聚知刊出版社
JZK publishing

数字司法公开中个人信息分层式保护

向彩花

天津工业大学，天津，300387；

摘要：数字司法公开通过数字化技术、平台，以庭审直播、法院案例库、12309 中国检察网等途径将各类司法信息向公众开放。数字司法公开的目的在于实现司法过程动态化监督与数据共享，同时也带来了泄露个人隐私的风险。本文尝试着从个人信息保护的多样性与合法性出发，根据信息的私密程度与授权程度，对个人信息采取分层式保护。并对数字司法公开中个人信息生命周期进行分析，突破“知情同意”二元逻辑的局限性，使司法数据公开存在正当性，体现出个人信息保护中的利益思维，实现个人信息差异化保护。

关键词：数字司法公开；信息处理原则；分层式保护

DOI：10.69979/3029-2700.25.06.071

问题的提出

随着《关于加强网络信息保护的决定》《中华人民共和国刑法修正案（九）》等法律法规的出台，我国在公民个人信息保护方面逐步加强和深化。2020 年，《中华人民共和国民法典》（以下简称《民法典》）进一步明确了个人信息保护的基本原则与具体规则，为司法实践提供依据。2021 年，《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）的颁布实施，推动我国个人信息保护法治建设进入新的阶段。数字法院、数字检察院等建设的推进，数字司法公开必是常态。然而，司法案件所涉信息面较为宽泛，包括公民的身份信息、联系方式、财产状况等敏感隐私。如何在信息流通中确保公民个体权益，成为个人信息保护争论中的焦点。

针对个人信息保护问题。场景化理论提出了根据信息主体、信息处理者、第三方主体、信息类型、处理原则五要素，区分不同场景下的信息处理方式，给数字司法个人信息分层式保护提供了新的思路。本文聚焦于数字司法活动中个人信息分层保护问题，探讨如何构建适应数字司法需求的个人信息分层保护模式。结合数字司法中个人信息收集、存储、使用、公开、删除等环节，旨在实现数字社会法治秩序的基本规律，针对不同层次的个人信息实施差异化的保护措施。通过分层保护模式，推动数字司法制度转型，实现司法程序与《个人信息保护法》的有机融合、兼顾个人信息保护的普遍性与司法领域的特殊性。

1 数字司法公开中个人信息分层式保护的需求与现状

1.1 数字司法公开中的个人信息分层式保护需求

司法机关在数字时代背景下积极推进了智慧司法建设，如智慧法院系统、智慧检察平台等以个人信息数据处理为核心，对海量信息资源进行分析。在数字司法转型中，有必要对个人信息进行分层式保护。智慧司法建设是建立在个人信息数据处理的基础之上，其背后是大量个人信息数据的收集与使用，无论是在民事诉讼、行政诉讼、还是刑事诉讼，个人信息均被视为法院诉讼证据的重要组成部分。实现社会治理与犯罪目标时，利用大数据技术收集、使用，往往是在信息主体不知情或未同意的情况下进行。单一的知情同意模式难以适应当前数字司法公开状况，于是就产生了分层分类的必然讨论思路。在应对数字司法公开中个人信息保护挑战时，构建分层式保护机制，明确不同层级个人信息处理原则，是实现个人权益全面保障的关键。《个人信息保护法》第 28 条将生物识别、宗教信仰、医疗健康、金融账户、行踪轨迹等信息列为敏感信息，并通过“等”“兜底式”的方式列举设置不同敏感度范围。《关于侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称《侵犯个人信息刑事解释》） 将个人信息分为最敏感、次敏感及非敏感三个层级，轨迹信息、通信内容、征信信息、财产信息为最敏感层信息；可能影响人身、财产安全的住宿信息、通信记录、健康生理信息、交易信息为次敏感层信息；其他公民个人信息为非敏感层信息。不同层级个人信息的流通共享标准也相应递减。推动个人信息分层式机制在数字司法公开中的应用，既提升公众意识，又通过技术发展支持法律体系的整体一致性，从

而更有力保障个人信息的安全。

1.2 数字司法公开与个人信息保护形成逻辑冲突

在提升司法数据的社会价值时，不可避免地需要以牺牲一定信息权益为代价。大数据的核心在于处理海量信息，单个或者少数个人信息数据本身无法直接创造社会价值，甚至有些数据不包含个人信息，是由于数据技术通过整合、分析从中获取个人信息，这些经过二次加工的信息也极易含有个人隐私。值得注意的是，司法数据作为一种特殊的公共数据资源，其特殊性主要体现在：第一，司法个案是数据来源的基础；第二，司法个案涉及的个人信息范围较为广泛。如何在数字司法公开与个人信息保护之间找到平衡点？各国在应对这一问题时，普遍采取了基于个人信息保护的立法路径，通过赋予公权力机关部门在公共利益的前提下限制个人信息权益。也就是将“公共利益”作为个人信息处理的基本依据，但一味地限制个人信息权益放大公共利益，只会虚设知情同意规则。高度重视数据公开必然会增加虚构、解密、滥用的可能性，这与个人信息保护之间存在逻辑冲突。最大限度保护案件当事人及其他诉讼参与人的个人信息权益，尽量减少数字司法公开给个人生活安宁造成困扰，是实现资源共享与权利保护之间平衡的关键。

1.3 司法数据的不当运作具有侵害个人信息的风险

在司法数据公开过程中，司法机关作为数据来源方，需要收集的当事人及其他诉讼参与人的身份信息、案件信息等个人信息进行技术性处理。随着科技法庭和网络法庭的普及，录音录像技术的便捷化使法院能够对审判和执行过程进行实时记录。互联网的广泛传播和快速网络速度，极大地拓宽了司法数据传播的渠道。信息传递方式已不再局限于传统的口头或书面形式，视频、文件等新型载体能够快速实现信息源和接收者之间的传递，从而大幅提升了信息传递效率。在处理个人信息时，若操作疏忽，可能会无意中泄露个人信息。司法数据被不当运作或被不法分子利用，个人信息泄露可能会加剧网络暴力和网络谣言的扩散。如部分当事人个人信息泄露，当事人可能会遭受网络攻击，甚至影响其正常生活。同时，个人信息被泄露、滥用易于网络谣言的滋生，损害当事人权益和产生社会舆论。法院在向公众公开案件信息时，需对案件信息进行筛选，并根据信息重要程度进行分层分级处理，确保不涉及个人隐私的内容对外公开。尤其是，未对个人信息进行有效识别和技术处理，当事人及其他诉讼参与人的个人信息被泄露，将成为不可避免的情况。

2 数字司法公开中个人信息分层式保护的路径

2.1 数字司法公开中个人信息分层式保护的基础

《个人信息保护法》通过详细规定国家保护个人信息义务，设立专门的行政法律责任章节，体现出个人信息既具有个人与公共双重属性。应当遵从客观性判断标准防止保护范围过于宽泛与模糊。在司法实践中，社会公众知情权与监督权以司法公开和程序透明为基础。为了满足社会多元化的公共利益需求，单一控制与支配个人信息，是不能体现出数据的流通与共享特征。同时也明确侵犯个人的知情权、决定权的法律地位，使信息主体有权限制或拒绝他人对其个人信息进行处理。这种权利的基础在于人格尊严，当权益受到侵害时，可以通过排除妨碍的请求权实现保护。当信息数据在流通或者共享的过程中，个人信息主体合法权益被侵犯时，可以请求对处理行为进行严格规范。这种具有排除妨碍功能的权利被界定为消极权利或者是防御权利。司法数据公开是一种大型的数据库，并非单个信息或是少量信息，是具较强社会属性。也就是说个人信息性质的定位不应局限于自决权的逻辑框架，而应被构建为兼具私人与公共特性的消极权利或者防御权利。

2.2 数字司法公开中个人信息处理场景

随着数字技术的快速发展，数字司法在提高司法效率、促进司法公正方面发挥着越来越重要的作用。传统线下诉讼模式正在向在线模式转变，涵盖立案、审判、执行等多个环节。本文着重探讨线上模式下数字司法中个人信息的处理环节，主要包括个人信息收集、存储、使用、公开及删除等场景。

2.2.1 数字司法公开中个人信息的收集与存储环节

个人信息的收集与存储环节主要集中在立案阶段，涉及当事人的基本信息、案件相关证据等，其中包括大量敏感信息。随着司法数字化的发展，当事人的诉讼行为从传统到现场逐渐演变为线上，法院通过线上平台接收起诉状、案件相关证据材料等在内的各类诉讼文件，这些文件不仅包含当事人的身份信息（姓名、性别、年龄、身份证号等）、联系方式等，还可能涉及生物信息

和行踪轨迹等敏感信息。为防范信息泄露，需要采取脱敏处理等综合性数据保护措施，以确保电子文件在存储和运输过程中的安全性，然而，各地司法机关的技术设备和人员水平参差不齐，甚至部分司法机构无法独立完成技术工作，导致技术性外包加重个人信息泄露的风险。为了确保个人信息的安全，司法部门在收集信息时需严格遵守信息收集的合法性、正当性、目的限制、公开透明等八项原则，严格界定信息收集的范围。还充分考虑个人信息的重要程度、敏感程度，采取差异保护，如对隐私或敏感类的信息加强文档访问权限和存储要求。

2.2.2 数字司法公开中个人信息的使用环节

在线庭审的引入显著提升了审判效果，得益于现代信息技术的支撑，司法过程转移至“屏对屏”模式，易导致在审理中交换的大量私密信息或是被记录永久保存，进一步威胁当事人的个人权益。任何具备访问权限的个体均可能非法录制庭审过程，并将含有敏感信息的视频片段上传至网络，导致个人信息广泛传播。在采取在线庭审时，需全面评估案件的复杂程度、隐私保护需求等因素，采取更为严格的风险评估和管理措施，避免审理信息的泄露、篡改或者滥用。

2.2.3 数字司法公开中个人信息的公开与删除环节

海量庞杂的上网文书内容所承载的个人信息等权利保护问题和大数据爬取、分析技术及商业化利用带来的安全风险问题日益突出。传统的司法程序中，法官依据质证的证据和庭审信息来推理出事实真相，而人工智能技术的应用了裁决的效率和精确度，但智能提升了司法决策的效率和精准度。智能辅助技术提供的案例推送和规则推送等无差别方式，缺乏场景因素的考量，易忽视个体隐私。为了满足社会公众在网络时代对司法公开的需求，实现更高水平的司法公正与司法效率，人们通过中国裁判文书网等专门司法公开平台获取案件信息。面对数字司法公开，信息主体并非公开主体，只是个人信息来源的主体，司法机关作为数字司法公开的主体，基于司法权运行方式的需要依法公开。公开过程中，若没有对隐私、敏感类的信息进行匿名化或者脱敏化处理，信息主体对该信息享有个人信息删除权。即使是匿名化，也并非使个人信息永久不具有识别性，随着信息技术的发展，匿名后的信息也将会失效，从而识别出个人信息。只有删除权还具有让信息丧失识别性，使其不再属于个人信息，对信息主体没有任何危害风险。

2.3 数字司法公开中构建个人信息分层式保护

随着互联网技术对数字司法的推动，在数字司法公开方面，我国已经实现了对“西方的换道超车”。在确保司法公正与高效的同时，避免个人信息安全问题，对个人信息进行合理保护，已经成为当前亟待解决的问题。要解决这一问题，有两个关键点：其一是合理保护个人信息，确保在数字司法领域内合理流动；其二是构建科学、合理的个人信息保护框架。具体来说，可以将个人信息按照其重要和敏感程度进行分层。例如，核心层的个人信息不涉及公共利益，个人信息的人身属性最强最为敏感，需要采取更严格的安全措施；而最外层的信息涉及公共利益，为了促进资源共享，可以特定保护。此外，在构建差异化保护框架时，还需考虑信息主体的授权程度。随着信息主体对其信息的重要程度增加，授权程度也逐级增高。

2.3.1 核心层：核心信息—严格授权

核心层个人信息是直接关联个人生活隐私的核心领域，并与个体的尊严紧密相关，这一领域包括能够直接识别个人身份的信息，具有极强的人身属性，包含了未被公开、未授权他人处理的隐私信息以及权利人设置了特别保护的信息。这些信息一旦泄露，将对个人生活产生重大影响，甚至导致财产损失、名誉受损等。此类核心信息是自权利人产生信息后就没有他人知晓或者不公开的信息，应受到严格的法律保护。只有当信息主体明确表示同意处理其信息，信息处理者才有权限接触或使用这些信息。当信息主体没有明确表达其同意或不同意的情况，法律要倾向于保护公民的隐私权益，应默认为不同意，推断其不授权。针对核心信息的侵害（他人非法获取此类信息），法律上应采取形式性的判断标准，也就是无需证明已造成实质性损害，即可认定该行为对信息主体法益构成侵害。

由于核心层个人信息具有最高的保密价值和人身属性，其社会价值和社会属性最低，尊重个人隐私和信息自决权是核心信息保障该类信息安全的基础，他人无权窥探或者使用这类信息，公民对这一领域的信息是享有绝对性的权利，从而保护其私人领域不受打扰。司法在处理核心信息时应当受到严格限制，尤其是在公开的情景下，只有在信息主体授权的条件下进行。应当严格遵循“授权同意”原则，信息在司法领域流通使用须建立在信息主体明确授权的前提之上，在技术上更是要采

取数据脱敏、加密存储、访问控制等强制性手段。为了更好地保障这类信息的隐私安全，从隐私领域转入公共领域，必须在授权同意或公开的情境下完成。对于授权真实性的责任应当由信息处理者承担，并保障整个授权流程的合法合规性。若信息处理者未对授权真实性进行验证，对信息主体造成了不利影响，信息处理者应当承担相应的法律责任。鉴于核心层信息最为隐私、敏感，在处理此类信息是应严格限制其用途并坚持“一事一授权”的原则。在此原则的限制下，信息处理者授权后的行为因受到严格限制，以避免其在平台或其他范围内擅自扩大个人信息的使用边界，更是体现了对个体自决权的尊重。

2.3.2 中间层：一般信息—有限授权

在数字经济的背景下，司法数据的共享与运用已经成为适应时代发展的重要方向。中间层个人信息是人类交互活动中最为频繁的数据，具有较高的身份识别性，其人身属性次于核心层的信息，但单个信息不具备识别信息主体的身份、财产等敏感信息，需要结合其他信息才能识别。中间层授权规则较核心层更为灵活，应当采取的是有限授权。有限授权强调信息主体的自主选择，要求信息处理者在限定的范围或时间内合理使用，实行概括性同意。中间层个人信息存在较高商业价值，在促进信息的有效流通时，保障信息主体信息安全与有效流通，可以实施“一范围一授权”原则。这类信息的流通仅限于信息主体与被授权方，在授权的范围内被授权方处理信息时，无需经过二次授权。信息处理者在处理这类信息只需要符合合理使用范围，对信息主体遵循概括性同意即可，但被授权人之外的第三人也负有不得侵犯其信息的义务。判断信息使用是否合理，需要采取比例原则，从必要性、紧迫性、预期收益与成本比例等方面进行评估以界定“合理使用”的边界。对于信息主体的概括授权部分，需基于客观目的原则，如违背公民目的使用信息的行为将承担相应责任。但信息主体没有明确反对情况下，其收集和使用行为已符合社会一般用途，此时可以免除信息使用者的责任。通过这样的标准，我们能够确保信息的使用既合理又符合道德与法律规范。

2.3.3 最外层：公开信息—推定授权

最外层的公开信息随着流通性的增强，其人身属性逐渐被剥离，社会属性最高，这类完全属于个人且与其活动关联的公开信息，通常源于个人本身。由于它们与个人之间的距离过于遥远，对个人的影响可以忽略不计。即便这类信息的可识别性极低，单独的一条信息也难以识别出一个人的身份、财产状况等敏感信息，值得注意的是，他人无虽然权在未经同意的情况下侵入私人领域，但在公共领域可以使用，并非“任意入侵”。最外层公开的个人信息仍然属于个人信息，也属于法律保护的范围，只是对其保护力度较弱。既然相对降低保护力度，对于公众获取信息同样遵循概括性授权标准，极易导致数字司法公开与个人信息保护两难困境。这类信息主要是由于信息主体自行披露或者根据法律要求公开，应当转为一种推断性的同意规则，也就是在处理这类信息时，符合人们预期的合理范畴，没有明确规定的不得随意使用或者再加工的行为，并且与处理信息主体公开信息的初衷相符合，可遵循“合理范围内推定授权”，信息处理者在合理范围内合法处理个人信息。

参考文献

[1]赵祖斌.从静态到动态:场景理论下的个人信息保护[J].科学与社会,2021,11(04):98-116.

[2]双重法益构造下的个人信息圈层式刑法保护[J].东南大学学报(哲学社会科学版),2024,26(04):87-97+151.

[3]高志宏.个人信息司法保护的利益衡量[J].当代法学,2024,38(01):31-43.

[4]李军,慕小璐.数字经济时代个人信息保护司法实践探析[J].河北法律职业教育,2024,2(11):46-51.

[5]夏伟.个人信息有序共享的法理言说与制度构建[J].南京师大学报(社会科学版),2023,(06):103-113.

[6]孔祥稳.个人信息自决权的理论批评与实践反思——兼论个人信息保护法第44条决定权之适用[J].法治现代化研究,2022,6(04):78-97.

[7]沈丽飞.司法领域个人信息保护面临的问题和对策[J].社会科学家,2023,(08):104-109.

作者简介:向彩花 19980724 性别:女，名族:侗族，籍贯:贵州，职务:学生，学历:研究生，单位:天津工业大学，研究方向:法学理论