主题研讨

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

王　苑

内容提要:《个人信息保护法》采取“概括+列举”模式规定敏感个人信息,这一规定可能带来多方面的不确定性:一是法律评价标准存在模糊性;二是技术驱动的新型敏感个人信息可能未被容纳;三是判断标准的多维性引发归入和择出难题。欧盟立法谨慎选择了“特殊类型个人数据”这一术语,其原则上禁止处理此类数据,但在特定场景下例外允许处理。我国敏感个人信息的规定缺乏特定的归入和择出标准,通过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,既有助于监管机构合理确定敏感个人信息的具体标准,同时也有助于司法实践科学合理地裁判侵害个人信息权益纠纷。

关键词:《个人信息保护法》　敏感个人信息　个人信息处理　场景要素

王苑,清华大学法学院助理研究员。

环球法律评论 GLOBAL LAW REVIEW

欧盟《一般数据保护条例》(*General Data Protection Regulation*)生效后,风险进路(risk-based approach)成为个人信息保护立法的重要趋势,风险控制的准确性要求对个人信息进行分类分层保护。〔1〕我国《个人信息保护法》也一定程度上借鉴了该保护模式,围绕敏感个人信息与一般个人信息的处理规则展开,设专节对处理敏感个人信息作出更为严格的限制。只有在具有特定目的和充分必要性的情形下,个人信息处理者方可处理敏感个人信息,并且应当取得个人的单独同意或者书面同意。〔2〕《个人信息保护法》第28条第1款对敏感个人信息作出一个较为宽泛的定义,即“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”,同时亦列举了

〔1〕 See Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 *Seton Hall Law Review* 995, 1012 (2016).

〔2〕 参见《关于〈中华人民共和国个人信息保护法(草案)〉的说明》,2020年10月13日第十三届全国人民代表大会常务委员会第二十二次会议。

七类具有“典型性”的敏感个人信息。该条虽然明确将“敏感性”作为敏感个人信息的核心特征,但却先验设定了个人信息之敏感与非敏感的“二分模式”,从而可能意味着落入敏感范畴的个人信息需加强保护,而敏感范畴以外的信息则无加强保护之必要或者保护密度很低。然而,对于敏感个人信息这一指向特定的规范性社会评价的概念,敏感与非敏感之间的界限是否清晰?所列举的敏感个人信息类型是否周延?敏感个人信息归入与择出的标准又将如何设定?上述问题殊值探讨。

一 敏感个人信息概念的检讨与反思

“法律概念是法律规范和法律制度的建筑材料。”〔3〕只有概念明晰,后续制度建构才能科学合理。若概念本身存在歧义,那么立基于其上的规范和制度构建的合理性就会受到质疑。敏感个人信息已成为我国实定法上的概念,其关系到个体的人格尊严,法律确有对其进行规制的必要。但“敏感”一词本身就带有极大范围的评价空间,所列举的类型也可能随着技术的突破而不断发展。这些都可能给敏感个人信息这一概念带来诸多不确定性,继而影响敏感个人信息处理规则的落实。因此,有必要从根源上对敏感个人信息概念进行检讨与反思,以明确实定法下判断敏感个人信息的标准是否可以解决既有难题以及如何应对未来实施难题。

(一)法律评价标准的模糊性

何为敏感?从个体角度出发,主观说认为“敏感”一词常被用以描述个体心理特征,带有强烈的主观色彩,具有很强的个体差异性。〔4〕客观说则认为敏感是社会多数人的共同心理,在很大程度上也与一国的政治、经济、文化等社会状况息息相关。〔5〕敏感个人信息本身在中国法体系内也并非新鲜事物,此前在国家推荐性标准《信息安全技术 个人信息安全规范》(GB/T 35273 - 2020)、相关司法解释中都有所提及。从《个人信息保护法》第 28 条第 1 款规定的表述可看出,立法采用了客观说,此处“敏感”即“造成侵害或危害结果上的容易性”。〔6〕然而,这一判定标准极不清晰。作为规范性概念,“敏感”本身应界定概念内涵,作出一定社会评价,但由于这一语词本身规范价值导向性不够明确,因而具有价值填补的必要。同时,该款中规定的“容易导致”一词本身就是一个含义不确定的表述,存在较大的语义空间,需要大量的实证资料来支撑;另外,“敏感个人信息”与“人格尊严受到侵害”或者“人身、财产安全受到危害”到底存在何种联系,后者范围如何,都需要进一步解释。上述概念的模糊性会带来一些问题。比如,个人信息处理者依据《个人信息保护法》第 28 条第 1 款并不容易准确判断出某一个人信息是否属于法律上的敏感个人信息,这就可能导致个人信息权益无法得到保障,同时也可能出现处理者义务泛化的问

〔3〕 [德]伯恩·魏德士著:《法理学》,丁晓春、吴越译,法律出版社 2013 年版,第 91 页。

〔4〕 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》,《比较法研究》2021 年第 5 期,第 35 页。

〔5〕 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 85 页。

〔6〕 参见程啸著:《个人信息保护法理解与适用》,中国法制出版社 2021 年版,第 259 页。

题,其可能为避免行政处罚等法律责任,而将所有的个人信息都视为敏感个人信息。再如,此种模糊性也可能会给数据治理带来困难。履行个人信息保护职责的部门在针对敏感个人信息的行政执法活动中,可能出现参考标准不明、惩处缺乏梯度甚至违反比例原则等问题。同时也影响国家网信部门针对“处理敏感个人信息”等新技术新应用制定专门的个人信息保护规则、标准。

另外,在司法实践中,概念模糊会导致法律适用较为困难,尤其是法官在认定是否构成侵犯个人信息罪的刑事案件上。具体来说,按照《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第5条规定的“非法获取、出售或者提供公民个人信息”的量级,有学者将个人信息分为“敏感信息”“重要信息”与“一般信息”三类,但这三类信息边界模糊,均存在交叉、重合的问题。比如财产信息和交易信息难以辨明,住址信息与住宿信息纠缠不清,行踪轨迹信息和手机位置信息高度重合,〔7〕这些都可能导致裁判的随意性。即便是在民事侵权纠纷案件中,法院在认定是否构成侵害个人信息权益时,是否属于敏感个人信息对于处理者的相应责任的认定也至关重要。

(二)技术驱动的新型敏感个人信息未被容纳

《个人信息保护法》第28条第1款列举了七类典型的敏感个人信息,即“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“不满十四周岁的未成年人的个人信息”。敏感个人信息的判定标准为“造成侵害或危害结果上的容易性”,由于信息本身就具有开放性,因而随着社会的进步发展,除了明确列举的七类敏感个人信息外,“容易造成侵害或危害”的敏感个人信息的类型具有进一步丰富的可能。

一方面,新的数据收集技术会产生新的信息类型。相较于法定的“敏感个人信息”而言,这些新的类型会模糊“敏感”与“非敏感”之间的界限。例如因网络活动而产生的行为数据、从社交网站上搜集到的数据、手机产生的位置数据以及其他“监视”用户行为及活动的智能设备所产生的数据,包括未来因人工智能的发展产生的可以关联到个人的数据,〔8〕其是否容易造成侵害或者危害,需要立法者不断重新评估和扩大敏感个人信息的种类,以协调恰当保护这些信息的机制。

另一方面,数据分析技术的发展可能令任何类型的信息都带有敏感性。任何信息在新的分析技术下都可能联系到特定的个人并产生一定的危险性,亦会模糊敏感信息与非敏感信息之间的界限。在很多情形下,并非收集的信息本身都是敏感的,而是对这些信息进行的分析可能产生一些令人担忧的境况。〔9〕许多数据库虽然会将数据对应的个人身份信息去除以达到匿名化和去识别化,但这些数据库若与其他数据库重新组合(比如撞库),也可能再次识别、关联到具体个人。甚至“任何使一个人区别于其他人的信息都可

〔7〕 参见周光权:《侵犯公民个人信息罪的行为对象》,《清华法学》2021年第3期,第35页。

〔8〕 See Müge Fazlioglu, Beyond the “Nature” of Data: Obstacles to Protecting Sensitive Information in the European Union and the United States, 46 *Fordham Urbar Law Journal* 271, 289 (2019).

〔9〕 Article 29 Data Protection Working Party, Opinion 03/2013 on Purpose Limitation, at 47, 00569/13/EN, WP203 (Apr. 2, 2013), https://ec. europa. eu/justice/article - 29/documentation/opinion - recommendation/files/2013/wp203_en. pdf,最近访问时间[2021 - 09 - 12]。

以被用来重新识别那些匿名数据”。[10] 公开的数据库中的非敏感个人信息也可能会让个人受到威胁,甚至带来人身、财产安全上的危害。[11]

总之,无论是因新的收集技术而产生的新型敏感个人信息,还是因数据分析技术提升而导致现有的非敏感个人信息的敏感化,均可能给信息主体的人格尊严以及人身、财产安全等带来重大伤害。因此,“敏感个人信息”的种类是无穷无尽的,关键是以何种标准判断敏感个人信息的归入和择出。

(三)判断标准的多维性引发归入和择出难题

敏感个人信息是不断发展的,归入或择出的判断标准亟需要件化。目前关于《个人信息保护法》所列七类敏感个人信息的考量因素的资料并不充分,[12] 因此,只能试图提取其中的公因式来确定敏感个人信息的判断标准。立法机关有关人士曾指出,敏感个人信息的特殊规定,“主要是考虑到此类信息一旦泄露或者被非法使用,极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,因此,对处理敏感个人信息的活动应当作出更加严格的限制”。[13] 也就是说,敏感个人信息是性质上可能给信息主体带来重大风险的信息,这与欧盟《一般数据保护条例》中依据数据类型可能遭遇的风险高低对个人信息进行分类保护的立法思路是一致的。本质上,敏感个人信息是为了预防个人信息泄露或非法使用给信息主体带来的风险,因此其具有“高风险性”。这种“高风险性”特征同样体现在美国的立法中,除了符合美国民众共同认知的教育信息、医疗信息、金融信息有专门的立法外,美国还因为一些特殊事件的发生而通过立法对特定类型的个人信息予以保护。比如,某位法官的录像带租赁信息被记者获取并披露这一社会事件,促成了美国制定《视频隐私保护法》(*Video Privacy Protection Act of 1988*, *VPPA*);而《驾驶员隐私保护法》(*Drivers Privacy Protection Act of 1994*, *DPPA*)的制定,也是受一些社会事件影响,较为著名的事件是某位知名女演员的粉丝获知女演员驾驶证上的家庭地址后对其跟踪并将其杀害。[14] 可见,对于“敏感信息”的认识,也是随着社会实践的发展甚至社会事件的触动,而不断有所意识的,并转化为相应法律规制。

另外,敏感信息和非敏感信息往往会在许多情形下相互转化。一方面,处理个人信息的目的与信息的敏感性密切相关。如果获取车辆信息的目的是为了确定其行踪轨迹,相较于获取该信息是为了推销保险,二者目的不同,信息主体对是否敏感的感受也存在明显不同。因此,单就车辆信息本身,很难评判到底其是属于敏感信息还是一般信息。[15] 另一方面,信息处理的场景也会影响敏感性的判断。比如,同一信息在不同的场景下,也

〔10〕 See Arvind Narayanan & Vitaly Shmatikov, Myths and Fallacies of “Personally Identifiable Information”, 53 *Communications of the ACM* 24, 26 (2010).

〔11〕 See Kirsten Martin and Helen Nissenbaum, Privacy Interests In Public Records: An Empirical Investigation, 31 *Harvard Journal of Law & Technology* 111, 111 - 143 (2016).

〔12〕 法工委的个人信息保护法释义书中,并未言明为何将这七类归入了敏感个人信息的理由。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。

〔13〕 参见《8 章 74 条,个人信息保护法来了! 全国人大常委会法工委经济法室副主任杨合庆权威解读十大亮点》,https://mp.weixin.qq.com/s/Y-031EBzOsbbN2JAEcOGBQ,最近访问时间[2021-09-11]。

〔14〕 See Paul Ohm, Sensitive Information, 88 *Southern California Law Review* 1125, 1141 (2015).

〔15〕 参见周光权:《侵犯公民个人信息罪的行为对象》,《清华法学》2021 年第 3 期,第 35 页。

可能落入不同的分类之中。以医疗健康信息为例,医生为诊断病情组织专家会诊,在会诊中该信息就不具有敏感性,但如果医生在办公室聊天披露病患的医疗健康信息,则这样的信息就具有敏感性。另外,有些个人信息单独看是不敏感的,但是一旦结合其他信息就具有了身份识别性,从而导致"敏感"。[16] 姓名、性别、工作单位等信息单独看来,很难被视为"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",因为它们都是人们社会交往活动最重要的媒介信息。然而,姓名、性别、工作单位等信息如果被不法分子获知,对于信息主体来讲可能就非常敏感。

综上,从单一维度(信息性质维度)判断敏感性,无疑是将个人信息视为一个静态客体。而现实生活中,个人信息不同于有体物,在场景中动态流动更能彰显其独特的价值。个人信息的敏感度是动态的,也应是多维度的,敏感个人信息的归入和择出均需要处理场景及处理目的等标准的引入。

二 比较法视角下敏感个人信息的转进

由于敏感个人信息的评价存在模糊性、概念边界不清,新类型的敏感个人信息又可能层出不穷,因此归入和择出的标准也存在争议。虽然英国、俄罗斯、巴西、日本、韩国等国在立法上确立了敏感个人信息制度,但是欧盟《一般数据保护条例》中却回避了敏感个人信息的概念,仅使用特殊类型数据这一法律术语。[17] 而美国直到现在也并未在联邦层面的法律中规定敏感个人信息。[18] 欧盟和美国立法均回避了敏感个人信息的提法,个中缘由值得深思。以下拟从比较法的角度,就敏感个人信息制度的发展进行一定梳理。

(一)一度为域外立法所否定的敏感个人信息概念

在欧盟数据保护的立法进程中,对于是否规定敏感个人数据存在长时间的徘徊和犹疑。"敏感数据"的概念最早出现在1980年经合组织(OECD)《个人信息隐私和跨境流通指南(草案)》(*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*)中,起草者试图给其下定义,但是最终版的指南中并未规定对其的特别保护,理由是"似乎对于何谓敏感的数据无法达成共识"。[19] 1981年《个人数据自动处理中的个人保护公约》(*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*)认为"敏感度"是进一步规范个人数据的使用中的关键因素。[20] 但在公约中也并未

〔16〕 参见高富平:《个人信息流通利用的制度基础——以信息识别性为视角》,《环球法律评论》2022年第1期,第84页。

〔17〕 欧盟《一般数据保护条例》第9条第1款规定,"禁止在个人数据处理中泄露种族或民族起源、政治观点、宗教信仰、哲学信仰、工会成员资格等个人信息,禁止以识别自然人身份为目的对个人基因数据、生物特征数据的处理,禁止对健康数据、性生活、性取向等相关数据进行处理。"

〔18〕 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85页。

〔19〕 Organization for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm,最近访问时间[2021-09-11]。

〔20〕 See Spiros Simitis, Revisiting Sensitive Data (1999), Review of the Answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108) (Strasbourg, 24-26 November 1999), http://rm.coe.int/09000016806845af, 最近访问时间[2021-11-20]。

采用敏感的概念。1995 年欧盟《关于涉及个人数据处理的个人保护以及此类数据自由流通的第95/46/EC 号指令》(*Directive 95/46/EC*,下称"《指令》")对信息的特殊种类进行了列举,依然并未使用"敏感个人数据"的概念;[21] 直到 2012 年通过的《个人数据处理中的个人保护公约》(*Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*),才在第 6 条中明确了"敏感数据"的说法,[22] 欧盟《一般数据保护条例》第 9 条沿袭了《指令》对特殊类型数据的规定。因此,在欧盟立法中,敏感数据直到2012 年才在正式的法律文件中出现,其他时候要么仅在立法说明中被提及,要么完全未被涉及。笔者以为,这表明立法者认为敏感个人数据并非是一个严谨的法律术语,或者至少是一个在文义上存在歧义、无法达成共识的术语,因此更大程度上是将其作为一个学理上的概念而讨论。同样,在美国联邦的立法中,虽然也有一些针对特定类型的个人信息保护的立法,但却从未将敏感个人信息作为一个法律概念确立下来。[23]

在《个人信息保护法》颁布之前,我国法律中也从未规定敏感个人信息的概念。2012 年《全国人民代表大会常务委员会关于加强网络信息保护的决定》中只是将个人信息区分为"身份信息"和"隐私信息",2020 年颁布的《民法典》第1033 条第 5 项以私密性界分个人信息,但是,私密信息和敏感个人信息概念的内涵和外延显然并不相同。[24] 因此,从法律层面而言,"敏感个人信息"一词乃是《个人信息保护法》首次使用的;当然,除了法律之外,我国一些规范性文件和标准中对于对敏感信息已有一些规定,并且存在某种延续性。比如《信息安全技术 个人信息安全规范》(GB/T 35273 - 2020)将个人敏感信息定义为"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"。而《个人信息保护法》与此一脉相承,可以说,在标准等层面对于敏感个人信息早已接受,并逐渐在法律中确定相关规则。

(二)立法价值的取舍——原则禁止抑或一般允许?

我国《个人信息保护法》在一定程度上借鉴了域外立法的相关规定,[25] 尤其在许多制度的架构上很明显参考了欧盟《一般数据保护条例》的设置。该条例第 9 条规定了"特殊类型的个人数据",对个人数据按照类型分类并据此对数据处理者施加不同的处理义务,尤其是要求进行数据保护风险评估,这与风险立法进路是相称的。[26]

欧盟《一般数据保护条例》对特殊类型个人数据采取了原则上禁止处理、例外允许处

---

〔21〕《个人数据自动处理中的个人保护公约》第 6 条、《关于涉及个人数据处理的个人保护以及此类数据自由流通的第 95/46/EC 号指令》第 8 条。

〔22〕Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (CETS No. 108, Strasbourg, 28/01/1981), http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108,最近访问时间[2021-09-12]。

〔23〕See Paul Ohm, Sensitive information, 88 *Southern California Law Review* 1125, 1141-1145 (2015).

〔24〕参见程啸:《个人信息保护中的敏感信息与私密信息》,《人民法院报》2020 年 11 月 19 日第 005 版;石佳友:《个人信息保护的私法维度——兼论〈民法典〉与〈个人信息保护法〉的关系》,《比较法研究》2021 年第 5 期,第 26 页。

〔25〕"从上世纪 70 年代开始,经济合作与发展组织、亚太经济合作组织和欧盟等先后出台了个人信息保护相关准则、指导原则和法规,草案充分借鉴了有关国际组织和国家、地区的有益做法。"参见《关于〈中华人民共和国个人信息保护法(草案)〉的说明》(2020 年 10 月 13 日)。

〔26〕参见丁晓东著:《个人信息保护:原理与实践》,法律出版社 2021 年版,第 68 页。

理的模式,有学者认为该条的规范意旨即为禁令。[27] 欧洲之所以采取禁令模式,与其历史文化有莫大关联。盖因20世纪时,欧洲曾经历过滥用"敏感"个人信息侵害人权的惨痛事件,[28]在反思过往之余,欧洲立法认为个人种族信息可能具有高度敏感性,带来极大的风险。但同时,立法者也意识到,特殊类型的个人数据又具有极高的利用价值和公共价值。因此,该条例对法定列举的几类信息也并非绝对禁止处理,而是通过例外允许处理的情况规定对主体权利的克减。此类权利克减往往是为了维护更高的价值,比如出于健康目的,包括公共健康和医疗服务管理等等,或出于公共利益的存档目的、科学或历史研究目的以及统计目的等等。同时还允许在必要时处理此类个人数据,比如在诉讼中或者庭外的其他法定程序中。可见,相较于一般允许的立法模式而言,禁令模式更侧重于对克减情形的精确列举。

我国法实际上并未明确禁止对敏感个人信息的处理,只是在处理此类信息时有更为严格的要求。究竟是采原则禁止还是一般允许(法无禁止即自由),实则体现的是立法价值的取舍。比如,在欧盟视为"敏感"的种族信息在我国似乎并不具备通识意义上的敏感性。也正是因为欧盟将个人数据权益视为一项人权,因此只要可能对人权有更高风险性的行为(如处理敏感个人信息),就应当明确禁止。我国虽然原则上允许处理敏感个人信息,但是在《个人信息保护法》第28条第2款中,又限制了处理的条件,规定在"具有特定目的和充分必要"以及"采取严格保护措施"的前提下,才可以对敏感个人信息进行处理。事实上,《突发公共卫生事件与传染病疫情监测信息报告管理办法》第8条第2款中规定,各级疾病预防控制机构负责开展现场流行病学调查与处理,搜索密切接触者、追踪传染源。故而,即便是《个人信息保护法》第28条第1款明确列举的绝对敏感的医疗健康信息,在上述所列法定情形下也会让渡于公共利益。这与欧盟《一般数据保护条例》中"禁令+例外"的立法模式有异曲同工之处。综上,欧盟禁令式立法与我国一般允许处理的立法模式之间,在实际维护人格尊严和人身财产安全的法律效果上,差异不大。

(三)欧盟特殊类型个人数据vs中国法的敏感个人信息

既然禁令式和一般允许的立法模式在价值追求上并无显著差异,那么欧盟《个人信息保护法》中的特殊类型个人数据是否就可以等同于我国的敏感个人信息呢?无论是在欧盟《一般数据保护条例》的立法说明中,[29]还是在相关评注中,[30]"特殊类型个人数据"都被概称为"敏感数据",概念的相似性可能导致了比较法研究上的误读误判。[31] 首先,欧盟《一般数据保护条例》正式法律文本中从未使用"敏感数据"这一定义,相反,其仅在立法说明中用敏感数据指代,立法说明并非正式的法律条文,其效力仅限于对正式法律

〔27〕 See Christopher Kuner, Lee A. Bygrave & Christopher Docksey ed., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, p. 365.

〔28〕 William Siltzer & Margo Anderson, The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses, 68 *Social Research* 481, 483-485 (2001).

〔29〕 GDPR, Recital 10, Recital 51.

〔30〕 See Christopher Kuner, Lee A. Bygrave & Christopher Docksey ed., *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, p. 369.

〔31〕 参见张新宝:《我国个人信息保护法立法主要矛盾研讨》,《吉林大学社会科学学报》2018年第5期,第50页。

条文的合目的性解释等方面,[32]即主要起到的是立法释义的作用和功能。在正式的法律条文中未采用敏感数据概念,实际上清晰地表明了欧盟立法者认为二者的内涵和外延是不同的。笔者以为,在立法上采用“特殊类型”而非“敏感”的缘由在于前者带有客观评价色彩,而后者更大程度上具有主观性。换言之,如果使用敏感一词,势必有民众质疑,自己主观上认为敏感的某类个人信息为何无法得到强化保护。而“特殊类型”这样的表述则不容易引起太多歧义。比如多数人会将银行账号、收入以及证件号等数据视为敏感信息,但这些数据却并不属于欧盟《一般数据保护条例》第 9 条规定的特殊类型个人数据。[33]

进一步说,欧盟《一般数据保护条例》对特殊类型个人数据并未规定概括条款,而是直接针对几类特殊类型的个人数据进行类型化列举,比如,种族或民族起源、政治观点、宗教信仰、哲学信仰、工会成员资格等个人信息——禁止泄露;个人基因数据、生物特征数据——禁止以识别自然人身份为目的;健康数据、性生活、性取向等相关数据——禁止处理。从立法技术来看,类型化列举模式事实上反对法官对特殊类型个人数据种类进行恣意扩大。立法上采取如此审慎的态度,也是因为对需要特殊评价的个人数据如果规定得过于宽泛,可能会导致个人信息处理者在信息处理过程中“畏首畏尾”,引发“寒蝉效应”,进而影响数据的利用和流通。这种不设立概括条款,单就已有一定共识的敏感个人信息单独保护的方式,在美国联邦层面的许多特殊类型个人数据保护如针对儿童的《儿童在线隐私保护法》(*Children's Online Privacy Protection Act of* 1998, *COPPA*)、针对基因医疗数据的《基因信息反歧视法》(*Genetic Information Nondiscrimination Act of* 2008, *GINA*),以及州层面的隐私保护法如加州《隐私保护法》(*California Privacy Rights Act of* 2020, *CPRA*)中都有所体现。反观我国法可知,对敏感个人信息设置概括条款,首先意味着可以根据概括条款解释出很多概念内的类型;其次非穷尽式列举更是存在无限列举的可能性。因此,纯粹从立法技术导致的结果来看,欧美立法的外延相对清晰固定,而我国立法则需进一步解释。

综上,欧盟《一般数据保护条例》中对特殊类型个人数据的保护规范与我国《个人信息保护法》中敏感个人信息的保护规定,都遵循了风险立法的进路,以预防个人信息被泄露和滥用所导致的风险为出发点,从制度意义及制度框架上实际起到了类似的规范效果。但是,二者却存在较为明显的差异:从立法技术上,前者采禁令模式,后者为一般允许;从内涵外延的确定性上,前者是客观表达,后者较为主观,易造成理解上的歧义;在规范的明确指引性上,前者规定了类型化的处理场景,后者则没有。因此,二者不能等量齐观。实际上,无论是采取欧盟式的类型化列举模式,还是采用美国的单行法规范的模式,都是为了提供一种法律上的确定性。而我国目前敏感个人信息的概念则显然过于模糊宽泛,确定性欠奉。

三 敏感个人信息的归入与择出构造

概括条款立法模式的优势在于,其可以妥善解决法律发展中新情况对体系的挑战,但

〔32〕 参见[奥]恩斯特·A. 克莱默著:《法律方法论》,周万里译,法律出版社 2019 年版,第 120 页。

〔33〕 Edited by Maciej Gawronski, *Guide to the GDPR*, Wolters Kluwer, 2019, p. 58.

环球法律评论 GLOBAL LAW REVIEW

弊端则在于导致相关概念可能欠缺确定性，无论是个人信息处理者还是执法、司法部门都需要对个人信息进行敏感与否的再识别，这极易造成法律适用上的混乱，因此需要就概念进行解释和规则构造。此外，为避免执法和裁判中的恣意，维护法的安定性，也有必要对敏感个人信息的一般定义进行解释论构造，以期为实践的归入择出提供一定标准，而场景化的二阶考量是解决这一问题的理论方向。

（一）归入与择出的标准：场景要素的考量

目前我国敏感个人信息的解释可能存在两种不同的结果走向：一是在法条中明确列举的几类个人信息被僵化对待、导致过度保护；[34] 二是未纳入法条规范列举的信息无法归入而得不到相应保护。如新闻杂志订阅信息一般不认为是敏感个人信息，但是某些小众化的偏好也可能被认为是敏感的。这两种弊端都背离了敏感个人信息制度的初衷。因此，引入更具解释力的理论，十分必要。

1. 场景理论的引入

场景会影响信息的性质，某类信息可能在某些场景下是敏感的，换个场景即不再如此。对于尼森鲍姆教授（Helen Nisenbaum）的隐私场景理论这一经典隐私理论，目前学界已展开了广泛的介绍和研究。有学者提出，所谓“场景”就是“具体情形具体分析”，[35] 从某个层面来看确实如此，场景的完整考量必然涉及到对具体情形的考量，但实际上场景还并不完全是情形，因为可能会将主体、客体、行为规范都纳入场景考量之中。

也有学者明确提出场景理论就是隐私保护领域的“动态系统论”，二者本质都源于对相互冲突的利益的权衡。[36] 在衡量侵害隐私与个人信息侵权的责任成立和责任承担上，隐私领域的“动态系统论”的观点是站得住脚的。但是，场景要件并非仅限于侵权责任成立和责任承担的作用，其还可用于指导规范的制定。此外，在判断个人信息敏感度的多因素考量方面，场景理论也能提供一种思考的角度，即对于敏感个人信息的判断需要精细化的各种要素的考量。

2. 影响敏感性的场景要素

信息本身不会直接带来损害，会带来损害的是信息所处的场景，完整的场景很容易识别信息主体，继而对个人信息权益造成威胁，因此必须对信息流通时的整体场景进行评估。我国既有研究对敏感性必须结合“场景要素”进行综合判定已形成基本共识，[37] 但不足之处在于，对场景化具体需要考量的要素为何，以及这些要素如何适用于敏感个人信息的判断的讨论基本上还停留于表面。

---

〔34〕 比如医院如果未经患者单独同意将患者的医疗健康信息（无法识别到特定个人）作为攻克疑难杂症案例的研究数据，若根据敏感个人信息的规定，这种行为就违反了信息处理者的义务。

〔35〕 参见胡凌：《功能视角下个人信息的公共性及其实现》，《法制与社会发展》2021 年第 5 期，第 178 页。

〔36〕 该观点来自于与清华大学法学院程啸教授的讨论。

〔37〕 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》，《当代法学》2022 年第 1 期，第 6－8 页；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》，《比较法研究》2021 年第 5 期，第 41 页；张勇：《敏感个人信息的公私法一体化保护》，《东方法学》2022 年第 1 期，第 69 页；孙清白：《敏感个人信息保护的特殊制度逻辑极其规制策略》，《行政法学研究》2022 年第 1 期，第 120 页。

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。[38] 也有学者认为确认信息敏感性的要素包括:数据控制者的利益、数据潜在的接收者、数据收集的目的、处理的条件、对相关人员的可能的后果。[39] 我国《个人信息保护法》第 51 条要求个人信息处理者应当考虑几个要素来确保信息处理活动的规范性,分别为:处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险。一方面这当然是处理活动合规性的要求,另一方面这些要素对于动态化敏感个人信息的归入也有重要意义。综合上述学说及立法,笔者将场景变量归纳为五个要素:信息主体、信息处理者、第三方主体、信息性质、处理目的。

其一,信息主体。信息主体的年龄、身份甚至性别会影响个人信息的敏感性,比如未成年人、犯罪记录、女性等等。其中,未成年人个人信息以及特定身份信息已经为《个人信息保护法》第 28 条第 1 款所列举。

其二,信息处理者。一是信息处理者的规模会导致信息由非敏感变为敏感;二是信息处理者的技术掌握可能会使信息由非敏感变为敏感。

其三,第三方主体。第三方主体往往是敏感个人信息的接收方,其与信息处理者或信息主体的关系可能影响信息的敏感度,比如一般而言,作为信息处理者的委托处理方相较作为信息主体指定的接收信息方更具敏感性。但有些场景中可能并不存在第三方主体,比如信息收集。

其四,信息性质。尽管必须承认有些信息可能与信息主体的人格尊严和人身、财产安全关系更为密切,但需特殊考虑的信息类型应尽量限缩,且信息性质不应当成为单独的考量因素。

其五,处理目的。首先,目的特定原则作为个人信息保护的“帝王原则”,[40] 也是处理敏感个人信息的必要前提;其次,处理目的是否合法正当必要,是个人信息保护影响评估的重要内容。换言之,若处理目的不合法、不正当、不必要,对信息主体的风险会显著升高,个人信息在该情形下也可能具有高度的敏感性。

此外,也有学者提出敏感度高低还与信息处理的方式、数据库类型都有关系。[41] 英国学者瓦克(Raymond Wacks)也认为影响个人信息敏感程度的间接因素还包括公开信息的规模大小、信息存续的时间长短等。[42] 笔者以为,处理方式可以为信息处理者要素所涵盖;而数据库类型显然不构成一个必要的考量点,同时也可为信息性质所包含;至于信

〔38〕 See Helen Nisenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2010, pp. 140 – 147.

〔39〕 See Spiros Simitis, Revisiting Sensitive Data (1999), Review of the Answers to the Questionnaire of the Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS 108) (Strasbourg, 24 – 26 November 1999), http://rm.coe.int/09000016806845af, 最近访问时间[2021 – 11 – 20]。

〔40〕 参见程啸:《论我国个人信息保护法的基本原则》,《国家检察官学院学报》2021 年第 5 期,第 9 页。

〔41〕 See Joel R. Reidenberg & Paul M. Schwartz, Data Protection Law and Online Services: Regulatory Responses (January 1998), http://www.paulschwartz.net/pdf/onlinesvcs_schwartz – reidenberg.pdf [https://perma.cc/PHZ4 – VRS6], 最近访问时间[2021 – 12 – 25]。

〔42〕 See Raymond Wacks, *Personal Information: Privacy and the Law*, Clarendon Press, 1989, p. 87.

息的规模大小和存续时长，规模巨大的信息处理不仅可能对个人信息主体权益造成危害，甚至还可能会对社会公共利益、国家安全等构成影响，而敏感个人信息可能更多是从个人权益角度进行界定的一个概念，规模大小和存续时长可以考虑由信息处理者要素所包含，因为信息处理者对信息的规模和存续时长具有控制力。

（二）场景要素考量的具体适用

通过实践理性认识和发现的规范中的要素，要使之具有说服力，就需要在实践中加以考量。实践包含立法与司法两方面，敏感个人信息的五要素标准的实践意义也需要在这两个方面对照检验。

1. 作为归入标准的适用

敏感个人信息的归入，即规范的制定者或者案件裁判者将原本不属于《个人信息保护法》第 28 条所列举范围的个人信息视为敏感个人信息。试以与汽车有关的数据为例，汽车数据并不属于《个人信息保护法》所确定的七类敏感个人信息，但是因为汽车数据直接关系到汽车设计、生产、销售、使用、运维等方面，其处理场景又可能对相关主体的人身、财产权益造成影响，因此在《汽车数据安全管理若干规定（试行）》中，车辆行踪轨迹、音频、视频、图像和生物识别特征这几类信息被归入为敏感个人信息，这拓展了《个人信息保护法》中对敏感个人信息的列举。根据该规定，以五要素标准检验，车主、驾驶人、乘车人、车外人员等（信息主体）的车辆行踪轨迹、音频、视频、图像（信息性质），如果被开展汽车数据处理活动的组织（信息处理者）以直接服务于个人的目的所处理（处理目的），这些类型的信息是敏感个人信息。

通过以上例证可知，一个完整的敏感个人信息的处理场景综合考虑上述五个场景要素是合理的，但问题在于五要素构成的场景同样可以适用于所有个人信息的处理，那么五要素对于敏感个人信息判断的独特意义为何？笔者以为，构造完整场景的意义旨在强调敏感与否不是根据信息性质“一刀切”的判断，而必须根据主体、客体、目的等因素综合判断。具言之，根据《个人信息保护法》第 62 条第 2 项针对敏感个人信息具体信息场景的细化，未来制定专门规则或标准时，或是最高人民法院针对敏感个人信息的界定需考虑的各项要素制定司法解释时，可以上述五要素为参照构造场景。同时，在个案中，无论是信息处理者的合规工作，还是执法者的执法判断，或是法官识别敏感个人信息以判断信息处理者义务履行情况等，都需要进行具体场景的判断和考量，而场景五要素可被作为规范考量的评价标准。

2. 作为择出标准的适用

在侵害个人信息权益的民事诉讼中，法官首先需要界定具体案件所涉个人信息是否属于敏感个人信息，一旦被界定为敏感个人信息，则对信息处理者的义务要求与针对非敏感个人信息的不同。但实际上，在涉敏感个人信息民事诉讼中，还存在另一种可能的情形，即所处理的个人信息的确是《个人信息保护法》第 28 第 1 款所规定的七类个人信息中的一类，但未严格按照法定要求处理该类信息，实际上也不构成违法。申言之，五要素标准可否适用于已经被法律所明确为敏感个人信息类型在特定场景下的择出，即七类敏

环球法律评论 GLOBAL LAW REVIEW

感个人信息在哪些场景下可以合理使用。[43] 以《个人信息保护法》第 26 条为例,该条规定完全符合五要素的构造:维护公共安全的组织(信息处理者)采集或识别关于自然人(信息主体)的个人图像、身份识别信息(信息性质),应当为维护公共安全所必需,遵守国家有关规定,并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的,不得用于其他目的(处理目的)。因此,对于人脸信息这类法定的敏感个人信息,在第 26 条所规定的场景下的处理不具有敏感性,可以合理使用。因此,五要素标准可以作为敏感个人信息场景择出的判断依据。

(三)价值判断:符合场景目的的考量

如果将隐私场景理论完全等同于"动态系统论"式的要素判断,认为场景仅能指无限细分的具体信息流动,则可能对该理论理解过于片面。隐私场景理论是在对隐私侵入论和隐私控制论的扬弃上发展起来的,侵入论和控制论存在一种将隐私视为绝对的个体价值的倾向,而忽视了隐私的公共价值和社会价值。场景理论的另一重理论贡献在于提供了一种价值判断的方法,超越"具体情形"式的一阶场景,进行以场景目的为核心的二阶考量,这对于判断敏感个人信息的择出意义重大。

1. 社会场景目的作为价值判断的标准

《个人信息保护法》第 28 条第 2 款规定了处理敏感个人信息的特定目的原则,场景理论是对特定目的的进一步深化,明确了特定目的应当指符合社会场景价值的目的。在隐私与个人信息保护中,有一些学者将特定目的等同于应用场景、技术场景或是行业场景的目的。技术或应用场景的目的,指的是处理者所定义的场景目的,技术场景或应用场景的目的取向更多代表了某个信息处理者的利益,比如平台企业希望追求更精准的个人画像来进行个性化推荐。而将特定目的解释为行业场景目的,可能相较应用场景目的有一定的进步,毕竟行业利益代表了一种集体利益(或团体利益),比如电商行业所追求的"集体最佳实践";但行业集体利益仍然只是小范围的利益集,不同于公共利益,可能背离场景所追求的伦理内涵,这一弊端也同样不容忽视。

尼森鲍姆教授吸收了哲学和社会学上对领域的分类,[44] 将第二阶的场景解释为"社会场景"。其划分实则是基于一种抽象的社会关系,包括教育场景、医疗场景、商业场景、社交场景、金融场景等等。这种场景划分主要有两方面的考虑:一方面,社会场景的概念有利于将场景五要素特定化,尤其是便于确定行为人的身份。在典型的教育场景中,五要素都应当与教育相关,比如学校收集学生的分数信息评估学生的学习情况或考评教师的教学绩效,但如果学校收集学生分数给校外培训机构,就超越了基础的教育场景。另一方面,社会学上场景的解释有利于在利益冲突时帮助法官快速锚定价值判断的标准,指明方向。比如教育场景的价值就包括了知识、传统和礼仪的传承;智力和批判能力的强化;人

〔43〕 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》,《当代法学》2022 年第 1 期,第 4 页。

〔44〕 场景一词借鉴了布尔迪厄的社会场域理论及沃尔泽的正义理论。See Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2010, pp. 166 – 167.

才的发现和培养;品格塑造、社会纪律和公民意识的发展。法学及司法裁判的特质正在于它“几乎完全是在与价值判断打交道”。[45] 在裁判说理阶段,尤其涉及到敏感个人信息的择出,须通过判断社会场景目的来实现法律漏洞的填补。

由上可见,社会场景目的和处理者处理目的是一组不同的概念。社会场景目的必须是符合大多人利益的社会所共同认可的价值,比如医疗健康场景以提升诊疗水平、救死扶伤等价值导向的目的。申言之,冲突利益之间的平衡和取舍并不是“任意”的,也无法以处理目的作为价值判断的依据,而是应当在特定社会场景的目标、目的和价值下进行。因此,将场景视为“社会场景”,任何个人信息的处理,只要与这一社会场景所追求的价值不冲突,那就存在其合理性。

2. 敏感个人信息的处理目的与场景目的是否一致

符合社会场景目的的敏感个人信息的处理可认定为不侵害个人信息权益。主观上,敏感个人信息的立法目的,是为了强化保护个人信息主体的利益。但《个人信息保护法》立法者自始至终都将促进个人信息合理利用之目的与保护个人信息权益相并列。该法第 1 条作为立法目的条款,统摄整部法律,敏感个人信息的处理自不例外。以医疗健康信息为例,对医疗健康信息的开发,不仅能给企业带来巨大的收益,同时还能有利于重大疑难疾病的攻克。因此,医疗健康信息的价值面向不是单一的,而是兼具显著的公共价值和社会价值。所以,敏感个人信息保护制度的目的不是要禁止此类信息的流通,而是追求在合法合理及必要的场景下,既维护个体安全、又促进信息的合理利用,最终是为了协调各方的利益、确立一种社会秩序。问题是,在保护主体和促进信息利用的立法目的相冲突时,是否应当以保护主体利益为绝对宗旨?两者之间可否找到一个合适的平衡点?符合社会场景目的的考量有助于解决这一难题。

社会场景目的导向的规范评价,追求的是敏感个人信息的处理目的与社会场景本身的目的和价值保持一致。因为场景中发生的规范性活动往往围绕着价值而展开,场景所追求的价值和目的的实现,是价值判断的基准。法官在结合制定法规则体进行场景目的的评价时,这种评价对于是否构成民事侵权或者是否构成侵犯个人信息罪都具有显著意义。比如,医疗健康信息在未经单独同意的情形下,被委托给医疗算法开发项目组研发疾病诊断,如果法官完全根据《个人信息保护法》中的敏感个人信息相关规则,那么信息处理者未获单独同意的处理行为显然构成违法,然而,如果从医疗健康信息用以造福社会的角度看,对上述情形下的信息处理的评价则另当别论。因此,对于敏感个人信息处理行为的评价,需要法官在个案中更进一步,超越既有的法律规范,从社会场景目的的角度对信息处理行为进行一个“二阶评价”,而非囿于规范的字面涵义。法律确定的“敏感个人信息”,在符合社会场景目的的情形下处理,可不限于法律所规定的敏感个人信息处理的必要前提和规范准则,换言之,可被视为一般个人信息来处理,也即社会场景目的考量可作为择出的标准。

《个人信息保护法》要协调个人信息主体和信息处理者之间的利益平衡,就不可能制

〔45〕 参见[德]卡尔·拉伦茨著:《法学方法论》(全本第六版),黄家镇译,商务印书馆 2020 年版,第 277 页。

定极其严苛的仅保护信息主体权益的法律;相反,最终呈现出的法律规范,实则是一种折中妥协的产物。法律之目的如果和社会目的不一致,无法满足社会发展需要的话,那么应当采社会学的解释,以贯彻法律公平正义,确保实质妥当性。〔46〕而尊重敏感个人信息处理的场景目的和价值,超越仅仅讨论个人权益、处理的危害以及各种利益之间如何衡量的层面,以社会场景的目的作为行为合法性的最终判断标准,是为了实现一种共同善。同时,对敏感个人信息的处理赋予法官评价空间,可以使得侵权法确定过错要件和确定举证责任时更为灵活,减少判决理由说明的困难。〔47〕当然这一空间并非毫无限度,而是应当由社会场景中的价值、目的所指引。因此,场景目的考量对于判断敏感个人信息处理行为的正当性、促进司法活动的精确化及社会价值导向的司法审判具有重要意义。

四 结 语

《个人信息保护法》中的敏感个人信息更多是一种社会评价和个人主观评价的结合,因此会随着社会文化的发展、个人感受的差异而发生变化,很难有非常明确的固定范畴。这种动态调整的可能性会带来归入择出的诸多问题,亟需理论构造的介入,确立一个清晰的评价标准。本文试图结合场景理论二阶性原理,弥合对敏感个人信息评价上的差异。

场景中的敏感性几乎已经是个人信息保护领域的共识,但是鉴于场景理论实质上是一个哲学理论,学科壁垒导致的话语体系差异较大,因此在转译为法学理论的过程中存在着一定的误差。隐私场景理论存在一个二阶性构造:

第一阶的场景,可以认为是具体案例或执法中单个的信息流动。在这一阶中,解释敏感个人信息须考虑五个要素,信息性质维度只是其中之一,法官在判断处理者是否违反了敏感个人信息的处理义务时,应当以“情形”作为基点。在完整的五要素场景中,通过考量处理行为对个人信息主体利益侵害或危害的“射程距离”,综合评判该信息是否具有敏感性,实现敏感个人信息的动态归入和动态择出。

第二阶的场景目的,笔者倾向于将其视为一种漏洞填补的场景原则。此处的场景,是社会学意义上的场景,比如教育场景、医疗场景、商业场景、社交场景等等。这些场景,本身就有自己的伦理取向和价值,理性人较容易辨别。场景理论认为,符合社会场景目的的处理行为,已经平衡了个体价值、公共价值以及社会价值,而非以牺牲个体价值来成就后两者。因此,法官在裁判说理中,社会场景目的、社会场景价值应作为价值判断的基准,对于敏感个人信息规则体系的漏洞,需要依靠这一原则来予以填补。

[本文为作者参与的2018年度国家哲学社会科学基金重大项目“大数据时代个人数据保护与数据权利体系研究”(18ZD146)的研究成果。特别感谢程啸教授为此文提出的诸多宝贵修改意见。]

〔46〕 参见梁慧星:《论法律解释方法》,《比较法研究》1993 年第 1 期,第 56 页。

〔47〕 参见朱虎:《规制性规范与侵权法保护客体的界定》,《清华法学》2013 年第 1 期,第 159 页。

［**Abstract**］ Sensitive personal information meets the requirements of risk-based legislative approach, which is an important legislative trend in the international protection of personal information. This important system has also been established in the Personal Information Protection Law. The purpose of strengthening the protection of sensitive personal information is to prevent the unreasonable disclosure or abuse of this kind of information, which can easily lead to infringement upon or harm to human dignity and personal or property safety of the individual. Article 28 of Chinese Personal Information Protection Law adopts the legislative model of "general clause + enumeration" in defining sensitive personal information, and provides that "'sensitive personal information' means the personal information of which the leakage or illegal use could easily lead to the violation of the personal dignity of a natural person or harm to personal or property safety", while at the same time lists seven types of "typical" sensitive personal information, namely "information on biometric identification, religious beliefs, specific identity, health care, financial accounts, and personal whereabouts, and personal information of minors under the age of fourteen". The first part of this article reviews and reflects on the current legislative model in China and points out that the "general clause + enumeration" definition of sensitive personal information may bring uncertainty in many respects: firstly, the vagueness of appraisal leads to unclear conceptual boundary; secondly, the development of technology may continue to give birth to new types of sensitive personal information, such as behavioral data; and thirdly, the multi-dimensional nature of judgment standard means that whether a piece of information is sensitive or not cannot be judged solely by the nature of the information. The second part of this article carries out a comparison between the Chinese mechanism and the similar mechanism in EU's General Data Protection Regulation, in which the legislator picks the term "special categories of personal data", rather than uses the term "sensitive data" directly. Meanwhile, General Data Protection Regulation regulates "special categories of personal data" in a contextual basis, namely, prohibiting processing in principle and allowing processing in some very specific contexts, thus avoiding the uncertainty caused by a vague general clause. In contrast, Article 28 of the Chinese Personal information Protection Law is to a certain extent a general provision that lacks specific classification standard. The third part of this article attempts to dynamically define sensitive personal information within the framework of contextual integrity, in which five elements, namely information subject, information processor, third-party, nature of information and purpose of information processing, are considered in a comprehensive way. The five-element standard is conducive to a dynamic definition of sensitive personal information, helps relevant departments reasonably identify specific standards of sensitive personal information, and enables judges to make scientific and reasonable decisions on disputes over the infringement upon the right to persona l information in judicial practice.

环球法律评论 GLOBAL LAW REVIEW

（责任编辑：姚　佳）