。例如，某平台规则未限制“同一用户注册多账号领券”，行为人通过多账号领券，属于平台“默许”的行为，不构成犯罪。其理由是：平台作为规则制定者，负有“完善规则、防范漏洞”的义务，若因自身疏忽导致规则漏洞，应承担相应风险，不能将责任转嫁于行为人，否则会过度扩张刑法的规制范围，抑制用户的合理行为边界[9]。

另一部分观点则认为，预设同意的前提是“平台对行为的明知与认可”，规则漏洞是平台的“过失疏忽”，而非“主动认可”，因此利用漏洞取财超出预设同意范围[10]。例如，某平台因工作人员失误，将“满 200 减 20”优惠券误设为“满 20 减 20”，行为人大量领取并使用，不属于平台预设同意，因平台的真实意图是“针对高消费用户的优惠”，而非“所有用户的无门槛优惠”，行为人利用漏洞取财违背平台真实意志，可能构成犯罪。其理由是：预设同意的本质是“平台的真实意志”，规则漏洞导致的“形式同意”并非平台真实意图，若将其认定为预设同意，会纵容行为人利用平台过失牟利，破坏公平的市场秩序。

3.2.2. 笔者观点：以“规则文义 + 行业惯例 + 普通理性用户认知”为三重客观判断标准

判定“利用漏洞取财”是否属于预设同意，需脱离对平台事后态度的依赖，聚焦行为发生时的客观依据，分三步展开分析：

第一，以平台规则文义为首要依据。行为发生时平台公布的《用户协议》《活动规则》是预设同意的

核心载体，需优先对规则文字表述、逻辑结构进行字面解释——若规则明确限定行为范围，行为人突破限制则超出预设同意；若规则未明确限定，但文义隐含“符合商业常理”的前提，则需结合后续标准进一步判断。例如，某平台规则写“新用户首次消费立减”，文义未禁止多账号注册，但“新用户”的通常理解为“首次注册的真实自然人”，这是规则文义的隐含前提。

第二，结合行业惯例辅助判断。不同行业的优惠活动存在普遍共识，可作为规则文义的补充解释依据：电商平台的“新用户优惠”通常限定“1 个自然人 1 次参与资格”，金融 APP 的“注册红包”以“获取真实客户、促进后续交易”为目的，生活服务平台的“补贴”禁止“虚假交易套利”——这些行业惯例无需平台单独写明，应视为预设同意的隐含边界。若行为人行为违背行业惯例即便规则未明确禁止，也应认定超出预设同意范围。

第三，以普通理性用户认知为最终校验标准。“普通理性用户”是指具备正常认知能力、了解基本平台规则的用户，其对行为是否符合规则的判断，可反映行为是否背离“预设同意”的合理预期：若普通理性用户认为某行为属于“合理利用规则”，则属预设同意；若普通理性用户明确感知行为“超出正常消费范畴”，则超出预设同意。

综上，仅当行为同时满足“背离规则文义隐含前提”“违背行业普遍惯例”“超出普通理性用户认知”，且严重背离平台优惠的基本商业逻辑时，才能认定超出预设同意范围；反之，若行为符合规则文义、行业惯例与普通用户认知，即便存在规则表述瑕疵，也应视为平台预设同意，不构成犯罪。

4. 不同类型网络“薅羊毛”行为的刑法定性分析

4.1. 利用平台漏洞类行为的定性

利用平台漏洞类行为需依据漏洞的技术属性与平台意志，分为系统漏洞与规则漏洞两类定性。

4.1.1. 利用系统漏洞类行为：构成盗窃罪

系统漏洞是平台技术层面的缺陷，平台对漏洞无预设认知，也无同意财物转移的意志。行为人明知是技术故障仍利用其获取“羊毛”，主观上具有非法占有目的；客观上通过非欺骗手段秘密转移平台控制的财物，符合盗窃罪“秘密窃取”的核心特征。例如，某电商平台因系统错误将商品价格从 1000 元标为 10 元，行为人大量下单转售获利，即构成盗窃罪。若“羊毛”仅为无价值的计算机数据，则可能构成非法获取计算机信息系统数据罪。

4.1.2. 利用规则漏洞类行为：构成诈骗罪

规则漏洞是平台运营规则的缺陷(如未限定新用户账号数量)，行为人需通过虚构事实。系统基于错误信息误判行为人符合优惠条件，进而处分“羊毛”，符合诈骗罪“欺骗－认识错误－处分财物”的逻辑。例如，行为人利用他人身份信息注册多个虚假账号领取新用户红包，即构成诈骗罪。若行为符合平台优惠核心目的，则属于平台预设同意，不构成犯罪。

4.2. 借助技术手段刷单类行为的定性

此类行为以伪造交易记录为核心，需结合“羊毛”价值与行为危害定性。

4.2.1. 刷单套取优惠券/现金补贴：构成诈骗罪

优惠券与现金补贴具有明确财产价值，行为人通过脚本软件、群控设备伪造交易，使平台误认其满足优惠条件并发放利益。该行为不仅侵犯平台财产，还破坏交易数据真实性，影响平台运营决策。例如，某用户通过刷单套取“满 200 减 100”优惠券 200 张，即构成诈骗罪。

4.2.2. 刷单获取积分：区分价值定性

若积分价值较低且未造成平台重大损失，属“情节显著轻微”，由平台通过扣除积分、封禁账号等民事手段处理；若积分价值较高，则构成诈骗罪。若刷单同时破坏平台系统，则可能构成破坏计算机信息系统罪，按“从一重罪论处”。

4.3. 恶意注册账号类行为的定性

此类行为围绕“伪造身份获取新用户权益”展开，需结合信息属性与获利数额定性。

4.3.1. 使用真实公民个人信息注册：构成牵连犯

行为人购买、盗用他人身份证号、手机号等信息注册账号，既侵犯公民个人信息权，又通过虚假身份骗取“羊毛”。二者属“手段–目的”牵连关系，按“从一重罪论处”。例如，非法获取 100 条公民信息注册账号获利 1 万元，需根据主要危害选择罪名。

4.3.2. 使用虚拟身份信息注册：仅定诈骗罪

若使用“接码平台”获取的虚拟手机号注册账号，未侵犯公民个人信息权，仅需判断获利数额：获利 3000 元以上构成诈骗罪；不足 3000 元则属行政违法，由平台封禁账号或行政机关罚款处理。若注册后利用账号实施其他犯罪，则需数罪并罚。

5. 结论

网络“薅羊毛”行为的刑法定性需紧扣数字经济背景下平台规则、技术特征与刑法教义学的适配性，核心在于通过“类型化分析”厘清行为边界，避免“同案不同判”或“刑法过度介入”。

从行为本质看，网络“薅羊毛”并非单一行为，而是涵盖“利用漏洞”“技术刷单”“恶意注册”的多元行为集合，其定性需以“羊毛属性”为基础——凡具备“管理可能性、转移可能性、价值性”的“羊毛”，均应认定为刑法意义上的财物，这是后续定性的前提。在此基础上，需结合“机器智能程度”与“平台预设同意”进一步区分：针对“强智能机器”的欺骗行为(如伪造身份骗领新用户红包)，符合诈骗罪逻辑；突破平台控制的秘密取财行为(如利用系统漏洞套取优惠)，则契合盗窃罪构成；涉及公民个人信息或系统破坏的，还需关联侵犯公民个人信息罪、破坏计算机信息系统罪等罪名。

从司法实践导向看，对网络“薅羊毛”行为的规制需把握“双重平衡”：一方面，要通过精准定性打击恶意套利的黑灰产行为，保护平台与合法用户权益，维护数字市场秩序，避免“法不责众”的纵容心态；另一方面，要严格区分“刑事犯罪”与“民事违规”，对符合平台预设同意、获利轻微的行为，应通过平台民事追偿或行政监管处理，防止刑法过度扩张侵蚀公民合理行为空间。

从制度完善层面看，需推动“司法认定 + 平台治理”的协同：司法机关可通过发布典型案例、出台指导意见，明确“机器能否被骗”“预设同意判定”等争议问题的裁判标准；平台则应强化规则设计与技术风控，减少漏洞产生的同时，通过清晰的规则告知明确用户行为边界，从源头降低“薅羊毛”行为的刑法定性争议，最终实现数字经济中“创新发展”与“法律规制”的良性互动。

参考文献

[1] 李鑫. P2P 网贷市场中的“羊毛党”及其对平台的影响[J]. 金融评论, 2016, 8(6): 32-47, 122.

[2] 刘明祥. 再论用信用卡在 ATM 机上恶意取款的行为性质——与张明楷教授商榷[J]. 清华法学, 2009, 3(1): 74-86.

[3] 张明楷. 许霆案的刑法学分析[J]. 中外法学, 2009, 21(1): 30-56.

[4] 陈兴良. 在 ATM 机上存假币取真币的行为构成盗窃罪[J]. 中国审判, 2009(6): 82-83.

[5] 高国其. 机器诈骗犯罪浅议[J]. 中国刑事法杂志, 2010(3): 34-40.
[6] 刘宪权. 论新型支付方式下网络侵财犯罪的定性[J]. 社会科学文摘, 2017(10): 77-79.
[7] 董文辉, 程汀. 网络交易“薅羊毛”行为的刑法分析[J]. 中国检察官, 2019(6): 3-6.
[8] 赵国玲, 邢文升. 利用漏洞转移财物行为的刑法教义学分析[J]. 国家检察官学院学报, 2019, 27(2): 89-107.
[9] 车浩. 盗窃罪中的被害人同意[J]. 法学研究, 2012(2): 101-121.
[10] 姜涛. 网络型诈骗罪的拟制处分行为[J]. 中外法学, 2019, 31(3): 692-712.