·专栏：信息管理实证研究重要理论的研究应用及其展望（十一）·

# 威慑理论及其在信息系统研究领域的应用与展望

吴 迪 袁勤俭*
（南京大学信息管理学院，江苏 南京 210023）

**摘 要**：［目的/意义］旨在帮助学术界深入理解威慑理论在信息系统领域中的应用与进展，从而为未来该理论在相关领域的研究提供思路和方向。［方法/过程］本文系统地梳理并评述了国内外关于威慑理论在信息系统领域的应用的研究文献，总结了研究取得的进展和不足之处。［结果/结论］威慑理论在信息系统领域内的应用成果主要集中在“威慑理论在信息系统安全研究中的应用”“威慑理论在数字盗版行为研究中的应用”和“威慑理论在在线社交媒体偏差行为研究中的应用”这 3 个方面；研究中存在“惩罚的敏捷性视角研究不足”“缺少跨国家（地区）、跨文化和跨平台的横向比较差异研究”等问题。

**关键词**：威慑理论；信息系统；惩罚；犯罪行为；信息安全策略
DOI：10.3969/j.issn.1008-0821.2024.07.014
〔中图分类号〕G202；TP39 〔文献标识码〕A 〔文章编号〕1008-0821（2024）07-0155-08

# Deterrence Theory and Its Application and Outlook in the Field of Information Systems Research

Wu Di Yuan Qinjian*
（School of Information Management，Nanjing University，Nanjing 210023，China）

**Abstract**：［Purpose/Significance］It aims to help academics gain a deeper understanding of the application and progress of deterrence theory in the field of information systems，so as to provide ideas and directions for future research on the theory in related fields.［Methodology/Process］This paper systematically sorted out and reviewed the domestic and international research literature on the application of deterrence theory in the field of information systems，and summarized the progress and shortcomings made in the research.［Results/Conclusions］The results of the application of deterrence theory in the field of information system mainly focus on “the application of deterrence theory in the study of information system security”，“the application of deterrence theory in the study of digital piracy” and “the application of deterrence theory in the study of online piracy”. The application of deterrence theory in the study of online social media deviant behaviors”；there are problems such as “insufficient research on the agility perspective of punishment”，“lack of cross-country，cross-cultural and cross-platform comparative differences”，etc.；the application of deterrence theory in the study of information system security”，“application of deterrence theory in the study of digital piracy” and “application of deterrence theory in the study of online social media deviant behaviors”. There are problems such as “insufficient research on the perspective of punishment” and “lack of cross-cultural and cross-platform comparative research”.

**Key words**：deterrence theory；information system；punishment；criminal behavior；information security policy

收稿日期：2024-04-01
基金项目：江苏省高校社会科学研究重大项目“集成超越推动江苏数字经济高质量发展对策研究”（项目编号：2021SJZDA043）；江苏省文化和旅游科研重点课题“新时代我省智慧旅游高质量发展路径研究”（项目编号：22ZD04）；南京大学新时代文科卓越研究计划“中长期研究专项”课题“数字化转型的实践逻辑与理论创新研究”。
作者简介：吴迪（1999-），女，硕士研究生，研究方向：政府数据开放、国家安全。
通信作者：袁勤俭（1969-），男，教授，博士，博士生导师，研究方向：电子商务与信息经济。

1763 年，意大利法理学家切萨雷·贝卡里亚(Cesare Beccaria)在《论犯罪与刑罚》一书中首次提出了威慑理论(Deterrence Theory)，其核心思想是：人是理性的，当人认识到不利行为被发现的风险较高，可能面临即时而严厉的惩罚，并且预期的惩罚会超过可能带来的利益时，就会放弃实施这一行为。

鉴于威慑理论在阻止不利行为方面的应用价值，越来越多的学者利用这一理论研究如何通过惩罚来影响决策过程。因此，部分学者已经对这些研究成果进行了述评：宋艳锴等[1]以刑罚的威慑效果为研究基点，对先行学者在法经济学框架下对刑罚的分析进行了全面综述，提出未来的刑罚政策制定不应仅仅局限于成本与收益的单一考量，而应扩展视角，更为深入地考虑到社会安全、公平正义以及公众参与等多维度的核心价值要素。此外，D'Arcy J 等[2]专门归纳了信息安全领域内威慑理论的应用情况，并指出在应用威慑理论时，自控力、道德信念等不同的变量因素以及研究方法的差异，可能导致威慑效果的不一致性。

由前述可知，现有综述性文献只研究了威慑理论在信息安全领域的应用，但除了信息安全领域，威慑理论还被应用于诸如数字盗版行为、在线社交媒体中偏差行为等问题的研究中。然而，在文献调研中未发现系统性地评述威慑理论在整个信息系统领域应用的文献。因此，本研究在简要介绍威慑理论的源起和发展之后，将重点梳理并阐述该理论在信息系统领域的应用现状，并在此基础上归纳出当前信息系统领域威慑理论应用研究存在的不足和未来研究的方向，以帮助研究人员了解威慑理论在信息系统研究领域的应用进展。

## 1 威慑理论起源与演化

### 1.1 威慑理论的起源

早期的刑罚理论主要是基于传统的报复性原则，有可能导致刑罚的过分严酷，因此需要一种合理且公平的刑罚理论。贝卡里亚受到启蒙时期人文主义提倡理性、人权和经典自由主义强调法律面前人人平等的影响，同时吸收了新古典经济学派“人是理性的”的思想，研究如何通过设计威慑机制来有效地预防犯罪。

1763 年，贝卡里亚[3]在《论犯罪与刑罚》一书中提出了威慑理论。该书阐述了惩罚的三大基本原则——确定性(Certainty)、敏捷性(Celerity)和严厉性(Severity)，并强调这些要素对于确保威慑的有效性的不可或缺。其中，确定性意味着必须确保人们能够预见犯罪的后果，从而在犯罪行为之前进行风险评估；敏捷性强调犯罪行为与随之而来的惩罚之间的时间间隔应尽可能短，以增强刑罚的警示效果；严厉性要求惩罚的严厉程度不仅需超过犯罪带来的潜在利益，而且还需要与犯罪的严重性相匹配。

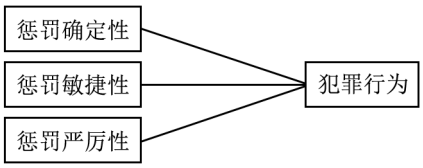


**图 1 威慑理论模型**

**Fig. 1 Deterrence theory Model**

### 1.2 威慑理论的演化

#### 1.2.1 融合非理性因素，丰富威慑效应的多元视角

贝卡里亚以“理性人”为假设构建了刑罚威慑理论，但这一假设忽略了复杂的人类行为动机和社会、文化等因素。为了弥补这一不足，Pratt T C 等[4]提出了“非法律威慑”对非理性因素进行补充，其中的“非正式威慑”主要依赖于社会规范和公众舆论对个人行为的影响；“羞愧威慑”则考虑了道德与羞耻的威慑力，使罪犯的行为公之于众，激发个人的羞愧感和愧疚感并对其自尊心造成冲击。研究表明，羞愧威慑能显著地减少人们犯罪的倾向，其效果能与正式或非正式制裁的影响力相比肩。此外，还有学者通过引入行为经济学的观点，认为个体决策中的过度自信、立即偏好、损失厌恶等认知偏差，可能影响犯罪者对犯罪收益和成本的判断，进而影响威慑效应。

#### 1.2.2 发展实证研究，强化威慑理论的科学验证

由于早期研究方法和实证技术的限制，贝卡里亚对威慑理论的探讨主要基于哲学思考和逻辑推理，而未经现代科学的严格验证。为进一步发展威慑理论，Becker G S[5]首次将经济学原理系统地应用于犯罪行为的分析，尤其是在《犯罪与惩罚：一个经

济学方法》中，他分析了犯罪行为的经济回报与法律制裁之间的权衡，并用实证数据测试了罚款和监禁对减少犯罪的效果。在 Becker G S[5]之后，其他学者也对威慑理论提供了显著的实证支持。例如，Levitt S D[6]的研究应用计量经济学工具来量化警力增加、监狱羁押率上升等因素对犯罪的制约效应，指出合理配置执法人员数量和监狱资源可以显著提高犯罪预防的效率。此外，Lee L[7]利用多年的横截面和时间序列数据，采用多种计量经济方法，验证了增加警力不仅可以直接威慑犯罪，还可能通过提高犯罪侦破率，产生间接的预防效果。通过对不同国家(地区)、不同类型犯罪的大量实证分析，这些学者证明了威慑理论在现代社会治安管理中的适用性和有效性，为政策制定者提供了关键的数据支持及政策建议，同时开创了利用现代计量方法来评估犯罪预防政策的新范式。

1.2.3 完善群体差异威慑，促进威慑策略的精准应用

不同群体对威慑的反应可能不同，但贝卡里亚在提出威慑理论概念时并没有明确区分不同个体或群体。为此，边沁[8]首次将刑罚的目的划分为“一般预防”和“特殊预防”，他认为刑罚不仅应该防止特定个体再次犯罪(特殊预防)，还应该通过展示对犯罪行为的惩罚，警示社会其他成员，防止他们仿效犯罪行为(一般预防)。这两种方式共同构成了一个更为全面和细致的威慑预防体系，更有效地应对不同类型的犯罪行为和犯罪者。为了进一步细化和个性化威慑策略，还有学者提出了区别性威慑以补充上述两种方式，主张根据不同群体的特定行为模式、心理状态和社会背景来定制威慑措施，其核心在于认识到一种统一的威慑方法无法广泛适用于所有情况，强调在威慑政策设计中考虑人群差异，以增强法律干预的有效性和针对性[9]。

1.2.4 扩展应用领域，实现威慑理论与多学科融合

威慑理论的起源可追溯至犯罪学领域，并在犯罪学和法律研究上的应用最为广泛和深入，主要涉及刑罚政策的制定及执行策略、预防犯罪的方法设计等方面。考虑到威慑理论对规则形成的影响，学者们已经开始探索将其应用到解决经济学问题之中，将此理论扩展应用于诸如惩罚性赔偿[10]、财税政策[11]以及垄断行为分析[12]。威慑理论与经济学的结合不仅丰富了法经济学领域的研究内容，也引入了一种新的、有力的逻辑和分析工具，为法经济学的发展贡献了新的理论视角和分析框架。这种跨学科的融合为评估政策的经济效果提供了坚实的理论基础。随着威慑理论的内涵逐步丰富和体系越加完善，越来越多的学者探索了其在其他领域研究的应用。信息安全研究中以威慑理论为基础提出的网络威慑成为近年来的研究热点，其核心是通过建立和维护强大的网络防御能力以及威胁实施有效的报复措施，以防止或减少潜在的网络攻击行为。

## 2 威慑理论在信息系统领域的应用研究

### 2.1 威慑理论在信息系统安全研究中的应用

即便应用了高级安全技术和全面的物理防护，信息系统安全依然面临外部攻击的威胁，同时其也可能因内部员工的恶意行为或无意疏忽而面临风险。因此，不少学者以应用威慑理论来研究如何有效威慑潜在的攻击者和内部员工以保证信息系统安全性。

2.1.1 威慑理论在信息系统内部安全研究中的应用

在当今信息技术迅猛发展的背景下，企业面临着日益增长的信息安全挑战。为此，绝大多数企业都制定了详尽的信息安全策略(Information Security Policy，简称“ISP”)，旨在规范和减少员工在信息系统使用过程中的违规行为，进而保护企业的信息安全。在这一背景下，威慑被认为是影响员工遵从 ISP 行为决策的一个重要因素，许多学者从这一理论出发，探讨如何通过制定明确、具体的 ISP 以及配套的潜在惩罚措施来有效促进员工遵从 ISP。

在 ISP 遵从行为的研究中，一种观点认为制裁的严厉性和确定性对 ISP 遵从行为意图有显著影响。李瀛[13]从社会控制视角，建立员工信息安全违规意愿概念模型。研究发现，制裁严厉性对员工的信息安全违规意愿有显著的抑制作用，而制裁确定性的影响并不显著。王冬梅[14]根据 S-O-R 行为形成模型并且运用模糊 DEMATEL 方法，对各影响因素和因素间的作用机理进行了分析，也发现了感知制裁严重性会对违背意图产生显著影响。然而，另一些学者却认为，与正式制裁相比，非正式制裁的作

用更加显著。Hu Q 等[15]发现在企业环境中，相比于正式制裁，员工自身的道德观念和自我管控能力在阻止 ISP 违规行为方面表现得更为有效。类似地，陈琳[16]也发现，员工的自我效能信念、与个人相关结果预期对其遵从 ISP 的行为都有显著的影响，而感知惩罚的确定性对其 ISP 遵从行为的影响却不显著。

鉴于员工违反 ISP 的行为会给组织带来巨大损失，有学者基于正式制裁的作用提出了应对措施。Kankanhalli A 等[17]通过对各个经济部门的信息安全管理人员进行调查并建立了一个信息系统安全有效性的综合模型。研究发现，单纯提高威慑措施的严厉性并不会显著提升信息安全的有效性。据此，他们提出组织在保障信息安全时，应更多地关注如何综合运用威慑与预防措施，而非仅仅依赖于提高惩罚的严厉程度。Fan J 等[18]对上海 21 家政府机构中专门从事政务信息共享流程的人员进行了调查，根据调查数据分析，进一步指出政府机构可以采取包括信息安全策略、安全意识培训、预防性安全软件和安全监控实践等多种信息安全对策来减少内部员工的信息滥用行为。林润辉等[19]更是通过威慑理论和理性选择理论的整合视角提出了制裁确定性和严厉性会通过违反代价，比如扣除工资绩效等，提高信息安全策略遵从意向。除此之外，许多研究还加入了非正式制裁因素(如道德规范和羞耻感)。Siponen M 等[20]通过探讨策略、道德和个人情感驱动力等对信息安全策略研究的影响，认为结合非正式威慑以及羞愧等道德标准元素，在某一程度上也能有效地产生威慑效应。Merhi I M 等[21]也认为，道德规范和指令性规范有助于减少员工对信息安全策略的抵触情绪。

综上可知，尽管基于威慑理论的 ISP 遵从行为研究提供了有价值的洞见，但存在以下局限性：①由于员工 ISP 的实际遵从行为数据收集难度较大，大部分的研究把 ISP 的遵从意愿当作实际遵从行为的替代，较少有员工实际遵从行为的研究成果。未来的研究可以通过收集员工过去自报的网络使用记录或观察他们网络使用行为来直观地研究实际遵从行为；②大多数研究都集中于个体层面，探讨个体的动机、信念、知识、技能和态度等因素及其对 ISP 遵从性的影响。相比之下，组织层面的研究则相对缺乏。因此，未来的研究可以考虑从工作组或组织层次来研究团队内部互动、组织文化、策略和资源配置等对信息系统安全管理的影响；③上述研究将员工视为潜在的信息安全风险，并将防止与制裁组织内员工 ISP 的违背行为作为研究的重点，但这些研究没有认识到组织内部人员可以转变为安全盟友，也未深入探讨威慑因素如何影响员工积极参与保护组织信息系统的行为。

### 2.1.2 威慑理论在信息系统外部安全研究中的应用

信息系统可能会通过电子邮件感染病毒或因黑客攻击等方式而遭受各种入侵者的攻击，这对于信息系统的数据安全、网络安全等造成了极大威胁。这种威胁不仅限于特定的个体或组织，而是波及整个网络空间。因此，除了个体和组织采取威慑策略之外，国家和政府在应对这些问题、维护信息系统安全中的威慑作用显得十分关键。

个体或组织面对信息系统网络安全威胁时，需要采取一系列有效的威慑措施来保障系统的安全。根据 Straub D W 等[22]的研究，这些措施包括威慑的确定性、信息系统的安全工作、关于处罚的信息传播、可接受的系统使用规范和政策等。具体而言，威慑的确定性意味着必须确保潜在的攻击者明白，任何网络攻击行为都会受到快速而严格的回应。信息系统的安全工作强调了持续的技术维护和更新是必要的，这包括定期的安全审查和漏洞修补。关于处罚的信息传播是指向内部用户和外部威胁者明确传达违反网络安全规定将面临的后果，这种策略的目的是提高潜在侵犯者对被发现和惩罚的风险感知。此外，制定和执行可接受的系统使用规范和政策对于创建一个安全的网络环境也至关重要，这包括对用户行为的指导和限制，确保所有人员都遵守既定的网络安全准则。

国家和政府作为保障信息系统安全的关键角色，可以通过完善立法加强执法来提高对非法行为的惩罚力度和威慑力[23]。韩竞科[24]以网络钓鱼为例，运用计量经济学中的断点回归设计，构建网络安全法威慑效应断点回归模型以检验实施立法对网络钓鱼

的威慑效应，研究发现，网络安全法的颁布对网络钓鱼具有显著的威慑作用。除此之外，李金在一项研究中也具体解释了这个观点。他使用了生物医疗行业的数据出境统计信息为实证基础，通过分析数据跨境传输的风险影响机制，发现相关法律的执行对数据的跨境传输具有显著的威慑效果。另外，也有研究提出，政府可以通过对入侵者执行强制性的惩罚来解决信息系统安全问题[25]。尽管这种建议看起来在理论上可行，但实证研究显示，在网络犯罪这一特别领域，仅依赖国家级的执法威慑可能效果有限[26]。其原因在于，惩罚的不公平性可能会激起激进的人(如黑客群体)的反感情绪[27]，从而减弱惩罚的威慑力。

综上，现有研究基于威慑理论提出了如何保障信息系统的安全性，但还存在两方面不足：①当前研究大多集中在特定国家(地区)的立法和执法层面，而缺乏不同国家(地区)横向比较的研究。如果能深入研究不同国家(地区)间的信息安全策略和实践，可以为信息安全治理提供更为丰富多元的视角和解决方案。未来的研究应当着重探索和分析各国(地区)在信息安全领域采取的威慑策略，特别是那些有效实施信息安全治理的案例，来帮助理论的发展并且启示实际政策制定；②技术进步推动了入侵手段的多样化和复杂化，同时使得攻击方式更为隐秘和高效。然而，传统的网络安全威慑策略研究侧重于探讨单一的个体或组织防护措施和国家层面的法律制裁，尚未构建起一个综合性的信息系统安全威慑策略体系。面对日益增长的新型网络威胁，这种单一维度的策略已显不足。因此，未来的研究工作应在技术、法律和战略等多个层面进行创新，涵盖个人、组织和国家(地区)各个环节，综合考虑惩罚的严厉性、确定性和敏捷性，构建一个更为全面和有效的多维网络安全威慑体系，有效预防和降低先进入侵技术带来的潜在风险。

### 2.2 威慑理论在数字盗版行为研究中的应用

数字化技术的发展以及互联网的普及，使得数字内容更容易被盗版者复制和分享，这不仅对版权所有人和创作者造成了经济上的损失，而且对相关产业的发展和创新产生了负面影响。因此，学界从威慑理论视角对如何保护数字版权进行了广泛探讨。

一些数字盗版研究将对法律后果的恐惧和对制裁可能性的感知作为主要预测因素。例如，Moores T T 等[28]认为，威慑理论中对盗版行为有重大影响的因素是对法律后果的恐惧和对制裁可能性的感知，对法律后果的恐惧和对制裁可能性的感知对盗版行为的态度有积极影响。Tan B[29]也发现这两个因素在很大程度上影响了消费者对数字盗版的态度。而 Arli D 等[30]对印度尼西亚学生样本的研究发现，对法律后果的恐惧和感知到的制裁可能性对盗版态度没有显著影响。有学者基于这两个因素对打击数字盗版行为提出了研究策略。Hati S R H 等[31]同样在对印度尼西亚样本研究时发现，对法律后果的恐惧和对制裁的感知的影响微乎其微，这表明打击数字盗版的执法力度薄弱，并认为当务之急是加强执法，尤其是针对盗版的执法。Moores T T 等[28]认为，需要将对法律后果的恐惧概念与对制裁可能性的感知区分开来，因为个人可能了解盗版的非法性，但可能不相信自己会被抓住。

许多学者基于威慑理论研究数字盗版行为都考虑了犯罪抑制和动机措施，以道德决策模型作为理论基础，纳入了羞耻、信念等衡量标准，以充分了解如何阻止个人实施盗版软件的犯罪行为。对盗版软件的研究表明，当个人认为这种行为是道德的而不是不道德的，他们就更有可能从事这种行为[32]。一项关于盗版软件的荟萃分析发现，一个人的道德信念和态度会影响其在计算机上从事非法盗版行为的可能性[33]。因此，Wolfe S E 等[34]提出，政策制定者可以通过在下载程序中加入煽动负罪感的声明来利用负罪感减少数字盗版行为。除此之外，宗教信仰被认为也是抑制犯罪行为的一个重要因素，宗教信仰在很大程度上影响着消费者对数字盗版的态度，宗教信仰较少的消费者更容易接受数字盗版。Arli D 等[35]建议管理者和决策者可以与宗教领袖密切合作，强调数字盗版的不道德性。

威慑文献还研究了以往的盗版行为对未来行为的影响。研究表明，过去有过盗版行为的人在未来更有可能从事这种行为[36]。这是因为过去的盗版行为减少了对未来盗版行为的抑制。例如，Higgins

G E 等[37]发现，过去的盗版软件也被证明可以预测未来的盗版软件。

文献回顾发现，威慑理论在数字盗版研究中的应用确实提供了关键的视角，但也存在一些局限性：①上述研究往往选择特定地域的群体作为研究对象，这导致研究结果可能受到特定文化、政治和法律环境的限制，在其他地区的可推广性还有待验证。因此，未来研究应扩展到更广泛的文化和地域背景，通过跨文化或比较研究的方法，以挖掘不同地域及文化背景下盗版现象的差异性，丰富盗版研究的全球视角，增强研究成果的通用性；②现有研究视角多聚焦于记录被盗版方的损失研究，但这种研究视角无法完全解释盗版现象背后的动因。鉴于此，未来的研究需要从消费者的视角出发，比较威慑措施(如法律惩罚)与激励机制(如价格折扣、增值服务等)在影响消费者选择方面的效果。这种双向比较不仅能够理解消费者的盗版行为选择的复杂性，也将为制定更有效、更精准的反盗版政策提供强有力的支持。

### 2.3 威慑理论在在线社交媒体偏差行为研究中的应用

随着在线社交媒体的出现和普及，人们越来越倾向于参与其中，但由于互联网的匿名性和虚拟性，传播虚假信息和谣言以及进行网络攻击等恶意行为也随之增加。在此背景下，威慑理论为分析此类非法与不道德行为提供了一个理论框架[38]。

由于威慑可作为一种预防性控制手段，具有包括恐吓、教育和强化在内的各种效果。一些学者认为可以通过制定规则、处罚、提高透明度和用户教育等手段，来防止或减少用户在社交媒体平台上散播偏见或错误信息的行为。例如，Boadi C 等[39]采用威慑理论从撒哈拉以南非洲的视角对青少年社交媒体用户的偏差和不道德行为进行研究，认为要确保社交媒体不被用于煽动暴力或传播危险谣言，有效的概念化和理论化规则处罚将有助于遏制个人在社交领域的数字平台上的攻击行为。张会平等[40]将威慑理论运用到用户传播谣言的行为研究中，发现制裁机制可以在一定程度上有效抑制网络谣言传播，但是还需加强宣传教育并改善信息沟通机制促使网民主动识别谣言。

此外，还有部分学者引入中和技术自我辩解的概念，通过中和技术和威慑理论的综合视角来研究其对在线社交媒体偏差行为的影响。Zhang S X 等[41]应用中和技术和威慑理论来研究 Facebook 用户在“评论页面”和“上传图片”两种不同网络欺凌情景中的不同反应，研究结果发现，因为用户参与攻击性网络行为会合理化自己对网络欺凌的责任和切断行为与受害者或行为与伤害之间的联系，所以中和技术会促成网络欺凌行为，而在做出网络欺凌的决定时，由于确定性可能代表了一种惩罚不可避免的保证，个人可能会认为制裁的必然性比严重性更重要。姬浩等[42]也发现，中和技术与社会热点事件网络谣言信息情绪化传播意愿正相关，会增强人们对社会热点事件网络谣言信息情绪化传播的意愿，正式制裁、非正式制裁和羞愧制裁呈显著负相关，会在一定程度上约束人们社会热点事件网络谣言信息情绪化传播行为的意愿。

通过对文献的梳理发现，上述研究突出了制裁和教育策略对于遏制社交媒体环境中不当行为的重要性。同时，也表明了理解用户行为背后的心理机制(如中和技术)对于设计有效的干预措施至关重要。然而，现有研究仍然存在着以下不足：①大多数研究主要聚焦于单一社交平台内的威慑机制。但在实际情境中，社交媒体用户往往在多个平台上活跃，而且不同的社交平台可能实施各异的规制策略。这些策略对用户行为的影响及其效率如何，还需要更广泛的比较和深入的评估。因此，未来的研究应当超越单一平台的限制，拓展至多平台的综合分析，对比不同平台的威慑策略有效性。这一点对于构建一个全面的、防范社交媒体不当行为的系统性策略框架，具有重大意义；②现有研究主要关注于探讨社交媒体平台制裁机制对用户偏差行为的影响，而用户个体可能基于理性因素对自身的偏差行为进行自我调整，这为平台制定威慑策略提供了另一种思路。因此，未来研究可以尝试将威慑理论与理性选择理论相结合，探讨在社交媒体环境中，如何通过综合考虑威慑因素和理性选择因素，更有效地预防和制裁偏差行为，从而为这一领域提供一个更加全

面和多元化的理论视角。

## 3 结论与展望

从前文可知，威慑理论认为人是理性的，当人认识到不利行为被发现的风险较高，可能面临即时而严厉的惩罚，并且预期的惩罚会超过可能带来的利益时，就会放弃实施这一行为。部分学者还从融合非理性因素、完善群体差异等方面进一步完善了威慑理论，不仅将其应用于信息安全问题的研究，还被应用于诸如数字盗版行为、在线社交媒体中偏差行为等问题的研究。

现有研究主要存在以下几点不足：①关于惩罚的敏捷性视角研究不足；②当前研究往往将意愿视作行为的等同物，但员工的行为意向并不总能代表员工的实际行为，有必要进一步验证各威慑因素对员工实际行为的影响；③缺乏组织层面的研究；④当前的个体或组织防护措施以及国家(地区)层面的法律制裁研究未能跟上技术入侵的快速发展；⑤研究对象单一，主要是研究信息技术企业、政府机构、被盗版方、社交媒体用户等直接受害群体对于威慑措施的反应；⑥现有研究倾向于选择特定国家(地区)、社交平台等进行纵向研究，这在一定程度上限制了对威慑机制普遍性与差异性的全面理解，同时也不利于在不同国家(地区)和社交平台间对威慑机制的比较与借鉴；⑦忽略了用户个体的理性因素对自身偏差行为的自我调整。

基于如上几点不足，未来的研究可以从以下几方面进行改进和探索：①可以探讨威慑理论的敏捷性与不利行为的直接因果关系，深入研究用户在知晓可能受到立即惩罚时的情感体验以及这种情感体验如何影响其对规则的遵守意愿等问题，拓展威慑理论在信息系统研究中的应用；②需要收集员工的行为数据，在行为意向研究的基础上进一步探索威慑因素对员工行为的影响，完善员工行为研究；③关注工作组或组织层次，研究组织文化和结构、团队的行为模式等中威慑因素的作用；④未来的研究需要在技术、法律和战略等多个层面进行深入创新，着重构建一个涵盖预防、检测和响应各个环节的，综合考虑惩罚的严厉性、确定性和敏捷性的，更为全面和有效的多维网络安全威慑体系；⑤关注消费者等潜在受害者，比较威慑措施与激励机制在影响决策方面的效果，从而形成更精准的威慑策略，营造更安全、全面且以人为本的信息系统环境；⑥进行更多跨文化调研、横向比较研究等来深入探讨不同国家(地区)、不同社交平台以及不同文化背景下威慑策略的特点和效果，丰富现有的威慑理论体系，也有助于形成更加全面和多元的威慑策略实践；⑦综合考虑威慑因素和理性选择因素，将威慑理论与理性选择理论相结合来探讨在社交媒体环境中更有效地预防和制裁偏差行为。

## 参 考 文 献

[1] 宋艳锴，张勇. 威慑理论：刑罚的经济学分析综述 [C] //法经济学的基础理论. 2005 年中国法经济学论坛会议论文集. 中国法经济学论坛会议. 哈尔滨：山东大学经济研究中心法经济学研究所，2005：196-205.

[2] D'Arcy J，Herath T. A Review and Analysis of Deterrence Theory in the IS Security Literature：Making Sense of the Disparate Findings [J]. European Journal of Information Systems，2011，20 (6)：643-658.

[3] 贝卡里亚. 论犯罪与刑罚 [M]. 北京：中国法制出版社，2005：3-15.

[4] Pratt T C，Cullen F T. The Empirical Status of Gottfredson and Hirschi's General Theory of Crime：A Meta-Analysis [J]. Criminology，2000，38 (3)：931-964.

[5] Becker G S. Crime and Punishment：An Economic Approach [J]. Journal of Political Economy，1968，76 (2)：168-169.

[6] Levitt S D. Using Electoral Cycles in Police Hiring to Estimate the Effect of Police on Crime [J]. American Economic Review，1997，87 (3)：270-290.

[7] Lee L. The Deterrent Effect of Police Patrol on Crime：A Replication [J]. The Annals of Regional Science，2001，35 (3)：471-484.

[8] 边沁. 道德与立法原理导论 [M]. 北京：商务印书馆，2017：12-16.

[9] 戈特弗里德森，赫希. 犯罪的一般理论 [M]. 北京：中国人民公安大学出版社，2009：43-65.

[10] 陈屹立. 惩罚性赔偿的根据与适用：法经济学观点 [J]. 思想战线，2007，33 (2)：67-73.

[11] 杨杨，杜剑. "互联网+" 背景下税收合作性遵从实现的路径分析 [J]. 税务研究，2016，(5)：37-42.

[12] 张晨颖. 损失视角下的垄断行为责任体系研究 [J]. 清华法学，2018，12 (5)：193-208.

[13] 李瀛. 员工信息安全违规意愿的实证研究 [D]. 大连：大连理工大学，2011：21-22.

[14] 王冬梅. 理性选择视角下信息安全违背行为影响因素实证研究 [D]. 镇江：江苏科技大学，2015：24-25.

[15] Hu Q，Xu Z，DinevT，et al. Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? [J] Communications of the ACM，2011，54 (6)：54.

[16] 陈琳. 影响员工遵从信息安全政策的要素研究 [D]. 大连：大连理工大学，2011：13-15.

[17] Kankanhalli A，Teo H H，Tan B C Y，et al. An Integrative Study of Information Systems Security Effectiveness [J]. International Journal of Information Management，2003，23 (2)：139-154.

[18] Fan J，Zhang P J，Zhao X J. Study on the Impact of Security Countermeasures on E-Government Information Misuse [C] // Services Systems and Services Management. Proceedings of the 8th. Conference on Services Systems and Services Management，Tianjin：Institute of Electrical and Electronics Engineers，2011：1-6.

[19] 林润辉，谢宗晓，吴波，等. 处罚对信息安全策略遵守的影响研究——威慑理论与理性选择理论的整合视角 [J]. 南开管理评论，2015，18 (4)：151-160.

[20] Siponen M，Soliman W，Vance A. Common Misunderstandings of Deterrence Theory in Information Systems Research and Future Research Directions [J]. Database for Advances in Information Systems，2022，53 (1)：25-60.

[21] Merhi I M，Ahluwalia P. Examining the Impact of Deterrence Factors and Norms on Resistance to Information Systems Security [J]. Computers in Human Behavior，2019，92：37-46.

[22] Straub D W，Nance W D. Discovering and Disciplining Computer Abuse in Organizations：A Field Study [J]. MIS Quarterly，1990，14 (1)：45-60.

[23] Homoliak I，Toffalini F，Guarnizo J，et al. Insight into Insiders and IT：A Survey of Insider Threat Taxonomies，Analysis，Modeling and Countermeasures [J]. ACM Computing Surveys，2019，52 (2)：30-43.

[24] 韩竟科. 网络安全立法的威慑效应研究 [D]. 镇江：江苏科技大学，2022：22-24.

[25] Kim S H，Wang Q H，Ullrich J B. A Comparative Study of Cyberattacks [J]. Communications of the ACM，2012，55 (3)：66-73.

[26] Png I P，Wang C Y，Wang Q H. The Deterrent and Displacement Effects of Information Security Enforcement：International Evidence [J]. Journal of Management Information Systems，2008，25 (2)：125-144.

[27] Bouffard L A，Piquero N L. Defiance Theory and Life Course Explanations of Persistent Offending [J]. Crime & Delinquency，2010，56 (2)：227-252.

[288] Moores T T，Nill A，Rothenberger M A. Knowledge of Software Piracy as an Antecedent to Reducing Pirating Behavior [J]. Journal of Computer Information Systems，2009，50 (1)：82-89.

[29] Tan B. Understanding Consumer Ethical Decision Making with Respect to Purchase of Pirated Software [J]. Journal of Consumer Marketing，2002，19 (2)：96-111.

[30] Arli D，Tjiptono F. Consumer Digital Piracy Behaviour among Youths：Insights from Indonesia [J]. Asia Pacific Journal of Marketing and Logistics，2016，28 (5)：898-922.

[31] Hati S R H，Fitriasih R，Safira A. E-textbook Piracy Behavior：An Integration of Ethics Theory，Deterrence Theory and Theory of Planned Behavior [J]. Journal of Information Communication and Ethics in Society，2019，18 (1)：1-19.

[32] Wagner S C，Sanders G L. Considerations in Ethical Decision-Making and Software Piracy [J]. Journal of Business Ethics，2001，29 (1-2)：161-167.

[33] Liang Z L，Yan Z. Software Piracy Among College Students：A Comprehensive Review of Contributing Factors，Underlying Processes，and Tackling Strategies [J]. Journal of Educational Computing Research，2005，33 (2)：115-140.

[34] Wolfe S E，Higgins G E，Marcum C D. Deterrence and Digital Piracy：A Preliminary Examination of the Role of Viruses [J]. Social Science Computer Review，2008，26 (3)：317-333.

[35] Arli D，Kubacki K，Tjiptono F，et al. Religiousness and Digital Piracy Among Young Consumers in an Emerging Market [J]. Young Consumers，2017，18 (1)：40-53.

[36] Nagin D S，Paternoster R. The Preventive Effects of the Perceived Risk of Arrest：Testing an Expanded Conception of Deterrence [J]. Criminology，1991，29 (4)：561-587.

[37] Higgins G E，Wilson A L，Fell B D. An Application of Deterrence Theory to Software Piracy [J]. Journal of Criminal Justice and Popular Culture，2005，12 (3)：166-184.

[38] Xu B，Xu Z，Li D. Internet Aggression in Online Communities：A Contemporary Deterrence Perspective [J]. Information Systems Journal，2016，26 (6)：641-667.

[39] Boadi C，Kolog E A. Social Media Aggression：An Assessment Based on the Contemporary Deterrence Theory [C] //Digital Innovation and Entrepreneurship. Proceedings of the 27th，Montreal：Association for Information Systems，2021：1-5.

[40] 张会平，郭昕昊，郭宁. 突发事件中网络谣言识别行为意向的影响因素研究 [J]. 现代情报，2017，37 (7)：60-65.

[41] Zhang S X，Yu L，Wakefield L R，et al. Friend or Foe：Cyberbullying in Social Network Sites [J]. ACM SIGMIS Database：the Database for Advances in Information Systems，2016，47 (1)：51-71.

[42] 姬浩，苏兵，吕美. 网络谣言信息情绪化传播行为的意愿研究——基于社会热点事件视角 [J]. 情报杂志，2014，33 (11)：34-39，28.

(责任编辑：郭沫含)