

数字司法背景下的个人信息保护研究

施依琴

杭州师范大学沈钧儒法学院, 浙江 杭州

收稿日期: 2025年5月21日; 录用日期: 2025年5月30日; 发布日期: 2025年6月30日

摘要

在数字司法加速推进的背景下, 个人信息保护面临技术应用与法律规制的双重挑战。大数据、人工智能等技术的司法场景嵌入, 虽提升了司法效率, 但也加剧了个人信息泄露、算法歧视、数据滥用等风险。传统保护机制因法律滞后性、制度分散化及技术适配不足, 难以应对动态化、场景化的个人信息处理需求。本文以数字司法为研究场域, 通过分析数据采集、处理、共享、公开四个环节的现状与法律风险, 提出了法律规制、技术治理、协同治理三个维度的个人信息保护优化路径, 以平衡司法效能和公民权益。

关键词

数字司法, 个人信息保护, 信息泄露, 法律规制

Research on Personal Information Protection in the Context of Digital Justice

Yiqin Shi

Shen Junru Law School, Hangzhou Normal University, Hangzhou Zhejiang

Received: May 21st, 2025; accepted: May 30th, 2025; published: Jun. 30th, 2025

Abstract

Against the backdrop of accelerated digital justice advancement, personal information protection faces dual challenges from technological applications and legal regulation. The integration of technologies such as big data and artificial intelligence into judicial scenarios, while enhancing judicial efficiency, has exacerbated risks including personal information leakage, algorithmic discrimination, and data misuse. Traditional protection mechanisms struggle to address dynamic and scenario-specific personal information processing demands due to legal lag, fragmented systems, and insufficient technical adaptation. This paper explores digital justice as a research field, analyzing current conditions and legal risks across four stages: data collection, processing, sharing, and disclosure. It

proposes optimized protection pathways from three dimensions—legal regulation, technical governance, and collaborative governance—to balance judicial efficacy and citizens' rights.

Keywords

Digital Justice, Personal Information Protection, Information Leakage, Legal Regulation

Copyright © 2025 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. 引言

习近平指出，当今时代，数字技术作为世界科技革命和产业变革的先导力量，日益融入经济社会发展各领域全过程，深刻改变着生产方式、生活方式和社会治理方式[1]。当前人类社会正处于智能革命的深水区，司法系统作为社会治理的关键环节，正经历着由数字技术引发的系统性变革，数字司法应运而生。以大数据、人工智能等现代信息技术手段为支撑的司法数字化改革，通过对司法数据进行算法挖掘，与司法工作深度融合，推动实现更高维度的“数字正义”的生成[2]。个人信息作为数字司法活动中的重要数据资源，其安全性、隐私性和合规性直接关系到司法公正、社会稳定和个人权益三重价值目标的实现。在数字司法背景下，从刑事侦查中的生物特征识别到民事执行中的财产线索追踪，从类案裁判规则的智能生成到司法廉政风险的预警防控，个人信息已成为现代司法活动不可或缺的基础要素。与此相对应的是，司法数据也面临着个人信息保护、数据安全等前所未有的挑战。由于数字技术的复杂性和个人信息处理的敏感性，个人信息在数字司法活动中面临着被泄露、滥用和非法获取等多重风险。

因此，开展数字司法背景下的个人信息保护研究具有重要的现实意义和理论价值。本研究旨在深入探讨数字司法活动中个人信息的保护现状、问题与挑战，分析个人信息保护的法律层面、技术治理和协同治理三个方面，提出针对性的策略与建议，同时，本研究也将为数字司法的健康发展、司法公正的实现以及个人权益的保障贡献一份力量。

2. 数字司法中个人信息处理的现状与挑战

随着信息技术的迅猛发展，数字司法已成为现代司法体系的重要组成部分。在提升司法效率、增强司法透明度的同时，数字司法也带来了个人信息处理的诸多挑战。

2.1. 数字司法中个人信息处理的典型场景分析

1) 数据采集：技术赋权下的“全息画像”

在数字司法时代，电子诉讼平台的深度应用正在重构司法数据采集的方式和范围。司法数据采集逐渐从传统的线下模式向线上模式迁移[3]，这一变革不仅使得数据采集更加便捷、高效，还为构建更为全面、准确的“全息画像”提供了可能。

在司法数据采集过程中，个人信息内容呈现多元化特征。从数据属性维度，法院在身份认证中收集的个人信息，既有姓名、性别、职业等非敏感个人信息，也有身份证号码、手机号码等敏感个人信息；从数据来源角度，既有政府机构掌握的个人信息，也有网络服务商、网络运营商等商业机构掌握的个人信息，还有自然人所掌握的个人信息；从数据类型划分，既有资产类个人信息，比如手机号码、电话号码

等。^[4]这些数据不仅提高了司法程序的安全性和准确性，这些数据也有助于分析当事人的行为模式，为司法决策提供辅助信息。在数据采集方式上，电子诉讼平台通常采用自动化、智能化的手段进行。通过构建“全息画像”，法院可以更加深入地了解当事人的情况，从而做出更为公正、合理的判决。同时，数据采集还有助于提高司法效率，减少人为因素的干扰，确保司法程序的公正性和透明度。

2) 数据处理：从“个案管理”到“预测性司法”

从“个案管理”到“预测性司法”的演变过程，是数据处理技术在司法领域应用不断深化的体现，同时也反映了社会治理理念和司法实践的变革。

作为一种早期的数据处理方式，个案管理主要关注个体或特定案件的数据记录、分析和处理。在这一阶段，数据处理技术相对简单，主要依赖于人工操作和基础的计算机工具。个案数据通常被保存在纸张上或简单的数据库中，用于记录案件的基本信息和处理过程。这种管理方式虽然能够满足基本的案件处理需求，但在数据规模、处理效率和准确性方面存在明显局限。

然而，随着大数据时代的到来，个案管理的方式已经无法满足司法领域对于海量数据分析和预测的需求。此时，预测性司法应运而生。预测性司法是一种司法实践的总称，依托预测性算法挖掘数据之间的联系或模式，自动化预测刑事司法中的各种与法律相关的风险问题，如首次犯罪可能性、人身危险性、再犯风险性等各类具有法律意义的风险事项，并协助司法人员作出逮捕、起诉、缓刑等决策^[5]。这种预测能力为司法决策提供了更加科学、准确的依据，有助于实现风险防控和精准打击犯罪的目标。

预测性司法演进折射出社会治理理念和司法实践的深层转型。传统的司法实践主要关注对个体案件的公正处理，而预测性司法转向构建系统性风险防控体系。这种从被动裁断到主动预防的治理逻辑跃迁，既维护了法律适用的稳定性，又实现了司法资源配置效率与程序正义保障的协同优化^[4]。

3) 数据共享：打破“数据孤岛”现象

在国家大数据战略的背景下，各级司法机关及行政主管部门正迎来司法智能化升级和国家治理体系与治理能力现代化转型的历史机遇^[6]。检察机关推进多部门协同办案机制与司法数据资源共享，既是深化检察系统整合、提升法律监督效能的关键路径，更是实施智慧检务战略的核心基础。这种机制创新通过构建数据互联平台，不仅强化了监督体系的整体性，更为构建数字时代的法治监督格局提供了制度保障和技术支撑^[7]。当前政法机关信息化建设呈现出“纵向通畅、横向阻隔”的特征。各级办案机关虽已构建起本系统内的数字化工作平台，实现业务条线数据贯通，但部门与部门之间的数据无法互联互通，数据壁垒依然存在。由于技术、管理和法律等多方面的障碍，这些数据被分散存储在各自的信息系统中，形成了一个个数据孤岛，导致海量数据的价值难以真正释放其效用。

在多重现实背景的挑战下，司法数据共享仍在不断突破和探索中。近年来，随着信息技术的飞速发展和政法系统数字化改革的深入，各地政法机关围绕司法数据共享进行了积极的探索，推动形成“数据互认、业务互通”的新型治理格局。例如，甘肃、浙江、贵州、江苏等地已基本建设完成政法系统大数据共享协作平台。上海市浦东新区立足引领区建设，建立浦东新区执法司法大数据信息协同共享机制，积极探索跨部门执法司法大数据开放共享和系统集成^[7]。在司法数据融通实践中，标准化数据治理框架的构建发挥着关键作用，实现了政法机关与政府行政部门之间一定程度、一定范围的工作协同和业务数据共享。这些平台通过统一的数据标准和规范，确保不同司法机关或部门之间可以无缝对接和共享数据。

4) 数据公开：司法透明新纪元

个人信息保护和数据安全在信息社会中也成为越来越重要的司法公开价值取向。有学者认为，“一直以来，司法公开都不是司法的核心价值，其在本质上不过是实现其他司法价值的手段或工具”^[8]。

司法数据公开意味着司法机关依法将审判流程、裁决依据、执行动态等核心司法信息，通过社交媒

体、官方网站等渠道向公众开放[9]。这一举措不仅有助于提升司法透明度，还能有效防止司法腐败，保障公众的参与权、知情权、参与权和监督权。同时，司法数据的公开还能为政策制定、学术研究提供宝贵的数据支持。

国际司法透明化进程中，司法信息公开制度的建设已成为法治现代化的重要维度。以我国司法改革实践为例，我国最高人民法院通过“中国裁判文书网”等平台，实现了全国范围内裁判文书的在线公开。该平台运行数据显示，截至2025年3月，中国裁判文书网已达到了千亿级访问量，为社会公众获取司法决策依据提供了便捷通道。此外，一些地方还尝试将执行信息公开、庭审直播等纳入司法数据公开的范畴，进一步拓宽了公开的广度和深度。

2.2. 现存问题与风险

1) 采集阶段：数据采集范围过度扩张

作为特殊类型的个人数据，诉讼信息采集应遵循最小必要原则。然而当前司法大数据平台普遍要求收集力求大而全，在未建立精准的采集边界定义机制情况下，司法实践中存在数据过度采集问题。首先，信息类型泛化存在泛化趋势，司法数据采集从传统的身份信息扩展至生物识别数据、包括在线诉讼操作轨迹在内的行为数据、社会关系数据等；其次，对收集信息的场景延伸至如法院安检闸机、移动执行终端等智能设备实时采集位置、活动轨迹等非必要信息；最后，尚未对因司法活动产生的相关个人信息有效地对数据进行脱敏处理和数据清洗，造成不必要的泄露。

2) 处理阶段：司法大数据画像的算法歧视

算法歧视的制度化则是另一大隐忧。司法人工智能系统若持续训练于带有历史裁判偏差的数据集，长此以往，算法歧视将逐渐制度化，进一步加剧司法不公现象[9]。

2013年威斯康辛州检方对埃里克·卢米斯(Eric Loomis)提起五项刑事指控，涉及拉克罗斯(La Crosse)驾车枪击案。尽管卢米斯否认直接参与枪击行为，但司法记录显示其承认在案发当晚后续时段实际控制涉案车辆。最终通过辩诉交易程序，被告人仅对“未经车主同意而驾驶汽车罪”与“企图逃避交通官员罪”两项轻罪作出有罪答辩。该案因涉及算法风险评估工具COMPAS的司法适用问题，成为美国刑事司法领域算法透明性争议的典型案例，引发了关于算法决策工具是否符合正当程序原则的违宪审查争议[10]。

量刑辅助系统虽然在提升裁判质效方面具有一定价值，但是预测性司法可信度通常是有赖于运作原理的透明和可解释的。[11]相比之下，量刑辅助系统的决策过程往往难以追溯和解释算法的运行规则对于普通人来说很难充分理解，这可能导致司法裁判过程的缺乏透明度，从而对司法公信力产生一定影响。在司法大数据画像的生成过程中，当事人往往无法知晓算法是如何运作并生成风险评估的，这种缺乏透明的情况违反了《个人信息保护法》第二十四条的规定，即自动化决策应保证透明。¹作为数据主体的当事人，有权了解自己的个人信息是如何被处理和使用的。然而，在当前的司法大数据画像应用中，这一权利往往无法得到充分保障。侵害知情权不仅损害了当事人的合法权益，还可能影响公众对司法系统的信任。因此，加强算法透明度和保护当事人知情权，是司法大数据画像应用中必须重视的问题。

3) 共享阶段：信息共享平台的安全防控与第三方外包的责任真空

信息共享是大数据侦查效能提升的重要因素。其平台建设通过强化数据资源整合能力，有效满足了侦查机关跨层级、跨部门的协同办案需求。然而，数据的高度集中存储也同步放大了安全防控压力，攻击者利用系统漏洞实施入侵的风险显著增加，公民个人敏感信息及案件数据面临更高泄密概率。这种安全脆弱性进一步催生了地下数据交易等灰色产业链。尽管公安机关在信息共享实践中已构建数字水印嵌

¹ 参见《中华人民共和国个人信息保护法》第24条规定。

入、访问权限分级控制及操作留痕审计等多重技术防护体系，但是公安民警利用职务便利实施的违规查询、批量导出及黑产勾连等违法行为仍屡禁不止，[12]如李某某侵犯公民个人信息案²、聂某某和董某等侵犯公民个人信息案³等。这类内部信息泄露问题暴露出权限管理机制的结构性漏洞，成为侵蚀公民信息安全的新型风险点。

除此之外，第三方服务商的失控也是司法数据安全的一大隐患。司法机关不具备专业的数据处理保存能力，在数据处理能力相对有限的情况下，司法机关就需要委托或引入第三方企业参与开发建设，有些数据甚至需要委托第三方企业代为保管。这种技术外包模式在提升系统研发效率的同时，也导致敏感数据流转环节增多，部分司法机关甚至将包含公民生物特征、财产信息等核心要素的司法数据库委托至第三方服务器，使数据泄露的潜在危害突破传统监管边界。

以杭州互联网法院及其数据保存单位杭州安存网络科技有限公司作为典型样本，其研发的“安存语录”在阿里云、腾讯云等9大云端保存了超过2.9亿次语音通话记录，云存储平台储存了超过56.8亿封电子邮件、超过5000亿条借贷、抵押等金融信息[12]。如此海量个人信息数据，若保管存储不当，将会产生巨大的安全问题。

4) 公开阶段：匿名化失效问题

司法裁判文书的公开机制在践行司法透明原则的同时，也潜藏着对当事人权益的侵害风险。鉴于文书中往往记载着当事人身份信息、案由经过及裁判结果等完整案件要素，当涉及婚姻纠纷、债权债务等敏感案件时，未经脱敏处理的公开文书无疑会造成公民的个人信息泄露。裁判文书上载明的个人信息和相关事实一旦披露，有的会对当事人的声誉造成一定的影响[13]。实践中，有些已公开的裁判文书会列明详细的个人基本资料与身份信息。如“刘文超袭警案”的裁判文书详细载明了被告人的姓名、性别、出生日期、居民身份证号码、民族、文化程度和户籍所在地。⁴更有甚者，即便采用姓名隐匿等初级脱敏手段，攻击者仍可基于“外部数据+模糊信息”的关联方式破解这种匿名，出现匿名化失效的情况。例如在某抢劫案件中，公开判决书隐去了被害人姓名，但基于其记载了被害人姓氏及“省交通厅厅长”职务信息及案件时空特征等信息，新闻记者完成了被抢劫家庭的身份信息识别。⁵这种匿名化失效不仅只是个人信息泄露问题，完整身份画像的泄露为网络暴力、精准诈骗等衍生犯罪提供作案信息，司法案例中的细节被商业化利用，可能引发对当事人持续性的骚扰与名誉侵害。最后，这种数据失控现象将严重削弱公众对司法公开制度的信任基础，形成数据安全治理领域的恶性循环。

3. 个人信息保护的优化路径

3.1. 法律规制：分类分级与院企协作的双轨机制

司法数据分类分级制度是一个细致且严谨的体系，旨在平衡司法透明度与个人信息保护、国家安全之间的关系。需以《中华人民共和国数据安全法》为基准框架，构建司法领域专项数据治理体系。重点推进《人民法院数据安全管理办法》实施细则的制定，系统优化司法数据全生命周期管理机制，特别针对数据分类分级、数据交互、数据集纳管理等核心环节，形成覆盖采集、传输、存储、应用全链条的技术标准体系，实现司法数据安全防护的标准化与精细化升级。例如，《人民法院数据安全管理办法》将法院司法数据分为一般数据、重要数据、核心数据三个等级和业务领域、所属范围等五大维度，在此基础上可进一步建立清单制的数据保密和开放共享动态目录，并明确不同等级与类别数据的差异性管理要求，

² 参见苏州市虎丘区人民法院(2017)苏0505刑初332号刑事判决书。

³ 参见北京市第三中级人民法院(2019)京03刑终47号刑事判决书。

⁴ 参见北京市朝阳区人民法院(2021)京0105刑初3012号刑事判决书。

⁵ 参见安徽省合肥市中级人民法院(2018)皖01刑初12号刑事判决书。

避免出现以保密为由的数据垄断行为[14]。

在司法数字化建设过程中同时也离不开第三方技术支持，但涉司法数据的“院企”协作机制尚存在完善空间，亟需构建系统化的供应商监管体系，对其进行事前、事中、事后全流程管理。在准入阶段，需构建多维评估体系，重点核查企业综合资质、行业信用等级、过往项目实施成效及数据安全防护水平。其中应设立专项核查指标，着重验证服务商在涉密数据处理领域的技术积累与合规记录，同时，合作条款须明确签订专项保密条款及合规数据处理契约，通过法律文本固化各方权责，将法律风险防患于未然。在事中管理环节，需重点构建全流程管控体系。一是贯彻数据最小化原则，限定供应商仅获取必要数据并严格约束使用范围，禁止超限处理或二次利用；二是强化技术防护，要求对传输与存储数据实施加密，必要时采用脱敏技术剥离敏感标识；三是建立分级访问控制机制，通过权限审批、操作留痕实现精准溯源。同步完善动态监管框架，定期开展安全评估与合规审计，确保防护措施符合现行法规要求。同时须强制供应商制定应急预案，明确安全事件即时通报义务与应急处置流程。此外，应将数据安全培训纳入合作约束条款，确保相关人员掌握规范操作要求，系统性提升风险防范能力。在事后阶段，需完善违约追责与退出机制。供应商违反数据保护义务时须承担赔偿责任、解约等法律责任，并明确退出规程，强制其在合作终止后彻底销毁或安全移交全部敏感数据，消除残留风险。

3.2. 技术治理：隐私增强技术的司法嵌入

技术治理在司法领域的深入应用，特别是隐私增强技术(Privacy-Enhancing Technologies, PETs)的嵌入，通过技术手段实现数据“可用不可见”，是平衡司法效率与隐私保护的关键工具，为数据的保护与利用开辟了新的路径。

近年来，区块链和联邦学习(federated learning, FL)广泛应用于分布式场景下的数据共享。联邦学习是一种分布式机器学习方法，旨在实现在不将参与方的私有数据上传到中央服务器的情况下，以隐私保护的方式交换中间模型参数，从而协作完成分布式任务。当前，联邦学习的研究主要集中在如何保护隐私和确保安全性方面[15]。在医疗领域，针对医疗数据共享中的“数据孤岛”问题，就提出一个基于联邦学习的医疗数据共享与隐私保护方案。而差分隐私技术是一个重要的隐私保护手段，其采用对数据添加噪声的方法来保护隐私。卢云龙等设计了一个基于区块链和联邦学习的安全数据共享系统[16]，同时引入差分隐私(differential privacy, DP)用于抵抗成员推理攻击，增强系统的安全性。医疗数据与司法数据一样，具有高度敏感性和隐私性，在司法领域，通过结合区块链和联邦学习技术共享医疗数据，有助于推动司法数据跨部门跨机构安全共享和有效交流。

3.3. 协同治理：政府、协会、企业等多方联动

首先，要完善行业自律，激发市场内驱力。行业自律体系的现代化转型需构建政府监管与市场自治的协同治理框架。以中国互联网协会 2002 年颁布的《中国互联网行业自律公约》为制度原型，推动行业规范从单一道德约束向技术治理赋能升级。通过引入动态风险评估、合规认证等创新机制，建立“公约承诺 - 技术验证 - 信用披露”的新型自律模式。此类升级后的自律规范不仅要求成员企业恪守“最小必要”原则处理用户信息，更需通过定期安全审计与技术检测形成可执行标准，从而在法律监管体系外构建具备技术公信力的前置性防护层。

其次，公众赋能与公益诉讼，构建社会监督网。公众参与和公益诉讼机制的创新为数据安全治理注入新动能。检察机关通过开发“政务公开信息法律监督模型”等技术工具，构建政府信息公开的“智能防火墙”。以兴庆区人民检察院的实践为例，该模型运用 NLP 技术自动筛查政府文件中的敏感信息，对未脱敏文档启动行政纠错程序，形成“技术监测 - 检察建议 - 整改反馈”的闭环监督。在民事救济领域，

《个人信息保护法》确立的集体诉讼制度通过风险分担机制降低维权成本，其“举证责任倾斜”设计显著提升了违法成本，倒逼企业建立全生命周期的数据安全防护体系[17]。

4. 结语

进入数字化时代，大数据是生产资料，云计算是生产力，互联网是生产关系，数字技术是竞争的利器[16]。随着科技的飞速发展和数字化转型的深入，司法活动正经历着前所未有的变革。然而，我们也必须正视个人信息采集和智能设备应用所带来的挑战。如何在保障司法公正和效率的同时，确保个人信息的合法、安全和有效使用，成为了亟待解决的问题。本文提出了一系列措施和建议，包括加强法律法规建设、完善个人信息保护机制、提升公众个人信息保护意识等，以期在推动司法数字化转型的同时，切实保障个人隐私权益。

展望未来，随着人工智能、大数据等技术的不断发展，司法活动将进一步实现智能化、自动化和高效化。但同时也需要我们保持清醒的头脑，审慎应对技术变革所带来的挑战和风险。只有在确保个人信息安全和隐私权益得到充分保障的前提下，司法数字化转型才能持续健康发展，为社会的公平正义和法治建设作出更大的贡献。

参考文献

- [1] 习近平向 2022 年世界互联网大会乌镇峰会致贺信[J]. 中国人才, 2022(12): 7.
- [2] 王福华. 互联网司法的正义体系[J]. 中国法学, 2024(1): 124-144.
- [3] 洪延青. 数字司法中的个人信息保护[J]. 学习与探索, 2024(10): 75-82.
- [4] 徐梦醒. 大数据时代司法判决的可预测性研究[J]. 西部法学评论, 2017(5): 61-69.
- [5] 王禄生. 论预测性司法[J]. 中国社会科学, 2024(6): 80-99, 206.
- [6] 赵龙, 刘艳红. 司法大数据一体化共享的实践探微——以破除“数据孤岛”为切入点的逻辑证成[J]. 安徽大学学报(哲学社会科学版), 2019, 43(6): 130-138.
- [7] 赵珏. 执法司法大数据信息协同共享机制初探[J]. 中国检察官, 2022(23): 11-14.
- [8] 左卫民. 反思庭审直播——以司法公开为视角[J]. 政治与法律, 2020(9): 91-100.
- [9] 范明志. 论司法信息公开的“三重属性”及规则体系[J]. 法律适用, 2024(6): 92-109.
- [10] 江溯. 自动化决策、刑事司法与算法规制——由卢米斯案引发的思考[J]. 东方法学, 2020(3): 76-88.
- [11] 刘艳红. 人工智能的可解释性与 AI 的法律责任问题研究[J]. 法制与社会发展, 2022, 28(1): 78-91.
- [12] 詹建红, 侯刘果. 大数据侦查中个人信息保护的困境及其破解[J]. 经贸法律评论, 2025(1): 140-158.
- [13] 张建伟, 赵润卓. 司法文书公开向司法数据公开的转变及其规则构建[J]. 河北法学, 2025, 43(3): 53-68.
- [14] 卢荣婕. ChatGPT 赋能智慧法院建设: 机遇、挑战和规制[J]. 重庆邮电大学学报(社会科学版), 2024, 36(3): 83-93.
- [15] 赵婵婵, 马坤明, 石宝, 等. 基于差分隐私的自适应联邦学习隐私保护方案[J]. 科学技术与工程, 2025, 25(7): 2849-2855.
- [16] Lu, Y., Huang, X., Dai, Y., Maharjan, S. and Zhang, Y. (2020) Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT. *IEEE Transactions on Industrial Informatics*, **16**, 4177-4186.
<https://doi.org/10.1109/tii.2019.2942190>
- [17] 高志宏. 隐私、个人信息、数据三元分治的法理逻辑与优化路径[J]. 法制与社会发展, 2022, 28(2): 207-224.