E-Commerce Letters 电子商务评论, 2025, 14(10), 1776-1783
Published Online October 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14103330

Hans汉斯

C2C平台静默授权模式的合法性与合理性分析

——以闲鱼APP为例

刘儒倩

浙江理工大学法学与人文学院，浙江 杭州

收稿日期：2025年9月7日；录用日期：2025年9月24日；发布日期：2025年10月23日

摘　要

本文以闲鱼APP为例，分析C2C平台静默授权模式的合法性、合理性及其法律风险。静默授权虽在提升用户体验方面具有一定合理性，但其本质上侵害了用户的知情权与选择权，违反《个人信息保护法》的知情同意原则。文章创新性地提出，平台作为数据控制者应对用户承担信义义务，其核心在于忠实、勤勉与充分披露。通过构建以信义义务为基础的平台责任体系，可为治理隐私侵权提供法理支撑，推动平台在个人信息处理中履行更高标准的保护义务。

关键词

C2C平台，隐私权，个人隐私保护，静默授权，信义义务

Legitimacy and Rationality Analysis of the Silent Authorization Model in C2C Platforms

—A Case Study of Xianyu APP

Ruqian Liu

School of Law and Humanities, Zhejiang Sci-Tech University, Hangzhou Zhejiang

Received: September 7, 2025; accepted: September 24, 2025; published: October 23, 2025

Abstract

This paper takes the Xianyu APP as a case study to analyze the legality, rationality, and legal risks of the silent authorization model employed by C2C platforms. While silent authorization offers certain

文章引用: 刘儒倩. C2C 平台静默授权模式的合法性与合理性分析[J]. 电子商务评论, 2025, 14(10): 1776-1783.
DOI: 10.12677/ecl.2025.14103330

practical benefits in enhancing user experience, it fundamentally infringes upon users' right to know and right to choose, violating the principle of informed consent established in the Personal Information Protection Law of China. Innovatively, this article proposes that platforms, as data controllers, should bear fiduciary duties toward users, centered on loyalty, diligence, and full disclosure. By constructing a platform accountability framework based on fiduciary obligations, this study provides a jurisprudential foundation for addressing privacy infringements and encourages platforms to adopt higher standards of protection in personal information processing.

Keywords

C2C Platform, Rights of Privacy, Personal Privacy Protection, Silent Authorization, Fiduciary Duty

1. 引言

随着数字经济的快速发展，C2C 平台已成为日常生活的重要组成部分，但其在用户授权机制上普遍存在“静默授权”行为，严重侵害用户个人信息权益。静默授权以默认设置、隐性操作等方式，在用户未充分知情的情况下获取并使用其个人信息，违背了个人信息保护的核心原则。本文以闲鱼平台为研究对象，剖析静默授权的具体样态与法律风险，旨在揭示平台滥用技术优势与用户信赖的实质，为进一步完善平台责任体系提供理论依据与规制路径。

2. 何为静默授权

2.1. 静默授权的概念

静默授权是指在某些特定的情境下，用户在未明确表达同意的情况下被认为已经同意某项操作或服务的授权方式。这种授权方式通常发生在用户使用软件、应用程序、网站或其他在线服务时。广义上静默授权的情境可能包括默认设置、隐形操作和继续使用。默认设置是指用户在安装应用程序或注册服务时，默认接受了一些预设的设置和条款，即默认情况下视为同意。隐性操作是指用户在使用某个功能或服务时，可能在未经过特别提醒或明确同意的情况下被认为已经授权。继续使用是指用户在收到更新或变更通知后，如果继续使用服务而没有明确表示反对，可能被视为已经默许了变更。狭义上的静默授权主要是指用户在使用某个功能或服务时，在未经过特别提醒或明确同意的情况下被认为已经授权。

2.2. 闲鱼平台以静默授权模式获取个人信息的具体样态

以闲鱼平台为例，用户通过支付宝账号登录时，平台默认同步支付宝的实名信息，比如姓名、身份证号等个人信息，无需二次确认。比如闲鱼 APP 的隐私政策的“信息收集及使用”一章里表明“您授权我们可自支付宝公司处获取您对应支付宝账户的必要认证信息用于上述目的”[1]这种跨平台账号互通实质上也属于静默授权，因为用户虽然有授权支付宝登录协议，但未被告知闲鱼具体获取的数据范围。例如，

[1]《咸鱼隐私政策》第二章第一节：“为了确保我们是在为您本人提供服务，我们可能会根据您提供的上述信息及其他能够证明的信息(如邮箱等)校验您的身份。若存在依法需确定您必要身份的场景(包括依法保护未成年人权益、打击电信网络诈骗、为您扣缴税费、行政执法或司法诉讼中相关主体认定)时，您授权我们可自支付宝公司处获取您对应支付宝账户的必要认证信息用于上述目的。”

用户首次使用支付宝授权登录闲鱼后，闲鱼直接获取用户基础身份信息，过程中无独立弹窗说明数据获取范围与用途。

闲鱼平台的隐私政策在“分享互动”一节里还表明“同时，我们可能需要读取您的手机相册以便于您分享或接收被分享的图片或视频”[2]，该条并未说明在读取的时候需要征求用户的单独同意，也属于以静默授权方式侵害用户的个人信息。

在“委托处理”这一小节里表明“我们可能委托授权合作方处理您的个人信息，以便授权合作方代表我们为您提供某些服务或履行职能[3]。”这也属于以静默授权方式侵害用户个人信息，因为闲鱼措辞模糊，未明确告知“合作方”是谁、具体处理目的为何。将关键信息隐藏在冗长的隐私政策中，用户无法真正知情，只能在“用户服务就须全部同意”的捆绑模式下被动接受，这侵害了用户的知情权和选择权。其结果是，用户在不了解个人数据将被谁、用于何种具体场景的情况下，就默许了一个可能非常广泛的授权，为信息滥用埋下隐患，违背了个人信息保护中“目的明确”和“自愿知情同意”的核心原则。

在“物流小节”里表明“我们会向为闲鱼社区用户提供物流综合服务的相关服务商披露订单相关的配送信息，并由其根据商品及/或服务提供主体的选择向相应的物流配送主体同步相关配送信息[4]。”但是实际情况是，不止物流服务商、物流配送主体，卖家在订单页面可直接看到买家的完整收货地址，精确到省市区、街道门牌、姓名电话，买家地址在交易创建后即对卖家完全可见，用户无关闭选项。即使交易完成，订单记录仍保留在买卖双方账号中，若卖家账号被盗，黑客可批量导出买家地址、电话等敏感信息。比如 2021 年咸阳警方破获的闲鱼用户数据贩卖案中，黑产人员通过盗用卖家账号窃取近万条地址信息[5]。这也是以静默授权的方式，将用户的完整收货地址默认、强制地向卖家展示，且用户无法关闭此功能。这种做法远超“物流配送”的必要范围，严重违背了“目的明确”和“最小必要”原则。

3. 静默授权的合法性与合理性分析

3.1. 静默授权合理性分析

静默授权的存在固然有其一定的合理性，比如它常可以提升用户体验、简化流程、提高操作便利性，可以减少用户在使用服务时的操作步骤，能够减少用户需要进行的选择和确认，使整个流程更为简便快捷。而且在一些场景下，用户可能并不愿意或不方便频繁地进行授权确认。静默授权的使用可以减少用户的主动参与，提高用户的参与度。但是，与其合理之处比起来，不合理之处是更为突出的。

不合理之处可以归结于两个方面，第一个方面就是 C2C 平台掌握太多个人信息，过于侵入公民私人空间，公民在平台面前逐渐毫无隐私可言。在进入大数据时代之前，传统的纸质信息存储和传播主要依赖于纸质载体。但随着互联网新技术的普及，人们开始更多地通过网络来收集和存储个人信息。尽管信息载体发生了变化，但信息的常规收集方法仍然保持不变[1]。大数据时代之前传统的纸质收集

[2]《咸鱼隐私政策》第二章第三节：“当您分享或接收被分享的信息、参加活动等情形下，我们会读取您的剪贴板内容以判断是否存在相关口令、分享码、链接，以实现跳转、分享、活动联动等功能或服务，但我们仅在本地识别出剪贴板内容属于闲鱼社区跳转、分享、活动联动等指令时才会将其上传我们的服务器，并不会收集、存储您的剪贴板其他信息，且单独的剪贴板信息无法识别您的个人身份。同时，我们可能需要读取您的手机相册以便于您分享或接收被分享的图片或视频。”

[3]《咸鱼隐私政策》第三章第三节：“我们可能委托授权合作方处理您的个人信息，以便授权合作方代表我们为您提供某些服务或履行职能。我们仅会出于本政策声明的合法、正当、必要、特定、明确的目的委托其处理您的信息，授权合作方只能接触到其履行职责所需信息，且我们将会通过协议要求其不得将此信息用于其他任何超出委托范围的目的。如果授权合作方将您的信息用于我们未委托的用途，其将单独征得您的同意。”

[4]《咸鱼隐私政策》第五章第一节：“为保证您购买的商品及/或服务能够顺利、安全、准确送达、提供，我们会向为闲鱼社区用户提供物流综合服务的相关服务商披露订单相关的配送信息，并由其根据商品及/或服务提供主体的选择向相应的物流配送主体同步相关配送信息。您理解并同意相应物流服务商、物流配送主体不可避免地获知及使用您的配送信息，用于完成交付目的。”

[5]西部法制报，旬邑首例侵犯公民个人信息案宣判，http://esb.xbfzb.com/html/2021-04/17/content_18424_4329987.htm。

方式可使行政相对人清晰得知自身的哪些信息在何时何处被收集，但是在大数据时代，当我们的各种智能设备向世界打开了窗户，我们也打开了一扇世界可以从中窥视我们的窗户，我们的行动踪迹时时刻刻在“出卖”着我们[2]。同时，通过利用大数据的综合分析和数据挖掘技术，C2C 平台可以在信息主体不知情的情况下收集个人信息。只需简单地敲几下键盘或点几下鼠标，就可以轻松地进行个人信息的对比分析，从而形成一张清晰、具体的人格图。用户在掌握这些信息的平台面前无处可逃，这与所谓的“透明人”无异，他们的个人信息也可以随时被获取、使用或传播，这使得用户感到非常不安[3]。

所以我国法律对平台获取公民个人信息的权力进行了限制，也就是公民有个人信息知情权。个人信息的知情权意味着信息提供者有权了解其个人信息被收集和处理的相关事宜。在知情同意原则的基础上，本人对个人信息有最终决定权，他人收集、利用与处理这类信息须经本人同意。

第二个方面就是平台因为设计、技术、人力等方面的原因，在公民不知情的情况下获取了数量如此巨大、内容如此敏感的个人信息，有严重的安全隐患，这些安全隐患存在于平台对个人信息的存储、利用环节。首先，在存储方面就存在很严重的安全隐患。平台为什么要获取公民个人信息，不仅因为便于日常的操作管理，而且因为我们的个人信息蕴藏着极大的经济价值。公民个人信息难以得到完全的保障，有严重的泄露风险。其次，在利用方面也存在很大的安全隐患。平台获取我们的个人信息肯定不止是收集后存储起来，个人信息更大的价值在于利用，个人信息的操作肯定也是平台工作人员来操作，平台工作人员不可避免的拥有调取、查看公民个人信息的权限，由于平台的内部安全管理机制存在缺陷，导致个人信息的流失问题日益加剧[4]。

综上，以静默授权的方式来获取公民的个人信息是相当不合理的，既然存在巨大的风险，那么就更应该保障公民的知情权，平台更加要履行透明、清晰的告知义务，告知公民他们的个人信息将被获取多少、怎么被获取和用于何种目的[5]。

3.2. 静默授权合法性分析

《中华人民共和国个人信息保护法》(以下简称“《个人信息保护法》”)第 73 条规定，个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。像闲鱼之类的 C2C 平台属于个人信息的处理者，必须受到《个人信息保护法》的约束。

从《个人信息保护法》第 14 条规定 [6]和《个人信息保护法》第 18 第一款 [7]的规定可以看出，C2C 平台处理用户的个人信息，原则上都是要取得用户同意的，静默授权方式是才例外，只有在法律、行政法规规定应当保密或者不需要告知的情形的才可以采用静默授权的方式。但是闲鱼隐私政策中很多以静默授权方式获取用户个人信息的做法反而成为了默认的情形，明显和法律规定的相冲突。

《个人信息保护法》第 23 条规定 [8]可以看出，如果平台要向其他个人信息处理者提供处理的个人信息的，有义务向用户告知接收方的名称、姓名、联系方式、处理目的等必要信息，而且要取得个人的单独同意。由此可见，告知和取得向对方的单独同意是不可逾越和省略的法定程序，很显然闲鱼平台的静默授权条款没有做到。

[6]《个人信息保护法》第 14 条：“基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。”

[7]《个人信息保护法》第 18 条第一款：“个人信息处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。”

[8]《个人信息保护法》第 23 条：“个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的，应当依照本法规定重新取得个人同意。”

《个人信息保护法》第 28 条[9]和第 29 条[10]可以看出法律对于敏感个人信息的保护是很严格的，前文已经提到过，闲鱼提供服务需要收集用户支付宝的信息，但是未能表明是哪些信息，支付宝的个人信息甚至都包含了人脸面部识别特征、证件号码、医疗健康信息等，这些都属于个人敏感信息，在收集的时候要更加小心，和其他个人信息需要授权不同，敏感信息的授权法律单独列出一条，强调应当取得个人的单独同意，应当取得书面同意也要从其规定，闲鱼隐私政策中含混不清的说辞明显不合法。

4. 规制路径：以信义义务赋能平台责任

4.1. 国内外相关研究现状梳理

国内研究主要围绕《网络安全法》《电子商务法》《个人信息保护法》展开，强调平台的“安全保障义务”和“守门人责任”。但责任基础多局限于侵权责任法、合同法，对平台道德层面的约束力不足。学者开始探索更具前瞻性的责任范式，如冯果、薛亦兴提出从“权利规范模式”转向“行为控制模式”，为信义义务的引入提供了理论铺垫[6]。王茵芝认为强调应区分“数据信义义务模式”与“数据信托模式”，主张以前者为核心，其法律结构源于信义法而非信托法，避免了信托财产适格性的争议[7]。邢会强从主体、客体、内容三个维度系统批判了该理论的内在缺陷，认为其与我国法律体系不兼容，且加强公法规制是更优路径[8]。

美国学者 Balkin 提出了“信息信义义务”理论，试图通过普通法上的信义法理来约束科技巨头的权力。他认为，传统的受托人，如医生、律师、会计师因其客户向其透露了大量敏感信息并依赖于他们的专业知识，而被法律施加了信义义务。他们必须将客户的利益置于自身利益之上，不得欺骗或背叛客户的信任。同样，用户向数字平台透露了大量关于自身、其朋友、其偏好和其活动的敏感信息，比如个人信息、搜索历史、私信内容等。用户依赖于这些平台提供的服务进行沟通、工作和日常生活。这种关系具有不对称的信任和依赖特征。正因为平台在这种关系中拥有巨大的权力和知识优势，它们应像传统受托人一样，承担起相应的法律义务。这些义务主要包括保密义务和忠实义务[9]。

4.2. 将“信义义务”理论引入中国数据保护法语境的法理依据和可行性

4.2.1. 法理依据：信义关系的本质与数据场景的契合性

信义法的产生，旨在规制一种特殊的社会关系：一方(委托人)基于信赖，将其重要利益置于另一方(受托人)的控制之下，而受托人享有处置该利益的自由裁量权，这使得委托人处于易受伤害的脆弱地位法律为防止受托人滥用权力，遂施加严格的信义义务，以弥补委托人自我保护能力的不足。这一法理基础具有高度的抽象性和适应性，并不局限于传统的信托关系，而是可以扩展到医生-患者、律师-客户、董事-公司等任何具备类似特征的关系中。信义法是不断发展的，是一个相对开放而非封闭的法律关系体系，随着社会和经济的发展，不断有新的社会关系被确认为信义法律关系而纳入信义法的范畴当中[10]。尤其在英美法系中，信义关系广泛存在于律师与客户、会计师与客户、医生与患者、监护人与被监护人、雇主与雇员等社会关系之中，配偶之间、朋友之间等新型信义关系也在不断被讨论[11]。

制度的构建需具备现实的条件和具体的语境，在我国的制度环境和法律体系下，数据受托人信义义务制度具备理论上的兼容性和制度上的可行性，能够以信义法的基本原理为依据，在信义关系的成立、信托客体的适格、信义义务的内容上得到良好的阐释[6]。

[9]《个人信息保护法》第 28 条：“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。”
[10]《个人信息保护法》第 29 条：“处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。”

我国虽然没有普通法与衡平法的二元划分，但仍然拥有信义法适用的法律环境和制度空间。《个人信息保护法》第 5 条规定的“诚信原则”是数据控制者信义义务构建的法理基础，诚信原则与信义法中所强调的忠诚地对待信任、积极地履行义务、不得欺诈或获取不当利益的基本法理相通[12]，信义法律规则可以作为诚实信用原则在特定社会关系下的制度进阶[13]，为了更好地实现司法裁判中的公平正义理念。

我国《公司法》中董事、监事、高管的忠实勤勉义务，《信托法》中受托人的信义义务，均为处理不对称关系提供了成熟的制度先例。这表明信义法理在我国法律体系中并非陌生概念，其引入数据领域具备本土法律资源的支持[14]。

4.2.2. 数据控制者与数据主体关系的“信义化”特征

从数据处理活动中各方主体的权利义务关系看，其符合信义法律关系的基本特征。

第一，用户对于平台存在高度的信赖。用户必须依赖平台提供的技术环境、信用体系和纠纷解决机制才能进行交易，这种依赖是实质性的。用户对平台的信赖包括信任和依赖，前者是指用户认为平台能够信守承诺保护用户的数据权益，后者是指用户依赖于平台提供的服务及相关的数据处理能力。

第二，平台和用户之间存在明显的不平等性。一方面，数据处理者具有专业和技术优势，以数据主体无法理解的方式开展相关的数据处理活动；另一方面，数据处理者具有信息优势，其相较于数据主体能够掌握更多有效信息[15]。

基于这种不平等地位，数据处理者很可能利用其优势在数据处理活动中损害数据主体的权益，谋取不当利益。

第三，受托人享有对特定标的或事务的自由裁量权是信义关系的典型特征，数据处理关系与这一特征具有高度相似性。平台对用户数据的处理拥有几乎绝对的权力。从算法的设计、数据的挖掘到隐私政策的解释与执行，平台行使着广泛的、单方面的自由裁量权，这直接关乎用户的核心利益——隐私权与财产权。因此，将信义义务应用于平台与用户的关系，并非生搬硬套，而是对数字时代新型信任关系的法律回应。

综上，静默授权不是孤立的技术问题或合规漏洞，而是平台利用其信息控制优势地位和用户信赖，未能保护用户最基本利益的直接表现。C2C 平台静默授权乱象的根源，不在于技术复杂性或法规执行难，更在于平台定位与责任的错位。

平台已从单纯中介演变为拥有巨大信息控制权和管理权的准公共设施，用户对其存在高度合理信赖。静默授权正是平台滥用其优势地位和用户信赖，将自身商业利益凌驾于用户隐私权益之上的典型表现。现有的法律保护，如《个人信息保护法》里的条款主要通过事后救济和形式合规的模式保护用户隐私权，但是当平台利用复杂条款、默认设置、以静默授权方式侵害用户权益时，用户往往难以维权。因此，有必要引入一种更高标准的、以忠实和诚信为核心的信义义务，来重新审视和规制平台的行为。

用户在平台上活动时，其个人信息和隐私完全处于平台的控制之下。这种控制不仅是物理上的，更是技术上和规则上的。用户出于对平台“会妥善保护我的数据”的合理信任，才愿意让渡其隐私。这种信任的让渡与患者信任医生、客户信任律师并无本质区别。平台作为强大的、专业的技术控制方，有义务回应这种信任，保护处于脆弱地位的用户的隐私利益，这正是信义义务的核心精神——保护弱者，防止权力滥用。平台不仅是数据的“持有者”，更是数据的“控制者”和“裁决者”。它决定了哪些数据被收集、数据如何被分析、谁能访问数据以及数据泄露后的应对措施。例如，平台可以利用用户的聊天记录和浏览行为进行用户画像，甚至可能将数据分析能力作为增值服务提供给第三方商家，这其中蕴含着巨大的利益冲突。信义义务中的“忠实义务”恰恰要求平台在处理这些数据时，必须将用户的隐私利益置于其自身的商业利益之上，禁止自我交易和利用机会牟利。

闲鱼等C2C平台与用户之间的关系早已超越了简单的技术服务提供者与使用者的合同关系，有必要引入信义义务的规则来对平台进行规制，在现有合规框架上，探索确立平台对用户的信义义务，尤其在涉及用户核心利益的关键环节，应要求平台承担更高的行为标准。

4.3. 信义义务在平台场景下的具体内涵、适用范围和判断标准

就具体内涵而言，信义义务在C2C平台的具体内涵主要是忠实义务与勤勉义务。忠实义务是信义义务最核心的部分，其本质是消极不作为义务，要求平台必须以数据主体的最佳利益行事，避免自身利益与数据主体利益发生冲突。具体包括禁止损害用户利益和禁止操纵与歧视。前者是指不得泄露和滥用个人信息，不背叛用户，不损害用户利益，不造成利益冲突，不以用户意想不到的或违反社会规范的方式使用个人信息[9]，后者是禁止平台利用用户的个人信息来操纵和歧视用户，并且在某些情况下应禁止其与第三方共享个人信息，数字企业不得违反其隐私政策承诺[16]。勤勉义务是积极作为义务，要求平台以专业和审慎的态度管理数据，采取积极措施保护数据主体权益。主要包括安全保障义务和信息披露义务。安全保障义务要求平台谨慎地进行数据收集、处理、利用、履行保护义务，并采取如制定内部制度、数据分类管理、匿名化和加密处理等措施[6]。信息披露与告知义务是指所有平台均应负担信息披露义务，包括获取数据时披露范围和使用目的，使用数据时定期披露使用方式和第三方分享数据的情况等[7]。

就适用范围而言，为避免信义义务泛化，其适用对象应具有特定性，主要针对在数据关系中占据绝对优势地位的平台。承担“类信义义务”的主体应是与用户之间存在持续性服务关系、实质性控制力以及用户依赖性的数据控制者。主张所有数据控制者均承担信义义务的观点会导致主体过于宽泛[8]。更合理的标准是聚焦于那些对用户数据享有自由裁量权、用户对其服务存在高度依赖的平台。平等主体之间的数据处理活动、数据主体对数据控制者缺乏高度信赖的数据处理活动、数据控制者缺乏对数据处理的自由裁量权等情形，难以产生法定的数据信义关系。

就判断标准而言，合理期待标准与善良人管理标准可以结合判断。合理期待标准是判断平台行为是否违反忠实义务的关键，是看其是否违背了“合理用户”的期望。“如果在线服务提供商以‘合理的用户’无法期望的方式使用个人信息，则该在线服务提供商可能违反了其义务。这是一个客观标准，需结合社会普遍认知和具体场景进行判断。善良管理人标准即要求数据处理者“像处理自己的事务一样履行受托职责”，其履职水平应达到“本行业内一般数据从业者的数据保护标准”，介于数据安全保护所需的最低限度和其所能承受的最高限度的消灭之间[6]。

5. 结语

C2C平台静默授权行为不仅构成对《个人信息保护法》的违反，更深刻反映了平台在数字治理中的责任缺失。引入信义义务理念，要求平台在数据处理中履行忠实、勤勉与充分披露的义务，是对现有法律框架的重要补充。未来应通过立法与司法实践进一步明确平台的信义责任，强化用户权益保护，推动构建更加公平、透明、可信的数字交易环境。

参考文献

[1] 陈晓勤. 大数据背景下政府信息形成权的行使[J]. 苏州大学学报(哲学社会科学版), 2017, 38(3): 83-89.

[2] 张才秦, 齐爱民, 李仪. 大数据时代个人信息开发利用法律制度研究[M]. 北京: 法律出版社, 2015: 66.

[3] 特蕾莎·M·西奥多·克莱普尔. 大数据时代的隐私[M]. 郑淑红, 译. 上海: 上海科学技术出版社, 2017: 42.

[4] 涂子沛. 数据之巅: 大数据革命, 历史、现实与未来[M]. 北京: 中信出版社, 2014: 4.

[5] 王利明. 论《个人信息保护法》与《民法典》的适用关系[J]. 湖湘法学评论, 2021, 1(1): 25-35.

[6] 冯果, 郭浩宇. 数据受托人信义义务的理论阐释与制度进路[J]. 财经法学, 2024(2): 3-18.

[7] 王茵芝. 数据信义义务理论下数据主体保护的简析[J]. 互联网天地, 2022(11): 53-57.

[8] 邢会强. 数据控制者的信义义务理论质疑[J]. 法制与社会发展, 2021, 27(4): 143-158.

[9] Balkin, J.M. (2016) Information Fiduciaries and the First Amendment. *UC Davis Law Review*, **49**, 1183-1234.

[10] Frankel, T. (1983) Fiduciary Law. *California Law Review*, **71**, 795-836. https://doi.org/10.2307/3480303

[11] Bodie, M.T. (2015) Employment as a Fiduciary Relationship. *Georgetown Law Journal*, **103**, 819-888.

[12] 赵磊. 信托受托人的角色定位及其制度实现[M]. 北京: 法律出版社, 2013(4): 91-100.

[13] 赵姿昂. 论推定信托在中国的引入[M]. 北京: 法律出版社, 2019: 148-150.

[14] 赵廉慧. 论信义义务的法律性质[J]. 北大法律评论, 2020, 21(1): 1-25.

[15] Arora, C. (2019) Digital Health Fiduciaries: Protecting User Privacy When Sharing Health Data. *Ethics and Information Technology*, **21**, 181-189. https://doi.org/10.1007/s10676-019-09499-x

[16] Dobkin, A. (2018) Information Fiduciaries in Practice: Data Privacy and User Expectations. *Berkeley Technology Law Journal*, **33**, 1-49.