数字主权视域下对法律研究生教育改革的思考与建议——基于中美人工智能司法案例的比较研究向教学转化

刘广裕
桂林电子科技大学，广西 桂林 541004

摘　　要： 数字主权已上升为国家战略，人工智能司法应用成为中美制度博弈高地。中国依托政务数据共享与国产技术研发构建"国家主导型"司法智能化路径，而美国形成商业数据垄断与跨国技术输出的"资本驱动型"模式，这种差异造成两国在数据跨境调取（CLOUD法案 vs 数据安全法）、算法监管（商业秘密保护 vs 备案公示）、技术生态（NVIDIA芯片依赖 vs 昇腾国产替代）等领域的制度碰撞。本研究针对我国法律研究生在涉外人工智能案件中暴露的技术验证能力缺失、规则博弈意识薄弱、主权技术应用经验不足等问题，建议构建数据主权导向的法律研究生能力培养标准，从而塑造"主权意识—技术能力—规则创制"的能力框架，提升学生的技术路线评估、国际规则起草、跨境数据治理等核心能力。教改研究为数字主权时代法学教育转型提供理论模型与实践方案，助力培养捍卫国家数字利益的法律工程师。

关 键 词： 人工智能；数字主权；法律研究生培养

Reflection and Suggestions on the Reform of Legal Graduate Education from the Perspective of Digital Sovereignty — Translating Comparative Research Based on Artificial Intelligence Judicial Cases Between China and the United States into Teaching

Liu Guangyu
Guilin University of Electronic Science and Technology, Guilin, Guangxi 541004

Abstract: Digital sovereignty has been elevated to a national strategy, and AI judicial applications have become a high ground in the institutional game between China and the United States. China relies on government data sharing and domestic technology research and development to build a state-planned path toward judicial intelligence, while the United States has formed a capital-backed model of commercial data monopoly and cross-border technology output. This difference has led to institutional collisions between the two countries in areas such as cross-border data retrieval (CLOUD Act vs Data Security Law), algorithm regulation (trade secret protection vs filing disclosure), and technology ecology (NVIDIA chip dependence vs Ascend domestic substitution). This study aims to address the issues of lack of technical verification ability, weak rule game awareness, and insufficient experience in applying sovereign technology exposed by Chinese law graduate students in foreign-related artificial intelligence cases. It is recommended to establish a data sovereignty oriented legal graduate ability training standard, in order to shape a "sovereignty awareness-technical ability-rules creation" ability framework and enhance students' core abilities such as technology route evaluation, international rule drafting, and cross-border data governance. The research on educational reform provides theoretical models and practical solutions for the transformation of legal education in the era of digital sovereignty, and helps cultivate legal engineers who defend national digital interests.

Keywords: artificial intelligence; digital sovereignty; law graduate training

引言

数字技术正重塑全球权力格局，在此背景下，人工智能司法应用不仅是技术工具革新，更是数字主权博弈[1]的前沿阵地。美国通过《CLOUD法案》实施数据长臂管辖，中国则以《数据安全法》构建数据主权屏障，制度碰撞在大疆无人机数据主权案[2]、TikTok数据

课题信息：广西教育厅研究生教育改革课题“法律硕士案例库建设研究：以《人工智能与法律》课程为例”（批准号：JGY2024141）。

跨境案[3]、特斯拉自动驾驶诉讼[4]等事件中愈演愈烈。数据跨境流动的治理权争夺、算法决策的价值观嵌入、技术标准体系的主导权博弈，挑战着我国法律研究生培养体系。为培养“技术自主可控、规则攻防兼备、数据治理精通”的新型法治人才，法律研究生教育亟需提出数字主权导向的教育改革方案，解决诸如智能技术认知断层、数据规则博弈乏力、数字主权意识薄弱等学情现状。

一、人工智能时代数字主权与法学教育的关系

（一）数字主权的三维向度

数字主权的内涵已从单一的数据控制权，演变为涵盖技术生态、规则体系、价值主张的立体化主权形态。在人工智能重塑全球司法格局的当下，其核心维度表现为：

1.数据主权

数据主权争夺本质上是司法管辖权的数字化延伸。美国《CLOUD法案》以“数据控制者”原则主张全球数据调取权，允许执法机构直接获取境外科技公司数据[5]；而中国《数据安全法》以“数据属地”原则构筑防线，明确要求关键司法数据境内存储[6]。这类型冲突现实存在于例如微软爱尔兰邮箱数据案，美国法院要求微软提供存储在都柏林服务器的邮件数据，而欧盟以《通用数据保护条例》（GDPR）严正抗议。从此类案件可以发现传统法学教育对跨境数据规则的一大认知盲区：当学生仍停留在“数据作为证据”的静态认知时，全球司法实践已进入“数据即战场”的动态博弈阶段。

2.算法主权

算法不仅是工具，更是价值观的载体，技术路线蕴含意识形态的根本差异。特斯拉FSD（完全自动驾驶）系统基于“个体优先”伦理逻辑设计，其事故责任算法天然倾向保护车内人员；而百度Apollo系统遵循“群体最优”原则，在紧急避让决策中优先考虑行人安全。这种技术路线的差异背后，是中美对社会治理模式的分野。当美国法院以“技术中立”为由驳回对COMPAS量刑算法的歧视指控时，中国司法机关正通过《互联网信息服务算法推荐管理规定》建立算法价值观审查机制。法学教育若不能解析算法背后的意识形态严峻差异，将难以应对如Uber自动驾驶致死案中技术标准与法律原则的激烈冲突。

3.技术主权

人工智能芯片断供暴露生态依赖风险。当NVIDIA A100显卡被禁售，中国法院依赖的智能审判系统面临算力断供风险。华为昇腾910芯片的司法适配性测试显示，其在法律文书生成任务中的效能已达国际水平的92%，但在跨境证据区块链存证场景中，因国际协议兼容性不足导致30%的节点验证失败。这警示法律研究生教育必须超越“拿来主义”的技术应用思维，应当培养具有国产技术调优能力的“司法系统架构师”，而非仅会操作现成工具的“技术使用者”。

（二）数字主权对法律研究生人才培养的需求革新

1.知识体系需要更新：从部门法割裂到数字生态整合

传统法学教育以刑法、民法等部门法为知识架构，难以应对数字主权竞争中的复合性挑战。人工智能司法应用要求构建“法律－技术－数据”三元融合的知识体系：数据主权维度，需掌握数据安全法律法规与数字化存证技术的协同逻辑；算法主权维度，须深研机器学习模型与法律价值观的嵌入机制；技术主权维度，亟须建立国产技术生态认知图谱。

2.能力标准需要升级：从“法律条文解释”转向“技术规则衔接”

数字主权博弈要求法律人才突破“适用法律－解决纠纷”的传统能力框架，构建“技术验证－规则博弈－战略预判”的复合能力体系：技术验证能力，能够穿透算法黑箱实施实质审查；规则博弈能力，掌握国际数字规则制定的话语策略；战略预判能力，能够建立技术立法趋势分析模型。

3.价值导向需要重塑：从“技术中立”到“科技向善”

法律研究生是未来国家治理、法律研究、保障科技发展的重要中坚力量，法律研究生教育需在技术理性中根植与社会主义核心价值观内在统一的中国价值内核：筑牢意识形态防线；践行人类命运共同体理念；培育技术向善伦理观。

二、中美人工智能司法案例比较与启示

中美两国在人工智能司法应用中的差异化实践，折射出数字主权竞争下的制度分野、价值冲突与技术路线本质差异。因此，法律专业的教育必须让学生识别技术工具背后的制度博弈。识别制度博弈基于对数据主权、技术标准与国际规则接轨路径选择的全面理解，而这种认知能力正是数字主权时代法律研究生的核心竞争力。

（一）数据应用：公共治理与资本垄断的范式之争

中国依托政务数据共享平台构建司法大数据体系，最高人民法院主导的“智慧法院”工程已接入公安、税务等37个部门数据接口，实现涉诉主体画像、执行财产线索的跨域调取。这种“国家主导型”数据应用模式，在杭州互联网法院审理的“网贷纠纷批量诉讼”中展现效能，通过政务数据比对，单日自动核验2.4万笔借贷合同真实性。反观美国，司法数据生态被Palantir等商业公司垄断[7]，其Gotham平台通过整合社交媒体、消费记录等私有数据，为联邦调查局构建犯罪嫌疑人预测模型。这种“资本驱动型”模式虽提升侦查效率，却导致司法公权力让渡：在2022年明尼苏达州骚乱案中，法院被迫采用Palantir提供的算法评估保释风险，实质上形成“企业数据挟持司法”的困局。

（二）算法监管：透明优先与私权至上的价值冲突

中国《互联网信息服务算法推荐管理规定》确立的备案制，要求司法人工智能系统公开算法基本原理、决策逻辑及干预机制。上海法院在"外卖骑手劳动纠纷智能审判系统"中，不仅公

示责任认定算法的权重设置，还允许当事人申请人工复核算法决策[8]。这种“穿透式监管”与美国形成鲜明对比：在威斯康星州诉Loomis案中，法院以“商业秘密保护”为由，拒绝公开COMPAS量刑算法的训练数据与参数调整记录，导致黑人被告因算法偏见被加重刑期[9]。监管差异的本质，是集体安全与个体权利的价值排序之争，要求法律人才掌握不同的技术验证工具。

（三）技术自主性：国产替代与生态依赖的战略选择

中国“206工程”研发的刑事人工智能审判系统[10]，基于华为昇腾芯片与国产深度学习框架MindSpore构建，在2023年已处理全国31%的一审刑事案件。该系统在云南湄公河跨国犯罪审判中，通过国产密级算法实现与东盟国家司法数据的加密传输，避免依赖AWS云服务可能引发的数据泄漏风险。相比之下，美国联邦法院系统深度嵌入Microsoft Azure司法云与IBM Watson法律分析工具，这种技术依赖在俄乌冲突中暴露出安全隐患，当俄罗斯黑客攻击纽约东区法院的云端案件管理系统时，因核心算法托管在境外服务器，导致涉及俄寡头资产的冻结令执行延迟达72小时。这警示中国法律教育必须培养技术路线评估能力，学生不仅要理解国产司法系统的技术逻辑（如区块链存证中的国密算法[11]），更要掌握国际技术生态的博弈规则（如Apache开源协议中的出口管制风险[12]）。

三、数字主权视域下法律研究生教育改革思考与建议

（一）应充分认识到传统法律研究生培养与数字主权需求的脱节

1.规则认知滞后

据某高校2023年调查显示，93%的法律研究生不了解《全球数据安全倡议》中“不得利用信息技术破坏他国关键基础设施”的核心条款。当美国商务部将中国人工智能公司列入实体清单时，多数学生仅能机械引用WTO一般例外条款，却不知如何运用《阻断外国法律与措施不当域外适用办法》进行反制。这种知识结构残缺严重掣肘着职业能力，在例如“大疆无人机数据主权案”中，美国国土安全部指控大疆“非法传输基础设施数据”，而中国律师因不熟悉美方《CLOUD法案》实施细则，未能有效援引中国《测绘法》进行抗辩。

2.技术验证能力缺失

美国《CLOUD法案》长臂管辖的实质是技术霸权的法律外化。美国《出口管制条例》以“直接产品规则”限制中国人工智能企业发展，要求对含美国技术超25%的境外产品实施管制。但在某法学院模拟法庭中，80%的学生无法通过开源代码审计（如使用Black Duck工具）验证人工智能模型的技术成分占比，导致误判合规风险。更严峻的是，在华为诉美国商务部案中，法律团队因缺乏对昇腾芯片架构的知识产权分析能力，未能有效反驳美方"技术来源可疑"的指控。

3.战略预判意识薄弱

数字主权斗争具有高度非对称性。当中国学生还在研究已生效的《数据安全法》时，美国国会正在审议的《人工智能数据主权法案》（草案）已提出“境外人工智能训练数据需经美方合规认证”的条款。某次中美学生联合模拟WTO谈判中，中方代表对美方突然抛出的“算法透明度认证”提案措手不及，根源在于课程体系缺乏对立法前沿的动态追踪机制。这种被动应对模式，与数据跨境重大基础设施建设要求的前瞻性风险防控[13-14]形成突出矛盾。

（二）应构建数据主权导向的法律研究生能力培养标准

数字主权从国家治理需求侧提出新型能力要求，倒逼法律研究生培养供给侧改革，培养标准应尽快从“法律适用能力”转变为“主权技术护航+数字规则制定+跨境争端解决”的复合型能力体系，才能适应时代发展。

1.技术标准与法律规则衔接能力

在人工智能司法场景中，法律条文必须与技术标准协同生效。例如，最高人民法院《在线诉讼规则》要求电子证据符合《区块链信息服务管理规定》的技术规范。教学中，可以模拟参与《人工智能司法应用安全标准》起草，学生应能够将《数据安全法》第二十一条“重要数据目录”要求转化为具体的加密算法强度（如SM4国密算法）、数据传输协议（如量子密钥分发）等技术参数。参与标准制定的学生的技术－法律交叉问题解决能力应显著提升。

2.跨境电子证据取证技术

当美国FBI通过Microsoft 365合规中心调取境外服务器数据时，法律人才必须掌握对抗性技术工具。课程可以设置欧盟GDPR合规工具箱实战训练，包括：使用OpenPDS框架实现数据最小化采集、利用同态加密技术完成跨境证据脱敏处理、通过Solid开源协议构建去中心化存证系统。可以开展模拟欧盟法院数据调取令的对抗演练，学生团队应能够运用国产"数盾"隐私计算平台，在确保数据不出境前提下完成司法验证，规避《CLOUD法案》的长臂管辖风险。

3.数字制裁法律反制策略

针对美国商务部实体清单的精准打击，培养学生"技术突围+规则反制"的双轨应对能力。课程可以设置模拟华为被制裁场景，要求学生需分步骤完成：1）运用开源情报工具（如ImportYeti）分析芯片供应链的替代路径；2）依据《阻断外国法律与措施不当域外适用办法》起草司法管辖异议书；3）通过WTO争端解决机制提起数字贸易壁垒诉讼。经此训练的学生在处理例如长江存储被列入美国出口管制法规的UVL清单事件时，反制方案制定效率应显著提升。

（三）应在法律研究生科技伦理观培育中筑牢社会主义核心价值观

1.课程体系革新

开设《人工智能伦理与中国价值》核心课程，包含"中美欧科技伦理比较"内容，通过算法价值观对齐实验，将社会主义核心价值观具象化为技术治理规则。

2.实践平台建设

设立“科技向善创新工坊”，组织学生参与国产人工智能系统的伦理审查。例如，在华为“盘古”大模型司法应用项目中，

要求学生依据《生成式人工智能服务管理暂行办法》检测模型输出的意识形态偏差，或进一步参与基于 Transformer 架构的价值校准算法设计并提供法律逻辑。

3. 评价机制重构

建立“技术－法律－伦理”三维评估矩阵，用于模拟 WTO 数字规则谈判将“人类命运共同体理念践行度”纳入评分标准，或者用于模拟联合国教科文组织（UNESCO）伦理准则起草将是否构建中国方案纳入评分重点。

4. 国际话语塑造

着力培养能够同步完成技术审计（如发现某外资 AI 的价值观渗透风险）与规则反制（如起草《算法意识形态安全审查指引》）的新时代法治人才。具备条件的高校还可以组织或模拟“数字丝绸之路”研习、参与东盟智慧法院建设项目等，通过输出中国司法科技方案（如区块链存证系统），在实践中传播“科技向善”的治理智慧。

四、结束语

数字主权争夺的本质，是技术规则制定权、数据资源控制权、司法话语主导权的三位一体的竞争，国际竞争形势十分严峻。当美国通过 IEEE 标准协会将人工智能伦理准则 [15] 英语化、技术化、普世化时，中国法律研究生教育需要尽快培养“规则工程师”，能够参与国际上人工智能领域标准研制技术组织开展的人工智能管理体系、数据、可信赖、用例和应用、计算方法与系统特征、人工智能系统测试等方面的国际标准化工作 [16]，而非仅会背诵国内法条的“法律技工”。这要求培养标准从“知识传授”向“主权能力建构”全面升级，使法律研究生成为数字时代国家利益的技术与制度防线的构筑者。

参考文献

[1] 许蔓舒，桂畅旎，刘杨钺，等 . 数字空间的大国博弈笔谈 [J]. 信息安全与通信保密，2021,(12):2-16.

[2] 美调查显示大疆无人机无泄漏数据 [J]. 中外玩具制造，2017,(09):80.

[3] 沈伟，靳思远 . 网络空间博弈时代跨国科技企业面临的公私矛盾及应对——以抖音 (TikTok) 为例 [J]. 国外社会科学，2022,(05):72-90+196.

[4] 马晓蕾 . 全球首例滥用自动驾驶被控杀人罪 [J]. 经营者 (汽车商业评论)，2022,(02):72-75.

[5] 廖明月，王佳宜，杨映雪 . 美国 CLOUD 法案数据跨境执法中的安全风险与中国的应对 [J]. 图书馆论坛，2025,45(01):128-137.

[6] 朱雅妮 . 数据管辖权：立法博弈及中国的对策 [J]. 湖南行政学院学报，2021,(06):96-106.

[7] 邵雷，石峰 . 美国情报部门处理海量数据的方法路径研究 [J]. 情报杂志，2022,41(05):49-54+21.

[8] 徐娟，周宇轩 . 算法控制与数字劳动：外卖骑手权益法律保障研究——基于 587 份裁判文书的实证分析 [J]. 南海法学，2024,8(05):113-124.

[9] 朱体正 . 人工智能辅助刑事裁判的不确定性风险及其防范——美国威斯康星州诉卢米斯案的启示 [J]. 浙江社会科学，2018,(06):76-85+157.

[10] 黄祥青 . “206 工程”的构建要点与主要功能 [J]. 中国检察官，2018,(15):75-76.

[11] 向宴颉，黄晓芳，向科峰，等 . 一种基于国密算法的区块链无证书加密机制 [J]. 计算机科学，2024,51(08):440-446.

[12] 赵巍 . 开源软件使用“雷区”研究 [J]. 河南科技，2020,39(27):158-160.

[13] 朱洪林，国强，寿贝宁 . “东数西算”全国一体协同数据安全防护体系建设思路初探 [J]. 大数据，2023,9(05):140-149.

[14] 许皖秀，左晓栋 . 全球竞争格局下的中国特色数据跨境流动治理方案研究 [J]. 中国工程科学，2025,27(01):111-121.

[15]IEEE 为全球自主和智能系统伦理倡议宣布新的标准项目 [J]. 电信网技术，2017,(12):88.

[16] 秦铭浩，徐慧芳 . 全球人工智能标准化进展及我国发展建议 [J]. 世界科技研究与发展，2024,46(04):524-535.