敏感个人信息保护制度的解释性重构

丁晓东*

内容提要 我国与域外法律大多以类型列举或存在严重侵害风险界定敏感个人信息，在保护方式上采取二元保护、强化保护。但敏感个人信息保护的理解与适用存在挑战，其界定存在不确定性，保护方式也不尽合理。这一挑战的根源在于敏感个人信息具有场景化特征，个人信息并非因其本身而敏感。在立法层面对敏感个人信息保护进行重构不具有必要性与可行性，应在解释与适用过程中对其进行重构。敏感个人信息的界定应以目的解释为主、参照文义解释，价值判断应以我国国情为依据，风险认知判断应以专家判断为主、兼顾公众感知风险，判断因素应考虑信息主体、处理主体、处理方式、识别概率等。敏感与非敏感个人信息的分类保护应迈向场景化、动态化：在行政监管中，应采取自下而上的场景化保护；在司法与行政执法案例中，应采取以案释法的场景化保护。就强化保护措施而言，应迈向监管下的自我监管。衔接敏感个人信息与私密信息，应在个人信息保护与隐私权保护两种制度下进行分析。

关键词 个人信息保护 敏感个人信息 反歧视 场景化 私密信息

目 次

* 中国人民大学法学院教授。本文系2023年度国家社科基金重大项目“当代中国数字法学基本范畴体系研究”（项目批准号：23&ZD154）的阶段性成果。

一、引　言

敏感个人信息保护是个人信息分类分级保护的重要制度。我国《个人信息保护法》在第二章第二节中专门规定了敏感个人信息的处理规则。其中，第 28 条规定了敏感个人信息的定义和一般规则，将敏感个人信息界定为“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”；在处理规则方面，该条规定处理敏感个人信息必须“具有特定的目的和充分的必要性，并采取严格保护措施”。第 29 条至第 32 条、第 55 条进一步规定了处理敏感个人信息的特殊保护方式，例如，取得个人的单独同意，向个人告知处理敏感个人信息的必要性以及对个人权益的影响，处理未成年人信息应当取得未成年人的父母或者其他监护人的同意，事前进行个人信息保护影响评估等。域外部分国家和地区也采取了类似立法，例如欧盟《一般数据保护条例》第 9 条将某些类型的数据列为“特殊类型个人数据”，对其设置严格的强化保护制度。

敏感个人信息的法律解释与制度适用面临挑战，尤其面临互联网与大数据等技术变革所带来的法律挑战。一方面，敏感个人信息的概念解释与界定方法存在争议。敏感个人信息应当以法律中的列举为准，还是以处理个人信息可能导致自然人“受到危害”为准？[①] 目前，大量常见类型的个人信息是否属于敏感个人信息尚不明确，例如，个人照片、个人视频、个人声音、身份证号码、手机号码、工作单位、家庭住址信息未被我国《个人信息保护法》所列举，但这类信息也可能在某些场景下具有敏感性。另一方面，敏感个人信息保护方式也存在争议。在敏感个人信息界定不确定性的背景下，我国《个人信息保护法》中所规定的敏感与非敏感个人信息的二元保护框架是否合理？是否应当像有的学者所言，个人信息保护应放弃敏感个人信息这一概念以及相应的制度工具？[②]

针对敏感个人信息法律保护，学界已经进行了很多分析与研究，但仍然存在众多空白与不足。首先，已有研究并未充分引入比较法与历史研究视角。其次，已有研究并未对敏感个人信息“因何敏感”问题进行深入分析。最后，已有研究并未对敏感个人信息的制度困境提供具体解决方案。本文努力在这些方面进行创新性论述：在视角方面，全面分析敏感个人信息保护的来龙去脉以及欧美等国家和地区在敏感个人信息问题上的立场；在原理层面，对敏感个人信息为何具有不确定性、其制度为何存在过严或过宽问题进行法理思考，阐述敏感个人信息因何敏感；在制度层面，对个人信息保护界定与保护方式提出了新方案。笔者认为，在立法层面，敏感与非敏感个人信息的二元划分具有表达

① *See* Karen McCullagh, *Data Sensitivity: Proposals for Resolving the Conundrum*, Journal of International Commercial Law and Technology, Vol.2:190, p.190-201 (2007).

② *See* Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, Northwestern University Law Review, Vol.118:1081, p.1081-1138 (2024).

功能，可以向社会传递敏感个人信息强化保护的信息。考虑到我国《个人信息保护法》制定不久，域外各国也普遍在立法中引入敏感个人信息概念，并对其进行特殊保护，笔者认为，在立法层面对敏感个人信息制度进行重构既无必要、也不可行，但在法律解释与法律适用层面可以对这一制度进行重构。基于此，本文首先分析敏感个人信息界定与保护方式的挑战，此后从历史与原理的角度对其进行反思，最后对敏感个人信息的界定与保护方式进行解释性重构。

二、敏感个人信息界定与保护的难题

敏感个人信息保护面临两方面的挑战或难题：其一，敏感个人信息的范围不确定，这对敏感个人信息的界定提出了挑战。其二，对敏感个人信息的保护方式也存在难题，无论是敏感与非敏感个人信息的二元保护、敏感个人信息的强化保护措施、敏感个人信息与私密个人信息的交叉，都存在若干难题或困境。③

（一）敏感个人信息界定的难题

敏感个人信息首先面临界定的难题。我国《个人信息保护法》采取了“法律目的 + 开放列举”的定义方式，一方面将“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”界定为敏感个人信息，另一方面又采取了列举式的规定，将“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”7 类信息列举为敏感个人信息。④从法律解释来看，对上述规定可以采取文义解释与目的解释两种方法。如果采取文义解释的方法，那么《个人信息保护法》第 28 条所列举的 7 类个人信息就必然属于敏感个人信息。与之相对，如果采用目的解释的方法，则法律对敏感个人信息的界定应当以侵害风险为标准。如果某一信息并不会带来较为严重的侵害风险，即使此类信息属于被列举的范围，其也不应被纳入敏感个人信息范畴。同样，即使某类信息从未被纳入《个人信息保护法》或相关法律法规和标准中的敏感个人信息范畴，但只要其存在更大的侵害风险，则此类信息仍然应当被视为敏感个人信息进行保护。⑤

基于法律目的的解释方法还可以进一步细分。《个人信息保护法》第 28 条并未直接说明判断个人信息敏感性的主体。第一种理解是这种主体是信息处理者，即敏感个人信息是相对信息处理者而言的，如果信息处理者能够利用此类信息造成重大侵害，则此类信息就属于敏感个人信息。第二种理解则将此类主体界定为个人信息主体，只要个体感觉某类信息处理具有敏感性，则此类信息就应当被划入敏感信息。第三种理解则将此

③ 一般个人信息也存在类似问题，参见丁晓东：《论个人信息概念的不确定性及其法律应对》，载《比较法研究》2022 年第 5 期，第 46-60 页。

④ 参见杨合庆主编：《中华人民共和国个人信息保护法释义》，法律出版社 2022 年版，第 86 页。

⑤ 参见王利明：《敏感个人信息保护的基本问题——以〈民法典〉和〈个人信息保护法〉的解释为背景》，载《当代法学》2022 年第 1 期，第 3-14 页。

类主体界定为技术人员或不特定公众，从他们的角度判断个人信息泄露或非法使用的风险。在很多情形下，不同主体对于敏感性的判断可能非常不同。

即使对敏感个人信息采取统一的界定与解释方法，敏感个人信息的范围也仍然具有不确定性，因为很多看上去非敏感的个人信息也可以推断出敏感个人信息。以《个人信息保护法》第 28 条所列举的医疗健康信息为例，个人的就诊记录、用药记录、病史、身体症状可以直接揭示个人的医疗健康信息，但个人的食品消费记录、运动习惯、网页浏览记录也可以间接揭示个人的医疗健康情况。法律如何归类此类可以间接推断出敏感个人信息的一般个人信息将是一个两难问题：如果法律将此类可以推断出敏感个人信息的信息排除在外，那么其结果将是很多具有敏感个人信息特征的信息无法得到严格保护；相反，如果将可以推断出敏感个人信息的信息包括在内，那么大量的普通个人信息都会成为敏感个人信息。因为通过个人信息的比对、分析与汇聚融合，信息处理者或第三方都有可能推断出敏感个人信息。甚至一些看似非个人信息的信息，也可能在某些场景下成为敏感个人信息。⑥ 例如，微博、抖音等社交软件上显示的用户 IP 所属国家与省份，这类信息一般不会成为个人信息，因为一个国家与省份至少有上百万或上千万的人口，但如果某位网络用户前一天的 IP 地址在国内某个省份，第二天显示在域外某个国家，这就显示了这位网络用户的行踪轨迹，其 IP 地址就可能成为个人信息甚至是敏感个人信息。

在互联网与大数据时代背景下，敏感个人信息的界定存在更多不确定性。在网络搜索等技术的帮助下，人们可以获取大量的公开个人信息和相关背景信息，相关主体通过将这些信息与某一信息结合，就可能将某一信息转化为敏感个人信息。例如，美国某在线网站曾经公布了 2 千万条经过匿名化处理的个人搜索记录，单从这些搜索记录来看，这些信息并不是敏感个人信息，甚至可能都不算个人信息，但是相关主体通过将这些信息与网络可以获取的公开信息进行结合比对分析，就很容易破解其中的很多信息。《纽约时报》甚至随机选取了一位用户，通过公开信息比对分析找到了这位用户的家庭住址并登门拜访。⑦ 再比如，在“剑桥分析丑闻案”中，剑桥分析公司最初收集的主要是个人的非敏感个人信息，但通过大数据的汇聚与融合分析，最终推断出了大量个人的政治倾向等敏感个人信息。⑧ 随着信息技术的发展与数据分析行业的兴起，可以预见，从非敏感个人信息中推断出敏感个人信息的情形将更为常见。

（二）敏感个人信息保护方式的难题

敏感个人信息的保护方式也存在难题与挑战。首先，在敏感个人信息界定不确定的背景下，对这一类型的信息进行特殊保护的制度设计是否仍然有必要？已经有不少学者

---

⑥ *See* David L. Mothersbaugh et al., *Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information*, Journal of Service Research, Vol.15:76, p.76-98 (2012).

⑦ *See* Michael Barbarom & Tom Zeller, *A Face Is Exposed for AOL Searcher No. 4417749*, at http://www.nytimes.com/2006/08/09/technology/09aol.html (Last visited on Sep. 11, 2024).

⑧ *See Facebook–Cambridge Analytica Data Scandal*, at https://en.wikipedia.org/wiki/Facebook–Cambridge_Analytica_data_scandal (Last visited on Sep. 13, 2024).

表达了对敏感个人信息保护的担忧甚至反对。例如,保罗·奎因和吉安克劳迪奥·马尔基里对欧盟《一般数据保护条例》中的敏感个人信息保护进行了研究,指出欧盟在界定敏感个人数据上具有很大的不确定性。这种不确定性包括两方面:一方面是敏感个人信息面临不断膨胀的难题,很多传统上被认为不属于敏感个人信息的信息,都可能在大数据时代被纳入敏感个人信息的范围,这一情形可能使敏感个人信息保护失去意义;另一方面,敏感个人信息的范围也可能被人为限制或缩小,导致很多具有敏感性的个人信息未能得到应有的更高级别保护。⑨ 美国学者丹尼尔·索洛夫的立场则更为激进,其不仅指出了敏感个人信息的高度不确定性与制度困境,而且直接主张废除敏感个人信息这一概念与相应制度。索洛夫认为,个人信息保护应当关注数据的“使用、伤害和风险”,而不是个人信息是否敏感。⑩

其次,敏感个人信息的强化保护措施也需要进一步讨论。我国《个人信息保护法》主要从以下方面对敏感个人信息进行强化保护:其一,在合法性基础方面,处理敏感个人信息应当具有特定的目的和充分的必要性,即在一般个人信息的目的限定与最小必要等原则基础上进行升级;⑪ 其二,在告知同意方面,处理告知同意除了应当向个人告知一般个人信息所需要告知的事项,还应当“向个人告知处理敏感个人信息的必要性以及对个人权益的影响”,而且应当取得个人的“单独同意”;⑫ 其三,在预防与技术保护措施方面,处理个人信息除了遵循一般个人信息所需要的要求,还应当进行个人信息影响评估与采取其他强化保护措施。⑬ 但上述制度设计存在不少落地难题,其解释与适用存在争议。例如,就合法性基础而言,如果个人信息的敏感性可能在收集后发生变化,那么对于某一信息的收集是否需要在收集之初就区分一般目的限定和特定目的限定、最小必要性和充分必要性?就告知同意而言,告知同意的问题已经被广泛讨论,其核心问题在于这一制度日益流于形式,无法真正保护个人信息权益。⑭ 在此背景下,敏感个人信息保护所要求的强化告知同意是否可以有效保护敏感个人信息?就预防与技术保护措施而言,《个人信息保护法》所设置的相关制度是否可以对敏感个人信息进行有效保护?

最后,敏感个人信息与私密信息的制度衔接也需要回应。我国《民法典》没有采用敏感个人信息的概念,但引入了私密信息的概念。相反,《个人信息保护法》则采用敏感个人信息的概念,并未规定私密信息。在敏感个人信息与私密信息存在交叉的背景

---

⑨ *See* Paul Quinn & Gianclaudio Malgieri, *The Difficulty of Defining Sensitive Data — The Concept of Sensitive Data in the EU Data Protection Framework,* German Law Journal, Vol.22:1583, p.1583-1612 (2021).

⑩ *See* Daniel J. Solove, *supra* note 2, 1081-1138.

⑪ 参见刘权:《论个人信息处理的合法、正当、必要原则》,载《法学家》2021 年第 5 期,第 1-15 页。

⑫ 参见《个人信息保护法》第 29、30 条。

⑬ 参见《个人信息保护法》第 28-31、55 条。

⑭ *See* Neil Richard & Woody Hartzog, *The Pathologies of Digital Consent*, Washington University Law Review, Vol.96:1461 (2019); Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, Pace Law Review, Vol.40:310, p.310-398 (2020);万方:《个人信息处理中的“同意”与“同意撤回”》,载《中国法学》2021 年第 1 期,第 167-188 页。

下，[15] 法律适用将面临一系列问题，例如，私密信息与敏感个人信息如何区分？当某类个人信息既属于私密信息又属于敏感个人信息时，法律应当如何适用？在此类信息处理中，个人信息主体与监管机构除了依据《个人信息保护法》提起权利主张和进行监管之外，个人是否也可以依据隐私权框架对相关行为提起隐私侵权之诉？

三、敏感个人信息的场景化特征

分析上述难题，需要追溯个人信息保护以及敏感个人信息的发展历史，从原理或法理层面对敏感个人信息保护进行分析。个人信息保护的制度目标并非保护个人信息本身，而是保护个人信息处理中的相关权益。因此，敏感个人信息呈现场景化特征，其敏感性往往因为其处理所涉及的不同因素与其保护的不同权益而不同。

（一）敏感个人信息场景化的历史性

在很长一段时间内，个人信息保护制度都未明确规定敏感个人信息。例如，美国1973 年发布的奠定个人信息保护制度雏形的《公平信息实践准则》未规定敏感个人信息。甚至直到今天，美国联邦层面制定的一系列法律也并未直接区分敏感与非敏感个人信息。在欧洲，敏感个人信息的概念虽然在 20 世纪 70、80 年代就已经在瑞典、德国黑森州的立法中出现，但法律并未对其作出特殊规定。1980 年，经济合作与发展组织（OECD）在制定《保护私隐及个人信息跨境流动指引》时提到了敏感个人信息，但认为各国对于何种个人信息具有敏感性有不同的认知，因此统一敏感个人信息的界定是不可能的。[16]

美国虽然没有引入敏感个人信息的概念，但其联邦层面的立法却与敏感个人信息立法具有类似性，主要通过以下法律针对某类具有敏感性、风险性的个人信息进行规制：1970 年制定的个人信息保护法的雏形《公平信用报告法》针对征信类个人信息，1974 年制定的《家庭教育权利与隐私法》针对学生的教育类个人信息，1974 年制定的《隐私法》针对美国规制机构所收集的个人信息，1988 年制定的《视频隐私保护法》针对涉及视频租借、购买等的个人信息，1994 年制定的《司机隐私保护法案》针对司机的个人信息，1996 年制定的《健康保险便携性和责任法案》针对医疗健康类个人信息，1998 年制定的《儿童在线隐私保护法》针对在线收集的儿童类个人信息，1999 年制定的《格拉姆 - 里奇 - 布莱利法案》针对金融类个人信息进行保护，2008 年制定的《基因信息非歧视法案》针对基因类个人信息，等等。综合而言，美国在联邦层面没有统一的个人信息保护法，其所制定的法律仅仅针对特殊类型或具有敏感性的个人信息。

敏感个人信息保护正式成型的关键节点是 1981 年由欧盟国家所主导的《在个人数

---

⑮ 参见韩旭至：《敏感个人信息的界定及其处理前提——以〈个人信息保护法〉第 28 条为中心》，载《求是学刊》2022 年第 5 期，第 132-145 页。

⑯ *See* Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), para 19(a).

据自动处理方面保护个人的公约》(以下简称《108 号公约》)。[17] 这部公约将“种族出身、政治观点、宗教或其他信仰、健康或性生活”、与犯罪记录相关的个人数据等列为“特殊类型”的数据,并规定除非成员国法律提供充分保护,不得对此类数据进行自动化处理。[18] 不过《108 号公约》并没有设定统一的敏感个人信息保护规则,各缔约国可以自行采用不同的保护措施。其后,1995 年欧盟制定的《数据保护指令》采取了开放列举的界定方法,将“揭露种族或民族出身、政治观点、宗教或哲学信仰、工会会员资格、有关健康或性生活”的数据列入“特殊类型”范畴,但规定成员国可以在此基础上增添敏感个人数据的类型。在处理规则方面,《数据保护指令》规定除非具有个人“明确同意”等合法性基础,成员国原则不得处理此类数据。[19] 2016 年制定的《一般数据保护条例》继承了《数据保护指令》关于敏感个人数据的大部分规定,同样规定了除非获得数据主体的明确同意以及为了少数特定目的,数据处理者原则上不得处理敏感个人数据。不过《一般数据保护条例》也有若干不同:一是扩大了敏感个人数据的范围,在列举范围中增加了基因数据、生物特征数据、性生活和性取向几类数据;二是采取了穷尽式样列举的方法,明确规定敏感个人数据只限于其列举的类型,成员国不得再增加敏感个人数据的类型。

在欧盟《一般数据保护条例》的影响下,美国州层面制定的综合性个人信息保护法也引入了敏感个人信息保护。美国加利福尼亚州于 2020 年制定的《加利福尼亚州隐私权利法案》首次引入了敏感个人信息的概念。根据其界定,这类信息主要包括:披露消费者社会保险、驾照、州身份识别、护照号码的个人信息,消费者的登录账户、金融账户、借记卡或信用卡号码,以及允许访问账户的任何必需的安全或访问代码、密码或凭据,消费者的精确地理位置,消费者的种族或民族出身、宗教或哲学信仰或工会会员资格,消费者购物中心、电子邮件和短信的内容,消费者的基因数据、生物特征信息,与消费者健康、性生活或性取向有关的个人信息。之后,美国科罗拉多州、弗吉尼亚州、犹他州、康涅狄格州的个人信息保护法也引入了敏感个人信息保护。[20]

我国的敏感个人信息保护同样受到域外特别是欧盟的影响。在《个人信息保护法》制定之前,我国法律并未明文规定敏感个人信息。《网络安全法》《电子商务法》《消费者保护法》都未区分敏感个人信息与一般个人信息。《民法典》也没有采用敏感个人信息的概念,而是采取“私密信息”的概念,规定对“私密信息”适用隐私权的相关规定。不过在行政法规、国家标准层面,一些制度引入或采用了敏感个人信息的概念。国务院

---

⑰ 《108 号公约》的签署方除了欧洲国家,还包括俄罗斯、墨西哥、阿根廷等国家。

⑱ *See* Council of Europe, Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (1981), Article 6.

⑲ *See* Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Eur. O.J. 95/L281), Article 8.

⑳ *See* Colorado Privacy Act (CPA), COLO. REV. STAT. § 6-1-1303(24); Virginia Consumer Data Protection Act, VA. CODE ANN. § 59.1-575; Utah Consumer Privacy Act, UTAH CODE ANN. § 13-61- 101(32); Connecticut Act Concerning Personal Data Privacy and Online Monitoring, UConn. Public Act No. 22-15 § 1(27).

于2013年发布的《征信业管理条例》规定，征信机构不得采集“个人的宗教信仰、基因、指纹、血型、疾病和病史信息”。2013年实施的国家标准《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》明确提出了个人敏感信息，将其界定为“一旦遭到泄露或修改，会对标识的个人信息主体造成不良影响的个人信息”。该标准还提出，“各行业个人敏感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。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等”[21]。2021年，《个人信息保护法》借鉴了欧盟的相关规定并结合我国国情，正式在法律层面确立了我国的敏感个人信息保护制度。

（二）敏感个人信息场景化的具体表现

综合敏感个人信息保护的发展历史可以发现，敏感个人信息的界定与保护取决于不同因素，这促成了敏感个人信息的场景化特征。以美国为例，美国联邦层面之所以对某些特定领域进行立法，是因为这些领域的个人信息处理产生了较大风险，特别是此类风险引起了公众关注。例如，针对征信个人信息立法是因为20世纪70年代美国征信企业获取了大量的消费记录等信息；针对教育个人信息立法是因为很多教育机构泄露学生的个人信息；针对规制机构的个人信息立法是因为美国的水门事件等一系列事件引发了公众对于美国政府的不信任。在此类立法过程中，一些突发性的公共事件也促成了美国国会立法，从而将一般个人信息转换为敏感个人信息。例如，美国著名的保守派法官罗伯特·伯克在被里根总统提名为美国最高法院法官人选后，其个人录像租借记录被一些记者获取和报道，导致其提名失败，这一事件促成了1988年的《视频隐私保护法》。再比如，一位疯狂的粉丝通过购买司机的驾驶信息，找到并枪杀了好莱坞女星丽贝卡·谢弗尔，这一事件促成了1994年制定的《司机隐私保护法案》。[22]

相较而言，欧盟对敏感个人信息的界定与保护偏重身份性因素，与反歧视的制度目标密切关系。[23]分析欧盟在多个文件中所列举的敏感个人信息，会发现其主要类型都是容易导致身份歧视的个人信息。《108号公约》《数据保护指令》和《一般数据保护条例》都包含了种族出身、政治观点、宗教或其他信仰等个人信息。《一般数据保护条例》所增加的基因数据、为了特定识别自然人的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，也都与反歧视的制度目标密切相关。相反，一些可能导致人身财产损害却不太可能引发歧视风险的数据反而未被欧盟视为敏感个人信息。例如，即使是个人的金融账号与密码、家庭住址、个人通信信息等类型的个人信息，《一般数据保护条例》也没有将其列入敏感个人信息。有关调查表明，欧洲的很多民众也认为金融账号等

---

[21] 国家质量监督检验检疫总局、中国国家标准化管理委员会《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。

[22] *See* Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, 1995, p.174-211.

[23] *See* Sandra Wachter, *Affinity Profiling and Discrimination by Association in Online Behavioral Advertising*, Berkeley Technology Law Journal, Vol.35:367, p.367-430 (2020).

信息具有高度敏感性,[24] 但欧盟《一般数据保护条例》等个人信息保护法并未将其列入敏感个人信息范围,反而将其他民众感知不那么敏感、但容易导致身份歧视的个人信息纳入其中,这凸显了欧盟的个人信息保护法将反歧视视为其核心制度目标。[25]

我国的敏感个人信息保护受到欧盟与美国的影响,但具有鲜明的中国国情因素。一方面,我国《个人信息保护法》中的敏感个人信息保护类似欧盟,其列举的“生物识别、宗教信仰、特定身份、医疗健康”等敏感个人信息也与欧盟的规定基本重合。这种列举表明,我国也将反歧视视为个人信息保护的目标之一。但另一方面,我国《个人信息保护法》将敏感个人信息界定为“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”,并且将“金融账户、行踪轨迹”也列举为敏感个人信息,这充分说明我国的敏感个人信息保护并不局限于反歧视,而是具有保护公民人身、财产以及其他人格尊严等多重目标。而且,即使是反歧视这一制度目标,我国的个人信息保护法也与西方存在较大区别。由于美欧历史传统中较为特殊的种族、民族等歧视,西方的反歧视具有较为强大的反区分传统(anti-classification)或“遮蔽身份”(identity-blind)的观念,[26] 这使得西方特别是欧盟将某些特定类型的身份性信息视为天然具有敏感性[27]。我国与欧盟的反歧视观念与面临的问题并不完全相同,我国更注重个人身份所引发的个体侵害与社会不公,而非消除所有的身份识别。例如,对于“民族”类信息,我国并不认为识别个人民族信息就一定会导致歧视,而是将民族信息视为辨识公民身份的公开或半公开信息。《个人信息保护法》的一审稿曾经将个人的“民族”信息也列举为敏感个人信息,但在终稿中被删除,就反映了我国与西方在看待敏感个人信息方面的差异。

综合而言,某类个人信息之所以敏感或不敏感,并非这类个人信息天然敏感或不敏感。相反,某类个人信息之所以敏感,是因为此类个人信息涉及某些重要的个人权益,对其进行处理或保护不当会带来重大风险;在不同场景下,处理某类个人信息所带来的风险非常不同,这就导致了敏感个人信息的界定容易受到多重因素的影响。

四、敏感个人信息界定的解释性重构

在我国与域外对敏感个人信息进行事前统一界定的背景下,可以通过法律解释将敏感个人信息的界定合理化。本部分分别从解释方法、价值判断、考虑因素出发,对我国敏感个人信息的界定进行解释性重构。

---

[24] *See* Consumer Fin Prot. Bureau, *Using Publicly Available Information to Proxy for Unidentified Race and Ethnicity* 1,3 (2014), at https://files.consumerfinance.gov/f/201409_cfpb_report_proxy-methodology.pdf (Last visited on Sep. 11, 2024).

[25] 参见李成:《人工智能歧视的法律治理》,载《中国法学》2021 年第 2 期,第 143 页。

[26] *See* Owen M. Fiss, *Groups and the Equal Protection Clause*, Philosophy & Public Affairs, Vol.5:107, p.107-177 (1976).

[27] *See* Reva. B. Siegel, *From Colorblindness to Antibalkanization: An Emerging Ground of Decision in Race Equality Cases*, Yale Law Journal, Vol.120:1278, p.1278-1367 (2011).

（一）敏感个人信息的解释方法

由于数字时代的立法面临一系列滞后性与不适应性的难题，在解释方法上应对《个人信息保护法》第28条采取目的解释的方法，将“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害”作为判断敏感个人信息的最终依据。而对于法律所列举的“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”，则可以将其作为参考标准而非终极标准。

采取目的解释的方法可以使得敏感个人信息界定更为合理。一方面，即使立法者明确列举了敏感个人信息的类型，这些个人信息也可能敏感程度不高，对其进行更严保护并不合理。例如，《个人信息保护法》所列举的特定身份未必比其他个人信息更为敏感，很多人都愿意公开或半公开自己的职业、社团归属等特定身份，并不觉得这类信息有多敏感。个人行踪轨迹也未必比个人家庭住址更为敏感，很多人可能愿意公开自己的行踪轨迹，但不愿意公开自己的家庭住址，因为公开自己的行踪轨迹主要涉及少量个人隐私，而公开家庭住址则可能给自己和家人带来侵扰甚至是安全威胁。另一方面，法律未列举的个人信息也可能在很多场景下具有高度敏感性，将它们视为非敏感个人信息可能造成保护不足。例如，个人照片、个人声音、个人视频、家庭住址、工作单位地址、阅读记录、网页浏览记录、消费购买记录，甚至是个人的IP地址、个人的Mac号、车架号等设备类信息，都可能成为敏感个人信息，这些信息不但可以推断出个人的生物识别信息、行踪轨迹等个人信息，而且一旦被犯罪分子掌握，也可能给个人带来较大风险。

文义解释的方法则可以作为界定敏感个人信息的参考方法。对于我国法律所列举的7种敏感个人信息，可以将其作为判断某类个人信息是否为敏感个人信息的重要参照，例如，可以推定这些属于敏感个人信息，但允许相关主体根据目的解释的方法对这些归类进行辨析。一方面，法律法规既然将某些个人信息列举为敏感个人信息，这些列举就反映了立法者的考量，而且这些列举也较为清晰。如果完全不顾法律法规的列举类型，则立法的权威性将受到威胁。另一方面，立法者对于敏感个人信息的界定也明确了以保护目的作为最终依据。在敏感个人信息具有不确定性，敏感个人信息与非敏感个人信息容易相互转换的背景下，如果以文义解释为最终依据，则法律对于个人信息相关的权益就可能保护过严或保护不足，违背了敏感个人信息保护的初衷。

（二）敏感个人信息界定中的价值判断

就价值判断而言，敏感个人信息的界定首先应首先结合我国国情，由我国民众对其进行判断。对于何谓敏感，不同国家和地区往往有不同价值取向。惠特曼曾经提出，欧洲人常常以“尊严”的视角看待隐私，而美国人则常常以“自由”的视角看待隐私。[28]在立法层面，欧洲各国在2018年《一般数据保护条例》实施之前对敏感个人信息进行

[28] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, The Yale Law Journal, Vol.113:1151, p.1151-1221 (2004).

了不同界定。例如，德国和奥地利等国家长期拒绝对敏感个人信息进行法律统一界定；芬兰将工会成员信息纳入敏感个人信息；葡萄牙和爱沙尼亚将基因数据列入敏感个人信息，但将个人财物数据排除在外。[29]《一般数据保护条例》统一界定了敏感个人信息，对其进行封闭式的列举。但这种做法的主要目的是统一欧盟法与欧盟的“数字统一市场战略”（digital single market strategy），避免欧盟个人信息保护的分裂割据，而不是指这类列举就是普适性、无可争议的。

对我国而言，敏感个人信息更应当结合我国的具体国情进行判断。与欧盟和美国不同，我国的隐私与个人信息保护文化与我国独特的政治、经济、社会现状密切相连。在法律解释与适用层面，我国对于敏感个人信息的界定也应当以我国民众对于个人信息敏感性的价值判断为最终标准。当然，在数据跨境流通问题上，敏感个人信息涉及不同国家和地区，当我国和其他国家与地区对于敏感个人信息的判断标准不同而导致数据跨境难题时，对敏感个人信息的判断就不能仅仅采取单边主义的立场，而应根据相关协议、标准与双边磋商来解决。[30]

在具体风险认知问题上，应注重中立性专业人员对敏感个人信息的判断，[31]同时结合普通个人对敏感个人信息的风险感知。在个人信息的敏感性判断中，专业人员往往依据个人信息泄露或违规使用带来的实际风险进行客观判断，而个人则常常依据其感知进行主观判断，二者并不总是一致。笔者认为，应首先注重中立性专业人员的判断，因为此类判断不仅可以合理判断与预防相关风险，还可以提供相对客观统一的标准。[32] 同时，法律也应当兼顾公众或普通个人的一般风险感知，因为公众的风险感知关乎民众对于个人信息处理的信任。[33] 如果公众对个人信息保护丧失信心，那么即使个人信息处理没有造成实际风险，也会影响个人信息的合理保护与合理利用。[34] 当然，参与判断个人信息敏感性的应当是一般民众，而非具体的个体。具体个体对于个人信息敏感性的判断千差万别，如果以每个个体的感知作为判断标准，敏感个人信息将完全无法判断。

（三）敏感个人信息界定的考虑因素

其一，个人信息的敏感性应考虑个人信息主体的身份。一些风险防御能力较弱的当事人的个人信息应归入敏感个人信息，其中，最为典型的是未成年人个人信息。未成年

---

[29] *See* Spiros Simitis, *Revisiting Sensitive Data*, at https://rm.coe.int/16806845af (Last visited on Sep. 11, 2024).

[30] 参见彭岳：《数据隐私规制模式及其贸易法表达》，载《法商研究》2022 年第 5 期，第 102-117 页；张继红、蔡雨倩：《敏感个人信息跨境流动的国际规制》，载《广西社会科学》2023 年第 7 期，第 107-118 页。

[31] 不过此处所指的专业人员应当是具有中立性的专业人员，而非作为信息处理者的专业人员或者与信息处理者具有利益关系的专业人员。

[32] *See* Cass R. Sunstein, *Laws of Fear: Beyond the Precautionary Principle*, Cambridge University Press, 2005, p.1-25.

[33] *See* Dan M. Kahan & Paul Sloivic, *Cultural Evaluations of Risk: "Values" or "Blunders"?*, Harvard Law Review, Vol.119:166, p.166-172 (2006).

[34] *See* Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in the Twenty-First Century*, University of Miami Law Review, Vol.69:559, p.559-630 (2015); 丁晓东：《基于信任的自动化决策：算法解释权的原理反思与制度重构》，载《中国法学》2022 年第 1 期，第 99-118 页。

人由于心智尚未成熟，缺乏自主意志，其个人信息处理可能带来较大风险。[35] 某些场景下的老年人也可能处于弱势地位，具有较高的被侵害可能性。例如，老年人的联系信息一旦被诈骗分子获取，再加上其他部分可信信息，就可能会成为电信诈骗的重点对象。残障人士、性少数群体等主体由于在社会上较为容易遭受歧视，反映这类群体身份的个人信息应当被认定为敏感个人信息。不过正如上文所述，我国的个人信息保护虽然将反歧视作为重要目标，但并不是将其作为唯一目标。《个人信息保护法》第 28 条明确提到敏感个人信息的界定范围要考虑“人格尊严”“人身、财产安全”等因素，说明个人信息与敏感个人信息所要保护的法益更为多重，与反歧视法的制度框架并不完全重合。就此而言，一些不具有歧视风险的个人信息主体可能会因为其身份而被纳入敏感个人信息，例如未成年人；一些具有一定歧视风险的个人信息主体则可能不会因为其身份而被纳入敏感个人信息，例如女性群体。此外，特殊身份的处理也可能有助于反歧视。[36]

其二，个人信息的敏感性应考虑处理主体。目前，各国法律实务与法学研究没有对个人信息的处理主体作出明确界定，或者进行了不同界定。例如，我国《个人信息保护法》没有明确说明识别个人信息的主体，第 28 条对敏感个人信息的界定中也未明确说明造成侵害风险的主体；欧盟《一般数据保护条例》“重述”第 26 条规定，个人信息识别的主体包括“控制者或其他人”；英国的信息委员会（ICO）规定，个人信息的识别主体为“有动机的侵入者”；[37] 美国早在 20 世纪 70 年代就通过《隐私法》将政府机构视为重点规制对象。对于不同的处理主体或识别主体，个人信息的敏感性将非常不同。例如，对于进行自动化处理的大型企业而言，个人家庭住址、工作单位地址可能并不敏感，因为大型企业一般都对这类信息进行加密化、去标识化处理，大型企业处理此类信息一般不会直接带来风险。但对于潜在的个人处理者而言，此类信息则具有高度敏感性，因为个人处理者更有可能泄露此类信息，对他人生活安宁与家庭安全造成威胁。国家机关与非国家机关处理个人信息所带来的风险与所涉敏感个人信息的界定也存在区别，因为二者对个人信息的利用方式、保护方式、侵害风险都非常不同。[38] 此外，在分析判断敏感个人信息时，还需要分析个人信息是否被其他处理者共享或者违规泄露，如果信息被共享或违规泄露可能被哪些主体获取。

其三，敏感个人信息界定应考虑信息处理方式。个人信息的处理方式千差万别，罗纳德·李恩斯曾经归纳了不同识别类型：L 类查找型识别（look-up）是为了查找某一个体，例如，通过姓名、电话或护照号码等标识符对特定个人进行查找；R 类确认型识别（recognition）是为了验证某人的身份，例如，利用人脸识别信息验证银行顾客的身份；C

㉟ 参见张素华、尹晓坤：《未成年人个人信息同意能力的理论证成及判定》，载《财经法学》2023 年第 6 期，第 3-17 页。

㊱ *See* Žliobaitė, I. & Custers, B. *Using Sensitive Personal Data may be Necessary for Avoiding Discrimination in Data-Driven Decision Models*, Artificial Intelligence and Law, Vol.24:183, p.185 (2016).

㊲ *See* Information Commissioner's Office, *Anonymisation: Managing Data Protection Risk Code of Practice*, (Nov. 20, 2012), at https://ico.org.uk/media/1061/anonymisation-code.pdf (Last visited on Sep. 11, 2024).

㊳ 参见赵宏：《告知同意在政府履职行为中的适用与限制》，载《环球法律评论》2022 年第 2 期，第 36-51 页。

类归类型识别（classification）是为了对某人进行归类，例如，将某人归入某一种族或某一消费群体；S 类会话型识别（session）是为了不同设备之间的交互与对话，例如，网站利用 cookie 技术识别顾客先前添加在购物车里的购买商品，以便进行下一步操作。[39] 在不同的识别类型中，个人信息的敏感性会发生变化。例如，在 L 型查找型识别的情况下，身份证号码、护照号码等具有唯一标识性的识别可能导致特定个体被唯一识别，此类个人信息理应归入敏感个人信息的范畴。但在 C 类归类型识别或 S 类会话型识别中，身份证号码、护照号码不仅不具有敏感性，甚至都无法直接识别个人。而对于种族出身、政治观点、宗教或其他信仰、性取向等身份类信息而言，这类信息可能在 C 类归类型识别中识别个人的特定身份，带来歧视风险，但在其他识别类型的识别中，这类信息则很难直接识别具体个人，其敏感性程度要低很多。

其四，敏感个人信息界定应考虑信息被识别的概率或可能性。敏感个人信息在被收集后，信息处理者往往对其进行一定的加密、去标识化处理，但此类个人信息一般仍然被认为属于个人信息，因为其仍然可以被间接识别或通过关联的方式而识别个人。不过从侵害风险来看，个人信息的识别程度显然会影响个人信息的敏感性。[40] 如果个人信息被识别的概率较高，其可以轻易被直接识别，则此类信息应具有更高的敏感性；相反，如果个人信息被重新识别的概率较低，则此类信息的敏感性应较低。个人信息的扩散性则是个人信息被识别概率的另一个维度，个人信息已经在多大程度上公开，是否容易进一步扩散，会直接影响个人信息被不特定主体识别的概率。[41] 在司法实践中，曾经有案例对司法诉讼文书中所公开的姓名、性别、家庭住址、电话号码等个人信息是否属于敏感个人信息有过争论。[42] 判断这类有限公开的个人信息是否属于敏感个人信息，应结合其进一步扩散所增加的识别概率以及可能带来的风险进行分析。

需要强调的是，敏感个人信息由于其场景化特征，其判断因素并不局限于上述列举因素。在域外，已有众多学者对其进行讨论，例如，法理学与个人信息保护领域研究的专家雷蒙·瓦克斯指出，敏感个人信息界定应当结合信息披露的规模、信息的历史久远程度、信息的可能接受者等因素进行综合考虑。[43] 信息隐私领域研究的学者海伦·尼森鲍姆也提出，隐私保护应当考虑具体场景，分析个人信息所涉及的行为者、信息种类、传输原则等要素。[44] 我国学者也进行了类似的讨论与分析。例如，有学者指出，敏感个人信息应当结合“泄露该信息是否会导致重大伤害”“给信息主体带来伤害的几率”“社会大

---

[39] *See* Ronald Leenes, *Do They Know Me? Deconstructing Identifiability*, University of Ottawa Law & Technology Journal, Vol.4:135, p.148 (2007).

[40] *See* Sophie Stalla-Bourdillon & Alison Knight, *Anonymous Data v. Personal Data - A False Debate: An EU Perspective on Anonymisation, Pseudonymisation and Personal Data*, Wisconsin International Law Journal, Vol.34:284, p.284-322 (2017).

[41] 参见刘晓春：《已公开个人信息保护和利用的规则建构》，载《环球法律评论》2022 年第 2 期，第 52-68 页。

[42] 参见余建华：《业委会在公众号公布起诉状被业主起诉》，载《人民法院报》2022 年 8 月 16 日，第 3 版。

[43] *See* Ramond Wacks, *Personal Information: Privacy and the Law*, Clarendon Press, 1989, p.238-239.

[44] *See* Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009, p.140-160.

多数人对某类信息的敏感度”这三个因素进行判断。[45] 有学者认为个人敏感数据应以“损害后果、一般隐私期待”为判断标准的静态列举模式结合以“损害后果、一般隐私期待、使用目的”为标准的动态场景模式予以认定。[46] 有学者主张结合“损害的严重性、发生可能性、公众认可度、技术可预见性等因素”判断个人信息的敏感性。[47] 有学者从个人信息内容与个人信息所处的环境进行分析，主张分析个人信息是否“具有强工具性和唯一识别性”，分析“信息处理者的认知能力、信息应用能力及信息存在状态”。[48] 还有学者指出，应当“综合考量个人信息主体、信息处理者、第三方主体、信息性质和处理目的等五个要素，动态界定敏感个人信息”。[49] 这些观点各自提供了独特视角，也揭示了敏感个人信息的场景化特征。[50] 本文的研究与这些研究具有一定的共通性，但本文和其他学者所列举的因素仅仅有助于分析某类个人信息在具体场景下是否具有敏感性，而非可以衡量某一类型个人信息是否必然属于敏感个人信息，因为，个人信息并非由于其本身而敏感或不敏感，其敏感性会随着具体场景而变化。

五、敏感个人信息保护方式的解释性重构

敏感个人信息的保护方式也应当通过法律解释进行重构。首先，基于法律解释的敏感个人信息保护应当抛弃“先界定、后保护”的保护方式，转为在不同场景中对敏感程度不同的个人信息进行区分保护。其次，敏感个人信息的强化保护框架应当给予信息处理者一定的自我监管空间，在此基础上进行强制监管，促使其保护措施与具体场景中的风险相适应。最后，应认识到隐私权与个人信息保护两种制度的差异，在此基础上实现私密信息与敏感个人信息制度衔接的协调。

（一）从二元区分到行业区分与个案区分

上文提到，由于敏感个人信息的高度场景化，包括索洛夫在内的一些学者主张彻底抛弃敏感个人信息，转而关注个人信息的使用、伤害和风险。笔者认为，索洛夫的这种分析对于揭示敏感个人信息的高度不确定性具有重要意义，但其提出的这一对策过于激进，忽略了当今人们普遍接受敏感个人信息的现实，而且也不符合个人信息分级分类保护的要求。更为合理的方案是，在承认与接受敏感个人信息的不确定性的基础上，采取更具有操作性、动态性和贴近个人信息场景化特征的保护模式。这种保护方式并不直接

---

[45] 参见胡文涛：《我国个人敏感信息界定之构想》，载《中国法学》2018 年第 5 期，第 235-254 页。

[46] 参见苏成慧：《论可交易数据的限定》，载《现代法学》2020 年第 5 期，第 147 页。

[47] 参见谢琳、王漩：《我国个人敏感信息的内涵与外延》，载《电子知识产权》2020 年第 9 期，第 4-16 页。

[48] 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，第 33-49 页。

[49] 参见王苑：《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》，载《环球法律评论》2022 年第 2 期，第 85-99 页。

[50] 参见郑泽星：《论侵犯公民个人信息罪的保护法益——场景化法益观的理论构造与实践立场》，载《清华法学》2023 年第 3 期，第 90-105 页。

依赖于法律法规对个人信息的界定，而是根据不同场景对不同个人信息进行动态保护。事实上，对于一般个人信息，索洛夫自己也采取这种进路，批评欧姆放弃个人信息界定的主张。欧姆曾主张，在大数据时代，个人信息与非个人信息的区分已经没有意义，任何非个人信息都可以演变为个人信息，因此应当放弃个人信息这一概念，改由风险规制的路径对相关信息实践进行规制。[51] 但索洛夫批评了这种主张，指出个人信息概念仍可以作为一种有效的制度工具，并提出已识别个人信息、可识别个人信息、不可识别个人信息的三元保护框架。[52] 在敏感个人信息问题上，索洛夫前期较为实用主义与稳健性的主张应该得到延续，其废除与取消敏感个人信息的主张则过于激进，反而是欧姆教授在敏感个人信息问题上的稳健性立场值得肯定。[53] 不过，为了适应敏感个人信息界定的场景化特征，法律也应当避免对其进行事前统一界定，在行政监管与司法或行政执法案例中采取更为场景化的保护方式。

在行政监管层面，相关法律解释与行政法规、规章可以对敏感个人信息采取自下而上的场景化保护方式。该保护方式指的是，法律避免在较高层级对敏感个人信息进行统一强化保护，但在较低位阶的规章、行业标准、具体领域操作规范层面对敏感个人信息进行分领域与分场景界定。尤其是在各个行业性与细分领域，由于具体行业与细分领域的业态相似，其处理个人信息的收集方式、种类、利用方式、存储与保护方式、泄露与下游风险都会具有类似性，因此由具体行业与细分领域对敏感程度不同的个人信息进行区别保护更具合理性。此外，具体行业与细分领域制定的行业标准与领域规范也更容易调整，可以根据个人信息所带来的风险动态调整不同类型个人信息的区别保护，[54] 避免高层级的法律法规制定后所形成的滞后或步调不一致问题。

在司法或行政执法案例中，法律应通过个案对敏感个人信息进行场景化保护。相比监管规则，敏感个人信息的司法或行政执法案例既有弱势也有优势。弱势在于，司法或行政执法案例往往缺乏专业机构所需要的专业性人才，而且对于相关案例的裁决都是事后的，难以对敏感个人信息进行事前规制与事前风险预防。不过司法或行政执法案例对敏感个人信息保护也有优势。首先，在司法或行政执法案例中，裁决者具备接触正反双方意见的机会，可以通过双方举证、辩论等形式而深入个人信息实践的具体场景，这可以使裁决者获取更为完整全面的信息，更为场景化地感知某一具体场景下个人信息的敏感性。其次，敏感个人信息的事前界定常常不科学，存在过宽和过窄保护，而敏感个人信息的事后保护则可以避免此类问题。通过案例来形成敏感个人信息的相关规则，也是许多国家在个人信息保护领域的长期实践，更为符合敏感个人信息与一般个人信息保护的相

---

[51] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, UCLA Law Review, Vol.57:1701, p.1701-1778 (2010).

[52] *See* Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, New York University Law Review, Vol.86:1814, p.1883 (2011).

[53] *See* Paul Ohm, *Sensitive Data*, Southern California Law Review, Vol.88:1125, p.1125-1196 (2015).

[54] 参见苏宇、高文英：《个人信息的身份识别标准：源流、实践与反思》，载《交大法学》2019 年第 4 期，第 54-71 页。

关特征。例如，美国联邦贸易委员会积累了丰富的个人信息保护实践判例，形成了个人信息保护的“普通法”规则；[55] 欧盟法院、欧洲人权法院以及欧盟各国监管机构的判例已经成为个人信息保护的重要法律渊源；欧洲数据保护委员会（EDPB）在其发布的各类个人信息保护指南中也列举了大量案例，通过案例来阐述和把握其个人信息保护的一般规则。我国近年来也积极在法院与监管部门推动个人信息保护的典型司法案例与执法案例，以此应对个人信息保护的场景化与不确定性问题。通过司法或行政执法案例保护敏感个人信息，更符合一般原理。正如大量研究表明，通过自下而上的案例串联来形成规则，在很多场景中比自上而下的规则确定更为合理。即使在成文法时代，司法或行政执法案例也具有其独特优势，应当发挥其制度功能。[56]

（二）敏感个人信息统一强化保护的重构

对敏感个人信息进行一般性的强化保护，可能同时导致保护不足与保护过度。解决上述困境，应首先认可信息处理者具有较强能力和一定动力对敏感个人信息进行强化保护。在实践中，信息处理者也会对个人信息进行分级分类保护，但这种分级分类并不一定对应敏感与非敏感个人信息的二元划分和二元保护措施。在有的情形中，信息处理者可能对某些看似非敏感的个人信息进行严格保护。例如，社交软件企业一般对通讯信息、小范围公开的朋友圈信息进行最高级别保护，严防此类信息的泄露与违规使用。在其他情形中，信息处理者可能将信息的敏感性分为两级以上的多个级别，或者对所有信息进行一体化的严格保护，而非仅仅将其列为敏感个人信息与非敏感个人信息。对于信息处理者自发采取的敏感个人信息保护或分类分级保护，法律应给予信息处理者自我规制一定的空间，允许信息处理者对敏感个人信息进行一定程度的自我界定、自我分级与自我监管（self-regulaiton）。

不过信息处理者的分类分级保护也应当受到法律的强制性监管，而非完全的自我监管。完全自由放任的自我监管可能带来一系列问题。信息处理者的分类分级保护可能并不科学合理，甚至可能通过虚假的分类分级保护规避监管。例如，信息处理者可能采取“代理”（proxy）策略，即通过处理非敏感个人信息实现对敏感个人信息的处理。信息处理者也可能刻意混淆与掩盖其处理敏感个人信息所带来的风险，或者并未采取与处理敏感个人信息风险相应的保护措施。在这些情形中，完全自我监管都可能导致大量敏感个人信息无法得到合理保护。[57] 尤其是一些没有市场竞争压力、从第三方获取信息的信息处理者，以及没有严格上级监管压力的公权力机构，由于缺乏外在压力，他们在进行信息处理时往往缺乏对个人信息进行合理保护的动力，同时也没有足够的个人信息保护能力。在这类情形中，应当避免赋予此类信息处理者的自我监管权力。[58] 赋予信息处理

---

[55] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, Columbia Law Review, Vol.114:583, p.585 (2014).

[56] *See* Guido Calabresi, *A Common Law for the Age of Statutes*, Harvard University Press, 1982, p.1-21.

[57] *See* William McGeveran, *Friending the Privacy Regulators*, Arizona Law Review, Vol.58:959, p.959-1026 (2016).

[58] *See* Woodrow Hartzog, *Privacy's Blueprint: The Battle to Control the Design of New Technologies*, Harvard University Press, 2018, p.1-10.

者对敏感个人信息进行一定程度的自我监管，应当仅限于已经采取严格个人信息保护措施的信息处理者。法律对于敏感个人信息的保护在发挥信息处理者积极性的同时，应当积极履行其整体性的监管职责，实现“监管下自我监管”（regulated self-regulation）。[59]

首先，就敏感个人信息处理的合法性基础而言，机械性地监管将导致个人信息保护与利用平衡的难题。一方面，如果对合法性基础进行严格解释，要求处理所有可能推断或演化为敏感个人信息的信息都必须满足“特定的目的和充分的必要性”，将导致大量一般个人信息无法得到合理利用。另一方面，如果对合法性基础进行宽松解释，允许信息处理者处理所有并非具有显著敏感性的个人信息，则信息处理者可以轻松规避法律对于敏感个人信息的强化保护。为避免此类困境，法律应当赋予信息处理者一定程度的自我规制，允许其对处理敏感个人信息的必要性进行解释与说明，但同时应当对这类解释与说明进行严格监管，预防信息处理者过度收集与处理不必要的敏感个人信息。在这一过程中，法律应当重点监管收集与处理对产品或服务不具有改善作用的敏感个人信息。

其次，在告知同意流于形式的背景下，机械性解释告知同意将无助于法律真正保护敏感个人信息，[60] 反而给用户体验带来更多的干扰 [61]。为了真正发挥告知同意的作用，一方面，信息处理者应当在符合业务场景与遵循行业惯例的情形下对告知同意进行一定程度的优化设计，避免过多弹窗、同意选项对个体造成的侵扰；另一方面，法律应当对信息处理者的告知进行重点监管，对处理敏感个人信息所带来的风险，法律应要求信息处理者在其隐私政策中进行重点说明与详细披露，以便为信息处理者内部组织、执法机关、社会组织与个人提供信息索引。[62] 告知同意虽然无法在交互场景下让个体充分知情，但对于信息处理者内部组织、执法机关、社会组织与非交互场景下个人，却可以成为他们的个人信息说明书，有利于敏感个人信息保护从高度依赖个体本位保护走向社会保护与合作治理。[63] 因此，敏感个人信息告知同意制度的设计虽然可以适度放松，但应当充分履行处理敏感个人信息的特殊告知与说明义务。

最后，就安全保护措施而言，以形式合规要求信息处理者采取相关措施，信息处理者可能也会采取形式主义的对策，即在形式上采取相关措施，但实质上却未必真正合理保护敏感个人信息。为了避免安全保护措施走向形式主义，法律应当允许信息处理者采取符合具体场景与现实风险的保护措施，同时对此类自我监管措施进行监管。目前，《个人信息保护法》在安全保护措施方面设置了事前个人信息影响评估，事中加密、去标识化、专人保护，事后实施应急预案等措施。敏感个人信息保护除了按照法律规定应当进

---

[59] *See* Winston J. Maxwell, *Principles-Based Regulation of Personal Data: The Case of 'Fair processing'*, International Data Privacy Law, Vol.5:205, p.205-216 (2015).

[60] 参见冉克平：《论〈民法典〉视野下个人隐私信息的保护与利用》，载《社会科学辑刊》2021 年第 5 期，第 103-111 页。

[61] 参见杨惟钦：《敏感个人信息告知同意规则的制度逻辑、规范解释与补强》，载《财经法学》2024 年第 1 期，第 100-115 页。

[62] *See* Peter Swire, *The Surprising Virtues of the New Financial Privacy Law*, Minnesota Law Review, Vol.86:1263, p.1263-1324 (2002).

[63] 参见余成峰：《数字时代隐私权的社会理论重构》，载《中国法学》2023 年第 2 期，第 169-188 页。

行事前个人信息影响评估，加密、去标识化等保护方式也应当被重点监管，以降低敏感个人信息的泄露风险与侵害风险。

（三）私密信息与敏感个人信息保护衔接的重构

对于私密信息与敏感个人信息保护的衔接，应首先认识到私密信息与敏感个人信息是隐私权保护与个人信息保护两种制度下的概念，应在两种制度框架中分析二者的区别与关系。就隐私权保护与个人信息保护而言，二者的核心区别是隐私权保护属于传统人格权保护的范畴，[64]其保护以侵权法为依托，将侵权方与被侵权方拟制为一对一的平等主体。而个人信息保护则是一种公私法混合的制度，其针对的是信息处理关系。[65]波斯特将这两种制度区分为尊严隐私与数据隐私。[66]个人信息保护制度之所以产生，是传统的隐私权保护无法应对具有“大规模微型侵权”特征的信息处理关系。在处理关系中，个人很难对较为隐蔽和专业化的个人信息处理进行预防与救济。为了解决隐私权保护的不足，在个人信息保护框架中，法律除了仍然对个体进行赋权之外，同时引入了国家保护义务与监管责任，[67]以此弥补个体救济能力与动力的不足。

从隐私权保护与个人信息保护的关系出发，就能理解私密信息应基于侵权法在司法个案中判断，其范围无需也难以进行事前界定。《民法典》第 1032 条第 2 款规定，“隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息”；第 1034 条第 3 款规定，“个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定”。《民法典》在引入私密信息概念的同时，并未对这一概念进行界定。不过从私密个人信息所依赖的侵权法特征来看，这种立法留白反而更为合理。因为相比敏感个人信息，私密个人信息的判断更具有主观性，更可能因为人际关系等场景的变化而变化，也更可能因为具体人际关系和信息获取规范的变化而变化。[68]例如，家庭住址信息是否为私密信息，如果涉及私密信息侵权的原告和被告为朋友关系，则人们可能认为此时的家庭住址信息不是私密信息；但如果原告和被告是陌生人关系，则人们可能认为此时的家庭住址信息属于私密信息。相对而言，敏感个人信息虽然也具有不确定性，但此类不确定性相对较弱。特别是在具体行业与细分领域，对敏感个人信息的范围以及如何处理此类信息有一定的共识。对私密信息则很难进行此类行业性与领域性界定，因为私密信息的概念是隐私侵权的下位概念，一旦个案中的隐私侵权成立，则该案中涉及的个人信息在这一个案中就成为私密信息。反之，当个案中的隐私侵权不成立，则该案中涉及的个人信息就不应当被认定为私密信息。

私密信息保护与敏感个人信息保护两种制度也可以更好衔接。对于不存在信息处

---

[64] 参见彭诚信：《论个人信息权与传统人格权的实质性区分》，载《法学家》2023 年第 4 期，第 146-159 页。

[65] 参见周汉华：《个人信息保护的法律定位》，载《法商研究》2020 年第 3 期，第 44-56 页。

[66] *See* Robert C. Post, *Data Privacy and Dignitary Privacy: Google Spain, The Right to Be Forgotten, and the Construction of the Public Sphere*, Duke Law Journal, Vol.67:981, p.981-1072 (2018).

[67] 参见王锡锌：《个人信息国家保护义务及展开》，载《中国法学》2021 年第 1 期，第 145-166 页。

[68] *See* Robert C. Post, *The Social Foundations of Privacy: Community and the Self in the Common Law Tort*, California Law Review, Vol.77:957, p.957-1010 (1989).

理关系的情形，应在具体司法个案中确定私密信息的范围，因为这类情形主要依赖于侵权法保护，并不涉及一般行政监管。较为复杂的是存在信息处理关系，[69] 而又同时提起隐私权之诉与个人信息之诉，此时就可能同时涉及私密信息保护与敏感个人信息保护两种制度的衔接。例如，在“朱某诉百度公司隐私权纠纷案”中，朱某在某互联网企业搜索“减肥”“丰胸”等关键词后，会在浏览相应的网页时出现诸如“减肥”“丰胸”“人工流产”等广告。[70] 在此类案件中，如何界定私密信息与敏感个人信息？在笔者看来，此类情形的基本原理仍然未变，仍然应按照隐私权保护与个人信息保护的不同制度框架来判断。就私密信息而言，其分析关键是此类信息处理在特定场景与关系中是否违背个体的合理隐私期待；就敏感个人信息而言，其分析关键则是此类个人信息处理是否违背了互联网广告行业对于敏感个人信息的界定，以及结合个人信息主体的身份、识别主体、处理方式等因素，分析此类情形的处理是否给个人带来较高风险。[71] 总而言之，只要从隐私权保护与个人信息保护两种制度框架出发，私密信息与敏感个人信息保护的关系就可以迎刃而解。

六、结　语

作为个人信息分类分级保护的制度工具，敏感个人信息的统一界定与特殊保护在立法层面已经成为我国和大多域外国家和地区的共识。但在界定上，敏感与非敏感个人信息的边界日趋模糊。在保护方式问题上，敏感与非敏感个人信息的二元保护框架、敏感个人信息保护的强化保护、敏感个人信息与隐私权和私密信息的交叉性也面临众多挑战。对这些问题与挑战进行分析，可以发现其根源在于个人信息保护的目标与特征。个人信息保护的目标在于通过个人信息保护具体场景中的相关权益与预防相关风险，而非保护个人信息本身。因此，个人信息的敏感性必然具有场景化特征，不可能一成不变或通过其本身去判断。

在各国立法或实证法对敏感个人信息统一界定与特殊保护具有高度共识的背景下，修改现行立法并不现实。较为现实与可行的方法是通过法律解释对敏感个人信息保护进行重构，使得这一制度更加合理。具体而言，对敏感个人信息相关法律法规的解释应采取目的解释的方法，同时参照文义解释；对敏感个人信息的价值判断应以我国民众的价值判断为最终依据，对敏感个人信息的风险认知应当以中立性专家为主、兼顾民众感知风险，对敏感个人信息的判断因素应当考虑个人信息主体、信息处理主体、处理方式、识别概率等因素。在法律解释与法律适用过程中，应当放弃绝对化的敏感与非敏感个人信息二元保护，转而采取动态化、场景化的分类保护。在涉及行政监管的法律解释中，应

---

[69] 参见程啸：《论我国个人信息保护法中的个人信息处理规则》，载《清华法学》2021 年第 3 期，第 55-73 页。

[70] 这一案件发生在《民法典》和《个人信息保护法》生效之前，但作为研究对象仍然具有典型意义。参见江苏省南京市鼓楼区人民法院（2013）鼓民初 3031 号民事判决书；江苏省南京市中级人民法院（2014）宁民终 5028 号民事判决书。

[71] 参见郭传凯：《敏感个人信息处理规则的反思与修正》，载《政法论坛》2024 年第 3 期，第 102-113 页。

当采取自下而上的分类保护；在涉及司法与行政裁判的法律解释中，应当采取案例式的分类保护。就涉及强化保护措施的法律解释而言，对敏感个人信息进行执法应当采取自我规制下的强制性规制。就私密信息与敏感个人信息的关系而言，应分别在隐私权保护与个人信息保护的制度框架下进行判断。综合而言，敏感个人信息保护制度虽然面临挑战，但通过对其进行解释性重构，这一制度仍然可以保持生机与活力。

Abstract: Most laws in China and abroad classify sensitive personal information by type or define it as having a serious risk of infringement. In terms of the protection method, these laws adopt sensitive and non-sensitive distinctions and provide enhanced protection for the former. However, there are challenges to understanding and applying sensitive personal information protection. Its definition is indeterminate and its dual protection method is insufficiently rational. The root of this challenge lies in the contextualized nature of sensitive personal information; personal information is not sensitive *per se*. It is not necessary or realistic to reconstruct sensitive personal information protection at the legislative level. Therefore, it should be restructured in the process of interpretation and application. Specifically, the definition of the concept should be mainly based on purpose interpretation with a reference to textual interpretation; its value judgment should be based on national conditions; its risk analysis should be mainly based on expert judgment, taking into account public perception of risk, and judgment factors should consider the information subject, processing subject, processing method, identification probability, etc. The classification and protection of sensitive and non-sensitive personal information should adopt contextual and dynamic approaches. With regard to administrative regulation, we should adopt a bottom-up contextual approach; with regard to judicial and administrative law enforcement cases, a case-based contextual interpretation of sensitive information should be adopted. To strengthen protective measures, a regulated self-regulation approach should be adopted. The connection between sensitive personal information and private information should be analyzed under two institutional modules: personal information protection and privacy protection.

（责任编辑：赵毅宇）