Dispute Settlement 争议解决, 2026, 12(4), 179-188
Published Online April 2026 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2026.124115

Hans汉斯

论推荐算法下个人信息的民法保护

丁丽萍

青岛科技大学法学院，山东 青岛

收稿日期：2026年3月8日；录用日期：2026年4月1日；发布日期：2026年4月10日

摘　要

推荐算法是一种利用用户和物品相关数据，通过特定的计算逻辑和模型，为用户筛选并提供可能感兴趣、符合其需求物品或内容的技术手段。个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息。国内对推荐算法下个人信息的民法保护问题的研究开始于互联网大数据时代，彼时各类互联网平台借助推荐算法为用户提供个性化服务，在这个过程中大量收集、使用用户个人信息，个人信息安全风险逐渐暴露，相关争议和纠纷不断涌现。随着此类现象愈发频繁，针对个人信息保护，我国出台了相应的专门法律予以回应，但是在保护力度和保护级别方面还不足够，基于此，本文将在研究国内外个人信息保护的现状基础上，进一步提出推荐算法下个人信息的民事保护建议。

关键词

推荐算法，民事规则，个人信息保护

The Civil Law Protection of Personal Information under Recommendation Algorithms

Liping Ding

Law School of Qingdao University of Science and Technology, Qingdao Shandong

Received: March 8, 2026; accepted: April 1, 2026; published: April 10, 2026

Abstract

Recommendation algorithms are technical means that utilize user and item-related data, through specific computational logic and models, to screen and provide users with items or content that they may be interested in and that meet their needs. Personal information refers to all kinds of information that can identify a specific natural person either alone or in combination with other

文章引用: 丁丽萍. 论推荐算法下个人信息的民法保护[J]. 争议解决, 2026, 12(4): 179-188.
DOI: 10.12677/ds.2026.124115

information, recorded in electronic or other forms. Research on the civil law protection of personal information under recommendation algorithms in China began in the era of Internet big data. At that time, various Internet platforms used recommendation algorithms to provide personalized services to users, during which they collected and used a large amount of user personal information, gradually exposing the risks to personal information security and leading to the continuous emergence of related disputes and conflicts. As such phenomena have become increasingly frequent, China has introduced corresponding specialized laws to address the protection of personal information. However, the protection intensity and level are still insufficient. Based on this, this article will, on the basis of studying the current situation of personal information protection at home and abroad, further propose suggestions for the civil protection of personal information under recommendation algorithms.

Keywords

Recommendation Algorithms, Civil Rules, Protection of Personal Information

1. 推荐算法与个人信息概论

(一) 个人信息民法保护的基本理论

《中华人民共和国民法典》(以下简称《民法典》)人格权编对于个人信息做出了界定，即个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。与个人信息关联着一个核心概念即“可识别性”，在学界围绕“可识别性”尚还存在不同观点：一种观点认为个人信息不应该拘泥于静态，而是一种动态的可识别性，随着科学技术的发展和数据的积累，原本不具有可识别性的碎片化个人信息，在大量数据的堆积之下逐渐形成个人画像，仍然可作为个人信息进行保护[1]。王利民教授认为个人信息的可识别性应该做广义的理解，当许多不具有可识别性的个人信息结合起来可以指向某一具体的人时仍然属于个人信息的范畴[2]。齐爱民教授则认为可识别性是个人信息的核心要素[3]，此外的形式要素：“可固定和可处理”同样是界定个人信息的一面。尽管对于“可识别性”这一关键要素学界尚可一致，但是可识别的范围多大这一关乎个人信息保护范围的关键问题还未得到共识。

对于个人信息的法律属性国内尚未达成一致观点，主要有五种观点：财产权说，一般人格权说，隐私权客体说，新型民事权利说以及具体人格权说。

财产权说所认为的只要不与法律与公共利益相抵触，那么所有权人对个人信息享有占有、收益、处分权能。然而此种观点事实上不攻自破，它混淆了个人信息的财产利益和人格利益，数据发展的时代，信息已然成为一种商品，但此类利益可以通过保护专利、著作的方式加以保护[4]，也就不难看出民法侧重保护的是其人格利益。

一般人格权说和隐私权客体说均有明显不足之处。虽然一般人格权是对人格的概括保护，弥补了具体人格权的不足。但是，其过于抽象概括，不利于司法裁判也不利于对个人信息更好地保护[5]。隐私权客体说则根植于英美法系，强调隐私权是人格不可分离的一部分的人格权理论。尽管大陆法系也延用人格权理论，但二者关于隐私的概念也不一致，大陆法系的民法保护的仅限于不愿他人知晓的那部分隐私

[6]，自然也就不适合我国的本土国情。

新型民事权利说，此学说是数据时代发展的产物。在个人信息在从保护到深化利用的过程中，个人信息权益不再是上述权利的任何一种，而是独立的新型民事权利，如李伟民认为个人信息权利是与股权与知识产权并列的[7]。

具体人格权说，是大多数学者的观点。以王利明学者为代表，从隐私权和个人信息权益的区别出发理清二者的不同，指出隐私权作为人格权利并不能完全涵盖个人信息权益。随着大数据和算法时代的到来，个人信息被界定为具体人格权，法律保护个人信息是为了维护个人的人格尊严和人格平等，确认个人对其信息享有平等、自主支配的权利。如果将个人信息权作为财产权，势必妨害人格的平等性。但这并不排斥其财产属性，对于个人信息并非如同所有权一般直接占有，使用，收益，处分。而是自然人通过商品化或者公开化的方式、来处理利用个人信息。

笔者赞同个人信息的具体人格权说。首先，个人信息应看作具体人格权的一种。原因在于：第一，个人信息不论是敏感的隐私信息或是可识别的个人信息，比如基因等隐私信息、性别、兴趣爱好、浏览记录等一般信息都与人格的形成发展密切相关。并且与个人隐私侵权相同，个人信息的泄露也会损害人格尊严。第二，个人信息作为一项民事权利加以保护，而不仅仅是一种民事利益，有助于在绝对权的角度对信息主体提供更高水平的保护。个人信息的义务主体并非特定的义务人，因此将其界定为绝对权中的人格权保护并非不妥。

其次，个人信息具有财产属性，在大数据背景之下，精确的算法对我们的个人信息进行整合与分析，我们便经常会收到各种精准推送，又或者平台之间通过协议转卖个人信息进行商业利用，这无不体现出个人信息商业价值，也即财产属性。

最后，除了上述两种属性，个人信息还具有公共属性，比如疫情防控期间，人们让渡了一部分个人信息，方便国家进行防控。

(二) 推荐算法的概述

随着大数据和生成式人工智能的发展，推荐算法目前已被广泛应用，涵盖到网络购物，视频音乐，搜索引擎，新闻资讯等各个领域。推荐算法是指网络服务平台对用户个人信息进行收集、识别、标记，从而针对用户的行为、特征、偏好以及物品(如购物品类、观看的视频、阅读的文章等)的属性进行个性化的信息服务推荐和决策的一种技术手段，其具有数据依赖性、决策的不透明性、推荐的精确性。

过度收集、隐蔽收集用户个人信息。一方面，以海量数据为支撑的推荐算法，隐私条款往往复杂冗长，用户既没有专业知识能够完全理解也少有人会完全读完。推荐算法的运用多是在用户同意的边界范围外，或是越过用户告知同意规则，调取用户提供信息背后的个人信息，比如浏览记录、购物车商品、收货地址、搜索历史、观看时长等，并且据此而窥探用户画像。另一方面，推荐算法是许多计算机语言代码组成的自然语言，夹杂着烦琐的数据材料和运算规则，对于绝大多数人而言，这是一个无法洞悉的“算法黑箱”[8]。在这个背景之下，鲜有用户能够完全知晓运作规则以及实际用途，也难以察觉平台间的数据追踪与共享。

擅自恶意泄露个人信息。近年来，推荐算法泄露个人信息的案件屡见不鲜。分析 2018 年的 Facebook-Cambridge Analytica 数据泄露事件 [1]。可以发现数据泄露致使用户收到“精准推送”的新闻而被操纵选举态度，推荐算法在平台间数据共享传输安全性不足，导致用户个人信息被第三方应用滥用，同时黑客能

[1]英国政治咨询公司通过 Facebook 第三方性格测试应用非法获取约 8700 万用户数据，用于政治广告定；事件导致 Facebook 被美国联邦贸易委员会罚款 50 亿美元，并推动《通用数据保护条例》(GDPR)的强化实施。以及 2021 年 TikTok 数据泄露事件因 API 设计漏洞致用户隐私信息(如邮箱、手机号)暴露风险，虽未确认大规模泄露，但引发欧美对其数据存储(美国与新加坡)及跨境流动的审查，加剧地缘政治争议。

够利用漏洞抓捕个人信息，对于个人信息的恶意泄露不仅侵犯个人信息安全还可能导致财产安全等问题。比如违法犯罪分子通过对于个人用户喜好的了解，制定有针对性的诈骗方案，多数人难以识破骗局，极大地危害人身和财产安全。

违法使用个人信息，引发算法歧视。个性化推荐初衷应是为用户提供更加有针对性的更加便利的推荐服务，然而现实不理想。算法歧视是指算法在决策过程中基于种族、年龄、性别、收入等敏感特征，对某些特定群体的不公平对待[9]。设计者本身在设计算法时不可能是完全中立者，加之算法黑箱的内部运行规则难以洞悉，使得个人信息被不恰当的分类、过滤、关联、排序，进而引发算法歧视。比如，美国医疗算法将黑人患者排除在治疗的优先位置，又比如我国外卖平台算法对于不同地区的骑手的配送费存在歧视，往往是偏远地区的分配更少骑手而配送费用更高。对于个人信息的违法使用，要通过使用前和使用中等环节及时干预，否则会进一步引发更多法律问题。

2. 推荐算法下个人信息的民事保护现状

(一) 推荐算法下个人信息保护的民事立法现状

2021 年和 2022 年相继颁布《个人信息保护法》以及《互联网信息服务算法推荐管理办法》日益凸显出国家对于个人信息保护的重视，以及对推荐算法活动的规范性提出要求。《民法典》第 111 条规定自然人个人信息受到民事法律保护，在人格权编第 1034 到第 1038 条规定了对于个人信息保护的具体规定。《民法典》第 1035 条第二款规定了个人信息处理中的“处理”是指个人信息的收集、存储、使用、加工、传输、提供、公开等。两项重要的规则：一是告知同意规则；二是目的限制规则。

告知同意规则是认定个人信息处理者行为是否合法的一个基础性原则。如前文所述，个人信息具有一定的公共属性，但绝不存在“个人信息是可以自由使用的，除非个人信息上存在明确可识别的个人权益，否则就不能赋予信息主体干预他人使用的自由”[10]。个人信息可以单独或结合起来识别特定的自然人，其上有民事权益。单单为了保护公共利益而不分界限的让渡全部个人信息上的民事权益，漠视了个人信息上承载的民事权益，只能导致大量以维护公共利益之名而行侵害私权利之实的恶行，最终的结果是既无法维护公共利益，更无法保护民事权益。私权保护与公法规制之间不是非此即彼的关系，而是应当通过两者共同构建个人信息保护的制度基石[11]。我国民法采取告知同意规则这一标准化模式，既使得个人信息处理者要明确合法范围，又使得作为自然人的信息主体能够在保障个人人格尊严不受侵犯。同时《个人信息保护法》第 18 条又兼顾了个人信息公共价值。

目的限制规则的规范是关于《民法典》第 1035 规定处理个人信息应当遵循合法、正当、必要原则的概括，其中的正当性和必要性的要求与《个人信息保护法》第 6 条一脉相承。

首先，应该明确目的的内涵：一是此种目的需要明确、清晰的表达；二是这种目的是有限度的，并不是笼统、一概而论的。比如，网络企业在告知个人时宣称“本公司有权将所收集的个人信息用于任何本公司业务发展所需之合法用途”显然此类表述中的处理目的就是不明确的。其次，目的限度原则包括四个方面的内容：第一，最基础的是目的要合法即不违反法律法规的规定，不违背公序良俗。前述的告知同意规则已经论述，在此不在赘述。第二，最核心的是与处理目的直接相关，然而在推荐算法的背景下这一核心要素已然受到挑战，推荐算法窥探个人画像的精准个性化推送、广告推销等都背离了这样的目的限制规则。例如，“北京百度网讯科技公司与朱烨隐私权纠纷”，此案中朱烨在搜索引擎中以“减肥”“丰胸”等关键词进行搜索。而后该搜索引擎则通过其搜索记录生成个人画像，多次进行有关此种内容的广告推送。按照处理目的的直接相关性而论，朱某的直接目的是使用该搜索引擎，搜索引擎获取其关键词等信息也并没有问题，而关键的问题在于百度公司将个人信息披露给第三方广告公司并且进行广告推送的行为，且先不论朱某是否同意第三方处理个人信息，此种目的显然以及与处理目的并非直接

相关。第三，处理个人信息要采取对个人权益侵害最少的方式；第四，收集的个人信息限于实现处理目的的最小限度，也就是不能过度收集。

随着该技术的进一步发展，2021 年我国针对个人信息保护出台《个人信息保护法》，全文涵盖了八章，重点包括个人信息和敏感个人信息概念的界定、个人信息处理规则的规定、个人信息跨境提供规则、个人信息跨境提供规则以及法律责任。因为涉及面广、影响范围大、发生频率高，广大人民群众苦“个人信息滥用”久矣，因此本法第二十四：“通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。通过自动化决策方式做出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式做出决定。”针对社会各方面对于用户画像、算法推荐等新技术新应用高度关注，对相关产品和服务中存在的信息骚扰、“大数据杀熟”等问题强烈反应。个人信息保护法立足于维护广大人民群众的网络空间合法权益，对利用个人信息进行自动化决策做出有针对性规范，明确要求提供个人拒绝的选项。在此基础上，2022 年 3 月 1 日起实施的《互联网信息服务算法推荐管理规定》(以下简称《管理规定》)更是对于推荐算法应用扩大引起的社会广泛关注的大数据“杀熟”、算法歧视、算法诱导沉迷等问题的积极回应。不仅明确算法推荐主体的相关责任，赋予用户知情权，选择权，拒绝权，还体现了一些算法治理的国际原则和共识。它的主要内容包括：一是明确受监管的推荐算法服务主体类型。《管理规定》第 2 条将应用算法推荐技术定义为“利用生成合成类、排序精选类、个性化推送类、检索过滤类等算法技术向用户提供信息。”这一规定，几乎涵盖了各种短视频、电子商务、新闻媒体等形式的推荐算法提供主体，只要是内嵌与推荐算法的服务主体，都落入保护范围。二是赋予用户法律上的自主选择性。该规定在《电子商务法》和《个人信息保护法》的基础上进一步详细赋权用户知情权，自主选择权和退出权，如该规定明确要求保障算法选择权，应当向用户提供不针对其个人特征的选项，或者便捷的关闭算法推荐服务的选项，以及不得根据消费者偏好、交易习惯等特征利用算法在交易价格等交易条件上实施不合理的差别待遇等。同时在第五章规定了相应的法律责任，让用户的自主权真正得到落实。三是建立分级分类治理的治理理念。《管理规定》第 23 条规定网信部门会同电信、公安、市场监管等有关部门建立算法分级分类安全管理制度，根据算法推荐服务的舆论属性或者社会动员能力、内容类别、用户规模、算法推荐技术处理的数据重要程度、对用户行为的干预程度等对算法推荐服务提供者实施分级分类管理。具体问题，具体分析，明确责任的大小，维护技术发展利用于保护二者的动态平衡。

(二) 推荐算法下个人信息案件的司法实践现状

在万物互联、人工智能、云计算、推荐算法等信息利用技术日益发展的时代，各种 APP 层出不穷，海量数据以及个人信息无所遁形，对于个人信息的保护与利用成为这个时代绕不开的课题。《民法典》中对个人信息的定义、处理原则、免责事由、救济措施等做出原则性的规定，开启了个人信息保护的新时代。

与一般的侵权案件相比，个人信息案件的独特之处在于，对于个人信息的侵犯往往并不能满足侵权的所有要件，而是在某个侵权的环节，诸如收集、泄露或者使用环节。目前对于个人信息的保护，不仅可以依据《民法典》人格权编的人格权请求权提起诉讼，还可以依据《个人信息保护法》所赋予的权利如，查询、复制、更正、删除等权利请求侵权救济，这使得对个人信息的保护更加周延。当事人的诉请更加明确，以个人信息为单独案由提起的诉讼案件数量上升明显，个人位置信息、网络行为痕迹、软件使用记录、通讯录或好友关系数据等与人格利益息息相关的信息被认定为个人信息受到保护。

以海量数据为支撑的推荐算法，应用于各行各业如，交通、酒店、金融、电商、物流等等。从涉案行业来看，这些行业所开发或者应用的 APP 与算法工具往往有着大量的用户，案件呈现出群体性特征。然而这些用户数量巨大的个人信息处理者处于优势地位，在个人信息受到侵害时，单个用户因为知识、时

间、资金等限制往往缺乏维权的动力。为了应对这种情况，《个人信息保护法》确立了个人信息公益诉讼制度，运用检察机关、消费者组织、社会组织等力量，对于大规模侵害用户个人信息的行为提起公益诉讼。案件调研发现，个人信息保护法实施以来，以检察机关、消费者组织为原告的个人信息公益诉讼案件明显增多，个人信息民事公益诉讼在个人信息保护中日益发挥重要作用。

3. 现行法律规范对个人信息保护的不足

(一) 推荐算法驱动下带来的个人信息界定的法律挑战

对于个人信息的界定我国民法围绕可识别性展开。《民法典》和《个人信息保护法》将个人信息区分为敏感信息和一般个人信息，敏感信息因其与人格尊严密切相关，一旦遭到非法使用和泄露，会严重侵害其人格尊严的一类信息，比如指纹、面部特征、宗教信仰、医疗健康等信息。对于敏感个人信息处理时采取书面同意的处理规则，然而在推荐算法技术的发展下个人信息仅仅围绕可识别性显示出不足之处。在推荐算法技术的使用下，非可识别的个人信息，比如浏览记录，购买记录，兴趣爱好等信息，通过整合形成的用户画像仍然具有可识别性。譬如这样几组信息：① 小李在某网站上多次购买与法律相关的书籍；② 小李获得模拟法庭最佳辩手一等奖的记录；③ 小李曾在社交平台分享自己在某某大学的生活，以上任何一个信息尚不属于可识别的个人信息，然而组合成用户画像非常容易定位到小李是某高校的一名法律学生，并且具有唯一性。可见，对于个人信息是否具有可保护性，仅仅从单一的静态角度界定对于应对算法技术的发展已经显示出不足。

(二) 推荐算法发展与个人信息处理规则失衡

1) 告知同意规则的困境

告知同意规则在信息处理者和个人信息主体之间以桥梁的形式将二者联通，随着网络信息技术的发展以及数据的过量，“桥梁”两端的主体都呈现出了新的变化，这些变化使得该规则陷入了新的困境。

从信息处理者角度看，通过数据分析、算法整合，信息数据可以分析出市场趋势，消费喜好，甚至可以操控民众的选择。在现实中最为典型和重要的信息处理者是信息网络服务商和数据企业，告知同意规则通常以隐私条款的形式落实。隐私条款的篇幅普遍较长，且用语专业晦涩，提供的信息趋于饱和，甚至严重过载。国外有研究成果表明，如果信息主体要阅读提供给他们的所有隐私政策，那么每年需平均付出 244 个小时；如果只是粗略阅读，那么每年需平均付出 154 个小时。这意味着在信息网络社会，每人将平均每天花费 40 分钟阅读和理解各种网站、手机应用等服务的隐私政策[12]。显然，如此繁杂的隐私条款，信息处理者背后真正的目的已经背离为了获得信息主体的同意，信息主体在面对庞杂的隐私条款时，选择一键同意，知情同意规则没有有效的运用。

从信息主体来看，有两方面的问题。一是在告知方面，隐私条款的设计以信息主体为“理性人”的角度进行，事实上，在算法黑箱下如何获知算法的运行和结果产出的过程并非人人都能，即便是设计者对算法技术自动化决策的过程也无法完全知晓。二是在同意方面，拒绝条款则无法使用 APP 等规定实际上剥夺了真正的同意权利，比如扫码点餐必须进行登录注册。为了平衡信息的利用和信息保护，也非所有信息都需要进行同意，一刀切的保护无疑增加了不必要的负担。

2) 目的限制规则的困境

在倡导数据共享流通的趋势之下，信息保护不能因噎废食，充分挖掘个人信息的价值，加之合理的利用不仅能够促进企业的发展也能带动互联网技术的发展。但推荐算法的动态特性使得目的限定规制出现了一些困境。一方面，信息处理主体一开始同意处理的目的，在算法深度挖掘和学习的过程中会向其目的边界扩展，如何区分兼容性用途与实质性偏离，是目的限定规则不可回避的问题。例如，收集用户行为数据用于“提升服务质量”，后续可能被用于个性化定价或心理画像。另一方面，算法应用场景的

快速迭代，如果任何主体的数据二次利用都需要信息主体的同意，无疑会增加信息主体的负担，也会导致信息利用的限制，不利于信息流通和发展。也是对上述告知同意规则的架空，实践中缺乏动态同意机制，用户无法及时追踪数据用途变化。

(三) 推荐算法下个人信息侵权救济困境

1) 举证困难

个人信息主体通过告知同意规则将个人信息的部分使用权利让渡给信息处理主体，然而后续对于信息的保存、利用以及与第三方共享的过程等步骤并不在信息主体所能掌控的范围内，加之算法黑线的不透明性，是举证侵权行为时不可避免遇到问题。此外，在确定侵权主体时也存在困难，算法通过收集大量数据，加以分析进行精准的推送等个性化推荐服务。那么当精准推送的信息侵犯个人信息时侵权主体是谁的问题难以确定。一方面，广告投放人通常以虚拟号码拨打电话、发送短信，仅凭来电信息无法确定侵权人；另一方面，广告商家不承认购买过侵犯受害人权益的广告服务，也无法认定广告商家为侵权人[13]。个人信息侵权具有隐蔽性、技术复杂性和难以感知性，一方面对过错进行证明的难度大，另一方面被侵权人通常是个体自然人，而侵权人往往都是企业组织或公权部门，被侵权人与侵权人相比，无论是在财力、专业技术、诉讼能力上都难以对抗，如果将个人信息侵权责任一律以过错归责原则来认定，将远远超出被侵权人的举证能力，使法律赋予司法机关的权利救济功能落空，挫伤被侵权人的诉讼维权积极性。

2) 损害赔偿认定困难

个人信息作为具体人格权具有人格权属性和财产属性，目前《民法典》对于侵害个人信息后如何救济规定的并不清晰。《个人信息保护法》第六十九条第二款明确规定了侵害公民个人信息的民事赔偿责任主要有两个依据：一个是个人受到的损失，另一个是侵害者因非法处理个人信息获得的利益。然而在实践中都存在不同程度的困境。

一方面，损害后果难以量化。相较于传统的侵权案件能够通过医疗费、误工费等费用对损害后果进行量化并且合理弥补因侵权所造成损失。个人信息保护案件更多地体现在精神损失上，而认定信息侵权导致的精神损失又十分的主观，难以真正得到确认。继续以上述广告推销为例，大量的骚扰电话，短信轰炸客观上不会对信息主体造成什么财产损失，而是更直接地体现为精神上的损失。根据《民法典》第1183条的规定，请求精神损害赔偿的标准是达到严重的程度。在数据快速流通的时代，要达到严重程度的精神损害在短时间内难以达到，个人信息面临的风险程度要远大于会造成的可救济的损失。

另一方面，侵权者获得利益难以确定。推荐算法技术为个人信息处理者带来的利益远不止直接的经济利益，还包括间接的战略利益和数据黏合衍生利益。如推荐算法优化用户体验，延长用户停留时间，但黏性带来的长期收益难以精确拆分。然而，实际案件裁判过程中多以“实际情况确定赔偿数额”，使信息主体维权的积极性大大降低。除此之外，判决信息处理者删除、修改、停止使用个人信息，也难以通过个人信息主体进行监督落实，使得维权的实效难以保障。

4. 推荐算法下个人信息保护路径

(一) 明确个人信息范围

1) 建立个人信息分级保护机制

在大数据时代，信息的共享已成为不可阻挡的趋势，加之推荐算法的整合运作之下，个人信息的保护内容与保护强弱不可分离[14]。过分的个人信息保护难以适应时代发展要求。欧盟DPIA的风险等级划分方式，欧盟在GDPR中通过设置“数据保护影响评估”(DPIA)对个人信息保护的风险进行等级划分。GDPR将个人信息划分为高、中、低三个等级。DPIA避免了数据的僵化分类，通过“信息敏感性 + 场

景风险程度”的模式对于应对算法的动态化也不失是一种好的路径。我们也不妨通过同样的方式结合本国国情将个人信息在民法上进行细化分级保护。

基于此，可以将个人信息保护分为三个等级。第一级：低敏感个人信息，如姓名、职业、年龄、出生日期等采取行为规制模式加选择退出机制，这类信息着重通过规制信息的收集、存储、流通和流动等过程行为，对于信息主体可以通过选择不予同意进行排除信息的利用，此种信息在最大程度上可以适用，一方面促进数据的共享与流通，服务于公共目的或者促进商业发展；另一方面，当出现损害情形时也相对容易寻找责任主体，各个环节的信息加工处理者通过举证证明自己的行为不存在过错，进一步帮助信息主体排除非责任主体。第二级：一般敏感个人信息，如，家庭住址，通讯信息、信用卡号等，对此类信息采取明示同意并且规定更为严格的信息处理者的民事责任的方式加以保护，比如对于滥用推荐算法泄露个人的住址导致个人生活安宁受到侵犯，可以采取惩罚性赔偿的补救措施。因为此类信息具备极高的个人识别性，同时一旦泄露或者被滥用会对个人利益产生比较严重的后果。第三级：高度敏感个人信息，如指纹、基因信息、生物特征等，既要通过个人书面明确同意，也要通过法律设置严格的条件予以处理。

2) 建立多场景个人信息动态保护

在上述分级的基础之上，在实践中还应结合不同的场景具体分析个人信息的保护程度。一方面，在多重信息叠加构建的场景下，即使只是低敏感的个人信息，在形成的用户画像之后也可能造成严重的个人利益损失。比如常见的线上购物，关注平台商家后经常受到短信或者电话的推销，并且无法拒绝。另一方面，高度敏感的个人信息，比如生物特征在面对保护国家利益或者公共利益的场景时，即使未通过信息主体的书面同意，也未必会对其权益造成不良影响，诸如对于某种病原体携带者向社会的公布。

(二) 完善个人信息处理规则

1) 信赖关系引入告知同意规则

在前文中提到告知同意规则的困境主要存在于两个方面，一是，隐私条款的冗长，信息主体无法获知全部内容；二是，算法黑箱下隐私条款基于信息主体理性人的角度出发，给处理者和信息主体两者都分别带来了不同的困境。

个人信息的披露受到控制，算法中对隐私的感知在很大程度上受到算法环境中因素的制约，特别是个性化和信任等因素，最近的研究表明隐私和自我披露之间存在联系，因此本文提出了所谓个人信息保护中的信赖关系[15]。信赖关系是指信息主体基于对信息处理者的信任与依赖，或为了获得某种许可使用或为了获得某种利益，同意将个人信息交给信息处理者进行收集、分析、使用、甚至交易。信赖关系当中的告知同意规范结构呈现为“分级信赖 + 按需同意 = 合法处理”，意味着自然人主要依据对信息处理者的信赖程度，作出不同需求的同意决定[16]。从信息处理者角度看，既不强求其以繁杂的条款履行告知义务，告知其全部的处理方式、目的以及用途，也不对信息处理者苛以严格的算法解释要求，使得推荐算法得以继续应用不至高于成本压力。从信息主体来看，摆脱“理性”人的桎梏，同意不再是全有或者全无的方式作出，也不要求同一信息必然对同一使用目的作出同样的同意。通过分级信赖，事实上也就是通过对个人信息进行的分级保护内容，对其进行按照需求的同意。任何的规则都不能做到事无巨细，最重要的是建立起处理者和主体之间的互信互赖的纽带，以一种积极的价值取向去规制行为，从而促进个人信息权益的保护和社会经济效益的最大化。

2) 构建合理预期下的目的限定规则

在现有的目的限定规则下，要求与处理目的直接相关，推荐算法导致个人信息的兼容性用途与实质性用途的偏离，以及二次利用的重复同意，成为该规则面对数据共享时代的大难题。而合理预期下的目的限定规则是解决个人信息共享与保护的良好路径。

合理预期标准是指，基于个人信息主体的视角，在特定场景下，用户对个人信息处理的范围、方式

和目的所持有的客观、合理的预判。这种标准也并非一成不变，会随着技术发展社会价值观念的变化而改变。通过分级保护，将个人信息分为了上述三类，进一步加入合理预期的概念，客观视角以“普通理性人”的预期为基准，结合不同因素，比如：数据控制者的告知、数据敏感性、行业惯例等，进一步判断是否超出客观目的以及与初始目的是否存在关联。对于上述一般敏感信息(如健康、生物识别、行踪轨迹等等)，用户对其使用范围的预期更严格，通常需单独、明示同意。一般信息，如用户名、浏览记录等，合理预期范围较宽，但仍需与场景相关。因此也就不得不进行动态的目的性兼容评估。当个人信息二次利用于新的用途时，需要进行关联性评估。可以通过新目的与初始目的是否存在逻辑联系；上下文一致性，数据处理场景是否发生变化，如从医疗转为商业营销通常不兼容；数据性质，对于不同性质的数据类型，给予不同的关注度，如敏感数据兼容性门槛更高；以及对于用户影响即新用途是否对用户权益产生其他人格或者财产损失。几大方面进行动态的评估，一方面，防止不必要的二次同意，提高信息流通效率；另一方面，在面对推荐算法精准推送或者用户画像描绘是否侵犯个人权益的问题时，更加灵活。

(三) 完善个人信息侵权救济机制

1) 细化信息主体认定与侵权归责原则

在推荐算法这一背景之下，个人信息的互通互换并非单独存在于一个信息处理者之下，而是数个已知或者潜在的信息处理者。这种信息处理者呈现出复数的状态，也正是算法案件侵权主体难以确定的一大原因。对此，程啸教授认为，在个人信息泄露的案件中，如果存在着数个信息控制者，信息主体无法确定是谁泄露了个人信息时，此时应当适用共同危险行为制度[17]。然而，这种观点并非建立在认为行为人实施了共同危险行为，而是因为其行为造成了“证据损害”。作为一种侵权法上的责任，共同危险行为责任不能单单考虑权利人存在的客观的证明困境，也要同时注意兼顾潜在行为人应受保护的行动自由。

如此，基于证据法的角度或许可以给复数侵权主体的认定提供一些实践意义上的思路。通过高度盖然性的标准来证明侵权主体，也就是说，由信息权人列举出可能的侵权人，法官按照高度盖然性标准初步确定侵权人。如果被告无法证明被列举的其他主体有较高滥用信息的可能，则按照通用性侵权法律制度去认定；如果证明了这种可能性，权利人可以基于《民法典》第 1170 条转而诉诸共同危险行为责任，选择某一主体承担责任。

个人信息侵权具有难以发觉、技术复杂、隐蔽的特点，个人信息的侵权人往往是企业和公权部门。较以前相比，大型的企业比如，腾讯、阿里巴巴等，它们处理个人信息的能力不亚于公权力部门。通过现有的过错归责原则或者过错推定原则虽然能够在一定程度上减轻被侵权人的举证负担，基于前述的个人信息分类，一般的个人信息可以采用过错责任归责原则，相对敏感的个人信息采用过错推定原则也能得到较为充足的保护。但是当企业进行自动化决策严重侵犯个人敏感信息，或者公权力部门滥用权力侵犯个人信息等情形出现时，应当同时引入无过错责任，提高被侵权人维权的积极性。因此，应适用不同的归责原则，即针对使用自动数据处理系统的公务机关、非公务机关以及未使用该系统的传统信息侵害行为分别适用无过错责任和过错责任[18]。

2) 健全侵权损害赔偿机制

不同于可实际估量的损害结果，在大数据背景下对个人信息的侵害更加呈现出风险危害的趋势。正如瓦格纳所言：“一项没有出现在损害清单中的无形财产，会被潜在的加害者遗忘，如果人们知道无须为某种损害承担责任，也就没有避免损害的动力了。”[19]将推荐算法等技术可能造成的风险类型化，承认其未来会造成的损失，将是认定损害赔偿的第一步。对此可以借鉴美国的经验。一是采用法官酌定赔偿数额。根据《个人信息保护法》提到的两种方式确定外，由法院酌定赔偿数额更为一种适宜的路线。个人信息无形损害，因难以被计量，需要法官在个案场景中，综合衡量侵权人的过错程度、具体侵权行为和方式、造成的后果和影响等因素来确定个人信息无形损害的数额[20]。二是确定最低赔偿数额标准。

《加州消费者隐私法案》(CCPA)第 1798.150 节中的规定，在侵权事件发生后，每位消费者可以要求“每次事件赔偿不少于 100 美元且不超过 750 美元的损害赔偿金或实际损害赔偿金，以数额较大者为准。”我国，也可以尝试通过在侵权责任上确定最低赔偿数额。这一规定不仅有利于解决个人信息侵权导致的精神损害或隐性风险实际损失难以计算的问题。为信息权人提供兜底保障，避免因举证困难而放弃维权。还通过明确侵权行为的“价格下限”，即使受害者实际损失难以量化时，侵权方也需承担法定最低赔偿，促使相关信息处理者合规行动，增加违法成本。此外，还能够提高司法的公信力，约束法官的自由裁量权，防止出现同案不同判。

参考文献

[1] 张新宝. 从隐私到个人信息: 利益再衡量的理论与制度安排[J]. 中国法学, 2015(3): 38-59.

[2] 王利明. 论个人信息权的法律保护——以个人信息权与隐私权的界分为中心[J]. 现代法学, 2013, 35(4): 62-72.

[3] 齐爱民. 个人信息保护法研究[J]. 河北法学, 2008, 26(4): 15-33.

[4] 邢会强. 大数据交易背景下个人信息财产权的分配与实现机制[J]. 法学评论, 2019, 37(6): 98-110.

[5] 王利明. 论个人信息权在人格权法中的地位[J]. 苏州大学学报(哲学社会科学版), 2012, 33(6): 68-75, 199-200.

[6] 张里安, 韩旭至. 大数据时代下个人信息权的私法属性[J]. 法学论坛, 2016, 31(3): 119-129.

[7] 李伟民. “个人信息权”性质之辨与立法模式研究——以互联网新型权利为视角[J]. 上海师范大学学报(哲学社会科学版), 2018, 47(3): 66-74.

[8] 刘伟兵. 人工智能时代意识形态风险的生成逻辑与科学防范[J]. 河海大学学报(哲学社会科学版), 2024, 26(6): 10-19.

[9] 钟晓雯. 算法推荐网络服务提供者的权力异化及法律规制[J]. 中国海商法研究, 2022, 33(4): 63-72.

[10] Post, R. (1989) The Social Foundation of Privacy: Community and Self in the Common Law Tort. *California Law Review*, **77**, 957.

[11] 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.

[12] 吕炳斌. 个人信息保护的“同意”困境及其出路[J]. 法商研究, 2021, 38(2): 87-101.

[13] 秦华, 高允菁. 个人信息保护的当下困境及司法应对——以手机 APP 对个人信息的使用为切入点[J]. 天津法学, 2022, 38(2): 55-70.

[14] 童云峰. 证立与提倡: 读者个人信息的民法分类分级保护[J]. 现代情报, 2021, 41(12): 97-106.

[15] Shin, D., Kee, K.F. and Shin, E.Y. (2022) Algorithm Awareness: Why User Awareness Is Critical for Personal Privacy in the Adoption of Algorithmic Platforms? *International Journal of Information Management*, **65**, Article ID: 102494. https://doi.org/10.1016/j.ijinfomgt.2022.102494

[16] 王崇敏, 蔺怡琛. 告知同意规则在信赖理念下的反思与出路[J]. 海南大学学报(人文社会科学版), 2025, 43(2): 117-129.

[17] 程啸, 阮神裕. 论侵害个人信息权益的民事责任[J]. 人民司法, 2020(4): 60-65.

[18] 叶名怡. 个人信息的侵权法保护[J]. 法学研究, 2018, 40(4): 83-102.

[19] (德)格哈德·瓦格纳. 损害赔偿法的未来——商业化、惩罚性赔偿、集体性损害[M]. 王程芳, 译. 北京: 中国法制出版社, 2006: 55.

[20] 项焱, 张雅雯. 大数据时代个人信息无形损害的正当性基础与认定规则[J]. 江苏行政学院学报, 2022(5): 127-136.