

个人信息处理中告知同意的效力与例外

算法推荐场景下同意的实质化与撤回

赵跃

(安徽国运律师事务所, 安徽 合肥 230000)

摘要: 告知同意是我国个人信息保护法的基础规则,却在算法推荐场景中普遍失灵。用户面对长篇隐私政策,往往不加阅读即点击同意;平台以概括授权换取一次性同意,将目的限定化为形式;拒绝同意的后果是服务不可用,自愿性因此被架空。本文主张,告知同意的效力不能仅以形式要件判断,而应作实质化审查。在告知一侧,须满足可理解性、可区分性与可追溯性三项要求:以分层告知替代一揽子告知,以显著提示替代隐蔽条款,以版本留痕替代事后抗辩。在同意一侧,须区分一般同意与单独同意,凡涉及敏感个人信息、对外提供、公开披露、自动化决策的,须取得单独同意;自愿性的判断,应以拒绝的可行性为标准,不得以服务不可用相要挟。在效力上,同意仅为处理行为的正当性基础,不构成责任的概括免除;超出告知目的的处理,同意不及;同意被撤回的,此后处理即失其基础。在救济上,应适度缓和用户的举证负担,由处理者就告知的履行、同意的取得、处理的必要性承担举证责任。算法推荐的关闭权,是同意撤回权的具体形态,其实现须以便捷、无歧视、可即时生效为要件。

关键词: 告知同意; 算法推荐; 个人信息保护; 单独同意; 撤回同意

中图分类号: D923.8 **文献标识码:** A **文稿编号:** WJLT(2026)02-0001-13

Effect and Exceptions of Informed Consent in Personal Information Processing

ZHAO Yue

(Anhui Guoyun Law Firm, Hefei 230000, Anhui, China)

Abstract: Informed consent is the foundational rule of China's personal information protection law, yet it generally fails in algorithmic recommendation scenarios. Users click agree without reading lengthy privacy policies; platforms trade blanket authorization for one-time consent, reducing purpose limitation to a formality; refusal means the service becomes unavailable, hollowing out voluntariness. This article argues that the effect of consent must be reviewed substantively rather than formally. On the information side, three requirements must be met: comprehensibility, distinguishability and traceability, achieved through layered notice, prominent warning and versioned records. On the consent side, general consent must be distinguished from separate consent, which is required for sensitive information, external provision, public disclosure and automated decision-making. Voluntariness should be measured by the feasibility of refusal, and service unavailability may not be used as coercion. Consent is merely a ground of legitimacy, not a blanket exemption from liability; processing beyond the notified purpose is not covered, and processing after withdrawal loses its basis. In terms of remedies, the user's burden of proof should be moderated, while the processor bears the burden regarding notice, consent and necessity. The right to disable algorithmic recommendation is a concrete form of withdrawal and must be convenient, non-discriminatory and immediately effective.

Key words: informed consent; algorithmic recommendation; personal information protection; separate consent; withdrawal of consent

说明: (本文为作者个人研究观点, 不代表所在单位意见)

作者简介: 赵跃, 安徽国运律师事务所执业律师, 主要研究民事诉讼与个人信息保护。

一、问题的提出

安装一个应用, 第一次打开, 屏幕上弹出隐私政策。长达数十页, 字号细小, 条款繁密。多数人不看, 直接点击同意。这一个动作, 构成了此后一切个人信息处理的正当性基础。

个人信息保护法以告知同意为基本规则。第十三条将取得个人同意列为处理个人信息的首要合法性基础；第十四条要求同意由个人在充分知情的前提下自愿、明确作出；第十七条要求处理者在处理前以显著方式、清晰易懂的语言真实、准确、完整地告知有关事项。

规则的设计，寄望于个人的理性选择。个人知情，方能同意；同意，方生效力。此一链条，在纸面上完整，在实践中却常常断裂。

断裂的第一处，是知情。隐私政策由处理者单方拟定，专业术语密集，条款相互援引，普通用户难以理解。所谓告知，往往沦为形式：文字已展示，内容未传达。

断裂的第二处，是自愿。多数应用将同意作为使用的前提，不同意则无法使用。面对此种设计，用户的选择空间近乎为零。形式上的自愿，实质上的被迫。

断裂的第三处，是明确。概括同意取代具体同意，一次授权覆盖收集、存储、使用、加工、传输、提供、公开的全流程。目的限定原则，在概括授权中被稀释。

断裂的第四处，是撤回。法律赋予个人撤回同意的权利，实务中却难以行使。撤回的入口隐蔽，撤回的后果不明，撤回后服务是否降级，均无保障。

算法推荐，是上述断裂最为集中的场景。推荐系统须持续收集用户的浏览、点击、停留、搜索、位置等信息，据以刻画偏好、预测行为、推送内容。收集的广度与处理的深度，远超一般业务所需。

在这一场景中，告知同意面临双重困境。一方面，推荐的准确性依赖于数据的规模，处理者有强烈的扩张收集的动机；另一方面，推荐的个性化难以事先描述，告知的内容必然笼统，同意的对象因而不确定。

于是出现一种悖论：越是需要具体同意的场景，越难以取得具体同意；越是难以取得具体同意的场景，处理者越倾向于以概括同意替代。规则的严格，反而催生了形式的敷衍。

本文试图回答三个问题。其一，告知同意的效力基础是什么，是意思表示，还是风险自负，抑或程序合规。其二，在算法推荐场景中，告知与同意应达到何种实质标准，方能产生正当性。其三，同意被撤回或者被拒绝后，处理者与用户的权利义务如何重新配置。

三个问题，层层递进。第一个问题关涉性质，第二个问题关涉标准，第三个问题关涉效果。性质不明，标准无据；标准不立，效果难定。

方法与材料上，本文以个人信息保护法的规范体系为基础，以比较法上的场景化同意与动态同意为参照，以我国监管执法与司法裁判的实践为经验素材，力求在保护与利用之间求得平衡。

须先说明本文的立场。本文不主张废弃告知同意，而主张实质化。废弃论者认为，个人无力管理自己的信息，同意只是神话，应以场景合理期待与国家监管替代。此说有其洞见，但忽视了同意在人格自主上的价值。

实质化的路径，是在保留同意制度的前提下，提高告知的质量，收紧同意的标准，强化撤回的保障，辅以举证责任的调整。四者并举，方能使同意从形式回归实质。

二、算法推荐场景中告知同意的失灵

失灵的表现，可从四个维度观察。其一是认知维度：用户不读、不懂、不记。其二是结构维度：条款由处理者单方拟定，用户无从协商。其三是经济维度：同意的成本由用户承担，收益由处理者获取。其四是技术维度：处理的复杂性超出用户的想象，告知的内容无法覆盖。

认知维度的实证基础，来自对用户阅读行为的观察。研究表明，多数用户从不完整阅读隐私政策，即便阅读，理解程度亦有限。面对专业性极强的表述，普通用户难以形成有效的认知。

不读的原因，不只是懒惰。阅读的成本与收益严重不对称：阅读数十页文本，耗时数十分钟，所能改变的结果近乎为零。理性的用户自然选择不读。此种理性，恰恰是制度设计的失败。

不懂的原因，在于表述的专业化。匿名化、去标识化、共同处理、委托处理、跨境传输，这些概念对普通用户而言近乎外语。告知的义务虽已履行，理解的可能却未建立。

不记的原因，在于同意的时点与处理的过程相分离。用户在注册时点击同意，此后的处理持续进行，用户既不知何时处理，也不知处理何种信息。同意的记忆，随时间淡化。

结构维度的失灵，源于格式条款的固有缺陷。隐私政策由处理者单方拟定，用户只能接受或者拒绝，无从协商。这与合同法上格式条款的规制逻辑相通：条款拟定方负有不偏离核心义务的义务，不得以形式上的同意掩盖实质上的不公平。

经济维度的失灵，源于成本与收益的错配。同意的成本由用户承担，包括阅读的时间成本与隐私的风险成本；收益由处理者获取，包括数据的商业价值与算法的优化。成本与收益的分离，使处理者缺乏提高告知质量的激励。

技术维度的失灵，源于处理的复杂与告知的简化的矛盾。推荐系统涉及特征提取、模型训练、实时推断等多个环节，每一环节均可能涉及个人信息处理。告知若须覆盖全部环节，将冗长至无法阅读；告知若简化，则必然遗漏。

四重失灵叠加，形成一个闭环：告知越冗长，用户越不读；用户越不读，处理者越敢于扩张条款；条款越扩张，告知越冗长。闭环一旦形成，自我强化，难以打破。

算法推荐的特殊性，还在于目的的不确定性。传统的信息处理，目的特定而明确，如办理银行业务、配送商品。推荐的目的，是优化用户体验、提升点击率、增加停留时长，这些目的本身模糊，且随算法迭代而变动。

目的不确定，导致目的限定原则难以适用。个人信息保护法第六条要求处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方

式。若目的本身无法确定，限定即无从谈起。

实务中的应对，是将目的表述为提供个性化服务、改善产品体验之类的概括语句。此类表述在文义上并无不当，在功能上却等于无表述。目的的限定，被稀释为一句空话。

另一特殊性，在于处理的持续性。推荐系统须持续收集行为数据，持续更新用户画像。此种处理，不同于一次性的交易处理，其正当性基础不能仅靠一次同意，而须有持续性的保障机制。

持续处理，也使撤回权的意义凸显。若用户在一次同意之后即失去控制，则其人格自主在漫长的处理过程中被持续侵蚀。撤回权的作用，正是在持续处理中保留一个中断的节点。

比较法上的经验，可资参照。欧盟通用数据保护条例以同意为合法性基础之一，同时强调同意的自由作出，并规定拒绝同意不得导致服务不可用，除非该处理为履行合同所必需。此一规定，直指自愿性的核心。

该条例还规定，同意须以清晰平实的语言、易于理解的形式作出，若以书面声明方式作出，须与其他事项明确区分。此一要求，指向告知的可区分性，防止同意被捆绑于其他条款之中。

我国个人信息保护法亦有类似规定。第十四条规定，法律、行政法规规定处理敏感个人信息应当取得个人单独同意的，从其规定；第十七条规定，处理者应当以显著方式、清晰易懂的语言作出告知；第十五条规定，个人有权撤回同意。

规范的供给并不缺乏，缺乏的是规范的实效。告知的形式已被要求，告知的实质未被检验；同意的作出已被要求，同意的质量未被审查。此即失灵的规范根源。

要恢复实效，须从效力基础入手。若认为同意只是一种程序合规的手续，则实质化无从谈起；若认为同意是一种意思表示，则其效力须受意思表示规则的检验。下一节即从此展开。

三、同意的性质与效力基础

关于同意的性质，学理上有三种主张。其一为意思表示说，认为同意是个人处分其信息权益的意思表示，适用民法关于意思表示的规定。其二为授权行为说，认为同意是授权处理者实施处理的单方行为。其三为违法阻却事由说，认为同意使原本违法的处理行为获得正当性。

三种主张，观察的角度不同，结论却可相容。同意既是意思表示，也是授权，同时构成违法阻却事由。三者并非互斥，而是同一现象的不同层面。

意思表示说的意义，在于引入民法的一般规则。意思表示须真实、自由、明确；受欺诈、受胁迫的意思表示可撤销；重大误解的意思表示可撤销。这些规则，同样适用于同意。

据此，若处理者以虚假的告知诱使同意，或者以服务不可用相要挟迫使同意，则同意的效力可以争辩。此一思路，为实质化审查提供了教义工具。

授权行为说的意义，在于界定同意的范围。同意授予处理者在一定范围内处理的权利，超出范围的处理，不获授权。此说与目的限定原则相合，也为越界处理的违法性提供了说明。

违法阻却事由说的意义，在于说明同意的功能。个人信息处理本须有合法性基础，同意即为其中之一。有同意，则处理不违法；无同意，则处理违法，除有其他合法性基础。

三说之中，本文以意思表示说为基础。理由是，同意在本质上是个人对其人格权益的自主处分，其效力来源于个人的自主决定。授权与阻却违法，均为自主决定的法律效果，而非独立的基础。

以意思表示说为基础，可以推出三项结论。其一，同意须具备意思表示的一般要件：行为能力、真实、自由、明确。其二，同意适用意思表示的解释规则：不得作扩大解释，有疑义时，应作有利于个人的解释。其三，同意的瑕疵，可依民法的一般规则救济。

第一项结论，指向自愿性。同意的作出，须无欺诈、无胁迫、无不当影响。在算法推荐场景中，服务不可用是否构成胁迫，须具体判断。若该服务具有市场支配地位或者构成生活必需，则拒绝的后果严重，同意难谓自由。

第二项结论，指向范围。同意的对象是特定的处理行为，而非概括的一切处理。告知未涉及的处理，同意不及。条款含义不清的，应作有利于个人的解释，不得推定为已获同意。

第三项结论，指向救济。同意的瑕疵，可主张撤销；同意被超越，可主张侵害；同意被撤回，处理即失其基础。救济的通道，包括民事诉讼、行政投诉与检察公益诉讼。

须强调，同意不等于免责。实践中，处理者常以用户已同意为由，主张免除一切责任。此一主张不能成立。同意仅使处理获得正当性，不免除处理者的法定义务，如安全保障义务、删除义务、更正义务。

同意亦不等于无限授权。个人信息保护法第十四条要求同意由个人在充分知情的前提下自愿、明确作出，法律、行政法规规定处理敏感个人信息应当取得单独同意的，从其规定。同意的范围，受告知的内容与法律的规定双重限制。

同意的效力，还具有时间性。同意作出后，处理者得在同意范围内处理；但若处理的目的、方式、种类发生变更，则须重新取得同意。此即同意的动态性，也是持续处理场景中保障个人控制的关键。

实务中的误区，是将一次同意视为永久授权。用户在注册时的同意，被用于此后数年的一切处理，包括新增的业务、新增的第三方共享。此种做法，超出了同意的范围，侵害了个人的自主决定权。

正确的做法，是建立同意的生命周期管理。同意的取得、变更、撤回、更新，均应有

记录；处理的目的、方式、种类发生实质变更的，应重新告知并取得同意；同意的有效期，宜与处理的目的相匹配，不宜设为永久。

同意的效力基础既明，方可讨论标准。若同意是意思表示，则其质量取决于告知的质量与自愿的程度。下一节讨论告知的实质化，再下一节讨论同意的实质化。

四、告知的实质化

告知是同意的前提。不知情，则无所谓同意。个人信息保护法第十七条要求，处理者在处理前应以显著方式、清晰易懂的语言，真实、准确、完整地告知处理者的名称与联系方式、处理目的与方式、信息种类与保存期限、个人行使权利的方式与程序。

规范的表述已属周全，落实却不易。显著方式如何判断，清晰易懂如何衡量，真实准确完整如何检验，均须具体的标准。本文提出三项要求：可理解性、可区分性、可追溯性。

可理解性，指告知的内容须使普通用户能够理解。衡量的标准，不是法律人的理解，而是具有一般认知能力的用户的可能理解。判断的方法，可参考文本的可读性、术语的密度、句式的复杂程度、示例的有无。

提高可理解性的方法，是分层告知。第一层为核心告知，以一页篇幅、通俗语言说明最关键的事项：收集何种信息、用于何种目的、与谁共享、保存多久、如何撤回。第二层为详细告知，以完整文本说明全部条款。第三层为技术说明，以供专业人士查阅。

分层告知的价值，在于降低认知成本。用户无须阅读全文，即可掌握关键信息；有进一步需求者，可查阅详细文本。此一设计，兼顾了效率与充分，较为可行。

我国实务中，已有平台尝试以图表、摘要、问答的形式呈现隐私政策。此类尝试值得肯定，但尚无统一的标准。监管宜出台指引，明确摘要的必备事项与呈现方式，避免以摘要之名行掩盖之实。

可区分性，指不同性质的告知事项须相互区分，不得混同。个人信息保护法要求处理敏感个人信息取得单独同意，对外提供、公开披露亦须单独同意。单独同意的前提，是单独的告知。

若将敏感信息的处理、第三方共享、跨境传输等事项，混入一揽子条款，用户的一次点击即覆盖全部，则单独同意形同虚设。此即捆绑同意，应予禁止。

可区分性的实现，须在界面设计上落实。凡须单独同意的事项，应以独立的弹窗、独立的勾选框呈现，不得预设勾选，不得以继续使用视为同意。此一要求，看似技术细节，实则关乎同意的有效性。

可追溯性，指告知的内容与版本须可查证。处理者应保存各版本的隐私政策、告知的时间与方式、用户的同意记录。发生争议时，处理者须举证证明其已履行告知义务、已取得有效同意。

可追溯性的价值，在于解决举证难。个人信息处理具有技术性、隐蔽性，个人难以证明处理者未告知。若将举证责任配置于处理者，则可迫使其规范告知流程，也便于监管核查。

三项要求，分别对应三个维度：内容、结构、证据。内容可理解，用户方能知情；结构可区分，同意方能具体；证据可追溯，责任方能落实。三者缺一，告知即不完整。

告知的例外，亦须讨论。个人信息保护法第十八条规定，处理者处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知。此为例外，适用应严格。

此外，紧急情况下为保护自然人的生命健康和财产安全无法及时告知的，处理者应当在紧急情况消除后及时告知。此一规定，兼顾了应急的需要与事后的补救。

告知的例外，不得被滥用。实务中，有处理者以商业秘密为由，拒绝告知第三方共享的具体对象；以技术复杂为由，拒绝说明算法的基本逻辑。此类做法，超出了例外的范围。

正确的处理，是区分层次。第三方的名称可以告知，具体的算法参数可以不告知；处理的目的可以告知，模型的权重可以不告知。以层次化的告知替代全有或全无的拒绝，方为妥当。

告知的语言，亦须讲究。清晰易懂，意味着避免生僻术语，避免长句套句，避免以引用代替说明。若必须使用术语，应附解释；若必须援引其他文件，应提供链接并保证可访问。

告知的时点，须在处理之前。事后的告知，不能补正处理的正当性。实务中，有处理者在收集信息之后，才在更新后的隐私政策中告知，此做法不符合事前告知的要求。

告知的变更，须重新履行。处理目的、方式、种类发生变更的，应重新告知并取得同意。仅是文字调整、格式优化的，可不重新取得同意，但仍应告知。此一区分，兼顾了稳定与灵活。

五、同意的实质化

同意的实质化，包含四项要求：具体、自愿、明确、可撤回。四项要求，分别对应同意的对象、同意的自由、同意的表达与同意的存续。

具体，指同意的对象须特定。概括同意一切处理，不符合具体的要求。同意的对象，应包括处理的目的、信息的种类、处理的方式、保存的期限、共享的对象。

实务中的做法，是将同意细分为若干项。收集基本信息、收集位置信息、收集生物识别信息、向第三方共享、用于个性化推荐、用于广告推送，各自独立取得同意。此一细分，使同意具备了可辨识的对象。

细分的程度，须有节制。分项过多，用户将不堪其扰，反而倾向于一键同意。经验的

做法，是将核心业务所必需的处理归为一组，将非必需的处理另列，逐项取得同意。

何为必需，须以服务的性质判断。地图应用收集位置信息，为导航所必需；社交应用收集通讯录，为好友推荐所必需，但为广告推送则非必需。必需与非必需的区分，是同意具体化的关键。

自愿，指同意的作出须无不当影响。判断的标准，是拒绝的可行性。若拒绝同意将导致服务完全不可用，且该服务为生活所必需或者具有市场支配地位，则同意难谓自愿。

个人信息保护法第十六条规定，处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务，但是处理个人信息属于提供产品或者服务所必需的除外。此条为自愿性提供了规范依据。

适用此条的关键，在于所必需的范围。所必需，应限于实现产品或者服务基本功能所必需的处理，不包括改善服务质量、提升用户体验、广告推送等附加功能。

据此，用户拒绝个性化推荐，处理者不得拒绝提供基本服务。用户拒绝向第三方共享信息，处理者不得以此为由限制功能。用户的拒绝，只能导致相应附加功能的不可用，不得导致基本服务的丧失。

实务中的做法，与此相反。多数应用为用户拒绝非必需的信息收集时，直接退出或者限制使用。此一设计，实质上剥夺了用户的选择权，违反了第十六条的规定。

明确，指同意须以清晰的方式作出。沉默、预设勾选、继续使用，均不构成明确同意。个人信息保护法第十四条要求同意由个人在充分知情的前提下自愿、明确作出，此处的明确，指向积极的作为。

单独同意，是明确同意的特殊形态。个人信息保护法第二十三条规定，向其他处理者提供个人信息的，应当向个人告知接收方的名称、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意。

第二十五条规定，处理者公开其处理的个人信息的，应当取得个人单独同意。第二十六条规定，在公共场所安装图像采集、个人身份识别设备，所收集的个人图像、身份识别信息用于维护公共安全之外的用途的，应当取得个人单独同意。

第二十九条规定，处理敏感个人信息应当取得个人的单独同意；法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。第三十九条规定，向境外提供个人信息的，应当取得个人的单独同意。

上述五处单独同意，覆盖了对外提供、公开披露、公共场所图像识别、敏感信息处理、跨境提供五类高风险处理。此五类处理的共同特点，是风险显著高于一般处理，故须以更高的同意标准控制。

单独同意的实质，是使个人对每一项高风险处理作出独立的判断。故其形式，应为独立的告知、独立的勾选、独立的确认，不得与其他事项捆绑，不得以概括同意替代。

实务中的违反，形式多样。有的将敏感信息的处理混入一般条款；有的以同意隐私政

策的方式，一并取得对外提供的同意；有的以默认勾选的方式，取得单独同意。此类做法，均不符合单独同意的要求。

可撤回，指同意的存续须受个人控制。个人信息保护法第十五条规定，基于个人同意处理个人信息的，个人有权撤回其同意。处理者应当提供便捷的撤回同意的方式。

撤回的效力，指向将来。撤回不影响撤回前基于同意已进行的处理的效力。此一规则，兼顾了处理的稳定性与个人的控制权。

撤回的便捷性，须有具体的标准。入口应在显著位置，操作应简便，不得设置不合理的条件，不得要求说明理由，不得因撤回而降低服务质量。此四项，可作判断的参考。

实务中的障碍，多在入口隐蔽与流程繁琐。用户须经多层菜单，方能找到撤回的选项；有的应用要求提交书面申请，经审核后方可撤回。此类设计，实质上阻碍了权利的行使。

四项要求，构成同意实质化的框架。具体使同意有对象，自愿使同意有自由，明确使同意有形式，可撤回使同意有存续。四者兼备，同意方为有效的正当性基础。

须补充一点：同意并非唯一的合法性基础。个人信息保护法第十三条列举了七项基础，包括订立合同所必需、履行法定职责所必需、应对突发公共卫生事件、为公共利益实施新闻报道、法律行政法规规定的其他情形。

故在判断处理的正当性时，不应只问有无同意，还应问有无其他基础。若处理为订立合同所必需，则无须取得同意；若处理为履行法定职责所必需，则同意与否不影响合法性。此一区分，可避免将一切处理都压在同意的框架内。

但须注意，所必需的范围应严格解释。为订立合同所必需，限于合同履行不可分割的处理；为履行法定职责所必需，限于法律明确规定的职责范围。不得以所必需为名，扩张处理的边界。

六、拒绝推荐与撤回的实现

用户如何关掉算法推荐、关掉之后平台还能推什么，站内平台算法推荐能不能关掉一文已作面向当事人的梳理；本文所要补充的，是这一权利在教义上的定位与效力边界。

算法推荐的关闭权，是同意撤回权在推荐场景中的具体形态。个人信息保护法第二十四条第三款规定，通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求处理者予以说明，并有权拒绝处理者仅通过自动化决策的方式作出决定。

同条第一款规定，利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。第二款规定，通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。

此条为关闭权提供了直接的规范依据。信息推送与商业营销，须提供不针对个人特征

的选项，或者提供便捷的拒绝方式。二者择一，处理者可选择实现方式。

实务中的做法，多以提供关闭选项的方式实现。问题在于，关闭的入口往往隐蔽，关闭的效果往往不彻底。用户关闭个性化推荐后，仍可能收到基于人口属性、地理位置、时段等信息的推荐，实质上仍属个性化。

本文认为，关闭权的实现，须满足三项要件：便捷、无歧视、即时生效。便捷，指入口显著、操作简单、无需理由。无歧视，指关闭后不得降低基本服务质量，不得提高价格，不得限制功能。即时生效，指关闭后立即停止基于个人特征的处理，不得以缓存、延迟为由继续。

三项要件的规范依据，分别来自第十五条的便捷要求、第十六条的反歧视要求、第二十四条第二款的拒绝效力。三者结合，构成关闭权的完整内容。

关闭的技术效果，须予说明。关闭个性化推荐，不等于停止一切推荐。处理者仍可基于内容的属性、时效、热度进行推荐，只是不得基于用户的个人特征。二者的区分，是判断关闭是否彻底的关键。

实务中，处理者常以关闭后推荐质量下降为由，劝导用户重新开启。此一做法，属于不当影响，违反自愿性原则。关闭的选择，应由用户自主作出，处理者不得以任何方式施加压力。

关闭的存续，亦须保障。关闭的选择应被记录，不得因应用更新、账号切换、设备更换而失效。若因技术原因失效，处理者应及时恢复并告知用户。

除关闭权外，个人还享有删除权、更正权、查阅权、复制权、可携带权。个人信息保护法第四十五条至第四十七条对此作了规定。这些权利，共同构成个人对信息的控制体系。

删除权的适用情形有五：处理目的已实现、无法实现或者为实现处理目的不再必要；处理者停止提供产品或者服务，或者保存期限已届满；个人撤回同意；处理者违反法律、行政法规或者违反约定处理个人信息；法律、行政法规规定的其他情形。

删除权的实现，难点在于技术。个人信息分散于多个系统，删除须逐一执行；备份数据中的信息，删除更为困难。实务中的做法，是采取不可逆的去标识化处理，替代物理删除。此一做法，可资认可，但须确保不可复原。

可携带权的实现，难点在于格式。个人信息保护法第四十五条规定，个人请求将个人信息转移至其指定的处理者，符合国家网信部门规定条件的，处理者应当提供转移的途径。此一权利，旨在破除锁定效应，促进竞争。

权利的行使，须有程序的保障。个人行使权利，处理者应在合理期限内答复；拒绝的，应说明理由；个人对答复不满的，可向监管部门投诉或者提起诉讼。此一链条，须畅通。

实务中的障碍，在于答复的期限不明、理由不清、救济不畅。个人提交申请后，往往

长期无回应；处理者以各种理由拒绝，却不说明依据；个人投诉后，监管的处理周期较长。这些障碍，削弱了权利的实际效果。

改进的方向，是建立标准化的响应机制。处理者应设置专门的通道，明确答复的期限，规范拒绝的理由，提供救济的指引。监管部门应建立投诉的处理时限，公布典型的处理案例。此一机制，可提高权利实现的效率。

七、侵害的救济与举证

侵害个人信息的责任，兼具民事、行政、刑事三重性质。民事上，侵害个人信息权益造成损害的，应承担赔偿责任；行政上，违反个人信息保护法的，由履行个人信息保护职责的部门责令改正、警告、没收违法所得、罚款；刑事上，情节严重的，构成侵犯公民个人信息罪。

民事救济的难点，在于损害的证明。个人信息的侵害，往往表现为风险而非现实的损害。信息被泄露，用户可能遭受精准诈骗、骚扰电话、差别定价，但这些损害难以量化，也难以证明与泄露之间的因果关系。

个人信息保护法第六十九条规定，处理个人信息侵害个人信息权益造成损害，处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。前款规定的损害赔偿，按照个人因此受到的损失或者处理者因此获得的利益确定；个人因此受到的损失和处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。

此条确立了过错推定的归责原则。个人无须证明处理者的过错，处理者须自证无过错。此一配置，减轻了个人的举证负担，符合信息处理的技术性与不对等性。

但损害的证明，仍是难题。损失难以确定，获利难以查明，法院只能根据实际情况酌定。实务中的判赔数额，往往偏低，难以形成有效的威慑。

本文主张，在损害数额的确定上，可采三种方法。其一，以处理者的获利为基准，按其因侵害所获得的利益确定；其二，以个人的损失为基准，包括为制止侵害支出的合理费用；其三，以法定赔偿为兜底，由法院根据侵害的情节、后果、过错程度酌定。

酌定的因素，可包括：信息的敏感程度、侵害的范围与持续时间、处理者的过错程度、是否及时采取补救措施、是否主动告知、是否配合调查。因素的明确，有助于统一裁判尺度。

举证责任的分配，须进一步细化。个人信息保护法第六十九条已将过错要件的举证责任倒置，但因果关系与损害数额的举证责任，仍由个人承担。此一部分，宜适度缓和。

缓和的方法，是表见证明与事实推定。个人证明存在信息泄露的事实与自己遭受的损害，且二者之间具有通常的关联，即可推定因果关系成立；处理者若不能证明损害另有原因，则应承担责任。

实务中，法院已在部分案件中采用此一思路。如信息泄露后用户遭受精准诈骗，法院

认定泄露与损害之间具有因果关系，判令处理者赔偿。此一裁判，值得肯定。

行政救济的作用，不容忽视。个人信息的侵害，往往涉及众多用户，单个诉讼的成本高、收益低。行政监管的介入，可以集中处理，提高效率。

个人信息保护法第六十六条规定，违法处理个人信息或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得；拒不改正的，并处一百万元以下罚款；情节严重的，由省级以上部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款。

此条的罚款幅度，具有相当的威慑力。实务中的适用，已出现数起高额罚款的案例。此一趋势，有助于促使处理者合规。

检察公益诉讼，是另一条路径。个人信息保护法第七十条规定，个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织，可以依法向人民法院提起诉讼。

公益诉讼的价值，在于解决大规模小微侵害的救济难题。单个用户的损害虽小，聚合起来却十分可观；单个诉讼虽不经济，公益诉讼却可一次解决。此一制度，填补了私人救济的空白。

三种救济，各有其功能。民事救济填补损害，行政救济维护秩序，刑事救济惩治严重违法。三者的衔接，须以避免重复评价与填补救济空白为原则。

救济的最终目的，不在于赔偿，而在于规范。通过责任的施加，促使处理者改进告知的方式、提高同意的质量、保障撤回的便捷。此即救济的预防功能。

八、结语

告知同意，是个人信息保护法的基石。基石的稳固，不取决于条文的繁密，而取决于实效的有无。形式上的告知、形式上的同意，无法支撑实质上的正当性。

本文主张的实质化，包含四个环节。告知的实质化，以可理解、可区分、可追溯为标准；同意的实质化，以具体、自愿、明确、可撤回为标准；撤回的实现，以便捷、无歧视、即时生效为标准；救济的完善，以过错推定、因果推定、数额酌定为标准。

四个环节，环环相扣。告知不实，同意无效；同意不自愿，处理失据；撤回不畅，控制落空；救济不力，规范失灵。任一环节的缺失，都会使整个制度的效果打折。

从更远处看，本问题的实质，是如何在数据的利用与人格的保护之间取得平衡。过度保护，阻碍创新；保护不足，损害尊严。平衡的取得，靠规则的精细，也靠技术的支撑。

技术的支撑，值得期待。隐私计算、联邦学习、差分隐私等技术，可以在不获取原始信息的前提下完成计算，从而减少收集的必要。技术的进步，或将改变告知同意的适用场景。

但技术不能替代规则。技术方案的选择，仍须由规则约束；技术效果的宣称，仍须受

监管核查。规则的完善，是技术向善的前提。

愿每一次点击同意，都是真正的知情选择；愿每一项信息处理，都有可查的正当基础。此即本文的初衷。

参考文献

- [1] 《中华人民共和国个人信息保护法》第十三条至第十八条、第二十三条至第二十六条、第二十九条、第三十九条、第四十四条至第四十七条、第六十六条、第六十九条、第七十条。
- [2] 《中华人民共和国民法典》第一千零三十四条至第一千零三十九条。
- [3] 《中华人民共和国网络安全法》第四十一条、第四十二条。
- [4] 《常见类型移动互联网应用程序必要个人信息范围规定》（国信办秘字〔2021〕14号）。
- [5] 程啸：《个人信息保护法理解与适用》，中国法制出版社2021年版。
- [6] 张新宝：《个人信息收集的告知同意原则》，《中国法学》2021年第5期。
- [7] 丁晓东：《算法推荐的法律规制》，《法学研究》2022年第3期。
- [8] 王锡锌：《个人信息权益的三重构造》，《中外法学》2021年第4期。