Dispute Settlement 争议解决, 2025, 11(5), 184-191
Published Online May 2025 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2025.115184

Hans汉斯

APP隐私协议的缺陷及对策探究

何米那

南京理工大学知识产权学院，江苏 南京

收稿日期：2025年4月22日；录用日期：2025年5月21日；发布日期：2025年5月30日

摘 要

随着数字经济的发展，APP市场呈现爆发式增长。各类应用程序涵盖了生活的方方面面，从社交类的微信、微博，到购物类的淘宝、京东，再到出行类的滴滴、高德地图等，用户数量庞大且使用频率极高。但发展的同时，也面临着诸多问题。国家计算机病毒应急处理中心多次公布存在隐私不合规行为的移动APP，2024年上半年全网监测到的数据泄露事件较2023年下半年增长60%。隐私协议对APP运营者处理用户个人信息的行为起着规范与约束作用，是APP实现合规运营必不可少的部分。然而，当下部分隐私协议存在诸多隐患，如隐私泄露风险较高、对未成年人等特殊群体个人信息的保护力度不足等。针对上述问题，本文提出双重规制路径：一方面，通过细化同意规则的分层适用、建立动态更新机制与增强协议可读性，重塑知情同意规则的法律效力；另一方面，构建包含监护人协同授权、数据使用限制等在内的未成年人保护体系。在此基础上，提出公私协作治理模式，论证了平台自律、行业标准、政府监管与公众参与协同作用的可行性，并设计了涵盖法律框架、技术支撑、监督体系的协同治理框架。通过多主体协同治理，方能破解APP隐私协议的制度困局，实现个人信息保护与数字经济发展的动态平衡。

关键词

隐私协议，知情同意，协同治理

Exploration of the Defects and Countermeasures of APP Privacy Agreements

Mina He

School of Intellectual Property, Nanjing University of Science and Technology, Nanjing Jiangsu

Received: Apr. 22nd, 2025; accepted: May 21st, 2025; published: May 30th, 2025

Abstract

With the development of the digital economy, the APP market has witnessed explosive growth. A wide range of applications cover all aspects of life, from social media platforms like WeChat and

文章引用: 何米那. APP 隐私协议的缺陷及对策探究[J]. 争议解决, 2025, 11(5): 184-191.
DOI: 10.12677/ds.2025.115184

Weibo to shopping platforms such as Taobao and JD.com, and even transportation platforms like Didi and Autonavi Maps. They have a huge user base and are used very frequently. But while developing, it also faces many problems. The National Computer Virus Emergency Response Center has repeatedly disclosed mobile apps with non-compliant privacy practices. In the first half of 2024, the number of data leakage incidents detected across the entire network increased by 60% compared to the second half of 2023. The privacy agreement plays a regulatory and restrictive role in the behavior of APP operators in handling users' personal information and is an indispensable part for apps to achieve compliant operation. However, at present, some privacy agreements have many hidden dangers, such as a relatively high risk of privacy leakage and insufficient protection of personal information of special groups such as minors. In response to the above problems, this paper proposes a dual regulatory approach: On the one hand, by refining the hierarchical application of consent rules, establishing a dynamic update mechanism and enhancing the readability of agreements, the legal effect of informed consent rules is reshaped; On the other hand, a protection system for minors should be established, including collaborative authorization by guardians and restrictions on data usage. On this basis, a public-private collaborative governance model was proposed. The feasibility of the synergy of platform self-discipline, industry standards, government supervision and public participation was demonstrated, and a collaborative governance framework covering the legal framework, technical support and supervision system was designed. Only through multi-subject collaborative governance can the institutional predicament of APP privacy agreements be broken, and a dynamic balance between personal information protection and the development of the digital economy be achieved.

Keywords

Privacy Agreement, Informed Consent, Collaborative Governance

1. APP 隐私协议的缺陷

1.1. 告知同意原则在实践中呈现出形式主义倾向

告知同意原则包括告知 + 同意两部分的内容。但就目前各大 APP 隐私协议来看，均存在无法有效告知和“绑架式”的同意问题。隐私政策是一种重要的信息披露方式，但是在实践中越发趋于形式化。首先，隐私政策通常内容冗长，并且晦涩难懂。随着我国对个人信息保护力度的不断加强与用户维权意识的提高，隐私政策的内容也逐步完善，篇幅也大幅增加。隐私政策的长篇大论中还夹杂着许多专业术语，即便是专业人士和技术人员，也很难短时间内完全理解其中的含义。尽管这些隐私条款都采用了加粗或下划线等形式引起用户注意，便于阅读。但是因为字数过多，用户很难把所有的注意力都放在隐私政策上，全部理解显然不现实[1]。有国外学者推算，如果要通读网络隐私政策，一个人平均每年需要大约 244 个小时。这还是在十年前，随着社会生活的全面数字化，各类物联网、智能家居收集个人信息的场景无处不在，隐私政策的复杂性、专业性更甚于以往[2]。此外，网络运营者为了满足立法要求及规避自身的法律风险，通常将隐私政策制定得“专业”“冗长”“繁琐”“晦涩”或“面目可憎”。在不具备专业知识的情况下，用户可能无法正确理解条款的含义，更遑论洞悉相关条款的内涵了[3]。以淘宝 APP、京东 APP 中的隐私协议为例，淘宝 APP 的隐私政策共有 15,450 字、京东 APP 的隐私政策共有 16,441 字，通常普通民众每分钟阅读量为 200~400 字，按此计算普通民众需要 39~82 分钟才能读完上述隐私协

议的内容。如果再考虑用户自身理解力所带来的偏差，所需时间可能更长。用户如果切实需要使用相关服务，只有一种选择即点击“同意”框。这种“同意”与真正意义上的心甘情愿、明明白白的“同意”差距甚远。就个人信息的采集与处理流程而言，APP 平台采集的个人信息往往经过多轮处理和分析，并在不同的信息处理主体间流转。在最初的收集阶段，知情同意原则还可能实现，但是在后续的多次流转阶段，再次落实知情同意原则就具有较大的经济成本和实际困难。除此之外，在个人信息收集和处理的每一个环节中，强制征得知情同意也会对个人信息的合法自由流动造成不利影响，对大数据相关产业的健康发展不利[4]。

1.2. 未成年人的个人信息保护条款成一纸空文

有学者对常见的 26 家网络平台企业应用程序 APP 隐私协议的内容进行比较，发现 26 家 APP 隐私协议均有对未成年人个人信息收集使用的相关规定。有的隐私协议的规定相对完善，如爱奇艺 APP 设有专门的未成年人隐私保护政策；有的隐私协议的规定则比较粗糙。以拼多多为例，《拼多多隐私政策》第 7 条规定，“我们非常重视未成年人的个人信息保护，在电子商务活动中我们推定您具有相应的民事行为能力。若您为 18 周岁以下的未成年人，请您及您的监护人仔细阅读本政策，并在征得您的监护人同意的前提下使用我们的服务或向我们提供信息”。再以购物平台为例，购物平台推出的有关未成年人的隐私政策内容依然有待考量。如得物、淘宝等 APP 隐私政策要求未成年人请监护人阅读政策，并且征得监护人同意使用服务和提供信息。通常情况下，未成年人是不会关注这条细则的，更不会请监护人一同阅读。也就是说，电商平台面对未成年人是否具有相应的民事行为能力考虑欠周，更遑论平台是否会采取积极手段确保未成年用户的使用已经取得了监护人同意[5]。

1.3. 大数据背景下的信息过度收集

APP 开发者凭借大数据、人工智能的技术赋能或赋权，在事实上与个人信息主体之间形成一种非对称的权力结构，数据处理者的权力与信息主体的权利呈现出非均衡性，显然数据处理者占据优势地位[6]。通过整合用户在使用过程中产生的碎片化数据，即使是与核心功能无直接关联的次要数据，也被纳入采集范畴。这对于 APP 使用者来说是不公平的，也在无形之中加剧了个人信息过度收集现象。更令人担忧的是，它还可能暗中采集用户的搜索历史，详细记录用户在 APP 内的每一次搜索行为，以及精准计算用户的使用时长，精确到分秒。收集完这些数据后，开发者会借助复杂的机器学习算法，精心构建出极为详尽的用户画像。如此一来，便能够实现精准广告投放，将各类广告精准无误地推送给目标用户。这种行为已然严重违背了数据最小必要原则[1]。更为严重的是，通过先进的数据挖掘技术，极有可能从这些看似平常的数据中，挖掘出用户潜在的健康状况、经济水平等高度敏感信息。有研究指出，APP 中包含的第三方服务提供商可以在用户没有察觉的情况下获取隐私信息[7]。这些被获取的隐私信息，如同一颗“定时炸弹”，对用户隐私构成极大的威胁，使得隐私泄露风险大大增加，也给用户的信息安全带来了前所未有的挑战。

2. APP 隐私协议的规制路径

2.1. 完善知情同意规则在 APP 隐私协议里的适用

首先，应当优化隐私协议的内容架构，降低隐私协议的理解难度。尽量使用通俗易懂的词语表达隐私协议的具体内容，文风应简洁、明快、易懂；关于不得不涉及的专业术语等内容，建议作出可理解的

[1] 参见《全国人民代表大会宪法和法律委员会关于〈中华人民共和国个人信息保护法(草案三次审议稿)〉修改意见的报告》，2021 年 8 月 20 日，http://www.npc.gov.cn/npc/c2/c30834/202108/t20210820_313091.html，最后访问日期：2024 年 12 月 2 日。

解释性说明[8]。此外，可以增加风险提示、应急预案措施等条款，通过这些条款向用户展示使用 APP 可能面临的风险以及网络平台为保障用户信息安全所采取的应急预案，以增强用户对个人信息收集和使用情形的知情权和合理预期[9]。

其次，应当避免默认勾选与强制同意，采取分步同意与弹窗提示的方式。确保用户同意隐私协议的操作是明确、自愿的，不能默认勾选“同意”选项，也不能以拒绝同意就无法使用 APP 等强制方式来获取用户同意，应给予用户充分的选择权，如设置“同意”与“拒绝”按钮，且按钮的表述应清晰明确，无歧义。对于涉及多种功能或不同类型个人信息收集的 APP，可以采用分步同意的方式，在用户使用到相应功能或需要收集特定信息时，再弹出隐私协议提示框，详细说明该功能或信息收集的相关情况，并请求用户同意，而不是在首次使用 APP 时一次性要求用户同意所有内容。当前大部分网络运营者采取“一揽子”计划式的“选择退出”模式，以减轻平台个人隐私信息维护的成本，增加信息商业活动的顺畅度。然而，个人隐私信息保护并不是一次性的买卖，知情同意原则不能降级为包山包海的“一揽子计划”，缺少协商机制的知情同意原则难谓权利与义务的对等。个人信息收集与使用的授权只有在充分尊重传播语境和技术发展的基础上才能发挥持续效用。因此，转换“选择退出”模式，构建“选择退出”+“选择进入”的可协商式同意模式显得尤为重要[10]。从用户的角度而言，这种模式促使用户更加关注自己的个人信息使用情况。因为用户需要自己做出“选择进入”的决策，他们就会更仔细地了解平台的隐私政策和信息收集方式。

2.2. 完善未成年群体的保护规定

隐私条款中大多将未成年人的年龄界定为 18 岁以下，大部分 APP 对未成年人使用产品或服务进行条款约束符合我国当前的法律精神，但这并不意味着排除了未成年人的使用风险，实践中仍然缺乏防止未成年人注册和使用产品和服务手段[11]。有学者认为，隐私政策披露机制应当在遵守既有法律规范的基础上，探索更为灵活多元的适合未成年人个人信息保护的机制。比如在年龄设定上，要重点保护不满 18 周岁的未成年人个人信息，并且通过行使删除权针对未成年人进行个性化的保护。同时也需要对监护人的权利行使进行有效规制和验证[12]。

APP 隐私协议对个人信息的采集应当采取限制收集原则，强调仅收集与提供服务直接相关且必要的数据。对于未成年人，需要更加谨慎地权衡数据收集的必要性。未成年人隐私具有极高的敏感性，因此在收集未成年人数据时，应当严格遵循最小化原则[13]，即仅收集为实现具体服务所必需的信息。与此同时，在征得同意的方式上，需详细说明如何获取未成年人及其监护人的同意。此外，对于不同年龄段有不同的要求，如对于低龄儿童可能需要监护人明确的书面同意，而对于青少年可以采用电子签名等方式。对于不满 13 周岁的未成年人，要求监护人通过填写专门的同意表格(可在 APP 内或官方网站下载)，并签字确认后，APP 才能收集相关数据。对于 13~17 周岁的未成年人，在收集敏感信息(如位置信息、健康数据等)时，可以通过弹窗提示，要求未成年人在获得监护人同意后，以电子签名的方式确认授权。此外，当数据泄露时也需有相应的应急响应机制。包括及时通知监护人、采取补救措施等。若发现涉及未成年人数据的泄露事件，应当在具体时间，如 24 小时内启动应急响应机制，立即采取技术手段阻止数据泄露的进一步扩大。同时，尽快通知未成年人的监护人[14]，告知泄露的数据内容、可能产生的风险以及正在采取的补救措施。

2.3. 推动企业自我约束与行业规范建设

在大数据浪潮席卷全球的当下，APP 作为用户接入数字世界的核心枢纽，其开发者的数据处理行为不仅直接关乎全球数十亿用户的信息安全、隐私权益等核心利益，更深刻影响着数字经济的健康发展与

行业创新的可持续性。当用户轻点屏幕完成 APP 安装的瞬间，实际上已将个人生活轨迹、消费偏好、健康状况等敏感数据的使用权悄然托付，而这些数据一旦被滥用，轻则导致精准骚扰、广告轰炸，重则可能引发身份冒用、金融诈骗等恶性事件。若任由数据处理乱象滋生蔓延，不仅会破坏公平竞争的市场秩序，更会扼杀行业创新活力，阻碍数字经济高质量发展。因此，引导 APP 开发者树立正确的数据伦理观显得尤为关键。

这一目标的达成，离不开行业协会的主动担当与深度参与。通过制定统一的数据收集自律公约，明确数据收集的边界与准则，使企业在操作时有章可循。同时，建立行业黑名单制度，对那些罔顾公约、肆意过度收集用户信息的企业，进行公示与严厉惩戒。此外，APP 运营者应积极响应自律号召，主动采用数据最小化收集方案。在 APP 设计的初始阶段，便将数据保护理念深度融入其中，而非事后补救；主动接受社会监督，定期发布详实的数据收集与使用报告，向用户清晰展示数据的采集范围、处理流程及最终去向，以公开、透明的运营模式提升用户信任度，从而在激烈的市场竞争中赢得用户的长期支持与青睐。

3. 基于 APP 隐私协议的思考：探索公私协作的治理模式

3.1. APP 隐私协议公私合作治理模式的可行性

技术的迅猛发展对 APP 治理提出了更加严苛的要求。其中，不仅需要政府等公共部门强化监管并提高治理能力，还需要重视平台等主体在 APP 治理中的作用。隐私协议作为规范 APP 运营的指南，其地位不容忽视。在行政干预以及市场自由化压力的不断博弈下，一种介于不受管制的市场与政府控制之间的第三条道路出现[15]，并逐渐演化为公私协同治理的新治理范式。因为没有任何一个公共或私人行为者能够拥有解决复杂动态和多样化问题所需要的所有知识和信息[16]，公私合作治理模式不否认政府治理的权威性，但也强调了私人主体在治理中的角色，倡导通过各方的共同协作来促进治理活动转化为各方共同解决问题的过程[17]。具体而言，公私协同治理模式不仅倡导多元主体平等参与来表达理性共识，也致力于推动信息要素、目标要素、规范要素等各治理要素之间的互通和共享，避免在权力互赖与自我赋能中出现价值和工具的迷失[18]。易言之，秉承公私融合理念的治理路径要求在规制私主体的经济权力时借鉴公法对公共主体规定的义务规则[19]。在 APP 隐私协议治理过程中，公私协同治理具有明显优势：公私合作治理模式通过整合政府、APP 开发者和用户代表等多方资源，显著提升 APP 隐私协议的治理效能。政府提供法律框架和制度保障，确保隐私协议符合公共利益和社会伦理。APP 开发者凭借技术专长，贡献创新方案，保障用户隐私安全。用户代表则反映实际需求，使协议更贴近用户期望。这种合作促进了隐私保护技术和服务模式的创新，平衡了各方利益，避免了过度监管和商业利益对隐私保护的忽视。同时，公私合作增强了 APP 隐私协议的社会信任和合法性，有利于 APP 行业的健康发展，促进数字生态系统的稳定与繁荣。此外，通过这种多维度的合作能够实现隐私保护与行业发展的双赢。

3.2. 公私合作治理模式在 APP 隐私协议中仍然面临着挑战

(1) 不同利益诉求的冲突

政府监管机构主要关注的是公共利益，即保障广大用户的隐私安全、维护市场秩序和社会稳定。我国政府部门既要充当个人数据政策的制定者和监管者，又要充当个人数据处理的直接参与者。仅靠目前的部门设置开展隐私治理工作仍然存在着一定的障碍和局限[20]。其目标是通过严格的法规和监督确保 APP 隐私协议符合法律标准，防止数据滥用。而 APP 开发者的利益诉求则更多地与商业利益相关。他们希望通过收集和利用用户数据来优化服务、进行精准营销以获取经济收益。对于开发者来说，过度限制数据收集可能会影响其产品的功能开发和商业竞争力。用户则侧重于个人隐私权益的最大化，要求 APP

开发者在收集、存储和使用数据的每一个环节都要保证透明度和用户的控制权。这种不同主体间利益诉求的巨大差异，使得在制定隐私协议时很难达成各方都满意的共识。

(2) 合作机制的复杂性

一方面，公私合作治理模式涉及多个利益相关者，这就导致在决策过程中需要考虑众多的意见和因素。在制定 APP 隐私协议时，政府、开发者和用户代表都需要参与决策，每一个条款的确定都可能需要经过反复的讨论和协商。另一方面，在公私合作治理模式下，当 APP 隐私协议出现问题，如隐私泄露事件发生时，责任界定可能会变得模糊不清。政府监管机构、APP 开发者和用户代表可能会相互推诿责任。责任界定的模糊性会直接影响问题的解决效率，也会削弱公私合作治理模式的公信力。

3.3. APP 隐私协议治理之公私协同治理的框架构建

首先，应当明确公私协同治理的主体。其中，政府监管部门应占据主导地位，工业和信息化部、国家互联网信息办公室等部门需制定宏观政策与法规，及时出台针对 APP 隐私协议内容规范的强制标准，明确告知同意原则的具体实施细则，规定隐私协议必须以显著且易懂的方式呈现关键信息，以保障用户能够真正理解并自愿同意。同时，网信办需承担监督 APP 运营者落实未成年人个人信息保护条款的责任，定期审查相关条款的合规性。行业协会在公私协同治理中应发挥承上启下的关键作用。一方面，其要协助政府部门解读政策，组织 APP 运营者参与培训，确保运营者准确理解并严格遵守相关规定；另一方面，应制定行业自律公约，例如互联网协会可牵头制定 APP 隐私保护自律准则，设立行业内的隐私协议示范模板，引导企业规范遵循[21]。此外，还需建立健全行业内部监督机制，对于违反自律公约的企业，给予警告、通报等相应处理。APP 运营者作为隐私协议的制定和实施主体，必须严格遵循法律法规与行业自律要求，积极投入资源优化隐私协议设计，采用通俗易懂的语言、可视化图表等形式展示隐私政策[22]，正如支付宝在隐私协议中以图文并茂的方式介绍数据收集与使用规则一般，以醒目的颜色和图标突出显示用户对自身数据的查询、更正、删除等权利，并配以详细的操作步骤截图和文字说明，引导用户便捷地行使这些权利，确保用户在需要时能够迅速找到并操作。除此之外，APP 运营者还应加强内部数据安全管理，针对未成年人个人信息，需设置专门的保护流程，如加密存储、限制访问权限等。此外，以数据安全评估中心为例的第三方机构也在公私协同治理中扮演着重要角色。数据安全评估中心可以运用专业的风险评估方法和工具，对 APP 的数据处理流程进行全面分析。例如，评估 APP 在数据收集环节是否采取了足够的安全措施，防止数据被非法获取；在数据存储环节是否采用了加密技术，确保数据的安全性；在数据使用和共享环节是否经过用户的明确授权等[23]。第三方检测认证机构可对 APP 隐私协议的合规性进行评估，像赛可达实验室等能够推出 APP 隐私协议合规认证服务，通过技术检测与内容审查，为符合规定的 APP 颁发认证标识。数据安全评估中心则可对 APP 数据处理活动进行风险评估，进而为政府监管和企业改进提供有力依据。

其次，需要注重不同治理主体之间的平等协商。在传统的风险规制中，通常的判断、评估、执行的主体都是行政机关，行政相对人、被监管主体以及公众等作为私主体则往往缺乏足够的参与渠道，只能发挥非常有限的作用。其原因在于，传统的公权规制的模式下，公权力机关与其他的私主体处在完全不对等的位置，许多能参与表达的私主体(如专家、相对人等)所提出的意见仅仅只能作为决策机关的参考，并不具有外部约束性。如此一来，公权力机关在执行相关的风险规制时常常并不在乎私主体的看法，参与治理的私主体成为了“有名无实”的摆设，这也进一步固化了传统风险规制中的公私二分局面在协商共治的背景下，所有治理主体在风险识别、沟通、执行等方面都需处在平等的地位上，只是不同主体在其中所发挥的作用有所不同[19]。在平等协商的基础之上，需要强化信息共享和透明度。信息共享和透明度是公私协同治理成功的关键。APP 开发者应定期向政府和公众披露其数据处理的详细情况，包括数据

的收集、使用、存储和共享方式。这种透明度不仅有助于建立用户信任，也是合规性的要求。有学者发现，一些智能招聘 APP 可以向求职者解释算法的筛选标准，让求职者知道自己为什么被选中或淘汰[24]。政府则应通过公开渠道，如官方网站和社交媒体，公布监管政策和执行情况，以增强公众对隐私保护工作的信任。透明度的提升也意味着对 APP 开发者的监督更为严格，这要求开发者在数据处理上更为谨慎和负责。

最后，APP 经营者应当制定灵活的响应和调整策略。隐私协议不应是一成不变的文档，而应是活生生的指南，能够反映最新的技术实践和市场趋势。定期对隐私协议进行审查和更新是确保其与时俱进、符合当前技术和法律要求的关键步骤。随着人工智能、大数据、云计算等前沿技术的发展，新的隐私保护挑战不断涌现。APP 经营者需要快速识别这些挑战，并及时更新政策和措施，以保护用户隐私免受新风险的威胁。治理框架的灵活性不仅体现在对技术变革的快速响应上，还应包括对市场趋势的敏感度。这意味着 APP 经营者需要持续监测市场动态，如用户行为的变化、竞争对手的策略、以及监管环境的调整，并据此调整隐私政策和实践，确保治理框架的长期有效性。同时也使得 APP 经营者能够在保护用户隐私的同时把握技术发展带来的机遇，维持竞争力和市场领导地位。通过这种前瞻性的治理策略，APP 经营者不仅能够满足当前的合规要求，还能够预见并适应未来的变化，从而在数字经济中保持可持续发展。

参考文献

[1] 李昕孺. APP 隐私政策的缺陷及完善[J]. 湖北经济学院学报(人文社会科学版), 2023, 20(3): 98-101.

[2] 丁晓东. 隐私政策的多维解读:告知同意性质的反思与制度重构[J]. 现代法学, 2023, 45(1): 34-48.

[3] 马新彦, 张传才. 知情同意规则的现实困境与对策检视[J]. 上海政法学院学报(法治论丛), 2021, 36(5): 99-109.

[4] 田野. 大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例[J]. 法制与社会发展, 2018, 24(6): 111-136.

[5] 王旭, 刘斌斌, 王嘉昌. 基于文本分析的 App 隐私政策框架优化研究——以购物类 App 为例[J]. 图书情报导刊, 2023, 8(1): 54-63.

[6] 陈林林, 严书元. 自动化决策中数据处理者的合理分析义务[J]. 吉首大学学报(社会科学版), 2022, 43(6): 19-28.

[7] 王新宇, 牛犇, 李凤华, 等. APP 隐私泄露风险评估与保护方案[J]. 通信学报, 2019, 40(5): 13-23.

[8] 朱光, 李凤景, 沈雨萌, 等. 社交媒体隐私政策的阅读意愿研究——基于 TAM 模型与自我效能理论视角[J]. 现代情报, 2022, 42(1): 150-166.

[9] 李晓磊, 邓丹. 网络平台企业隐私协议存在的主要缺陷及完善对策——以隐私协议知情同意条款为中心展开实证研究[J]. 辽宁师范大学学报(社会科学版), 2022, 45(5): 59-66.

[10] 范海潮, 顾理平. 探寻平衡之道: 隐私保护中知情同意原则的实践困境与修正[J]. 新闻与传播研究, 2021, 28(2): 70-85.

[11] 徐雷, 徐润婕. 移动 APP 隐私条款可获得性及内容分析研究[J]. 现代情报, 2020, 40(7): 82-91.

[12] 张基利, 康兰平. 电商平台中公民个人信息保护的规范路径探讨——基于 APP 隐私政策的实证研究[J]. 现代商贸工业, 2022, 43(21): 181-183.

[13] 王浩然, 施小垚. 大数据视域下未成年读者个人信息保护研究[J]. 南海法学, 2023, 7(4): 33-43.

[14] 曾霞. 大数据时代未成年人个人信息保护的困境与完善措施[J]. 楚天法治, 2023(14): 10-12.

[15] Lobel, O. (2012) New Governance as Regulatory Governance. In: Levi-Faur, D., Ed., *The Oxford Handbook of Governance*, Oxford University Press, 65-82.

[16] Eliassen, K.A. and Kooiman, J. (1993) Managing Public Organization. Sage Publications Ltd.

[17] Scott, J. and Trubek, D.M. (2002) Mind the Gap: Law and New Approaches to Governance in the European Union. *European Law Journal*, **8**, 1-18. https://doi.org/10.1111/1468-0386.00139

[18] 孙萍, 闫亭豫. 我国协同治理理论研究述评[J]. 理论月刊, 2013(3): 107-112.

[19] 毕文轩. 论电商平台知识产权的公私协同治理模式[J]. 上海交通大学学报(哲学社会科学版), 2024, 32(8): 68-81.

[20] 吴进进, 钱阳. 政府数字治理的隐私监管: 加拿大隐私专员制度的经验借鉴[J]. 贵州大学学报(社会科学版), 2023, 41(2): 45-56.

[21] 本刊编辑部. App 专项治理, 来自安全行业的建议[J]. 中国信息安全, 2019(4): 67-69.

[22] Diamantopoulou, V. and Pavlidis, M. (2017) Visual Privacy Management in User Centric Open Environments. 2017 11*th International Conference on Research Challenges in Information Science* (*RCIS*), Brighton, 10-12 May 2017, 461-462. https://doi.org/10.1109/rcis.2017.7956577

[23] 何艾星, 郑旭飞, 谢明天, 等. 面向 APP 应用的隐私合规的检测方法[J]. 人工智能科学与工程, 2024(1): 31-40.

[24] 雷渊智, 姜向阳. 人工智能招聘中个人隐私保护: 挑战、困境与出路[J]. 湖南行政学院学报, 2024(4): 18-27.