E-Commerce Letters 电子商务评论, 2024, 13(4), 1594-1600
Published Online November 2024 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2024.1341312

Hans汉斯

网络支付APP中用户信息安全的法律问题研究

苏渝婷

贵州大学法学院，贵州 贵阳

收稿日期：2024年8月8日；录用日期：2024年10月30日；发布日期：2024年11月6日

摘 要

在大数据时代，网络支付因其便捷性而得到了人们的广泛使用，但由于部分网络支付APP在用户不知情的情形下会擅自读取手机号码、地理位置、通讯录等用户信息，这就不可避免地导致近年来用户信息被过分读取、泄露的案件屡禁不止。为营造安全健康的网络支付运营环境、切实提升用户安全感，通过法条检索、文献梳理的方法研究发现虽然目前国家出台了很多相关法律法规，但当前仍存在着法律法规落实不彻底、网络支付APP行业不自律、政府技术水平有限、执法效率较低、司法救济机制不完善、用户安全意识薄弱的一系列挑战。为了应对这一现状，应当落实法律法规与行业自律有机结合；建立独立的用户信息监管机构；同时加强公益诉讼，采用举证责任倒置模式，进而为网络支付用户的信息安全保驾护航。

关键词

网络支付APP，用户信息，信息安全

Research on Legal Issues of User Information Security in Online Payment APP

Yuting Su

Law School of Guizhou University, Guiyang Guizhou

Received: Aug. 8th, 2024; accepted: Oct. 30th, 2024; published: Nov. 6th, 2024

Abstract

In the era of big data, online payment has been widely used because of its convenience. However, some online payment apps will read user information such as mobile phone number, geographical location and address book without users' knowledge, which inevitably leads to cases in which user information has been over-read and leaked in recent years. In order to achieve a safe and healthy operating environment for online payment and effectively enhance users' sense of security, it is

文章引用: 苏渝婷. 网络支付 APP 中用户信息安全的法律问题研究[J]. 电子商务评论, 2024, 13(4): 1594-1600.
DOI: 10.12677/ecl.2024.1341312

found that although many relevant laws and regulations have been promulgated in China at present, there are still a series of challenges, such as incomplete implementation of laws and regulations, lack of self-discipline in online payment APP industry, limited technical level of the government, low law enforcement efficiency, imperfect judicial relief mechanism and weak users' safety awareness. In order to cope with this situation, we should implement the organic combination of laws and regulations and industry self-discipline; establish an independent user information supervision institution; at the same time, we will strengthen public interest litigation and adopt the inverted burden of proof model, thus escorting the information security of online payment users.

Keywords

Online Payment APP, User Information, Information Security

1. 我国关于用户信息保护的立法概况

目前我国关于用户信息保护的立法涵盖了宪法、法律、部门规章等多个领域，分别从不同角度进行了规定。

1.1. 宪法

《宪法》第 33 条第 3 款规定“国家尊重和保障人权”。《宪法》第 40 条进一步提出对公民的通信自由、通讯秘密予以保护，列举了能够对相关内容进行检查的情形并将其法定化。这表明我国从根本法的层面对公民的合法权益予以最高保护，网络支付平台无权擅自读取用户信息。

1.2. 法律

《中华人民共和国民法典》第一百一十一条“自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”

《刑法》修正案(九)在第二百八十六条后增加一条，作为第二百八十六条之一“网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有特定情形的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金。”[1]这在原先法条的基础上从网络服务提供者的角度进一步细化了针对造成特定加重结果的具体惩罚措施，强化了互联网服务提供者的网络安全管理责任，侧面反映了网络支付用户的信息权益不受侵害。

2021 年出台的《个人信息保护法》以专门法的形式进一步加强了对个人信息的保护，规定了处理个人信息应取得相关许可，履行具体要求；[2]明确列举了信息处理者从获取信息、处理信息、影响评估、补救措施等全过程的义务；[3]规定了对违法处理用户信息者给予相应的处罚措施。[4]《个人信息保护法》的出

[1](一)致使违法信息大量传播的；(二)致使用户信息泄露，造成严重后果的；(三)致使刑事案件证据灭失，情节严重的；(四)有其他严重情节的。

[2]具体见《中华人民共和国个人信息保护法》第三十二条。

[3]具体见《中华人民共和国个人信息保护法》第五十七至五十九条。

[4]具体见《中华人民共和国个人信息保护法》第六十六条。

台确立了个人信息的处理规则，一定程度上保护了公民合法的信息权益，弥补了我国个人信息保护方面的不足具有里程碑式的意义。

1.3. 部门规章

由工信部发布的《电信和互联网用户个人信息保护规定》从信息收集和使用规范、安全保障措施、监督检查、法律责任几个方面规范电信企业和网络经营者的行为，其中在安全保障措施部分规定了电信和网络经营者的相关防范措施。[5]

全国信息安全标准化技术委员会在 2020 年 9 月发布了《网络安全标准实践指南——移动互联网应用程序个人信息保护常见问题及处置指南》，该指南列举出了当前网络中对个人信息保护十大常见问题和相应的处置指南。常见的情形例如：超范围收集与业务无关的用户信息，针对该情形给出了包括但不限于遵循最小必要原则、在用户拒绝收集相关信息时运营商不得拒绝提供基本业务功能的处置方式；未经用户同意向第三方提供用户信息的，应取得用户同意、使第三方所需使用的权限最小化，该规章给网络运营商、网络用户提供了具有现实意义的参考。

2. 网络支付 APP 中用户信息保护的范围界定

2.1. 用户信息的范围

按照通常理解，“用户信息”是指在使用互联网应用程序过程中涉及的用户姓名、电话、身份证号码、地理位置等信息，其范围十分广泛。

2.2. 用户信息与个人信息的区别

关于个人信息我国许多相关法规都有提及，其中《民法典》第一千零三十条提到个人信息是能够单独或者与其他信息结合识别特定自然人的各种信息。[6]其中“识别特定自然人”、“各种信息”表明个人信息的范围是无法具象化的，只要是能够识别出特定自然人身份的信息都属于个人信息的范围，突出了其具有可识别性。程啸教授在其文章中曾提到随着社会的发展进步，个人信息的范围越来越广泛，除了传统的电话号码、住址等信息外，还有一些虽然本身不足以识别特定自然人但与其他信息结合后就能识别出特定自然人的信息，如爱好、习惯、兴趣、职业等，也可以成为个人信息的内容这一观点具化了《民法典》的规定[1]。

关于二者的区别，一方面，由于“用户信息”往往指在网络空间这一领域中涉及的信息，而“个人信息”涉及到网络空间、现实生活等多方领域，所以相较于“用户信息”而言，个人信息的范围更加广泛，个人信息包含用户信息，属于整体与部分的关系。另一方面，个人信息具有可识别性的特点，而网络支付 APP 读取到的用户信息却不一定能够具体识别出特定的用户身份。我国早在 2012 年 12 月出台的《全国人民代表大会常务委员会关于加强网络信息保护的决定》中就提到“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息”。这条规定虽未明确提出“个人信息”这一概念，但本质上已将可识别个人身份的电子信息与普通的电子信息予以区分[2]。

3. 网络支付中用户信息安全的现实挑战

虽然目前我国出台了很多关于用户信息保护的立法文件，也提出了一系列的措施办法，但在网络生

[5]具体见《电信和互联网用户个人信息保护规定》第十三条。

[6]《民法典》第一千零三十四条规定：自然人的个人信息受法律保护。个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

活支付中用户信息泄露的案件还是频繁发生。通过考察分析本文分析出以下几个方面的原因。

3.1. 法律法规落实不彻底，网络支付 APP 行业不自律

一方面，立法的目的不在于立，而在于贯彻落实，在于能够真正地解决现实问题。目前关于用户信息保护制度的规定分散在法律、部门规章等法律法规当中整体缺乏系统性[3]。每当有新的立法的出台，就会从中央到地方层层传达，相关部门学习条文内容，但在现实实践中由于执法部门水平有限、法律理解不到位等客观因素往往很难真正贯彻落实法律法规的精神和内容，这会导致法律没有足够的震慑力使网络支付平台运营商产生畏惧心理。另一方面，部分网络支付行业自律性低，主要体现在以下几个方面：一是随着大数据时代的不断发展，互联网行业有着巨大的经济利益，部分运营商为了牟利就会在未经用户同意的情况下将获取的用户信息出卖给其他机构或是进行商业化处理。二是网络支付运营商内部监管、惩罚机制不完善，难以确保工作人员真正地依照内部规定处理用户信息，对违规工作人员的惩罚措施也难以起到规制、示警的作用。三是有的网络支付运营商法律意识薄弱，责任意识较低[4]。很多网络支付运营商更多关注的是产品本身的质量而往往会忽视其做法是否符合法律规定，即使认识到可能与法律相悖，但由于利欲熏心、责任心弱也会放任不管。

3.2. 政府技术欠缺且无专门监管部门

在大数据时代网络行业技术水平不断升级，政府技术质量的优劣直接影响政府的执法效果，但目前我国政府在网络技术方面仍存在一些缺口有待填补，首先是核心技术掌握在外国厂商手中，政府需要通过进口的方式获得较为先进的技术手段。其次是我国信息产业自主研发能力有限在创新科技方面有待提升。再次全国各级政府部门数量较多，国库资金有限，缺少充足的人才培养、技术研发经费[5]。除此之外，我国缺乏独立的用户信息监管部门，当前对于公民信息安全的监管主要是由国家网信部门和县级以上政府的有关部门，其中部分机构对于信息保护的专业水平较低、职责分工模糊，在一定程度上会影响问题的有效解决。对此建立一支具有专业知识的独立信息监管部门刻不容缓。

3.3. 执法效果欠佳

尽管目前国家出台了许多关于用户信息保护的法律法规，但当网络支付侵权案件发生时实际的执法效果却并不理想，究其原因主要归于以下几点：首先是法律法规大多仅有原则性的处罚规定，而缺乏具体的处罚规则、惩罚措施，理论与实践脱轨，有时甚至出现法律不明、理解不到位、执法存在差异的情况，这严重影响执法效果[6]。其次，各监管部门间职责分工不明确，《个人信息保护法》第 60 条中规定可以处理公民个人信息的部门有国家网信部门、国务院有关部门、依据国家规定有个人信息保护和监督管理职责的县级以上地方政府有关部门。法律规定的管理部门众多，不可避免地出现各部门间互相推诿的情况，当用户受到不同类型的信息侵害时不免疑惑到底该找哪个部门进行救济。再次，是执法人员配备、培训不足，APP 行业的快速发展蕴含着许多的专业知识，执法人员作为执法的关键，应当对行业知识、执法流程步骤有着充分的了解，执法队伍整体能力有待提升。最后，惩罚力度较轻，如果仅仅停留在轻微的行政处罚或口头警告的层面，会导致违法成本过低，法律威慑力不足，难以使违法者改过自新从而影响了法律执行的效果。

3.4. 司法救济机制有待完善

除了事前监管与防御，事后救济对于维护网络支付用户信息合法权益也至为重要。目前很多用户信息遭受到侵害后都会通过民事救济的方式维权但效果往往不佳，通过分析可以得出主要有以下几个方面的原因：一是用户信息在网络空间中具有流通性、无形性的特点，可以被不断地复制传播，维权用户很

难描述清楚具体的被侵权范围与侵犯对象。二是网络支付运营商掌控着用户信息处于主导地位，可以随时销毁所收集到的用户信息，这会导致用户难以拿到充分的事实证据。三是个别用户会因专业知识不足以致损害事实认定困难，再加上维权成本过高，维权之路往往出现障碍[7]。由此可见，一般侵权责任的适用与私益救济的方式不适用于网络信息侵权案件，应当另辟蹊径，其司法救济模式有待继续完善。

3.5. 用户安全防范意识薄弱

在很多网络支付过程中用户信息泄露事件中，很大一部分原因在于用户本身安全意识不足。其中大学生、中老年人往往是网络安全防范意识最薄弱的群体，通常表现为：在公共场合随意链接公共开放 wifi；在下载支付 APP 时随意点开不明链接；在进入支付页面时为了节省时间而跳过对隐私政策内容的阅读；在他人怂恿下下载不明支付软件；当受到侵害时法律意识薄弱不知找谁救济、如何救济等等。究其原因，对于大学生而言这类群体涉世未深思维想法简单，对网络平台运营商发出的授权请求缺乏警惕性与辨别能力[8]。对于中老年人而言，随着年龄增长跟不上时代的发展潮流，对网络电子产品缺乏充足的了解更是难以识别其安全性。因此加强用户的安全防范意识对防范用户信息泄露至关重要。

4. 网络支付中用户信息保护的路径优化

通过对网络支付中用户信息泄露原因的考察分析可以发现多方都存在着漏洞，为了弥补这些漏洞需从法律法规、网络支付 APP 行业自身、政府、技术水平、司法救济模式、用户安全意识几个方面齐头并进、共同努力。

4.1. 落实法律法规与行业自律有机结合

法律法规的落实需要各级相关部门的共同努力，可以以专业的法律部门为主导根据现行有效法律对网络支付运营商提出法律层面的具体规定和要求，进一步细化网络支付运营商对用户信息可以获取和禁止获取的范围，并严格依照法定的条件和程序进行。对于网络支付开发商的违法违规行为，不允许出现任何凌驾于法律之上者，都要严格依照法定程序予以惩处并向社会示警示告。这样可以使法律规定与网络支付运作搭建链接，使静态的法律条文转化为动态的实践中，有利于法律法规得到充分的贯彻落实[9]。此外，网络支付运营商本身要建立内部自律机制，由于索取用户信息的范围是由信息处理者提前单方拟定的格式文本，很难充分考虑到每位用户的意愿，对此企业应当加强与用户的沟通交流，用心倾听用户的建议，把握好向用户索权的范围[10]。针对日常业务活动中的突发性信息安全事件网络支付运营商应及时采取合理的补救措施并将相关真实情况告知当事人[11]。网络支付企业内部要对接触用户信息工作人员建立完善的监管机制，定期进行专业知识和法律知识培训，对工作人员的违规行为要建立专门的惩罚制度[12]。同时网络支付 APP 的注册审批机构应设立严格的市场准入机制，要求应用商店加强对上架 APP 的审核力度[13]。除了注重网络支付本身的质量外，也要加强对申请商的责任意识和法律意识的考察。

4.2. 健全行政监管，加强技术更新

一是以法律部门为主导，抽调电信、网络、计算机等相关部门的优秀人才，组建一支具备专业知识的独立信息监管部门，明确办事章程、划定职责范围，并可以根据实际需要设立部门分支机构，如法国和西班牙分别设有隐私监管部门和数据保护监管部门作为个人信息监管机构，由此可以提高用户信息监管的效率与保障水平[14]。二是优化政府的监管机制，建立严格的审查监督制度，对网络支付行业活动进行指导，但与此同时也不能过分干预，因为倘若政府监管力度过强、范围过广，必然会压制网络支付行业自身管理的发展，无法充分体现其独立的话语权[15]。除了常规的监督、检测工作外，还可以设立有关信息安全的意见收集网站，用户可以通过该网站对在网络支付过程中出现的问题与意见进行反馈，这有

助于政府有针对性的解决现实问题，提高监管质量。三是要建立政府内部的监管与惩罚机制。政府部门人员基于工作职责可以直接对用户信息进行收集、处理，但若不注重内部人员监管不可避免的就会出现工作人员被他人利诱，利用职权便利泄露用户信息的情况。四是强化政府技术的创新与升级，国家和政府应加大对技术创新的资金支持，鼓励信息安全技术的研发，提高防火墙技术与信息泄露追踪技术，努力使不断优化的技术应用到全国各行政区域政府，争取在事前预防和事后追责全过程都建立起强大的技术屏障。

4.3. 细化执法规则，提升执法效果

一是可以根据实际需要，进一步细化执法规则，划定职责与分工明确执法的程序与步骤。有关部门可以根据需要作出相应的立法解释、司法解释，颁布相关的指导案例、典型案例，避免法律不明，执法不当。二是在建设独立信息监管部门的基础上下设多个专管部门以应对 APP 用户信息泄露、信息侵权、信息交易等涉及不同类型的用户信息案件，这样可以使用户了解什么情况下找什么部门救济，从而提高各部门执法效率。三是要加强执法队伍建设，增加资金投入，根据信息时代的发展风向定期对工作人员进行专业方面的培训，引进精通网络信息保护的优秀人才，建设出一支专业过硬、与时俱进的执法队伍[16]。同时要加大对侵害网络支付用户信息行为的惩罚力度，对于违法违规收集用户信息的行为，政府部门可以采取将其纳入黑名单，记入征信系统等方式以起到示警示范作用[17]。

4.4. 举证责任倒置，重视公益诉讼

一方面，由于网络支付运营商掌控着用户的信息，与用户所处地位不对等，如若按照“谁主张，谁举证”的模式将会增大举证难度且对用户而言是不公平的。对此可以采取举证责任倒置的模式使网络支付运营商承担举证责任，只需要运营商证明在对用户信息进行收集、处理、传输过程中未实施侵权行为且尽到了合理的注意义务，这样一来可以降低用户举证责任的难度，增强网络支付运营商的责任意识[18]。另一方面，在网络信息维权案件中私益诉讼的力量微弱，例如诉讼成本过高、损害数额较小且难以计算、案件数量众多等等，而如若通过公益诉讼的方式，就可以借助公众的力量比如法院、网信办、计算机专家等联合协作，通过多方的共同努力针对不同类别的网络信息侵权案件进行分类处理，这样不仅可以降低维权成本，而且也有助于提高司法效率，保障用户的合法权益[19]。

4.5. 增强用户安全意识

加强法律安全知识教育，提高用户的安全防范意识应通过学校、单位、社区等多方面多领域推进，高校应创新网络安全意识教育的方法，将传统的理论讲座融入到思政课程、普法课程、计算机应用课程当中，建立全新的安全防范意识框架，并根据时代发展引进最新典型案例，将理论与实践相结合[20]。单位、社区可以通过开展组织生活会、海报宣传的方式帮助用户养成良好的使用习惯，熟练掌握有关网络支付信息保护的安全措施，例如：在官方应用商城下载 APP，不随意点开不明链接；用户要对各类不知名支付 APP 或链接授权个人信息的请求提高警惕，尽可能地缩小对网络支付平台信息授权的范围；对于弹出的授权窗口，要经过认真考虑再决定是否同意访问；在公共场所尽量不使用公共 WIFI；当个人信息受到侵害时及时保留证据并向有关部门反映以维护自身合法权益[21]。

5. 结语

大数据时代网络支付 APP 为我们带来便利的同时也伴随着用户信息泄露风险的逐渐增多，如何保护好用户信息安全这一时代命题得到了越来越多的关注。必须严格贯彻落实相关法律法规将理论与实际结合起来，具体包括加强行业自律，构建内部监督、惩罚机制，提升网络支付 APP 运营商法律意识和责任

意识；同时建立专门的用户信息监管机构提高监管效率与专业程度，构建政府外部监督与内部监督有机结合；在执法、司法层面则需要从实际出发细化执法规则，加强执法队伍建设；完善司法救济机制，推进举证责任倒置，重视公益诉讼。除此之外，用户在日常生活中也要主动学习相关法律知识与使用指南，养成良好的使用习惯。唯其如此才能促使网络支付 APP 行业健康良性发展，用户的信息安全也会得到更有效的保护。

参考文献

[1] 程啸. 民法典编纂视野下的个人信息保护[J]. 社会科学文摘, 2019(11): 71-73.

[2] 詹星. 侵犯公民个人信息犯罪中“公民个人信息”范围探析[J]. 中国检察官, 2021(9): 11-14.

[3] 潘飞. 论 App 用户个人信息的法律保护[J]. 河北企业, 2024(3): 152-154.

[4] 武煜熹, 安小米. 大数据时代 APP 用户个人信息保护的困境和解决对策[J]. 网络空间安全, 2020, 11(10): 22-25.

[5] 史卫民. 大数据时代个人信息保护的现实困境与路径选择[J]. 情报杂志, 2013, 32(12): 155-159, 154.

[6] 张志钢, 高志宏, 王学涛, 等. 数字时代公民个人信息司法保护的挑战与应对[J]. 人民检察, 2023(S1): 62-64.

[7] 张月昕. 大数据时代个人信息保护的困境与有效进路[J]. 中阿科技论坛(中英文), 2023(3): 158-162.

[8] 张德峰. 关于高校学生网络安全意识的培养[J]. 哈尔滨职业技术学院学报, 2022(3): 96-99.

[9] 张泽昊. 手机 APP 个人信息安全的法律保护[J]. 网络空间安全, 2023, 14(5): 1-5.

[10] 李畅畅. APP 个人信息保护政策困境与应对路径[J]. 信息安全研究, 2024, 10(2): 177-183.

[11] 龚文博. 网络平台处理个人信息的合规义务及其出罪路径[J]. 华东政法大学学报, 2024, 27(2): 52-66.

[12] 王永明. 大数据环境个人信息泄露防范措施解析[J]. 网络空间安全, 2023, 14(1): 76-80.

[13] 许偲. APP 违规行为之规制路径研究[J/OL]. 华北电力大学学报(社会科学版): 1-7. https://kns.cnki.net/kcms2/article/abstract?v=hFA5SNLyt3gC2JRSN8ukMCI-Vmbhm9HCUOBNC6bv8aoHfMIwF-wEpg3MYGU-Kb8CuVt9g-mqQe8glDn211FM7N7l2PjC7V6HzNdKG-Zur8ljkOm7uu7Ifk6CWoYQAATT-jAkPF8gMcDkurtPOLDEzltsjC2omRrQ4tkyxCOihFnr4=&uniplatform=NZKPT, 2024-04-11.

[14] 邰江丽. 关于 App 收集个人信息实务及规范研究[J]. 北京航空航天大学学报(社会科学版), 2019, 32(4): 7-12.

[15] 张继红. 大数据时代个人信息保护行业自律的困境与出路[J]. 财经法学, 2018(6): 57-70.

[16] 陈慧, 胡晓航. 数字法治政府背景下个人信息的行政法保护研究[J]. 科技创业月刊, 2023, 36(11): 121-126.

[17] 王越, 顾鑫, 刘洋. 大数据时代个人信息保护思考[J]. 合作经济与科技, 2024(2): 190-192

[18] 胡向腊. 互联网个人信息保护的法律规制思考[J]. 武汉冶金管理干部学院学报, 2019, 29(4): 36-38.

[19] 王婧怡, 崔聪聪. App 收集使用个人信息的治理困境及建议[J]. 长春师范大学学报, 2023, 42(7): 48-51.

[20] 王广丽. 当代大学生自主网络安全意识宏观培养路径研究[J]. 改革与开放, 2023(17): 62-66.

[21] 时斌. APP 个人信息保护的路径选择与重构[J]. 人民论坛, 2020(15): 146-147.