E-Commerce Letters 电子商务评论, 2025, 14(12), 2745-2750
Published Online December 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14124172

Hans汉斯

电子商务领域下个人信息的保护研究

——以网络支付为例

杨　杰

贵州大学法学院，贵州　贵阳

收稿日期：2025年11月3日；录用日期：2025年11月21日；发布日期：2025年12月17日

摘　要

随着电子商务成为我国经济发展的关键，网络支付作为其核心环节，在带来巨大便利的同时，也使得个人信息保护面临严峻挑战。本文以网络支付为例，系统研究了电子商务中的个人信息保护问题。文章首先对电子商务及网络支付进行了简要概述，其次梳理了以《个人信息保护法》为核心的立法保护体系与行业自律机制构成的保护现状。进而，本文从法律文本、行业治理、企业内部及监管机关四个层面，深入剖析了当前保护体系存在的困境。针对当前存在的问题，研究提出了一套对应的实践措施：通过推动细化规则与整合体系以完善法律文本，通过构建行业自律与监督机制以强化行业治理，通过内控合规与技术赋能以压实企业责任，并通过创新协同监管与科技执法以提升部门效能。研究结论表明，电子商务个人信息保护亟需构建一个贯通法律、行业、企业与监管四个层面，以法治为基石、技术为手段、方能实现数字经济发展与个人权益保障的有机平衡。

关键词

电子商务，网络支付，个人信息保护，《个人信息保护法》

Research on the Protection of Personal Information in the Field of E-Commerce

—Taking Online Payment as an Example

Jie Yang

School of Law, Guizhou University, Guiyang Guizhou

Received: November 3, 2025; accepted: November 21, 2025; published: December 17, 2025

Abstract

With e-commerce becoming a key driver of China's economic development, online payment, as its

文章引用: 杨杰. 电子商务领域下个人信息的保护研究[J]. 电子商务评论, 2025, 14(12): 2745-2750.
DOI: 10.12677/ecl.2025.14124172

core component, brings significant convenience while also posing severe challenges to personal information protection. This paper takes online payment as a case study to systematically examine the issue of personal information protection in e-commerce. The article begins with a brief overview of e-commerce and online payment, followed by an analysis of the current protection landscape, which consists of a legislative safeguard system centered on the "Personal Information Protection Law" and industry self-regulation mechanisms. Subsequently, the study delves into the existing challenges in the current protection framework from four dimensions: legal provisions, industry governance, corporate internal compliance, and regulatory oversight. To address these issues, the research proposes a set of corresponding practical measures: refining rules and integrating systems to improve legal provisions, establishing industry self-regulation and supervision mechanisms to strengthen industry governance, enhancing internal compliance and technological empowerment to reinforce corporate responsibility, and innovating collaborative supervision and technological enforcement to boost regulatory efficiency. The findings indicate that personal information protection in e-commerce urgently requires the construction of a comprehensive system spanning legal, industry, corporate, and regulatory dimensions, with the rule of law as the foundation and technology as the means, to achieve a balanced development between digital economy growth and personal rights protection.

Keywords

E-Commerce, Online Payment, Personal Information Protection, "Personal Information Protection Act"

1. 引言

在数字经济成为全球经济增长新引擎的宏观背景下，我国的电子商务实现了跨越式发展。然而，其爆发式增长在深刻改变消费生态与经济结构的同时，也使得作为其核心支撑的网络支付环节，成为个人信息泄露与滥用的高风险区。“大数据杀熟”、支付数据违规共享、跨境数据主权冲突等问题频发，暴露出当前个人信息保护体系在操作性、协同性与前瞻性上的多重不足[1]。现有研究多集中于法律条文解释或技术治理单一路径，缺乏对法律、行业、企业与监管等多维度治理框架的系统整合，尤其缺乏对网络支付这一高风险场景下法律、行业、企业、机关部门之间联系的深入理论解构。本文在既有研究基础上，试图构建一个多层次、动态协同的治理体系，弥补现有研究在系统性与操作性上的不足。鉴于此，本文将研究视角聚焦于网络支付这一具体且高风险的应用场景，旨在系统剖析其个人信息保护的特殊性、现实困境与治理路径，为数字经济时代的安全保障提供参考。

2. 电子商务与网络支付概述

2.1. 电子商务的发展与特征

电子商务，通常指通过互联网等信息网络销售商品或提供服务的经营活动。根据国家统计局数据，2024 年，全国网上零售额 155,225 亿元，比上年增长 7.2%。其中，实物商品网上零售额 130,816 亿元，增长 6.5%，占社会消费品零售总额的比重为 26.8%，其作为国民经济关键地位日益凸显。电子商务以其突破时空限制、降低交易成本、重构产消关系的典型特征，催生了直播电商、社交电商、跨境电商等多

元化商业模式[2]，形成了规模庞大、结构复杂的线上交易生态。

2.2. 网络支付的模式与核心地位

网络支付是用户通过互联网、移动网络等远程渠道，发起和执行的电子支付行为。它是电子商务完成交易的“临门一脚”，也是其不可或缺的关键基础设施。根据中国互联网络信息中心(CNNIC)数据，截至 2025 年 6 月，我国网络支付用户规模已达 10.22 亿，占网民整体的 91.0%。伴随智能手机的普及率提高和电子商务的蓬勃发展，中国的网络支付市场出现了爆炸性增长，移动支付用户数量急剧攀升，各类在线支付平台如支付宝、微信支付相继涌现，并迅速率先占据亚洲乃至全球市场的主导位置[3]。其核心地位体现在：一方面，它整合了用户的身份信息、银行账户、交易习惯等高度敏感的个人信息；另一方面，其高效、便捷的特性是保障电子商务流畅体验、留住用户的基础。正因如此，网络支付环节也成为个人信息安全风险聚集和传导的关键部分。

3. 网络支付下个人信息保护现状

3.1. 立法保护

我国已初步形成了一套层次分明、覆盖面广的个人信息保护法律体系，为网络支付场景下的信息治理提供了坚实的法律依据。

在顶层设计层面，2021 年 11 月 1 日正式实施的《中华人民共和国个人信息保护法》具有里程碑意义。它确立了以“告知–同意”为核心的个人信息处理规则，为网络支付平台处理用户数据划定了基本红线。其第二十八条更将支付账户、交易记录等金融信息明确列为“敏感个人信息”，要求只有在具有特定的目的和充分的必要性[4]，并采取严格保护措施的情形下，方可处理，这为支付信息提供了更高层级的保护标准。

在专门领域规制上，《电子商务法》明确规定了电子商务经营者对用户个人信息的保护义务与安全保障责任；《网络安全法》则确立了关键信息基础设施运营者的数据本地化与出境安全评估要求。特别值得注意的是，新修订并于 2025 年 10 月 15 日施行的《中华人民共和国反不正当竞争法》明确规定第十三条“经营者利用网络从事生产经营活动，应当遵守本法的各项规定。经营者不得利用数据和算法、技术、平台规则等，通过影响用户选择或者其他方式，实施下列妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为”，这为打击通过非法获取、滥用支付数据进行的恶性竞争行为提供了新的法律武器。

在监管执法层面，国家网信办、工业和信息化部、市场监管总局等相关部门持续开展专项整治行动，对违法违规处理个人信息的平台企业进行约谈、下架应用乃至高额处罚，形成了相当的法律威慑力。

3.2. 行业保护

除法律强制规范外，行业自律与企业内部治理在个人信息保护中也扮演着重要的角色。

一方面，主要的网络支付平台，如支付宝、微信支付等，为应对严格的法律监管和提升用户信任，已逐步建立起一套内部合规风控体系。这包括设立数据保护官(DPO)、制定内部数据安全管理规范、对员工进行隐私保护培训等。

另一方面，行业自律组织也在积极发挥作用。中国支付清算协会等机构定期发布行业风险提示与最佳实践指南，推动成员单位共同遵守更高的数据安全标准。此外，在《个人信息保护法》的推动下，大型平台企业开始承担起“守门人”责任，不仅需要管理自身行为，还需对其平台内经营者的个人信息处理活动进行监督，初步形成了“平台自查 + 行业监督 + 行政监管”的多重防护格局。

4. 网络支付下个人信息保护存在的问题

4.1. 法律文本层面

法律规定分散且系统性不足。目前我国关于用户信息保护的规定散见于《民法典》《个人信息保护法》《网络安全法》等多部法律以及各类部门规章中。这种分散化的立法模式缺乏系统性，导致网络支付机构在合规实践中需要参照多个法律文件，增加了合规难度与法律适用的不确定性。

部分条款原则性强但操作性有待细化。尽管《个人信息保护法》确立了以“告知–同意”为核心的个人信息处理规则，但在网络支付这一具体场景中，如何准确界定“必要原则”、如何在具体业务流程中落实“最小必要原则”，“最小”和“必要”的概念不确定性亦会增加原则适用的难度[5]，这些问题仍需更细致的指引。

4.2. 行业自身治理层面

行业自律性不足。网络支付运营商在巨大的经济利益驱使下，未能建立起有效的内部自律规范。有的会在用户不知情的情况下，将获取的用户信息进行商业化处理或提供给其他机构，行业自律性的不足直接导致了用户信息的泄露和滥用。

行业标准执行力与内部监督机制弱。虽然中国支付清算协会发布了《个人支付信息保护指引》等团体标准，但对单位的约束力和标准的实际执行效果仍有待观察。同时，部分运营商内部监管、惩罚机制不完善，难以确保工作人员严格依照内部规定处理用户信息，对违规人员的惩戒也往往未能起到应有的警示作用。

4.3. 企业层面

企业内部管理与技术防护存在漏洞。企业内部的管控漏洞是信息泄露的主要风险源之一。例如，2025年初，澳大利亚急救机构 Ambulance Victoria 公布了一起罕见却典型的内部数据泄露事件：一名前员工在离职前，将包含数千名员工的敏感信息复制并带离，包括住址、工资信息和银行账户等。这暴露出企业在内部权限管理和员工行为监控方面存在严重短板。此外，部分支付机构，尤其是中小机构，在网络安全技术投入上相对不足，系统防护能力薄弱，易成为网络攻击的目标。

企业用户界面设计与告知义务履行不规范。在实际操作中，部分企业未能以清晰、明确的方式履行告知义务，甚至存在故意误导用户的行为。如 2018 年“支付宝年度账单事件”，支付宝在不显眼处默认勾选“我同意《芝麻服务协议》”选项，既可以“直接向第三方提供相关信息”，也有权“不支持撤销对第三方的信息查询授权”。这种通过默认勾选同意方式收集用户信息，不符合国家标准精神。这种“诱导同意”[6]或“强制同意”的做法，实质上是对用户的知情权和选择权极度不尊重甚至是侵犯。

4.4. 部门机关层面

部门监管职责交叉与协同执法挑战。网络支付监管涉及央行、网信办、工信部、市场监管总局等多个部门。虽然《个人信息保护法》第六十条已经明确了国家网信部门的统筹协调地位，但在实践中，多头监管和职能交叉的问题依然存在。这可能导致监管重叠或监管真空[7]，也可能因不同部门间的执法标准和尺度不一，给企业合规带来困扰，并影响法律实施的整体效果。

部门监管技术能力与执法效率面临挑战。面对快速更新的网络支付技术和海量的数据处理活动，监管部门同样面临技术能力与执法资源不足的挑战。有研究指出，部分执法部门可能存在技术水平有限、对法律理解不到位的情况，这会影响执法效率和对违法行为的精准打击。此外，一些基层监管组织在技术手段的应用上可能存在滞后，容易形成监管的薄弱区。

5. 网络支付下个人信息保护的实践措施

对于上述所提到的四大层面问题，本部分提出一套系统化的治理方案，旨在有效化解网络支付中的个人信息保护困境。

5.1. 推动细化规则与整合体系

为解决法律规则分散的问题，必须推动法律文本从“有法可依”向“有细则可循”的转向。首先建议监管部门，联合制定具有高度针对性的实施细则。该细则应明确核心概念，对“必要个人信息范围”、“用户同意有效性标准”、“匿名化处理的技术要求”等关键概念作出清晰界定，为司法裁判和行政执法提供统一尺度。其次引入场景化应用规则[8]，针对支付开户、营销推广、跨境结算等不同业务场景，设定差异化的个人信息收集、使用和存储规范，提升法律的可操作性，再者应该加强法律体系的内部协调，启动对《个人信息保护法》《电子商务法》《反不正当竞争法》等相关条款的立法完善，消除一些潜在的法律适用冲突，构建内在统一、相互支撑的个人信息保护法律体系。

5.2. 构建自律标准与监督机制

为弥补行业自律机制的不足，应充分发挥行业组织的引领作用，将软性约束转化为硬性规范。

第一，制定并推行更高标准的行业公约。由中国支付清算协会等行业组织牵头，制定网络支付行业个人信息保护公约，并建立配套的认证与评估体系。对严格遵守公约的企业给予公开表彰，并在业务创新、资质申请等方面提供便利，形成正向激励。

第二，建立行业内部的黑名单共享与联合惩戒制度。设立行业性的信息共享平台，对查实存在严重违规收集、滥用用户信息的机构及从业人员纳入黑名单，并在成员单位间进行通报，实施联合业务限制，大幅提高其违法违约成本。

5.3. 强化内控合规与技术赋能

针对企业内部漏洞与设计缺陷，必须将保护义务从法规文本转化为实际行动。

首先企业需要建立健全数据安全管理体系：企业，特别是大型平台企业，应严格落实《个人信息保护法》第五十八条规定的对个人信息保护义务。其次要设立独立监督机构：设立直接对董事会负责的数据保护官(DPO)和独立的内审机构，定期开展数据安全审计与风险评估。再者企业应强化技术防护：加大对数据加密、脱敏、防泄漏等安全技术的投入，并建立严格的内部权限管理制度，确保员工只能访问其职责必需的最小范围数据。践行“设计即隐私”与“默认即隐私”理念：在产品研发和界面设计的初始阶段，就将个人信息保护作为核心要素嵌入其中。再而对于 APP 用户界面要进行优化：彻底摒弃“支付宝年度账单”事件中默认勾选等误导性设计，确保用户在充分知情的前提下进行授权。最后设置用户权限管理：为用户提供清晰、便捷、持续的权限管理入口，允许用户随时查看、修改和撤回授权。

5.4. 创新监管模式与提升执法效能

为应对监管交叉与能力挑战，监管机关必须转向智慧监管、协同监管。

第一，构建部门协同执法机制：在中央网信办的统筹协调下，由央行、工信部、市场监管总局等部门参与，设立跨部门“数据安全联合办公室”。其核心职能包括：(1) 制定统一的网络支付个人信息保护执法标准与裁量标准；(2) 协调重大复杂案件的跨部门联合执法行动；(3) 建设并管理全国性的“网络支付合规与风险信息共享平台”，归集各部门监管信息与违规数据；(4) 组织开展针对性的监管科技研发与应用培训。

第二，统一执法标准：部门之间要共同制定具体执法指南，明确案件移送与联合调查程序，避免多头执法与监管套利。

第三，建设信息共享平台：部门间要着手打通数据壁垒，实现对支付机构合规状况的实时、全景式洞察。

第四，提升监管科技应用水平：监管部门应积极运用大数据、人工智能等技术手段，引进市场高水平检查科技，开发自动化合规监测系统，对网络支付平台的数据处理活动进行动态监测与风险预警。同时，加强对基层执法人员的专业技术培训，并配发便携式取证设备，全面提升对新型数据违法行为的发现与查处能力。

6. 结论

本研究以网络支付为例，深入剖析了电子商务领域个人信息保护的现状、挑战与出路。研究表明，在数字经济高速发展的背景下，网络支付中的个人信息安全已不再是一个单纯的技术或管理问题，而是一个涉及法律、技术、经济的复杂工程。

当前，我国已在立法层面构建了较为完善的顶层设计，但法律原则在具体场景的落地实施仍面临监管协同、规则实效、技术风险与跨境协调等多重考验。未来的保护工作，必须超越静态、孤立的治理模式，转向构建一个动态、联合协调的治理框架。这一框架应以《个人信息保护法》的严格实施为根本保障，以先进技术为主要防护，以平台、行业、用户和监管方的多元共治为关键支撑，并以积极的国际规则对话为外部助力。

唯有通过多方协作、多管齐下，才能有效应对不断演变的风险，最终在激发数字经济活力的同时，坚实筑牢个人信息的法律保护屏障，实现发展与安全之间的动态平衡。

参考文献

[1] 王迪羽珊. 大数据“杀熟”中消费者权益保护问题研究[J]. 中国品牌与防伪, 2025(8): 71-73.

[2] 石林. 数字经济推动电子商务高质量发展的实践路径[J]. 商场现代化, 2025(20): 55-57.

[3] 王涛. 数字经济背景下我国网络支付市场的竞争政策与创新发展[J]. 中国经贸, 2024(32): 37-39.

[4] 王嫔梅, 韩廷峰. 告知同意原则的理解与适用[J]. 法制博览, 2024(20): 7-10.

[5] 胡李楠. “最小必要原则”适用的解释路径[J]. 法律方法, 2023, 45(4): 360-377.

[6] 陈梦蕾, 罗颖嘉, 朱侯. 基于扎根理论和机器学习的隐私政策诱导同意研究[J]. 信息资源管理学报, 2024, 14(5): 75-90.

[7] 李禹霏, 陆静. 我国金融监管体制的主要问题及改革建议[J]. 现代商业, 2017(18): 187-188.

[8] 郑树明. 论个人数据的场景化保护[J]. 中国价格监管与反垄断, 2025(9): 88-90.