财经法学 No. 2，2023
pp. 21 - 35

敏感个人信息的界定及其完善

莫　琳*

内容提要：敏感个人信息的界定是我国《个人信息保护法》的重要内容。因为比非敏感个人信息更能反映和影响个人信息主体的重大利益，《个人信息保护法》对敏感个人信息采用更为严格的保护制度。《个人信息保护法》第 28 条第 1 款对敏感个人信息的界定采取客观风险标准。在法学视角下，“敏感”与“高度损害风险”相关联，敏感个人信息处理的损害风险程度较高。损害风险可以单独或同时来源于个人信息内容的固有性、个人信息被非法使用时的工具性以及非敏感个人信息与敏感个人信息的关联性。《个人信息保护法》对敏感个人信息的界定尚不能涵盖所有损害风险来源，应在第 28 条第 1 款的基础上辅以场景化路径界定敏感个人信息，具体以个人信息是否揭示或关联敏感内容、受损害主体是否包括其他关联利益人为客观考虑因素。

关键词：个人信息保护法　敏感个人信息　损害风险　场景一致性理论

一、引　言

2021 年 8 月 20 日，我国在个人信息保护领域的专门立法《个人信息保护法》出台，明确将个人信息分为敏感个人信息和非敏感个人信息。由于敏感个人信息比非敏感个人信息更能反映和影响个人信息主体的重大利益，且与个人人身、财产权利的联系更为密切，敏感个人信息在一般个人信息处理规则的基础上，适用更为严格的保护制度。《个人信息保护法》在第二章中设专节规定敏感个人信息的处理规则，主要包括：个人信息处理者处理敏感个人信息的前提条件为“具有特定目的＋充分必要性＋采取严格保护措施”（第 28 条第 2 款）；应当取得个人的单独同意或是书面同意（第 29 条）；处理不满 14 周岁未成年人个人信息应当取得其父母或者监护人的同意，

* 莫琳，暨南大学法学院博士研究生。
本文为国家社会科学基金重大项目“国际法与国内法视野下的跨境电子商务建设研究”（17ZDA141）的阶段性成果。

并为此制定专门规则（第 31 条）；应当遵守法律、行政法规规定的其他限制条件（第 32 条）。个人信息处理者处理敏感个人信息的义务还包括必须进行事前影响评估（第 55 条）。纵观不同法域的理论基础、立法情况以及行业规范，敏感个人信息保护规则存在的意义在于，防范其处理过程中极易产生的高度损害风险。敏感个人信息处理规则是我国《个人信息保护法》的重要内容之一，给予敏感个人信息特殊保护的做法与世界主流个人信息保护立法规则保持一致，标志着我国从制度上保证了个人信息保护体系的完善，为信息化社会中新型经济的有序发展提供了坚强有力的保障。

敏感个人信息特殊保护的首要问题应聚焦于如何界定敏感个人信息。《个人信息保护法》对此采取了“抽象概括＋非穷尽式列举”的界定方式。“概括”涉及法律如何给出概念（即下定义），“列举”涉及行为如何罗列。〔1〕其第 28 条第 1 款规定，敏感个人信息是指“一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息”。此为在法律规范中抽象界定敏感个人信息的内涵和外延，给予综合性定义，并明确列举敏感个人信息的非穷尽性示例。列举类型既依据信息内容，又以年龄为划分界限。该款规定凸显了我国当下急需保护的敏感个人信息类型，具备实践上的指引性，该表述也为未来技术与商业模式变化所可能出现的新型敏感个人信息预留了一定空间。

我国《个人信息保护法》中的“敏感”一词已完成由日常语境向法律语境的含义转化，但敏感个人信息的界定依然存在边界模糊的争议，尚不能涵盖所有损害风险来源。虽体现了敏感个人信息损害风险来源中的个人信息内容的固有性和个人信息被非法使用时的工具性，但却忽略了非敏感个人信息与敏感个人信息的关联性，难以及时跟上未来个人信息保护进程。因此，有必要进一步完善敏感个人信息的界定，以场景化路径丰富敏感个人信息的界定视角。本文首先深度剖析敏感个人信息的内涵，解释“敏感”一词在法律语境中的含义转化，对敏感个人信息的高度损害风险进行类型化分析。其次，基于损害风险来源检视我国《个人信息保护法》第 28 条第 1 款，进而结合场景一致性理论框架论述其在敏感个人信息方面的应用考量。最后，为推动我国构建多层次敏感个人信息保护体系而提出彰显时代性的敏感个人信息界定的完善建议。

二、敏感个人信息的内涵界定

（一）“敏感”一词在法律语境中的含义转化

如何理解法律语境中的“敏感”一词，是明确界定敏感个人信息内涵的首要前提。“敏感”在日常语境下具有较强主观性，通常用来表示个人的强烈感官输入。在心理学领域，敏感通常与焦虑等情绪相生相伴。“焦虑敏感性”是指应激事件使个体产生的担心、恐惧等情绪，是个体身上的一种稳定人格特质。〔2〕“感觉加工敏感程度”（sensory processing sensitivity，简称 SPS）

〔1〕 参见谢晓尧：《法律文本组织技术的方法危机——反思“互联网专条”》，载《交大法学》2021 年第 3 期。

〔2〕 参见杜艳玲、郎红娟、高丽、贺世喆、曹宝花：《军人焦虑敏感与心理应激关系及心理弹性中介作用的研究》，载《华南国防医学杂志》2021 年第 2 期。

被描述为一种由遗传决定的气质或人格特征，能够反映个体中枢神经系统敏感程度的增加以及个体对身体、社会和情绪刺激的深层次认知加工。〔3〕敏感情绪是一种“感官防御”（sensory defensiveness），与自身的经历、经验和行为有密切关系。〔4〕由于心理学上的个体敏感程度高低极具差异，“敏感”一词在法律语境中的含义需进行转化理解，不能直接以日常语义理解敏感个人信息。显然，敏感个人信息并非单纯指代“令个人产生敏感情绪的个人信息”。否则，无异于将界定敏感个人信息的决定权完全交由个人信息主体，缺乏明确标准。因此，在法学视角下，“敏感”与“高度损害风险”相关联，意味着处理敏感个人信息而产生的损害风险程度较高。通过剖析我国《个人信息保护法》第28条第1款的内在逻辑可知，界定敏感个人信息采取客观风险标准。正是由于敏感个人信息处理往往伴随着高度损害风险，才值得法律对其严格保护。

世界主流国家的敏感个人信息保护理论和实践，都基本完成了对“敏感”一词在法律语境中的含义转化。美欧信息隐私法认为敏感个人信息往往与更大的风险相关联，因此，对敏感个人信息处理进行风险评估是必不可少的步骤。〔5〕在个人信息保护中，风险评估具有重要意义。〔6〕根据美国法律，处理敏感个人信息被认为是高风险行为。21世纪初，美国《关于执行电子政府法案的指南》（Guidance on Implementing the E-Government Act）就已指出，考虑到个人健康和财务信息的隐私风险增强，要求监管机构在处理个人健康和财务信息前对其进行隐私风险影响评估。欧盟《一般数据保护条例》（General Data Protection Regulation，简称GDPR）以个人信息的性质为基石，在其鉴于条款中指出，敏感个人信息值得法律特别保护的基本理由在于，敏感个人信息在具体处理场景下可能会对个人基本权利和自由造成重大风险。〔7〕即敏感个人信息是其处理可能给基础权利和自由带来高度损害风险的一类个人信息。

“敏感”一词的法律化过程虽弱化了其主观性，但并非完全摒弃个人信息主体的内在感受。界定敏感个人信息离不开社会公众基于一般经验和生活常识的整体性价值认可。〔8〕法律依然需要考虑社会公众在具体场景下对个人信息敏感与否的认可程度，而非指个案中单一个人信息主体的纯粹心理情绪。保罗·欧姆（Paul Ohm）评估某一个人信息是否敏感时指出，需要考虑处理该个人信息的风险是否反映了多数主体的利益。〔9〕有学者对比多个国家和地区的隐私保护法律后发现，法律规范已列举的敏感个人信息类型获得社会公众的较高认可。〔10〕受区域历史文化、道德观念等多方面因素的影响，大多数国家和地区都认可医疗健康信息是敏感个人信息。其来源

〔3〕 See E. N. Aron, A. Aron & J. Jagiellowicz, Sensory Processing Sensitivity: A Review in The Light of The Evolution of Biological Responsivity, 16 (3) *Personality and Social Psychology Review* 262 (2012).

〔4〕 See Sofie Boterberg & Petra Warreyn, Making Sense of it All: The Impact of Sensory Processing Sensitivity on Daily Functioning of Children, 92 *Personality and Individual Differences* 80, 81 (2016).

〔5〕 See Muge Fazlioglu, Beyond the “Nature” of Data: Obstacles to Protecting Sensitive Information in the European Union and the United States, 46 (2) *Fordham Urban Law Journal* 271, 306 (2019).

〔6〕 参见刘颖：《我国〈个人信息保护法〉中的“守门人”条款》，载《北方法学》2021年第6期。

〔7〕 See General Data Protection Regulation, Recital 51.

〔8〕 See Karen McCullagh, Data Sensitivity: Proposals for Resolving the Conundrum, 2 (4) *Journal of International Commercial Law and Technology* 190 (2007).

〔9〕 See Paul Ohm, Sensitive Information, 88 (5) *Southern California Law Review* 1125, 1155 (2015).

〔10〕 参见王敏：《敏感数据的定义模型与现实悖论：基于92个国家隐私相关法规以及200个数据泄露案例的分析》，载《新闻界》2017年第6期。

于个人信息主体在医疗、健康、卫生领域的社会活动，不仅是反映个人人格权益的信息载体，还是具有公共属性的社会工具。〔11〕这反映了社会公众对某类个人信息是否敏感存在着合理期待，具有不希望其被泄露和非法使用的诉求。〔12〕因此，在具体场景中判断敏感个人信息是否符合社会公众的合理期待，应是法律所允许的合理考虑。

（二）敏感个人信息的高度损害风险

1. 损害的类型

敏感个人信息的高度损害风险不只是带来主观上的人格损害，即个人信息一旦被泄露或者被非法使用给个人信息主体造成的消极感受，还包括在客观上造成的人身损害和财产损害。第一，人格损害关乎个人基本权利与自由，如侮辱、羞耻以及遭受歧视性待遇等强烈主观性不适带来的精神损害。敏感个人信息的损害风险类型已从传统的识别型向歧视型、控制型扩散。〔13〕与非敏感个人信息相比，敏感个人信息更容易导致人格损害已在国际立法层面形成共识。1981 年，欧洲理事会公布的《关于个人数据自动化处理的个人保护公约》（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data，简称 108 公约）特别指出，数据处理应采取保障措施防止敏感个人信息对个人信息主体的利益、权利和基本自由可能造成的风险，特别是造成歧视的风险。同时，反对任何形式的歧视行为也是联合国人权保护的重要内容。比如，未经本人同意透露一个人的遗传信息可能会使其在就业、保险、教育和社会生活的其他领域受到歧视。〔14〕“保障人权”和“守护人类尊严”等全球性伦理准则共同为保护敏感个人信息以防范人格损害提供了理论支撑。因此，宗教信仰、医疗健康以及特定身份等敏感个人信息被多数国家的个人信息保护立法所认可，并为不同国家的社会公众所普遍珍视。

第二，人身损害是指敏感个人信息的不当处理可能危及个人人身安全。涉及保障人身安全目的的敏感个人信息包括身份证件号码、电话号码、电子邮件地址、家庭和工作地址以及实时位置等信息。这些敏感个人信息的损害风险来源于，其能够高度识别个人身份并与个人人身安全相关联。一旦泄露极易被不法使用，容易导致个人信息主体遭受人身损害。

第三，财产损害指的是经济价值损失，包括财产实际损失和期待利益损失。例如，作为敏感个人信息的金融财务信息往往容易导致可以衡量的经济损害。支付宝平台中的花呗、芝麻信用等信贷产品改变了许多人的消费习惯。我国法院在案件处理过程中意识到，金融服务行业涉及诸多敏感个人信息类型，与公民的资金安全直接相关，若处理不当可能引发金融风险。〔15〕我国司法实践中已有不少案例表明，处理贷款情况、征信报告、银行流水账单等个人信息具有高度损害风

〔11〕 参见莫琳：《公共卫生安全视角下医疗健康个人信息的保护与限制》，载《电子知识产权》2022 年第 5 期。

〔12〕 参见吴标兵、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。

〔13〕 参见宁园：《敏感个人信息的法律基准与范畴界定——以〈个人信息保护法〉第 28 条第 1 款为中心》，载《比较法研究》2021 年第 5 期。

〔14〕 参见联合国经济及社会理事会决议《基因隐私权与不歧视（E/2004/L. 13/Rev. 1）》（2004/9 ）。

〔15〕 参见“蚂蚁科技集团股份有限公司与海南庆德大信息科技有限公司侵害商标权纠纷案”，杭州铁路运输法院（2020）浙 8601 民初 489 号民事判决书；“芝麻信用管理有限公司、蚂蚁科技集团股份有限公司等与山西有码科技有限公司侵害商标权纠纷案”，浙江省杭州市西湖区人民法院（2020）浙 0106 民初 4288 号民事判决书；“蚂蚁科技集团股份有限公司与杭州融动科技有限公司侵害商标权纠纷案”，浙江省杭州市西湖区人民法院（2020）浙 0106 民初 4289 号民事判决书。

险，符合社会公众对此类信息的认知程度和整体性期待。此外，处理敏感个人信息还容易造成期待利益损失。在相关案例中，个人信息处理者不当处理医疗健康个人信息，容易造成个人信息主体的期待利益损失。例如，药店留存的个人用药记录存在错误录入的情况，将导致消费者无法购买商业保险保障自身权益，之后就医使用医保卡也难以得到相关保障，〔16〕这对医疗健康个人信息的应用活动造成了财产损害。

2. 损害发生的可能性

损害发生的可能性是界定敏感个人信息时必须考虑的因素，这是敏感个人信息与非敏感个人信息的关键区别。我国《个人信息保护法》第 28 条第 1 款使用“容易导致”这一表述，实际上指向的是一种相对的概率，即损害发生的可能性。对于一般自然人而言，敏感个人信息本身并不必然具有明确的实质性价值，而是更多地体现为一种价值载体。个人信息处理者处理敏感个人信息过程中更容易侵害人格权利和人身、财产安全等实质性价值目标。由于敏感个人信息处理行为并非必然使个人遭受明确的、固定的损害，对敏感个人信息严格保护的目的不在于要求损害后果的实际发生，而是要求存在造成个人信息主体的不特定法益被侵害的可能性。

受个人信息处理者掌握的信息识别技术的应用能力、个人信息主体与个人信息处理者的特殊关系等因素影响，不同场景中损害发生的可能性存在差异。例如，随着现代电子信息技术的逐渐成熟，电子交易类型的个人信息更容易被个人信息处理者非法使用。再如，在医疗、法律等专业服务场景中，个人信息主体和个人信息处理者存在较强的信赖关系，个人信息处理者作为特殊信赖主体对个人信息主体负有保密义务。此时，一旦个人信息处理者超出原始目的不当处理敏感个人信息，损害发生的可能性便迅速增高。在我国《个人信息保护法》的立法过程中，敏感个人信息损害发生的可能性要求发生了变化。《个人信息保护法（草案）》和《个人信息保护法（草案二次审议稿）》采取相对宽泛的标准，无论何种类型的损害，其发生存在可能性即可，仅仅要求“可能”导致个人受到歧视或者人身、财产安全受到严重危害。而最终出台的《个人信息保护法》则反映了立法者的严谨考量，规定敏感个人信息是“容易”导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，明确了敏感个人信息损害发生的可能性较高。从“可能导致”到“容易导致”的表述，《个人信息保护法》对敏感个人信息处理行为提出了更高的合规要求，清晰指出处理敏感个人信息比非敏感个人信息更容易导致损害的发生，进一步明确我国个人信息保护体系，有益于全面提升个人信息保护水平。

三、基于损害风险来源检视我国敏感个人信息的界定

（一）敏感个人信息的损害风险来源

进一步而言，敏感个人信息的损害风险究竟来源于何处，是个人信息保护规范必须清晰认识到的另一重要问题。唯有如此，方能使敏感个人信息的界定趋于完善。保罗·欧姆认为隐私损害

〔16〕 参见“程某等与开州区亿鑫药品超市侵权责任纠纷案”，重庆市开州区人民法院（2020）渝 0154 民初 5576 号民事判决书；“程某等与开县长沙镇桔香村卫生室侵权责任纠纷案”，重庆市开州区人民法院（2020）渝 0154 民初 5749 号民事判决书。

（privacy harm）揭示了敏感个人信息的多样性形式，主要涵盖固有敏感个人信息（inherently sensitive information）、工具敏感个人信息（instrumentally sensitive information）和推断敏感个人信息（inferentially sensitive information）。〔17〕本文借鉴此种分类方法，认为敏感个人信息的损害风险来源可以分为以下三种类型：个人信息内容的固有性、个人信息被非法使用时的工具性以及非敏感个人信息与敏感个人信息的关联性。敏感个人信息的损害风险可以单独或同时来源于以上三种不同类型。换句话说，只要个人信息满足三种来源中的一种，即应界定为敏感个人信息。

1. 个人信息内容的固有性

个人信息内容的固有性是指，信息内容所传达的实质含义是个人信息敏感与否的内在决定因素，同时也影响了潜在处理风险的高低。在处理个人信息过程中，信息内容本身一经泄露便容易导致个人信息主体遭受损害，使其具备敏感性。如医疗健康信息，其信息内容本身的泄露即可侵害人格尊严。欧盟立法机构始终坚持以保障人格权利为出发点进行个人信息保护，他们意识到个人信息内容的固有性便足以引起个人权益侵害风险，触发敏感个人信息的特殊保护机制。欧盟第 29 条数据保护工作组（Article 29 Data Protection Working Party，简称第 29 条工作组）强调，基于风险方法（risk-based approaches）评估个人数据处理风险时必须考虑个人数据的内容和性质。〔18〕由于历史背景和文化传统不同，损害风险来源于个人信息内容固有性的个人信息具体类别，最终因各法域的公众整体性期待和社会包容度不同而存在差异。例如，美国和欧盟法律均将政治观点明确列举为敏感个人信息，但对于财务信息是否作为敏感个人信息保护则有不同的选择。〔19〕而我国《个人信息保护法》列举的敏感个人信息中并未包括政治观点，仅在标准和指南等规范性文件中提及政治观点具有一定程度的敏感性。〔20〕

2. 个人信息被非法使用时的工具性

个人信息被非法使用时的工具性是指个人信息作为工具被非法使用时的损害风险。个人信息的工具性决定其具有社会性与公共性，体现在能够使得个人在社会中标识自己并与社会建立更为广泛的联系。〔21〕个人信息不仅是反映个人权益的信息载体，还是人类发挥主观能动性改造世界的重要决策依据，承载着在公共领域中发挥信息交换功能以促进社会进步的使命。在信息化时代，个人信息的财产属性日益凸显，作为社会交往工具的个人信息被非法利用的可能性陡然剧增。美国经济学家霍肯在 20 世纪曾断言，信息商品市场将取代传统的物质商品市场从而占据经济主导地位。在信息技术尚不发达的年代，个人信息通常被记录于纸质载体，不具备强烈的财产属性。但在信息化社会中，海量增长的信息数据被用于投入生产物品与劳务，成为实体经济产业

〔17〕 参见前引〔9〕，Paul Ohm 文，第 1170 页。

〔18〕 See Artical 29 Data Protection Working Party，Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks，2014，p. 4.

〔19〕 See Amitai Etzioni，A Cyber Age Privacy Doctrine：More Coherent，Less Subjective，and Operational，80（4）*Brooklyn Law Review* 1263，1278（2015）.

〔20〕 参见《信息安全技术 个人信息安全规范》（GB/T 35273—2020）第 9.4 条；《信息安全技术 公共及商用服务信息系统个人信息保护指南》（GB/Z 28828—2012）第 3.7 条。

〔21〕 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。

数字化发展的基础性战略资源。为了生活便利或获取经济利益，个人信息主体逐渐接受对敏感个人信息进行商业化利用的行为。随着技术允许虹膜、指纹、人脸等生物识别信息作为密码完成身份认证程序，生物识别信息的应用场景在不断拓展，指纹解锁、刷脸支付设备得到广泛应用。例如，被称为我国“人脸识别第一案”中的原告为了获取微信支付年卡费的便捷和经济利益，对身份证号、银行卡号等敏感个人信息采取了积极主动的商品化利用。〔22〕然而，在巨大的经济利益诱惑下，成熟的信息技术应用使得敏感个人信息容易被非法使用，从而导致高度损害风险。如今，个人信息处理者利用公民身份号码、电话号码、家庭地址等信息进行诈骗、跟踪等非法活动已经成为网络犯罪惩治的重中之重。

3. 非敏感个人信息与敏感个人信息的关联性

敏感个人信息的损害风险还可以来源于非敏感个人信息与敏感个人信息之间的关联性。信息分析技术日新月异，个人信息范围快速扩张。个人信息大量聚合处理极易模糊非敏感个人信息和敏感个人信息之间的边界，使得原本不敏感的个人信息通过结合其他个人信息亦能够揭示或关联敏感内容，这些推断结果容易产生侵犯个人信息权益的高度损害风险。消费记录并非法律明文列举的敏感个人信息类型，但在具体处理场景中，消费记录可以推断得出敏感个人信息或与敏感个人信息相关联的其他信息。比如，保险公司根据饮食消费记录推断得出个人健康信息，并据此针对消费者调整健康保险费用，很可能导致投保成本增加，使个人遭受经济价值损失。再如，肤色、身高等信息可以揭示健康或种族信息等敏感内容。

进一步而言，非敏感个人信息和敏感个人信息并非泾渭分明，它们之间可以相互转换。2021年，荷兰数据保护局（DPA）对于其国内一政治党派泄露了支持者电子邮箱的行为进行处罚。〔23〕在这一场景中，电子邮箱信息的性质发生了变化。电子邮箱由原本的一般个人信息可以转化成揭示政治观点的敏感个人信息。该党派支持者的电子邮箱信息被泄露，意味着电子邮箱持有者的个人政治观点信息同时被披露。因此，应当合理地认为，个人信息是否敏感还应在不同的场景中加以具体判断。在“庞理鹏与趣拿公司等隐私权纠纷案”中，我国法院即是运用了场景化认定方法对个人信息敏感与否进行具体分析。法官充分考虑了本案中预订机票的特殊场景，结合当事人行程安排信息推断原本属于一般个人信息的姓名、电话号码具有整体上的敏感属性。〔24〕“黄某与腾讯公司隐私权、个人信息权益网络侵权责任纠纷案”的法官也认为，判断个人信息内容的性质时，有必要深入实际处理场景，以“场景化模式”探讨该场景中是否存在侵害隐私的行为。〔25〕

（二）对我国《个人信息保护法》第28条第1款的检视

《个人信息保护法》第28条第1款以“抽象概括＋非穷尽式列举”界定敏感个人信息具有可

〔22〕 参见“郭兵诉杭州市野生动物园服务合同纠纷案”，浙江省杭州市富阳区人民法院（2019）浙0111民初6971号民事判决书。

〔23〕 See European Data Protection Board News, Dutch DPA: PVV Overijssel fined for failing to report data breach, available at https://edpb.europa.eu/news/national-news/2021/dutch-dpa-pvv-overijssel-fined-failing-report-data-breach_en, last visited on Jan. 23, 2022.

〔24〕 参见北京市第一中级人民法院（2017）京01民终509号民事判决书。

〔25〕 参见北京互联网法院（2019）京0491民初16142号民事判决书。

操作性，抽象概括为在法律实践中判断个人信息是否敏感提供了指引，非穷尽式列举又为新类型敏感个人信息的鉴别预留了一定空间。然而，明确列举的敏感个人信息类型具有强涵摄性，立法者的有限理性无法完全准确预测个人信息敏感程度之变化，现有的列举主义必将很快显得捉襟见肘，对判定普罗透斯之面似的敏感个人信息应接不暇。各列举项包含诸多具体的个人信息类型，应视作对敏感个人信息常见类别的提示。〔26〕若将列举信息类型一概认定为敏感个人信息，既可能保护过度又可能保护不足。因此，敏感个人信息的界定仍需置于处理场景中作具体判断。

对敏感个人信息的部分列举，似乎表明敏感可以被客观地归因于特定的个人信息类型。这种理解并不全面，实际上掩盖了敏感与相关场景因素之间的相互依存关系。我国《个人信息保护法》第 28 条第 1 款明确敏感个人信息容易导致个人人格尊严和人身、财产安全受到损害，体现了损害风险来源中个人信息内容的固有性和个人信息被非法使用的工具性，但却忽略了非敏感个人信息与敏感个人信息之间的关联性。敏感个人信息的表现形式日益丰富，忽视非敏感个人信息与敏感个人信息之间的关联性容易导致该条款的实际适用障碍，无益于敏感个人信息主体的个人权益保护和信息化技术的更新迭代。

场景化界定路径是司法实践中具体判断敏感个人信息范畴的可行路径。敏感个人信息范畴之所以难以准确界定，与敏感个人信息保护和其他权利的冲突，以及实践中判断敏感与否高度依赖具体处理场景有关。个人信息保护立法需要特别关注非敏感个人信息和敏感个人信息之间的关联性和可转化性。在高度损害风险标准之下，敏感个人信息的界定须结合场景因素，融入场景化界定路径。如从血液中提取的蛋白酶信息和 DNA 信息是否敏感，需结合个人信息处理者应用能力、识别能力和识别目的等具体场景因素进行综合判断。为了避免敏感个人信息的界定无法回应科技进步带来的新问题、无法解决司法实践中出现的新情况，应在现有“抽象概括＋非穷尽式列举”界定方式的基础上，辅以场景化界定路径构建多层次敏感个人信息保护体系，方能使我国《个人信息保护法》在基本理念上顺应历史发展规律，为敏感个人信息保护和信息化经济建设的长足发展预留充分的空间。

四、敏感个人信息场景化界定路径的理论框架及应用考量

（一）场景一致性理论框架

大数据处理场景的广泛性已然宣告场景化时代的到来，站在科技的风口上，便真如斯考伯和伊斯雷尔所预测的那样，占据场景便能赢得未来。〔27〕在复杂的网络传播环境下，能否掌握个人信息处理场景已经成为信息产业角力的重要考量。在信息传播场景化导向的背景下，个人信息处理场景日趋多元，个人信息保护立法及后续配套政策和标准文件必须尽快形成对策，以应对个人信息处理场景的复杂性。因此，个人信息场景化保护愈发受到学界的广泛关注。

〔26〕 参见前引〔13〕，宁园文。

〔27〕 参见〔美〕罗伯特·斯考伯、谢尔·伊斯雷尔：《即将到来的场景时代》，赵乾坤、周宝曜译，北京联合出版公司 2014 年版，第 1 页。

由于个人信息商品化活动持续活跃，〔28〕美国学者较早重视个人信息保护，认为个人信息是一种新类别的“黄金”，大力倡导对个人信息的场景化保护。〔29〕近年来，我国学者曾尝试论证场景化保护应用于我国个人信息保护领域的合理性，大多受到美国学者海伦·尼森鲍姆（Helen Nissenbaum）的场景一致性（contextual integrity）理论的启发。场景抽象地泛指日常生活中经历着的各种独立性社会空间，主要包括技术场景、商业场景、行业场景和社会场景四类理解，海伦·尼森鲍姆倾向于将场景理解为社会领域（social domain）。〔30〕场景由决定和支配着行为者、行为和限制等关键方面的规范构成，来源包括历史、文化、法律、惯例等。〔31〕场景既包括空间和环境，也包括具体行动的实时状态，其作为社会交往的基础条件和核心构成显示出强烈的流动性。〔32〕尊重场景即是遵守各领域的内生规范。

在美国隐私政策碎片化的背景下，场景一致性理论深受迈克尔·沃尔泽（Michael Walzer）的多元正义理论（pluralist theory of justice）影响，倡导尊重隐私保护的场景以挑战传统隐私保护理论。场景一致性理论被称为“隐私的替代基准”，以“适当性规范（appropriateness）—流动性规范（distribution）”为保护框架探析公民对公共监控（public surveillance）的不安根源，以应对信息技术带来的隐私挑战。场景一致性理论立足于预期的个人信息流（personal information flow），依据不同场景中的具体因素来保护信息隐私，强调个人信息的衍生利用行为不得与初始场景相悖，以确保个人信息流通适当。以场景中的规范来评估个人信息处理行为是否侵犯隐私取决于三个关键变量，包括行为主体（actors）、信息类型（information types）和传输原则（transmission principles）。〔33〕若有任何一个变量存在问题，就会出现“表面上的违反”（prima facie violation）。因此，个人信息的收集和传播必须在具体场景中是适当的，并遵守该场景的内部流通规范。

适当性规范是个人信息场景化保护的基础，要求在特定场景中，某一类信息的处理符合常理且具有必要性。如在医疗环境中，患者向就诊医生提供个人健康状况信息是恰当的，反之则为不恰当。流动性规范强调衍生数据的合理使用，要求个人信息从发送方向接收方或其他第三方的转移尊重个人信息流的场景规范。这与多元正义理论强调每个领域都有属于本领域的独特正义规范保持一致。“个人信息的使用和流通是否遵守信息流的场景规范”与“个人信息在某个特定场景中的使用具有适当性”同等重要，共同构建了有序利用个人信息的场景化监督体系。〔34〕场景一致性理论揭示了社会领域对适当性个人信息流的高度依赖，强调信息隐私逐渐涵括个人信息被恰当流通的权利。在现代生活中，信息隐私极具相对独立的社会空间性，倘若脱离了场景而孤立地审视个人信息，便无法准确判断该个人信息处理行为是否侵犯个人隐私。因此，尊重场景，便是

〔28〕 See Paul M. Schwartz, Property, Privacy, and Personal Data, 117 (7) *Harvard Law Review* 2056, 2069 (2004).

〔29〕 See Helen Nissenbaum, Privacy as Contextual Integrity, 79 (1) *Washington Law Review* 119, 121 (2004).

〔30〕 See Helen Nissenbaum, Respecting Context to Protect Privacy: Why Meaning Matters, 24 *Science and Engineering Ethics* 831 (2018).

〔31〕 参见前引〔29〕，Helen Nissenbaum 文，第 138 页。

〔32〕 参见王敏芝：《媒介化时代“云交往”的场景重构与伦理新困》，载《暨南学报（哲学社会科学版）》2021 年第9 期。

〔33〕 参见前引〔30〕，Helen Nissenbaum 文。具体而言，信息类型与信息性质相关；行为者系场景中涉及的角色，包括主体、发送方和接收方的参与人；传输原则包括个人信息共享和进一步传播的条件以及在场景中因素变化的潜在影响阈值等。

〔34〕 参见林凌、程思凡：《个人信息场景化传播困境及保护研究》，载《当代传播》2021 年第 5 期。

尊重权利人在不同社会空间中的隐私诉求。

（二）场景一致性理论应用于敏感个人信息界定的考量

场景一致性理论认为，个人信息的敏感程度是决定隐私侵权发生与否的关键因素。该理论解决隐私侵权问题的思路在于，摒弃传统上的敏感与非敏感个人信息的固定二分法，充分考虑信息处理场景判断个人信息敏感与否，并运用场景规范使个人信息处理活动符合“适当性规范—流动性规范”保护框架。〔35〕由于个人信息的敏感程度极不稳定，容易在不同的个人信息处理场景下发生变化，〔36〕需要对个人信息进行差别化场景保护。场景一致性理论中的“敏感”概念极具隐私意义，在很大程度上保留了心理学上的主观色彩。其认为界定敏感个人信息除了符合社会公众心理预期的客观标准之外，还应该在具体场景中考虑个人信息主体的主观感受，以此评估个人信息处理是否可能给个人信息主体带来损害风险。个人信息敏感与否取决于个人信息主体对信息处理场景的预测与假设，如果个人信息的处理活动违反了个人信息主体的合理期待，便会产生自身利益受到侵害的主观感受。〔37〕但即使是同一种类型的个人信息，个人信息主体在具体场景中依然会产生不同的主观感受，代表着不同的合理期待。〔38〕例如，个人政见信息在政治会议场景中处理是合适的，但不适合被应用于零售、医疗等场景。因此，当个人信息主体认为某一类型信息为敏感个人信息时，便同时确定了其对该类型个人信息在特定处理场景中的合理期待。《金融服务现代化法案》（Gramm-Leach-Bliley Act，简称 GLBA）中对敏感个人信息的保护便体现了极强的主观考量，从遵循个人信息主体的意愿角度区分敏感个人信息，一旦个人信息主体认为某一个人信息具有敏感程度，即可拒绝金融机构对该个人信息进行处理。〔39〕

场景一致性理论以多元正义理论为基石，力图避免某一场景内侵犯隐私的“暴政”，有助于应对信息科技时代下的公共监视问题，从而具有很强的政治哲学意义。在识别一种新的信息应用实践如何影响隐私权利方面，该理论是非常有效的。〔40〕然而，场景一致性理论有其自身的局限性，从而决定其无法具有独立的规范效力。场景是保护隐私的重要因素，但它不应该取代包括敏感个人信息保护规则在内的启发式规则。〔41〕许多学者试图进一步发展场景一致性理论思想并将其应用于实践，但均发现这一概念并不容易融入正式法律。〔42〕

---

〔35〕 参见前引〔29〕，Helen Nissenbaum 文，第 136 页。

〔36〕 See Kirsten Martin & Helen Nissenbaum, Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables, 18 (1) *Columbia Science and Technology Law Review* 176, 215 (2016).

〔37〕 See Helen Nissenbaum, A Contextual Approach to Privacy Online, 104 *the Journal of the American Academy of Arts & Sciences* 32, 38 (2011).

〔38〕 See Paula Kift & Helen Nissenbaum, Metadata in Context: An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program, 13 (2) *A Journal of Law and Policy for the Information Society* 333 (2017).

〔39〕 See Federal Trade Commission, How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act, available at https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm, last visited on Jan. 4, 2023.

〔40〕 See Gabe Maldoff & Omer Tene, Putting Data Benefits in Context: A Response to Kift and Nissenbaum, 13 (2) *A Journal of Law and Policy for the Information Society* 383 (2017).

〔41〕 参见前引〔9〕，Paul Ohm 文，第 1146 页。

〔42〕 See Bernd Justin Jütte & Annelies Vandendriessche, Responsible Information Sharing: Converging Boundaries between Private and Public in Privacy and Copyright Law, 10 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 310 (2019).

其一，场景一致性理论中的场景因素复杂繁多，若独立运用其界定敏感个人信息缺乏可供实践的明确标准。场景是一个模棱两可的术语，它有可能使任一个人信息在某一场景下成为敏感个人信息。〔43〕并且，场景是影响个人信息处理风险的外因。〔44〕倘若判断个人信息敏感与否仅仅依据场景，则使敏感个人信息保护制度陷入被动，法律规则的预防功能将无法实现，进一步加深司法实践中认定敏感个人信息的标准鸿沟，为个案判断带来不堪重负的压力。其二，场景一致性理论下，从隐私权利中衍生的“敏感”概念过于宽泛，强调个人信息主体对敏感个人信息处理场景的个体性期待，以超强的主观感受界定敏感个人信息，并以此评估个人信息处理风险，难以达成充分发挥敏感个人信息保护兼具个人属性和社会属性的平衡效果。司法实践中，法院判断微信好友列表和读书信息的性质时，认识到敏感个人信息保护和隐私保护均体现了自然人的人格尊严和人格自由价值，但个人信息权益同时涉及信息利用和流通价值。〔45〕因此，敏感个人信息保护与隐私保护的不同之处在于，后者保护个人不愿为他人知晓的信息私密性，强调个人主观意愿，前者更强调个人信息不当利用导致信息主体遭受的客观风险。进一步而言，即使在相对一致的场景下，由于互联网产品和相应用户的广泛性和差异性，不同个人信息主体对同一信息具有不同程度的敏感期待。如在电子商务平台购物时，有的用户对针对性的广告推送十分反感，而有的用户则乐意接受该定向广告推送带来的便利。显而易见，若敏感个人信息是指信息被披露便使个人信息主体容易感到尴尬或不安的信息，那么在此定义下，所有的个人信息都有可能因其披露条件的变化而变得敏感。这会引起敏感个人信息过强保护的失控局面，“同案不同判”的司法诉累情况将不可避免。

鉴于场景一致性理论中个人信息“敏感”概念的自身局限性，场景化保护不能独立作为界定敏感个人信息的路径。因此，场景一致性理论可为我国《个人信息保护法》第 28 条第 1 款提供一种理论上的启发和制度上的有益补充，但实践难题的具体适用方案仍需进行适当调整。

五、我国敏感个人信息界定的完善

梅因深刻地指出，社会需求和社会主张总是或多或少地领先于法律，我们可能会无限地接近弥合它们之间的鸿沟，但永久的趋势是他们会重新拉开差距；因为法律是稳定的，社会是进步的，一个民族的幸福程度取决于鸿沟缩小的速度。〔46〕个人信息保护作为信息化社会经济生活迅猛发展的制度保障，必须紧密结合特定时期的社会需求和社会主张，不断适应社会生活变化，及时回应和解决个人信息保护面对的现实问题。目前，实践中我国《个人信息保护法》在界定敏感个人信息的具体类型方面存在较大解释空间。在科技爆炸时代，法律规范界定敏感个人信息应与时俱进，才能有针对性地回应由科技进步带来的种种新问题，并充分满足信息化社会中敏感个人信息保护的需要。我国尚未形成完善的敏感个人信息保护体系，此时寻求敏感个人信息界定的更

〔43〕 参见前引〔30〕，Helen Nissenbaum 文。

〔44〕 参见前引〔13〕，宁园文。

〔45〕 参见北京互联网法院（2019）京 0491 民初 16142 号民事判决书。

〔46〕 See Henry Sumner Maine, *Ancient Law*, Cosimo Classics, 2005, p. 15.

优解，以有效发挥我国个人信息保护立法的后发优势可谓正当其时。本文建议在《个人信息保护法》第 28 条第 1 款的基础上，辅以场景化路径以完善敏感个人信息的界定，具体考虑个人信息是否可以揭示或关联敏感内容、受损害主体是否包括其他关联利益人，最终构建多层次敏感个人信息保护体系。

（一）辅以场景化界定路径构建多层次敏感个人信息保护体系

我国个人信息保护理论和法律实践中应具备不采取一刀切的方式来理解和保护敏感个人信息的智识。将敏感个人信息概括划入相对固定的概念中，并不是有效保护敏感个人信息的唯一选择。实证研究已经表明，个人信息敏感与否离不开信息处理场景的考量。〔47〕性别、出生日期、籍贯等人口统计学信息通常被认为不敏感。但在求职场景中，人口统计学信息与身份号码、照片、健康状况等个人信息相结合，其敏感程度陡然增高，应被认为属于敏感个人信息。此前，我国的行业标准指南在界定敏感个人信息时，已经体现场景化界定的思路。各行业敏感个人信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定，〔48〕为敏感个人信息的场景化界定留下解释空间。在我国司法实践中，场景化界定也已欣然可见，司法机关立足于具体场景衡量个人信息敏感程度。在一般生活场景中，特别是熟人群体中，真实姓名并不敏感，但在电子商务交易中真实姓名则被认为属于敏感个人信息。在“安娜与淘宝公司网络服务合同纠纷案”中，法院认为电子商务平台的自然人商家在开设淘宝店铺时留存的真实姓名、手机号码等个人信息具有敏感性，不宜全部对外公示。〔49〕淘宝公司作为平台经营者，对自然人商家在开设店铺时留存的敏感个人信息有保障责任。

未来，针对不同的信息处理场景，单一的敏感程度衡量标准应当发展成一个差异化、动态调整的标准体系。我国《个人信息保护法》应在积极利用概括列举式界定保持敏感个人信息保护体系可操作性的同时，以场景化界定路径作为补充和辅助手段。一是规定其他规范性文件可以参考各行业特点，定期适当调整敏感个人信息范围；二是在具体个案中，由司法机关依据信息处理的特殊情况，判断法律规范明文列举范围之外的个人信息是否属于敏感个人信息；三是通过执法和司法实践的不断归纳总结，结合技术专家组的意见，形成更具场景操作性的敏感程度界定标准。把定期调整、更新敏感个人信息清单的权利适当下放给各行业领域，可以全面保障敏感个人信息保护的有效性。允许各行业领域进行场景化界定可使敏感个人信息保护更契合行业特征，有利于对法律规范并未明文列举的敏感个人信息作出差异化安排，加快构建多层次敏感个人信息保护体系。

（二）敏感个人信息场景化界定路径的客观考虑因素

1. 个人信息是否揭示或关联敏感内容

敏感个人信息的损害风险不仅来源于个人信息内容本身和被非法使用时的工具性，还来源于

〔47〕 See David L. Mothersbaugh et al., Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information, 15 (1) *Journal of Service Research* 76 (2012).

〔48〕 参见《信息安全技术 公共及商用服务信息系统个人信息保护指南》（GB/Z 28828—2012）第 3.7 条。

〔49〕 参见杭州互联网法院（2019）浙 0192 民初 5468 号民事判决书。

非敏感个人信息与敏感个人信息的关联性，后者往往容易被法律所忽视。在大数据和人工智能时代，我国《个人信息保护法》需要特别关注敏感个人信息和非敏感个人信息之间的转化可能。美欧个人信息保护法律中的敏感个人信息范围，包括能够揭示或关联所列信息种类的个人信息。欧盟1995年的《数据保护指令》（Data Protection Directive，简称DPD）和GDPR规定特殊类别的个人信息时，同时使用了“揭示”（revealing）和“关联”（concerning）的表述。根据GDPR第9条第1款规定，敏感个人信息包括可能揭示种族或民族起源、政治观点、宗教或哲学信仰、工会成员资格的个人数据，以及有关健康、自然人的性生活或性取向的数据。对此，应理解为敏感个人信息不仅涵盖了在信息性质上具有敏感程度的信息，还包括可以揭示和关联敏感内容的个人信息。〔50〕欧洲数据保护委员会（European Data Protection Board，简称EDPB）指出敏感个人信息除了明确列举的种类，还包括其他被认为敏感的个人信息。〔51〕举例而言，照片并非GDPR所列举的敏感个人信息种类，但GDPR仍然承认在具体场景中认定照片的敏感程度。如果处理照片时使用了能够识别自然人的特殊技术手段，照片可被敏感个人信息中的生物识别信息的定义所涵盖。第29条工作组也认为，如个人照片和图像可以显示种族或健康信息，可被视为敏感个人信息。〔52〕美国《弗吉尼亚州消费者数据保护法》（The Virginia Consumer Data Protection Act）、《加州隐私权利法案》（The California Privacy Rights Act）、《华盛顿州隐私法案》（The Washington Privacy Act）等法律界定敏感个人信息范围也使用了关键词“揭示”。美国的立法草案中，敏感个人信息范围囊括了处理或传输是为了识别敏感个人信息的其他任何类型的信息，以及与敏感个人信息定义中各信息种类相关的个人信息，〔53〕进一步强化了避免因为信息类型之间的相互转化而逃脱监管的情形。

敏感个人信息范围不局限于法律规范所列举的信息类型，非敏感个人信息结合其他额外信息可能与敏感个人信息相关联，或者可以揭示敏感内容。如电子商务平台收集的手机号码、收货地址等个人信息与购物列表、搜索记录等辅助个人信息结合起来，可以揭示或关联个人信息主体的宗教信仰等敏感内容。在此场景下，手机号码、收货地址、购物列表和搜索记录可一并属于敏感个人信息。假设个人信息处理者已知一个清真寺的地理位置，同时获取了个人信息主体前往该地理位置的频率信息，则个人宗教信仰信息已然被揭示。因此，此场景中的地理位置信息应当被认定为敏感个人信息进行特殊保护。此外，揭示犯罪历史和人物社会危险性的犯罪记录、能够从中推断学生品行的教育记录等个人信息，因与敏感内容密切关联也应属于敏感个人信息。然而，我国《个人信息保护法》并未强调能够揭示或关联敏感内容的个人信息为敏感个人信息。因此，《个人信息保护法》中敏感个人信息界定的完善思路应该着眼于能够覆盖损害风险来源的因素。揭示或关联敏感内容的个人信息也应列入敏感个人信息范围，此为场景化界定

〔50〕 See Artical 29 Data Protection Working Party, Advice paper on special categories of data (sensitive data), 2011, p. 5.

〔51〕 See European Data Protection Board, Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment [Article 39. 4 of Regulation (EU) 2018/1725], 2019, p. 5.

〔52〕 参见前引〔50〕，第29条工作组文件，第8页。

〔53〕 See United States Consumer Data Privacy Act of 2019; Consumer Online Privacy Rights Act.

路径的重要内容。

2. 受损害主体是否包括其他关联利益人

一般而言，非敏感个人信息仅仅影响个人信息主体。而敏感个人信息因具有高度损害风险，更容易导致个人信息主体本身以外的其他受到实质性影响的关联利益人同时遭受损害。因此，受损害主体包括其他关联利益人的个人信息也应被认为是敏感个人信息。敏感个人信息保护规则应同时保障个人信息主体以及其他受到实质性影响的关联利益人。唯有如此，才能真正保障敏感个人信息主体的切身利益免受损害。对于受损害主体问题，GDPR 第 82 条规定“任何遭受物质或非物质损害的人”都有权获得控制者或处理者的赔偿。普遍的限制性解释是，GDPR 最终旨在保护数据主体的权利，只有数据主体才能援引第 82 条获得民事救济。但有学者不同意这种限制性解释，认为有权获得损害救济的主体应扩大解释为任何可能遭受损害的人。〔54〕这符合 GDPR 的宗旨，即毫无例外地保护自然人的所有基本权利和自由。诸如，遗传基因信息的不当使用所造成的损害深远、长久而不可逆，且受损害主体难以预计。联合国经济及社会理事会决议《基因隐私权与不歧视》也承认，与一个可识别的人相关的遗传信息有时可能与该人家庭成员或其他人有关，因此在处理这类个人信息时也应考虑到关联利益人的权益。我国《个人信息保护法》要求网信部门统筹协调、推进敏感个人信息保护具体规则的制定工作，构建完善的敏感个人信息保护体系的重要性不言而喻。敏感个人信息的界定是较为复杂的系统工程，我国需充分考虑敏感个人信息场景化界定的客观因素，确保敏感个人信息保护的多维视角。

六、结　语

信息技术对人类社会影响的深度和广度都是空前的，个人信息保护和利用的角力在敏感个人信息方面表现得更为焦灼。敏感个人信息保护的目标应是在充分保护个人信息主体重大利益的同时，尽可能地释放敏感个人信息的社会价值。如今，部分敏感个人信息已存在合法进入数据市场的现实需求。如医疗健康个人信息不仅关乎个人权益，还在很多场景中蕴含极大的公共利用价值。《福州市健康医疗大数据开放开发实施细则》中就有关于根据不同的处理场景对敏感个人信息进行脱敏脱密处理后开放的规定。

法律无法脱离社会经验而存在。敏感个人信息保护体系不应也无法抛弃个人信息主体集合下的实质性利益，对敏感个人信息的界定正需要基于生活经验尽可能地反映社会公众对于“敏感”的整体认可度。即使我们无法全面预估科技发展的最终走向，但我们至少可以看到，敏感个人信息的损害风险来源、敏感个人信息处理导致的损害类型以及损害发生的可能性都是有增无减。我国《个人信息保护法》未来应在制度安排上作出有力回应，在现有“抽象概括＋非穷尽式列举”界定方式的基础上，辅以场景化界定路径回应信息社会的风险需要。具体而言，需以个人信息是否揭示或关联敏感内容、受损害主体是否包括其他关联利益人为场景化界定路径的客观考虑因

〔54〕 See A. B. Menezes Cordeiro, Civil Liability for Processing of Personal Data in the GDPR, 5 (4) *European Data Protection Law Review* 492, 495 (2019).

素，有效控制敏感个人信息处理过程中的损害风险。如此，方能为科技发展带来的敏感个人信息界定变化预留足够的空间，也才能更好实现敏感个人信息保护与利用的平衡。

Abstract：The definition of sensitive personal information is an important content of the Personal Information Protection Law. Because it can reflect and affect the major interests of the subject of personal information more than non-sensitive personal information, the Personal Information Protection Law adopts a more strict protection system for sensitive personal information. Article 28 (1) of the Personal Information Protection Law defines the objective risk standard for sensitive personal information. From the perspective of law, "sensitive" is associated with "high risk of damage", and sensitive personal information processing has a higher degree of risk of damage. The risk of damage can be derived independently or simultaneously from the inherence of personal information content, the instrumentality of illegal use of personal information, and the relevance of non-sensitive personal information and sensitive personal information. The definition of the sensitive personal information in the Personal Information Protection Law is still can not cover all damage risk sources, and should define sensitive personal information with contextualized aspects path on the basis of Article 28 (1). In particular, objective factors are considered based on whether the personal information reveals or concern sensitive content and whether the damaged subject includes other related interests.

Key Words：personal information protection law, sensitive personal information, risk of damage, contextual integrity

（责任编辑：武　腾　赵建蕊）