财经法学 No. 1，2024
pp. 100 - 115

敏感个人信息告知同意规则的制度逻辑、规范解释与补强

杨惟钦*

内容提要：《个人信息保护法》区分信息类型，为敏感个人信息配置了强告知同意规则。告知同意规则以信息自主、自决为首要价值基础，有其自身制度逻辑，但也有诸多自限性缺陷。在信息风险社会，告知同意规则对于敏感个人信息的保护具有重要意义，应进一步发掘并赋予其新的价值功能内涵，即风险的预防与分配。为准确适用敏感个人信息之告知同意规则，消弭法规范中诸多不确定性及该制度的自身缺陷，应对告知同意规则之适用范围、告知事项与标准、同意形式与要求等做出恰当解释，以期在实现信息自决的同时能更好地实现风险的控制；同时，基于敏感个人信息“敏感度”与“风险性”的动态特征，应对其告知同意规则做动态性机制补强，以使信息处理符合信息主体的风险预期。

关键词：敏感个人信息　告知同意　风险控制　单独同意　动态性

一、引言

信息社会中，不同类型的个人信息所蕴含的主体价值、损害风险及所涉利益冲突各有不同，因此应被赋予不同的法律关切度。《中华人民共和国个人信息保护法》（以下简称《个保法》）与欧美等域外立法经验一致，区分一般个人信息与敏感个人信息，给予后者更高强度的保护。同时，不同立法例中个人信息保护制度虽有差异，但其发展历程基本都以个人信息自主控制模式为主线而展开，〔1〕强调信息主体积极参与、控制个人信息的使用范围、处理方式与目的及其正确性与完整性等。〔2〕

* 杨惟钦，云南大学法学院副教授。
本文为国家社会科学基金项目“类型化视角下的个人信息私法保护研究”（21BFX088）的阶段性成果。

〔1〕 参见刘金瑞：《个人信息与权利配置——个人信息自决权的反思和出路》，法律出版社 2017 年版，第 33 页。

〔2〕 参见胡文涛：《我国个人敏感信息界定之构想》，载《中国法学》2018 年第 5 期。

以“个人信息自决”“信息不对称理论”为基础的告知同意规则虽存在诸多缺陷，但仍然是处理个人信息的正当性基础，是规制信息处理行为、实现个人信息保护与信息自主控制的重要机制。在敏感个人信息领域，告知同意规则仍无可替代，但应结合信息风险社会特征及敏感个人信息保护需求对其进行新的价值阐释。鉴于敏感个人信息的高敏感度及高风险性特征，《个保法》为其设置了保护力强于一般个人信息的强告知同意规则，以期实现更严、更细的安全控制。同时，敏感个人信息的“敏感度”具有动态性特征，这种动态性不仅体现为其类型归入的动态，亦体现为其“风险”因场景转化而呈现的动态，因此，告知同意规则在关注敏感个人信息高风险性的同时，亦应回应其动态的风险控制要求。〔3〕

二、告知同意规则的内在逻辑及在敏感个人信息保护中的价值

（一）告知同意规则的内在逻辑与自限性缺陷再认识

1. 告知同意规则的内在逻辑

告知同意规则作为个人信息保护的基石性制度，植根于自主价值，要求对个人信息的处理必须经过本人真实的同意，且应当以事先充分的知情为前提。美国学者查尔斯·佛里德（Charles Fried）对此有准确描述：隐私（信息）的意义不仅仅是将我们的信息屏蔽而不为外界所知，而更应该理解为我们能够按自己的意愿控制自己的信息。〔4〕其逻辑起点在于信息主体具有信息自决的权利，从而保障人格自由与人格尊严。恰如洛克所言，“既然一切人自然都是自由的，除他自己同意以外，无论什么事情都不能使他受制于任何世俗的权力”〔5〕。由是，告知同意规则是信息处理者为获得处理他人个人信息之正当性基础而告知信息主体相关事项，个人信息主体在信息充分、可理解的情况下基于理性判断与风险评估而做出同意的程序性机制。

比较法上对告知同意机制所依托的基础性权利有不同的解释路径，以基本权利保障为视角展开个人信息保护的德国将其解释为“信息自决权”，欧盟沿袭了这一“基本权利和自由”的路径，将其阐释为“个人数据被保护的权利”，〔6〕从而将告知同意规则项下的义务视为一种公法义务。而注重消费者保护与行业自律的美国法采纳了由韦斯廷（Westin）提出的观点，为实现自由与自治，隐私应解释为包含个人得控制自己于何时公开何种个人信息之权利的宽泛隐私观念，〔7〕从而扩张了既有的隐私体系，创设出契合信息社会要求的积极隐私类型——信息隐私，以解决告知同意的基础权源问题。

告知同意规则早在1970年的《德国黑森州数据保护法》中便以原则的形式出现，而1973年美国政府发布的《记录、计算机和公民权利》报告（即“公平信息实践准则”报告）也包含了告知同意原则。其后无论是美国的《儿童在线隐私保护法案》《影视隐私保护法案》《公平信用报告

〔3〕 See Müge Fazlioglu, *Beyond the “Nature” of Data: Obstacles to Protecting Sensitive Information in the European Union and the United States*, 46 Fordham Urban Law Journal 271, 287-288 (2019).

〔4〕 See Charles Fried, *Privacy*, 77 Yale Law Journal 475, 482 (1968).

〔5〕〔英〕洛克：《政府论》（下篇），叶启芳、瞿菊农译，商务印书馆2017年版，第74页。

〔6〕 欧盟《一般数据保护条例》第一章第1条第2款规定：“本条例保护自然人的基本权利与自由，特别是自然人享有的个人数据保护的权利。”

〔7〕 See Alan F. Westin, *Privacy and Freedom*, Atheneum, 1967, p. 7.

法》，还是 80 年代国际经合组织（OECD）颁布的《有关隐私保护个人数据跨国流通指南》《有关个人数据自动处理过程中的个人保护公约》，或者欧盟的《数据保护指令》及《一般数据保护条例》（GDPR）等都延续了这一规则，并发展了更加细致的内涵。

我国在《个保法》颁行之前，《中华人民共和国民法典》（以下简称《民法典》）第 1035 条已将“告知同意”作为处理个人信息的首要合法条件予以规定，更早前的《中华人民共和国消费者权益保护法》（第 29 条）、《中华人民共和国网络安全法》（第 22 条）、《关于加强网络信息保护的决定》（第 2 条）、《征信业管理条例》（第 12 条），以及作为国家标准的《信息安全技术——个人信息安全规范》等一系列法律、法规及规范性文件中也确立了告知同意规则，使其成为特定领域、特定行业信息保护中的重要行为遵循，《个保法》作为信息领域的基本法也最终确认了告知同意规则的地位。有学者进一步指出，《个保法》采取了与欧盟类似的立法进路，个人信息不仅是一项私法所保护的人格权益，也可视为一项公法上的基本权利，〔8〕这使得告知同意规则更容易被理解为公法意义上的保护机制。“无论是我国还是欧美，隐私政策都呈现公私法融合特征，是一种多维法律制度工具。”〔9〕有学者更明确指出，告知同意规则中的“告知”实则具有公法与私法的双重属性。〔10〕因此，告知同意规则亦是内含公法意蕴的合规行为准则。

2. 告知同意规则的自限性缺陷再认识

作为共识性的信息处理行为规范，告知同意规则在被各国立法及国际法规范普遍采纳的同时，其在大数据时代的实践效果也一直饱受诟病，究其原因在于，发端于“小数据”时代的“告知同意”跨进大数据时代后，面对海量信息的密集收集、多形式频繁处理、多主体交叉共享等情状，必然出现有效同意之成本与难度的增加，从而导致同意效果的虚化，甚至于整个规则的异化，〔11〕实践中“有效告知”与“真实同意”较难完整实现，告知同意机制渐有失灵之嫌，导致信息主体对个人信息实际上并未形成有效控制。

告知同意规则在实践中呈现的具体缺陷与不足主要有如下几点：其一，与告知内容相关的告知文件（如隐私政策），为满足“充分”“明确”等规范要求，复加规避合规风险的考虑，往往尽述其详，导致告知内容繁复、冗长，且包含太多专业术语与结构化描述，内容晦涩难懂。其二，面对不同生活情境中的众多告知文件，信息主体通常既无专业能力，也无时间和耐心进行阅读和判断，其同意也不过是合并了侥幸心理的无奈之选，这种同意，因缺乏充分的知悉与理性的判断而没有实际意义。其三，基于背景知识与认知的不同、专业知识的普遍缺乏，信息主体对信息风险预见能力存在天壤之别，从而无法保证所有的被告知者皆能做出理性的判断与选择，此时信息自决一定程度上流于形式。其四，对信息风险的预见难度还会随着风险与损害的“远期性”“潜在性”“动态性”特征而加剧。此外，还存在被诱导的可能性，即信息主体往往被精心设计的告知形式所“套路”，如“捆绑式同意”“不经意的勾选同意”“默认勾选”等刻意地引导用户完成不真实的同意，这被学者哈里·布里吉努（Harry Brignull）称为“暗黑模式”（dark patterns）。〔12〕因此，

〔8〕 参见王锡锌：《个人信息国家保护义务及展开》，载《中国法学》2021 年第 1 期。

〔9〕 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》，载《现代法学》2023 年第 1 期，第 36 页。

〔10〕 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。

〔11〕 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。

〔12〕 See Jamie Luguri & Lior Jacob Strahilevitz, *Shining a Light on Dark Patterns*, 13 Journal of Legal Analysis 43, 44 - 46 (2021).

公法规制层面上不仅应重视“告知同意”的实质内容，也应关注告知与同意形式的正当性。更有甚者，告知同意机制的多元标准追求会导致内部悖论现象的发生，〔13〕即告知同意规则的各要求之间、要求与措施及效果之间，可能出现不易调和的冲突与矛盾。如上缺陷与困境源自告知同意机制内部构造本身，或关乎告知内容，或关乎告知人与同意人，其属于告知同意规则的内在自限性引发的缺陷与困境。

告知同意机制的失灵还会因外部环境——不确定的多方信息行为参与主体所构成的市场环境与经济结构等外部因素——而引发。这些因素引发处理者与信息主体间“持续性的信息不平等关系”〔14〕，形成告知同意机制的外部自限性缺陷，因为市场普遍存在缔约力能与缔约机会不对等的情况，数据市场也不例外。同时附加交易对象的有限可选择性，使得信息主体往往不具有与信息处理者讨价还价的空间与能力，导致不放弃信息权益就等于要放弃被提供服务，而许多这样的服务属于非竞争性服务，因此信息主体实际上毫无选择的余地。

由于理论与实践、理想与现实间的拉锯关系，告知同意规则在适用中始终面临如下争议：告知同意规则自限性缺陷引发的制度失灵能否消弭及如何消弭。较为激进的观点甚至建议放弃该规则以其他机制取而代之，如用以“知情权”为前提、以“严格责任”为保障的“宽进严出＋删除权”机制取代告知同意规则。〔15〕告知同意规则在“弃”与“扬”之间如何选择？在弃与扬的争论中，“弃”方的力量还因“社会控制”的个人信息保护理念的影响而得以加强。对此，笔者认为，在《民法典》与《个保法》已经确认该规则的当下，直言应当放弃并非妥当之选。信息主体一定程度上享有信息自决的权利始终应当是被坚守的价值。即使该规则的诸多缺陷与不足导致信息自主与自决不易完整实现，但其仍然是保障信息安全的重要控制阀。正如学者所言：“在个人信息的‘全生命周期’中，知情同意是一道‘闸口’，无论是信息采集、利用，还是相应转换、转移，均绕不开‘知情同意’。”〔16〕按照实用主义的经验，选择法律规范，对其进行解释并进而适用时，应以现实需要为重要考量，〔17〕那么解困之道也许便是适度放松理论争议，回归工具主义理性，以大数据时代的信息生态环境及信息处理行为特征为考量，努力重塑告知同意规则，不断完善和改良规则细节，最大程度地消弭告知同意规则的缺陷。

（二）告知同意规则在敏感个人信息保护中的价值

敏感个人信息由于“高敏感度”与“高风险性”特征，需要法律赋予更强的保护力，目前信息领域里告知同意规则的基础性地位仍然存在，而敏感个人信息高度关乎主体的人格尊严与人身、财产利益，若摒弃“告知同意”路径，采绝对禁止处分方案或有例外的绝对禁止处分方案，都无法契合当代信息实践需求。此外，敏感个人信息的“社会性”与“公共性”特征大大弱于一般个人信息，因此，即使主张放弃告知同意规则的学者也肯认，敏感个人信息领域应保留该规则的适用。如大力主张个人信息保护理念应当从“个人控制”转向“社会控制”的学者也认为：基

〔13〕 参见吕炳斌：《个人信息保护的“同意”困境及其出路》，载《法商研究》2021年第2期。

〔14〕 程啸：《个人信息保护法理解与适用》，中国法制出版社2021年版，第154页。

〔15〕 参见任龙龙：《论同意不是个人信息处理的正当性基础》，载《政治与法律》2016年第1期。

〔16〕 姚佳：《知情同意原则抑或信赖授权原则——兼论数字时代的信用重建》，载《暨南学报（哲学社会科学版）》2020年第2期，第48页。

〔17〕 See Richard A. Posner, *The Problems of Jurisprudence*, Harvard University Press, 1993, pp. 423－470.

于敏感信息所蕴含的重要主体价值，应当给予个人必要的控制，对于敏感个人信息的处理仍然需要经过个人的同意，由信息主体自我控制个人信息的收集和使用。〔18〕因此，无论在逻辑上还是实践中，告知同意规则都依然是敏感个人信息的重要处理规则。需要思考的问题应当是，如何在敏感个人信息保护的特殊要求下设计出切合价值追求与实践需要的告知同意规则，在敏感个人信息领域最大化地消除该规则的自限性缺陷，让这一“必要控制阀”发挥出最大效益。在比较法上，欧盟 GDPR 确认了告知同意规则于敏感个人信息领域的适用，且特别强化规定了敏感个人信息的具体告知内容与同意标准等；而历来注重行业自律及从业者与信息主体自治安排的美国虽没有针对敏感个人信息保护的统一立法，但在一些特别领域的立法中［典型如《消费者隐私权利法案（草案）》（Administration Discussion Draft：Consumer Privacy Bill of Rights Act of 2015）］也明确要求处理敏感个人信息的前提是取得信息主体的知情同意。更具代表性的伊利诺伊州立法《生物信息隐私法案》（The Biometric Information Privacy Act），要求个人、公司、合伙企业等私人实体收集他人生物信息时需要告知并取得同意，而且告知与同意都应当是书面的。〔19〕如上立法正是通过告知同意内容的细化、标准的提高，强化告知同意规则的风险防范功能并努力实现其缺陷的消弭。

进一步言之，如果说告知同意规则的逻辑起点在于为实现个人信息保护而寻找处理他人个人信息的正当化基础，那么，在敏感信息的场域里，告知同意规则的存在意义更在于机制转化作用下的高风险防范。其具体机理在于：其一，更高要求下的敏感个人信息强告知同意规则可以强化主体风险意识，通过特定告知形式提醒信息主体权利状态、权利意识以及风险的可能性、风险的防范。其二，强告知同意要求也对信息处理者形成激励与警示。告知内容要求与同意形式要求的提高不仅强化了告知同意的规范意义，更促进信息处理者内部信息风险控制文件与机制的完善及相关流程的自我规范，最终达到信息风控机制的整体优化与健全的效果。其三，强告知同意规则对信息处理者提出了更高的要求，促使其采取更为审慎的行为与更高级别的风险防范技术，从而促进其信息技术手段上的革新与投入。因此，目标转化下的告知同意制度重塑，能够契合敏感个人信息保护中高风险防范的根本规范要求，同时也体现了对敏感个人信息处理行为的规制加强。故，针对敏感个人信息高度关联自然人人格尊严与各项权益的特点，合理、妥当设置强告知同意规则细节，可实现敏感个人信息保护与利用间的有效平衡，兼顾公益与私益。

三、我国敏感个人信息告知同意规则的进路与反思

（一）我国敏感个人信息告知同意规则的进路

在《个保法》之前，我国并没有体系化的敏感个人信息保护规则，《民法典》也没有区分一般个人信息与敏感个人信息分别进行规范。最早提及敏感个人信息保护的规范是《信息安全技术——个人信息安全规范》这一国家标准，该规范首次对敏感个人信息做出了定义。此外，涉及

〔18〕 参见高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018 年第 3 期。

〔19〕 参见邢会强：《人脸识别的法律规制》，载《比较法研究》2020 年第 5 期。

敏感个人信息的规范主要体现在一些行业性的法规、规章及规范性文件中，典型如《征信业管理条例》《App 违法违规收集使用个人信息行为认定方法》《中国人民银行金融消费者权益保护实施办法》《国务院办公厅关于促进“互联网＋医疗健康”发展的意见》等。以上文件均体现了敏感个人信息应采取严格保护的理念并做出了具体规范，其中《征信业管理条例》第 14 条第 2 款、《中国人民银行金融消费者权益保护实施办法》第三章都规定了征信机构、金融机构采集个人金融账户信息等敏感个人信息的告知同意规则。

《个保法》颁行后，我国从领域基本法的高度对敏感个人信息保护问题做出了基础性、系统性的规范，法律层面以《民法典》第 1034 条、1035 条、1036 条为个人信息保护的规范基础，《个保法》第 28—32 条为敏感个人信息保护的主要规范，该法对敏感个人信息的强告知同意规则做出了原则性规定，同时配合以《征信业管理条例》为代表的一系列行政法规、部门规章、地方性法规、司法解释及其他规范性文件等，〔20〕形成一般立法结合特别立法，体现行业与部门特征、数据信息属性特征与保护要求的敏感个人信息告知同意规则体系。总体上，适用于敏感个人信息的强告知同意规则更加注重风险控制，要求信息处理者负担更重的告知义务。但《个保法》的相关规范较为粗放，为法律的适用留下较大讨论空间。

（二）《个保法》中敏感个人信息告知同意规则的反思

1. 告知内容与标准的含混模糊

《个保法》虽然明确了告知同意规则的基本要求，但标准却不甚清晰。根据该法第 30 条，除有特别规定不需要告知的以外，信息处理者不仅应告知信息处理中的一般告知事项，还应特别针对敏感个人信息处理的“必要性”及“对个人权益的影响”进行告知，而第 28 条第 2 款处理敏感信息的限制性规则是“只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息”。据此，敏感个人信息被处理时，处理者所负担的告知义务内容除由第 17 条规定的事项外，还包括处理行为的“充分的必要性”“特定的目的”“对个人权益的影响”。而规范中“充分”与“特定”的表述实属模糊、抽象的概念，为避免实践中的争议，需要进一步解释。另外，第 17 条所要求的“显著方式、清晰易懂的语言真实、准确、完整”也较为抽象，需要进一步明确其内涵。以上内容如不加以明确，无法杜绝告知同意中的陷阱，即信息处理者为规避风险使用过于抽象的表达、模糊的概念与高级的词汇来描述隐私政策等告知文件，从而隐藏针对敏感个人信息的潜在处理目的及对个人权益的影响等。〔21〕

2. 同意规则的实践难题

《个保法》规定，处理敏感个人信息应取得“单独同意”与特别法规定下的“书面同意”。〔22〕单独的同意与书面的同意属于何种同意，应当采取何种具体形式？“单独”具体以什么为标准？其与欧盟 GDPR 第 9 条第 2 款（a）项规定的“明确同意”（explicit consent）有何区别？单独同

〔20〕 地方性法规典型如《广东省社会信用条例》第 22 条第 2 款、第 3 款对征信机构采集敏感个人信息的范围及告知同意的条件作出规定。司法解释典型如《最高人民法院审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》，对使用人脸识别技术处理敏感个人信息的行为作出全面系统的规范。

〔21〕 See Sarah Wood，*Big Data's Exploitation of Social Determinants of Health*：*Human Rights Implications*，22 Columbia Science and Technology Law Review 63，81（2021）.

〔22〕 鉴于本文研究范畴的有限性，分析论证并不涉及未成年人个人信息保护中的“告知同意”规则。

意的反面意味着概括、笼统、一揽子式的同意，此时的单独同意所对应的告知内容应该如何细分拆解，方可使同意构成“单独同意”？是否意味着一项处理行为对应一个同意？抑或一项敏感信息对应一个同意？对于同意的形式又该如何确定，书面形式具体包括哪些？有学者将这样的形式标准阐释为“数据主体通过书面声明或主动做出肯定性动作来完成对其个人数据进行特定处理的明确授权”〔23〕，但实践中什么是肯定性动作值得思考。同意内容与形式的要求不仅涉及风险防范的效果，也涉及同意获得的成本及实现的可能性，因此消极的观点认为，再强的形式要求都无法保证信息主体是完全基于自愿作出同意。故有学者建议，敏感个人信息应当奉行绝对禁止处理原则，亦有学者提出应留下涉及“公共利益”“国家利益”等各种更高层级的利益需求（如科学研究等）之处理行为作为敏感个人信息禁止处理原则的例外事项。〔24〕

综上，强告知同意规则的诸多模糊与不确定必然导致其不能为信息处理者提供明确的行为指引，从而引发合规成本的提高，进而可能构成数据壁垒，阻碍数据信息的流通，制约数据信息价值的开发利用，同时亦为执法者与司法者留下过大的自由裁量空间。

3. 并未完全回应风险的动态性特征

信息的处理是动态的过程，信息所处场景亦可能不断转换，外加信息技术的发展与变革，致使信息处理风险呈现动态性特征，这使得信息主体很难基于静态的告知同意而形成信息风险的合理预期，这样的情势在敏感个人信息的处理中尤甚。一方面，敏感个人信息类型的归入已然具有动态性特征；另一方面，敏感个人信息在各处理环节中随着处理技术、处理主体、处理目的、储存设备、流动载体等要素的变化亦会发生敏感性的变动，信息风险高低随之变化。而告知同意规则建构在“个人信息处理活动应当符合信息主体对风险的合理预期”这一基础之上，因此，敏感信息告知同意规则体系亦应当满足动态性需求。但《个保法》仅在第 17 条第 3 款、第 22 条、第 23 条针对处理者、主体信息、处理目的、处理方式等事项的变化规定了再次告知的义务，却并未涉及因场景转换、数据聚合、算法技术等的变化引发风险变动时的再次告知与同意，故而并没有充分回应敏感个人信息告知同意中的动态性需求，无法完全实现对大数据时代信息频繁、深度处理与多次流转、利用带来的利益冲突的平衡。如学者言，我国的信息保护立法没有很好体现应有的风险管理理念，也没有实现对敏感个人信息的动态保护。而静态的告知同意规则并不能满足敏感个人信息保护的需要。〔25〕因此，对敏感个人信息告知同意规则进行完善时，动态性机制补强应当予以考虑，使必要的过程性“披露”与“告知”能有效进行，与之相应的“同意”也能实时更新。

四、价值重塑下敏感个人信息告知同意规则的解释与补强

（一）敏感个人信息告知同意规则的价值重塑

告知同意规则的自限性缺陷导致信息主体不能做出完全自愿且理性的决定时，其“个人控

〔23〕 韩新远：《个人行为轨迹信息的法律属性与分类保护研究》，载《交大法学》2021 年第 3 期，第 77 页。
〔24〕 参见程啸：《论我国个人信息保护法中的个人信息处理规则》，载《清华法学》2021 年第 3 期。
〔25〕 参见孙清白：《敏感个人信息保护的特殊制度逻辑及其规制策略》，载《行政法学研究》2022 年第 1 期。

制”功能被弱化，并且在技术层面“不管处理信息的技术有了多么显著的改进，人类的智能和意识在吸收信号方面将永远地受到限制”〔26〕。同时又必须承认，在信息主体与信息处理者的风险控制力量不对称的信息社会中，告知同意依然是一个最好的制约性保护构造。为此，让告知同意规则发挥“第一道阀门”的功能，将“自主”“自决”作为告知同意的核心价值的同时，其是否可以被发掘、赋予新的价值功能内涵与解释路径值得思考。

正如学者言，信息作为新型法益，其保护的理论基础等并不能仅从私权保护的角度展开，从公共维度出发，基于信息安全的社会控制角度理解应该更具有可行性。〔27〕对此，我们可以从风险控制的面向上重新解释告知同意规则的价值，深度理解告知同意并非仅仅为实现私法世界里的意思自治，其亦是公法意义上实现风险预防的有利构造。从比较法上看，“风险预防”理念其实已经应运而生，欧盟 GDPR 已经对此做出回应，有必要借此对告知同意规则进行完善。〔28〕风险的预防可作为客观法秩序建构的基础，而不应仅关注个体主观权利的保护。〔29〕“基于此，数据法建构的重心也应当从一味地强化个人控制权能转向规制具体的收集和使用行为，合理地界定个人控制在其中发挥的作用，通过精细化的利益平衡实现数据保护的私人价值与数据流通的公共价值之间的彼此促进和良性互动。”〔30〕

在规范的解释与设计上，敏感个人信息告知同意规则应转向风险控制功能与价值的实现，充分实践其公法规范意蕴，实现各方利益的恰当平衡。实际上，“意思自治”“信息的自主、自决”一直是告知同意规则风险控制功能实现的显性逻辑线，即由信息主体基于自愿，一定程度上自主控制个人信息的安全。在此之外，还存在一条隐性逻辑线——风险的分配，即通过国家之力的介入，要求信息处理者在何种限制性规定的约束下，履行何种告知同意义务，并配合设置何种退出机制方可处理敏感个人信息，从前提条件、行为规范、可选择路径等多个角度将风险在各方当事人间进行合理分配，最大限度地防止信息风险的发生。并且，以上规则的完备通过充沛其义务内容与标准，还有助于损害发生前职能部门对信息处理行为进行合规性监管，以及信息损害发生时过错的认定，并最终有助于损害责任的分配，从而促使风险防免义务承担者规范其信息处理行为，加强信息风险控制机制的建设。在告知同意规则的解释适用与完善上，应因循这两条“显”“隐”交错的逻辑线而展开。

就风险的分配而言，以一种概括的风险维度进行观察，在信息主体与信息处理者之间，前者的风险更多是被后者所控，〔31〕换言之，真正掌握并利用信息技术与风险控制系统的是处理者，在信息被收集、分析、挖掘、传输、共享等环节里，信息主体完全是个“局外人”，只能消极承受各种潜在的风险，因此，有学者指出：“《个人信息保护法》重点考虑了信息处理者特别是平台企业相对

〔26〕〔美〕肯尼斯·J·阿罗：《信息经济学》，何宝玉、姜忠孝、刘永强译，北京经济学院出版社 1989 年版，第 168 页。

〔27〕参见梅夏英：《民法权利思维的局限与社会公共维度的解释展开》，载《法学家》2019 年第 1 期。

〔28〕参见杨显滨：《我国敏感个人信息处理规则的规范解释与体系构造》，载《学术月刊》2022 年第 10 期。

〔29〕参见赵鹏：《“基于风险”的个人信息保护?》，载《法学评论》2023 年第 4 期。

〔30〕丁晓强：《个人数据保护中同意规则的“扬”与“抑”——卡－梅框架视域下的规则配置研究》，载《法学评论》2020 年第 4 期，第 136 页。

〔31〕参见姚佳：《知情同意原则抑或信赖授权原则——兼论数字时代的信用重建》，载《暨南学报（哲学社会科学版）》2020 年第 2 期。

于自然人所普遍具有的优势地位，强调信息处理者处理个人信息时应负有更大的责任……”〔32〕相较于一般个人信息，敏感个人信息的告知同意应该为处理者分配更多的风险，让其承担更多的义务与责任实属妥当。

综上所述，在对敏感个人信息告知同意规则之风险预防、风险分配的价值予以重新锚定后，以此作为价值基础，对规则体系进行新解释、新阐释与补强，使其法效果符合特定的价值追求，也许是克服告知同意规则的自限性缺陷且最大化地发挥其风险防控功能，进而实现信息保护与利用间的有效平衡的重要路径。

（二）敏感个人信息告知同意规则的解释与补强

1. 告知同意规则的辐射范围——“合理使用”情形下是否需要告知与同意

根据《个保法》，处理他人敏感信息的权限可以基于第 29 条之规定获得，即经由告知同意而获得，另亦可根据“合理使用条款”（或称为“除外情形条款”），即第 13 条第 1 款第（二）至（七）项之规定而获得。“合理使用”情形中处理他人敏感信息势必在一定程度上限制当事人的自主与自决，此时按照逻辑自是不需要再获得信息主体的同意，否则，将从事实上架空“合理使用”条款，即无论是基于个人的意愿抑或是基于公共利益考量之“合理使用”等情形都需要先告知后同意。为此，有学者指出《个保法》第 29 条之规定“处理敏感个人信息应当取得个人的单独同意……”，相较于《中华人民共和国个人信息保护法（草案二次审议稿）》第 29 条之表述“基于个人同意处理敏感个人信息的，个人信息处理者应当取得个人的单独同意……”，其删除了“基于个人同意处理敏感个人信息”这一前置限定仅是为了“使表述更加严谨凝练”〔33〕，而并非要将“单独同意”规则扩张适用于处理敏感个人信息的所有情形。

那么，在基于“合理使用”而处理敏感个人信息时虽无须获得个人的同意，但是否需要履行告知义务呢？即此时信息主体的知情权是否受到限制？从价值判断出发，“合理使用”条款限制了敏感个人信息主体自我决定的权利，即在信息权益保护与信息流通间更侧重于后者，此时是否有必要让信息主体再让渡出知悉自己的敏感个人信息被处理及被如何处理的权益呢？从信息主体的角度看，敏感个人信息毕竟高度关乎自身人格尊严与人身、财产安全，而每个人都是自己利益的最佳守护者，知情权能确保信息处理过程中个人“保持清醒的在场”〔34〕，这不仅让信息主体知情、了解自己敏感信息的去向与状态，更是其做出理性决策、风险评估及行使其他相关权利（如复制权、更正权等）、维护并救济信息权益的前提和基础。从处理者的角度看，恰当的信息披露将给处理者带来必要的合规压力，迫使其接受监督，〔35〕因此，在“合理使用”的情形下设置告知义务虽会增加处理者信息利用的成本，但也能促进其信息处理过程中的谨慎与勤勉。故而，应肯定“合理使用”情形下信息处理者仍有告知的义务。这也契合《个保法》第 44 条规定的知情权，符合《个保法》所规定的“公开”“透明”处理原则。

因此，在《个保法》框架下，告知同意规则中的“告知”，涉及基于“告知同意”及“合理

〔32〕 朱晓峰：《个人信息侵权责任构成要件研究》，载《比较法研究》2023 年第 4 期，第 135 页。

〔33〕 龙卫球主编：《中华人民共和国个人信息保护法释义》，中国法制出版社 2021 年版，第 140－141 页。

〔34〕 王锡锌：《国家保护视野中的个人信息权利束》，载《中国社会科学》2021 年第 11 期，第 130 页。

〔35〕 参见王锡锌：《国家保护视野中的个人信息权利束》，载《中国社会科学》2021 年第 11 期。

使用”情形下的敏感个人信息处理行为；而“同意”仅涉及基于告知同意规则而获准处理他人敏感个人信息的情形，“合理使用”情形无须同意。

2. 告知同意中的特别告知事项

《个保法》第 30 条在第 17 条的基础上增加了敏感个人信息的特别告知事项，再结合第 28 条第 2 款对“目的”与“必要性”的限制，相较于处理一般个人信息，处理敏感个人信息时所涉及的特别告知事项即为处理之“充分必要性”“特定目的”及“对个人权益的影响”。

在敏感个人信息领域，基于高风险与高敏感特征，信息处理行为的必要性被提升至“充分必要性”的高度，处理者的告知义务不仅仅针对处理行为与处理目的（往往表现为某种服务功能的实现）间的关联性而存在，也针对二者间联系的紧密程度而存在，告知需要说明处理之“高于一般的”“充分的”必要性的存在，即属于为实现特定目的而为的最小范围之处理。因此，在一般的必要性要求下，处理者需要向信息主体告知获取、处理其信息是为完成约定或法定的信息处理目的所需要的，其标准应遵循事物的普遍规律性，如用人单位在为入职者办理入职手续时为后续办理社保等事宜而获取其出生日期就满足必要性要求。而在“充分必要性”告知要求下，处理者还需要向信息主体说明此种必要性是“充分”的必要性，即信息的获取与利用不仅是目的实现不可或缺的条件，程度上应解释为一种“必要条件”的紧密关联，且在现有技术条件下不存在可行的替代方案，认知上可解释为“极其”必要，是“最小范围、最短期限、影响最小方式”〔36〕的处理。在告知的描述上不能过于笼统，仍然以入职信息的收集为例，用人单位需要向入职者说明要求其提供本人在某特定银行开户的“一类卡”银行账号是因为单位的开户银行为该银行且需要一类卡账号方能发放工资，即应有相关“充分必要性”要素的阐释，从而为信息主体提供完整、必要的判断要素，此时的告知即满足充分必要性的告知要求。

“特定目的”的告知，意在使信息主体充分、准确了解信息去向与用途，从而进一步判断处理行为的“充分必要性”与“妥当性”。而且，信息处理本就应由信息主体所知悉并形成预期，并且处理不应该超出其合理预期，而特定目的直接关联信息主体对可预见性的期待。〔37〕为便于形成准确、合理的预期，其必须是“特定化的、具体的、明确的目的，而不是泛泛的目的”〔38〕，是应当“符合社会场景价值的目的”〔39〕。这就要求信息处理者在履行告知义务前应将目的特定化下来，〔40〕而且，告知时应就目的做具体化、明确化、清晰化的陈述，不得含混其词，不得做概括式描述，如“为提供一系列服务”“为提供必要服务”“为完善、提升相应服务”等。

“对个人权益的影响”的告知应当针对信息主体人格尊严受到侵害以及人身、财产安全受到危害的可能性、范围、程度而展开，着力弥补信息主体对信息处理活动及潜在风险之专业性认知的不足，便于信息主体对风险形成预期。基于体系解释，这样的告知应当以《个保法》第 55、56

〔36〕 徐磊、刘春：《敏感个人信息保护的实践困境与破解之道》，载《情报理论与实践》2022 年第 3 期，第 48 页。

〔37〕 参见张新宝：《个人信息收集：告知同意原则适用的限制》，载《比较法研究》2019 年第 6 期。

〔38〕 王利明：《敏感个人信息保护的基本问题——以〈民法典〉和〈个人信息保护法〉的解释为背景》，载《当代法学》2022 年第 1 期，第 12 页。

〔39〕 王苑：《敏感个人信息的概念界定与要素判断——以〈个人信息保护法〉第 28 条为中心》，载《环球法律评论》2022 年第 2 期，第 96 页。

〔40〕 See Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation 15 (00569/13/EN 2013), p. 20.

条规定之评估为基础。由于敏感个人信息的诸多特征，其侵害风险与后果往往滞后显现，且会随着场景的变化而不断发生，而且其损害结果通常不可逆。因此，对个人权益的影响之判断与告知应考虑到风险的“非即时性”“潜在性”与“不可逆性”特征。

3. 告知与同意的标准与要求

告知同意规则包括告知规则和同意规则两部分，二者有机联系，协调统一而不可分割。就告知而言，《个保法》第 17 条规定了敏感个人信息处理中的告知标准，但未限制具体形式。“显著方式”“清晰易懂”“真实”“准确”“完整”之标准往往可以采取“弹窗”“超链接”“加粗”“下划线”等形式，并结合语言表达的简练、准确、通俗、不遗漏而实现。在语言表达上，应以普通人而非专业人士之理解能力为标准，尽力弥合处理者与信息主体的技术认知鸿沟，在唤起信息主体对风险的高度警觉的同时，最大化地传递告知事项内涵，使其对信息处理形成充分、完整、准确的理解，便于其实现信息自决、风险自决。在形式的选择上，行业性的规范指引具有重要意义，以《App 违法违规收集使用个人信息自评估指南》为例，其中“评估项 2”之下第 8 点“是否显著标识个人敏感信息类型”之评估标准的列举示例为：字体加粗、标星号、下划线、斜体、颜色等。由是，告知形式的选择应当以能够引起被告知者的充分注意为必要，结合信息处理的具体场景、行业惯例、社会普遍接受的标准，并参酌适用相应领域之特别法与行业规范性文件，实现告知显著、清晰，便于对方知悉。

就同意而言，根据《个保法》第 14 条、第 29 条的规定，处理敏感个人信息的同意，应当“自愿”“明确”作出，且形式上必须是“单独同意”，在法律、行政法规有特别规定时，还涉及“书面同意”的形式要求。所谓“自愿”与“明确”，即同意是在意思自由的状态下，肯定、无疑义地作出。所谓“书面同意”，通常包括纸质确认书、合同书、电报、传真类确认书等。

何为“单独同意”？从《个保法》区分信息类型并赋予不同保护力度的立法态度看，这里的单独同意首先应该解释出信息类型的区隔性要求，即处理敏感个人信息的同意应与处理一般个人信息的同意有所区分，同意应该仅针对敏感个人信息的处理而作出，不得与一般个人信息的处理事项合并。此为对“单独”第一层次的理解。然则，“单独同意”在适用上的最大难点在于明确同意所对应的告知内容所涉事项的单复数、集合性、概括性与划分标准，即单独同意能够涵摄多广的处理事项内容。对此，《个保法》并没有明确规定，实践中争议颇多。“单独同意”是否意味着针对一项敏感信息、一种处理方式、一个处理目的，均需要分别逐项进行同意？有学者认为，敏感信息处理中的同意属于一种特别同意，其要求将一切信息和可能风险告知信息主体，而非一般信息所适用的概括同意，在概括同意中并不一定仅针对一个具体的事项，也可能是针对将来信息处理行为概括的、一揽子的同意。〔41〕有学者认为这里的“单独”应解释为“独立的，不和其他一起的”，即该同意不能与其他信息混同或随意扩增其原有同意范围，其是独立且明确的“专项同意”。〔42〕如何将语义学中的“单独”转化为法学规范层面的“单独”？应当据何标准将告知

〔41〕 参见韩旭至：《个人信息保护中告知同意的困境与出路——兼论个人信息保护法（草案）相关条款》，载《经贸法律评论》2021 年第 1 期。

〔42〕 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。

内容解析为独立的单元，使每一个单元对应得到的同意构成“单独同意”？笔者认为，“单独同意”的规范旨趣在于对敏感个人信息主体的特别保护，力求敏感个人信息的处理风险不仅被突出显示，亦能清晰化、条理化，从而易读，便于信息主体风险自决，但制度设计不能顾此失彼，过于强调保护而严重妨碍信息流动。因此，告知内容要素过于细分的“逐项同意”方案并不可取，这一结论从体系解释出发已得到《个保法》第23条的验证。〔43〕同时，从实践层面出发，过细的逐项同意恐怕也只会让被告知者不胜其扰，无奈做出非理性选择，最终降低“告知同意”的实际效益。究其根源，信息主体同意处理者对其敏感信息进行处理的根本原因在于追求某种特定目的的实现。为此，建议以告知内容中的“特定目的”为框定标准，某项“特定目的”项下的所关联须告知内容（如敏感信息种类、处理方式等）即构成与“单独同意”对应的告知内容单元，该标准下所取得的同意即为“单独同意”。这样的标准粗细适中，不会造成告知内容过繁、告知频次过高，最为关键的是该标准能够使各项告知事项与信息处理目的之间形成明确的逻辑对应关系，使处理者的告知不仅易读，而且易懂，便于被告知者了解信息风险的同时亦能对信息处理之“充分必要性”作出准确判断，从而真正提高被告知者的知悉程度。此外，以“特定目的”为标准框定的告知内容单元，能够科学地划定“单独同意”的边界，合理化信息主体分别做出同意的空间，使就每个单元分别表达意愿成为可能，有效避免“搭售式”“捆绑式”同意的发生。同时，这样的标准也与欧盟GDPR序言所要求的“同意”涵盖的内容标准具有趋向上的一致性。

需要强调，由于告知与同意的对应关系，“单独同意”逻辑上必然要求“单独告知”与之对应，因此，“特定目的”所框定的内容标准同时成为“单独告知”与“单独同意”的标准。此外，按照国际惯例，“预先勾选”等不作为的同意不构成敏感个人信息领域的“单独同意”。

4. 告知同意规则中的动态性机制补强

（1）基于“权益影响”“风险预期”的告知同意动态性机制补强

“信息应用场景的动态化是大数据背景下信息技术的生命力之所在，是信息革命的价值之所在。但是，这种动态化的处理模式也决定了信息主体对知情的要求处于动态化之中……”〔44〕毕竟信息主体在做出事前的同意之后，相关信息所经历的处理与利用及由此引发的风险，即便是处理者本人也未必能完全准确预知，更何况信息主体。而在敏感个人信息领域，对风险的不可完全预知性特征尤强，因此，告知同意规则应对动态性需求有所回应。

《个保法》第17条规定，当处理目的、处理方式、处理的个人信息种类等重要告知事项变化时，处理者应当告知信息主体并获得其同意。这在一定程度上契合了本文所主张的动态性需求。但遗憾的是，《个保法》却未对第30条所涉及的敏感个人信息告知事项——“必要性”“对个人权益的影响”做出动态性的告知同意规范。如前所述，敏感个人信息被侵害的风险高于一般个人信息，为此法律应为其设置更强效的保护规范。故此，学界已有不少呼声主张运用场景完整性理

〔43〕《个人信息保护法》第23条规定：“个人信息处理者向其他个人信息处理者提供其处理的个人信息的，应当向个人告知接收方的名称或者姓名、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……”该条中，单独同意所涉及的告知内容显然是一系列事项集合形成的综合告知内容，而非一事项对应一告知、一同意。

〔44〕 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173页。

论发展、完善敏感信息告知同意规则以满足动态性需求，〔45〕典型如“分层—分阶段—分类”之告知同意规则的提出等。〔46〕场景完整性理论立基于个人信息保护与信息流动间的平衡需以信息所处的不同具体场景而判断，强调对个人信息的处理应维持信息获取时的场景，并遵循相应规则，信息处理者后续的处理行为若脱离原场景，相应的处理行为准则也应变化，以保证信息主体基于特定场景中作出的同意与场景风险相对应，并保障其合理的预期。〔47〕

场景完整性理论为个人信息的处理与保护提供了一种动态调整的可能路径。但遗憾的是，目前该理论对告知同意规则的构建仍然停留在抽象的、一般化的场景导向上，在适用基准与细则上不甚清晰，〔48〕无法直接据此完成敏感个人信息的动态化告知同意，但其为我们提供了一种规制信息行为的思路，即场景转换导致信息风险变化，因而信息主体的期待落空，为此需要动态化的告知与同意，从而使合理预期可以动态地回应敏感个人信息的高风险性。场景完整性理论的适用难点在于决定场景的因素复杂繁多，从而难以形成场景类型化的一致性标准，且各因素的权重也不易确定，但无论使用何种标准完成场景类型构建，皆为实现基于场景的信息风险动态化识别与区分，进而完成动态化告知与同意。而在敏感个人信息的各告知事项中，“对个人权益的影响”最为关乎信息风险的识别，实则是信息风险的另一维度表达，其极具动态性特征的同时也是信息主体形成风险预期、完成信息自决的重要考量事项。在比较法上，美国《消费者隐私权利法案（草案）》提出了基于隐私信息的动态风险及对消费者的权益的影响而应获得动态同意的方案。因此，告知同意规则应针对“对个人权益的影响”这一告知事项作动态性补强，即突破事前的一次性告知规则，在敏感个人信息的处理进程中，当发生“对个人权益的影响”的重要变化（或可理解为信息风险一定程度的升高）时，应再行告知义务并取得信息主体同意才能使信息处理行为继续维持合法性。正如学者言：“在风险分配客观性的基础上，由信息收集利用者成为控制和应对风险的主要主体更具客观性与可行性。”〔49〕因而，此种情况下要求信息处理者承担新的告知义务正当且合理。最终，告知同意规则动态性补强将有利于信息保护与信息流通利用之动态平衡空间的构建。

“对个人权益的影响”是否发生重要变化应当据何判断？在《个保法》框架下，这主要应依托于第 55、56 条规定的“个人信息保护影响评估”。换言之，基于风险控制与风险分配实现的告知同意规则的动态化设计，应该依赖动态化的影响评估。当然，目前《个保法》第 56 条中的评估仅为事前的一次性评估，这很难满足大数据时代个人信息保护的需要。针对敏感个人信息的保

〔45〕 正是基于风险的动态性，有学术观点认为应该用场景完整性理论取代“告知同意”规则，进行完全基于场景的动态性信息行为规制。

〔46〕 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。

〔47〕 See Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Washington Law Review 119, 120 - 148 (2004); Daniel J. Solove & Paul M. Schwartz, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 New York University Law Review 1814, 1815 - 1859 (2011); Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009, pp. 129 - 157.

〔48〕 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。

〔49〕 姚佳：《知情同意原则抑或信赖授权原则——兼论数字时代的信用重建》，载《暨南学报（哲学社会科学版）》2020 年第 2 期，第 50 - 51 页。

护影响评估，亦应进行必要的动态化补强。正如有学者强调，“在相当长的一段时间内，理论界与实务界把敏感个人信息保护影响评估的焦点放在‘处理目的、处理方式等是否合法、正当、必要’的单一评估模式上”，“理论界存在将敏感个人信息保护影响评估的重心转移到‘对个人权益的影响及安全风险’评估上来的趋势”〔50〕。由是，在场景完整性理论逻辑思路的启发下，我国法上告知同意规则的动态性补强可考虑引入动态系统论的评价体系，合理设置相关评价要素与权重，实现敏感个人信息保护影响的动态化评估，进而以此为依据实现“对个人权益的影响”的动态化告知同意，基于对风险变化的充分、及时知悉，使信息主体的同意动态地符合其预期，实现风险的分配正义。最终，动态化的风险披露与个人权益影响告知也必将使得“撤回权”的行使更有依据且有意义。

（2）“潜在型”敏感个人信息的告知同意规则

此外，在场景完整性理论与动态化规制的思维背景下，存在潜在敏感个人信息的两种典型情况，其告知同意规则的适用转换需要予以考虑。一般而言，实定法应对敏感个人信息的范围、类型作出初步界定，一项信息最终是否归入敏感个人信息，往往还需要进行结合实际的具体衡量，衡量时“强调动态客观的判断标准”〔51〕。归入敏感个人信息者，即当适用相应的强告知同意规制。但在下列两种特殊情形下，会发生非敏感信息向敏感信息的转化，即在信息的首次采集阶段，信息仅属于一般个人信息，但在后续的处理过程中其转化为或识别出敏感个人信息，此时，信息的持有及处理应考虑适用敏感个人信息之强告知同意规则。

情形一：信息的敏感度与处理方式、算法技术、数据库类型，甚至是数据库的容量高度相关，因此，属于非敏感信息的原始数据，经过专业的大数据聚合分析、深度挖掘、数据库关联比对等信息技术的处理，很可能转化或识别出敏感个人信息。例如网络购物平台掌握消费者的实名手机号码、购物列表、搜索记录清单后可以分析出信息主体的性取向、医疗健康等敏感信息，再通过比对其他数据库信息，如购物平台注册账号信息数据库中的信息，完全可以实现主体身份的识别，实现匿名化突破，获得敏感个人信息。其实，早在20世纪90年代末期，技术人员已经意识到匿名化仅仅是一种技术上的理论假设。〔52〕又如，有信息处理者通过实验证明，在掌握邮政编码、出生日期、性别三项信息后，通过多个数据库的联合比对，可以有87%的可能识别出信息主体的名字（实践中这一比例经常接近100%），甚至最终破解多项与特定身份相关的信息。〔53〕再如，长期的、连续时间段的地理位置信息的采集可以通过数据合并识别出行踪轨迹及隐私行为偏好等敏感个人信息。〔54〕这种非敏感信息向敏感信息转化的可能性会随着信息技术的日益进步而不断提高，〔55〕亦会随着数据信息渠道的扩张与互通而不断提高，从而出现学者描述的，微小

〔50〕 杨显滨：《我国敏感个人信息处理规则的规范解释与体系构造》，载《学术月刊》2022年第10期，第116页。

〔51〕 朱晓峰、黎泓玥：《私密信息与敏感个人信息区分保护论》，载《经贸法律评论》2023年第1期，第23页。

〔52〕 See Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA Law Review 1701, 1716 (2010).

〔53〕 See Jonathan Shaw, *Exposed: The Erosion of Privacy in the Internet Era*, September-October 2009 Harvard Magazine 38, 39 (2009).

〔54〕 See Paul Ohm, *Sensitive Information*, 88 Southern California Law Review1125, 1131－1189 (2015).

〔55〕 See Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 Columbia Business Law Review 494 (2019).

的隐私风险意外地成倍增加，形成累积性的风险效应现象。〔56〕为此，在静态的、事前的告知同意规则框架下，有学者甚至建议“禁止未经允许的以识别个人或推测个人敏感信息为目的的二次数据处理”〔57〕。当然，这样的禁止虽加强了对信息主体信息权益的保护，但却不利于数据信息的利用，有悖大数据时代信息社会的本质。何况，有的信息处理行为在处理之初并未预设或并不能预见处理后果将导出敏感个人信息，正如学者言，“大数据分析的奥秘就在于，在数据分析之前根本就没有‘目的’——分析师们也不知道会产生什么样的结果”〔58〕，因此，一刀切式的禁止处理并非良策，将其纳入敏感信息的保护框架、适用强告知同意规则，更能实现个人信息保护与个人信息利用的动态平衡。

情形二：个人信息的“敏感度”并不稳定，受很多变量因素的影响，因此，敏感度在不同的场景下有不同的呈现。〔59〕当属于非敏感个人信息的数据信息向其他信息处理者提供后，基于场景的转换，非敏感信息有可能异变为敏感信息。例如在某次文化活动中信息处理者获得了与基因有关的血型信息，基于场景，该信息或许并不敏感，但保险业者通过其他合法途径（如基于告知同意的向第三人传输）获取该信息后，该信息在新的场景下可能转化为敏感个人信息。〔60〕虽然针对信息传输行为《个保法》第 23 条已作出规定，即此时前位信息处理者需要进行单独的告知并取得同意，但这样的规定并未使信息处理行为受强告知同意规范的完整约束，亦未使之受“特定目的”“充分必要性”“采取严格保护措施”等限制性处理规则的约束，从而往往形成学者所描述的“多元信息处理主体的存在及与用户直接联系的缺失，使得对个人信息后续利用的第三方主体尤其是数据中间商的监管几近真空”〔61〕的局面。

因此，上述两种典型情况下，当信息类型发生异变时，信息风险增大，为重新建立信息主体的合理预期，处理者的告知义务应当加强，即针对类型异变后的信息，无论是知悉、持有，抑或是后续的处理，都应当适用敏感个人信息之强告知同意规则，此时如果不能取得信息主体的单独同意，处理者应当删除该敏感个人信息。

五、结　语

信息风险社会，告知同意规则的制度价值应该被重新认识，其不仅能实现信息自决，亦能发挥风险预防与风险分配之功能。敏感个人信息的高风险性特征决定了其应适用强告知同意规则；又基于其风险的动态性特征，信息保护和数据开发利用之间需要实现动态的利益平衡，应在立法

〔56〕 See Aaron Fluitt, Aloni Cohen, Micah Altman, Kobbi Nissim, Salome Viljoen & Alexandra Wood, *Data Protection's Composition Problem*, 5 European Data Protection Law Review 285, 292 (2019).

〔57〕 吴标兵、许和隆：《个人信息的边界、敏感度与中心度研究——基于专家和公众认知的数据分析》，载《南京邮电大学学报（社会科学版）》2018 年第 5 期，第 52 页。

〔58〕 龙卫球主编：《中华人民共和国个人信息保护法释义》，中国法制出版社 2021 年版，第 65 页。

〔59〕 See Kirsten Martin & Helen Nissenbaum, *Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables*, 18 Columbia Science and Technology Law Review 176, 215 (2016).

〔60〕 参见韩旭至：《个人信息类型化研究》，载《重庆邮电大学学报（社会科学版）》2017 年第 4 期。

〔61〕 范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016 年第 5 期，第 94 页。

完善上考虑增加以“权益影响”“风险预期”为考量指标的动态告知同意规则；同时，应通过对“告知”与“同意”之内容、形式、标准等规范要素的恰当解释实现规范意旨，努力克服告知同意规则的缺陷。

敏感个人信息的大数据利用场域丰富多样，各情境下敏感信息及处理行为各具特点，风险预防与风险分配实现中需要回应不同的需求，而作为领域基本法的《个保法》仅能对告知同意做出框架性规范。因此，由第17条、第30条等条款所规定的敏感个人信息告知事项、告知形式与告知标准等细节无法形成完全统一、细致且确定的规范标准。对此，一方面，针对其中的典型利用场景可考虑经由类型塑造而由特别法做出重点规范，在特别领域、特定行业，经由特别立法、司法解释或行业性特别规范予以确定，或提供范例指引；另一方面，敏感个人信息之保护与冲突利益间的平衡除仰仗信息行为规范的设计外，亦应强调保障其落实的机制。因此，应考虑在一定规模、掌握一定信息数据量的数据企业（平台）实行相关告知内容与同意形式的审查、备案制，并对其实施情况予以监督；同时可以考虑将如上企业的告知文件、隐私政策等参照格式合同条款予以规范和管理，从而通过国家之力消弭因“持续性的信息不平等关系”引发的告知同意规则的内、外部自限性缺陷。相信通过科学、合理、有效的“告知同意”设计，可以实现信息风险的有效控制及信息主体对风险的合理预期。

Abstract: The Personal Information Protection Law distinguishes between types of information and provides a reinforced informed consent rule for sensitive personal information. The informed rule has its own institutional logic and many self-limiting shortcomings. It is based on the primary value of information self-determination. In the information risk society, the informed consent rule is still of great significance in the protection of sensitive personal information. It should be explored and endowed with new values and functions, i. e., risk prevention and risk distribution. At present, in order to accurately apply the informed consent rule for sensitive personal information and eliminate the uncertainties in the law and the shortcomings of the system, the scope of application of the informed consent rule, the informing matters and standards, and the consenting forms and requirements should be appropriately interpreted to realize the self-determination of the information, and at the same time, achieve the control of the risks better. Meanwhile, according to the dynamic characteristics of the “sensitivity” and “risk” of sensitive personal information, the notice and consent rule should be supplemented with dynamic mechanism, so that the information processing meets the risk expectations of the subject of the information.

Key Words: sensitive personal information, informed consent, risk control, separate consent, dynamicity

（责任编辑：徐建刚）