财经法学 No. 6，2026
pp. 176 - 190

系统级智能体场景中知情同意规则的过程化重构

刘浩锴*

内容提要：知情同意规则旨在保障个人在充分知情的基础上对具体处理事项作出自主选择。系统级智能体将用户的概括性指令拆解为连续任务，通过系统权限调用、跨应用执行和上下文留存，使个人信息处理随任务执行持续展开。以授权时相对确定的处理事项为基础的一次性告知与概括授权，难以充分回应后续处理关系的变化。场景完整性理论强调信息流转应符合特定场景的信息规范。应结合参与主体、信息属性和传输原则的变化，判断后续处理是否仍处于个人授权时已知悉并同意的处理范围之内。据此，知情同意规则应围绕处理关系的形成、变更与退出作过程化配置。告知规则应按信息流转变化对授权判断的影响程度分层配置告知方式；撤回规则应区分系统权限调用、任务记忆复用和外部接收后的处理关系，确定停止处理与留存清理的具体范围。

关键词：系统级智能体　知情同意规则　场景完整性理论　个人信息保护

一、引　言

知情同意规则是个人信息保护法治体系的重要基石。[1]《个人信息保护法》（以下简称《个保法》）第13条将“取得个人的同意”列为个人信息处理的合法性基础之一，第14条、第15条、第17条分别规定了同意的有效条件、同意撤回和处理前告知。依托上述制度安排，信息主体得以了解具体处理事项，并通过意思表示对相应处理作出授权、限制或终止。[2] 系统级智能体的兴起，使上述规则面临新的适用问题。系统级智能体，是指依托终端设备、操作系统层级权限

* 刘浩锴，浙江大学光华法学院博士研究生。

本文为教育部哲学社会科学重大专项“社会主义法治建设实践与中国自主法学知识体系构建研究”（2023JZDZ012）的阶段性研究成果。

〔1〕 参见齐爱民：《信息法原论》，武汉大学出版社2010年版，第58页。

〔2〕 参见于海防：《个人信息处理同意的性质与有效条件》，载《法学》2022年第8期，第112页。

或跨应用调用能力，能够持续感知外部环境、理解用户概括性指令并自动完成多步骤任务的智能体形态。〔3〕部分智能体深度嵌入手机、个人电脑等终端，以端侧智能体的形态完成系统权限调用和跨应用执行；〔4〕部分智能体虽依托云端模型，但通过取得终端权限、调用平台服务或插件工具，同样能够组织多应用任务链条并持续调取个人信息。〔5〕以 OpenClaw、腾讯 WorkBuddy、Kimi Work 等应用或服务为代表，智能体正在从单一应用内的辅助工具，转向能够组织多应用任务链条的“代理式执行”系统。〔6〕用户发出概括性任务指令后，智能体可以将其拆解为多个步骤，在不同应用或服务之间读取信息并执行操作。在这种运行结构中，个人信息处理逐渐呈现出跨应用、连续性、链条化的流转特征。处理事项和授权关系可能随任务执行而变化，个人对具体处理事项的知悉、同意及撤回也面临更高的不确定性。

目前，学界已注意到人工智能场景下知情同意规则的适用困境。相关研究分别从同意标准的动态调整、风险评估以及同意规则的类型化适用等角度，尝试修正传统知情同意规则在复杂数据处理场景中的适用方式。〔7〕与此同时，智能体研究也在近期迅速展开。有研究从分层治理角度分析自主智能体的本体层、交互层和生态层风险，〔8〕有研究讨论智能体跨平台代理执行对互联网竞争秩序和平台边界的影响，〔9〕也有研究围绕智能体自主行动中的责任分配、系统权限配置和人机关系重塑等问题展开分析。〔10〕这些研究为理解系统级智能体的运行特征及其法律影响提供了分析基础。不过，智能体的持续感知、跨应用执行和上下文留存等特征，如何影响告知事项的呈现、同意范围的确定及撤回要求的落实，仍需结合任务执行中的具体处理关系进一步阐明。

有鉴于此，有必要从智能体执行任务过程中持续变化的个人信息处理关系出发，重新理解知情同意规则的适用。场景完整性理论强调，应结合特定社会场景中的角色关系、信息属性和传输

---

〔3〕 参见陈天昊：《端侧智能体的监管定位、风险结构与规范构建》，载《东方法学》2026 年第 1 期，第 31－32 页；傅宏宇：《OpenClaw 类自主智能体的分层治理》，载《法律科学（西北政法大学学报）》2026 年第 3 期，第 48－49 页。

〔4〕 参见张欣：《端侧智能体的治理挑战与制度回应》，载《比较法研究》2026 年第 3 期，第 117－119 页。

〔5〕 参见肖潇、王俊：《详解智能体 2.0：手机里的“互联互通”新战场》，载《21 世纪经济报道》2026 年 2 月 27 日，第 7 版。

〔6〕 See OpenClaw，*OpenClaw*，OpenClaw Docs，https://docs.openclaw.ai/，visited on 8 September 2026；腾讯云：《WorkBuddy》，https://cloud.tencent.cn/product/workbuddy，2026 年 9 月 8 日访问；Kimi，*Kimi Work Overview*，Kimi，https://www.kimi.com/en/help/kimi-work/overview，visited on 8 September 2026.

〔7〕 参见赵祖斌：《从静态到动态：场景理论下的个人信息保护》，载《科学与社会》2021 年第 4 期，第 110－112 页；姬蕾蕾：《论同意规则在个人信息保护中的适用——以情景类型化为视角》，载《苏州大学学报（哲学社会科学版）》2022 年第 2 期，第 73 页；陈统：《生成式人工智能场景下“告知同意”规则的失效与重构》，载《大连理工大学学报（社会科学版）》2025 年第 4 期，第 79 页。

〔8〕 参见傅宏宇：《OpenClaw 类自主智能体的分层治理》，载《法律科学（西北政法大学学报）》2026 年第 3 期，第 53－54 页。

〔9〕 参见鲍奕含：《AI 智能体跨平台代理执行的竞争法评价》，载《法律科学（西北政法大学学报）》2026 年第 3 期，第 62－63 页。

〔10〕 参见付新华：《谁应为智能体的错误负责？——智能体自主行动的法理分析与责任分配》，载《中国法律评论》2026 年第 3 期，第 212－216 页；刘傲、王壹：《智能体“离身代理”中的主体性伪造与算法责任重构——基于系统级人机交互权限的现象学考察》，载《南昌航空大学学报（社会科学版）》2026 年第 1 期，第 38－40 页；李伟鑫：《OpenClaw 类 AI 智能体的实践转向及其哲学反思》，载《海南大学学报（社会科学版）》2026 年 5 月 25 日网络首发，https://doi.org/10.15886/j.cnki.hnus.202603.0365，2026 年 9 月 10 日访问。

原则，判断个人信息流动是否符合相应的规范期待。〔11〕借助这一框架，可以识别具体处理关系的变化，为确定告知内容、判断同意范围及识别撤回所涉的后续处理提供依据。在这一意义上，知情同意规则应围绕处理关系的形成、变更与退出作过程化配置，使个人授权与任务执行中的具体处理事项保持对应。

二、系统级智能体场景中知情同意规则的适用困境

知情同意规则通过告知、同意与撤回的连续安排，使信息主体得以理解个人信息处理事项，并对相应处理予以授权、限制，或者退出相关处理关系。系统级智能体依托持续感知、跨应用执行和上下文留存，使个人信息处理随任务执行持续展开，告知事项、同意范围和撤回对象也更难确定。这种变化带来的现实挑战，集中表现为处理前告知的有效性弱化、有效同意的形成受限以及撤回效果的延宕。

（一）持续感知下处理前告知的有效性弱化

告知义务的有效履行，是信息主体作出同意的认知前提。〔12〕《个保法》第 17 条要求个人信息处理者在处理个人信息前，以显著方式、清晰易懂的语言真实、准确、完整地告知处理目的、处理方式、处理的个人信息种类、保存期限以及个人行使权利的方式和程序等事项。该规则的运行预设在于，个人信息处理行为具有相对可识别的启动节点，处理目的、处理方式和信息种类能够在处理前被相对明确地说明，信息主体也能够据此判断是否接受后续处理。〔13〕然而，系统级智能体的持续感知机制，使这一预设受到明显挑战。

1. 处理前告知时点难以固定

在一般应用场景中，个人信息处理通常与特定功能启动、权限申请或服务调用相联系。用户开启定位、上传文件、绑定账户或使用支付功能时，信息处理者能够通过隐私政策弹窗、功能开启前的浮窗提示等方式，将告知行为嵌入个人信息收集和使用之前。此时，处理行为具有相对清晰的发生节点，处理者可以在启动处理之前完成告知。告知行为在此作为一种程序性阻断装置，为用户了解处理事项并作出授权判断提供了理性审视的空间。

然而，系统级智能体的持续感知机制改变了这一关系。为理解用户的概括性指令并完成多步骤任务，智能体通常需要持续识别屏幕内容、文件状态或应用界面，并结合上下文调整信息调用范围。〔14〕在此情形下，个人信息处理不再总是表现为用户主动触发后的单次采集，而可能伴随屏幕变化、文件调用、应用切换和任务拆解持续发生。〔15〕只要持续识别过程涉及联系人、通信

〔11〕 See Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2010, pp. 129 - 157.

〔12〕 参见郭旨龙、李文慧：《数字化时代知情同意原则的适用困境与破局思路》，载《法治社会》2021 年第 1 期，第 26 页。

〔13〕 参见郑佳宁：《知情同意原则在信息采集中的适用与规则构建》，载《东方法学》2020 年第 2 期，第 202 - 205 页。

〔14〕 参见施羽暇：《从豆包手机助手看我国端侧智能体发展面临的三大挑战》，载《中国电信业》2026 年第 1 期，第 39 页。

〔15〕 See Tianbao Xie et al., *OSWorld: Benchmarking Multimodal Agents for Open-Ended Tasks in Real Computer Environments*, in A. Globerson et al. eds., Advances in Neural Information Processing Systems 37, Curran Associates, Inc., 2024, pp. 52042 - 52043.

内容、账户状态、日程安排等可识别信息，便已落入个人信息收集、使用、分析等处理活动的范围。由此，个人信息处理呈现为连续过程，后续处理事项的动态变化使“处理前”告知难以仅固定于初始启动时点。更关键的是，持续感知并非单纯延长采集时间，而是将原本分散的信息读取、内容分析、应用调用等连成同一处理链条。告知规则若仍只以某一功能启动点为锚，便难以界定后续文件调用、应用切换在何种情况下已经构成处理事项的变更。

在持续感知过程中，若将每次界面更新、上下文读取或者应用切换均视为告知事项变更，用户将频繁面对碎片化提示，告知机制容易转化为交互负担，但如果仅在初始安装或首次启用时作概括性告知，后续持续感知所涉及的具体信息种类和处理方式又难以被用户实际理解。概括而言，告知规则以处理前说明为基本形式，但系统级智能体的个人信息处理已经逐步转化为连续识别和动态调用过程，传统告知时点难以完整覆盖后续信息流转。

2. 告知内容颗粒度的失衡

告知规则要求个人信息处理者在适当时点说明处理事项，也要求告知内容足以支持信息主体形成有效理解。〔16〕在一般应用场景中，处理事项通常围绕特定功能展开，处理者可以将告知内容限定在某一服务、某类信息和某种处理方式之内。系统级智能体围绕概括性指令生成任务链条的运行方式，使这一告知结构发生变化。同一项用户指令可能在不同应用、不同文件、不同账户和不同上下文之间展开，处理目的、处理方式和个人信息种类不再完全由某一单点功能预先决定，而是在任务执行过程中随着场景转换逐步组合形成。

以用户要求智能体“安排一次出行”为例，系统可能需要读取“日历”中的空闲时间，识别“聊天记录”中的同行人信息，调用交通、住宿和支付服务，并将行程结果写入“日程”。对于信息主体而言，其授权指令表面上指向“出行安排”这一任务，实际处理过程却可能涉及身份信息、位置偏好、消费能力、社交关系和行程计划等多类个人信息。上述处理事项未必能在用户发出指令前完整列明，而可能在智能体理解任务、拆解任务并调用相应应用的过程中逐步显现。处理前告知由此难以准确对应任务链条中实际发生的个人信息流转。

由此，处理前告知在完整披露与有效理解之间面临内容颗粒度的失衡。告知过细时，处理者需要列举大量可能发生的信息调用组合，告知文本容易膨胀为难以阅读的技术清单，信息主体反而难以识别真正影响自身权益的关键事项。告知过粗时，处理者容易诉诸“提升服务体验”“完成智能任务”等概括表述，处理目的和处理方式被抽象化，个人信息种类也无法对应到具体场景。申言之，处理前告知虽仍可通过隐私政策或弹窗提示等形式完成，但其对信息主体识别处理事项、判断处理风险并决定是否授权的支撑功能受到明显削弱。〔17〕

（二）跨应用执行对有效同意的削弱

同意规则要求处理者将相关处理限定于个人自愿、明确同意的范围之内。〔18〕《个保法》第

〔16〕 参见范海潮、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》，载《新闻与传播研究》2021年第2期，第74页。

〔17〕 See Daniel J. Solove，*Introduction*：*Privacy Self-Management and the Consent Dilemma*，126 Harvard Law Review 1880，1883－1888（2013）.

〔18〕 参见陆青：《个人信息保护中“同意”规则的规范构造》，载《武汉大学学报（哲学社会科学版）》2019年第5期，第123－126页。

14 条要求同意由个人在充分知情的前提下自愿、明确作出，第 23 条、第 29 条又分别对向其他个人信息处理者提供个人信息、处理敏感个人信息等事项设置单独同意要求。上述规则以相对清晰的处理结构为运行前提，即信息主体能够识别处理者、处理目的、处理方式和个人信息种类，并在高风险个人信息处理环节作出独立判断。系统级智能体进入跨应用执行场景后，用户的一项概括性任务指令可能被拆解为连续操作，并在多个应用、平台、模型服务和插件工具之间展开。〔19〕这使得个人信息处理从单点应用内的功能使用，转向围绕任务链条展开的连续流转。〔20〕在这一结构中，有效同意首先受到初始权限配置的挤压，并在任务执行过程中继续受到任务链条扩张的牵动。

1. 高权限配置压缩同意的选择空间

系统级智能体实现跨应用执行，通常需要取得屏幕读取、文件访问、无障碍服务等权限，〔21〕或获得应用接口、网络服务的访问授权。〔22〕这些权限和访问授权是执行任务的技术条件。服务方将其与个人信息处理同意集中设置时，个人对权限的选择也可能同时决定其接受何种信息处理。传统单一应用内的同意通常围绕某项功能、某类个人信息或者某一处理目的展开，信息主体尚可在相对清晰的处理事项之间作出差异化选择。系统级智能体的初始配置则倾向于将屏幕内容、通讯记录、日程信息、文件资料、位置轨迹、支付信息等后续可能触及的个人信息处理事项，集中到启用服务、绑定账户、开放接口或者安装插件等前端环节。

个人信息处理事项被集中到前端配置环节后，同意选择的精细程度随之下降。系统级智能体的运行，通常要求用户在任务开始前对系统权限、应用接口和第三方服务等要素一并作出选择。此时任务尚未展开，后续调用哪些应用、接触哪些个人信息、引入哪些个人信息处理者，仍取决于智能体对任务目标的分解与执行路径的生成，信息主体难以及时感知。在这种结构下，信息主体虽仍可在形式上拒绝启用相关服务，但可选择的对象已不再是具体个人信息处理事项，而是相关服务的整体启用及其权限配置。知情同意规则的功能，原本在于使个人能够围绕相对明确的处理事项形成授权判断。〔23〕当授权范围在前端被概括化，后续处理事项又随任务执行才可逐步显现时，同意授权便容易从差异化授权收缩为整体接受或拒绝。由此，信息主体作出的同意表示难以细致对应后续具体个人信息处理事项，同意的自愿性基础随之减弱。〔24〕

2. 任务链条扩张削弱单独同意的特定性

在任务执行阶段，系统级智能体的跨应用执行会将用户的概括性指令展开为连续任务链

---

〔19〕 参见付新华：《谁应为智能体的错误负责？——智能体自主行动的法理分析与责任分配》，载《中国法律评论》2026 年第 3 期，第 210 页。

〔20〕 参见李伟鑫：《OpenClaw 类 AI 智能体的实践转向及其哲学反思》，载《海南大学学报（社会科学版）》2026 年 5 月 25 日网络首发，https://doi.org/10.15886/j.cnki.hnus.202603.0365，2026 年 9 月 10 日访问。

〔21〕 See OpenClaw, *MacOS Permissions*, OpenClaw Docs, https://docs.openclaw.ai/platforms/mac/permissions, visited on 11 September 2026.

〔22〕 See OpenClaw, *Transports and OAuth*, OpenClaw Docs, https://docs.openclaw.ai/cli/mcp/transports, visited on 11 September 2026.

〔23〕 参见陈峰、王利荣：《个人信息“知情同意权”的功能检视与完善进路》，载《广西社会科学》2021 年第 8 期，第 107 页。

〔24〕 参见石超：《个人信息处理同意规则虚置化的理性矫正》，载《中国特色社会主义研究》2024 年第 1 期，第 97 页。

条。〔25〕例如，用户发出“预订机票并写入日程”之类的指令后，系统级智能体可能需要读取通信软件中的出行安排，在出行服务中提交旅客信息，在支付应用中完成扣款，在日历应用中写入行程，并将确认信息同步至邮箱或者即时通信软件。任务链条扩张会削弱单独同意所要求的特定性。〔26〕其一，任务执行过程会不断生成新的个人信息处理事项。出行安排的读取、旅客信息的填写、支付信息的提交、行程结果的同步和订单记录的留存，可能涉及不同的处理目的、处理方式和个人信息种类，也可能牵连不同的个人信息处理者。其二，用户初始指令与后续高风险处理环节之间并不完全对应。用户在起点处发出的概括性指令，能够说明其希望完成订票和日程同步任务，却难以当然覆盖执行过程中出现的敏感个人信息处理以及向其他个人信息处理者提供个人信息等事项。任务链条越长，单独同意的触发节点、对象范围和履行方式越难被固定在初始授权时点。

即便通过即时弹窗逐点取得确认，也难以充分保障单独同意的特定性。系统级智能体的执行过程具有连续性和高频性，若在任务链条的每一关键节点均中断执行并要求确认，单独同意容易从高风险处理事项的审慎判断转化为维持任务继续的程序性回应。信息主体的注意力在连续确认中被稀释，难以实际识别处理者、处理目的、处理方式和个人信息种类的变化，其点击同意更多是在保证服务可用和交互连贯。〔27〕因此，初始概括授权不足以承接后续全部高风险处理事项，逐点确认也未必能够恢复单独同意的实质功能。

（三）上下文留存对撤回效果的延宕

撤回同意规则承担着知情同意机制中的退出功能。《个保法》第15条赋予个人撤回同意的权利。个人撤回同意后，个人信息处理者不得再以原同意为根据继续处理相关个人信息。在传统应用场景中，撤回同意通常能够对应到相对明确的数据项、留存位置和后续处理环节，信息处理者也较易据此停止相关处理。与此不同，系统级智能体依赖上下文信息开展任务、生成响应并调整后续执行路径，既有个人信息及其衍生线索可能分散留存在多个运行环节。由此，撤回同意不再只是单次授权的终止，还涉及多层留存信息能否被识别、清除并限制其后续影响。

1. 多层留存结构削弱撤回对象的可确定性

落实撤回要求，需要明确其所指向的个人信息及相关处理活动。在传统应用场景中，撤回对象通常可以具体化为账户资料、上传文件、搜索历史、交易记录或者某类结构化字段。系统级智能体依赖上下文信息执行任务，交互过程中涉及的用户指令、文件内容和应用调用结果，除形成前端可见记录外，还可能在后台形成任务过程记录、偏好标签和索引记录等留存内容。部分场景中，这类留存还可能分布于终端、云端和应用服务等不同环节。〔28〕在这种留存结构中，即便显性记录被移除，撤回效果仍可能无法覆盖由同一信息生成的关联线索。以职业身份画像为例，信息主体撤回围绕“职业背景为律师”处理的同意后，系统级智能体未必继续保存该字段本身，但

〔25〕 参见裴冠雄：《自主智能体的潜在风险与安全治理》，载《社会科学报》2026年3月26日，第4版。

〔26〕 参见李川：《生成式人工智能场域下个人信息规范保护的模式与路径》，载《江西社会科学》2024年第8期，第70页。

〔27〕 参见常宇豪：《论信息主体的知情同意及其实现》，载《财经法学》2022年第3期，第88－89页。

〔28〕 参见朱明哲、胡懋地：《本地优先与端云协同：基于OpenClaw的AI智能体部署范式重构与治理》，载《科学观察》2026年第4期，第93－94页。

历史检索记录、常用法学术语、文档处理习惯和任务偏好仍可能共同指向相近的身份特征，并继续影响后续任务匹配、内容生成或者服务推荐。为达成撤回效果，个人信息处理者不能仅停止新增收集或者移除前端记录，还需判断哪些后台记录、偏好标签、索引结果和调用信息与该身份信息存在关联，哪些内容还会在后续处理中延续该画像判断。可见，在系统级智能体场景中，撤回同意的作用范围已由某条可见记录，延伸至围绕特定个人信息形成的关联性留存及其后续使用。

2. 后续推理影响削弱撤回的阻断功能

撤回同意所要实现的控制，不止于收回对个人信息处理的既有授权，还在于阻断基于原同意继续进行的相关处理。〔29〕系统级智能体在处理后续任务时，通常会利用既有交互中形成的上下文线索。信息主体先前留下的历史指令、交互反馈、偏好标签等，可能被用于解释后续指令、补充未明示事项或者影响处理结果。用户以概括性指令发起任务时，这些线索可能帮助系统补全任务条件；即使指令相对明确，既有偏好也可能影响执行安排乃至结果呈现。个人信息处理者停止新增收集并移除前端可见记录后，若上述线索仍被用于后续判断，相关个人信息便仍以判断依据的形式参与后续处理。此时，前端记录的移除和新增收集的停止，未能阻止相关个人信息继续用于后续推理，撤回的阻断功能因而受到削弱。〔30〕

在相关个人信息被纳入模型训练语料的场合，停止其后续使用还面临模型关联难以识别的技术障碍。个人信息在训练环节中可能由单条记录转化为语料之间的统计关联，并经由模型参数参与后续输出。系统级智能体所调用的模型通常通过训练语料提取自然语言统计规律，并将相关规律保存在大规模模型参数之中。模型参数支撑后续内容生成和任务响应，却不同于账户资料、日志记录或者索引结果中的某一条记录，开发者也难以准确识别特定个人信息在模型输出中的具体作用路径。〔31〕当用户交互信息进入模型训练后，撤回要求的落实便不只涉及原始语料或前端记录。移除原始语料或前端记录后，相关个人信息是否仍通过模型关联参与后续输出，以及其后续使用能否被阻止或限制，仍存在不确定性。

三、场景完整性理论下知情同意规则的规范重释

在既有网络服务实践中，处理者通常将告知与同意集中于初始授权环节。个人信息处理者在处理前告知个人信息种类、处理目的、处理方式等事项，个人也可以围绕较为清晰的处理安排作出取舍。系统级智能体使后续处理事项更难在初始授权时集中呈现。在系统级智能体场景下，用户的指令可能会触发跨应用、连续性的任务链条，处理事项中的个人信息种类、处理目的、处理方式以及参与处理的主体，均可能随任务执行过程逐步展开或发生变动。由此，以授权时点的一次性同意表示为中心的解释框架，已难以充分回应信息流转过程中的持续正当性问题。场景完整性理论将信息流转置于具体社会场景之中，关注信息由谁向谁流动、流动何种信息以及依何种传

〔29〕 参见万方：《个人信息处理中的“同意”与“同意撤回”》，载《中国法学》2021 年第 1 期，第 175 页。

〔30〕 参见王苑：《中国语境下被遗忘权的内涵、价值及其实现》，载《武汉大学学报（哲学社会科学版）》2023 年第 5 期，第 165－166 页。

〔31〕 参见黄镝：《生成式 AI 对个人信息保护的挑战与风险规制》，载《现代法学》2024 年第 4 期，第 105－106 页。

输原则展开，并据此判断该流转是否符合场景中的规范期待。〔32〕以此观之，知情同意规则的解释重心应从授权时点的形式确认，转向信息流转过程及其场景适当性的判断。

（一）单次授权模式的解释限度

在处理事项相对确定的网络服务中，处理前告知与授权时同意通常围绕同一授权时点开展。个人信息处理者在处理前通过隐私政策、权限申请或者弹窗提示，呈现处理目的、处理方式、处理的个人信息种类、可能的接收方以及对个人权益的主要影响。个人再以勾选、点击确认等方式作出明确同意。〔33〕这种以授权时点统合处理前告知与同意表示的规则适用形态，可以概括为单次授权模式。处理者在授权时充分呈现上述事项，个人才能理解同意所覆盖的范围，处理者也才能以同意记录证明其取得相应处理依据。《个保法》第14条第1款关于充分知情、自愿、明确的要求，也将同意效力系于个人对特定处理事项的理解和选择。〔34〕个人无需掌握全部技术实现细节，但应能够理解其同意所指向的处理事项、信息流向和对个人权益的主要影响。由此可见，单次授权模式的适用空间，限于处理事项能够在授权时被集中呈现并保持相对稳定的情形。

然而，在系统级智能体执行任务时，处理事项往往随任务链条逐步生成，难以在授权时一次性呈现。例如，用户发出“整理报销材料”“订票并调整日程”“处理邮件并同步到日历”等指令时，用户能够明确的主要是任务目标或预期结果，具体的信息读取、应用调用等尚未充分展开。在该类任务中，系统级智能体通常不再局限于单一应用内部处理，而可能借助操作系统层级权限，通过屏幕识别、模拟点击等方式，在多个应用或服务之间连续执行。为推进任务，智能体需要读取不同来源的信息、调用相关应用或服务，并根据执行结果调整后续操作。相应的处理目的、处理方式、处理的个人信息种类和参与处理的主体，往往难以在授权时一次性列明，而要在任务执行过程中才能逐步显现。授权时作出的同意，只能覆盖个人已经充分知悉并明确同意的处理事项。智能体任务执行中新增的信息类型、应用调用等情况，仍需重新接受同意规则的检验。

个人同意的效力范围，应与其所指向的具体处理事项保持对应。《个保法》第14条第2款、第15条、第17条和第23条分别从处理事项变更、同意撤回、处理前告知以及向其他个人信息处理者提供个人信息等方面，维持同意效力与处理事项之间的对应关系。处理目的、处理方式或者处理的个人信息种类发生变化时，处理者应重新取得个人同意。个人撤回同意后，处理者不能继续以原同意作为处理依据。个人信息被提供给其他个人信息处理者时，也应围绕接收方和后续处理事项取得单独同意。这些安排共同限定了同意效力的延续范围。后续处理能否继续由原有同意覆盖，取决于其是否仍处于个人已经知悉并作出同意决定的处理范围内。个人信息处理从收集延伸至使用、提供和删除等环节，不同环节均可能影响同意的成立、延续和退出。〔35〕后续处理超出授权时已经呈现的处理范围时，既有同意便难以继续支撑相应处理。申言之，单次授权模式

〔32〕 See Helen Nissenbaum，*Privacy as Contextual Integrity*，79 Washington Law Review 119，136－143（2004）.

〔33〕 参见王叶刚：《论网络隐私政策的效力——以个人信息保护为中心》，载《比较法研究》2020年第1期，第129－130页。

〔34〕 参见高志宏：《大数据时代“知情—同意”机制的实践困境与制度优化》，载《法学评论》2023年第2期，第118－119页。

〔35〕 参见夏庆锋、戴媛媛：《个人信息处理同意规则的动态场景化完善》，载《安徽大学学报（哲社版）》2025年第5期，第118－122页。

主要依赖初始表示确定授权边界，因而难以及时回应系统级智能体任务执行中处理关系的持续变化。

（二）信息流转关系的场景化判断

单次授权模式的解释限度，集中表现为授权时点难以完整界定系统级智能体任务执行中的后续信息流转关系。个人曾作出同意表示，主要说明针对相应处理事项的授权关系已经形成。后续处理能否继续由原有同意支撑，应判断其是否仍处于个人授权时已知悉并同意的处理范围内。场景完整性理论以信息在特定社会场景中的适当流动为核心，能够为这一判断提供分析框架。〔36〕有学者以“场景相对的信息规范”说明信息流动的适当性，并以参与主体、信息属性和传输原则等变量刻画特定场景中的信息流动。〔37〕在知情同意规则的解释中，参与主体对应信息主体、个人信息处理者、受托人、接收方等在信息流转中的角色，信息属性对应个人信息种类及其敏感程度，传输原则对应限定用途、保密或经同意流转等条件。合理预期则需结合场景中的角色分工与信息流转规范加以判断，用以校验后续处理是否仍属原同意范围。〔38〕

系统级智能体中的信息流转，往往呈现出任务执行连续与处理关系分化并存的特征。用户发出概括性指令后，智能体可以借助系统层面的操作能力，通过界面识别和模拟用户操作在不同应用或服务之间推进任务，并将分散操作纳入同一任务链条。在这一过程中，相关信息的后续处理是否仍处于原授权范围内，应结合任务目的、信息属性、接收主体、传输原则以及后续用途加以判断。例如，用户要求智能体向朋友发送会议地址时，通讯录信息主要服务于联系目的。智能体根据联系人关系生成客户画像时，同一通讯录信息则进入关系评价、画像生成和商业利用范畴。定位信息用于导航、打车和营销推荐时，也分别对应路径指引、出行履约和商业推送。同一种类的个人信息因处理目的、接收主体或者后续用途不同，所适用的信息流转规范也可能有所不同。〔39〕相关信息是否仍服务于原任务、接收主体及其角色是否仍为原授权所涵盖、后续用途是否仍受原任务目的约束，构成判断信息流转关系是否变化的基本界限。

个人在同意时形成的合理预期，可以辅助判断后续处理是否仍处于原授权范围。〔40〕个人的合理预期通常围绕任务目的、实现该目的所需的处理安排、所处理个人信息的种类和敏感性、信息的基本流向，以及相关处理可能对个人权益产生的主要影响形成，原有同意能够覆盖的处理关

〔36〕 已有研究将场景完整性理论用于个人信息保护，但该理论在系统级智能体场景中的具体适用仍有进一步展开的空间。参见李文姝、刘道前：《人工智能视域下的信息规制——基于隐私场景理论的激励与规范》，载《人民论坛·学术前沿》2019 年第 6 期，第 74－75 页；赵祖斌：《从静态到动态：场景理论下的个人信息保护》，载《科学与社会》2021 年第 4 期，第 99－102 页；王苑：《目的限制原则的反思及其解释论构造——以〈个人信息保护法〉第 6 条第 1 款为中心》，载《华东政法大学学报》2024 年第 4 期，第 51－53 页；杜佳璐：《场景完整性视域下已公开个人信息处理的合理范围界定》，载《数字法治》2026 年第 1 期，第 74－75 页；王海洋：《个人信息保护中场景理论的反思与修正》，载《山东师范大学学报（社会科学版）》2026 年第 4 期，第 159－161 页。

〔37〕 See Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2010, pp. 140－150.

〔38〕 参见〔美〕海伦·尼森鲍姆：《何为场景？——隐私场景理论中场景概念之解析》，王苑译，载《网络信息法学研究》第 9 期，中国社会科学出版社 2021 年版，第 14－16 页。

〔39〕 参见刘浩锴、张峻通：《场景理论下教育数据的分类分级治理进路》，载《现代教育技术》2026 年第 5 期，第 80－81 页。

〔40〕 参见李金玉：《我国个人信息利用中利益平衡保护的优化路径》，载《陕西行政学院学报》2025 年第 3 期，第 55－56 页。

系也应在这一范围内确定。以“从聊天记录中提取会议时间”为例，读取与会议时间相关的片段、生成日程并向本人提醒，通常仍处于该任务所形成的预期范围内。后续处理继续分析聊天关系并形成联系人画像时，其用途和权益影响便会超出提取会议时间这一任务。若相关结果同步至商业推荐服务，接收主体和信息流向也随之实质改变。处理者主张后续处理仍受原有同意支撑，应说明相关信息与原任务之间的必要关联、接收主体及其角色，以及后续使用对个人权益的影响。概言之，个人作出同意时的合理预期，是判断后续处理是否仍属于同一信息流转关系的重要依据。

（三）信息流转过程中的告知、同意与撤回规则分工

在场景完整性理论下，个人信息处理行为应当置于具体信息流转关系中加以考察。〔41〕系统级智能体在跨应用执行任务时，可能因权限调用、第三方服务接入等环节改变信息流转关系，使处理目的、处理方式，处理的个人信息种类、信息接收方或者后续处理安排发生实质变化。告知、同意与撤回规则的适用，也应与处理关系的形成和变化保持对应，以维持个人授权的特定范围。

告知规则指向个人对任务执行中信息流转关系及其变化的识别。《个保法》第 17 条要求个人信息处理者在处理个人信息前，以显著方式、清晰易懂的语言，真实、准确、完整地向个人告知法定事项，其中包括个人信息的处理目的、处理方式，处理的个人信息种类、保存期限以及个人行使权利的方式和程序。系统级智能体跨应用执行任务时，处理路径常在授权后逐步展开，个人信息可能因权限调用、第三方服务接入等节点进入新的处理关系。第 17 条所要求的真实、准确、完整告知，在系统级智能体场景中应覆盖授权后发生的法定告知事项变更。告知内容需要呈现上述变化，使个人能够理解信息流转关系已经发生何种调整，并据此作出相应决定。

同意规则承接告知所形成的识别基础，用于确定特定处理能否纳入个人授权范围。〔42〕《个保法》围绕处理事项变化和处理风险差异设置不同同意要求，以限定同意能够覆盖的处理范围。其中，第 14 条第 2 款对应处理目的、处理方式和个人信息种类变更后的重新同意，第 23 条对应向其他个人信息处理者提供个人信息时的单独同意，第 29 条对应处理敏感个人信息时的单独同意。这些规则共同说明，同意的覆盖范围应限定于个人已经知悉并作出同意决定的具体处理关系。

撤回规则处理个人退出后续处理关系的问题。《个保法》第 15 条确认个人有权撤回同意，并要求个人信息处理者提供便捷的撤回方式。撤回前基于同意进行的处理不因撤回当然失效，撤回后的相关处理不能继续依赖撤回前的同意。〔43〕系统级智能体跨应用执行任务时，个人信息处理往往延伸至任务继续执行、系统权限调用、任务记忆保存以及第三方服务继续处理等后续环节。处理者应结合仍在执行的任务、持续调用的权限、继续保存或复用的任务记忆，以及向第三方提供信息后的处理关系，确定撤回事项所涉的后续处理。涉及任务记忆或者相关个人信息留存的，

〔41〕 参见罗澍、杨正杰：《场景理论视域下知情同意原则的反思与出路》，载《重庆邮电大学学报（社会科学版）》2026 年第 2 期，第 45 页。

〔42〕 参见武腾：《人工智能时代个人数据保护的困境与出路》，载《现代法学》2024 年第 4 期，第 121 页。

〔43〕 参见傅雪婷：《个人信息同意撤回与个人数据对价化》，载《南大法学》2022 年第 5 期，第 18 页。

还应与第 47 条关于撤回同意后删除的规则相衔接。〔44〕个人撤回同意后，处理者不得继续以撤回前的同意为依据收集、存储、使用、加工、传输或者提供相关个人信息。处理相关个人信息并非提供产品或者服务所必需的，处理者还不得以撤回为由拒绝或者停止提供产品或服务。由此，告知、同意与撤回共同维持个人同意与特定个人信息处理关系之间的对应。

四、系统级智能体场景中知情同意规则的过程化配置

系统级智能体对知情同意规则的冲击，集中呈现为任务执行过程中信息流转关系的持续变化。按照场景完整性理论，个人信息流动是否适当，应结合参与主体、信息属性和传输原则，判断其是否符合相应场景中的信息规范。〔45〕由此，知情同意规则应围绕信息流转关系的形成、变更与退出作过程化配置。告知规则保障个人知悉处理事项及其变化，同意规则明确后续处理能否由原同意覆盖的判断标准，撤回规则要求处理者停止撤回事项所涉的后续处理，并依法删除相关个人信息或限制其后续处理。

（一）信息流转变化的告知规则配置

系统级智能体场景中的告知规则，应围绕法定告知事项的变化，形成过程化的告知节点配置。《个保法》第 17 条关于处理前告知和事项变更告知的要求，应落实到任务执行中处理关系形成和变化的具体环节。处理者新增个人信息种类、改变处理方式、新增接收主体，或者将任务信息转入后续用途时，应在相关处理实施前，使个人能够识别变化内容及其与当前任务目的之间的关系。处理者不能仅凭初始授权记录，主张其已经就后续法定告知事项的变更履行了告知义务。

告知内容的配置，应以《个保法》第 17 条列明的处理者身份、处理目的、处理方式、个人信息种类、保存期限和权利行使方式等事项为基础，并将其具体化为特定任务中的处理关系说明。处理者应说明何种个人信息因何种任务目的被调用，由谁处理，向谁流动，是否进入其他应用、云端服务或者后续使用环节，以及相关处理可能对个人权益产生何种影响。模型推理、界面自动化和权限调用不必被展开为完整技术说明，但由此引起的处理目的、处理方式、信息种类或接收主体变化，应在告知中具体说明。在个人信息种类方面，智能体调用通讯录、聊天记录、日程、定位、支付信息等不同类型信息时，告知内容应说明该信息与当前任务目的之间的必要关联。在处理主体和后续用途方面，同一信息流向新的接收主体，或者被用于模型训练、商业画像等后续处理时，告知内容还应呈现接收方、后续用途和保存安排。涉及敏感个人信息的，处理者还应依《个保法》第 30 条说明处理的必要性以及对个人权益的影响。

告知方式应根据信息流转变化对个人授权判断的影响程度形成分层配置。〔46〕在系统级智能体场景中，《个保法》第 17 条关于显著方式和清晰易懂语言的要求，可以通过不同提示设计落实

〔44〕 参见程啸：《论〈个人信息保护法〉中的删除权》，载《社会科学辑刊》2022 年第 1 期，第 108－109 页。

〔45〕 See Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Washington Law Review 119, 153－154 (2004).

〔46〕 See Florian Schaub et al., *A Design Space for Effective Privacy Notices*, in Eleventh Symposium on Usable Privacy and Security (SOUPS 2015), USENIX Association, 2015, p. 5.

到任务执行过程之中。〔47〕其一，个人已经充分知情并有效同意，后续处理仍在原同意范围内的，告知方式可以保持低干扰。此时，处理者可以通过任务状态提示或者权限调用标识，说明当前任务正在调用何种信息，以维持任务运行过程的可见性。其二，跨应用读取、外部服务传输等操作改变信息流向或参与主体时，处理者应通过强化提示说明变化内容。处理者应在任务节点中呈现信息流向、接收方身份及其处理角色，使个人能够识别后续处理由谁参与、信息向何处流动。其三，涉及尚未授权的敏感个人信息处理、处理目的变更或超出原同意范围的任务信息后续利用时，告知方式应转为阻断式告知。〔48〕依法需要重新取得同意或者取得单独同意的，处理者应先完成相关告知并取得相应同意，再实施相关处理。

（二）授权范围变动的同意规则配置

系统级智能体场景中的同意规则，应围绕具体处理事项与个人授权范围之间的对应关系展开。系统级智能体可以将一项任务指令展开为连续处理链条，后续处理是否仍处于原授权范围内，应依处理目的、处理方式、个人信息种类、接收主体和后续用途等场景要素的变化加以判断。处理关系仍在原同意范围内的，原同意可以延续；处理目的、处理方式或者个人信息种类发生变更的，应重新取得同意；法律要求单独同意的处理事项，则应取得单独同意。

原同意能否延续，应以个人已经充分知悉并同意的处理事项为基准。个人已对完成既定任务所需的处理作出有效同意，且后续操作未超出该范围的，原同意可以延续。〔49〕处理目的、处理方式和个人信息种类均未发生变更，且未新增独立接收主体的，相关信息的提取、调用等可以随任务执行继续处于原授权范围内。例如，个人要求智能体整理日程、检索本地文件或者生成报销清单时，系统为排序日程事项、定位本地文件或者提取票据要素而调用相应信息，仍属完成既定任务所必要的处理。任务链条的连续运行和个人对任务结果的期待，并不能当然延续授权范围。在连续执行过程中，处理目的、个人信息种类、接收主体或者任务外后续用途发生变化，并使后续处理超出原同意覆盖事项的，应认定为处理关系已经发生实质变化。〔50〕处理者主张原同意延续的，应能够说明后续处理与既定任务之间的必要关联，并以相应记录证明授权范围未发生实质改变；不能作出说明的，应转入重新同意或者单独同意的判断。

其中，重新取得同意适用于处理目的、处理方式或者个人信息种类发生变更的情形。〔51〕《个保法》第 14 条第 2 款要求在处理目的、处理方式或者个人信息种类发生变更时重新取得个人同意，第 17 条第 2 款则要求处理者将告知事项的变更部分告知个人。可见，重新同意应围绕已经向个人告知的变更事项展开。〔52〕是否发生变更，应以原先已经充分告知并取得有效同意的处理

〔47〕 参见夏庆锋：《网络空间个人信息保护的通知义务完善与动态匿名化》，载《江汉论坛》2022 年第 3 期，第 101－102 页。

〔48〕 参见石佳友、刘思齐：《人脸识别技术中的个人信息保护——兼论动态同意模式的建构》，载《财经法学》2021 年第 2 期，第 73 页。

〔49〕 参见田野：《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》，载《法制与社会发展》2018 年第 6 期，第 121 页。

〔50〕 参见宁园：《个人信息保护中知情同意规则的坚守与修正》，载《江西财经大学学报》2020 年第 2 期，第 124－125 页。

〔51〕 参见何晓斌：《个人信息保护中告知同意的开放结构及其公法实现》，载《行政法学研究》2023 年第 1 期，第 146－147 页。

〔52〕 参见贺彤：《个人信息数据的权利界定》，载《大连理工大学学报（社会科学版）》2025 年第 4 期，第 88 页。

事项为基准。在连续任务中，实质变更通常表现为任务目的延展、处理方式替换或者信息种类扩大。〔53〕例如，个人授权智能体从聊天记录中提取会议时间，所形成的同意范围通常限于会议时间提取。智能体进一步分析联系人关系并形成画像的，处理目的已经发生变化，相关处理即超出个人原同意所覆盖的授权范围。〔54〕处理者重新取得同意时，应使个人能够针对变更后的处理事项作出继续授权、拒绝处理或者收窄任务范围的选择。个人选择继续授权的，后续处理只能在变更后的同意范围内继续；个人拒绝或者收窄授权的，处理者应停止或者调整相应处理。

基于个人同意处理个人信息时，单独同意的适用应以《个保法》明确列明的特定处理事项为界。〔55〕在系统级智能体任务执行链条中，向其他个人信息处理者提供个人信息和处理敏感个人信息，是单独同意配置的两个重点事项。向其他个人信息处理者提供个人信息的判断，应从接收方在具体信息流转关系中的角色展开。服务方依处理者约定处理个人信息，且不自主决定处理目的、处理方式的，相关处理适用第 21 条委托处理规则，处理者应通过委托约定和监督义务控制受托处理范围。服务方接收个人信息后自主决定处理目的、处理方式的，处理者向其提供个人信息应依第 23 条取得个人的单独同意，并向个人告知接收方名称或者姓名、联系方式、处理目的、处理方式和个人信息种类。据此，系统级智能体接入订票、支付、地图、办公协作或者云端模型等外部服务时，处理者应先识别服务方是否能够自主决定接收后的处理目的、处理方式，再确定是否需要取得第 23 条所要求的单独同意。处理敏感个人信息时，单独同意的触发依据在于处理事项涉及第 28 条意义上的敏感个人信息。智能体调用生物识别、金融账户、行踪轨迹等敏感个人信息的，处理者应依第 29 条取得个人的单独同意，并依第 30 条说明处理必要性及其对个人权益的影响。

（三）后续处理停止的撤回规则配置

系统级智能体场景中的撤回规则，应以个人退出撤回事项所涉后续处理关系为重心。《个保法》第 15 条规定，撤回不影响此前基于同意已进行的处理活动的效力。撤回后的相关处理，则不能再以原同意为依据。〔56〕系统级智能体执行任务时，个人信息处理会随任务步骤分布于系统权限、任务记忆和外部服务衔接之中，初始授权记录主要反映个人曾经作出的同意，难以显示撤回后相关信息是否仍被继续读取、复用或者向外流转。因此，第 15 条确立的时间界限，应落实到撤回事项所涉的信息流转关系，使撤回后的相关处理不再继续依赖撤回前的同意。

撤回方式是否符合《个保法》第 15 条的便捷要求，应同时考察撤回对象是否明确、撤回意思能否作用于相应的信息处理环节。系统级智能体执行任务时，撤回事项所涉个人信息往往随任务执行、系统权限调用、任务记忆留存等环节延续。其一，撤回事项涉及正在执行的任务时，相关信息的读取、整理或者传输仍直接服务于该特定任务。撤回方式应使个人能够针对该任务退出

〔53〕 参见陈龙江、陈佳文：《由静态到动态：脑机接口技术下知情同意规则的完善》，载《河南社会科学》2026 年第 4 期，第 87 页。

〔54〕 参见廖丽环：《个人信息处理中同意规则弱化适用的路径优化——基于情境脉络完整性理论的场景细分》，载《法制与社会发展》2022 年第 6 期，第 177 页。

〔55〕 参见王叶刚：《个人信息处理中的个人明确同意》，载《中国应用法学》2025 年第 2 期，第 156－158 页。

〔56〕 参见肖冰、刘冠合：《个人信息同意撤回权之“任意性”辨析》，载《南京大学学报（哲学·人文科学·社会科学）》2025 年第 5 期，第 57 页。

后续处理关系。其二，撤回事项涉及系统权限调用时，相关权限可能在不同任务之间持续发挥作用。通讯录、定位、日程、文件等权限一经开启，智能体后续任务仍可能据此访问相关个人信息，撤回方式应使个人能够针对特定权限退出持续调用关系。其三，撤回事项涉及任务记忆时，相关信息可能在当前任务结束后继续被使用。已经形成的任务记忆若继续用于后续推理、个性化推荐或者任务偏好识别，撤回方式应使个人能够针对记忆中相关信息的后续使用作出撤回。

个人撤回同意后，处理者应停止撤回事项所涉后续处理。系统级智能体执行任务时，相关信息可能处于任务执行、系统权限调用、任务记忆复用以及外部主体接收后的处理关系之中。处理者应按照这些处理关系分别停止相应处理。其一，相关信息仍用于正在执行的任务时，处理者应停止在该任务中继续读取、调用或者传输撤回事项所涉个人信息。任务能够在剥离该项个人信息处理后继续完成的，处理者可以调整任务范围。该任务的完成以处理撤回事项所涉个人信息为必要条件，且处理者不能另行取得合法处理依据时，应终止相应任务。其二，处理者通过系统权限继续读取或者调用撤回事项所涉个人信息的，应停止该项访问。相关权限仍可能支持后续任务调用该部分信息的，也应在撤回事项范围内停止后续访问。其三，相关信息已经留存于任务记忆中的，处理者应停止将撤回事项所涉信息继续用于后续推理、个性化配置等复用环节。其四，相关信息已经由外部主体接收并处理的，处理者应依接收方的法律地位确定后续处理如何停止。接收方属于受托人的，处理者应依《个保法》第 21 条调整处理指令，要求受托人在委托范围内停止相关处理。接收方作为其他个人信息处理者自主决定接收后的处理目的、处理方式的，处理者应停止继续向其提供相关信息，并向个人说明接收方及相关处理事项。接收方能否继续处理相关信息，则应依其与个人之间的处理关系另行判断。

撤回事项所涉个人信息已经留存的，个人信息处理者应依《个保法》第 47 条删除相关个人信息。〔57〕对于“法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的”情形，信息处理者则“应当停止除存储和采取必要的安全保护措施之外的处理”。系统级智能体可能将相关个人信息保留在任务记忆、日志记录等系统留存形态中。相关内容仍属于《个保法》第 4 条所称个人信息的，应适用第 47 条关于删除及其例外的规定。若删除个人信息从技术上难以实现或者法定保存期限未届满，个人信息处理者应采取访问控制、隔离保存、调用限制等措施，使相关信息不再参与后续任务执行、模型推理等。〔58〕处理者还应能够通过处理记录、权限调用记录、对外提供记录，以及依法形成的个人信息保护影响评估报告和处理情况记录，证明撤回后停止相关处理、删除个人信息或者依法限制后续处理的要求已经落实。由此，告知规则使个人识别处理关系变化，同意规则确定后续处理能否继续纳入授权范围，撤回规则则要求处理者停止相应处理，并依法删除留存信息或限制其后续处理。

〔57〕 参见郭红伟：《论个人信息同意撤回权制度的适用障碍及其消除》，载《苏州大学学报（哲学社会科学版）》2024 年第 5 期，第 108 页。

〔58〕 参见刘权：《论个人信息保护负责人——以〈个人信息保护法〉第 52 条为中心》，载《行政法学研究》2024 年第 5 期，第 127－128 页。

五、结　论

系统级智能体将知情同意规则置于持续任务执行之中。告知、同意与撤回规则应围绕系统级智能体任务执行中的具体信息流转关系重新配置。场景完整性理论通过角色关系、信息属性和传输原则识别处理关系，并以场景规范校验合理预期，为判断原同意的覆盖范围提供依据。据此，告知规则应在法定告知事项发生变更时，使个人能够识别相关信息为何被调用、向何处流动以及是否进入后续用途。同意规则应依处理目的、处理方式、个人信息种类与接收主体的变化，判断原同意能否延续、是否应重新取得同意及是否适用单独同意要求。撤回规则应进一步作用于任务执行、系统权限调用、任务记忆和外部流转中的后续处理。由此，知情同意规则能够随任务执行中的信息流转变化，维持个人授权与具体处理事项之间的对应关系，落实撤回后的停止处理与留存清理要求，以保障个人在持续处理过程中的自主选择。

Abstract: Informed consent rules aim to ensure that individuals can make fully informed and autonomous choices about specific processing activities. System-level AI agents break down users' high-level instructions into sequences of tasks. They use system permissions, perform operations across applications, and retain contextual information, allowing personal information processing to continue as tasks unfold. One-time notice and broad authorization, premised on relatively well-defined processing arrangements at the time consent is given, struggle to accommodate subsequent changes in processing relationships. The theory of contextual integrity holds that information flows should conform to context-specific informational norms. Whether subsequent processing remains within the scope of the individual's original informed consent should be assessed in light of changes in actors, information attributes, and transmission principles. Accordingly, informed consent rules should be organized around the formation and modification of processing relationships, as well as individuals' withdrawal from them. Notice rules should adopt a tiered approach, matching the form of notice to the impact of changes in information flows on individuals' consent decisions. Rules on withdrawal of consent should distinguish among processing relationships involving the use of system permissions, the reuse of information stored in task memory, and processing by external recipients. They should specify which processing must cease and which retained information must be deleted or subject to restrictions on further processing.

Key Words: system-level AI agents, informed consent rules, contextual integrity theory, personal information protection

（责任编辑：王叶刚）