

智能化背景下隐私政策的困境及消解路径

孙晓宇,夏保华

(东南大学哲学与科学系,江苏南京 211189)

摘要:随着人工智能技术的广泛应用,用户的数据隐私安全成为研究的焦点之一。为了保护用户的数据隐私安全,企业提供了隐私政策。然而,大多数隐私政策不仅存在不可解释、不透明、不公平、实用性不强和及时性较低等问题,还忽略了用户的预测隐私。因而在具体实践中,隐私政策既不能有效保护直接获取得到的隐私,又会侵犯到预测隐私,违背了最初的目的,产生了隐私政策的保护悖论。本文参照以人为本的人工智能框架,提出要开发以人为本的隐私政策,以尽可能消解隐私政策的困境,确保用户的数据隐私安全。

关键词:人工智能;隐私政策;预测隐私;以人为本

中图分类号:G315

文献标识码:A

近年来,网络平台或应用(App)发展迅速,成为人们日常生活中不可或缺的一部分。它们在改变人们生活方式的同时,也可能会侵害人们的权益,例如,隐私泄露,危及用户的数据隐私安全^[1,2]。APP在未经用户授权的情况下,不当或过度收集和使用有关用户行为、个人偏好、位置和其他用户信息数据的事件频发^[3,4]。甚至有些App还要求共享详细的用户信息^[5]。为了整顿这种乱象,保护用户的数据隐私安全,政府相关部门出台了一些法律法规,明确要求在线网络平台或APP的开发商(文中统称为企业)必须规范收集、处理、分享用户信息数据的各种行为,并且企业需要将这些实践行为总结为具体、透明的在线隐私政策提供给用户^[6],确保告知用户知晓信息数据被使用的情况。隐私政策(也指商业隐私政策)成为规范和监督企业使用用户信息数据的常用方法,也是隐私保护的重要途径^[7]。有研究表明,大约64%的用户更倾向于信任那些能够提供明确隐私政策的企业^[8]。

虽然目前隐私政策逐渐普及,但用户的数据隐私安全似乎更易受到挑战,加剧了用户对隐私的担忧,用户也越来越不信任企业。学者们对在线隐私政策展开了广泛的讨论和研究。大多数学者认为隐私政策存在许多问题。例如,有部分学者指出,这是由于隐私政策没有有效地告知用户在线平台或APP

的隐私问题,导致用户无法安全、安心地使用在线平台或APP,即没有做到使用户获得知情同意的权利^[9-11]。阿里·苏尼亚耶夫(Ali Sunyaev)等学者通过调查了许多APP的隐私政策后发现,它们很少会关注到APP自身,因此最终没有向用户提供任何有效的信息^[12]。还有学者表明,隐私政策的篇幅过长,通常使用偏向法律的专业术语,用户需要花费大量的时间去阅读它们^[13,14]。然而,有学者提出了相反的观点,他们认为如果从道德的角度来看,隐私政策的知情同意不具有知情同意方面的缺陷^[15]。还有学者发现,绝大多数用户倾向于不阅读隐私政策,因为它们多是冗长又繁琐,用户不希望在阅读隐私政策上花费太多时间和精力^[16,17],由此企业将责任归结为用户。目前的研究大多是停留在隐私政策常见的问题上,例如,表现形式上的冗长、繁琐,很少会关注其衍生的更深层次的局限性。

本文认为隐私政策自身不仅具有上述的各种问题,导致应用层面的困境,不能有效的实现隐私保护,还会侵犯到用户的预测隐私,产生隐私政策的保护悖论。本文首先概述了隐私政策的概念、基本内容及其性质特征,在第二部分详细分析了隐私政策中不仅存在当前各界提出的一些常见问题,还会由此衍生出不可解释、不公平、不透明和实用性较差等方面的缺陷,并且隐私政策主要关注的是直接收集

获取的隐私,忽略了预测隐私的内容。但实际上隐私政策既不能保护直接收集获取的隐私,又会侵犯更多的预测隐私,由此隐私政策可能无法达到隐私保护的目,结果可能引发隐私安全风险,违背了最初制定隐私政策的目的,产生了隐私政策的保护悖论。最后,为了尽可能消解隐私政策的困境,本文参照以人为本的人工智能(Human Centered AI)框架,提出要开发以人为本的隐私政策,切实为用户服务,以确保用户的数据隐私安全。

1 隐私政策及其性质

1.1 隐私政策的概念和基本内容

隐私政策(privacy policy,也称用户协议、隐私协议或隐私声明等,在文中统称为隐私政策)是指一种机制或一份隐私声明,通常以在线文件或单独链接的形式呈现给用户,用以披露在线网站平台或APP如何收集、使用、储存、共享和管理用户的个人信息数据,旨在帮助潜在用户评估和决定是否使用企业给定的在线网站平台或APP^[18]。并且在线网站平台或APP对用个人信息数据的处理通常需要用户的同意或相关的法律依据^[19],隐私政策也代表了用户和企业之间的法律契约^[20]。由此隐私政策的初衷是确保用户充分知晓其个人信息数据的收集、处理和存储方式,公开企业在用户信息处理中的各项实践,明确各种数据实践行为的正当性和必要性,并增强用户的自主决策能力,使他们能够基于信息做出选择。同时保障用户和社会公众对企业数据实践的监督权,从而更为客观地维护用户的数据隐私安全。

虽然不同隐私政策的内容不尽相同,但它们的基本内容至少都需要包含:(1)有关用户身份和联系方式的详细信息;(2)用户的哪些信息数据会被收集、使用、管理和分享;(3)收集和使用个人信息数据的具体目的;(4)是否会分享给第三方,以及如何共享、转让和公开个人数据;(5)用户的权限有哪些(比如说,访问、拒绝和限制使用、删除个人数据等);(6)用户的信息数据如何被存储^[21]。

1.2 隐私政策的性质

学界对隐私政策进行了广泛探讨,但关于隐私政策的性质并没有一个相对统一的观点。其中主要的观点有两种:一是隐私政策具有合同性质;二是隐私政策是一种工具,用以规范或监督企业的数据实

践行为。

(1)合同学说。合同学说认为隐私政策代表了企业与用户之间签订的一种具有法律效力的契约,它规定了企业收集、使用、分享用户信息数据的目的和方式等。斯科特·克林斯沃斯(Scott Killing-sworth)非常坚定地认为隐私政策是一种合同,具有合同的目的和所有特征,但是只有在用户选择了企业所提供的隐私政策,点击了“同意”后,隐私政策才能被执行^[22]。伍德罗·哈佐格(Woodrow Har-tzog)也持隐私政策具有合同性质的观点,建议将在线网站的功能和设计视为可被执行的承诺,并提出能更准确地反映网站和用户之间协议的方法^[23]。托马斯·哈利(Thomas Haley)也认为,隐私政策被广泛地应用于人们的日常生活,在法律诉讼中,它构成了违约索赔的基础,具有合同的性质^[24]。

(2)规范工具或企业自律学说。丹尼尔·索洛夫(Daniel Solove)和伍德罗·哈佐格指出,隐私政策本质上不应该被视为合同,因为即使隐私政策看起来和合同类似,但很少有案件将隐私政策按照合同法规定的内容进行执行^[25]。因此,隐私政策是否具有合同的性质存在争议,有学者提出了规范工具或企业自律学说。该学说认为隐私政策是用来使企业的数据实践行为符合相关法律法规的一种工具,甚至可以起到部分监督的作用,由此隐私政策有时也被视为企业的自律准则。并且企业通过隐私政策实现通知和选择的模式,该模式旨在使个人负责其个人信息的收集和使用^[26],而企业需要明确、有效地告知用户其个人信息被收集、使用和分享的目的和范围等,用户根据告知的内容做出选择和同意的决定。

总体而言,虽然学界关于隐私政策的性质尚未达成一个共识,但本文认为以上两种观点并非是相对立的,可以进行融合,即隐私政策既具有合同的属性,又是一种可以进行规范或监督的工具。并且隐私政策最主要的性质是具有法律属性,必须符合相关法律法规的要求。隐私政策制定的初衷是:一方面,企业向用户承诺或保证收集、处理、使用或披露个人信息数据的正当性、必要性、透明性等,确保用户的数据隐私安全,另一方面是企业自我约束和监督的承诺,由此隐私政策是企业数据实践行为的依据,保障用户数据隐私安全的重要措施。然而,在具体实践中,隐私政策不仅在表现形式上存在不足,还可能会衍生出其他的问题,影响用户的数据隐私

安全。

2 隐私政策的困境

通常隐私政策在表现形式上是冗长又繁琐,但隐私政策除了这些问题外,还会衍生出其他问题,导致应用层面的困境,进而影响到隐私保护的有效性。本文将隐私政策的问题分为常见的问题和衍生的问题两大类,以下对隐私政策出现的问题进行分析(见下表1),并在此基础上指出隐私政策不仅不能保护隐私,反而可能会侵犯用户更多的隐私,产生隐私政策的保护悖论。

表 1 隐私政策的问题
Table 1 Issues of the privacy policy

常见的问题	衍生的问题
内容繁冗	可解释性较低
专业性较强	透明性较差
语言模糊	公平性较低
概念争议	实用性不强
知情同意难题	及时性较低

2.1 隐私政策常见的问题

隐私政策常见的问题是指目前各界普遍讨论的隐私政策存在的问题,具体表现为内容的繁冗、专业性较强、语言模糊、概念争议和知情同意难题几个方面。

(1)内容繁冗。大多数隐私政策的内容十分繁琐,长篇累牍,动辄字数上万,甚至中间还会穿插各种链接的内容作为补充。据相关调查显示,手机应用商店中5款下载过亿的APP的隐私政策的字数总和超过13万,平均每款APP用户需要阅读的内容大约2.7万字,篇幅长度堪比一篇学位论文^[27],严重阻碍了用户的阅读和理解。

(2)专业性较强。隐私政策包含了大量偏向法律的术语和专业的技术名词,例如,“像素标签”和“网站信标”等,增加了隐私政策的复杂性。隐私政策还可能会隐含一些损害到用户正当权益的内容,比如说,有些隐私政策的条款可能将责任归为用户,那么即使用户的权益受到侵犯,用户也很难寻求帮助。

(3)语言模糊。隐私政策是由自然语言编写的,模糊性是其本质属性。隐私政策对信息数据收集、使用、存储和共享的各个过程的描述是模糊

的^[28]。例如,有研究提到A网站的隐私政策中有条款规定:“根据您的选择与A企业互动的方式,我们可能会收集您的个人信息……”“我们可能会从业务合作伙伴、承包商和其他第三方收集您的个人信息和其他信息。”“如果您使用B企业的帐户访问我们的产品和服务,B企业可能会与我们分享您的个人信息……”从中可以看出,隐私政策多使用“可能”等不确定的表述,极具模糊性^[29]。

(4)概念争议。隐私政策中通常使用“个人信息”一词,包括用户姓名、电话、邮箱、位置信息、浏览记录,等等,并将其归为隐私。但“隐私”和“个人信息”这两个概念在定义和如何界定均存在争议。一方面,隐私和个人信息的概念没有一个明确和统一的定义。因为随着社会和技术的发展,隐私的内涵会不断地发生变化,具有高度的动态性和不确定性。尤其是在当前智能化的社会中,隐私的概念又会进一步外延,从传统的隐私概念,如,私人领域、独处的权利和自由等,延伸到个人隐私数据和信息等,但其本质上仍是一个具有争议性的概念,在实践过程中也会产生诸多分歧^[30]。个人信息的概念亦是如此,各界也十分关注如何明确地界定个人信息,比如说,从国家标准的层面来看,个人信息可以通过识别性来定义,即将能够识别公民身份的信息认定为个人信息,但围绕“识别”一词可能有不同的解释路径^[31],这使个人信息的界定具有不确定性。在司法解释中,个人信息的内涵更为宽泛,不仅包含识别性信息,还包括一些可以反映自然人特定活动状态的信息^[32]。另一方面,隐私和个人信息之间的界限也是不确定的。有研究通过个人信息来界定隐私,认为隐私是对个人信息的控制^[33]。还有学者认为隐私和个人信息存在部分交叠与重合,只有私密信息属于隐私的范围^[34]。然而,人工智能技术能够进行推断和预测,即从直接收集得到的、不包含个人隐私的信息中推断出其他包含个人隐私的内容,即预测隐私(predictive privacy)^[35]。

(5)知情同意难题。隐私政策主要涉及到对用户信息数据的收集和处理,因而知情同意原则是其实践的前提,即隐私政策必须使用户知悉哪些信息数据会被收集、使用、存储以及分享,并且用户点击“同意”后,企业才能获取收集和处理用户信息数据的权限。然而,隐私政策在践行知情同意原则的过程中面临着巨大的挑战。有学者认为知情同意原则应用困难的原因在于:用户很少阅读隐私政策,或阅

读了但不能够充分理解隐私政策,或缺乏足够的专业知识来充分评估是否做出“同意”的选择以及其他各种因素阻碍了用户的理性决策^[36]。此外,大多数用户可能是被迫做出“同意”的选择,无自主选择权^[37]。因为如果不点击“同意”,用户则无法安装和使用相关的服务,因而只能被迫同意隐私政策的所有内容,但实际上企业的数据实践行为和隐私政策中声明的条款可能存在着显著差异^[38]。

2.2 隐私政策衍生的问题

隐私政策衍生的问题是指隐私政策中的深层次问题(为了与上文中隐私政策常见的问题进行区分),主要可概括为可解释性较低、透明性较差、缺乏公平性、实用性不强和及时性较低。

(1)可解释性问题。隐私政策的可解释性较差问题。首先,隐私政策是用自然语言进行编写的,但自然语言具有多样性和模糊性,这不仅使用户难以从中提取有用的信息,更难理解其含义。其次,隐私政策在编写过程中偏向使用专业的法律术语,对用户而言,晦涩难懂,用户无法完全理解,更无从谈及控制个人信息数据。最后,隐私政策的内容一般较为繁冗,存在重叠的信息数据实践概念,缺少明细的分类和组织架构,可能会导致较差的可解释性,致使用户无法把握整个隐私政策的内容^[39]。

(2)透明性问题。虽然许多企业提供了隐私政策,但仍有部分企业在数据实践中会出现一些违规行为,其中一个非常重要的因素是隐私政策缺乏透明性。比如说,有学者调查了与健康相关的APP后发现,这些APP的数据收集过程远不透明^[40]。还有学者通过对上万个网站提供的约百万份隐私政策进行分析发现,隐私政策不仅在可读性和透明度方面存在问题,始终未能充分披露常见的跟踪技术和第三方的存在,并且随着时间的变化,隐私政策变得越来越长,难以理解^[41]。还有学者指出,一些隐私政策的条款是由企业提供的,可能更多的是保障企业的利益^[42]。并且随着人工智能技术的嵌入,信息数据收集、使用和分享的方法也变得越来越智能和复杂,缺乏可解释性,由此隐私政策是不透明的,不能明确和清晰地描述信息数据收集和处理的实践过程,用户难以了解自身的哪些信息数据会被收集,如何被使用等。此外,从上文中可知,隐私政策中包含具有争议性的概念和模糊性的描述,这也会导致隐私政策缺乏透明性。

(3)公平性问题。隐私政策在实践过程中可能

存在不公平问题。一方面,隐私政策的语言较复杂,篇幅较长。有研究指出,只有具备一定程度大学教育水平的用户才有可能理解一份隐私政策,普通用户难以理解^[43]。甚至还有研究指出,即使是具备法律专业的用户也会出现阅读和理解方面的障碍^[44]。那么对于一些弱势群体来说,如,未成年人、老年人群体,尤其是患有认知障碍的群体,能够阅读并理解隐私政策更是困难重重^[45],并且如果他们的信息数据在未“同意”的情况下被使用和分享,他们将面临高度的隐私风险。另一方面,如前文所述,隐私政策可能难以真正地践行知情同意原则,即大多数用户是在被迫的情况下同意隐私政策所规定的全部内容,用户并没有选择权,由此即使用户意识到个人隐私受到侵犯,可能也难以维护自己的合法权益,极具不公平性。

(4)实用性问题。隐私政策的实用性不强。隐私政策的内容冗长复杂且专业性较强,包含许多法律术语和其他专业性术语,用户很难阅读和理解其中的条款,导致大多数用户不愿意阅读隐私政策。据一项调查显示,大约70%的用户很少或从不阅读隐私政策,为了使用软件,用户不能不点击同意按钮,但并不知道让渡了哪些权利^[46]。此外,隐私政策中规定的信息数据收集的范围较为宽泛,几乎涵盖了用户的所有个人信息数据,并且对个人信息数据的使用和共享缺乏透明性,更易产生隐私泄露的风险。

(5)及时性问题。隐私政策的及时性较低。隐私政策的制定通常是依据相关的法律法规,但法律法规从起草到正式实行的过程相对比较漫长,具有一定的滞后性,这会影响到隐私政策的及时性。另外,随着人工智能的发展,用户的信息数据在不断地增长,可能会使隐私政策的内容变得更繁杂,增加了更新的时间和成本,导致更新速度不及时。

总之,隐私政策不仅存在诸多当前各界关注的常见问题,如,内容繁杂,篇幅较长,偏向使用法律和专业性术语,使用的概念具有争议性以及无法适用于知情同意原则等,在此基础上,隐私政策还衍生出不可解释、缺乏透明性、不公平、实用性较差和更新不及时等问题,影响到隐私保护的有效性,造成隐私政策的保护悖论。

2.3 隐私政策的保护悖论

首先,隐私政策自身的问题和局限性导致产生隐私风险。从上文中可知,隐私政策存在诸多问题,

即使企业已经提供了隐私政策,但实际上用户并不知晓自己的哪些信息数据被收集、使用和分享,以及具有哪些权利和责任。并且隐私政策是由企业提供的,它们更多的是为了使企业的利益最大化,而不是保障用户的权益。那么一些隐私政策对用户而言可能只是一种形式上的隐私保护,实质上可能已经成为保护企业的手段,使企业能够合理和合法地收集、使用和分享用户的信息数据,并不能起到有效确保用户数据隐私安全的作用。

其次,隐私政策忽略了预测隐私。隐私政策所承诺保护的隐私属于直接收集得到的隐私。然而,随着人工智能的广泛应用,隐私的内涵在不断地延伸,不仅包括直接收集得到的隐私,还包括预测隐私。预测隐私是指利用直接收集得到的隐私进一步预测得到的其他隐私。即人工智能技术允许基于许多的匿名数据对第三方进行预测,预测隐私包括购买力、性别、年龄、健康状况、性取向、种族和宗教信仰等^[35],如,已知一个人的购买记录和浏览记录等,可以推断出这个人的购买力和购买偏好。在一个人不知情的情况下,即违背了他的意愿,以许多已获取的数据为基础对此人的其他个人信息进行预测时,他的预测隐私就被侵犯了。简而言之,侵犯预测隐私不是通过窃取或泄露某人的个人信息,而是通过从许多网络平台或其他用户那里收集得到的数据,然后通过分析和推断得出的预测信息^[47]。大多数隐私政策有条款提到,为了使用户享受优质的服务,提高用户的体验感,企业必须通过直接收集得到的用户信息数据进行分析,为用户提供更加贴切和精准的商业服务。由此企业直接收集得到的信息数据可以被进一步预测和推断出用户的其他信息数据。即使企业通过直接收集得到的信息数据(不涉及到用户的隐私),但经过预测和推断出的信息数据可能已经属于用户预测隐私的范畴,威胁到用户的隐私安全。并且隐私政策还规定了可以从第三方获取有关的信息数据,那么企业获取得到的信息数据越多,预测和推断的精度就越高,得到的预测隐私的内容就越多、越精准,用户失去的预测隐私可能也越多,从而可能导致隐私政策丧失了保护用户隐私的功能^[48]。

再次,企业保留了修改隐私政策的权利,可能会侵犯到用户的隐私。一些隐私政策规定了企业具有更新和修改的权利,有些企业受到某些因素的影响,可能会违反自己的隐私政策,或是在用户不知情的

情况下修改隐私政策的内容。虽然隐私政策有相关内容提到,会在变更时通知用户。但在大多数情况下,隐私政策的知情同意机制可能是无效的。一方面,用户不愿意阅读隐私政策;另一方面,即使用户阅读了修改后的隐私政策,也很难理解其内容,并且没有参与和选择权,只能被迫同意和接受,使隐私政策失去了实质性的隐私保护作用。

最后,在隐私政策撰写过程中,选择使用自然语言或专业技术语言也带来了复杂的权衡问题。一方面,自然语言通俗易懂,使用自然语言能够使用户,尤其是非技术背景的用户,更易理解和接受隐私政策的内容。然而,自然语言具有一定的模糊性^[49],导致隐私政策在具体实践过程中会出现争议和误解。比如说,在面对法律纠纷时,由于其部分内容表述不甚精确,可能会出现不同的解读,从而影响隐私保护的有效性。另一方面,专业技术语言的使用虽然可以提高隐私政策的精确性,避免出现争议,但其专业性和复杂性增加了阅读的难度,普通用户很难理解和接受,削弱了隐私政策的可接受性和透明性,进而影响隐私保护的效果。

综上所述,隐私政策最终产生了隐私保护悖论,即制定隐私政策的目的是为了使用户了解自己的哪些信息数据会被收集以及如何被使用,并承诺保护直接收集得到的数据隐私安全。然而,实际上用户并不清楚企业如何收集和使用信息数据,还将会导致预测隐私的泄露。简而言之,制定和实施隐私政策的初衷是为了透明化和约束数据收集、处理、储存和分享的各个过程,确保用户的数据隐私安全,但在具体实践中,隐私政策带来了许多问题,给用户造成了一定的障碍,不仅不能有效保护用户的数据隐私,反而可能引发用户更多的数据隐私被泄露的后果,违背了隐私政策的初衷,我们将此现象称为隐私政策的保护悖论。

3 消解隐私政策困境的路径

隐私政策自身的局限性及隐私政策的保护悖论可能会对社会产生一些负面的影响,比如说,导致用户信任危机,损害企业自身的形象,扰乱市场秩序,甚至可能会造成市场失灵^[50],最终引起公众质疑隐私保护的意義和价值,产生隐私保护的无谓论^[48]。为了消解隐私政策的困境,保护用户的数据隐私安全,本文参照以人为本的人工智能(Human Centered

AI, HCAI) 框架提出发展以人为本的隐私政策, 并基于前文中隐私政策存在的问题, 提供一些可供参考的实践措施。

3.1 以人为本的隐私政策及其框架

以人为本的人工智能主要关注的是用户的需求, 所以潜在用户和其他利益相关者共同参与设计过程中对于开发以人为本的人工智能系统非常重要^[51]。以人为本的人工智能系统旨在指导技术研发人员在设计过程中适当授权用户, 增强和扩大用户的权力, 以支持用户的自我效能感 (self-efficacy)、提高创造力、明确责任和促进共同参与, 满足用户想要的各种服务, 更好地控制隐私和安全^[52]。此外, 以人为本的人工智能系统在设计、开发和实施过程中能够通过良好的技术实践, 安全开放的管理策略, 独立良好的监督结构, 构建安全、可信、可靠的人工智能系统^[53]。

隐私政策的服务对象主要是用户, 因而隐私政策的设计和开发可以参照以人为本的人工智能系统, 即开发以人为本的隐私政策。由此, 以人为本的隐私政策也主要是为用户服务, 将个人的差异、需求偏好、价值期望等纳入隐私政策的考量范围内^[54], 了解用户的利益诉求, 满足不同用户对数据隐私的各种需求, 并通过提供可解释、透明、公平、实用和更新及时的隐私政策以及增强管理和监督机制, 切实保障用户的隐私权益, 以提高隐私政策的安全性、可靠性和可信任程度。

3.2 以人为本隐私政策的实践路径

(1) 简化语言, 突出重点。隐私政策的服务对象是用户, 但大多用户无法理解隐私政策, 因而隐私政策需要缩短篇幅、简化语言, 突出其重点内容, 向用户提供清晰、易于理解的信息 (主要涉及信息数据收集和处理的目的是、方式、范围、与第三方共享时可能产生的风险以及用户的权利等), 使用户能够真正把握隐私政策的内容。另外, 对于较为专业的术语尽量使用通俗易懂的语言进行表述, 复杂抽象的概念可以使用图形来表示, 将技术语言中复杂的内容直观化, 使之符合用户的一般认知范围, 帮助用户更好地理解隐私政策的技术细节和实施流程, 从而消除隐私政策和用户之间的差距, 促进隐私政策更好地应用于实践, 增加隐私政策的实用性和可解释性。

(2) 明晰隐私政策的内容表述。如前文中所述, 隐私政策的条款中经常会使用“可能”等含义不

确定的表述, 比如说, “可能会收集用户与企业之间互动的信息” “可能会在相关联的机构间披露用户的数据信息” 等, 这些不清晰的语言描述会给企业操纵用户数据隐私的空间和权力, 导致用户数据隐私泄露的风险, 因此隐私政策的条款在制定过程中必须使用含义明晰、肯定的语言进行表述, 避免使用模棱两可的词语。

(3) 规范隐私相关的概念, 开发个性化的数据隐私模式。隐私政策涉及到的“隐私” “个人信息” 的概念均具有争议性。政府相关法律法规、企业和用户对这些概念的理解存在一定的差异性, 没有形成一个统一的认知。理论上的争议导致在实际应用过程中经常会发生一些争论, 因而需要规范隐私相关的定义。但任何一方的定义方式均不能满足需求, 故需要政府、企业和用户三方共同进行定义。三方的定义方式既能符合相关法律法规的要求, 又能满足企业和用户的隐私需求。由此企业可以采用个性化的数据隐私模式, 即将数据隐私划分为收集、使用、管理与分享三大部分, 分别进行操作和处理。简而言之, 一种模式是指企业收集、使用、管理与分享用户的信息数据必须在相关的法律法规和各种伦理规范允许的范围内进行; 另一种则是指在法律法规和各种伦理规范的基础上, 在数据收集、使用、管理与分享的不同阶段, 用户能够自主选择哪些信息数据可以或不可以被收集、使用、管理与分享。这种个性化的数据隐私模式不仅可以解决由概念争议带来的实践困境, 又能使用户参与其中, 同时也约束了企业的权力。

(4) 优化隐私政策的知情同意机制。知情同意不能较好地适用于隐私政策, 带来了许多实践的难题, 因而需要优化知情同意机制, 保护用户的权益和隐私。隐私政策的阅读率较低是影响用户“知情” 的重要原因, 上文中的简化隐私政策内容, 降低用户的阅读难度, 减少阅读时间, 重点突出用户最为关心的内容, 如数据收集的类型、使用目的、如何存储以及第三方的共享, 提高用户的阅读兴趣等, 这在一定程度上能够使用户“知情”。对于“同意” 的问题, 建议采取分层级和可选择的“同意”, 根据不同信息数据类型的敏感性进行划分。如, 根据数据信息的敏感性不同, 将数据实践活动分为不同的层级。依据相关法律法规中的敏感性数据信息, 如医疗健康数据、住址、身份信息和行踪轨迹等, 这类信息必须要设置为最高的层级, 而相对于不敏感的信息, 可以放

在较低层级。在相关法律法规允许的范围内,可以提供多种可选的“同意”选项,如用户可以根据实际需求选择只同意数据的收集,而拒绝非必要的数据处理和分享等;或者只同意收集某一类信息,拒绝收集其他类型信息;或是只同意用于基础使用功能的数据收集,拒绝商业广告应用和进一步分享等。在每个层级中,向用户提供可选的“同意”选项,用户可以进行自由选择。并增加选择限制和“同意”的撤回,撤回的过程须简单明了,撤回同意后,APP 应立即停止与数据相关的各种实践,以提高隐私政策中知情同意机制的透明性和可靠性。

(5) 严格规范数据的使用。预测隐私的安全是当前隐私政策面临的重大挑战之一。利用人工智能技术,企业能够基于既有的用户数据进行数据分析和推断,从而得到关于用户个人偏好、信仰等预测信息,威胁用户的数据隐私安全。因而必须严格规范相关企业对用户数据的使用情况,不仅要确保企业数据收集和处理等过程的合法性和透明性,只允许使用必要的数据进行分析和预测,还要对数据分析和预测的结果和应用进行严格的控制,避免不当使用,从而有助于增强用户的数据隐私安全,并增强用户对企业的信任。

(6) 加强对技术的监管和增加预测隐私相关的可选项。人工智能具有一定的预测分析功能,能够基于已有的不敏感且容易获得的信息进一步预测其他信息。在监管不足的情况下,企业可能会利用人工智能技术对用户的信息进行预测,预测得到的信息可能包含个人隐私,如,健康状况、购买信息和种族等。因而,一方面需要加强技术层面的评估和监管,确保技术的合理和公正应用,对于违反监管规定和隐私保护措施的企业,监管机构应采取适当的惩罚和违规处理措施,以保护监管的有效性。另一方面,隐私政策中需要增加预测隐私的相关条款,并添加是否允许被追踪以及是否允许被预测信息的选项供用户自行选择,保障用户的预测隐私权益。

除以上的途径外,隐私政策还需要提高数据使用的透明度和用户的参与度。隐私政策还需要增强信息数据实践过程的可见性,增加用户的参与度和互动,提升用户对企业的信任,从而有利于建立良好的企业形象,促进形成健康、有序的市场秩序。此外,企业内部也需要加强对法律法规的监测和跟踪,简化内部隐私政策的制定流程,增加隐私保护、法律等相关的专业人才,定期审查和更新隐私政策的内

容,提高隐私政策的及时性,以适用于人工智能技术的发展,切实保护用户的数据隐私安全。

4 结 论

人工智能的发展引起了人们对隐私的担忧,尤其是各类 APP 过度收集和使用用户的隐私数据,导致隐私泄露的事件频发。相关法律法规要求企业必须提供隐私政策以保护用户的隐私权益。隐私政策的主要目的也是为了监督和约束企业的数据实践行为,承诺保护用户的数据隐私安全,具有一定的法律属性。然而,隐私政策不仅内容复杂、冗长、专业性较强、概念模糊具有争议性等,影响用户阅读和理解,还在可解释性、透明性、公平性、实用性和及时性等方面存在困境。尤为重要的是,隐私政策忽略了预测隐私的内容,只规定了保护直接收集得到的隐私安全。但实际上隐私政策不仅不能确保直接收集得到的数据隐私安全,还会侵犯更多的预测隐私,影响隐私保护的有效性,产生隐私政策的保护悖论。由此为了消解隐私政策的困境,保障用户的隐私权益,本文提出发展以人为本的隐私政策,即采取简化隐私政策、增强数据隐私的透明性和可见性,开发个性化的数据隐私模式,采用严格的数据使用规范,提高用户的参与度等实践措施,以增强隐私政策的可解释性、透明性、公平性、实用性和及时性,消解当前隐私政策面临的困境,实现安全、可靠和可信的隐私政策,确保用户的数据隐私安全。

参考文献:

- [1] Mohsen F, Karastoyanova D, Azzopardi G. Early detection of violating mobile apps: A data-driven predictive model approach [J]. *Systems and Soft Computing*, 2022, 4: 200045.
- [2] 陈小平. 人工智能伦理治理: 一种新型问题的底层逻辑和创新探索 [J]. *生命科学*, 2022, 34(8): 983 - 989. Chen X P. AI ethical governance: The underlying logic and innovative exploration of a new-type issue [J]. *Chinese Bulletin of Life Sciences*, 2022, 34(8): 983 - 989.
- [3] Castro C. Mobile privacy: Over 7 out of 10 apps collect more data than needed [EB/OL]. <https://www.techradar.com/computing/cyber-security/mobile-privacy-over-7-out-of-10-apps-collect-more-data-than-needed>. 2023-09-28/2024-08-27.

- [4] 徐伟,李文敏. 数智时代 App 收集个人信息的安全风险与法律应对[J]. 山东行政学院学报, 2025(1): 113 - 121. Xu W, Li W M. Security risks and legal responses to APP collection of personal information [J]. Journal of Shandong Academy of Governance, 2025(1): 113 - 121.
- [5] Myers Z. Shopping apps that share the most user data [EB/OL]. <https://cbs4indy.com/news/shopping-apps-that-share-the-most-user-data/>. 2024 - 01 - 02/2024 - 08 - 28.
- [6] Official Journal of the European Union. General Data Protection Regulation (GDPR) - legal text[EB/OL]. <https://gdpr-info.eu/>. 2018 - 05 - 25/2024 - 08 - 27.
- [7] Steinfeld N. "I agree to the terms and conditions": (how) do users read privacy policies online? An eye - tracking experiment[J]. Computers in Human Behavior, 2016, 55: 992 - 1000.
- [8] Fazlioglu M. IAPP privacy and consumer trust report - executive summary [EB/OL]. <https://iapp.org/resources/article/privacy-and-consumer-trust-summary/>. 2023 - 03/2024 - 08 - 27.
- [9] Watanabe T, Akiyama M, Sakai T, et al. Understanding the inconsistency between behaviors and descriptions of mobile Apps[J]. IEICE Transactions on Information and Systems, 2018, 101(11): 2584 - 2599.
- [10] Ahmad A. Ethical implications of artificial intelligence in accounting: A framework for responsible AI adoption in multinational corporations in Jordan[J]. International Journal of Data and Network Science, 2024, 8(1): 401 - 414.
- [11] 王俐智. 隐私政策“知情同意困境”的反思与出路[J]. 法制与社会发展, 2023, 29(2): 210 - 224. Wang L Z. Reflections on and solutions to the "informed consent dilemma" of privacy policy[J]. Law and Social Development, 2023, 29(2): 210 - 224.
- [12] Sunyaev A, Dehling T, Taylor P L, et al. Availability and quality of mobile health App privacy policies[J]. Journal of the American Medical Informatics Association, 2015, 22(e1): e28 - e33.
- [13] Ramanath R, Liu F, Sadeh N, et al. Unsupervised alignment of privacy policies using hidden markov models [EB/OL]. <https://aclanthology.org/P14-2099.pdf>. 2014 - 06 - 12/2025 - 03 - 12.
- [14] 高充彦,谢毅. 企业隐私政策的影响及其机制——基于用户视角的综述与展望[J]. 首都经济贸易大学学报, 2023, 25(5): 95 - 112. Gao C Y, Xie Y. The impact and mechanisms of corporate privacy policy——Literature review and research prospect from the user perspective[J]. Journal of Capital University of Economics and Business, 2023, 25(5): 95 - 112.
- [15] Chomanski B, Lauwaert L. Online consent: How much do we need to know? [J]. AI & Society, 2023: 1 - 11.
- [16] Meier Y, Schäwel J, Krämer N. C. The shorter the better? Effects of privacy policy length on online privacy decision - making [J]. Media and Communication, 2020, 8(2): 291 - 301.
- [17] Saeed S. A customer - centric view of e - commerce security and privacy [J]. Applied Sciences, 2023, 13(2): 1020.
- [18] Prichard J, Mentzer K. An analysis of APP privacy statements[J]. Issues in Information Systems, 2017, 18(4): 179 - 188.
- [19] Hjerpe K, Ruohonen J, Leppänen V. Extracting LPL privacy policy purposes from annotated web service source code[J]. Software and Systems Modeling, 2023, 22(1): 331 - 349.
- [20] Ibdah D, Lachtar N, Raparathi S M, et al. "Why should I read the privacy policy, I just need the service": A study on attitudes and perceptions toward privacy policies[J]. IEEE Access, 2021, 9: 166465 - 166487.
- [21] Iubenda. The need for privacy policies in mobile Apps - an overview[EB/OL]. <https://www.iubenda.com/blog/the-need-for-privacy-policies-in-mobile-apps-an-overview/>. 2013/2014 - 09 - 28.
- [22] Killingsworth S. Minding your own business: Privacy policies in principle and in practice[J]. Journal of Intellectual Property Law, 1999, 7(1): 57 - 97.
- [23] Hartzog W. Website design as contract[J]. American University Law Review, 2010, 60: 1635 - 1671.
- [24] Haley T D. Illusory privacy[J]. Indiana Law Journal, 2022, 98(1): 75 - 123.
- [25] Solove D J, Hartzog W. The FTC and the new common law of privacy[J]. Columbia Law Review, 2014, 114: 583 - 676.
- [26] Reidenberg J R, Russell N C, Callen A J, et al. Privacy harms and the effectiveness of the notice and choice framework[J]. I/S: A Journal of Law And Policy, 2015, 11: 485 - 524.
- [27] Li L, Chen J. What are the "Holes" in the App user agreement you haven't read? [EB/OL]. https://www.lwxsd.com/pcen/info_view.php?tab=mynews&VID=21873. 2022 - 03 - 17/2024 - 12 - 11.
- [28] Hosseini M B, Heaps J, Slavin R, et al. Ambiguity and

- Generality in Natural Language Privacy Policies [C]. 2021 IEEE 29th International Requirements Engineering Conference (RE). IEEE, 2021: 70 – 81.
- [29] Reidenberg J R, Bhatia J, Breaux T D, et al. Ambiguity in privacy policies and the impact of regulation [J]. The Journal of Legal Studies, 2016, 45 (S2): S163 – S190.
- [30] 孙晓宇, 叶斌. 人工智能“隐私”概念的困境 [J]. 自然辩证法研究, 2022, 38 (4): 61 – 66. Sun X Y, Ye B. The dilemma of the concept of “privacy” in artificial intelligence [J]. Studies in Dialectics of Nature, 2022, 38 (4): 61 – 66.
- [31] 曹博. 个人信息可识别性解释路径的反思与重构 [J]. 行政法学研究, 2022 (4): 133 – 144. Cao B. Reflection and reconstruction on the interpretation path of personal information identifiability [J]. Administrative Law Review, 2022 (4): 133 – 144.
- [32] China Briefing. The PRC personal information protection law (final): A full translation [EB/OL]. <https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/>. 2021 – 08 – 24/2024 – 09 – 13.
- [33] Westin A F. Privacy and Freedom [M]. New York: Atheneum Publishers, 1967: 119 – 131.
- [34] 张芷维. 隐私和个人信息的界分: 私密信息的司法判定标准 [EB/OL]. https://www.thepaper.cn/newsDetail_forward_21266319. 2022 – 12 – 22/2025 – 03 – 15. Zhang Z W. The boundary between privacy and personal information: Judicial criteria for determining private information [EB/OL]. https://www.thepaper.cn/newsDetail_forward_21266319. 2022 – 12 – 22/2025 – 03 – 15.
- [35] Mühlhoff R. Predictive privacy: Towards an applied ethics of data analytics [J]. Ethics and Information Technology, 2021, 23 (4): 675 – 690.
- [36] Solove D J. Introduction: Privacy self – management and the consent dilemma [J]. Harvard Law Review, 2012, 126: 1880 – 1903.
- [37] 李梦珂. 隐私政策视角下知情同意原则探析 [J]. 广东开放大学学报, 2022, 31 (1): 44 – 48. Li M K. On the principle of informed consent from the perspective of privacy policy [J]. Journal of Guangdong Open University, 2022, 31 (1): 44 – 48.
- [38] Kim K. Take these 5 steps to stop Apps from collecting your data now [EB/OL]. <https://www.pcmag.com/how-to/take-these-steps-to-stop-apps-from-collecting-your-data-now>. 2023 – 03 – 06/2024 – 10 – 09.
- [39] Adhikari A, Das S, Dewri R. Privacy policy analysis with sentence classification [EB/OL]. <https://ieeexplore.ieee.org/abstract/document/9851977>. 2022 – 08 – 18/2024 – 10 – 27.
- [40] Tangari G, Ikram M, Ijaz K, et al. Mobile health and privacy: Cross sectional study [J]. BMJ, 2021, 373.
- [41] Amos R, Acar G, Lucherini E, et al. Privacy Policies over Time: Curation and Analysis of a Million – document dataset [C]. Proceedings of the Web Conference, 2021, 2021: 2165 – 2176.
- [42] Sirota D. Beyond the privacy fine print: Making privacy more transparent [EB/OL]. <https://www.entrepreneur.com/article/294068>. 2017 – 05 – 10/2024 – 09 – 21.
- [43] Powell A, Singh P, Torous J. The complexity of mental health app privacy policies: A potential barrier to privacy [J]. JMIR MHealth and UHealth, 2018, 6 (7): e9871.
- [44] Reidenberg J R, Breaux T, Cranor L F, et al. Disagreeable privacy policies: Mismatches between meaning and users’ understanding [J]. Berkeley Technology Law Journal, 2015, 30: 39.
- [45] Trivedi J K. Cognitive deficits in psychiatric disorders: Current status [J]. Indian Journal of Psychiatry, 2006, 48 (1): 10 – 20.
- [46] Chinanews. “I have read and agree”? 70% of respondents rarely or never read the App user agreement [EB/OL]. https://www.tellerreport.com/life/2022-03-31-%22i-have-read-and-agree%22--70--of-respondents-rarely-or-never-read-the-app-user-agreement.BJzirl_GQq.html. 2022 – 03 – 31/2024 – 10 – 14.
- [47] Mühlhoff R. Predictive privacy: Collective data protection in the context of artificial intelligence and big data [J]. Big Data & Society, 2023, 10 (1): 20539517231166886.
- [48] Sun X, Ye B. Privacy preserving or trapping? [J]. AI & Society, 2024, 39 (3): 1369 – 1379.
- [49] Shaik T, Tao X, Li Y, et al. A review of the trends and challenges in adopting natural language processing methods for education feedback analysis [J]. IEEE Access, 2022, 10: 56720 – 56739.
- [50] Marotta – Wurgler F, Chen D L. Does contract disclosure matter? [with comment] [J]. Journal of Institutional and Theoretical Economics, 2012: 94 – 123.

- and a research agenda on interventions [J]. *Decision Sciences*, 2008, 39(2): 273 – 315.
- [29] 宋艳,陈琳,李琴,等. 人工智能伦理风险感知、信任与公众参与 [J]. *科学学研究*, 2022, 40(7): 1153 –

- 1162, 1171. Song Y, Chen L, Li Q, et al. AI ethical risk perception, trust and public participation [J]. *Studies in Science of Science*, 2022, 40(7): 1153 – 1162, 1171.

Analysis of the construction of the Metaverse "user base" from the agenda setting perspective: Research based on deep learning text analysis

CHENG Xu – sen, ZHANG Xiao – ling, XUE Tong, LEI Si – yu, YANG Bo

(School of Information, Renmin University of China, Beijing 100872, China)

Abstract: Based on the agenda setting theory and technology acceptance model, this research utilizes deep learning text analysis method to explore the state, causes and effective road to construct metaverse public cognition from the two levels of information transmission and reception. By analyzing the metaverse news and user's comments data from 2021 – 2023, this research reveals the meta – cosmic agenda communication is a game involving multiple agents, and the secondary communication of information by opinion leaders dominates the formation of public emotional cognition. The content of the media agenda does not coincide with the focus of public comment and contrary to the news, the sentiment of user comments is negative, which is due to the interaction of multiple external variables such as policy culture, which affect the perception of technological usefulness and ease of use. This paper analyzes the “user element” of meta – universe from multiple angles and at a deep level, which provides reference for the new quality productivity forces integration of meta – universe innovation and development, meta – universe policy formulation, product innovation and content publicity.

Key words: new quality productivity forces; Metaverse; technological innovation; public cognition; agenda setting

(上接第 660 页)

- [51] Axelsson M, Oliveira R, Racca M, et al. Social robot co – design canvases: A participatory design framework [J]. *ACM Transactions on Human – Robot Interaction (THRI)*, 2021, 11(1): 1 – 39.
- [52] Shneiderman B. Human – centered artificial intelligence: Three fresh ideas [J]. *AIS Transactions on Human – Computer Interaction*, 2020, 12(3): 109 – 124.

- [53] Shneiderman B. Human – centered artificial intelligence: Reliable, safe & trustworthy [J]. *International Journal of Human – Computer Interaction*, 2020, 36(6): 495 – 504.
- [54] Ozmen G O, Winslow B, Andolina S, et al. Six human – centered artificial intelligence grand challenges [J]. *International Journal of Human – Computer Interaction*, 2023, 39(3): 391 – 437.

Dilemma and resolution approaches of privacy policy in the context of intelligentization

SUN Xiao – yu, XIA Bao – hua

(Department of Philosophy and Science, Southeast University, Nanjing 211189, China)

Abstract: With the widespread adoption of artificial intelligence (AI) technology, ensuring the privacy of user data has become a significant research concern. Enterprises establish privacy policies to safeguard user data privacy. However, most of these policies exhibit several weaknesses, such as lack of transparency, opacity, unfairness, low practicality, and timeliness. Furthermore, they often overlook predictive private information provided by users. Consequently, these privacy policies are ineffective in protecting acquired privacy and may inadvertently violate predictive privacy, contradictory to their original intent, creating a privacy policy paradox. Drawing upon the human – centered AI framework, we suggest the development of human – centered privacy policies to address the challenges posed by current privacy policies effectively and ensure the data privacy security of users.

Key words: Artificial Intelligence; privacy policy; predictive privacy; Human Center