敏感个人信息的界定与处理路径完善

朱鸿静
（中国人民公安大学　法学院，北京　100083）

摘　要：进入数字经济时代，个人信息尤其是敏感个人信息的保护成为全球关注的焦点。《中华人民共和国个人信息保护法》虽然对敏感个人信息进行了专门规定，但在实践中仍面临判断标准的模糊性、处理规则的不确定性等诸多问题。对此，可以在平衡数据要素流通与个人权益保护的基础上，完善敏感个人信息的精准界定与差异化处理规则。具体来说，在界定方式上，借鉴域外立法经验，提出以法定标准为基础兼采多元因素准确认定敏感个人信息，并引入场景理论；在处理规则上，细化敏感个人信息处理的前置条件，构建场景化的知情同意规则，鼓励行业自治，为数字经济高质量发展提供制度保障。

关键词：敏感个人信息；处理规则；判断标准
中图分类号：D923；D922.16　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.08.008
引用格式：朱鸿静. 敏感个人信息的界定与处理路径完善［J］. 网络安全与数据治理，2025，44(8)：53-57.

Definition of sensitive personal information and improvement of the path of handling

Zhu Hongjing
(Law School, People's Public Security University of China, Beijing 100083, China)

Abstract: Entering the era of digital economy, the protection of personal information, especially sensitive personal information, has become a global concern. Although the Law of the People's Republic of China on the Protection of Personal Information has made special provisions for sensitive personal information, in practice, it still faces many problems, such as ambiguity in judgment standards and uncertainty in processing rules. In this regard, the precise definition of sensitive personal information and differentiated processing rules can be improved on the basis of balancing the circulation of data elements and the protection of personal rights and interests. Specifically, in terms of definition method, drawing on overseas legislative experience, it is proposed to accurately identify sensitive personal information on the basis of legal standards and multiple factors, and to introduce the scenario theory. In terms of processing rules, it is proposed to refine the preconditions for the processing of sensitive personal information, to construct scenario-based rules for informed consent, and to encourage industry autonomy, in order to provide institutional safeguards for the high-quality development of the digital economy.

Key words: sensitive personal information; processing rules; judgment criteria

0　引言

随着数字化时代的到来，人工智能、算法推荐、大数据等各种新兴数字技术正无形渗透到人们的日常生活中，而这些智能技术能够获得突破性进展，与公民的个人信息有着密不可分的联系。由于信息主体对自己的重要信息采集采取更为谨慎的态度，如何平衡信息保护与利用之间的关系，给予敏感个人信息充分保护的问题日益受到大众的关注[1]。《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）中单设“敏感个人信息处理规则”一节，对敏感个人信息进行特殊保护，完善了个人信息保护的法律体系。但在实际应用过程中，上述规定仍存在内容较为抽象的现实问题，导致这些规定难以产生预期的实施效果。要给予敏感个人信息充分保护，首先应准确界定好敏感个人信息的范围，将属于敏感个人信息的信息纳入进来，对其适用严于一般个人信息的规则，对于那些不属于敏感个人信息的信息，及时排除出去，避免给信息处理者造成过重的负担。在个人信息保护领域形成强弱有别的保护格局，可避免“引发过度保护或保护不足的弊端”[2]，使敏感个人信息获得全面切实的保护。因此，本文选取敏感个人信息界定和

处理规则上存在的难题进行分析，并提出相应的完善建议。

1 敏感个人信息保护面临的现实困境

1.1 敏感个人信息判断标准的模糊性

1.1.1 我国立法中的判断标准

从提升法的安定性的角度出发，我国《个人信息保护法》第28条可以归纳出敏感个人信息判断的几个法定标准：人格尊严标准，人身、财产安全标准，未成年标准。

首先是人格尊严标准。人格尊严标准的确立植根于宪法第38条关于人格尊严权的规范基础，并与民法典一般人格权制度形成法解释学上的制度渊源。鉴于二者间的内在逻辑关联，该标准成为界定敏感个人信息类型的重要法定依据。从风险规制维度分析，敏感个人信息相较于一般个人信息具有显著突出的侵害风险，可能对信息主体的人格法益造成不可逆损害。虽然现行个人信息保护规范体系已建构人格尊严保障机制，但敏感个人信息因其特殊的识别效能和损害强度，在人格权保护维度呈现出更高效力层级的制度功能。身体健康状况便是与人格利益相关的敏感个人信息[3]，一旦被非法利用，可能会产生歧视和不平等对待，严重影响信息主体的正常生活和工作。基于此，人格尊严标准作为敏感个人信息的判断标准，更凸显了敏感个人信息保护制度在个人信息保护中的重要地位，更有效地保护个人信息。

其次是人身、财产安全标准。身份证号、电话号码等可以精准定位到个人的信息，若不当处理，很容易产生人身攻击和恶意骚扰的问题。如果这些对于人身安全至关重要的个人信息遭到泄露，将会产生不可估量的风险。例如，公民的人脸照片如果未经处理予以应用，会带来人身安全受损的风险。从朴素的价值观理解，生命、健康作为最重要的法益，是一个人得以存在和生活的根基，将其作为敏感个人信息予以保护具有应然性。域外立法缺少对财产安全的关注，但在某些情况下，金融账户信息的泄露也会危及公民的人身权益，使之难以维系基本生活。因此，对财产安全具有重大影响的信息也应当成为敏感个人信息的组成部分。

最后是未成年标准，即考查信息主体的年龄条件，给予14周岁以下未成年的个人信息特别保护。未成年人由于生理心理尚未发育成熟，在信息处理方面难以形成正确判断，如果其个人信息被不法分子获取，不仅给未成年人带来巨大创伤，更会波及他们的监护人和家庭，造成难以控制的社会影响[4]。美国、欧盟等域外立法中并未提及未成年这一标准，但我国社会实践中出现了一些利用未成年信息对其监护人进行诈骗的案例，为了维护未成年主体和其家长的合法权益，我国将其列入敏感个人信息，对未成年人加强保护，这也是《个人信息保护法》的首创。

1.1.2 “敏感性”的判断难题

敏感个人信息本质上仍属于个人信息，但是由于其涉及和关联的人身财产权益远大于一般性的个人信息，因此对敏感个人信息进行特殊的立法已经成为国际通例。各国在认定敏感个人信息的问题上，大多以公民个人信息被非法利用或者泄露后损害公民合法权益的风险程度即“敏感性”为标准。但是敏感二字究竟应当作何解释，主观说认为敏感具有很强的个性化色彩，是对人的心理状态的一种描述。客观说认为其与社会环境有着密切联系，易导致伤害或者损害结果[5]。综合说认为应当兼采主观客观标准[6]。一方面，个人信息的敏感程度并不是一成不变的，场景的转换、变量的增加或者减少，都可能产生个人信息从一般个人信息向敏感个人信息转变的结果。另一方面，从语言解释上说，敏感二字具有极大的不确定性，是一个模糊不清的表述，存在很大的解释空间。但其作为法律概念，概念内涵的界定应当是明确的，为了实现准确应用，需要进行价值填补[7]。这要求法官说理充分，也为学术研究留下了讨论空间，由此产生了“敏感性”的判断难题。

1.2 敏感个人信息处理规则适用的不确定性

1.2.1 敏感个人信息处理前置条件过于原则化

根据我国《个人信息保护法》第28条第2款的规定可知，我国对敏感个人信息的处理活动并不是全部禁止，而是通过附加一些前置条件进行操作，这些前置条件包括特定目的、充分必要性和采取严格措施。法律文本并没有对这些处理敏感个人信息的核心要件进行相关阐述和界定，仅使用高度抽象性的词语做出界定，无疑会增加司法实践的裁判难度。敏感个人信息处理的前置条件该作何解释，学术界目前没有形成统一看法，司法实践中法官的处理方式也不一致。司法实践中，应当尽量减少法官行使自由裁量权的次数，但是目前并不存在关于处理敏感个人信息前置条件的权威解释，容易陷入任意解释和目的落空的困境。与此同时，企业在处理敏感个人信息时将效益作为首要追求的目标，往往会不积极履行相关义务。例如使用空洞概括的语言达到法律规定的标准[8]，推卸己方责任，此种规范实施异化将直接消解敏感信息特别保护机制的规范效力，易引发法律解释的恣意性风险。针对这一问题，可以出台更为直接的细化规定，以实现有效的规范指引。

1.2.2 知情同意规则适用僵化

知情同意规则是指在收集、使用个人信息之前，信息处理者应当详尽地告知信息主体其个人信息被收集、处理的具体方式，并需要事先征求信息主体的明确同意。信息处理者处理敏感个人信息时，也应当履行告知义务，清晰告知信息主体处理方式、范围，在获得其同意后，才能进行相应的处理活动[9]。根据《个人信息保护法》第29条规定可知，信息处理者在处理敏感个人信息之前，需获取信息主体明确且独立的同意，同时规定了在法律、行政法规有规定的特定情况下，该同意应以书面形式表达。这一规定虽然为信息处理者设置了获取单独同意的义务，起到了形式规制的作用，但未能充分彰显个人信息处理规则之规范意旨，难以发挥知情同意规则的实质效用，在实践中可能导致这一规则的空置和虚化[10-11]。因此，应当赋予知情同意规则更强的灵活性，以更好应对司法实践中不断变化的应用场景。

2 敏感个人信息的多维判断标准

2.1 域外立法实践中的判断标准

2.1.1 美国

美国对认定敏感个人信息的规定存在明显的风险导向和实用主义特征，更加关注信息泄露是否导致身份盗窃、歧视性待遇等现实风险。因此美国并未在全国建立统一的敏感个人信息判断标准，联邦立法与州立法并行。联邦层面如《健康保险携带和责任法案》界定医疗健康数据为敏感信息，《儿童在线隐私保护法》聚焦儿童隐私保护；州层面如《加州消费者隐私法》增加地理位置作为敏感个人信息。与此同时，行业拥有较大的自主权，允许企业联合基于业务类型制定行业规范，但需履行披露义务（如在隐私政策中标明）并提供用户退出机制。

2.1.2 欧盟

欧盟在敏感个人信息保护方面规定较为严格，信息类型与人格尊严关联度高。其制度贡献集中体现在《通用数据保护条例》（以下简称GDPR）中。作为当前敏感个人信息领域影响深远的立法，GDPR明确将“特殊类别数据”定义为可能引发人格尊严或基本权利重大风险的信息，在处理方式上采取“原则禁止+例外豁免”模式。值得关注的是，GDPR突破传统静态标准，引入“场景动态评估”机制（即使是GDPR中未列明的数据，如果在特定场景下会严重侵害合法权益，也属于敏感个人信息的范畴），并赋予信息主体更有力的控制权。

美国与欧盟在敏感个人信息判断标准上的核心内容可以精简为表1所示。

表1 美国、欧盟敏感个人信息判断标准

	美国	欧盟
立法模式	分散立法，联邦与州法律并行	统一、严格的禁止性规则
界定方式	各州自治、行业自治	明确列举
敏感个人信息的范围	侧重风险导向与实用主义	侧重伦理与人格尊严相关数据
具体敏感个人信息示例	社保号、驾照号、生物识别数据、健康信息等	种族、政治观点、宗教信仰、健康数据、性取向等

2.2 以法定标准为基础兼采多元因素评估

2.2.1 利益类型

相比于一般信息，敏感个人信息泄露给信息主体带来的损害更为直接和迫切。这是由于敏感个人信息承载的利益与公众的隐私关联更为紧密，个人可以清楚地感知风险存在对其产生的困扰。人格尊严是敏感个人信息识别的基础，包括三重利益维度：其一为人格法益，包括人身安全、隐私权益及名誉尊严等民事权益；其二为数字社群关系法益，其突破传统人格权之规范边界，是涵盖人身权益和财产权益的混合型法益；其三为物质利益，既涵盖信息主体因违法处理行为所致之直接经济损失，亦包含要求获得信息商业化利用产生的正当收益的权利。

2.2.2 侵害程度

刑法在认定某些行为是否为犯罪行为时，会在侵害程度上设定标准，并且利用数额、情节和次数进行细化。敏感个人信息可以借鉴刑法的定义方式，将个人信息受侵害程度作为判断标准，从个人信息被侵害概率的高低上区分个人信息是否属于敏感个人信息。我国《个人信息保护法》从草案二审稿到正式法律文本对“敏感信息”的定义，由“人身、财产安全受到严重危害”改为“人身、财产安全受到危害”，恰恰印证了这一点，即敏感信息认定原则上采取了侵害烈度较为轻缓的“一般侵害程度”。

2.2.3 风险概率

某些信息与信息主体关联紧密，更容易受到侵害，因此风险概率也是敏感个人信息的重要判定标准。该类信息不仅承载着与主体人身权益、财产秩序直接关联的核心法益，更因其在数据深度挖掘、算法建模及用户画像构建等场景中具有高度预测价值[12]，已然成为数据处

理者竞相获取的战略性资源。如果放任处理者攫取、追逐，每个个体将处于信息随时被泄露的巨大风险之中。因此，在具体判断敏感个人信息时，可以适当观察其风险概率，为全面保护敏感个人信息提供手段保障。

2.3 引入“场景理论”

我国《个人信息保护法》在认定个人信息方面确立的是静态化的判断标准，一贯采用这样可识别性的标准，可能会无形中增加保护敏感个人信息的困难。迅速发展的技术极大地冲击了静态标准的原有地位，从实际出发，直接在具体场景中进行判断的方式优点逐渐凸显。在这样的背景下，动态化认定敏感个人信息的“场景理论”应运而生。即在原有基础上，在具体情境中多因素考量，实现敏感个人信息判断的精准化、多元化。同时，如何在个人信息保护和信息利用之间实现平衡，是《个人信息保护法》从拟定草案到公布时永恒不变的热点关注问题。信息作为信息化时代企业运作的重要资源，一味地给予敏感个人信息特殊保护，信息的自我价值将难以发挥实际效用，也会给社会发展进步带来不利影响。由此可知，引入场景理论，将为敏感个人信息提供更加直接的定义和管理，可以更好地规制敏感个人信息的处理行为。

3 完善敏感个人信息处理规则

3.1 细化敏感个人信息处理的前置条件

3.1.1 特定目的

特定目的源于目的限制原则，在敏感个人信息处理方面具体可以借鉴欧盟 GDPR 第 5（1）（b）条，引入“直接关联性”要求，即处理敏感个人信息应当限定在法律直接规定或者双方明确约定的范围内，处理方式必须与初始收集目的直接相关。例如，企业收集人脸信息用于门禁系统，不得擅自用于广告推送。智能穿戴设备记录的信息主体身体健康信息，未经允许不得另作他用。并且尽量避免在条款中使用“为提供更好的服务”“为不影响使用”等笼统的表述。

3.1.2 充分必要性

充分必要性实现了比例原则的引入，信息处理者应当在必要范围内对个人信息进行危害最小化的处理。在不处理个人信息就可以达到相应效果的情形下，应当通过其他不会对个人信息造成侵害的方式进行替代[13]，即处理行为必须具备充分性条件。在实践中要求企业证明处理手段对目的的达成是“最小侵害”。例如，某景区以“安全管理”为由收集游客指纹，若可用二维码替代，则指纹收集不具备必要性。同时，可以由网信办联合行业协会发布《敏感信息处理必要性指南》，明确金融、医疗、教育等领域的合规标准，增强针对性，细化不同敏感程度信息的充分必要性标准。

3.1.3 采取严格保护措施

不同于“一旦泄露或者非法使用”等事后保护措施，“采取严格保护措施”从前端就给予敏感个人信息非同一般个人信息的特殊保护。《个人信息保护法》第 51 条、56 条均是这一保护措施的体现，从中可以归纳出以下三方面的措施：一是组织措施，要求建立涵盖全周期的管理制度及系统性风险防控体系，通过对从业人员进行不间断、持续性的合规培训，确保组织决策层与执行层治理效能之协同；二是操作措施，按照信息的敏感程度分级分类储存，从源头防范敏感个人信息被不法利用；三是技术措施，如数据加密、访问控制、定期审计等，对相关数据进行匿名化和去标识化处理[14]，使其不再敏感。

3.2 构建场景化知情同意规则

3.2.1 “场景理论”的具体应用

知情同意规则为信息处理者的处理行为设置了门槛，只有在获得信息主体同意的前提下，其后续的处理行为才具有正当性。面对实践中出现的信息主体被迫同意、变相强迫同意的情况，应当突破现有的知情同意规则，引入动态化的场景理论[15]。为了保证信息主体的自主决定权，如果信息处理者的行为严重损害信息主体权益，其有权撤回同意，确保信息主体始终自主掌握个人信息的具体动态并做出判断，动态化落实知情同意规则。具体来说，可以根据不同场景设计差异化的知情同意规则。例如，在紧急公共卫生事件中，可以适当放宽知情同意的要求。实践中一些 APP 存在不勾选同意选项就不能使用应用程序，或者利用信息主体法律意识淡薄的弱点进行概括同意的授权，从而虚化了知情同意规则。这样动态化的制度设计，更容易获得信息主体真实、有效的同意表示[16]，有利于全流程的敏感个人信息保护的实现。

3.2.2 潜在型敏感个人信息的处理规则

在场景化理论应用下，潜在型敏感个人信息主要存在于以下两种情形中：第一种情形，针对当今日渐精进的技术的出现，许多原来属于一般个人信息的信息，通过大数据整合分析、数据库关联对比等手段（如通过算法推断的个人偏好），实现数据之间的互通互联[17]，获得敏感个人信息；第二种情形，个人信息的敏感度不是一成不变的，受到其他变量的影响，信息的敏感程度在不同的场景下有不同呈现。某些信息在获取时并不敏感，但这一信息在新的场景下可能会成为敏感个人信息，而其他信息处理者无需通过严格的敏感个人信息途径即可获得，形成学者们描述的“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”的局面[18]。对于可能在未来被识别为敏感的信息，建议建立动态评估机制，及时调整保护措施，确保告知同意原则真正得到落实；信息处理者在处理方式、处理情景发生变化时，及时向信息主体进行披露，重新询问并征求其同意意见；同时保留信息主体的撤回同意权，要求处理者及时删除相关个人信息，并保证今后不再使用和处理，实现知情同意规则在潜在型敏感个人信息保护的贯彻落实，确保信息处理的合规性[19]。

3.3 鼓励制定行业标准

作为个人信息处理活动的核心主体，企业在敏感信息保护领域具有不可推卸的责任[20]。基于其掌握海量数据资源的技术优势及对系统性风险防控缺陷的深入了解，行业主体应当建立与数据处理规模相匹配的安全保障体系。2021 年上海市快递行业在行政主体指导下签署的信息安全自律公约，即为其他行业履行保护敏感个人信息的义务树立了模范标准。该内容要求企业通过组织架构优化、风险评估强化及防护体系迭代等方式，实质提升个人信息全生命周期管理能力，从而在数字经济发展与公民基本权利保护之间构建动态平衡。

在强化企业主体责任的基础上，亟需构建层次化的规范体系以完善治理格局。行政主管部门应主导制定具有行业适配性的技术标准，重点规制生物识别、行踪轨迹等特殊类别信息的采集边界、处理规则及存储要求。此类技术规范应具备三重制度功能：其一，通过明确合规指引增强企业风险管理预期；其二，依托行业自治机制形成差异化监督模式；其三，衔接《个人信息保护法》确立的监管框架，形成“法律－标准－契约”的多维治理体系。此制度设计既能弥补成文法滞后性缺陷，亦可激发社会共治效能，最终实现个人信息处理活动中各方权益的均衡保障。

4 结论

敏感个人信息的保护是《个人信息保护法》中的核心问题，也是实现数字时代个人权益保障的关键。本文通过分析我国敏感个人信息保护面临的现实困境，借鉴域外立法经验，提出了完善判断标准和处理规则的具体建议。综上所述，唯有构建兼具原则性与适应性的规则框架，方能实现个人信息保护与数字文明发展的共生共荣。未来，应进一步结合技术发展和社会需求，动态调整敏感个人信息的保护策略，以实现个人信息保护与数据利用的平衡。

参考文献

[1] 陈姿含. 人工智能算法决策中的敏感个人信息保护 [J]. 法律科学（西北政法大学学报），2024，42（6）：63－75.
[2] 郭传凯. 敏感个人信息处理规则的反思与修正 [J]. 政法论坛，2024，42（3）：102－113.
[3] 韩新远. 敏感个人信息的多维认定与严格保护 [J]. 数字法治，2024（2）：106－117.
[4] 邹开亮，王馨笛. 敏感个人信息保护视阈下平台企业数据合规制度要论 [J]. 北京科技大学学报（社会科学版），2024，40（2）：87－93.
[5] 自正法，袁紫藤. 未成年人个人信息保护的逻辑结构与规范路径 [J]. 南海法学，2023，7（4）：20－32.
[6] 米铁男，李瑞雪. 数据共享背景下的敏感个人信息保护法律问题研究 [J]. 北京邮电大学学报（社会科学版），2023，25（3）：40－46.
[7] 谢潇. 利益衡平视角下个人信息处理规则研究 [J]. 重庆交通大学学报（社会科学版），2023，23（2）：26－35.
[8] 邓灵斌. 欧盟、美国敏感个人信息保护法律规制比较研究及我国立法特色分析 [J]. 图书馆，2023（3）：67－73.
[9] 莫琳. 敏感个人信息的界定及其完善 [J]. 财经法学，2023（2）：21－35.
[10] 陈佳峯. 法律行为理论下个人信息保护的知情同意研究 [J]. 中国政法大学学报，2023（2）：197－207.
[11] 韩旭至. 敏感个人信息处理的告知同意 [J]. 地方立法研究，2022，7（3）：67－82.
[12] 高富平，尹腊梅. 数据上个人信息权益：从保护到治理的范式转变 [J]. 浙江社会科学，2022（1）：58－67，158.
[13] 孙清白. 敏感个人信息保护的特殊制度逻辑及其规制策略 [J]. 行政法学研究，2022（1）：119－130.
[14] 武腾. 最小必要原则在平台处理个人信息实践中的适用 [J]. 法学研究，2021，43（6）：71－89.
[15] 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 [J]. 比较法研究，2021（5）：33－49.
[16] 谢琳，王漩. 我国个人敏感信息的内涵与外延 [J]. 电子知识产权，2020（9）：4－16.
[17] 郑志峰. 人工智能时代的隐私保护 [J]. 法律科学（西北政法大学学报），2019，37（2）：51－60.
[18] 丁晓东. 个人信息私法保护的困境与出路 [J]. 法学研究，2018，40（6）：194－206.
[19] 丁晓东. 什么是数据权利？——从欧洲《一般数据保护条例》看数据隐私的保护 [J]. 华东政法大学学报，2018，21（4）：39－53.
[20] 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（5）：92－115.

（收稿日期：2025－03－09）

作者简介：

朱鸿静（2001－），女，硕士研究生，主要研究方向：民商法。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部