

浅析当代社会网络支付中的法律问题

郑晓丽

贵州大学法学院, 贵州 贵阳

收稿日期: 2025年3月20日; 录用日期: 2025年4月9日; 发布日期: 2025年5月13日

摘要

随着智能手机的普及和移动互联网的发展, 网络支付用户规模持续扩大, 从城市到农村, 从年轻人到老年人, 越来越多的人开始使用网络支付。网络支付普遍化、便利化的同时也存在着许多的安全隐患, 尤其是当代社会网络支付的法律问题显得尤为重要。本文探讨了网络支付中的主要法律风险, 包括用户隐私保护、交易安全、数字鸿沟等。当前法律框架在应对新兴支付技术时存在滞后性, 导致消费者权益保护不足等问题。通过分析上述风险, 本文提出完善网络支付法律体系的建议, 如强化数据安全规范、明确各方权责等, 以促进网络支付行业的健康发展, 平衡技术创新与风险防控。

关键词

网络支付, 支付安全, 第三方支付, 法律规定

A Brief Analysis of Legal Issues in Online Payment in Contemporary Society

Xiaoli Zheng

School of Law, Guizhou University, Guiyang Guizhou

Received: Mar. 20th, 2025; accepted: Apr. 9th, 2025; published: May 13th, 2025

Abstract

With the popularization of smart phones and the development of the mobile Internet, the scale of online payment users has continued to expand. From cities to rural areas, from young people to the elderly, more and more people have begun to use online payment. While online payment has become widespread and convenient, there are also many security risks. Especially in contemporary society, the legal issues of online payment are particularly important. This article discusses the main legal risks in online payment, including user privacy protection, transaction security, and the digital divide. The current legal framework lags behind in dealing with emerging payment technologies,

resulting in insufficient protection of consumer rights and interests. Through the analysis of the above risks, this article puts forward suggestions for improving the legal system of online payment, such as strengthening data security regulations and clarifying the rights and responsibilities of all parties, to promote the healthy development of the online payment industry and balance technological innovation and risk control.

Keywords

Online Payment, Payment Security, Third-Party Payment, Legal Regulations

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

随着互联网技术的飞速发展和智能设备的普及,数字化浪潮席卷全球,深刻改变着人们的生活方式。其中,网络支付作为数字经济的重要组成部分,以其便捷、高效、安全的特性,迅速融入人们的日常生活,成为现代社会不可或缺的支付方式。从线上购物、外卖点餐到线下扫码支付、公共交通出行,网络支付已深度融入人们的衣食住行,覆盖了日常生活的方方面面,成为不可或缺的一部分。然而,其快速发展也带来了一系列潜在的法律问题。

2. 当前我国关于网络支付的立法现状

在数字化时代,随着网络信息技术的迅猛进步与发展,网络犯罪逐渐成为主要的犯罪类型之一。为了有效规制此类行为,我国相继出台了一系列专门的法律条例,旨在打击网络犯罪、保护用户信息安全并维护网络空间的秩序。

2021年1月22日,中国人民银行发布《非银行支付机构客户备付金存管办法(修订)》,进一步规范客户备付金管理,强化支付机构的风险防控责任,保障用户资金安全;2021年,全人常发布《中华人民共和国数据安全法》,规范数据处理活动,保护个人和组织的数据安全,为网络支付中的数据保护提供法律依据;2021年8月,《中华人民共和国个人信息保护法》,明确个人信息处理规则,强化对个人信息的保护,防止网络支付中的信息泄露和滥用;2022年,中国人民银行发布《网络支付安全技术规范》,制定网络支付安全技术标准,要求支付机构采用先进技术手段保障交易安全;2023年11月24日,国务院常务会议审议通过《非银行支付机构监督管理条例》,着力营造稳定、透明、规范、可预期的法治化营商环境,有利于促进支付服务市场长期规范健康发展。在我国目前现有的法律当中没有对第三方支付平台个人信息进行精准的定义,以《金融机构客户保护法》第28条规定:“本办法所称客户金融信息,是指银行、支付机构通过开展业务或者其他合法渠道处理的客户消息,包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他与特定客户购买、使用金融产品或者服务相关的信息”作为基础,结合关于个人信息的分类即基本个人信息、伴生个人信息和预测个人信息[1]。

我国针对网络支付的法律法规体系不断完善,涵盖了支付机构管理、用户资金安全、数据保护等多个方面。这些法律法规为网络支付行业的健康发展提供了坚实的法律保障,同时也为应对新兴技术带来的挑战奠定了基础。虽然存在《中华人民共和国消费者权益保护法》为基础,《人民银行法》《中国人民银行金融消费者权益保护实施办法》作为补充的保护框架。但是,我国尚未出台一部专门针对金融消费

者权利保护的综合性法律,相关权益保护内容分散在多部法律法规和政策文件中,缺乏系统性和协调性。

3. 网络支付存在的安全隐患与问题

3.1. 用户信息隐私保护

网络支付依赖于用户提供大量个人信息,这些数据在传输、存储和使用过程中面临多重风险,使得隐私保护成为亟待解决的难题。首先,数据泄露风险是网络支付隐私保护的主要威胁之一。支付平台和金融机构存储着海量用户数据,一旦遭遇黑客攻击或系统漏洞,这些敏感信息可能被窃取并用于非法活动。近年来,全球范围内多次发生大规模数据泄露事件,导致数百万用户的支付信息外流,给个人隐私和财产安全带来巨大威胁。其次,数据滥用问题日益突出。一些支付平台和第三方服务商在用户不知情或未明确同意的情况下,过度收集和使用用户数据,甚至将数据出售给广告商或其他商业机构。这种数据滥用不仅侵犯了用户的隐私权,还可能导致用户被精准营销、骚扰电话甚至诈骗信息困扰。此外,技术依赖与透明度不足也加剧了隐私保护问题,当前的信息处理技术使得信息的可识别性在直接可识别与不可识别的双重状态徘徊,但却始终未能实现匿名性的极致[2]。网络支付的技术复杂性使得普通用户难以了解其数据如何被收集、存储和使用。许多支付平台在隐私政策中使用晦涩难懂的法律术语,用户往往在未充分理解的情况下同意条款,导致隐私保护意识薄弱。最后,跨境支付中的隐私风险也不容忽视。在全球化背景下,跨境支付涉及不同国家和地区的法律法规,数据流动可能面临监管空白或冲突。用户的支付数据在跨境传输过程中可能被第三方截获或滥用,增加了隐私泄露的风险。

大数据技术在网络支付中的应用虽然提升了便利性,但也存在漏洞,容易导致信息泄漏。数据时代,个人信息的高价值使许多网络平台“迷失”,不以隐私政策为准则,过度收集个人信息[3]。数据传输过程中若未充分加密容易被截获,并且数据分析中的隐私保护不足,可能导致用户敏感信息被滥用。此外,大数据隐私保护技术存在一定的漏洞,诸如数据盗窃、对抗性攻击、加密解码、安全数据存储问题、交易日志管理、端点验证及实时安全监控等。这些缺陷导致在信息传递过程中,数据信息的监管力度不足,缺乏必要的技术支持。技术治理的滞后,不仅削弱了移动支付平台抵御恶意攻击的能力,也为攻击者在移动社交平台上实施攻击提供了机会。此类安全漏洞可能导致用户信息泄露,显著增加支付过程中遭受恶意攻击的风险,对个人、企业乃至整个社会产生负面影响,最终导致更为严重的经济损失。

3.2. 用户资金安全问题

信息化网络支付的普及使得个人信息泄露风险显著增加。用户在支付过程中需提供银行卡号、身份证信息、手机号等敏感数据,这些信息可能因支付平台技术漏洞、黑客攻击或内部人员泄露而外流[4]。此外,部分支付平台过度收集用户数据,甚至将数据用于商业营销或非法交易,进一步加剧了隐私泄露问题。同时,网络支付平台可能遭受网络攻击,导致用户资金被盗或支付系统瘫痪。此外,诈骗、钓鱼网站等也威胁着用户的资金安全。随着网络信息技术的高速发展,网络诈骗的手段和方法也随之更新和变化,成为数字化时代最主要的犯罪类型。根据中国公安部数据显示:2020年,破获网络诈骗案件32.2万起,同比上升60%以上;2021年,网络诈骗案件数量持续增长,公安部开展的“断卡行动”共打掉“两卡”违法犯罪团伙4.2万个。而电信网络诈骗、网络赌博等违法犯罪活动主要通过网络支付途径转移、清洗资金。

3.3. 数字鸿沟问题

所谓的数字鸿沟是指不同社会群体之间在获取、使用信息技术和数字资源方面存在的差距。2024年年末,全国60岁及以上老年人口已达3.10亿人,占全国人口的22%,其中65岁及以上老年人口达2.20

亿人，占全国人口的 15.6% [5]。而在当今人口老龄化愈发严峻的时代，老年群体的数字鸿沟问题显得尤为重要。部分老年人对智能手机和网络支付操作不熟悉，难以享受数字化支付的便利，甚至可能因操作失误造成经济损失。在一些偏远地区，网络基础设施不完善，网络支付的普及率较低，导致这些地区的人群无法享受数字化支付的红利。

3.4. 第三方支付平台的风险

随着数字经济的快速崛起和电子支付的普及，作为网络支付方式之一的第三方支付已在我国支付体系中占据重要地位。杨彪认为“我国第三方支付的发展历程概括为四个阶段：起初的网关支付阶段，随后进入信用中介阶段，然后发展到行业支付应用阶段，最终进入一个规范与成长并重的阶段。在十多年的时间里，第三方支付行业在交易规模、机构数量以及消费者接受度等方面实现了飞跃式的发展，并已成为我国支付服务市场和金融经济发展中一支不容忽视的力量。” [6]第三方支付是指由独立于买卖双方的第三方机构提供的支付服务，作为交易中介，保障资金安全并促进交易完成。第三方支付通过提供安全、便捷的支付服务，已成为现代支付体系的重要组成部分，主要包括支付宝支付、微信支付等，然而这些便利支付也随之带来了不少的安全漏洞。

第三方支付以其高效的支付能力著称，但其安全性始终是人们关注的焦点。检察机关在办案中发现，在非法集资、电信网络诈骗、网络赌博、非法经营“地下钱庄”等多种犯罪活动中，不法分子利用第三方支付作为支付结算通道，非法收付、转移违法犯罪资金[7]。在第三方支付行业中，支付效率与安全性的矛盾尤为突出，尤其是在非授权行为的事后责任分担机制尚未明确的情况下。目前，现行法律对此类问题缺乏有效的解决方案，相关研究也相对不足。第三方支付作为新兴的网络技术，正以高速不断发展和更新，极大地推动了支付方式的变革。然而，法律的发展往往滞后于现实社会的快速变化，导致现有法律法规难以全面覆盖第三方支付领域的新问题和新挑战，由此产生了诸多法律漏洞和监管空白。这些漏洞不仅可能引发资金安全、用户隐私保护等方面的风险，还可能为不法分子提供可乘之机。因此，亟需完善相关法律法规，以应对第三方支付快速发展带来的复杂局面。

4. 关于网络支付存在的安全隐患与问题的完善

对于本文前述的网络支付所存在的安全隐患以及法律漏洞，作者认为应该从以下几点进行改善弥补。

4.1. 加强用户信息隐私保护

首先，应该利用技术措施加强对于用户信息隐私的保护。技术措施作为保护用户隐私的有效手段，要不断的升级更新最新的技术加以保护用户的信息隐私，防止出现技术漏洞而泄漏用户信息隐私。隐私保护技术涵盖数据加密技术、匿名化处理技术和访问控制技术[8]。对存储在数据库或文件系统中的敏感信息进行加密，防止数据泄露时被恶意利用。此外，在我国《中华人民共和国宪法》和《中华人民共和国民法典》当中只笼统地规定了公民享有隐私权的原则性规定，缺乏具体的规定，尤其是在当今大数据时代背景下关于网络用户的隐私权内容。作者认为应当出台专门的网络用户隐私权保护的具体法规，明确其适用范围、判定标准以及赔偿救济等内容。同时，明确用户信息处理规则，保障用户知情权和选择权，完善用户信息保护制度，防止用户的信息泄漏，支付机构处理用户信息应当遵循合法、正当、必要和诚信原则，公开用户信息处理规则，明示处理用户信息的目的、方式和范围，并取得用户同意。最后要推动建立争议纠纷多元化解机制，保障用户权利救济渠道，支付机构应当及时妥善处理与用户的争议，履行投诉处理主体责任，切实保护用户合法权益，鼓励用户和支付机构之间运用调解、仲裁等方式解决纠纷，推动纠纷高效解决。

4.2. 保障用户资金安全

平台需要明确支付服务协议公平原则,保障用户公平交易权,同时以公平监管保障行业公平竞争,强化全链条全周期监管,维护行业良性发展秩序,切实防范业务异化、资金挪用、数据泄露等风险。通过机器学习和大数据分析,实时监控交易行为,识别异常交易(如大额支付、异地登录等)并触发风险控制机制。

4.3. 缩小数字鸿沟

在时代快速前进的步伐中应当注重保障弱势群体的权利,加强关注老年人群体的智能需求。建立老年人数字需求服务平台,发挥基层自治组织以及家庭单位的作用积极推动老年人智能技术的提高和运用,消除老年人群体的信息障碍。在社区、老年活动中心等场所开设免费的数字技能培训班,教授老年人如何使用智能手机、电脑和常见应用程序。制作适合老年人的图文并茂或视频教程,内容涵盖基础操作、网络安全知识等。加强农村和偏远地区的网络基础设施建设,确保老年人享受到数字化服务[9]。

4.4. 规范第三方支付平台

第三方支付平台的规范化至关重要,这不仅关系到用户资金安全,还涉及数据隐私、市场秩序和社会稳定。第三方平台应当承担起其社会责任,增强平台的安全性。不断完善平台的安全技术,防止用户信息隐私的泄漏以及不法分子的乘虚而入[10]。

在金融科技快速发展,新型金融产品和服务层出不穷的社会背景下,应该尊重和体现社会发展的客观规律,加快建立一部综合性专门法律,整合现有规定,填补监管空白,形成统一的保护框架,不断提高法律质量,推进科学立法、民主立法,专门法律能够及时应对新风险,规范金融机构行为,维护金融市场秩序,这不仅是保护金融消费者权益的迫切需要,也是推动金融市场健康发展的关键举措。

5. 结语

大数据时代的到来极大地推动了网络信息技术的进步,促进了网络支付的多样化和便利性,使得支付方式更加智能和高效。然而,与此同时,它也带来了一系列新的安全隐患,如数据泄露、隐私侵犯、网络诈骗等问题,对用户的信息安全和资金安全构成了潜在威胁。因此,在享受技术红利的同时,必须高度重视并有效应对这些安全挑战。本文从这一时代背景出发,浅析了网络支付中存在的主要安全隐患和问题,具体包括用户信息隐私安全、用户资金安全、信息泄露、老年群体的“数字鸿沟”以及第三方支付平台的风险。通过对上述问题的探讨,本文进一步分析了我国当前在网络支付领域的立法现状,并提出了粗浅的个人建议。希望这些思考能为完善网络支付的安全机制和法律监管提供一定的参考,推动网络支付在安全与便利之间实现更好的平衡。

参考文献

- [1] 邢会强. 大数据时代个人金融信息的保护与利用[J]. 东方法学, 2021(1): 47-60.
- [2] 万方. 隐私政策中的告知同意原则及其异化[J]. 法律科学(西北政法大学学报), 2019, 37(2): 61-68.
- [3] 齐爱民. 信息法原论[M]. 武汉: 武汉大学出版社, 2010: 76.
- [4] 张衡. 大数据时代个人信息安全规制研究[M]. 上海: 上海社会科学院出版社, 2020: 239.
- [5] 金牛, 于韦翔. 养老服务机器人化转型的发展基础、现实困境与优化路径——基于 TOE 理论的视角[J/OL]. 科学与管理, 1-11[2025-03-05]. <https://link.cnki.net/urlid/37.1020.G3.20250226.0952.002>
- [6] 曹红辉, 等, 著. 中国电子支付发展研究[M]. 北京: 经济管理出版社, 2012.

-
- [7] 李红虹. 第三方支付的风险及其防范[J]. 今日财富, 2024(11): 62-64.
 - [8] 欧明建. 大数据背景下企业会计信息化建设存在的问题及对策研究[J]. 商业会计, 2020(16): 115-117.
 - [9] 王宇. 老龄社会的网络传播需考虑“适老化”问题[J]. 现代视听, 2020(11): 94.
 - [10] 魏绚兮. 安全漏洞频现电子商务中第三方支付的安全性有待加强[J]. 中国商界, 2024(10): 24-25.