

新兴科技浪潮下律师业务的破局与护航：拓展与风控之道

赵雅杰

河南良承（新乡）律师事务所，河南省新乡市，453000；

摘要：随着数字经济与人工智能的迅猛发展，新兴科技正深度重塑法律服务行业。律师既迎来技术赋能带来的业务拓展新契机，也面临技术风险引发的执业合规挑战。本文基于法律实务经验与行业观察，系统剖析新兴科技对律师业务的双重影响，深入探讨破局路径与护航策略，旨在为法律从业者提供兼具理论价值与实践意义的参考。

关键词：人工智能；法律服务；技术赋能；风险防控；数据合规；科技伦理

DOI：10.64216/3080-1486.25.11.059

引言

在数字经济与人工智能深度融合的时代大背景下，新兴科技如人工智能、大数据、区块链、云计算等，正以颠覆性的力量重塑法律服务行业的底层逻辑。律师作为法律职业共同体的核心成员，既站在技术赋能带来的业务边界拓展机遇前沿，也承受着技术风险衍生的执业合规挑战。如何在科技浪潮中实现业务创新与风险防控的动态平衡，成为律师行业可持续发展的关键命题。本文基于法律实务经验与行业观察，系统梳理新兴科技对律师业务的双重影响，深入探讨破局路径与护航策略，以期在法律从业者提供理论参考与实践指引。

1 新兴科技赋能：律师业务的机遇延展

新兴科技与法律服务的深度融合，突破了传统业务的时空限制与服务模式，为律师行业创造了三类核心增量空间。

1.1 技术驱动的服务类型创新

人工智能（AI）技术在法律领域的应用，重构了法律检索与文书处理的效率边界。以智能法律检索系统为例，借助自然语言处理技术与法律数据库的深度关联，它能在秒级完成跨法域、跨层级的法规条文与裁判要旨匹配，大幅降低信息检索成本。

《最高人民法院关于民事诉讼证据的若干规定（2019 修订）》第十四条明确电子数据的法定证据地位，结合《人民法院在线诉讼规则》第十六条关于区块链存证的效力认定规则，催生了“数字证据存证与质证”这一新型法律服务需求。律师可依托区块链不可篡改的特性，为客户提供电子合同签署、网络侵权取证等全流程技术合规服务，形成差异化的专业优势。例如，在知识产权侵权案件中，律师利用区块链存证技术，可快速固定侵权证据，提高维权效率，增强客户对律师服务的信任。

1.2 数据要素的合规需求爆发

大数据技术的普及使数据成为企业核心资产，但相关法律法规对企业数据管理提出了严格要求。《中华人民共和国个人信息保护法》（以下简称《个保法》）第六条“最小必要原则”与第十三条“合法性基础”的严格规定，要求企业在数据收集、存储、传输全链条建立合规体系。

实践中，企业对数据跨境流动合规（如《数据出境安全评估办法》第三条的风险评估要求）、用户隐私协议设计（需符合《个保法》第四条“可识别性”界定）等需求激增。这为律师拓展“数据合规顾问”“跨境数据流动专项服务”等业务提供了广阔空间。例如，某跨国企业计划将用户数据传输至境外服务器，律师可依据相关法律法规，为其制定详细的数据出境合规方案，包括进行安全评估、签订标准合同等，帮助企业规避法律风险。

1.3 智慧协同的服务模式升级

云计算与协同办公平台的应用，推动律师服务从“线下主导”转向“线上 + 线下”融合。例如，通过云端合同管理系统，律师可实时参与跨国企业的多语言合同谈判，同步完成条款审查与风险提示；借助智能合同审查工具（如基于自然语言处理的条款识别模型），可在 10 分钟内完成一份 50 页商业合同的风险点标注，效率较传统人工审查提升 80% 以上。

此类技术工具的引入，不仅优化了客户体验，更使律师能够将精力聚焦于复杂法律问题的策略制定，实现服务价值的阶梯式提升。比如，在处理大型企业的并购项目时，律师利用云端协作平台，可与团队成员、客户实时沟通，快速完成大量合同的审查与修改，提高项目推进效率。

2 技术风险外溢：律师执业的新型挑战

技术赋能的另一面是风险的复杂化与隐蔽化。律师在拓展新兴业务时，需警惕以下三类核心风险。

2.1 数据安全与隐私保护的连带风险

律师在提供数据合规服务过程中，不可避免接触客户的敏感信息（如用户个人信息、商业数据）。若因技术系统漏洞或管理疏漏导致数据泄露，可能触发《中华人民共和国数据安全法》第二十九条“数据安全事件报告义务”，甚至因“非法提供个人信息”被追究《个保法》第六十六条规定的行政责任或刑事责任。

例如，某律所因未对客户数据采取加密存储措施（违反《网络安全法》第二十一条“数据加密义务”），导致客户千万级用户信息泄露，最终被监管部门处以50万元罚款并公开通报，严重损害行业声誉。这一案例警示律师，在处理客户数据时，必须严格遵守相关法律法规，加强数据安全管控。

2.2 技术依赖与专业判断的失衡风险

AI法律工具的“结果输出”虽高效，但可能因算法偏见或训练数据偏差导致错误结论。例如，某智能合同审查系统因训练数据中缺乏新型金融衍生品条款，未能识别出“对赌协议”中的隐性违约条款，若律师完全依赖系统结论而未进行人工复核，可能因“未尽审慎义务”违反《律师法》第三条“以事实为根据，以法律为准绳”的执业原则，进而引发客户索赔。

这表明，律师在使用技术工具时，不能过度依赖，应保持专业判断能力，对工具输出结果进行人工审核，确保法律服务的准确性和可靠性。

2.3 跨境合规与监管套利的冲突风险

新兴科技业务常涉及跨国数据流动与法律适用冲突。例如，国内企业向境外传输用户个人信息时，需同时满足《个保法》第三十八条“安全评估或标准合同”要求与欧盟《通用数据保护条例》（GDPR）的“充分性认定”规则。若律师对境外法律理解偏差，可能出具错误的合规意见，导致企业面临境内外双重处罚。

《促进和规范数据跨境流动规定》第三条、第四条虽明确部分数据出境豁免情形，但具体适用需结合业务场景精准判断，对律师的跨法域知识储备提出了更高要求。律师需要不断学习和掌握国际法律法规，提高跨境合规服务能力。

3 破局之道：新兴科技业务的拓展路径

面对机遇与挑战，律师需从“技术适配、能力升级、生态构建”三方面系统推进业务拓展。

3.1 技术适配：工具引入与风险评估并重

律师应建立“技术工具准入 - 使用 - 评估”全流程管理机制。首先，选择符合《区块链信息服务管理规定》第九条“安全评估”要求的技术服务商，确保工具的合规性；其次，在使用AI法律工具时，需同步建立“人机协同”审查机制——由律师对系统输出结果进行“二次验证”，重点核查涉及人身权、重大财产权等核心条款的合法性；最后，定期对技术工具的准确性进行评估，若发现算法偏差（如对某类新型合同条款的识别率低于80%），应及时停用并与服务商沟通优化。

例如，某律所引入智能法律检索系统时，对多家服务商进行严格筛选，选择通过安全评估的产品。在使用过程中，要求律师对系统检索结果进行人工复核，确保法律意见的准确性。同时，定期对系统进行评估，根据评估结果与服务商协商改进，提高系统的性能和可靠性。

3.2 能力升级：培养“法律 + 科技”复合型团队

律师事务所需通过“内部培养 + 外部引进”双轨模式构建专业团队。一方面，鼓励现有律师学习数据安全法、算法伦理等科技相关法律知识（如参加《科技伦理审查办法（试行）》专题培训），掌握基础技术术语（如“哈希值校验”“脱敏处理”）；另一方面，引进具有计算机科学背景的法律人才，形成“技术解读 + 法律分析”的协同工作模式。

例如，某头部律所组建“数据合规部”，团队成员包括前网络安全工程师与资深民商律师。前网络安全工程师负责解读技术问题，资深民商律师进行法律分析，二者协同工作，可同时完成数据流动路径设计与法律风险论证，成为行业标杆。这种复合型团队能够更好地应对新兴科技带来的复杂法律问题，为客户提供更全面、专业的服务。

3.3 生态构建：联动科技企业与监管机构

律师应主动参与科技企业的合规体系建设，通过“嵌入式服务”深度理解技术逻辑。例如，为AI企业提供“算法公平性审查”服务时，需结合《生成式人工智能服务管理暂行办法》第六条“安全可信”要求，协助企业建立算法透明度报告制度；同时，积极参与监管政策研讨（如《人工智能生成内容标识办法》第十条“标识义务”的落地细则），通过行业协会反馈实务需求，推动规则与实践的良性互动，为业务拓展营造有利的政策环境。

比如，某律所与一家AI企业建立长期合作关系，为其提供全方位的合规服务。律所律师深入了解企业的算法技术，帮助企业制定算法公平性审查方案，建立透

明度报告制度。同时,律所律师积极参与行业监管政策研讨,将企业在实践中遇到的问题反馈给监管部门,为政策的制定提供参考,促进了行业的健康发展。

4 护航之策: 执业风险的防控体系

为实现业务拓展与风险防控的平衡,需构建“制度 - 技术 - 文化”三位一体的风控体系。

4.1 制度层面: 完善内部合规管理

律师事务所应依据《律师事务所管理办法(2018 修正)》第二十三条“执业管理制度”要求,制定《新兴科技业务操作指引》,明确数据处理、技术工具使用、跨境合规等关键环节的操作标准。例如,规定“接触客户敏感数据需经合规委员会审批”“AI 工具输出结论需附算法说明”等细则;同时,建立“风险预警清单”,针对数据泄露、算法偏见等高频风险设置触发条件(如单日数据访问量异常增长 30%),一旦触发即启动应急响应程序(如《数据安全法》第二十九条要求的“立即补救 + 报告”)。

某律所制定了详细的《新兴科技业务操作指引》,对律师在处理新兴科技业务时的各个环节进行规范。在数据处理方面,明确要求律师在接触客户敏感数据前,必须向合规委员会提交申请,说明数据使用的目的、范围和方式等。在 AI 工具使用方面,规定 AI 工具输出结论必须附算法说明,以便律师进行审核和解释。同时,建立风险预警清单,对可能出现的风险进行实时监控,一旦触发预警条件,立即启动应急响应程序,有效防范风险。

4.2 技术层面: 强化数据安全保障

在数据处理环节,严格遵循《个保法》第六条“最小必要原则”,仅收集与服务目的直接相关的信息;采用符合《网络安全法》第二十一条要求的加密存储、访问控制等技术措施,确保数据“存得稳、传得安”;对于跨境数据流动,利用《促进和规范数据跨境流动规定》第三条、第四条的豁免规则,合理设计数据出境路径,降低合规成本。

例如,某律所在处理客户数据时,严格按照最小必要原则进行收集,避免过度收集客户信息。在数据存储方面,采用加密技术对数据进行存储,防止数据泄露。在数据传输过程中,设置访问控制,只有授权人员才能访问数据。对于跨境数据流动,律所根据相关规定,合理设计数据出境路径,确保数据出境合规,降低企业的合规风险。

4.3 文化层面: 培育科技伦理意识

律师需将科技伦理融入执业理念,遵守《科技伦理审查办法(试行)》第三条“增进人类福祉、合理控制风险”的原则。例如,在为 AI 企业提供服务时,不仅要审查技术合法性,更需关注算法是否存在性别、种族等隐性歧视;在参与数据交易中介服务时,依据《数据安全法》第三十三条“审核数据来源”的要求,拒绝为“数据来源不明”的交易提供法律支持,维护行业的社会公信力。

某律所注重培养律师的科技伦理意识,定期组织律师参加科技伦理培训和学习活动。在为 AI 企业提供服务时,律师不仅关注技术的合法性,还对算法进行伦理审查,确保算法不存在歧视性问题。在参与数据交易中介服务时,律师严格审核数据来源,拒绝为来源不明的数据交易提供法律支持,赢得了客户的信任和社会的认可。

5 结语

新兴科技浪潮下,律师行业正经历从“经验驱动”到“技术赋能”的深刻变革。机遇与风险并存的背景下,律师需以“开放拥抱技术”的姿态拓展业务边界,以“审慎防控风险”的态度坚守执业底线。通过技术适配、能力升级、生态构建实现破局,依托制度完善、技术保障、伦理培育完成护航,最终推动律师行业在数字时代实现高质量发展,为法治中国建设注入科技与法律融合的新动能。在未来的发展中,律师应不断学习和掌握新兴科技知识,提高自身的综合素质和竞争力,更好地应对科技变革带来的挑战和机遇,为推动法律服务行业的创新发展贡献力量。

参考文献

- [1]《最高人民法院关于民事诉讼证据的若干规定(2019 修订)》(最高人民法院,2020 年 05 月 01 日)
- [2]《中华人民共和国个人信息保护法》(全国人民代表大会常务委员会,2021 年 11 月 01 日)
- [3]《中华人民共和国数据安全法》(全国人民代表大会常务委员会,2021 年 09 月 01 日)
- [4]《网络安全法》(全国人民代表大会常务委员会,2016 年 11 月 7 日)
- [5]《区块链信息服务管理规定》(国家互联网信息办公室,2019 年 02 月 15 日)
- [6]《中华人民共和国律师法(2017 修正)》(全国人民代表大会常务委员会,2018 年 01 月 01 日)

作者简介:赵雅杰(1990.11—)女,汉族,河南省长葛市人,本科。