Open Journal of Legal Science 法学, 2024, 12(9), 5586-5593
Published Online September 2024 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2024.129796

Hans汉斯

网络公共场所私密信息的界定与司法保护

徐梦婷

武汉大学法学院，湖北 武汉

收稿日期：2024年8月5日；录用日期：2024年8月15日；发布日期：2024年9月11日

摘　要

在互联网时代，物理空间的隐私侵权问题逐渐延伸到网络空间，随着对传统上“公共场所无隐私”理论的打破，网络公共场所隐私的界定也逐渐为学界所关注。在《民法典》将个人信息权益和隐私权两者区分的二元保护路径下，作为交叉地带的私密信息适用隐私权规则保护，这也引起司法实践中对私密信息的界定和保护难题。“场景一致理论”在承认信息流动中风险存在的前提下，采用独特的风险评估方法对个人信息流动每个阶段的隐私进行预测。立足在网络环境中场景不断变化的情况下，尽可能降低信息流动中造成的隐私风险。

关键词

网络公共场所，私密信息，场景一致性理论

The Definition and Judicial Protection of Private Information in Network Public Places

Mengting Xu

School of Law, Wuhan University, Wuhan Hubei

Received: Aug. 5th, 2024; accepted: Aug. 15th, 2024; published: Sep. 11th, 2024

Abstract

In the Internet era, the issue of privacy infringement in physical space has gradually extended to cyberspace. With the breaking of the traditional theory of “no privacy in public places,” the definition of privacy in online public places has gradually attracted the attention of the academic community. Under the dual protection path of the *Civil Code* that distinguishes the rights and interests of personal information from the right to privacy, the privacy rules are applied to the protection of

文章引用：徐梦婷. 网络公共场所私密信息的界定与司法保护[J]. 法学, 2024, 12(9): 5586-5593.
DOI: 10.12677/ojls.2024.129796

private information as a cross-zone, which also causes the definition and protection of private information in judicial practice. On the premise of acknowledging the existence of risks in information flow, the "Contextual Integrity" uses a unique risk assessment method to predict the privacy of each stage of personal information flow. Based on the changing scene in the network environment, the privacy risk caused by information flow should be reduced as much as possible.

Keywords

Network Public Places, Private Information, Contextual Integrity

1. 引言

基于现代公共管理技术的发展，公共场所中监控和追踪技术记录下人们的一举一动，就此引发了个人在公共场所隐私权被侵犯的现象。然而这一现象伴随着互联网技术的迅速发展，扩展了人们在现实生活中的空间。以往以私人领域和公共领域区分的二分法无法适应网络场景的多样性，因此也引发了在网络空间公共场所中如何对个人隐私进行保护的思考。《中华人民共和国民法典》(简称《民法典》)中规定了个人信息的保护，区别于《民法总则》之前将个人信息适用关于隐私权保护的模式，体现出立法者意识到个人信息保护的价值和重要性。其中，《民法典》第一千零三十四条第三款规定："个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。"由此可知该条款中对私密信息适用隐私权规则保护，私密信息成为隐私权和个人信息保护二元区分保护模式下的交叉地带。面对该立法现状，司法实践中产生了对私密信息概念的界定和认定的难题。

在网络空间中，个人信息一旦产生就会面临被不合理收集和利用的风险。且网络空间的去中心化趋势，很难单独地来对单个数据进行分析，信息主体和信息接收者都已经意识到，当少量数据进行组合时可能会发生质变，孤立的信息可能不会呈现出实质内容，但进行整合后，可能会造成信息的彻底泄露。知道一个人的职业、邮政编码、教育水平及大学毕业院校，就可以高度肯定地推断出他的收入水平，刻画出他的人格画像。对于聚合性信息的隐私风险预测和保护在如今具有很重要的意义，在司法实践中也不乏数据处理者(通常是企业)侵犯个人信息的案例，其中已经呈现出可能对个人隐私侵害的趋势。因此对个人信息中私密信息的认定成为人们在面对上述情况下对自己隐私保护的主要依据，本文将分析关于私密信息纠纷的案例，探求在司法实践中认定私密信息的判断标准，同时为网络公共场所中不同场景下个人隐私的保护提供思路。

2. 网络公共场所中私密信息的特征

(一) 作为"新型公共场所"的网络空间

网络空间提出的公共场所，与之相对应的是传统物理空间的公共场所。一般认为，物理公共场所是指任何人都可以自由进入和离开的地方。例如公园、广场、车站、街道等。只要是人们能够不受限制地进入和活动的空间，就可以被视为公共场所。公共场所的资源和设施是开放共享的，不具有排他性，不会对进入者设置专门的限制或者门槛。任何人，无论其身份、地位或背景，都可以自由进入并使用这些场所。这些特征使得公共场所区别于私人场所或限制进入的专用场所。网络作为人际交往的重要媒介，

已经成为现实生活的重要组成部分。这使得以往根据身体能否进入来判断公共场所的标准已经逐渐被打破([1], pp. 91-93)，如在“方某等开设赌场”案件中，法院经审理后认为，被告以营利为目的，利用手机在网络上建立“微信群”的方式，开设赌场从中获利，情节严重，其行为均已构成开设赌场罪。

2013 年 9 月 9 日最高人民法院和最高人民检察院公布的《关于办理利用信息网络实施诽谤等刑事案件使用法律若干问题的解释》中[1]，将网络空间包含在“诽谤罪”和“寻衅滋事罪”认定的“公共场所”范围中。可见，网络空间作为现实世界的延伸，将网络空间视为“新型公共场所”并没有超过国民预测的可能性([1], p. 91)。

(二) 网络公共场所中私密信息的特征

1) 信息隐私化

对于隐私概念的探讨，不同地域、不同国家基于不同的文化都有不同的理解。隐私观念早就存在，在物理空间中通过围墙、住宅相隔就能得以保护的亲密关系是最初隐私权保护的客体。张新宝教授指出，“知羞耻”“掩外阴”的心态是人类认识隐私的开端[2]。目前通说为《民法典》对隐私的定义：“隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。”以“不愿为他人知晓”可以看出，民法典规定的是一种消极不受侵扰的隐私权，也是一种以“隐”为核心的隐私界定[3]。但随着互联网的发展，人类如今进入大数据时代，隐私的传播范围也逐渐从物理空间扩展到了网络空间。原本在物理空间的公共场所公开的信息不属于隐私范畴，但转化为网络空间公共场所后就很有可能成为私密信息。例如基于现代公共监控技术的发展，人脸识别已经能精准地识别一个人的身份信息，一般现实场景中人脸都是公开的，并不属于隐私范畴，但人脸识别可以使这种信息成为私密信息。传统物理空间中定义的隐私范畴已经不能完全适用于网络公共场所中，信息隐私化使得隐私界限在不断拓宽。

2) 整合性

在现实空间，公共场所能够很轻易地根据物理空间的分隔而辨别出来，一墙之隔可以将公共领域和私人领域区分出来。但是在网络空间，借助网络传播平台，人们公开个人信息，这使公与私的边界变得模糊，逐渐出现了私人领域公共化的现象。在进入大数据时代之前，人们的隐私主要以生物隐私的方式存在，隐私主体可以通过对自己隐私可感可知的方式来主动掌握，了解其所处的状态。进入大数据时代后，整合型隐私作为一种公民隐私的新类型开始出现并不断增加[4]。它基于大数据而产生，与生物隐私相比较，具有隐形性、多样性、可变性等多种特征。而在对公民的伤害方面，则具有“无感伤害”的特征，数据公司不当收集和使用用户信息从而侵犯隐私并不是不存在，而是隐私主体没有及时感知，导致伤害具有滞后性。对整合型隐私的伤害不仅仅表现为隐私主体在短期内“无感”，有时还不断主动提供伤害的资源——持续提供数据信息以促使隐私主体接受个性化服务。由此，“隐私悖论”成为每个现代社会成员深陷其中的一个困局。由于进入数字化社会，社交媒体也始终大力倡导用户进行内容的创作、分享和协作，人们尽管有着自己隐私可能受到侵犯的担忧，却又不断地公开个人信息甚至私密信息。

3) 价值双重性

从根本上来说，个人信息权益和隐私权都体现了立法者保护人格尊严和个人自由的价值取向。但从两者法律属性上讲，个人信息权益和隐私权保护的客体也有不同，个人信息未上升为权利，保护的客体是信息的合理利用和流通，体现的价值是财产利益和精神利益。隐私权是绝对权，保护的客体是人格尊严，体现的主要是精神利益。这就意味着，隐私权，其实也是指传统的隐私权，具有完全的至少是更强烈的人格尊严性，而个人信息则同时具有尊严性和资源性的双重价值([5], p. 66)。私密信息首先属于个人信息，在此基础上具备“隐私利益”，这一标准区分出私密信息和非私密信息。在司法实践中检验私密信

[1]参见浙江省丽水市莲都区人民法院(2015)丽莲刑初字第 799 号刑事判决书；浙江省丽水市中级人民法院(2015)浙丽刑终字第 254 号刑事判决书。

息，司法机关必须做出判断，所涉案件的个人信息到底是跟当事人人格尊严有关，还是仅具有流通价值。

3. 司法实践中网络公共场所私密信息的定性难题

“公共场所无隐私”的规则最初是由《论隐私权》一文中提出的，普罗瑟教授认为，人们身处公共街道或公共场所时，是不享有独处权的，构成侵犯隐私权的情形，应当侵犯私人性质的事务，这个范围不包括侵扰他人私人事务、私人场所、或者私人内容。他的观点得到了美国法院的采纳和支持，除此之外，他还在美国的隐私侵权责任制度中确立了公共场所无隐私的一般规则([6], pp. 351-352)。1967 年，美国联邦最高法院在 Katz v.United States 一案([6], pp. 351-352)中提出了合理的隐私期待理论之后，“公共场所无隐私”观点暴露出他的不足之处。之前以“场所”用来判断公民是否拥有隐私权的单一模式被打破，只要个人主动隐瞒自己的行为，不愿将更多信息与他人分享，即使他身在公共场所，法律也应该保护其隐私权不被侵犯。近年来，网络公共场所中隐私侵权案件频发，关于私密信息的争议主要来源于信息处理者与信息主体之间关于个人信息的案件纠纷。信息处理者利用信息处理技术处理和传输个人信息，在此过程中是否侵犯私密信息是争议的中心。基于私密信息的交叉地位，对私密信息的检验意味着将适用不同的法律规则，产生不同的法律效果。因此，司法实践中对私密信息的检验至关重要，但关于私密信息的检验标准并没有明文规定，在实践中也存在着不同的判断方法，产生诸多问题。

(一) 网络公共场所中私密信息难以检验

在“黄某诉腾讯科技(深圳)有限公司等隐私权、个人信息权益网络侵权责任纠纷案”(以下简称微信读书案)中，原告认为微信读书软件在未获得本人授权的情况下，自动关注微信好友并向其展示自己读书信息侵犯了自己的个人信息权益和隐私权。在判决理由中，法院逐一分析了微信好友关系、读书信息是否属于个人信息和隐私，以及微信读书软件利用这两个信息使得关注好友可以查看原告读书信息是否构成原告个人信息权益或隐私权的侵害[2]。另外，在“王某某诉青岛天一精英人才培训学校隐私权纠纷案”(以下简称司考成绩案)中，原告认为培训学校通过互联网公开其考试成绩用于广告宣传的行为侵犯了自己的隐私权[3]。这两个案例中，都是个人信息在网络公共场所公开而产生隐私权纠纷问题。在微信读书案中，法官判断个人信息私密性时提出两点：一是要对个人信息进行合理的层级划分，划入隐私的个人信息，应强调其“私密性”，对于不具有“私密性”的个人信息可以依法合理利用以促进互联网发展；二是，关于“私密性”的检验不应完全取决于个人意志，而应符合社会一般合理认知；三是要结合社会背景，在尊重用户的差异性下探讨是否侵害隐私的行为。司考成绩案中二审法院也认为隐私的范围，应该以社会普通大众对隐私的认识为评判标准，而非原告主观的个人标准。以上两个案例的判决结果都认为涉案信息并没有涉及侵犯隐私权问题，仅侵犯原告的个人信息权益。然而对于所提到的“社会普通大众对隐私的认识”并没有一个明确的标准，在实践中法官成为了决定个人信息是否具有私密性的宣判者。在承认是个人信息的同时，以信息不具有私密性的以果寻因的主观判断方法来认定所涉信息不属于私密信息，具有强烈的主观价值判断色彩，这种做法将导致陷入私密信息检验的混乱局面。

产生个人信息私密性检验的难题，追根溯源是因为《民法典》时代后赋予司法机关进行个人信息“私密性检验”的义务。关于个人信息与隐私权保护的问题最初起源于《民法总则》第 110 条和第 111 条的体系性结构[7]，隐私权和个人信息保护处于民法总则的不同条款，已经体现出立法者将两者区分保护的趋势。在《民法总则》此项规定之前，还没有关于个人信息保护的独立规范，对个人信息的保护主要适用隐私权规范，因此也就不存在个人信息保护是否独立于隐私权的问题。司法实践中也主要是将个人信息适用隐私权规则予以保护[8]，如“庞某诉中国东方航空股份有限公司、北京趣拿信息技术有限公司隐

[2]参见北京互联网法院(2019)京 0491 民初 16142 号。

[3]参见山东省青岛市中级人民法院(2019)鲁 02 终 7482 号。

私权纠纷案”中，并没有明确区分个人信息和隐私权的界限，而是直接将涉案的个人信息适用隐私权予以保护。在《民法典》中的“隐私权和个人信息保护”章节题目可以看出此时已经显示对二者区分保护的模式。其中作为二者交叉领域的“私密信息”单独规定适用条款，即个人信息中的私密信息优先适用隐私权的保护。没有规定的，适用有关个人信息保护的规定。《民法典》第1032、第1034条中关于个人信息保护的硬约束条款是《民法总则》中所没有的。这个规范是典型的裁判规范，作为对司法机关具有直接和刚性约束力的裁判规范，意味着对司法机关的裁判行为的硬约束([5], p. 64)。其中第1034条第三款中引发了关于对私密信息和非私密信息相区分的问题，在司法实践中体现为法官需要在具体案件的裁判中对个人信息是否可能被认定为私密信息进行判断，才能最终确定适用的规范。

(二) 忽略网络公共场所聚合信息的隐私风险

网络公共场所中私密信息的整合性特征是区别于现实公共场所隐私的一个重要特征。信息数字化会使得原本不会留痕的即时沟通，可随时随地通过数字方式留下痕迹，并传播到网络等公共空间[9]。孤立地分析互联网上个人的上网痕迹必然是不具有私密属性，但在信息时代几乎不可能出现单一收集和处理个人信息的情况，聚合型信息可以反映出信息主体的学历、工作、爱好，从而刻画出人格画像。况且网络空间的信息处理者也是把个人信息作为整体来进行收集和处理，因此“个人信息”这一概念本身就是信息集合体，孤立看待个人信息是对个人信息定义的误读。在“微信读书案”中，逐一分析所涉信息以及收集和处理信息行为是否侵犯隐私权，对每一种都得出仅侵犯个人信息权益而不涉及隐私侵犯的结论。采用同种方式的还有“抖音APP”案，法院逐一分析涉案信息中姓名、手机号、社交关系、地理位置是否属于个人信息和隐私[4]。但也有司法实践表明对聚合性信息的隐私风险的重视，例如在庞某诉中国东方航空股份有限公司、北京趣拿信息技术有限公司隐私权纠纷案中，法院认为单纯的姓名和手机号码不构成隐私信息，但结合行程信息后，整体也包含了隐私信息而成为隐私信息，最后判决被告侵犯原告的隐私权[5]。收集和处理个人信息是把信息作为整体，但在检验个人信息时却要逐一分析单个个人信息是否属于个人信息和隐私。此种情形表明，司法实践中对聚合性信息的隐私风险意识有待进一步加强，将涉案信息作为一个整体来看而不是逐一分析更能适应如今数字社会的发展。

(三) 隐私权规则的优先适用加重信息主体的证明负担

对于私密信息应优先使用隐私权规则来进行保护，前提是在立法上普遍认为隐私权对私密信息的保护程度更高。另外，也是基于权利不得减损原则和人格尊严高于私法自治的保护原则两个方面的考虑[10]。但从对私密信息进行事后保护的方式来看，可能会出现背离实体法设定原则的情况。私密信息的事后保护方式是规定信息处理者承担侵权损害赔偿责任，但观察个人信息保护规则的侵权责任原则可以发现两者存在的矛盾之处。《民法典》第1034条第三款的规定，对私密信息的保护将引致到《民法典》第1165条第一款的规定，在侵权责任的构成要件上遵循的是隐私权保护中的过错责任原则，如果以隐私权受到侵害主张对方承担侵权责任，信息主体需要证明对方的过错。然而《个人信息保护法》第69条第1款规定的确是过错推定原则，如果以个人信息权益受到侵害为由要求对方承担侵权责任，信息主体并不需要证明对方过错。因此我们可以发现存在的问题：私密信息的保护适用我们认为的保护力度更强的隐私权规则，但是在对私密信息进行事后救济时，隐私权规则的侵权责任构成要件须遵循过错原则，而个人信息保护规则适用的是过错推定原则。这一对比，可以发现适用个人信息权益保护法规则显然对私密信息的保护程度是更高的，在侵权的构成要件上也会大大减轻信息主体的证明负担。为了克服对私密信息进行保护时的法条竞合弊端，学界提出了诸多解决办法，有学者提出应删除第1034条第3款中关于“私密信息”的规定，以减少司法实践中对不同概念的区分[11]。此外，还有学者提出实体法上限缩适用的解释

[4]参见北京互联网法院(2019)京0491民初6694号。

[5]参见北京市第一中级人民法院(2017)京01民终509号。

方式[12]，分别调整适用隐私权规则和个人信息保护规则的私密信息范围来解决法条竞合问题。可见第1034条第3款在适应隐私权和个人信息权益区分保护模式的同时，又带来了新的适用难题，这也正是我们需要进一步完善的问题。

4. 网络公共场所私密信息检验中“场景一致性理论”的引入和司法对策

随着在网络公共场所中个人信息的利用和处理方式越来越复杂和频繁，传统的以公开与否来界定隐私的方式逐渐被质疑，学者和立法者急需一种更为灵活的检验私密信息的方式。“场景一致性理论”由此被人们所关注并应用到司法实践中，有学者也称之为情景脉络完整性理论[13]、场景化标准[14]等。为避免引起歧义，本文采用“场景一致性理论”来进行表述。在有关个人信息权益纠纷案件中，场景一致性理论提出的检验标准成为司法实践中对个人信息的私密信息检验的热门标准。本部分就“场景一致性理论”所提出的检验标准进行分析并对比我国司法实践的具体应用，进而在司法实践中进一步完善该理论的适用方式。

(一) 美国“场景一致性理论”与我国司法中的场景化模式

“场景一致性理论”是由美国学者海伦·尼森鲍姆提出，她并不致力于在复杂网络环境中塑造一个能普遍适用的隐私规则。身处于去中心化的互联网空间，信息在不同平台之间进行流动是不可避免地，而隐私是对信息流动的限制。她强调了信息流动应该符合特定场景中的规则和期望，而不是简单地看作信息的绝对控制权。该理论认为隐私保护应该考虑场景因素，并提供了一个评估信息流动合理性的框架[15]。“场景一致性理论”的核心构架是场景相关的信息规范，其中有四个关键要素：场景、行为主体、属性和传输原则([16], pp. 119-144)。要素发生变化时，信息流动的性质就会有所不同，因此判断是否侵犯隐私需要结合每个因素进行判断。该理论一经诞生就受到美国隐私立法者关注，最典型的是《消费者隐私权利法案(草案)》(Consumer Privacy Bill of Rights Act of 2015，简称CPBR)，其中专设“尊重场景”一节来进行描述，且透明度、控制性规则都必须根据具体场景的要求进行适用[17]。另外，在欧盟《通用数据保护条例》(General Data Protection Regulation，简称GDPR)中，该理论也被用来证明具体规则的合理性和有效性[18]。

在国内，司法机关也引入“场景一致性理论”，在不同场景下综合各种因素来判断是否违反信息流动的规则也被司法机关纳入考量依据。如微信读书案中法官采用的“场景化模式”，来对腾讯公司收集和处理信息的行为进行私密性检验[6]。在原告孙某某与被告北京百度网讯科技有限公司人格权纠纷案中，司法机关也有同样的表述：即“结合法律规定的认定标准，一般社会大众的普遍认知，以及信息的具体运用场景综合进行判断”[7]。可见，目前场景化模式成为检验私密信息的热门标准。有学者也指出，场景化模式并不是检验私密信息的合理标准，与民法典时代前的隐私权保护案例中的裁判思路其实并无二致[19]。究其原因，是因为“场景一致性理论”本身就比其他隐私理论复杂，难以在短时间内见效，需要在实践中进一步完善。但该理论提供了一个积极的隐私概念，给出了解决隐私问题的正确方向，具有重要的理论和实践价值。

(二) 网络公共场所中私密信息检验的具体展开

网络空间信息流动场景日益复杂多变，美国和欧盟逐渐摒弃“公开即无隐私”的绝对化隐私判断标准，转为采取更加灵活的“具体场景动态判断”的相对实质标准。我国学界对隐私信息的判断趋势也与之类似，呈现出从物理空间的公开与私密到关注信息内容私密与否的路径。因此，应借鉴场景一致性理论，立足我国司法实践，采用实质标准来检验私密信息。

[6]参见北京互联网法院(2019)京0491民初16142号。
[7]参见北京互联网法院(2019)京0491民初10989号。

1) 识别行为主体的特定关系

场景一致性理论指出，行为主体又分为信息主体、信息发送者和信息接收者([16], pp. 119-144)。在判断网络公共场所的个人信息是否具备私密性，应该基于行为主体之间的特定关系来决定。人们认为该信息是私密的，私密信息实际上是指对于特定主体来讲具有私密性。通常而言，当我们意识到自己的信息被分享时，我们介意的有可能不是信息被分享了，而是信息以错误的方式、向不适当的人分享了。在网络公共场所中，权利人基于事实行为而与他人形成的陌生关系，有助于个人展示个性与维持陌生领域的舒适性，在这种场景下，人们更加关注的是个人信息的匿名性。例如在微信读书案中，原告的诉求体现了并不希望好友知晓自己的读书信息，实质上也是要求个人信息匿名化，以追求在读书场景下的自由空间。另外，在朱某诉北京百度网讯科技公司隐私权纠纷案中，法院认为网络精准广告中使用 cookie 技术收集、利用的匿名网络偏好信息虽具有隐私属性，但不能与网络用户个人身份对应识别，网络服务提供者和社会公众无法确定该偏好信息的归属主体，不符合个人隐私和个人信息的‘可识别性’要求，因而该行为不构成侵犯隐私权[8]。因此，这个环节需要确定新的信息处理方法是否改变了信息主体、信息发送者和信息接收者。

2) 识别受影响的信息性质

另一个同样重要的要素是信息的性质：不仅是关于谁、分享给谁以及由谁分享，而是关于信息是什么。场景一致性理论将信息的属性、类型或性质作为信息规范中的另一个关键要素。某些属性的信息在不同场景中传输是否恰当是由信息规范决定的，比如在就医场景中，医生询问病人的身体状况是合理的，但是在工作场景中，老板这么做却是不恰当的(当然也有例外，如职业足球队教练询问球员的心脏状况)。因此，这个环节需要确定信息处理方式是否影响从信息发送方到信息接收方传输的信息类型。例如使用微信读书 app 阅读，不仅可以展示自己所读书籍名称，而且还能记录下所读时间。

3) 识别传输原则的改变

场景一致性理论框架中最显著的因素是传输原则，该原则限制场景中的信息流动，表明了某类信息能否进行传输的条件。其中最显而易见的是保密，规定接收信息的一方不得与他人共享信息，其他还有互惠、奖励、授权等等([16], pp. 119-144)。例如在医疗场景中，医生对获取的患者健康信息应该保密。因此，这个环节需要判断将个人信息从一方传输到另一方是否违背该场景的传输原则。如前述的微信读书案中，对于原告主张被告获取微信好友列表这一行为，其中传输原则是信息接收者和处理者的微信读书，应当在收集用户微信好友列表信息时获得信息主体的同意，该案中符合此传输原则，因而符合在线电子阅读场景下的信息规范。相反，对于被告公开原告所读书籍信息这一行为，此行为包含的传输原则是微信读书 app 作为信息的接收方应该负有对信息的安全保障义务，即若处理、传输具有较高风险的个人信息时，信息处理者应该对其处理行为对信息主体进行显著说明并获得同意。但是该案中微信读书 app 并没有遵循这一传输原则，所以该案中读书信息流动不合理，被告的行为构成侵权。

(三) 降低信息主体对过错要件的证明责任

如前所述，目前对私密信息主体的证明标准存在争议。在网络公共场所中，信息主体(信息发送者)和信息接收者通常处于一种处理信息技术不对等的状态，特别是当信息发送者和接收者是多个个人、甚至组织等集体时，对于信息主体来说，根本无法提供证据证明个人信息处理者在处理活动中有什么过错[20]。在庞某某诉东航公司、趣拿公司隐私权纠纷案[9]中，庞某根据诈骗信息可以证明自己的隐私权遭到侵害，但却无法确切地知晓侵权主体和证明其过错。审理法院采用事实推定的方法推定趣拿公司和东航侵害庞某的隐私权，这一事例表明在信息主体只能提出相应的初步证据下，法院可以根据该证据依照经验法则

[8]参见江苏省南京市中级人民法院(2014)宁民终字第 5028 号。

[9]参见北京市第一中级人民法院(2017)京 01 民终 509 号民事判决书。

来对侵害私密信息的情节形成高度确信，以降低信息主体处于信息不对等情况下的证明责任。在对私密信息进行保护出现法条竞合的情况下，采用降低信息主体证明责任的方法能够有效缓和司法实践中的冲突，更好地维护信息主体权益。

5. 结语

在网络公共场所中，对私密信息的定性与保护是一个复杂且不断发展的领域。基于《民法典》对私密信息的保护规则，但并没有明确指出私密信息的界定标准，面对信息隐私化、信息整合性和价值双重性的挑战，在实践中产生了私密信息界定的分歧。为了适应这一立法背景，需要在司法实践中引入对私密信息判断的新方法。场景一致性理论产生的背景正是为了应对互联网信息技术高速发展带来隐私侵害的风险，它提供了一个应对隐私风险挑战的正确方向。但对该理论的应用目前在我国仍处于初始阶段，要对其进行本土化改造和运用也需要各领域的专门知识和实证研究，需要在实践中不断的完善，以应对现代网络社会中复杂的隐私挑战。

参考文献

[1] 卢勤忠, 钟菁. 网络公共场所的教义学分析[J]. 法学, 2018(12): 91-105.

[2] 张新宝. 隐私权的法律保护[M]. 北京: 群众出版社, 2004: 13.

[3] 王秀哲. “隐”与“私”流变中的信息隐私权[J]. 河北法学, 2022, 40(11): 46-71.

[4] [美]伊莱·帕里泽. 过滤泡——互联网对我们的隐秘操纵[M]. 方师师, 杨媛, 译. 北京: 中国人民大学出版社, 2020: 3.

[5] 张建文. 在尊严性和资源性之间:《民法典》时代个人信息私密性检验难题[J]. 苏州大学学报(社会科学版), 2021, 42(1): 62-72.

[6] 张民安. 公共场所隐私权研究[M]. 广州: 中山大学出版社, 2016.

[7] 张建文, 高悦. 从隐私权的立法与司法实践看新兴权利保护的综合方式[J]. 求是学刊, 2019, 46(6): 102-111.

[8] 中华人民共和国最高人民法院. 中国法院的互联网司法[M]. 北京: 人民法院出版社, 2019.

[9] 李忠夏. 数字时代隐私权的宪法建构[J]. 华东政法大学学报, 2021, 24(3): 42-54.

[10] 王利明. 和而不同: 隐私权与个人信息的规则界分和适用[J]. 法学评论, 2021, 39(2): 15-24.

[11] 姬蕾蕾. 私密信息界定的司法困境及其破解方向[J]. 上海大学学报(社会科学版), 2022, 39(6): 94-108.

[12] 张建文, 时诚. 《个人信息保护法》视野下隐私权与个人信息权益的相互关系——以私密信息的法律适用为中心[J]. 苏州大学学报(社会科学版), 2022, 43(2): 46-57.

[13] 倪蕴帷. 隐私权在美国法中的理论演进与概念重构——基于情境脉络完整性理论的分析及其对中国法的启示[J]. 政治与法律, 2019(10): 149-161.

[14] 张建文. 危险的场景化标准:私密信息私密性检验的实践批判[J]. 数字法治评论, 2022(1): 61-76.

[15] Nissenbaum, H. (2004) Privacy as Contextual Integrity. *Washington Law Review*, **79**, 119-158.

[16] [美]海伦·尼森鲍姆, 著. 场景中的隐私——技术、政治和社会生活中的和谐[M]. 王宛, 等, 译. 北京: 法律出版社, 2022.

[17] Consumer Privacy Bill of Rights Act of 2015, Sec. 4, Sec. 103-104.

[18] Guinchard, A. (2018) Taking Proportionality Seriously: The Use of Contextual Integrity for a More Informed and Transparent Analysis in EU Data Protection Law. *European Law Journal*, **24**, 434-457. https://doi.org/10.1111/eulj.12273

[19] 谷兆阳. 论“场景理论”不是私密信息判断的合理标准[J]. 科技与法律, 2022(4): 83-93, 104.

[20] 程啸. 侵害个人信息权益的侵权责任[J]. 中国法律评论, 2021(5): 59-69.