大数据时代个人信息的法律保护研究

赵伟婷

云南民族大学，云南昆明，650504；

摘要：随着信息技术及互联网的快速发展，我国正稳步迈入大数据时代，数据资源化的发展趋势加快了科技创新的步伐，同时也给个人信息保护带来了前所未有的挑战。大数据环境下传统的“知情—同意”规则似乎已经捉襟见肘。为有效保护个人信息权益，本文尝试引入场景风险理论，进一步细化我国个人信息的保护规则，并针对我国实际提出完善个人信息保护的建议。

关键词：个人信息保护；告知同意；场景风险

DOI：10.69979/3029-2700.25.10.062

引言

大数据的普及和利用给人们的生活带来了多样化的选择，与此同时也带来不可忽视的个人信息保护危机。大数据时代商业模式快速革新，平台经济、算法推荐等新事物进入人们的视野，数据、信息越来越成为交易环节之一。例如近年来频繁出现的APP过度收集个人信息、互联网开盒、算法歧视等现象，都给个人信息保护带来了极大的挑战。因此，现阶段我国亟需构建完善的个人信息保护体系，以应对大数据时代的新挑战及协调好个人信息保护与数字经济发展的重大课题，探索大数据时代个人信息保护的可行路径。

1 大数据背景下个人信息保护的适用困境

大数据时代，个人信息保护的目的是防止滥用，同时合理规范运用个人信息，以实现数据价值和人格权益的平衡。我国《个人信息保护法》《民法典》规定个人信息的处理应遵循“知情—同意”规则，要求信息处理行为要为信息主体知晓且同意。然而大数据时代的个人信息保护存在数据安全与数据利用之间的价值冲突，两者呈现一定的紧张关系：若设下过多前置条件将不利于创新发展，而一味给数据处理者开绿灯又与个人信息保护的宗旨不符。

如何界定“合理使用”便成为个人信息保护领域不可回避的问题，传统的“知情—同意”规则对于大数据时代个人信息保护已是捉襟见肘。第一，“知情—同意”规则与数字时代发展趋势不符。其要求信息处理者在收集之前告知用户收集情况并征得同意，一般表现为APP的隐私条款。为应对法律检查，开发商会列出复杂冗长、专业性极强的隐私条款。然而，逐一阅读隐私条款的人极少，大多数用户直接点击同意以开启应用程序的使用，此种形式化告知的方式极大削弱了知情同意规则的实际效果。第二，个人信息的控制权被架空。“知情—同意”强调个人对信息的自决权益，预想用户通过同意条款来实现其控制权。然而隐私条款只有“是”与“否”两个选项，若用户选择“否”，将不能使用APP。在一定程度上侵犯了公民的自主选择权，也相当于架空了用户对个人信息的实际控制权。第三，超出授权范围获取个人信息。数据作为大数据时代的“石油”，当数据量越大，可挖掘有价值的信息也就越多。现实中，不少平台利用技术手段、格式条款获取同意，实际收集的信息远远超出个人授权的范围，而该同意条款相当于平台攫取数据的免责声明。

“知情—同意”规则似乎不再适应我国个人信息保护的实际需求，为有效保护大数据时代的个人信息权益，下文将引入场景风险理论，着重分析其可行性，同时结合我国实际提出个人信息保护的完善建议。

2 场景风险理论的概述

2.1 场景风险理论的可行性

“场景”一词源于尼森鲍姆的“情景脉络完整性”理论，指个人信息的后续使用、传播不能超过初始场景所预期的范围，在判断个人信息权益是否受损时可结合具体场景进行合理性考虑。欧盟《数据条例》及美国《消费者隐私权利法案（草案）》强调防范个人信息处理对个人造成损害，为“风险评估理论”奠定了基础。尽管“场景”与“风险”理念代表着两个维度，但二者最终都聚焦于保护个人信息保护的目标上。“场景”是出发点，“风险管理”是实现手段，风险评估与管控需围绕特定的场景进行，场景所涵盖的各项要素同时也构成风

险评估的具体衡量指标。[1]97在评估个人信息处理是否超过了同类场景下可预见的范围，亦要求信息处理者对于信息处理过程实施风险管理，以保障个人信息的安全。在实际生活中个人信息的利用场景多样化，基于不同的场景，信息主体将会产生不同的预期，例如日常闲聊与邮件来往，显然对后者保密性的预期会高于前者。并且，我国个人信息保护规则中也没有完整体现实际场景下风险指数、风险类别，对司法裁量也造成了一定困难。

尼森鲍姆认为个人信息保护并非着眼于信息类型，而是其分配和传输是否遵循场景所预设的信息规范准则。可见，场景风险理论主张相同信息、相似信息处理行为在不同的场景中会产生不同的法律后果。例如，在梁某诉汇法网一案中，汇法网通过技术手段抓取涉梁某信息的判决书并转载于其网站，梁某多次要求删除未果遂起诉。法院以公众监督权为重点，认为裁判文书真实，未含有侮辱诽谤等内容，所以不侵犯梁某的个人信息权益；而在伊某诉启信宝一案中，法院着重关注个人的信息控制权，认为贝尔塔公司收到删除要求未及时处理，有悖于伊某对已公开信息进行传播控制的意思表示，违反了合法性、正当性、必要性原则，最终支持伊某的诉求。[2]两案结果差异的实质在于不同场景下个人对已公开的个人信息再传播享有的控制权和裁判文书公开的利益之间何者占优先地位的问题。

引入场景风险理论有助于缓解“知情—同意”的适用困境，对个人信息的处理不再是“是”与“否”二元对立的判断，而是综合考量。不同信息主体对个人信息将产生不同预期，信息处理者根据信息主体的合理预期来判断是否需征求同意，如此一来，提高了信息处理的效率，也减少了信息处理过程中不必要的障碍。

在场景风险理论下，个人信息保护应遵循以下原则。第一，动态平衡原则。场景风险理论结合具体场景评估风险，强调的是一个动态过程，将信息处理风险控制在预期范围的行为。这便要求评估时根据场景的变化，对个人信息采取动态保护。第二，必要原则。对于“必要”的理解，张新宝认为必要包括充足、相关、不过量等要素；谢琳认为“必要”包括两方面，其一数据应以最小利用为限，其二处理方式产生的影响最低。可以说，必要性是针对处理手段的规范，在必要限度内处理和保护个人信息。第三，正当性原则。大数据时代，数据作为新的生产要素，进行数据利用、交易已不再陌生。个人信息具有较大价值，但对个人信息的收集要取之有度，调整好个人信息处理的手段与目的之间的关系。

2.2 场景风险理论与个人信息的保护

我国《民法典》第一千零三十四条明确个人信息定义及类型，该条款对个人信息作了兜底规定，然而此种定义并不能涵盖生活中复杂的个人信息类型，实际上，个人信息的界定是动态的，同时依赖于具体场景。在侵害个人信息的案件中，判断个人信息的处理是否给信息主体带来隐私风险时，并非着眼于其“是否构成个人信息”，而是该处理行为在特定情境下怎样被使用以及是否契合用户在相应场景中的合理预期。[1]100

场景风险理论在我国立法和司法裁判中都有所体现。在立法中，于 2025 年 6 月施行的《人脸识别技术应用安全管理办法》，对不同的应用场景、环节设定了差异化的法律义务和监管要求，对重点场景做出了针对性的规定。明确不得在旅馆客房、公共卫浴等可能侵害他人隐私的场景安装人脸识别设备。在公共场所安装图像采集、个人身份识别设备的场景，明确应为维护公共安全所必须，依法合理采集并设置显著标识。有效回应了实践中的“刷脸乱象”，通过个人信息影响评估制度、备案手续增强信息处理者的责任意识同时方便监管。

在司法裁判领域，我国相当大部分的判决也采取了场景风险理论。著名的郭兵诉杭州野生动物世界案、微信读书案、余某某诉查博士案中法官进行裁判说明时也多次提到“场景”和“合理预期”，在一定程度上也为个人信息的法律保护提供了方向。

以微信读书案中的读书信息为例，黄某认为微信读书 APP 未经同意，擅自获取好友关系并自动关注，同时将读书信息默认开放的行为侵犯其个人信息及隐私权。在该裁判过程中，法官以场景化模式进行综合考虑：首先，将微信好友关系迁移到微信读书不符合一般用户的预期。微信几乎承载了用户的全部社会关系，应用软件通过技术手段将此类社交关系迁移明显超越用户的合理预期。

其次，超强的数据分析能力增加用户个人信息泄露的风险。据《微信读书软件许可及服务协议》读书信息包括但不限于用户的书架、正在阅读的读物、读书想法及读书时长等主要痕迹。大数据强大的分析能力可以将用户的书架、想法、划线等进行组合并一定程度勾勒出用户具体的人格画像。用户有权自己决定是否将其公之于众，而微信读书未经同意将此类信息公开的行为可能会加剧个人信息泄露的风险。

第三，微信读书未以较高的“透明度”合理告知用户并获得同意，具有一定过错。微信读书获取同意的方式不够明确，协议直接以无提示的方式规定读书信息不属于个人隐私或不能公开的个人信息，意图规避法律风

险。即使软件配有私密阅读设置，但此种不明确的告知方式会影响用户的真实选择。因此，在该场景中读书信息应被归类为个人信息范畴，在未明确告知的情况下，App 运营者的行为明显不符合用户的合理预期，运营者存在过错，构成对个人信息权益的侵害。

3 场景风险理论下个人信息保护的完善建议

场景风险理论在我 1 国立法及司法中的适用，为我国个人信息保护提供了全新的视角。但新视角的引入并不意味着彻底解决了我国个人信息保护的问题，当务之急是将场景风险理论融入我国个人信息保护的本土化实践中。[3]

3.1 构建个性化评价方案

信息、数据的动态性极强，因此无法脱离具体的场景作单一判断。场景风险理论下个人信息权益的界定是动态的，其并不存在一个精确的定义，在判定时着重考量“被使用的方式”是否符合信息主体在该场景中的预期。在判断个人信息是否受损时，宜采取个性化的评价方案。逐渐弱化在个人信息收集阶段的明确区分，加大对个人信息使用阶段的评估，明晰个人信息被使用的场景是否符合信息主体的同意预期。

将个人信息的使用场景分为两类：一是以营利为目的处理个人信息，二是以维护公共利益为目的，对于前者设置与之相配备的强制同意规则，对后者可允许其在适当范围内处理个人信息，同时应明确基于公共需要处理个人信息的场景应符合必要性条件，公共主体在处理个人信息时需满足比例原则。对于前者处理个人信息的情形，重点考虑以下几个因素：用户对于平台收集信息的认知能力；平台提供的产品和服务的范围；平台处理信息的用途等，平衡好个人信息的利用与保护之间的关系。

为有效推动个人信息的保护，还可引入第三方监管机构。从个人信息的界定、分类、使用场景进行理论化的探究，对信息的处理、利用提出参考性意见。一方面，第三方机构的意见能为裁判提供思路，另一方面，可对数据处理者的行为进行监督并出具评估报告，若其违规两次以上则撤销其信息处理资格并予以惩罚。

3.2 明确风险管理责任分配

在我国本土化实践中，对个人信息利用是否合理应结合“风险管理”和“处理目的”两方面进行考虑，将处理信息的风险控制在合理的范围内。具体的考虑因素包括：第一，信息敏感程度。一般个人信息和敏感个人信息都属个人信息，但其敏感性程度不同，敏感度越高的信息，其处理越受限。第二，信息处理者的风险控制能力。风控能力越强，其风险发生的可能性越低、风险的危害性也越低。第三，处理目的适当。允许一般个人信息的处理与初始目的存在一定偏离，但必须与初始目的存在包含关系，若处理信息不适当产生的风险超出信息主体的预期，则为法律所禁止。

同时，要求信息处理者对风险进行评估，并对评估结果划分等级。当风险评估结果较低时，可以视为信息主体对处置行为已作出授权；若评估为高风险，则要求处理者必须向信息主体披露，并向信息主体作出是否继续的提示，若用户选择继续，信息处理者需对用户的信息安全作出防范措施。如此一来，增加了用户个人信息保护的透明度，同时也减轻了信息处理者的负担。

4 结语

大数据技术的发展对新时代个人信息的保护提出了更高的要求，个人信息安全和数字经济发展，二者同样重要。通过构建个性化评价方案、明确风险管理和责任分配来完善大数据时代的个人信息保护，在不同的应用场景配置不同的“同意”规则。同时明确信息处理者的风险评估及安全保障责任，构建完善的个人信息保护体系。

参考文献

[1]范为.大数据时代个人信息保护的路径重构[J].环球法律评论,2016,38(05):92-115.
[2]孙玉荣,卢润佳.“场景完整性理论”的应用检视和功能再造——以个人信息保护司法裁判为视角[J].北京联合大学学报(人文社会科学版),2022,20(03):70-79.
[3]邢会强.个人信息保护:从场景理论到差异性原理[J].经济法研究,2024,25(01):39-69.

作者简介：赵伟婷（1999.10-），女，白族，籍贯：云南大理，云南民族大学民商法学研究生，研究方向：民商法学。