

敏感个人信息保护的路径建构

王泽天

天津大学法学院，天津

收稿日期：2024年6月24日；录用日期：2024年7月10日；发布日期：2024年8月14日

摘要

伴随当前数字经济时代的纵深发展，个人信息安全面临着严峻的风险挑战。敏感个人信息由于其本身固有的高度人格属性更需要予以特别保护。确立敏感个人信息保护路径的前提是与私密信息做好内涵界分和法律适用衔接。不可忽视的是我国敏感个人信息保护相关法律制度并不健全，司法实践中诸多问题亟待解决。当前敏感个人信息保护存在“知情同意”规则面临现实困境、侵权行为和损害结果之间的因果关系难以证成、敏感个人信息侵权的损害赔偿难以落实等实践难题，因此应当不断进行评估调适，并最终确立高效可行的敏感个人信息保护方案。敏感个人信息保护的未來路径建构亟需通过细化告知—同意规则、利用算法技术推进因果关系的智慧化认定、严格落实敏感个人信息损害赔偿制度，型塑差异性与灵活度的规制机制。

关键词

敏感个人信息保护，私密信息，路径建构

The Path Construction of Sensitive Personal Information Protection

Zetian Wang

School of Law, Tianjin University, Tianjin

Received: Jun. 24th, 2024; accepted: Jul. 10th, 2024; published: Aug. 14th, 2024

Abstract

With the in-depth development of the current digital economy era, personal information security is facing serious risks and challenges. Sensitive personal information needs special protection because of its inherent high personality attributes. The premise of establishing the protection path of sensitive personal information is to do a good job in the separation of connotation and the connection of

law application with private information. It can not be ignored that the legal system related to the protection of sensitive personal information in our country is not perfect, and many problems need to be solved in judicial practice. At present, there are practical problems in the protection of sensitive personal information, such as the "informed consent" rule facing realistic difficulties, the difficulty in proving the causal relationship between the infringement act and the damage result, and the difficulty in implementing the damage compensation liability for the infringement of sensitive personal information. Therefore, it is necessary to constantly evaluate and adjust, and finally establish an efficient and feasible protection scheme for sensitive personal information. The future path of sensitive personal information protection needs to be constructed through the elaboration of the notify-consent rule, the use of algorithm technology to promote the intelligent identification of causality, and the strict implementation of sensitive personal information damage compensation system, so as to form a regulatory mechanism of diversity and flexibility.

Keywords

Protection of Sensitive Personal Information, Private Information, Path Construction

Copyright © 2024 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 问题的提出

随着互联网信息技术的不断迭代升级,个人信息以空前广度和深度被频繁挖掘利用^[1],创造出可观的经济价值和社会价值,不容忽视的是,个人信息尤其是敏感个人信息在安全方面受到诸多挑战,亟需法律法规予以特别保护。2021年8月通过的《个人信息保护法》细化了公民个人信息保护的程序和实体内容,首次在立法层面对一般个人信息和敏感个人信息进行区别保护。然而,从法律涉及到的五个敏感个人信息保护条文¹来看,其对敏感个人信息保护的规范逻辑与一般个人信息保护高度相似,没有聚焦敏感个人信息的专属特征进行特别保护。实践中大型网络平台依托优势地位侵犯敏感个人信息的案件层出不穷,人脸识别等生物识别信息被滥用更是屡见不鲜,这更使得敏感个人信息保护迫在眉睫。未来除需要进一步制定完善配套法律、法规外,突出《中华人民共和国民法典》第一千零三十四条与《个人信息保护法》敏感个人信息的处理规则相衔接是回应敏感个人信息保护现实困境的重要一招。进一步讨论的问题是,敏感个人信息保护缘何需要与私密信息的概念进行界分,目前敏感个人信息保护存在的现实困境以及如何建构敏感个人信息保护的路径。

2. 敏感个人信息的内涵界定与法律衔接

在讨论敏感个人信息保护之前,有必要对其进行内涵界定。从当前敏感个人信息的学术研究和法律实践来看,对敏感个人信息的内涵界定需要结合私密信息的特征进行探讨,私密信息是否应当划归敏感个人信息的范畴,与敏感个人信息保护适用相同的法律规定?如果不进行界定区分将陷入法律适用方面的困境,因此有必要在厘清二者内涵的基础上针对二者确立不同的保护方案,这是当前敏感个人信息保护法律实践的重要议题。

(一) 敏感个人信息与私密信息内涵界分

我国《个人信息保护法》第二十八条第一款规定了敏感个人信息的定义,将容易导致自然人的人格

¹ 《个人信息保护法》第2章第2节第28条至第32条。

尊严受到侵害或者人身、财产安全受到危害作为构成要件，并突出了“敏感性”的核心特征，最后规定了典型场景下的生物识别信息、宗教信仰信息等具体敏感个人信息。我国《民法典》第一千零三十二条第二款对隐私的概念和含义做出了规定，同时第一千零三十四条第二款对私密信息应当如何适用法律做出了规定，强调了“隐私性”是私密信息的特征。从两者的法律规定可以看出，两者的法律概念和法律适用均有不同，那么《民法典》所采用的私密信息和非私密信息二分法是否映射到《个人信息保护法》上的敏感个人信息和非敏感个人信息？敏感个人信息与私密信息的关系如何？目前学界存在较大的争议。一部分学者认为私密信息的外延远远大于敏感个人信息的外延，因此，私密信息能够完全包括敏感个人信息[2]。另一部分学者认为部分信息既可以属于敏感个人信息也可以是私密信息[3]，但也有的敏感个人信息并非私密信息，有的私密信息也并非敏感个人信息。

目前学界的主流观点认为敏感个人信息和私密信息之间是交叉重合的关系。一方面，二者在立法价值上存在交叉重合关系。私密信息保护的背后逻辑体现了个人信息权益和隐私权相交叉的立法价值，同样，敏感个人信息也将“敏感性”个人特征和个人信息权益合二为一。作为国家的根本大法，《宪法》第三十八条明文规定了“中华人民共和国公民的人格尊严不受侵犯”，确保了敏感个人信息保护的合法性，而私密信息虽未直接规定在《宪法》中，但《宪法》的诸多条文也明示了公民私密信息的重要性和合法性。另一方面，二者在内涵上存在交叉重合关系。敏感信息和私密信息都与自然人的个人尊严与人格自由密切相关。虽然两者是根据不同的标准、规制目的对个人信息作出的划分，但是不可否认的是两者与个人的人格尊严和自由高度关联，甚至可以直接定位到特定自然人。但是，依据《民法典》和《个人信息保护法》对敏感个人信息和私密信息所做出的定义，敏感个人信息和私密信息又存在各自所“互不干涉”的部分，相较而言，私密信息的“主观性”更强，具备更强的“个人控制特征”。“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”，这就决定了有些被划分为敏感个人信息的个人信息，可以依照主体的个人意愿不必再被划分为隐私信息。

(二) 敏感个人信息与私密信息的法律衔接

敏感个人信息和私密信息是《个人信息保护法》与《民法典》分别规定的内容，两者之间的话语混同在司法实践中容易带来系列问题[4]。因此，两者的法律适用竞合问题有待进一步厘清。具体而言，两者在调整范围、调整方法、具体规范等方面既有共性也有差异，如何选择法律适用，需要进一步明确。

我国的《民法典》生效时间早于《个人信息保护法》，虽然尚未引入敏感个人信息这一概念，但已在第一千零三十四条第二款中增加了生物识别信息、行踪信息等内容，实际上也为《个人信息保护法》创设“敏感个人信息”概念提供了可能。当然，仅从文义解释上来看，敏感个人信息保护与私密信息保护存在逻辑上的难以自治之处。一方面，以私密信息为内容的隐私权法律保护相较敏感个人信息看似更为严格，《民法典》对于私密信息保护应当适用隐私权的规定也证实了这一点；但在另一方面，法律对于敏感个人信息保护所采取的归责原则则更为严格，法律条文规定隐私信息的损害赔偿采取过错原则，而敏感个人信息采取过错推定原则。目前学者对这一观点也有不同的争鸣，有学者主张，二者可采取一般法与特殊法的关系适用[5]，就规则体系而言，《个人信息保护法》是领域法，其领域既包括公法规则，也包括私法规则，但其中的敏感个人信息保护规则大部分属于私法规则。因此，在法律适用层面，如果《个人信息保护法》有特别规定，则应当适用该规定，《个人信息保护法》没有做出特别规定的，一般适用《民法典》有关规定即可。还有学者主张《个人信息保护法》以宪法为依据，应与《民法典》平行适用[6]。笔者认为，两者之间并非是谁优先被适用问题，应该将其共同转化为同一制度模块进行具体适用。从法理层面分析，《民法典》和《个人信息保护法》的法律适用可以衔接[7]，若涉及敏感个人信息和私密信息重合的部分，此时虽然《民法典》和《个人信息保护法》是一般法与特别法的关系，原则上应当优先适用《个人信息保护法》，但鉴于对私密信息隐私权的保护位阶大于敏感个人信息保护的位阶，此时

应当依据《民法典》第一千零三十四条第三款的规定，优先适用隐私权的规定，没有规定的，适用有关个人信息保护的规定，但对于一种个人信息仅构成敏感个人信息但不构成私密信息的，则应当依据特别法优于一般法的原则，优先使用《个人信息保护法》的规定对敏感个人信息进行保护。

至于损害赔偿责任的归责原则，尽管目前对于敏感个人信息和私密信息采取不同的归责原则，但鉴于针对二者的侵权行为具有相当程度的严重性，对侵犯私密信息的行为采用过错推定原则有利于强化保护自然人人格权益的立法原意。

综上所述，《民法典》和《个人信息保护法》的众多条文背后都蕴含了多种治理工具，只不过《民法典》采取的是私法治理模式，而《个人信息保护法》更多的是公私法模式的大融合。正如美国法学家邓肯·肯尼迪(Duncan Kennedy)所提及：公法和私法并非完全对立的个体^[8]。关键要在确定法律问题诉求目标的基础上，深度理解两部法律提供的庞杂制度工具的优缺点，并在此基础上进行法律适用，绝不能盲目的进行制度工具叠加，否则会导致更为混乱的局面。

3. 敏感个人信息保护的现实困境

随着互联网信息技术的快速发展，数据信息的处理流通呈现“隐蔽性”“持续性”“不确定性”等新的特点。近年来，个人信息尤其是身份信息、通讯信息、银行账户等敏感个人信息遭受泄露侵犯的事件频发，给当事人的工作生活带来极大困扰，甚至导致一些社会影响较大的恶性事件。但受到侵害的当事人却难以获得及时有效的信息保护救济，更有甚者，敏感信息侵害方并未受到法律的及时制裁。目前的敏感个人信息保护在法律适用、维权成本等方面仍然存在很大的局限性，无法完全保障个人和社会的信息安全。

(一) “知情 - 同意”规则面临现实困境

《个人信息保护法》第二十八条、第二十九条规定了处理个人信息只有在具有特定的目的和充分的必要性，并采取严格保护措施，同时应当取得个人的单独同意的情形下，个人信息处理者才能处理敏感个人信息。但在实践中，敏感个人信息容易受到侵犯的主体主要为个人，而作为相对人的信息处理者则是具有高度专业性特征的大型互联网平台。这些平台在产业利益驱动下，仅仅存在有限理性，很少顾及敏感个人信息主体的安全利益。敏感个人信息主体并不具有专业知识和技术手段了解平台的信息告知同意规则，即使平台在用户隐私协议条款中加入了告知同意条款，但因条款过于冗长艰深，所谓的告知同意规则也沦为一纸空谈。更遑论现实存在的默认为同意、变相强迫收集、超范围收集、未按照法定要求单独征得同意、以模棱两可或目的不明的语言告知或征得同意等情形，知情同意原则对于敏感个人信息的侵权行为更加难以发挥预期处置功能^[9]。

以黄某与深圳某计算机公司等隐私权、个人信息保护纠纷案为例²，原告黄某在使用某社交 APP 登录某读书软件时发现，该读书软件在未经原告授权同意的前提下，自动为原告大量添加关注社交 APP 好友，此外将原告的相关阅读记录和信息公开化，社交 APP 好友可无障碍查阅。原告认为，被告的上述行为侵犯了原告的隐私权和个人信息权益，应当承担相应的侵权责任。被告则认为，在用户协议中已经约定了原告使用该读书软件则被告有权获得原告的相关社交数据以及向共同使用该软件的社交好友展示相关阅读信息，原告勾选了授权同意选项，可视为原告已经知情同意。法院认为，知情 - 同意不仅包括信息主体对收集信息种类的知情，还包括对收集、使用的目的、方式和范围的知情及同意，且应充分、自愿、明确。在本案中，某社交 APP 将社交好友名单以及阅读记录授权给读书软件的处理敏感个人信息的行为，应当首先明确告知原告公司处理、授权敏感个人信息的为的使用目、方式、范围以及种类并获得

² 黄某与被告腾讯科技(深圳)有限公司广州分公司、腾讯科技(北京)有限公司隐私权、个人信息权益网络侵权责任纠纷一审民事，(2019)京 0491 民初 16142 号。

原告的自愿、单独明确同意，被告所主张先前双方签订用户协议授权同意的行为不能认定该社交 APP 履行了充分的告知同意义务，原告的个人信息权利并未得到充分保障。由此可见，当前法律实践中大型互联网平台无视“知情-同意原则”，以“一揽子同意”规则代替“单独同意”规则的侵权行为屡见不鲜。

(二) 侵权行为和损害结果之间的因果关系难以证成

《个人信息保护法》第六十九条第一款内容采取了过错推定的立场，规定处理个人信息造成权益损害，信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。但在实践中运用过错推定原则存在不小的阻力。在侵权行为发生的认定上，人脸识别等人工智能技术的适用已普遍化，即使遭受到不法行为的侵害，敏感个人信息主体也难以得知具体的侵权责任人，甚至得知自己的权利已经遭受侵害也具有相当的困难性^[10]。

以“薛某与某网络有限公司隐私权纠纷案”为例³，薛某于某大型电子商务平台下单购买产品，该商务平台就案涉订单记录通过计算机自动化手段对薛某某的个人信息进行了收集活动，并以数据加密、部分脱敏形式向平台商家、送货第三方提供了上述信息。此后薛某连续三次接到境外疑似骚扰诈骗电话，对方掌握到了薛某案涉交易的商品信息、配送信息和支付宝账号等个人信息，并试图以此骗取薛某信任，诱导其添加微信进行“诈骗”操作。在本案中电子商务平台是否涉及未采取严格保护措施的情形下进行个人信息处理活动等情形，法院认为商务平台取得了信息安全管理体认证，同时对个人信息的流通采取了加密、去标识化以及留痕控制，对平台内商家进行了个人信息保护的警示教育，因此不构成侵犯隐私权。

在此案例中，尽管已经大大降低了个人信息侵权案件中个人信息主体因果关系证明标准，个人提供的证据只要足以证明个人信息处理者存在侵权行为的高度可能性，就初步完成了对因果关系的举证责任。但大型商务平台一方依托其技术背景，凭借强大的资本等优势可以证实自身尽到合理注意义务，而信息主体受制于条件有限很难提出反证。如果借助于专业鉴定机构，则会造成诉讼成本增加，进一步打击维权者的积极性。

(三) 敏感个人信息侵权的损害赔偿责任难以落实

笔者在北大法宝案例数据库进行类案检索发现，与敏感个人信息保护相关的民事诉讼案例里，即使是胜诉的案件，信息主体所获得赔偿金额数额普遍较低，而信息处理者侵权的高度隐蔽性以及专业性，也大大增加了信息主体维权的技术难度和成本。

第一，损害赔偿责任难以清楚地界定和计算。《个人信息保护法》对侵害个人信息的行为如何赔偿做出了规定，损害赔偿责任按照个人受到的损失或者信息处理者获得利益确定，难以确定的根据实际情况予以赔偿。⁴但在实践中，涉案金额往往较少或者是单条信息的获益难以进行计算，如果按照个人因此受到的损失或者敏感个人信息处理者因此获得的利益确定，便难以兼顾实质意义上的公平。

第二，被侵权人的精神损害赔偿难以获得法院的支持。按照《民法典》第 1183 条第 1 款⁵以及《个人信息保护法》第 69 条⁶的规定，对于侵害自然人的人身权益必须达到造成严重精神损害的程度方可获得精神损害赔偿。该法律条文明确规定了“严重性”的前置条件，但“严重性”的概念界定却难以进行具体化。

第三，就目前的裁判现状来看，法院支持精神损害赔偿请求的案例较少，且即使支持了被害人的精神损害赔偿请求，赔偿金额也存在畸轻情形。

³ 薛祥飞、浙江淘宝网络有限公司隐私权纠纷一案民事，(2022)浙 0192 民初 4259 号。

⁴ 《个人信息保护法》第 69 条第 2 款。

⁵ 《民法典》第 1183 条第 1 款。

⁶ 《个人信息保护法》第 69 条。

在“许某与中国某银行股份有限公司分行等民事纠纷案”中⁷，尽管被上诉人在未经许某准许的情况下，擅自获取许某某的个人信息，多次拨打上诉人电话，但法院认为某分行并无侵害徐某某个人信息权益的主观故意，也并未造成徐某某人身和精神严重损害，上诉人许某某要求各被上诉人赔偿精神损害抚慰金或公开致歉无事实和法律依据，因此不予支持上诉人的精神损害赔偿请求。

在“夏某与北京某科技有限公司侵权责任纠纷案”中⁸，法院既判处被告向原告赔礼道歉，也判决被告在该判决生效后十日内赔偿原告维权合理支出 1 元、精神损害抚慰金 1 元。从上述案例可以看出，敏感个人信息保护的相关赔偿制度仍然需要完善。

4. 敏感个人信息保护中规制路径的完善

针对我国敏感个人信息保护制度供给不足的现状，需要拓宽行政规制路径来搭建起敏感个人信息保护的基本框架，通过细化告知 - 同意规则、利用算法技术推进敏感个人信息处理智慧化转型、建立行业规制和奖惩激励制度、严格落实敏感个人信息损害赔偿制度等途径，进一步完善针对敏感个人信息保护的制度建构，切实回应敏感个人信息保护法律实践难题。

(一) 细化告知 - 同意规则

告知 - 同意规则是敏感个人信息处理的前置性条件，也是保障敏感个人信息自决权的重要基础。细化告知同意规则首要的前提是路径建构的目标要与敏感个人信息保护的价值追求保持一致。要在充分保护敏感个人信息主体人格权益的基础上，将敏感个人信息权益保障与数据利用原则相结合，既要充分保护自然人的人格尊严以及人身和财产安全，也要合理利用经过安全认证的自动化决策等个人信息处理行为，为市场营商主体提供稳定的政策预期。

在收集面部特征、指纹等敏感个人信息前，应当确保敏感个人信息的收集是为了实现服务提供所必需的，同时应当履行详尽充分的告知义务，包括使用的目的、方式和范围，并且应当确保敏感个人信息主体的单独同意是在完全知情的基础上做出的意思表示，同时不得以为征得敏感个人信息主体的明示同意而强制个人勾选用户协议否则便不提供相应服务从而得到非自愿性质的同意，更不得将多种服务或产品捆绑提供，诱使信息主体一次性做出多项授权同意。实践中大型互联网平台在关联主体中共享敏感个人信息或随意向第三方企业提供用户敏感个人信息的违法情形多发，此时敏感个人信息处理者应当重新向个人用户做出告知，在未得到个人用户的明示同意前不得将敏感个人信息做出共享、转让以及公开披露等行为。在敏感个人信息的流通环节，收集敏感个人信息数据用以形成个人画像，进而做出自动化决策的，个人信息处理者应当就其计算机自动决策行为不存在用户歧视或差别待遇作出说明。

当然，尽管“知情 - 同意”规则发挥了中流砥柱的作用，但实践中也存在无需同意即可收集信息的情形，例如为了国家安全、公共安全和利益，以及为了刑事起诉审判活动不得不收集敏感个人信息的，此时公共利益保护位阶大于敏感个人信息保护的位阶，应当明确无需取得敏感个人信息主体同意即可收集信息的规则。

(二) 利用算法技术推进因果关系的智慧化认定

敏感个人信息处理流程具有高度的自动化决策特征，资本和技术的紧密结合加剧了敏感个人信息保护和技术更新换代的矛盾。只有不断加强敏感个人信息处理的技术化、自动化创新，加强技术与制度的协同才能有效消除技术鸿沟，构建完善的敏感个人信息保护因果关系认定体系，同时通过行政监管的智慧化转型以有效应对系统性风险。

我国《网络安全法》《数据安全法》和《个人信息保护法》对人工智能、人脸识别等新兴技术作了特

⁷ 许某与中国某银行股份有限公司分行等民事纠纷案，(2023)辽 03 民终 1358 号。

⁸ 夏某与北京某科技有限公司侵权责任纠纷案，(2023)京 0166 民初 1296 号。

别限制,明确了由专门部门制定相关标准规则。这就需要行政机关及有关部门对敏感个人信息处理者履行准入监管职能,建立起监管者与敏感个人信息处理者的沟通机制。敏感个人信息处理者对其创新性敏感个人信息处理自动化决策进行先一步的设计,包括对敏感个人信息的脱敏化以及去标识化处理、流程的保密性、安全评估等由相关监管部门进行监管,只有当相关程序较为成熟并且风险较低时才可以获得批准,从而达到事先预防的效果。

网信部门应成立人工智能技术库,实现监管和算法的结合,将创新性信息处理方案备案登记作为前置程序,掌握对信息处理者的技术进行介入和反制的能力,确立风险管理导向,以算法预警为主导,发挥行政部门信息溯源、动向追踪的技术治理能力,从而为被侵害信息主体提出反证提供技术支持。

(三) 严格落实敏感个人信息损害赔偿制度

精神损害赔偿作为个人信息侵权救济的重要一环,其判定应以严重精神损害为前提。然而,对于何为“严重精神损害”,在个人信息侵权领域并无统一标准。因此,在司法实践中,应结合具体案件情境,综合考虑受害人的身份特征、被泄露信息的敏感性与私密性、侵权者的行为手段以及侵权行为的社会影响等因素,来评估精神损害的严重程度。

一是在敏感个人信息侵权案件中,受害人因信息泄露而产生的焦虑等不良情绪反应,属于侵权行为导致的常见精神损害后果。此类后果虽难以量化,但不宜直接依照传统观点否定其精神损害赔偿的正当性。相反,应结合受害人的个体感受、身份特征,被泄露信息的性质与敏感性、侵权行为的手段以及侵权行为所造成的危害结果和侵权行为是否造成被侵权人社会评价的降低等因素,综合判断其是否构成严重精神损害。

二是鉴于个人信息侵权的隐蔽性和分散性等特点,其损害结果往往难以直接证明。因此,在司法实践中,若受害人能够证明其个人信息存在被滥用或泄露的实质性风险,即可依据《中华人民共和国民法典》第九百九十七条的规定向人民法院申请人格权禁令,申请敏感个人信息处理者立即停止侵害、排除妨碍、消除危险。个人信息侵权往往导致受害人因信息被滥用而失去潜在的商业化利用价值,从而产生财产损失,当具体损失难以量化和计算时,法院可依据法律规定,结合案件具体情况充分考虑信息潜在的商业价值,酌情确定赔偿数额。

三是遵循比例原则引进惩罚性赔偿制度。尽管我国《民法典》并未规定敏感个人信息保护的惩罚性赔偿制度,但由于敏感个人信息权益天然内置人格属性和财产属性,大多数侵权人为获取巨额利润铤而走险,贩卖自然人的敏感信息,此时若仅仅对其处以填补性损害赔偿责任,则有失公允原则。

但适用惩罚性赔偿必须严格遵循比例原则。若为了敏感个人信息的保护而采取“一刀切”的行政规制方法,盲目的加大行政处罚的力度,将不利于高新技术的更新换代。因此,确立处罚标准不仅要衡量个人信息处理行为对于公共利益的侵害程度,更要高度关注侵害敏感个人信息利益的情况与侵害程度和处罚程度相匹配,严格遵循“金字塔式”的惩罚性赔偿构建标准,即情节较为轻微的大多数侵权案件——位于金字塔的低端,并不适用惩罚性赔偿制度,只有情节严重的少数侵权案件——位于金字塔的顶端才适用惩罚性赔偿制度。

总之,敏感个人信息侵权的损害赔偿判定是一个复杂而精细的过程,需要综合考虑多种因素。在司法实践中,应坚持公平、公正、合理的原则,确保受害人的合法权益得到充分保障。

5. 结语

当前敏感个人信息保护在司法实践中存在诸多困境,因此需要结合行政规制等手段构建综合性保护体制机制。在大数据技术呈现多元、复杂性特征的今天,敏感个人信息不断与经济社会文化相互交融,已然具有交互性和场景性的特征,因此,敏感个人信息的保护是一个长期动态过程。受到技术提升、个

人选择等多种因素的掣肘，前文所述规制路径势必会存在“失灵”情形，此时需要融入“场景化”处理手段，结合发生敏感个人信息侵权的现实场景，做出不同的判断，以此应对大数据时代敏感个人信息保护实践中频发的各类问题。在敏感个人信息保护面临的严峻复杂形势下，寻求跨部门、跨领域的法律合作或许是打开这一大门的钥匙。

参考文献

- [1] 田野, 张晨辉. 论敏感个人信息的法律保护[J]. 河南社会科学, 2019(7): 43-49.
- [2] 房绍坤, 曹相见. 论个人信息人格利益的隐私本质[J]. 法制与社会发展, 2019, 25(4): 99-120.
- [3] 程啸. 论个人信息权益与隐私权的关系[J]. 当代法学, 2022, 36(4): 59-71.
- [4] 张平. 大数据时代个人信息保护的立法选择[J]. 北京大学学报(哲学社会科学版), 2017(3): 143-151.
- [5] 王利明. 论《个人信息保护法》与《民法典》的适用关系[J]. 湖湘法学评论, 2021, 1(1): 25-35.
- [6] 周汉华. 平行还是交叉——个人信息保护与隐私权的关系[J]. 中外法学, 2021(5): 1167-1187.
- [7] 程啸. 论我国个人信息保护法中的个人信息处理规则[J]. 清华法学, 2021, 15(3): 55-73.
- [8] Kennedy, D. (1982) The Stages of the Decline of the Public/Private Distinction. *University of Pennsylvania Law Review*, 130, 1349-1357.
- [9] 张新宝. 个人信息收集: 告知同意原则适用的限制[J]. 比较法研究, 2019(6): 1-20.
- [10] 齐爱民, 王基岩. 大数据时代个人信息保护法的适用与域外效力[J]. 社会科学家, 2015(11): 101-104.