Open Journal of Legal Science 法学, 2023, 11(4), 3199-3206
Published Online July 2023 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2023.114456

Hans汉斯

大数据时代下敏感个人信息保护的路径完善

刘耀婷

贵州大学法学院，贵州 贵阳

收稿日期：2023年5月18日；录用日期：2023年6月13日；发布日期：2023年7月28日

摘 要

随着数据分析技术愈发成熟，个人信息面临着前所未有的挑战。其中，敏感个人信息较一般个人信息需要采取更加严格的保护措施。为了对敏感个人信息精准保护，应当以法律条文静态列举与特定情景动态判断为主要的判断方法，明确哪些个人信息属于敏感个人信息。此外，以保护个人信息、促进信息流通、实现经济效益最大化为基本原则，在现有法律保护的基础上提出完善“告知同意”这一关键措施：提高“告知同意”的标准、建构不同的“告知同意”结果。并且提出应对敏感个人信息进行再分级，对不同层级的敏感信息施以不同的保护手段，提高保护效率，推动大数据时代下的信息利用。

关键词

敏感个人信息，告知同意，大数据，层级

Improving the Path for Protecting Sensitive Personal Information in the Era of Big Data

Yaoting Liu

School of Law, Guizhou University, Guiyang Guizhou

Received: May 18th, 2023; accepted: Jun. 13th, 2023; published: Jul. 28th, 2023

Abstract

With the maturity of data analysis technology, personal information is facing unprecedented challenges. Among them, sensitive personal information requires stricter protection measures compared to general personal information. In order to accurately protect sensitive personal information, the main judgment methods should be static listing of legal provisions and dynamic judgment of specific situations, to clarify which personal information belongs to sensitive personal information. In addition, based on the basic principles of protecting personal information, promoting in-

文章引用: 刘耀婷. 大数据时代下敏感个人信息保护的路径完善[J]. 法学, 2023, 11(4): 3199-3206.
DOI: 10.12677/ojls.2023.114456

formation circulation, and maximizing economic benefits, this paper proposes the key measures to improve "informed consent" on the basis of existing legal protection: improve the standard of "informed consent", and construct different "informed consent" results. And it is proposed to re classify sensitive personal information, apply different protection methods to different levels of sensitive information, improve protection efficiency, and promote information utilization in the era of big data.

Keywords

Sensitive Personal Information, Inform and Agree, Big Data, Hierarchy

1. 问题的提出

随着科学技术不断发展，个人信息保护面临诸多挑战。由于大数据时代的便利性，人们获取他人的个人信息变得很容易，侵犯他人的隐私权也变得更加常见。例如互联网公司未经允许利用他人个人信息进行个性化推荐，或者利用技术手段剖析一般个人信息从而得到更深层次的个人信息进行售卖等，诸如此类的事情发生使得社会普遍开始意识到个人信息需要得到法律保护。事实上，并非所有的个人信息都需要得到法律层面的保护，因为存在某些个人信息是日常生活必须向社会公开的信息，就比如姓名、性别、年龄等。

敏感个人信息属于个人信息的一种。与一般个人信息不同，应对其采取高强度法律保护。因为与一般个人信息相比，敏感个人信息泄露容易对信息主体的人格尊严、人身以及财产造成损害。我国新颁布的《个人信息保护法》中就敏感个人信息作了概括说明与简单列举并行的定义方式，既说明了一般的判断方法，又列举了社会大众普遍认知的内容，相较之前的分散性保护措施，此次立法取得了突破性进展。可是在《个人信息保护法》中仍存在几个问题需要进一步讨论。第一，如何明确界定敏感个人信息。虽然在《个人信息保护法》中列举了哪些信息属于敏感个人信息，但实际上还有部分未列举的个人信息一般情况下不具有敏感性，在特定场景下具有敏感特征。例如个人在社交媒体上分享生活日常，表面上看是根据个人意愿所分享的信息，但由于在大数据这一背景下，通过技术可以挖掘出普通日常生活下更深层次的个人信息，此时就涉及到“敏感”层面。所以需要明确界定哪些个人信息是需要法律予以高敏感度保护的。第二，虽然法律规定使用他人个人信息需要当事人同意，但是“同意”应当达到什么样的程度以及利用者如何理解“同意”需要明确。由于数据技术应用上的专业性，用户并不能读懂冗长的知情同意书，涉及的专业性术语以及语句过于繁杂，导致用户并不能真正理解其点击的“同意”选项事实上在许可信息处理者哪些权限。敏感个人信息能得到实质保护的前提是个人能够真正实现“同意”。第三，法律对敏感个人信息保护较为笼统性，大众容易陷入误区。敏感个人信息的敏感度并不一致，有些信息遭到侵害对个人的影响较为轻微，有些信息遭到侵害却会带来毁灭性的影响。并且在大数据时代下，个人信息不仅仅具有信息属性，还具有经济属性。一方面，互联网公司多是根据分析用户偏好实现信息流通，以达到最终盈利目的。另一方面，社会管理对于个人信息的收集需求也在提升。一味对敏感个人信息统一保护，不利于经济发展，也不利于信息管理。《个人信息保护法》对于敏感个人信息遭到侵害的处理方式具有统一性，难以实现精确保护敏感个人信息。

本文旨在从上述三个问题展开，阐清敏感个人信息的判断方法、提出如何完善个人“同意”方案、最后就精确保护敏感个人信息提出分级保护解决措施。

2. 敏感个人信息的判断方法

基于主观损害风险与客观损害风险两种风险基准，为了达成对敏感个人信息认定的共识，通过横向比较世界各国关于敏感个人信息的界定方法，采取法律条文静态列举与特定情景动态判断两种措施，二者动静结合、相辅相成，共同作为启动敏感个人信息保护机制的关键一步。

2.1. 法律条文静态列举

法律条文静态列举的方式在世界各国通行。欧盟 GDPR 列举了敏感个人信息的类型，包括种族或民族背景、政治观念、宗教或哲学信仰、工会成员身份、基因数据、生物性识别数据,以及和自然人健康、个人性生活或性取向相关的数据。日本 APPI 列举了种族、宗教信仰、社会地位、病史、犯罪记录、犯罪受害人的记录及其他需要谨慎处理否则可能会带来社会歧视或不利的信息。泰国 PDPA 列举了有关性行为、犯罪记录、健康状况、国籍、种族、政治观点或宗教信仰的数据。巴西 LGPD 第五条规定种族或民族血统、宗教信仰、政治见解、工会或宗教隶属关系、哲学或政治组织成员身份、健康、性生活、与自然人有关的基因或生物统计数据为敏感个人信息。以上四份文件均将宗教信仰、种族、医疗信息列举为敏感个人信息。

这样的列举方式优势之处在于信息处理者及信息主体能迅速根据法律规定判断哪些信息不能被随意收集、泄漏、处理或须遵循更为严格的信息保护原则，有利于发挥法律的预防功能和指引功能，实现动态矫正的效果。但其缺点在于信息的内容与形式都会随科技发展、社会变迁而发生变化，单一列举会造成部分新的信息类型在保护方面无法可依。并且，由法律规定和判断信息是否敏感的立法方式并未考虑信息主体的主观感受，既可能保护过度又可能保护不足[1]。

2.2. 特定情景动态判断

个人信息是否具有敏感属性，需要在特定情景下予以判断。美国学者尼森鲍姆(Helen Nisenbaum)最早提出“场景理论”，他认为属性界定应当从简单二分法中跳脱出来，不能单一根据某个要素判断信息的性质，而应将具体问题纳入到具体情景中具体分析。尼森鲍姆教授研究发现，敏感信息与隐私期待的契合度高度取决于场景因素，她将场景变量特定化为五个要素，即信息主体、信息发送者、信息接收者、信息性质以及信息传输原则[2]。受该理论影响，经合组织在 1980 年制定《OECD 个资原则》时没有采取传统模式下列举个人敏感信息的方法，《个资保护协定》虽然以内容明确界定个人敏感信息，但其解释报告中提出：资料处理会对人产生伤害，并不是基于该资料之内容，而是该资料的使用情境。美国 2012 年《网络环境下消费者的数据隐私保护》也体现了依情境评估信息敏感性的理念，而 2015 年《消费者隐私权利法案》的政府讨论稿更是极力倡导情境理念[1]。

在大数据背景之下，如何根据“场景理论”判断个人信息的性质至关重要。信息与隐私不同，信息不是为了保护而存于世间，相反恰恰是为了流通、利用。而个人信息的主要价值在于社会交往的可识别性，是正常社会交流的媒介基础。基于个人信息的此类特征，判定方式并不能单一采纳法律条纹静态列举的非黑即白的方式，而应根据实际情景动态判断。随着数据挖掘技术的发展，信息处理者对不具有固定格式，不具有约定规则的非结构化数据[3]进行分析，一些表明上不具有敏感性的个人信息经过数据处理显现出其隐匿的一面。如用户为了运用网络公司提供的平台会允许其获取一些个人信息，通过这个平台上传自己的照片、分享日常生活经历，就算没有公布自己的身份、信仰，但是数据经过对其所处的环

境、生活特征也能分析出其具体的个人信息。此时一些看似平常的信息内容也具有了“敏感”性质。这样的判断方式也存在不足之处，最为明显的就是主观性太强，不同情景下信息的属性大不相同，难以有统一的认定标准。此时就应当以法律条文静态列举方式为导向，兼采特定情景动态判断，二者有机结合共同认定个人信息的“敏感性”。

3. 精进“告知同意”路径

我国《个人信息保护法》中明确规定了个人信息处理者应当向信息主体告知处理敏感个人信息的必要性以及对个人权益的影响，并且必须征得信息主体的单独同意。这一规定的确是将对敏感个人信息的处理权交给了信息主体本身，但是在实际生活中“告知”方式层出不穷，“同意”也并不简单。

学者徐磊、刘春对一些主流 APP 的个人信息保护政策进行横向对比，发现各 APP 的个人信息保护政策五花八门。有的内容过于冗杂，篇幅很长，关键信息不突出；有的内容过于简洁，重要信息并没有纳入其中，只字未提敏感个人信息，很大程度上侵犯了用户的知情权；还有的内容专业术语过多，难以理解，并且只是单一列举了敏感信息的种类，并没有告知如果用户同意平台利用其敏感个人信息所面临的风险程度[4]。此外，APP 推送的个人信息保护政策通常只出现在信息收集阶段，互联网平台在后续对信息的处理、使用、传递阶段并没有告知用户，这一系列行为究竟会不会带来风险、带来什么样的风险，用户一概不知。

另一方面，就信息主体的自决权而言，存在除了点击“同意”就别无选择的情形。当信息主体必须使用某一 APP 时，其所面临的无非就是“全有或全无”的选择空间，不勾选“同意”则意味着放弃使用权。面对此类情形，用户又如何通过“同意”来维护自身的权益。还有一些个人信息当时并没有损害人格尊严、人身或者财产的风险，但是在数据聚合技术处理后这样的风险会提升，非数据专业人员又怎么可能会预判到各种信息关联后将会导致什么样的不利后果。最为关键的是，同意与否很大程度上取决于个体的认知水平，当信息处理者的告知内容过于复杂、晦涩，普遍认知能力下的信息主体无法根据这一份告知书来判断其将面临的风险。

3.1. 设置严格的“告知同意”标准

如前所述，敏感个人信息与一般个人信息不同，敏感性的核心在于“高风险性”，一旦泄漏或者滥用，所引发的不利后果远高于一般个人信息，因此应当对敏感个人信息的“告知同意”作更高的标准要求。

一方面，法律应当明确规定个人信息保护政策中必须列明哪些条款，避免企业为了经济效益插科打诨，以冗长的内容掩盖没有列举的事实，以假乱真，侵犯消费者的权益。其中还应当对敏感个人信息的种类进行明显标注，增大字体或者更改字体颜色，确保履行告知义务。并且信息处理者应当在个人信息保护政策中用简单明了、通俗易懂的语言说明如果使用其平台将会触及哪些敏感个人信息，由专业人员将风险具体化，降低信息主体的同意成本，确保“同意”是信息主体的真实意思表示，尽可能避免因信息主体的个人认知水平而导致重大误解。此外，信息处理者还应当根据其专业性预先替用户判断哪些一般个人信息在经过数据处理分析后存在转变为敏感个人信息的风险。由于数据聚合技术的发展，用户难以判断自己之前同意利用的信息是否存在高风险性，这时就应该由数据处理者运用其专业知识替用户做出一个预判，确保信息主体真正控制自己的个人信息，而不再只是一个单一化的同意行为。

另一方面，应当建立一个动态的告知制度[5]。之前提到的“场景理论”中就一般个人信息在不同的场景下会转变信息属性作出了阐述。在互联网数据时代，最早的数据收集也许并不造成风险，但在后面的处理、使用、传递阶段是否会构成敏感性则无法确定。当信息属性转变，敏感个人信息面临危机，此

时的信息处理者就应当重新发出告知，让信息主体明确其面临的风险、决定是否继续同意。但是此时的重新告知，并不是时刻告知。我国《民法典》《个人信息保护法》以及《网络安全法》中都将特定目的作为敏感个人信息处理的重要规则。特定目的规则旨在对运营商予以目的性指引，进而在整体上规制运营商的敏感个人信息处理活动[4]。但是随着数据时代的推进，这样的目的限制不利于对信息的利用，也增加了“告知”的成本，所以与传统的特定目的限制理论相对，笔者认为在大数据时代应当对“目的”进行扩张解释。也就是说当信息处理者向用户明确告知了收集或者利用其敏感信息的目的并取得了用户的同意后，之后信息处理者的活动若在此前告知的目的范围内或与之相关联的其他目的，都无需向用户重新告知并取得用户的重新同意。主要理由在于收集和处理、使用个人信息存在时间差，由于网络科技的发展和商业创新可能一日千里，信息主体与信息处理者可能均未预见有重要价值的额外目的，如果不允许把敏感个人信息用于此额外目的，会造成资源上的浪费。此外，贯彻该原则既能够避免毫无限制地处理个人信息，又可以在一定限度内加强对个人信息的活用，起到平衡个人信息的保护与活用之作用[6]。

3.2. 设置区分性的“告知同意”结果

前面提到信息主体在面对 APP 的个人信息保护政策时，如果不同意其敏感个人信息被平台收集或处理时，将会直接不能使用该 APP。信息主体阅读个人信息保护政策后认为其中的某些信息如果被收集、利用会造成严重的风险时，可以选择完全同意或者部分同意，而选择完全同意与部分同意的用户能享受到的服务自然存在区别。如当视频网络平台需要收集用户的日常兴趣、浏览频率或者需要分析经过安全审核的自我上传视频等内容时遭到用户的拒绝，那么平台则不能违背用户的真实意思表示对其信息聚合分析。但与此同时，用户不能享受到平台对其个性化的视频推送，而需要在茫茫视频素材里找到自己喜欢的视频内容。笔者认为，只有设置区分性的同意结果，才能为信息主体的选择留有余地，从而避免在某种情况下必须使用某个平台却又陷入部分个人敏感信息可能会被不当利用的困境之中。基于此构想，各个 APP 是否可以设置两种运行模式：一种是勾选“完全同意”的用户运行模式，一种是勾选“部分同意”的用户运行模式，并且信息处理者应当在个人信息保护政策中具体说明勾选“部分同意”的后果，即进入该模式后在使用方面将会面临哪些限制。由信息主体根据自我对敏感信息的风险判断、平台的使用需求，综合考虑是否就敏感信息的收集或者处理进行授权。

4. 制定“敏感分级”保护制度

《中华人民共和国个人信息保护法》第二十八条中详细列举了敏感个人信息包括：生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。这些敏感信息种类的辐射范围很广，虽然可以对其进行匿名化处理或者加密处理，但是由于有被泄漏或者滥用的风险，大多数用户持拒绝态度，这对当下急需利用数据以实现经济发展造成了阻碍。若对所有的敏感个人信息采取同样的保护措施会容易造成保护不足或保护过度，并且会不利于数据流通以创造更大的社会价值。将敏感个人信息划分为高层级、中层级、低层级三个级别，对敏感性进行分级，更利于在运用数据实现经济效益的同时做到精准保护。

4.1. 高层级敏感个人信息

将生物识别信息、医疗健康信息、以及不满十四周岁未成年的个人信息认定为高敏感度的敏感个人信息，采取最为严格的保护措施。首先，运营商必须获得信息主体本人或者其父母、其他监护人的单独同意且是明示同意、书面同意，不得默示同意更不得推定信息主体同意。其次，必须在最初征求同意时阐明的目的范围收集、处理、利用、传递等，在后续阶段若发现这三类信息的潜在经济价值也不得采用

“目的关联原则”处理这三类信息，需要重新征求信息主体的同意。最后，信息主体还享有任意撤销权、删除权，一旦在使用过程中信息主体认为可能会对其造成风险，就可以撤销其同意决定、删除运营商收集或公布的个人信息，运营商必须立马采取救济措施，无需经协商等待处理结果。

生物识别信息是指“对自然人物理、生物或行为特征进行技术处理得到的能够单独或者与其他信息结合识别该自然人身份的个人信息”，主要包括指纹、人脸、声纹、虹膜、DNA、步态。这类信息都具有直接识别性、唯一识别性的特征，无需采取数据聚合技术即可以识别具体的个人，一旦遭到泄漏或者非法利用则会造成直接损失。当前使用最具争议性的是人脸识别。人脸识别技术作为一种生物识别技术，可以简单归纳为通过深度学习算法对脸部信息的特征提取和分类识别，该技术可用于识别照片，视频或实时人物[7]。就人脸识别而言信息处理者无法对其进行匿名化和加密化，因为一旦采取这类保护措施，那么人脸信息便失去其利用价值，不能收集也无法利用。所以对于生物识别信息这种直接明确指向性的个人信息应该认定为高敏感层级的敏感个人信息。

医疗健康信息是反映患者健康特征、贯穿全部医疗过程的具有个体识别性的健康信息，其涉及到患者的生理和心理健康状况、治疗过程和效果、遗传基因、病史病历等诸多方面。医疗健康信息与私密信息密切相关，是隐私权与个人信息的交互部分，因此侵犯医疗健康信息往往涉及到侵犯患者的隐私权、人格权，对这类信息的泄漏或者处理不慎极其容易造成信息主体人格上受到歧视、精神心理上遭受压力以及社会评价降低。去年 1 月份，日照市中心医院一医生在网上直播妇科手术片段，不仅暴露了患者的疾病信息，还暴露了患者的身体私密部位。日照市东港区卫生健康局以医疗信息泄漏为由对该行为处以五万元的罚款，涉事医生被依法依规注销执业医师资格证书、予以开除并且遭到刑事拘留[1]。这样的行为侵犯了患者的隐私权，泄漏了患者的医疗健康信息，严重影响到信息主体的日常生活，因此医疗健康信息应认定为高敏感层级的个人信息。

不满十四周岁的未成年人属于限制民事行为能力人与完全民事行为能力人相比，其判断能力、自我保护能力有相当大的差距。从社会现实来看，未成年人对新技术具有更强的适应力，设定较之传统民法更低的年龄保护标准有助于其从广泛的信息活动中受益[8]。十四周岁以下的未成年人与十四周岁以上的限制民事行为能力人相比，其生活经历、心智成熟度存仍有一定区别。面对复杂的隐私告知政策或者个人信息保护告知政策很难作出正确的选择，那些冗长、晦涩的内容对于他们的认知水平是个不小的挑战。此外，这个年龄段的未成年人心理上相对脆弱，其敏感个人信息遭到非法利用后会对其幼小的心灵造成难以泯灭的伤害，对其人格尊严以及人身造成严重的损害，这样的损害也许是永久性的。由于这样的特殊性，在法律将他们的个人信息设定为敏感个人信息，需要得到其父母或者其他监护人的同意运营商才可以收集、处理、利用的基础之上，笔者认为应该增强其敏感级别，以实现最高级别的保护。

4.2. 中层级敏感个人信息

将金融信息、行踪轨迹信息以及与二者相关的经数据聚合技术可识别出具体个人的其他信息设定为中层级的敏感个人信息。针对这两类信息，在告知同意上可以采取部分明示、部分模式的同意模式。根据客观权益侵害风险基准来判断，对于风险性较高的，应当明示同意，反之则默示同意。同时对于金融信息和行踪轨迹信息的使用目的范围限制适当放宽，不局限于目的本身。

近些年来，金融机构内部人士监守自盗，利用职权泄漏客户信息的事例层出不穷。金融信息包括财产信息、账户信息、信用信息、金融交易信息及其他衍生信息。对原始数据进行处理、分析后形成的能够反映特定个人某些情况的信息，例如个人消费或者投资意愿、支付习惯、风险偏好等等都属于金融信

[1]《日照中心医院：疑似直播妇科手术被抓医生系麻醉师，警方正调查》，载澎湃新闻 2022 年 1 月 19 日，https://baijiahao.baidu.com/s?id=1722354943623401433&wfr=spider&for=pc。

息的衍生信息[9]。在大数据时代，金融信息数据体量大、经济价值极高，稍有不慎，则可能导致个人金融信息被不法分子利用。并且由于数据互联互通，一旦泄漏，则会导致信息主体的金融信息在网络上全面铺开，造成巨大的经济损失。但是在不显示个人身份时单个的金融信息难以识别出具体的个人，多数情况下是信息联结后才具有唯一识别性，相比前面三种类型的敏感个人信息，金融信息不具有强度的直接识别性，风险性较低，应将其认定为中层级的敏感个人信息。

行踪轨迹主要是指信息主体所在的地理位置以及通常的行动路径，在大数据时代还包括随身携带的电子产品的定位信息。行踪轨迹数据信息收集的方式主要包括：使用应用软件(如社交软件、购买商品或服务软件、手机导航软件等)、手机本身的操作系统、第三方追踪工具等[10]。这类信息的泄漏主要是造成人身损害，如双方发生矛盾纠纷后，掌握行踪轨迹的一方可以直接去对方所在的场所实施打击报复，或者了解其家庭住址后趁其不在家实施盗窃等，在实践中并不少见。当信息主体的行动轨迹信息与其他个人信息聚合时，会有引发其他犯罪的可能，大学生父母常因诈骗分子掌握其子女的位置信息而受骗。但是过于严格的地理位置信息要求在紧急情况下存在局限性，如温州 20 岁女孩乘滴滴顺风车遇害后，滴滴公司客服拒绝向警方及时提供嫌疑人的车辆定位信息、车牌号码等详细信息，导致错过了可能的救援机会[2]。为了避免类似情况的发生，行踪轨迹信息应当认定为中层级敏感个人信息。

4.3. 低层级敏感个人信息

与前述敏感信息相比较，宗教信仰信息与特定身份信息的风险性较小，故将二者认定为低层级的敏感个人信息。保护措施的严格程度自然低于前述五种敏感信息。在知情同意方面，原则上允许默示同意，当信息聚合风险性提高时为例外。在收集、利用目的方面，允许在初始目的的范围内大幅度扩张解释，以不损害信息主体的权益为限。

宗教信仰是个人的一种主观意识状态。法律之所以将宗教信仰设定为敏感个人信息，很大原因在于社会中的非宗教信仰者易对宗教信仰者产生心理歧视，由歧视而引起群体之间的排外。出于主观权益侵害基准、保护信仰者的人格权，将该权利设定为敏感信息。再加上当前数据信息平台发展势头强劲，信息处理者可以利用信息主体的宗教信仰剖析其潜在的其他敏感内容，所以宗教信仰也值得与一般个人信息区分开来进行特殊保护。

特定身份信息的含义我国并没有明确规定。《个人信息保护法》草案一审稿和二审稿中规定了敏感个人信息的种类：种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪。可最终将“种族”与“民族”删除，而增加了“特定身份”概念，这说明了特定身份的内涵不止于此。学者叶鹏霄、肖冬梅认为特定身份信息应当包括种族、民族、身份证件及身份证件号码、犯罪记录[11]。事实上这些特定身份单一地来看并不容易具有高风险性，在正常的社会交际中通常被运用，但是信息主体主观上认为该两类信息就其生活的环境来说会对其造成极大的困扰、影响其正常生活并带来歧视，此时它们就存在高风险性。

5. 结语

在大数据时代下，个人信息的侵犯方式已从传统上的收集、归纳转变为云分析、数据聚合等方式。为了顺应时代的变化，需要加大对个人信息保护的力度。而敏感个人信息涉及人格权、人身权、财产权，并且与一般个人信息相比风险性极高，应当对其特别保护。我国《个人信息保护法》首次明确敏感个人信息的概念和内涵，提出收集和利用必须取得信息主体的单独同意，是个人信息保护在法律上的一大进

[2]《浙江乐清“滴滴顺风车司机杀人案”罪犯钟元被执行死刑》，载最高人民法院网 2019 年 8 月 30 日，https://www.court.gov.cn/zixun-xiangqing-179952.html。

展，但是该法律并没有对敏感个人信息的界定和特别保护措施作出具体的规定，需要加以明确。首先，对敏感个人信息进行精准保护第一步就是要判断哪些个人信息具有“敏感性”。其次，初步得出敏感结论以后要以法律条文为指引、场景理论为补充进一步确定个性信息的敏感度。最后，区别于一般个人信息，提高“告知同意”标准，并根据“敏感性”、“敏感度”对个人信息采取针对性的分级保护措施。

参考文献

[1] 胡文涛. 我国个人敏感信息界定之构想[J]. 中国法学, 2018(5): 235-254.

[2] 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[J]. 环球法律评论, 2022, 44(2): 85-99.

[3] 徐智, 王岳, 王欣. 结合区块链的非结构化大数据云存储优化研究[J]. 计算机仿真, 2021, 38(7): 304-307+354.

[4] 徐磊, 刘春. 敏感个人信息保护的实践困境与破解之道[J]. 情报理论与实践, 2022, 45(3): 42-49+41.

[5] 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.

[6] 杨智博. 韩国《个人信息保护法》的最新修正及其对我国之启示[J]. 华南理工大学学报(社会科学版), 2022, 24(1): 89-98.

[7] 张溪璠, 王晓丽. 人脸识别技术与应用的风险及治理研究[J]. 科学学研究, 2023, 41(3): 385-393.

[8] 冯恺. 个人信息处理中“儿童同意”的年龄标准[J]. 暨南学报(哲学社会科学版), 2021, 43(8): 89-100.

[9] 朱芸阳. 个人金融信息保护的逻辑与规则展开[J]. 环球法律评论, 2021, 43(6): 56-73.

[10] 赵哲. 大数据时代个人地理信息权的法律保护研究[J]. 苏州大学学报(哲学社会科学版), 2019, 40(3): 92-98.

[11] 叶鹏霄, 肖冬梅. 我国特定身份信息的界定[J]. 图书馆论坛, 2022, 42(7): 65-73.