

国标生效！身份证号码不属于敏感个人信息了？

作者：潘永建 | 邓梓珊 | 李佳琪

更新提要

结合我们近期对监管口径的了解，自今年 11 月敏感个人信息国标正式实施后，个人信息处理者在准备个人信息出境申报等项目中虽然可以将敏感个人信息国标列入参考范围，但监管部门仍然会审核申报材料中对身份证号码等字段为何敏感、不敏感的判断理由和/或佐证材料，基于敏感个人信息的定义原则，作出符合实际情况的综合判断。由此，在当前的监管口径下，企业是否应继续将身份证号码列为敏感个人信息的工作要点在于能否结合其实际影响“自圆其说”，而继续按照敏感个人信息保护身份证号码整体上仍是更为谨慎、妥善的合规做法。同时，如果企业贸然一改以往严格的认定标准、大幅放松对身份证号码的保护水平，还可能对企业内部管理的延续性、对消费者/员工等主体的合规承诺产生一定负面影响。

引言

不论是在个人信息与隐私保护的主题下，还是数据出境监管的主题下，敏感个人信息的识别和管理都是数据合规工作的重点。但实践过程中，我们意识到识别敏感个人信息并不是一个有“标准答案”的问题，也注意到了一些认知误区。这可能是因为我国现行法律法规对于敏感个人信息仅做了“后果测试”型的定义，并给出了少量列举示例，而相关推荐性国标给出的具体示例又需要结合场景进一步判断其敏感性，这就给实务工作造成困扰。因此，我们结合过往项目经验与法律观察，梳理了敏感个人信息识别的思路与疑难问题，希望能为大家提供实务参考。

.....
如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

本篇基于原敏感个人信息系列专题文章的第三篇作出更新，在前两篇我们分别探讨了敏感个人信息的“[定义、识别准则与实务案例](#)”及“[概念溯源与域外制度对比](#)”。

随着数字化转型逐步推进，身份证件及身份证信息无论是在个人生活还是企业事务中的使用频率都在提升。然而，小小一张身份证，其实汇聚了多种个人信息的排列组合。对此，你也许也曾产生过下列困惑：

- ① 身份证上有姓名、性别、民族等似乎不太“敏感”的信息，还有身份证号码、住址信息、人像照片等较为“敏感”的信息。这些信息和身份证的整体扫描件，分别都是敏感个人信息吗？
- ② 如果第一问答案并不统一，会不会有些情况下某一身份证件信息被认定为敏感个人信息，换个情况又不是敏感个人信息？

为探究这些问题，我们将在本文带你回顾敏感个人信息相关的法律定义与国家标准，通过案例观察法院对身份证件信息的认定思路，并结合我们近期了解到的监管口径与在项目中观察到的企业痛点，讨论我们究竟该如何“科学”地判断身份证号码等身份证件信息的敏感属性。

一. 敏感个人信息的法律定义与国家标准

为厘清身份证件信息的“敏感性”，我们首先需要回到问题的核心：敏感个人信息在法律上的定义是什么？以及，我国目前在国家标准层面到底是如何界定和规范它的？

根据《个人信息保护法》（“《个保法》”），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”，并列举几大敏感个人信息的类别“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”。然而，身份证件信息并未在列举类别当中。

当我们将目光转向更侧重于个人信息保护实务问题的国家标准，则能发现身份证件信息的踪影，如下表所标注：

文件	推荐性国家标准《信息安全技术 个人信息安全规范》 (GB/T 35273-2020, 简称“35273 国标”)	推荐性国家标准《数据安全技术 敏感个人信息处理安全要求》 (GB/T 45574-2025, 简称“敏感个人信息国标”)
效力	2020.03.06 发布，现行有效	2025.04.25 发布，现行有效 (已于今年 11 月 1 日起实施)
敏感个人信息的	3.2 个人敏感信息 <u>一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。</u> 注 1: 个人敏感信息包括<u>身份证件号码</u>、个人生物识别信息、银行账户、通信记录和内容、财产信息、征信信息、	3.2 敏感个人信息 <u>一旦泄露或非法使用，容易导致自然人的<u>人格尊严受到侵害或人身财产安全受到危害</u>的个人信息。</u> 注：敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户和行踪轨迹等信息和不满十四周岁未成年人的个人信息。

定义	行踪轨迹、住宿信息、健康生理信息、交易信息、14 岁以下(含)儿童的个人信息等。 - 注 2: 关于个人敏感信息的判定方法和类型参见附录 B。 - 注 3: 个人信息控制者通过个人信息或其他信息加工处理后形成的信息, 如一旦泄露、非法提供或滥用可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇等的, 属于个人敏感信息。																													
敏感个人信息示例	附录 B 表 B.1 个人敏感信息举例 表 B.1 个人敏感信息举例 <table> <tr> <td>个人财产信息</td><td>银行账户、鉴别信息(口令)、存款信息(包括资金数量、支付收款记录等)、房产信息、录、征信信息、交易和消费记录、流水记录等,以及虚拟货币、虚拟交易、游戏类兑换码财产信息</td></tr> <tr> <td>个人健康生理信息</td><td>个人因生病医治等产生的相关记录,如病症、住院志、医嘱单、检验报告、手术及麻醉记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史等</td></tr> <tr> <td>个人生物识别信息</td><td>个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等</td></tr> <tr> <td>个人身份信息</td><td>身份证号、军官证、护照、驾驶证、工作证、社保卡、居住证等</td></tr> <tr> <td>其他信息</td><td>性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等</td></tr> </table>	个人财产信息	银行账户、鉴别信息(口令)、存款信息(包括资金数量、支付收款记录等)、房产信息、录、征信信息、交易和消费记录、流水记录等,以及虚拟货币、虚拟交易、游戏类兑换码财产信息	个人健康生理信息	个人因生病医治等产生的相关记录,如病症、住院志、医嘱单、检验报告、手术及麻醉记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史等	个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等	个人身份信息	身份证号、军官证、护照、驾驶证、工作证、社保卡、居住证等	其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等	附录 A 表 A.1 敏感个人信息类别 表 A.1 敏感个人信息类别 <table> <tr> <th>类别</th><th>描述</th></tr> <tr> <td>生物识别信息</td><td>个人基因、人脸、声纹、步态、指纹、掌纹、虹膜和虹膜等生物识别信息</td></tr> <tr> <td>宗教信仰信息</td><td>个人信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动和特殊宗教信仰等个人信息</td></tr> <tr> <td>特定身份信息</td><td>残障人士身份信息、不宜公开的职业身份信息等其他个人信息</td></tr> <tr> <td>医疗健康信息</td><td>——与个人的身体或心理的伤害、疾病、残疾和疾病风险或隐私有关的健康状况信息*,如病症、既往病史、家族病史、传染病史、体检报告和生育信息等; ——在疾病预防、诊断、治疗、护理和康复等医疗服务过程中收集和产生的个人信息,如医疗就诊记录(如医疗意见、住院志、医嘱单、手术及麻醉记录、护理记录和用药记录)、检验检查数据(如检验报告和检查报告)等</td></tr> <tr> <td>金融账户信息</td><td>个人的银行、证券、基金、保险和公积金等账户的账号及密码、公积金联名账号、支付账号、银行卡磁道数据(或芯片等效信息)和基于账户信息产生的支付标记信息和个人收入明细等个人信息</td></tr> <tr> <td>行踪轨迹信息</td><td>连续精准定位轨迹信息、车辆行驶轨迹信息和人员连续的活动轨迹信息等个人信息</td></tr> <tr> <td>不满十四周岁未成年人个人信息</td><td>不满十四周岁未成年人的个人信息</td></tr> <tr> <td>其他敏感个人信息</td><td>精准定位信息、居民身份证照片、性取向、性生活、征信信息、犯罪记录信息* 和显示个人身体私密部位的照片或视频信息等个人信息</td></tr> </table>	类别	描述	生物识别信息	个人基因、人脸、声纹、步态、指纹、掌纹、虹膜和虹膜等生物识别信息	宗教信仰信息	个人信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动和特殊宗教信仰等个人信息	特定身份信息	残障人士身份信息、不宜公开的职业身份信息等其他个人信息	医疗健康信息	——与个人的身体或心理的伤害、疾病、残疾和疾病风险或隐私有关的健康状况信息*,如病症、既往病史、家族病史、传染病史、体检报告和生育信息等; ——在疾病预防、诊断、治疗、护理和康复等医疗服务过程中收集和产生的个人信息,如医疗就诊记录(如医疗意见、住院志、医嘱单、手术及麻醉记录、护理记录和用药记录)、检验检查数据(如检验报告和检查报告)等	金融账户信息	个人的银行、证券、基金、保险和公积金等账户的账号及密码、公积金联名账号、支付账号、银行卡磁道数据(或芯片等效信息)和基于账户信息产生的支付标记信息和个人收入明细等个人信息	行踪轨迹信息	连续精准定位轨迹信息、车辆行驶轨迹信息和人员连续的活动轨迹信息等个人信息	不满十四周岁未成年人个人信息	不满十四周岁未成年人的个人信息	其他敏感个人信息	精准定位信息、居民身份证照片、性取向、性生活、征信信息、犯罪记录信息* 和显示个人身体私密部位的照片或视频信息等个人信息
个人财产信息	银行账户、鉴别信息(口令)、存款信息(包括资金数量、支付收款记录等)、房产信息、录、征信信息、交易和消费记录、流水记录等,以及虚拟货币、虚拟交易、游戏类兑换码财产信息																													
个人健康生理信息	个人因生病医治等产生的相关记录,如病症、住院志、医嘱单、检验报告、手术及麻醉记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史等																													
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等																													
个人身份信息	身份证号、军官证、护照、驾驶证、工作证、社保卡、居住证等																													
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等																													
类别	描述																													
生物识别信息	个人基因、人脸、声纹、步态、指纹、掌纹、虹膜和虹膜等生物识别信息																													
宗教信仰信息	个人信仰的宗教、加入的宗教组织、宗教组织中的职位、参加的宗教活动和特殊宗教信仰等个人信息																													
特定身份信息	残障人士身份信息、不宜公开的职业身份信息等其他个人信息																													
医疗健康信息	——与个人的身体或心理的伤害、疾病、残疾和疾病风险或隐私有关的健康状况信息*,如病症、既往病史、家族病史、传染病史、体检报告和生育信息等; ——在疾病预防、诊断、治疗、护理和康复等医疗服务过程中收集和产生的个人信息,如医疗就诊记录(如医疗意见、住院志、医嘱单、手术及麻醉记录、护理记录和用药记录)、检验检查数据(如检验报告和检查报告)等																													
金融账户信息	个人的银行、证券、基金、保险和公积金等账户的账号及密码、公积金联名账号、支付账号、银行卡磁道数据(或芯片等效信息)和基于账户信息产生的支付标记信息和个人收入明细等个人信息																													
行踪轨迹信息	连续精准定位轨迹信息、车辆行驶轨迹信息和人员连续的活动轨迹信息等个人信息																													
不满十四周岁未成年人个人信息	不满十四周岁未成年人的个人信息																													
其他敏感个人信息	精准定位信息、居民身份证照片、性取向、性生活、征信信息、犯罪记录信息* 和显示个人身体私密部位的照片或视频信息等个人信息																													

表 1 我国相关国家标准对敏感个人信息的定义与示例

对比 35273 国标与敏感个人信息国标, 我们可以观察到几点关键变化:

- ① 在敏感个人信息的定义上:
- 35273 国标定义较《个保法》更为细致, **明确将“身份证件号码”列为敏感个人信息**;
 - 敏感个人信息国标沿袭《个保法》的定义分类, 其列举的基本分类与《个保法》保持一致, 定义中**未明确提及身份证件号码**等身份证件信息。
- ② 在敏感个人信息的示例上:
- 35273 国标仅对“4+1”类敏感个人信息类型展开列举(个人财产信息、个人健康生理信息、个人生物识别信息、个人身份信息, 以及其他信息), 并**将整体的“身份证”列入“个人身份信息”**;
 - 敏感个人信息国标则遵循《个保法》, 对“7+1”类敏感个人信息类型展开列举(生物识别信息、宗教信仰信息、特定身份信息、医疗健康信息、金融账户信息、行踪轨迹信息、不满十四周岁未成年人个人信息, 以及其他敏感个人信息), 而**仅将单独的“居民身份证照片”列入“其他敏感个人信息”, 且未再提及整体的“身份证”或单独的“身份证件号码”**。

此外，敏感个人信息国标的“转向”并非空穴来风，类似的修改思路此前已在全国网络安全标准化技术委员会 2024 年 9 月发布的技术文件《网络安全标准实践指南——敏感个人信息识别指南》(TC260-PG-20244A, “敏感个人信息识别指南”)中得到体现。

二. 实践中对身份证号码敏感性识别的解题思路

仅基于前节所述变化，我们也许会得出一个简单粗暴的结论——“按敏感个人信息国标，身份证号码不再算敏感个人信息了！”此结论一出，仿佛不少高风险的敏感个人信息处理场景便能原地消失，对应的合规评估申报及技术成本也能随之湮灭……

然而，这一结论真的能在实务中得到认可吗？至少从当前的监管与企业实践来看，**不能**。

一方面，结合我们近期对监管口径的了解，自今年 11 月敏感个人信息国标正式实施后，个人信息处理者在准备个人信息出境申报等项目中**虽然可以将敏感个人信息国标列入参考范围，但监管部门仍然会审核申报材料中对身份证号码等字段为何敏感、不敏感的判断理由和/或佐证材料，基于敏感个人信息的定义原则，作出符合实际情况的综合判断**。由此，在当前的监管口径下，企业是否应继续将身份证号码列为敏感个人信息的工作要点在于能否结合其实际影响“自圆其说”，而继续按照敏感个人信息保护身份证号码整体上仍是更为谨慎、妥善的合规做法。同时，如果企业贸然一改以往严格的认定标准、大幅放松对身份证号码的保护水平，还可能对企业内部管理的延续性、对消费者/员工等主体的合规承诺产生一定负面影响。

另一方面，敏感个人信息国标对敏感信息字段仅采取举例模式，而非绝对适用于企业在实践中面临的任何场景。“身份证号码”单独出现的情况下，有可能不构成敏感个人信息，因为即便泄露也未必会对个人信息主体合法权益造成损害。但企业在实践中仅收集单一身份证号码的情况堪称稀缺，而往往会在不同场景下收集个人信息主体的多项个人信息，且常常出现身份证号码与其他个人信息组合出现、甚至与其他海量信息汇聚融合的复杂情况。因此，**企业不宜仅依据国家标准给出的示例对身份证件信息简单“对号入座”，而应在困惑时回望《个保法》对敏感个人信息的定义原则，对不同场景下实际处理的身份证件信息予以场景化个案判断**，综合考虑单项个人信息、成组信息、汇聚融合后信息的敏感程度，铭记“灵魂三问”于心：

- ① 该(组)个人信息一旦遭到泄露或者非法使用，是否容易导致自然人的**人格尊严**受到侵害？
- ② 该(组)个人信息一旦遭到泄露或者非法使用，是否容易导致自然人的**人身安全**受到危害？
- ③ 该(组)个人信息一旦遭到泄露或者非法使用，是否容易导致自然人的**财产安全**受到危害？(这是身份证号码最易构成敏感个人信息的判定问题，例如，身份证号码后四位可能被用作验证信息，可能与其他个人信息结合用于身份验证办理贷款等)

值得补充的是，在近年涉及身份证件信息的相关司法案例中，也常常出现对敏感个人信息予以场景化个案判断的裁判说理，我们相信这也有助于企业伙伴在实践中作为判断的参考思路：

案号	法院	涉及身份证件信息是否属于敏感个人信息的说理(节选)
(2023)京 0491 民初 5576 号	北京互联网法院	“柴*的实名信息和私信信息中包含有柴*的 <u>身份证件号码</u> 及照片、人脸识别信息、婚姻关系等内容，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，故该信息同时属于敏感个人信息。”
(2024)京 04 民终 1620 号	北京市第四中级人民法院	“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的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。实名认证信息系公民在互联网使用过程中对其身份识别的相关信息，该信息包含用户身份信息、 <u>证件信息</u> 以及人脸识别等信息，该类信息一般情况下在特定范围内由用户设限公开，具有高度敏感性……”
(2021)沪 02 刑终 1055 号	上海市第二中级人民法院	“ <u>居民身份证信息</u> 涵盖居民的人脸、唯一身份号码、户籍地址信息，是公民重要的身份证件，在公民生产、生活中具备重要地位和作用，关系公民人身、财产安全，且具备相当程度隐私性，显然应认定为危及公民人身、财产安全的个人信息，对此，刑法应予以从严保护……”
(2024)沪 01 民终 410 号	上海市第一中级人民法院	“案涉保险单所载明信息为手机号、 <u>身份证号码</u> 、职业等信息，虽然包含了敏感个人信息，但上述信息一般情况下可适用于正常的社会生活和社交场合，用于个人身份的识别和社会交往，因而更多地具有积极利用的属性，而非通常意义上不愿他人知悉的私密信息。因此，上诉人主张被泄露的信息，难以界定为隐私权保护范畴。”
(2019)浙 0192 民初 5468 号	杭州互联网法院	“该卖家在开设淘宝店铺时留存的信息为个人真实姓名、 <u>身份证号</u> <u>码</u> 、手机号码、地址等、地址等具有一定敏感性而不宜全部对外公示的个人信息司作为平台经营者，一方面有义务对消费者因交易纠纷而申请的卖家身份信息予以披露，另一方面对自然人卖家在开设店铺时留存的个人敏感身份信息有必要的保障责任……”

表 2 涉及身份证件信息敏感性判断的司法案例

如经过个案判断，企业发现实际处理的身份证号码等身份证件信息的确可能对个人信息主体上述权益产生危害的，则建议从这一危害后果倒推回实际的业务场景，与业务、技术同事及外部法律顾问积极商讨不收集该信息或进一步脱敏、匿名化处理的可行性，并根据实际整改情况采取相应的保护措施，以免为企业带来本可以规避的合规成本。

如您希望就相关问题进一步交流，请联系：



潘永建
+86 21 3135 8701
david.pan@llinkslaw.com



邓梓珊
+86 21 6043 3793
susan.deng@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市朝阳区光华东里 8 号
中海广场中楼 30 层
T: +86 10 5081 3888
F: +86 10 5081 3866

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: Llinkslaw

本土化资源 国际化视野

免责声明：

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2025