·信息计量与科学评价·

社交网络用户隐私泄露情感损失计算研究

杨瑞仙[1,2] 刘佳涵[1] 孙 倬[1,2*]
（1. 郑州大学信息管理学院，河南 郑州 450001；
2. 郑州市数据科学研究中心，河南 郑州 450001）

摘 要：［目的/意义］随着社交网络的普及，用户隐私泄露问题日益严重，给个人和社会带来潜在风险。本研究针对社交网络用户隐私泄露问题，构建用户情感损失函数，旨在量化用户在隐私泄露情境下的情感损失。［方法/过程］本研究收集了微博用户生成文本数据，结合潜在狄利克雷分配（Latent Dirichlet Allocation，LDA）模型将隐私泄露分为社会生活、通信、位置和信息4个类型，通过情感分析将各隐私泄露类型下的用户情感细化，并在此基础上构造用户隐私泄露情感损失函数以对其情感损失进行计算。［结果/结论］研究结果表明，社交网络用户在隐私泄露情境下普遍表现出负面情绪，且不同类型隐私泄露导致的情感损失程度和离散程度存在差异。其中，通信隐私和位置隐私泄露造成的情感损失最为严重，而社会生活隐私泄露的影响相对较轻。此外，性别、地域分布、微博数量、使用年限等人口统计学变量对用户的隐私泄露情感损失存在不同程度的影响。

关键词：社交网络；隐私泄露；损失计算；LDA；情感分析
DOI：10.3969/j.issn.1008-0821.2025.10.007
〔**中图分类号**〕G203 〔**文献标识码**〕A 〔**文章编号**〕1008-0821（2025）10-0077-12

Research on the Calculation of Emotional Loss of Social Network User's Privacy Leakage

Yang Ruixian[1,2] Liu Jiahan[1] Sun Zhuo[1,2*]
（1. School of Information Management，Zhengzhou University，Zhengzhou 450001，China；
2. Data Science Research Center of Zhengzhou，Zhengzhou 450001，China）

Abstract：［Purpose/Significance］With the popularity of social networks，the problem of users' privacy leakage is becoming more and more serious，posing potential risks to individuals and society. In this study，the users' emotional loss function is constructed to quantify the users' emotional loss in the context of privacy disclosure.［Method/Process］This study collected text data generated by users on Weibo，and combined it with the LDA model to classify privacy leaks into four types：social life，communication，location，and information and information. It refined users' emotions under each type of privacy leak through emotional analysis. Based on this，the emotional loss function of users' privacy leaks was constructed to calculate their emotional losses.［Result/Conclusion］The results indicate that social network users generally exhibit negative emotions in the context of privacy disclosure. There are significant differences in the degree of emotional loss and dispersion caused by different types of privacy disclosure. Among them，the users' emotional loss caused by communication privacy leakage is the most severe，followed by information privacy leakage，social life privacy leakage，and location privacy leakage. In addition，demographic variables such as gender，geographical distribution，and the number of Weibo posts have varying degrees of influence on users' emotional loss of privacy disclosure.

Key words：social network；privacy leakage；loss calculation；LDA；sentiment analysis

收稿日期：2025-01-09
基金项目：国家社会科学基金项目“社交网络数据隐私风险识别与治理研究”（项目编号：22BTQ072）；河南省高等学校哲学社会科学创新团队项目“数据治理与交易流通”（项目编号：2024-CXTD-01）。
作者简介：杨瑞仙（1982-），女，教授，博士，博士生导师，研究方向：数据治理、数据隐私、科学计量等。刘佳涵（2000-），女，硕士研究生，研究方向：数据隐私。
通信作者：孙倬（1994-），男，副研究员，博士，硕士生导师，研究方向：数据隐私、数据要素等。

隐私泄露损失是指用户数据隐私被非法搜集、知悉、公开等行为所导致的损害。随着社交网络的快速发展，海量用户数据在社交网络中存储和传播。社交网络隐私泄露事件一旦发生，就会造成用户的隐私泄露损失。具体而言，隐私泄露直接触发用户的情感反应，导致用户情感上的损失，进而影响用户的相关感知和行为[1]，如降低用户对社交网络的信任程度及其披露意愿、导致用户产生社交网络倦怠，甚至影响用户对社交媒体的持续使用。此外，若相关舆论发酵，还可能造成涉事平台在声誉和经济上的损失[2]。因此，研究用户的隐私泄露情感损失对于社交网络数据隐私风险的治理有重要的学术和应用价值。

现阶段有关隐私泄露的研究主要聚焦两个方面：第一，聚焦技术维度的量化与算法改进，如隐私泄露风险[3]和隐私泄露程度[4]的量化。这些研究虽为判断隐私泄露的严重程度提供了方法，但却未能充分深入探究隐私泄露对用户心理与情感层面造成的影响。第二，聚焦隐私泄露对用户的影响，如用户先前的隐私泄露经历对其隐私关注与隐私披露[5]等方面的影响。值得注意的是，针对隐私泄露导致用户损失方面的研究尚显不足。

鉴于此，本研究结合潜在狄利克雷分配(Latent Dirichlet Allocation，LDA)主题模型与情感分析研究方法，构建社交网络用户隐私泄露情感词典，并通过收集社交网络中用户生成的文本数据，实现隐私泄露情境下用户情感损失的量化与分析，从而构建一个科学、系统的社交网络用户隐私泄露情感损失计算模型。研究用户的情感损失，有助于理解隐私泄露对用户心理机制的影响，为制定有效的隐私保护政策和干预措施提供科学依据。通过量化和分析用户的情感损失，可以更准确地评估隐私泄露事件的社会成本，为社交网络平台的风险管理和应急响应提供决策支持，既能丰富隐私泄露领域的研究，也对社交网络的治理具有指导意义。

1 相关研究

1.1 社交网络用户隐私泄露前因

社交网络用户隐私泄露是一个多维度、多层次的复杂问题，现有研究使用案例分析、统计分析等方法，总结出社交网络用户隐私泄露的前置影响因素，涉及用户自身[6]、技术与管理[7-8]、外部威胁[9]以及法律与政策环境[10]等方面。具体来说，其一是用户隐私保护意识薄弱，社交网络的开放性和透明度使得用户的个人信息更容易被获取和利用，加之用户群体缺乏对个人隐私信息的重视和保护意识，容易成为隐私泄露的薄弱环节。其二是技术与管理缺陷，技术的不完善和管理上的疏忽是用户隐私泄露的重大风险源。社交网络存在一定的技术漏洞，易造成如相关隐私信息被第三方挖掘利用、攻击者非法获取用户隐私信息等现象。另外，用户隐私信息安全体系不完善、用户信息运营单位自我监管不力、企业内部外泄数据等管理上的问题也会导致用户隐私泄露。其三是外部非法行为威胁。外部的黑客攻击和第三方企业的非法行为，对用户隐私信息构成了直接且严重的威胁。其四是法律与政策环境。不同地区的法律法规对隐私保护的要求不同，一些地区的法律与政策环境在保护用户隐私信息安全方面存在不足，缺乏有效的法律约束和监管机制。

1.2 隐私泄露对用户的影响

现有对隐私泄露的研究大多集中于社交网络隐私泄露对用户的影响方面，学者们结合信息系统学、传播学、社会学、心理学等领域的多种理论，主要通过问卷调查收集用户数据，综合扎根理论、结构方程模型等方法，深入探讨了隐私泄露对用户的情感态度及其行为模式的影响。其中，运用较多的理论有隐私计算理论(Privacy Calculus Theory，PC)[11]、沟通隐私管理理论(Communication Privacy Management Theory，CPM)[12]、计划行为理论(Theory of Planned Behavior，TPB)[13]、解释水平理论(Construal Level Theory，CLT)[14]、刺激—机体—反应模型(Stimulus-Organism-Response，SOR)[15]等。

情感是社交网络用户参与社交网络生活的重要组成部分，它不仅影响用户的反应、认知和社会判断，还作用于用户的各种信息行为[16]。隐私泄露通常会导致用户在社交网络中表达一系列负面情绪[17]，这种情绪反应深刻影响用户的心理状态，提升其对于隐私风险的感知水平，降低其对社交网络的信任程度[18]。同时，隐私泄露还显著影响用

户的隐私顾虑，也称为隐私关注[5]，促使用户更加谨慎地审视其在社交网络中的行为及其潜在后果，进而影响用户在社交网络上的披露意愿或行为[19]。

隐私泄露对用户的影响是多维度且复杂的，既包含了负面的心理与行为后果，也孕育了用户自我保护与积极应对的可能性。一方面，用户过往的隐私泄露经历还可能导致其出现“隐私疲劳”“隐私倦怠”等状态[20-21]，表现为用户对隐私保护活动的持续参与感到厌倦，伴随着消极情绪；另一方面，隐私泄露也可能促使用户采取积极的隐私保护措施，对个人信息进行更加谨慎的管理[12]，如调整隐私设置、使用隐私保护工具或服务等。

1.3 隐私度量

隐私度量指通过度量指标或度量方法来直观展示当前隐私信息的泄露风险，以披露隐私信息的风险大小来侧面描述当前隐私保护方法的保护强度[22]。相关研究从内容角度可分为算法层面和评价层面两类，具体如表1所示。

表1 隐私度量相关研究汇总

Tab. 1 Summary of Related Research on Privacy Measurement

类别	二级类别	研究内容	作者
算法层面	信息熵	结合信息熵、互信息、条件熵等基本概念，对隐私泄露情况进行度量	张宏磊等[26]、彭长根等[27]、Gu K等[28]
	K-匿名	通过适当改造数据，使得数据库中的每条记录在特定属性上与使得数据库中的每条记录在特定属性上至少与其他K-1条记录不可区分记录不可区分，从而在数据发布时保护个体的隐私	Liu C G等[29]、Wang H W等[30]、Ren W L[31]、姜火文等[32]
	差分隐私	添加一定量的随机噪声来保护个体的隐私，即使攻击者获得了数据集的访问权限，也无法确定特定的个人信息是否包含在数据集中	吴宁博等[33]、Zhao Y等[34]
评价层面	——	综合多个维度，对隐私泄露等情况进行量化评估	朱光等[35]、田波等[36]、杨瑞仙等[37]、Lin X J等[38]

1）算法层面。基于经典隐私度量算法，从技术角度进行完善，旨在提升隐私度量的效率与准确度。Shannon C E[23]提出的信息熵理论(Information Entropy)可量化信息的不确定性，成为了信息的度量和通信的理论基础，为隐私度量的研究提供了十分重要的理论支撑。除信息熵外，Sweeney L[24]提出的K-匿名模型(K-anonymity)也是一种简单且高效的隐私保护手段，K-匿名自提出以来得到了广泛研究，现如今已成为经典的隐私度量指标之一。Dwork C[25]提出的差分隐私(Differential Privacy)也为隐私度量提供了方法支持，该方法可通过添加噪声机制使数据失真来保护数据的隐私性，与传统的隐私保护方法相比，它定义了一个极为严格的攻击模型，大大降低隐私泄露风险的同时，极大地保证了数据的可用性。

2）评价层面。多基于文献调研、德尔菲法、层次分析等方法，从评价角度出发，通过建立相关隐私评估指标体系对隐私进行量化。信息熵理论、K-匿名模型和差分隐私等方法为隐私度量提供了坚实的理论基础和技术手段，基于文献调研和专家评估的方法则为隐私度量提供了量化的评价体系。

1.4 研究述评

通过文献梳理可以看出，目前，相关研究主要集中在隐私泄露的前因、影响以及隐私度量研究上，主要涉及计算机、信息资源管理、心理学等领域。尽管社交网络用户隐私泄露问题已受到广泛关注，但在研究过程中仍存在一些不足和挑战。一方面，当前研究对社交网络用户隐私泄露的机制和规律的探索还不够深入，现有研究多采用问卷调查方法，在研究方法上存在局限，受访者可能因为社会期望、个人形象管理等因素而不真实地回答问题，导致数据偏差，难以全面、深入地揭示用户隐私泄露行为；另一方面，用户隐私泄露所导致的损失包括经济、声誉、信任以及

情感等多个方面，但目前尚未有系统的研究对用户隐私泄露损失进行全面的量化评估和分析。因此，本研究通过收集用户社交网络中生成的实际数据，对用户在隐私泄露情境下的情感损失进行更为客观和深入地分析。

2 研究设计

社交网络为用户提供了实时的情感分享与交流的渠道，其中的用户生成内容(User-Generated Content，UGC)呈现了丰富的情感表达，涵盖了不同年龄层、性别和地域的用户对隐私泄露事件的即时反应，为研究用户隐私泄露情感损失提供了丰富的数据，使得情感损失的量化成为可能。因此，通过对社交网络 UGC 的情感分析，可以深入探讨隐私泄露情境下用户的情感损失及其心理特征。首先，采用 Python 网络爬虫技术，从微博这一具有代表性的社交网络平台采集用户发布的与隐私泄露相关的文本数据。其次，对所采集的数据进行去重、清洗、分词、去停用词等预处理操作，构建了社交网络用户隐私泄露数据集。接着将 LDA 主题模型与情感分析相结合，深入挖掘用户发布的隐私泄露相关文本内容，对不同隐私泄露类型下的用户情感进行细粒度分类。最后，构建社交网络用户隐私泄露情感损失函数，计算表达负面情感的用户在隐私泄露事件中的情感损失，具体的研究设计框架如图 1 所示。

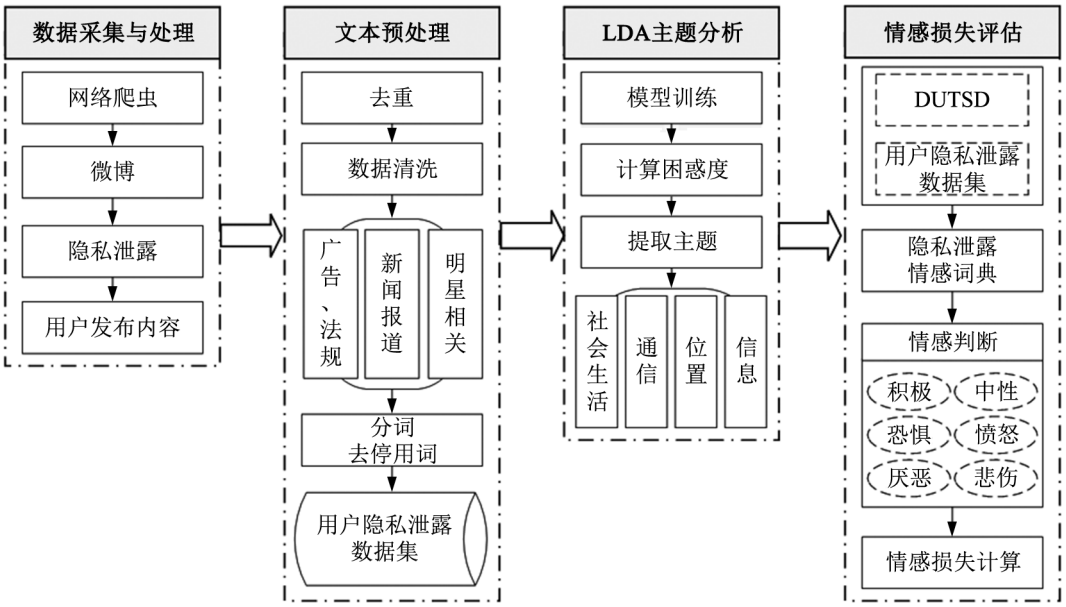

图 1 研究设计

Fig. 1 Study Design

2.1 主题分析

LDA 模型是一种发现文档主题分布的三层贝叶斯概率模型，属于无监督学习模型，包含词项、主题和文档三层结构，可以用来识别大规模文档集或语料库中潜藏的主题信息。其将每一篇文档视为一个词频向量，从而将文本信息转化为易于建模的数字信息。将每篇文档看作各种隐含主题的混合，而每个主题则表现为与该主题相关的词项的概率分布。已有研究发现，基于词频-逆文档频率(Term Frequency-Inverse Document Frequency，TF-IDF)算法的 LDA 模型可以降低主题之间的词汇相似度，使得主题特色更加鲜明。

基于 LDA 模型进行主题聚类的主要目的是通过对用户发表的内容进行主题挖掘，得到聚类后的主题及每个主题下的主要关键词，从中发现用户隐私泄露类型，为后续划分维度提供依据。本研究选用困惑度(Perplexity)指标求取最佳的主题数目[39]，如式（1）所示：

$$P(D)=exp\left\{-\frac{\sum_{d=1}^{M}\log p(w_d)}{\sum_{d=1}^{M}N_d}\right\} \tag{1}$$

其中，D 表示语料库中的测试集，M 表示文档数量，w_d 表示文档 d 中的总词数，N_d 表示每篇文档

的单词数，$p(w_d)$表示测试文档中w_d的出现频率。困惑度越低，模型预测效果越好。

2.2 用户隐私泄露损失情感词典构建

情感分析(Sentiment Analysis)是非常重要的文本挖掘手段，通常包括爬取信息、分词、定义情感词典提取每个文本中的情感词、通过情感词构建情感矩阵并计算情感分数、结果评估等步骤，基本流程如图2所示。

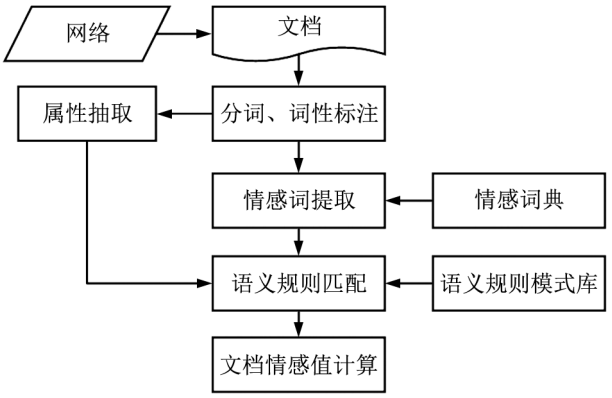

图2 情感分析基本流程

Fig. 2 Basic Flow of Sentiment Analysis

在当前的情感分析研究领域，几个颇具影响力的中文情感词典已得到广泛认可，其中包括大连理工大学中文情感词汇本体库(DUTSD)、知网的HowNet情感词典等。本研究选取了大连理工大学情感词汇本体库作为基础情感词典，该词典涵盖了27 466个情感词汇，并将情感划分为7个主要类别：乐、好、怒、哀、惧、恶、惊。鉴于社交网络用户对于隐私泄露事件普遍持有负面情感态度，本研究在DUTSD原有情感大类的基础上，进行了针对性地扩展与细化，划分为积极、中性、恐惧、愤怒、厌恶、悲伤6个具体类别，以更好地捕捉和分析用户在隐私泄露情境下的负面情感，同时也考虑到可能存在的积极或中性情感态度，具体分类如表2所示。

表2 情感分类

Tab. 2 Emotional Classification

情感	解释
积极	用户表现出的一种正面情绪状态，主要为用户对事件结果的乐观预期或对个人能力的自信
中性	用户表现出的一种无明显情感倾向的状态，对隐私被泄露的情感反应不强，或者情感反应处于平衡状态
恐惧	用户表现出的担忧、不安和恐慌的情绪状态，主要为用户对个人信息和隐私遭受侵害的担忧，以及对未来可能出现的负面后果的恐惧
愤怒	用户表现出的强烈不满和激动的情绪状态，通常伴随着对相关责任方的指责和对抗意愿，体现了个人对于正义和公平的强烈诉求
厌恶	用户对责任方产生的远离和排斥情绪，体现了用户对于侵犯隐私行为的反感以及对责任方失去信任和期望的情绪
悲伤	用户表现出的悲伤、失落和忧郁的情绪，主要为对隐私泄露带来的负面后果的悲伤和对当前情况的无力感

DUTSD中的词性种类共有7类，分别是名词(noun)、动词(verb)、形容词(adj)、副词(adv)、网络用语(nw)、成语(idiom)、介词(prep)。词典中的每个情感词汇均被赋予了明确的情感强度和情感极性标识，为情感词汇的情感力度提供了一个直观且可量化的衡量标准。情感强度的量化分为5个等级，分别为1、3、5、7、9，其中9代表情感强度最高，1则表示情感强度最低。在情感极性方面，划分为褒义、贬义和中性三大类，分别以1、2、0进行赋值，以体现不同情感词汇的情感倾向。

本研究结合在微博平台收集的用户隐私泄露相关文本数据，从预处理后的语料库中筛选出未收录于DUTSD但出现频次达到或超过20次的218个词汇，将其定义为特定情感词。社交网络用户隐私泄露情感词典的部分示例如表3所示。

2.3 用户情感损失计算

本研究结合否定词典和程度词词典，为了凸显贬义情感词汇的消极色彩，将其情感极性赋值转换为-1。用户情感损失函数如式（2）所示：

$$L = \sum_{i=1}^{n} p_i s_i \tag{2}$$

其中，L为情感损失值，p_i为第i个情感词汇的情感极性，s_i为第i个情感词汇的情感强度，n为文本中情感词汇的数量。L值越低，用户的情感损失程度越高。

表 3 用户隐私泄露情感词典示例

Tab. 3 Example of Emotional Dictionary of User Privacy Disclosure

词性	词语	情感强度	极性
noun	姓名、地址、访客、……	3	2
	风险、受害者、违规行为、……	5	2
verb	导致、举报、曝光、……	5	2
	偷窥、骚扰、暴露、……	7	2
adj	频繁、重大、异常、……	3	2
	委屈、高仿、严重、……	5	2
	有病、烦死、真服了、……	7	2
nw	取关、被盗、注销、……	3	2
	裂开、拉黑、避雷、……	5	2
	允悲、视奸、网暴、……	7	2

3 实证研究

3.1 数据收集与处理

3.1.1 数据收集与筛选

作为影响力较高的中文社交媒体，微博平台汇聚了海量用户的情绪表达、意见交流和观点分享，为研究社会热点问题提供了丰富的数据资源。故本研究利用微博这一典型社交平台获取研究数据，数据采集的时间范围为2023年1月1日—2024年5月31日，本文的研究对象是隐私泄露相关的微博文本，故以“隐私泄露”“信息泄露”“微博隐私”为关键词对相关内容进行爬取，共爬取数据70 103条。

在筛选微博数据时，笔者发现获取的微博数据存在内容混杂、数据质量低下的问题。为提高数据相关性，本研究首先排除了不涉及隐私泄露的文本，如广告、法律法规条文、考试试题以及带有“防止隐私泄露”“不会泄露个人信息”“隐私设置”等字样的内容。其次，新闻报道倾向于遵循客观性原则，其情感表达通常较为克制，与普通用户生成的文本相比情感态度并不明显。同时，涉及明星隐私泄露的讨论往往受到粉丝群体主观情感的影响，这种情感态度可能会偏离一般用户对隐私泄露问题的普遍感受。因此，本研究剔除了包含新闻报道和明星姓名的微博条目，以消除潜在的情感偏差。最后，鉴于微博转发机制导致的重复内容，以及不同账号发布相同文本的情况，本研究也进行了相应的删除处理。

在此基础上，本研究将爬取到的微博文本分为“隐私泄露相关”与“隐私泄露无关”两类，利用百度智能云平台进行数据相关性标注，首先人工标注了1 000条文本，然后使用平台进行智能标注，通过迭代优化，实现了数据的精准分类，最终形成了一个包含9 719条隐私泄露相关微博的精炼数据集，部分数据如表4所示。该数据集不仅包含微博文本，还包括发布时间、发布者id、性别、IP归属地等用户信息。数据集排除了上述干扰内容，确保了研究样本的客观性和代表性，有助于在后续分析中更准确地捕捉微博用户群体对隐私泄露问题的情感倾向和认知态度。

3.1.2 数据预处理

在处理微博文本数据时，本研究注意到微博平台特有的文本特征，如转发标记、@用户以及超话标签等，这些元素虽为用户所发布文本的一部分，但与用户隐私泄露后的情绪表达并无直接相关性。为提高文本分析的准确性，本研究采取了一系列文本预处理步骤：首先，采用正则表达式对微博文本进行清洗，以排除转发关系标识、用户提及、超话格式以及表情符号等非核心文本内容，旨在消除这些元素对后续分词过程的潜在干扰，确保分词结果的纯净度。其次，利用Jieba分词工具对清洗后的文本进行分词处理。最后，为进一步提升文本分析的精确度，在完成初步分词后，使用哈工大停用词表，剔除在文本中无实际意义的词汇和特殊符号。

3.2 LDA主题分析

本研究建立了LDA模型，其中参数alpha、eta值选取经验值，最大迭代次数为300。使用Python中的gensim库进行建模，并使用pyLDAvis库以可

表 4 微博用户隐私泄露相关数据示例

Tab. 4 Examples of Data Related to User Privacy Disclosure on Weibo

字段名	示例 1	示例 2	示例 3
发布内容	好奇怪，我在 tb 的收货地址只写到我家在哪条街几号楼[思考]从未写过楼层号码，然而今天快递通过菜鸟直接给我送货上门了(期间从未与我打过电话或发过短信沟通)，我这是隐私被泄露了……？[思考]	生活在这个社会，个人隐私真的是防不胜防的被泄露；这种所谓的“推荐”，难道不是应该默认“关闭”的吗；抖音真的是下三滥，时刻都在泄露用户隐私信息#抖音##抖音隐私设置#	真的无语，在小红薯上面咨询了一些种牙相关的，一年的时间内陆陆续续有骚扰电话打进来，真的很烦，信息泄露好烦啊
发布时间	2023/3/23	2024/2/28	2024/5/29
发布者 id	174****163	781****371	783****432
性别	女	男	女
IP 属地	广东	江苏	四川
全部微博数	52 287	3 551	91
加入微博时间	2010/5/23	2023/1/4	2023/4/27

视化的方式输出困惑度指数，如图 3 所示。由图 3 可知，主题数为 4 时，模型的困惑度最低。因此，LDA 主题模型共包含 4 个主题，主题聚类结果较为明晰。

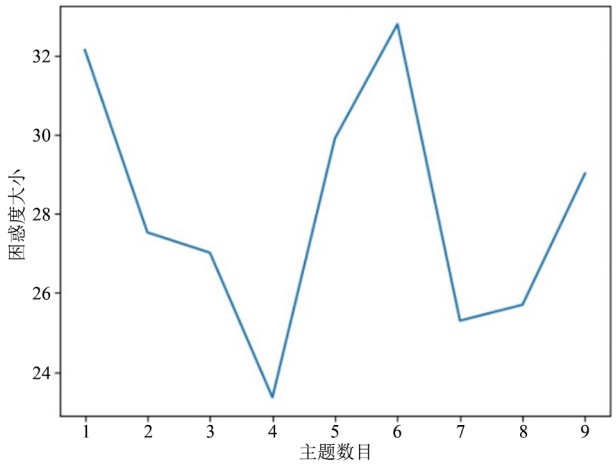

图 3 困惑度曲线图

Fig. 3 Confusion Graph

在上述基础上，本研究提取了各主题中词频位列前 30 的主题特征词。为了凸显各主题的独特性及其差异，经过对比筛选，仅保留了每个主题下最具代表性的高频特征词。通过对特征词的语义分析发现，每个主题下的特征词分布反映了社交网络用户隐私泄露的不同类型。综合各学者对隐私类型的定义[40-43]，本研究将 4 个主题分别命名：

主题 1，社会生活隐私泄露，即与个人在社会生活中的生活习惯、人际关系等相关的隐私被泄露，包括社交关系网络、个人兴趣爱好、购物消费记录等；主题 2，通信隐私泄露，即与他人交流相关的信息的隐私被泄露，包括手机号码、电子邮件等；主题 3，位置隐私泄露，即与个人所处位置相关的信息被泄露，包括工作地址、家庭住址、个人行程信息等；主题 4，信息隐私泄露，即与个人身份相关的隐私被泄露，包括姓名、年龄、性别、身份证号码、医疗健康信息、银行账号等。各主题的相关高频特征词如表 5 所示。

3.3 情感损失计算结果

3.3.1 情感类型判断

本研究基于构建的用户隐私泄露情感词典，深入分析用户对不同类型隐私泄露的情感反应。不同隐私泄露类型下用户情感分布如图 4 所示。由图 4 可知，不同主题下的用户情绪分布呈现出显著差异。在各类隐私泄露情境中，用户表现出积极情绪的比例最低，仅有少数用户发布的文本中无明显情绪色彩，这些用户客观地陈述了个人隐私遭受泄露的事实。相比之下，大多数用户在遭遇隐私泄露事件后，普遍表现出厌恶和悲伤的情绪，这主要源于对隐私泄露责任方的排斥以及对个人隐私泄露后自身困境的哀伤。

在社会生活和位置隐私泄露情境下，用户的悲伤情绪占比最为显著。大量用户通过社交媒体

表 5 微博用户隐私泄露主题提取结果

Tab. 5 Extraction Results of User Privacy Disclosure Topics on Weibo

主题概括	高频特征词
社会生活隐私泄露	微博、关注、知道、评论、看到、现在、朋友、微笑、感觉、记录、发现、觉得、好友、东西、朋友圈、功能、主页、微信、认识、设置、显示
通信隐私泄露	电话、诈骗、知道、手机号、客服、超话、收到、打电话、骗子、大家、账号、投诉、平台、收集、严重、已经
位置隐私泄露	用户、数据、快递、手机、安全、保护、问题、公司、行为、事件、使用、禁言、公民、影响、风险、法律、时代、提供、汽车、存在、涉及
信息隐私泄露	照片、个人隐私、公开、允悲、侵犯、属于、别人、网络、孩子、没有、应该、视频、媒体、现在、出来、网上、密码、实名、违法、举报

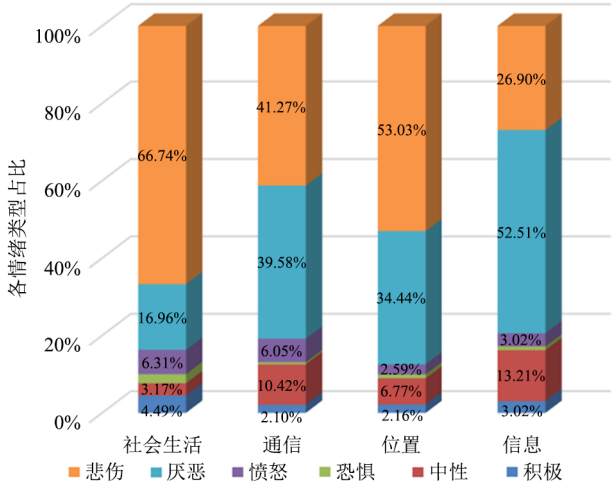

图 4 不同隐私泄露类型下用户情感分布

Fig. 4 User's Emotional Distribution Under Different Privacy Leak Types

表达了相关隐私被泄露的无奈与难过，反映出用户在遭遇社会生活与位置泄露的无助感。而在通信和信息隐私泄露情境中，用户的厌恶情绪占据较大比例。多数用户经历了陌生快递、电话被曝光、行程信息被泄露等事件后，才在社交媒体上发布了自己隐私被泄露的内容，并表现出对相关责任方的强烈反感。此外，社会生活和通信隐私泄露情境下用户的愤怒情绪占比较高，这进一步说明用户对社会生活与通信隐私的重视程度高于另外两种类型的隐私信息。此外，社会生活隐私泄露相关文本中用户的恐惧情绪占比最高，此类内容下用户主要表达了个人社交账号中的内容会被与自己相识的人看到的担忧。

3.3.2 情感损失计算

判断出各文本情感态度后，排除各类型下的积极与中性文本，将恐惧、愤怒、厌恶、悲伤4种情绪的文本继续进行情感损失计算。在对4个不同隐私泄露类型中的文本内容进行定量分析时，本研究采用了一系列统计指标，包括平均值、方差和标准差，以揭示用户的情感倾向及其分布特性。平均值(Mean Score)是衡量用户整体情感倾向的关键指标，方差(Variance)和标准差(Standard Deviation)量化了用户情感损失的分布离散程度，揭示用户情感反应的差异性。通过考察不同类型隐私泄露的情感损失程度及其分布特征，可以更深入地洞察用户在不同隐私泄露场景下的心理反应及其差异性。用户的各类型隐私泄露情感损失计算结果如表6所示，各类用户情感损失统计结果如表7所示。

表 6 用户情感损失计算结果

Tab. 6 Calculation Results of Users' Emotional Loss

类型	数据量	情感损失得分		
		平均值	方差	标准差
社会生活隐私泄露	2 532	−7.25	142.99	11.96
通信隐私泄露	1 503	−15.84	279.43	16.72
位置隐私泄露	632	−15.21	260.63	16.14
信息隐私泄露	3 824	−12.75	226.49	15.05

4 研究结果分析与讨论

4.1 研究结果分析

4.1.1 情感损失程度与类型相关性分析

通信隐私的泄露对用户情感所造成的伤害最为严重，其情感损失程度在四类隐私泄露中居于首位，平均情感损失得分达到−15.84。通信隐私涉及用户的电话号码、电子邮件等联系方式，该

表 7 各类用户情感损失统计结果

Tab. 7 Statistical Results of Emotional Loss of Various Users

用户特征损失类型		社会生活隐私		通信隐私		位置隐私		信息隐私	
		平均值	标准差	平均值	标准差	平均值	标准差	平均值	标准差
性别	男性	−8. 58	11. 28	−16. 05	15. 45	−17. 32	17. 92	−13. 28	15. 37
	女性	−6. 93	12. 1	−15. 72	17. 42	−14. 11	15. 05	−12. 41	14. 83
IP属地	西部	−6. 53	14. 7	−16. 58	15. 17	−12. 81	10. 12	−13. 56	14. 78
	中部	−7. 97	11. 27	−13. 56	13. 05	−14. 21	20. 30	−12. 70	16. 13
	东部	−7. 05	11. 22	−15. 15	14. 98	−14. 84	16. 84	−12. 56	14. 84
	东北	−6. 98	10. 82	−13. 42	17. 31	−15. 93	12. 36	−15. 11	16. 15
微博数量	＜500条	−7. 28	10. 81	−17. 00	17. 27	−18. 28	18. 55	−12. 83	16. 64
	≥500条	−7. 24	12. 34	−15. 45	16. 52	−14. 39	15. 36	−12. 74	14. 70
使用年限	≤1年	−8. 48	10. 16	14. 56	21. 35	−10. 98	8. 30	−12. 28	15. 54
	1~3年	−7. 59	11. 41	−17. 12	15. 68	−15. 67	14. 54	−12. 37	13. 55
	≥3年	−7. 18	12. 06	−15. 83	16. 59	−15. 35	16. 42	−12. 81	15. 13

类隐私一旦泄露，用户将面临垃圾短信、邮件和电话的骚扰，直接侵犯了用户的沟通自主权，破坏了用户对沟通渠道的控制感，甚至导致用户成为电信诈骗等犯罪活动的受害者，对用户的财产安全构成威胁。此外，垃圾信息的不断涌入和骚扰电话的频繁打扰，构成了对用户日常生活秩序的持续性干扰，加剧了用户在社交网络中的不安全感，从而引发用户强烈的负面情绪。

位置隐私泄露的平均情感损失相对较高，平均值为−15. 21，情感损失程度仅次于通信隐私泄露。位置隐私的范畴主要涉及用户的地理位置信息，包括但不限于行程路线、居住或工作地点等。此类信息直接关联到个人的行动轨迹和生活习惯，其泄露可能导致用户的行为模式被他人洞察。此外，位置隐私的泄露与个人的日常生活紧密相关，其影响具有即时性和持续性。用户在意识到自己的位置信息可能被他人获取时，可能会持续感受到焦虑和恐惧，这种心理负担是情感损失程度相对严重的主要原因。

信息隐私泄露情感损失平均值为−12. 75，信息隐私涉及个人的身份信息、医疗信息、财务信息等敏感数据。信息隐私通常较为私密，与通信隐私或位置隐私相比，其与用户的日常活动联系不那么紧密。这类信息的泄露可能不会立即对用户的日常生活造成干扰，从而使得情感损失相对较轻。而与社会生活隐私泄露相比，信息隐私泄露涉及的信息更为敏感和具体，社会生活隐私泄露一般不会直接导致严重的后果，用户通常会对社会生活隐私的泄露感到不快。但信息隐私泄露后果较为严重，可能导致用户财务安全、个人形象或信用受损，因此其情感损失更为严重。

社会生活隐私泄露的平均情感损失得分为−7. 25，在四类隐私泄露中的情感损失平均值最高，表明社会生活隐私的泄露对用户情感造成的损失程度较轻。社会生活隐私包括用户在社会生活中的生活习惯、人际关系等相关信息，该类信息范畴较为宽泛，且在一定程度上已被社会规范和公众预期所接受。此类信息泄露通常不会直接导致即刻的安全威胁，但可能会对个人的长期社会生活产生负面影响，与通信隐私泄露可能带来的直接骚扰或诈骗相比，其紧迫性和危害性较低。此外，社会生活隐私信息往往具有一定的可塑性，用户可以通过社会互动和自我呈现来调整或重塑社会形象，从而减轻隐私泄露带来的情感损失，故该类型隐私泄露对用户的心理冲击相对有限。

4. 1. 2 情感损失离散程度分析

研究结果显示，通信隐私泄露（方差 279. 43，标准差 16. 72）与位置隐私泄露（方差 260. 63，标准

差 16. 14)的情感损失的离散程度较为显著，表明了用户在遭受这两种隐私泄露时的情感损失具有显著差异性。此种差异主要归因于用户对隐私泄露潜在后果的不同感知，及其对相关隐私信息敏感度的个体差异。具体而言，用户对于隐私泄露可能引发的后果持有不同的实际体验，这导致相同隐私泄露类型下用户情感损失的差异化表现。例如，在通信隐私泄露情境中，某些用户可能仅遭受诸如电话推销或垃圾短信的轻微骚扰，情感损失相对较轻；而其他用户可能遭受如电信诈骗等，产生更为严重的后果，从而引发严重的情感损失。同样，不同用户对于同一类型信息泄露的敏感度也有差别。以位置信息泄露为例，部分用户可能对此类泄露表现出高度的警觉性，认为其居住安全和个人自由受到威胁，从而产生强烈的负面情感；其他情感损失程度较低的用户可能对位置信息的泄露持有较为宽容的态度，认为这种情况在社交网络互动中是不可避免的。因此，即便是在同一隐私泄露类型下，不同用户所表现出的情感损失程度亦呈现出显著异质性。

社会生活隐私泄露的情感损失得分离散程度最低，方差为 142. 99，标准差为 11. 96，表明用户在此类隐私泄露中的情感反应相对平稳，没有出现显著的波动。相比于其他 3 种类型的隐私信息，社会生活隐私内容通常较为公开，用户在社交网络日常互动中已经适应了一定程度的社会生活信息共享。社会生活隐私泄露中用户的整体损失程度较轻，这种较低的损失程度使多数用户在遭受此类隐私泄露时表现出相对温和的情感反应，如悲伤、厌恶等情绪。

4. 1. 3 人口统计学特征与情感损失的相关性分析

性别因素方面，研究结果显示，男性样本与女性样本在情感损失得分上存在显著差异。具体而言，男性样本的平均情感损失得分普遍低于女性样本，体现出男性群体面对隐私泄露时的情感反应更为强烈；地域分布方面，IP 属地分类揭示了情感损失得分的区域性差异。研究发现，中部与东部地区的用户在遭遇隐私泄露时所表现出的情感损失程度较高。

微博数量方面，发布数量较少的用户群体在隐私泄露事件中的情感损失更为严重，这表明在社交网络上披露内容较少的用户对其隐私泄露的敏感度更高，该群体在隐私保护方面持有更为坚定的立场；使用年限方面，使用年限较长的用户在隐私泄露事件中的情感损失程度相对较低，反映出随着使用经验的积累，用户对隐私泄露的容忍度有所提高。相反，使用年限较短的用户在遭遇隐私泄露时表现出更高的敏感性，这一群体由于较少接触社交媒体，在遭受隐私泄露时缺乏相关的应对经验和心理准备，从而导致情感损失程度较高。

4. 2 研究结果讨论

本文基于社交网络用户数据，对用户的负面情感进行细粒度划分，并计算用户的情感损失，揭示了不同类型与不同用户之间隐私泄露情感损失的差异，有助于更深入地理解用户在隐私泄露情境下的情感反应，为研究用户在隐私泄露情境下的信息行为提供了新的视角。

1）研究发现，多数用户遭遇隐私泄露时会表现出负面的情感态度，这一结果与谭春辉等[17]的研究结论一致，说明隐私泄露对用户情感的影响是普遍存在的。本研究认为，隐私泄露侵犯了用户对其个人信息控制权，引发了对信息安全以及对隐私泄露潜在后果的担忧，而社交网络的开放性、交互性、共享性等特性放大了用户隐私泄露影响，进而加深用户的负面情感体验。此外，该研究结果映射出用户对于隐私保护的期望与实际保护水平之间的差距，从而凸显出隐私保护在保障用户心理健康及促进社交网络健康发展方面的重要意义。

2）在本研究的 4 种隐私泄露类型中，通信隐私泄露导致的情感损失最为严重，其次是位置隐私泄露，而信息隐私泄露和社会生活隐私泄露的情感损失相对较轻。李睿等[44]测量了网络环境下用户的隐私泄露容忍度，将通信方式归纳至信息隐私中，该研究得出用户对信息隐私容忍度较低的结果，与本研究的研究结论一致。但李睿等认为，用户对位置隐私的容忍度较高，这与本研究的研

究结果相悖。对于这一差异，解释如下：一方面，本研究收集的是用户经历过隐私泄露之后的数据，而接受问卷调查的用户可能没有相关经历，填写问卷时更多地依赖于认知判断，可能存在事前评估与事后体验之间的差异；另一方面，用户在填写问卷过程中对于位置隐私泄露的容忍度可能受到特定情境的影响，而在实际社交网络环境中，隐私泄露的具体情境可能与问卷中所设定的情境有所不同。

3）人口统计学特征对情感损失有显著影响。第一，男性在隐私泄露事件中的情感损失得分普遍低于女性，显示出更强烈的情感反应。研究表明，男性的隐私披露行为更少[45]，故男性群体对于其隐私泄露更加难以忍受，从而比女性表现出更为强烈的情感反应。第二，在地域分布上，中国中部与东部地区的用户情感损失程度较高。地区文化、经济发展水平是造成不同地区间差异的潜在影响因素。经济发展水平较高的地区，用户对于个人隐私权益的维护意识及需求亦相应提升，从而可能在一定程度上加剧了这些地区用户在情感损失层面的感受。第三，在本研究中，较少进行自我披露的用户以及使用年限较短的用户群体在隐私泄露事件中的情感损失更为严重。已有研究表明，晚期注册用户比早期注册用户更注重个人基本信息的隐私安全[46]，与本文的研究结果相符。

5 总结与展望

本研究聚焦社交网络用户隐私泄露导致的情感损失，结合LDA主题模型与情感分析，实现了隐私泄露情境下用户情感损失的量化评估。通过深入剖析用户情感反应及差异，为研究社交网络隐私泄露问题提供了新的视角和方法，还为制定隐私保护政策和干预措施提供了科学依据。

此外，本研究仍存在局限，需要在未来的研究中进一步完善。第一，本研究主要基于用户生成的文本数据进行分析，而忽略了图像、视频等其他模态数据中蕴含的情感信息。未来可以结合图像、视频等多模态数据展开研究，更全面地分析用户的隐私泄露情感损失。第二，本研究主要关注用户的情感损失，而用户隐私泄露也可能导致经济损失。未来研究可以进一步探讨用户隐私泄露对其经济方面的影响，以更全面地评估用户隐私泄露损失。

参 考 文 献

[1] 李华强，周雪，万青，等. 网络隐私泄露事件中用户应对行为的形成机制研究——基于PADM理论模型的扎根分析[J]. 情报杂志，2018，37（7）：113-120.

[2] Tripathi M，Mukhopadhyay A. Financial Loss Due to a Data Privacy Breach：An Empirical Analysis [J]. Journal of Organizational Computing and Electronic Commerce，2020，30（4）：381-400.

[3] 谢小杰，梁英，王梓森，等. 社交网络用户隐私泄露量化评估方法[J]. 计算机工程与科学，2021，43（8）：1376-1386.

[4] 胡文彬，张宏宇，王晨曦，等. 社交网络中攻击背景下个人隐私泄露度量研究[J]. 南京大学学报（自然科学），2021，57（2）：289-298.

[5] Malandrino D，Scarano V. Privacy Leakage on the Web：Diffusion and Countermeasures [J]. Computer Networks，2013，57（14）：2833-2855.

[6] Wang Z，Yu Q. Privacy Trust Crisis of Personal Data in China in the Era of Big Data：The Survey and Countermeasures [J]. Computer Law & Security Review，2015，31（6）：782-792.

[7] 陆雪梅，古春生. 大数据环境下用户信息隐私泄露成因分析和保护对策[J]. 现代情报，2016，36（11）：66-70.

[8] 迪莉娅. 大数据环境下隐私泄露影响评估研究[J]. 情报杂志，2016，35（4）：141-146.

[9] 金元浦. 论大数据时代个人隐私数据的泄露与保护[J]. 同济大学学报（社会科学版），2020，31（3）：18-29.

[10] 肖成俊，许玉镇. 大数据时代个人信息泄露及其多中心治理[J]. 内蒙古社会科学（汉文版），2017，38（2）：185-192.

[11] 杨瑞仙，李兴芳，王栋，等. 隐私计算的溯源、现状及展望[J]. 情报理论与实践，2023，46（7）：158-167.

[12] 耿瑞利，王一凡. 社交媒体用户隐私管理策略的选择与影响：一项准实验研究[J]. 图书情报工作，2024，68（3）：94-104.

[13] 张一涵，袁勤俭. 计划行为理论及其在信息系统研究中的应用与展望[J]. 现代情报，2019，39（12）：138-148，177.

[14] 李贺，余璐，许一明，等. 解释水平理论视角下的社交网络隐私悖论研究[J]. 情报学报，2018，37（1）：1-13.

[15] 周涛，刘佳怡，邓胜利. 基于SOR模型的在线知识社区用户潜水行为研究[J]. 情报杂志，2022，41（7）：160-165，83.

[16] Nahl D. Affective and Cognitive Information Behavior：Interaction Effects in Internet Use [J]. Proceedings of the American

Society for Information Science and Technology， 2005， 42（1）：1-14.

［17］ 谭春辉，陈晓琪，梁远亮，等. 隐私泄露事件中社交媒体围观者情感分析［J］. 情报科学，2023，41（3）：8-18.

［18］ 李伟娟，林升栋. 社交媒体隐私侵犯后的信任修复机制探究［J］. 图书情报工作，2021，65（17）：33-44.

［19］ 程慧平，闻心玥，苏超. 社交媒体用户隐私披露意愿影响因素模型及实证研究［J］. 图书情报工作，2020，64（16）：92-104.

［20］ 臧国全，董文馨. 隐私无助的形成机理研究——以社交网络新浪微博为例［J］. 情报理论与实践，2022，45（9）：110-118.

［21］ Chen S B， Gu C Y， Wei J， et al. Research on the Influence Mechanism of Privacy Invasion Experiences with Privacy Protection Intentions in Social Media Contexts： Regulatory Focus as the Moderator［J］. Frontiers in Psychology， 2023， 13：1031592.

［22］ 熊金波，王敏燊，田有亮，等. 面向云数据的隐私度量研究进展［J］. 软件学报，2018，29（7）：1963-1980.

［23］ Shannon C E. The Mathematical Theory of Communication (Reprinted)［J］. M D Computing，1997，14（4）：306-317.

［24］ Sweeney L. k-Anonymity： A Model for Protecting Privacy［J］. International Journal of Uncertainty， Fuzziness and Knowledge-Based Systems，2002，10（5）：557-570.

［25］ Dwork C. Differential privacy［C］//Bugliesi M， Prennel B， Sassone V， et al. Lecture Notes in Computer Science. BERLIN：SPRINGER-VERLAG BERLIN，2006：1-12.

［26］ 张宏磊，史玉良，张世栋，等. 一种基于分块混淆的动态数据隐私保护机制［J］. 计算机研究与发展，2016，53（11）：2454-2464.

［27］ 彭长根，丁红发，朱义杰，等. 隐私保护的信息熵模型及其度量方法［J］. 软件学报，2016，27（8）：1891-1903.

［28］ Gu K， Li C， Deng Y. Social Privacy-Preserving Modeling Based on Graphical Evolutionary Game and Infectious Disease Dissemination Dynamics［J］. IEEE Transactions on Computational Social Systems，2024，11（3）：3882-3899.

［29］ Liu C G， Liu I H， Yao W S， et al. K-Anonymity Against Neighborhood Attacks in Weighted Social Networks［J］. Security and Communication Networks，2015，8（18）：3864-3882.

［30］ Wang H W， He J S， Zhu N F. Improving Data Utilization of K-Anonymity through Clustering Optimization ［J］. Transactions on Dataprivacy，2022，15（3）：177-192.

［31］ Ren W L， Ghazinour K， Lian X. KT-Safety： Graph Release via K-Anonymity and T-Closeness［J］. IEEE Transactions on Knowledge and Data Engineering，2023，35（9）：9102-9113.

［32］ 姜火文，曾国荪，马海英. 面向表数据发布隐私保护的贪心聚类匿名方法［J］. 软件学报，2017，28（2）：341-351.

［33］ 吴宁博，彭长根，牟其林. 面向关联属性的差分隐私信息熵度量方法［J］. 电子学报，2019，47（11）：2337-2343.

［34］ Zhao Y， Chen J J. A Survey on Differential Privacy for Unstructured Data Content［J］. ACM Computing Surveys，2022，54（10s）：1-28.

［35］ 朱光，崔维军，张薇薇. 信息生命周期视角下的大数据隐私风险管理框架研究［J］. 情报资料工作，2016（1）：99-103.

［36］ 田波，郑羽莎，刘鹏远，等. 移动APP用户隐私信息泄露风险评价指标及实证研究［J］. 图书情报工作，2018，62（19）：101-110.

［37］ 杨瑞仙，沈嘉宁，许帆，等. 社交媒体APP隐私政策评价指标体系构建及实证研究［J］. 情报理论与实践，2023，46（1）：81-89.

［38］ Lin X J， Liu H， Li Z， et al. Privacy Protection of China's Top Websites： A Multi-Layer Privacy Measurement via Network Behaviours and Privacy Policies［J］. Computers & Security，2022，114：102606.

［39］ 关鹏，王曰芬. 科技情报分析中LDA主题模型最优主题数确定方法研究［J］. 现代图书情报技术，2016（9）：42-50.

［40］ Banisar D， Davies S. Global Trends in Privacy Protection： An International Survey of Privacy， Data Protection， and Surveillance Laws and Developments［J］. The John Marshall Journal of Computer and Information Law，2012，18：1-111.

［41］ 邱均平，李艳红. 社交网络中用户隐私安全问题探究［J］. 情报资料工作，2012（6）：34-38.

［42］ 王树义，刘赛，马峥. 基于深度迁移学习的微博图像隐私分类研究［J］. 数据分析与知识发现，2020，4（10）：80-92.

［43］ 沈旺，代旺，高雪倩，等. 基于多重图的社交网络用户可信度评价方法研究——网络欺凌与隐私泄露视角［J］. 现代情报，2020，40（8）：27-37.

［44］ 李睿，张锐剑，李文立，等. 移动互联网环境下的隐私泄露容忍度测度方法［J］. 管理评论，2016，28（7）：102-111.

［45］ 杨瑞仙，许帆，沈嘉宁，等. 基于社会渗透理论的社交网络用户隐私披露行为研究［J］. 图书情报工作，2023，67（6）：84-95.

［46］ 胡昌平，仇蓉蓉，王丽丽. 学术社交网络用户的隐私保护研究——以科学网博客为例［J］. 情报学报，2019，38（7）：667-674.

（责任编辑：杨丰侨）