越南《人工智能法》述评

□ 张炎坤

2025年12月10日，越南国会表决通过《人工智能法》，自2026年3月1日起施行。该法共8章35条，是越南首次以专门立法形式对人工智能活动作出系统规范，填补了越南相关领域的制度空白，对各国探索系统化人工智能监管路径、推进人工智能治理制度化具有一定参考意义。

立法背景

近年来，越南将发展人工智能作为推进数字化转型和产业升级的重要方向，相关国家层面的制度布局持续推进。2021年，越南发布《2030年前人工智能研发与应用国家战略》，明确提出健全人工智能法律制度、完善数据和算力等基础设施、培育产业生态并拓展国际合作，同时设定到2030年在东盟处于领先位置、进入全球前列的发展目标。

这些国家战略在顶层设计层面对人工智能发展作出系统部署，也对制度供给提出了明确要求。随着人工智能技术和应用形态快速演进，单纯依赖分散的政策工具和部门规范，已难以为战略实施提供稳定、统一的制度支撑。在此背景下，越南制定《人工智能法》，以系统化法律规范回应风险治理与产业发展的双重需求，为人工智能战略落地提供了相对稳固的法律基础。

主要内容

构建人工智能风险分级治理框架

越南《人工智能法》以风险导向为统领，确立了人工智能系统分级分类、差异施策的治理框架。该法第9条按风险程度将人工智能系统划分为高风险、中风险和低风险三类，并将是否可能对生命健康、合法权益、公共利益和国家安全造成重大损害作为主要判断标准，同时要求结合人工智能系统的使用领域、用户范围和影响规模进行综合评估。

在制度运行上，该法第10条以提供者自行分类为起点，以主管机关通报和监督为支撑，要求中、高风险人工智能系统在投入使用前完成分类备案，明确规定检查方式随风险等级加重，从而使监管强度与风险水平相匹配。与此相衔接，该法第11条明确规定透明度义务，要求直接与人交互的人工智能系统明示其系统属性，并对人工智能生成或编辑的音频、图像、视频内容作出标识，避免公众对内容真实性产生混淆。

在风险处置与强化约束方面，该法第12条建立了事故报告与处置机制，明确人工智能系统开发者、提供者、部署者和使用者在严重事故发生时的协同责任，并赋予主管机关采取暂停、召回或重新评估等措施的权限。针对高风险人工智能系统，该法第13条、第14条引入合规性评估并强化管理要求，将合规性评估确立为投入使用的重要条件，并在数据管理、人类监督、技术档案留存和问责配合等方面提出更高标准。相较而言，该法第15条对中、低风险人工智能系统采取相对宽缓的制度安排，主要以透明度义务和必要的说明责任为约束，从而保持监管弹性。

夯实国家人工智能发展基础

越南《人工智能法》在规范路径上并未着力细化各类应用场景的具体规则，而是重点关注国家能力建设，通过基础设施、数据体系与核心技术布局，为人工智能安全发展和规模应用提供长期支撑。

在基础能力层面，该法将国家人工智能基础设施定位为战略基础设施，并在第16条明确其建设方向为统一、开放、安全且具备连接、共享和扩展能力的生态系统，强调由国家发挥导向、协调与保障作用。在此框架下，国家投资建设并运营面向公共服务的人工智能基础设施，覆盖共用算力与数据、训练测试平台和试验环境等方面，并同步布局基础模型、通用模型以及越南语和少数民族语言大模型等核心模型体系，以支撑科研活动、国家治理与创新创业。与基础设施建设相配套，该法第17条对服务于人工智能的数据库体系作出专门规定，要求国家数据库、部门数据库和地方数据库统一建立、更新并实现连接，在遵守数据保护与知识产权规则的前提下，为人工智能训练、测试、评估和应用开发提供数据支撑。该法第18条进一步规定将掌握核心人工智能技术确立为国家优先方向，聚焦通用模型、高性能计算与训练技术、人工智能硬件和半导体等关键领域，以增强技术自主能力并维护数字环境下的国家主权。

在发展动能层面，该法通过战略牵引、生态培育与资源配置机制，将前述能力建设转化为可持续的创新动力。该法第19条要求由政府颁布并定期审查更新国家人工智能战略，将技术、基础设施、数据与人力资源统筹纳入国家发展规划，并建立指标体系以评估发展水平。与此相衔接，该法第20条至第25条围绕市场培育、受控试验机制、发展基金、人力资源培养、联合集群建设以及对创新创业企业和中小企业的支持作出系统安排，形成覆盖研发、试验、应用与产业化的政策工具链条。

确立人工智能伦理与责任底线

越南《人工智能法》以价值约束和责任固化为主线，通过原则性、底线性规则回应人工智能广泛应用对权利保障与公共决策带来的挑战。其制度重点在于确立国家层面的伦理框架，并对公共管理与公共服务中的人工智能应用提出更高要求，防止技术介入稀释决策责任、冲击公平秩序。

在伦理框架建构层面，该法第26条确立了制定国家人工智能伦理框架的四项基本原则，包括确保安全可靠、避免造成生命健康与人格权益损害；尊重人权和公民权利、确保开发使用公平透明且无歧视；促进个人、社区和社会的福祉繁荣并实现可持续发展；鼓励人工智能研究开发和应用中的创造创新并强化社会责任，并要求该框架应根据技术演进、法律调整和治理实践变化适时审查更新。

在公共场景应用层面，该法第27条对在国家管理和公共服务中使用人工智能系统作出专门规定，明确责任不因技术介入而转移。要求人工智能系统不得替代依法享有决策权的主体，决策者仍应对人工智能辅助结果的审查与采用承担责任。对于高风险或者可能对人权、社会公平和公共利益产生重大影响的人工智能系统，使用机关还应制定影响评估报告，说明风险识别与控制措施，落实人类监督与干预机制，并依法公开相关内容。

形成人工智能监管与治理体系

在风险分级、发展支持和伦理约束等制度基础上，越南《人工智能法》以监督执法与责任追究增强约束力，以国家管理分工与协同运行提升执行效能，以规则衔接与国际合作拓展外部支撑，共同夯实人工智能监管与治理体系的运行基础，推动构建可执行、可问责、可协同的监管与治理体系，为法律实施提供了制度保障。

一是完善监督执法与责任追究机制，强化人工智能活动的法律约束。该法第28条明确人工智能领域的监督检查依照监察法律实施，主管机关有权对组织和个人履行法定义务的情况开展检查，并在必要范围内调取技术档案、运行日志和相关数据，同时要求监管活动遵守国家秘密、数据和知识产权保护等规定。在此基础上，该法第29条完善违法处理与损害赔偿规则，对违法行为设置行政、刑事和民事多层次责任，并针对高风险人工智能系统确立以部署者为核心的先行赔偿机制，部署者赔偿后可依协议向提供者、开发者等相关主体追偿，以此合理分配风险与责任。

二是明确国家管理分工，构建协同运行的人工智能治理结构。该法第30条明确由中央政府统一负责人工智能国家管理工作，科学技术部承担统筹实施职责，各部委和地方政府在职权范围内协同推进，形成上下贯通、分工明确的治理结构。围绕分工协同监管中信息和数据的调取、共享与使用，该法第31条进一步明确，依据该法规定获分派执行国家管理活动的国家机关、组织、个人，有责任对在执行任务过程中提供的信息、数据、商业秘密保密，包括法律规定的技术档案、训练数据、源代码和算法；组织、个人提供信息、数据必须确保必要性，与国家管理活动的范围、目的和内容相平衡，不得超出合理限度；提供的信息、数据必须按法律规定确保安全、保密。

三是促进规则衔接与国际合作，增强人工智能治理的开放性与稳定性。该法第32条对人工智能领域的国际合作作出原则性安排，鼓励在基础设施、数据资源、人力资源、科学研究和合规性评估结果承认等方面开展合作，为治理规则与国际体系衔接预留空间。

制度价值

越南《人工智能法》的制度设计对该国人工智能产业发展具有基础性意义，同时为区域治理与国际立法提供了可参照的制度经验。

一是为越南人工智能产业发展夯实制度基础。该法以风险分级治理为主线，将基础设施建设、数据资源配置和核心技术掌握明确为国家层面的法定任务，通过国家人工智能基础设施、国家数据库和核心模型研发等制度安排，降低应用门槛、实现安全可控。同时，该法明确公共管理和公共服务领域的人类决策责任不得被技术替代，为人工智能嵌入社会运行划定边界，有利于在扩大应用的同时防范系统性风险，增强人工智能治理的可持续性。

二是为越南人工智能治理规则的可预期性提供制度支撑。该法以风险分级为主线，将中、高风险人工智能系统的分类建档、告知披露和监管介入条件程序化，并通过留痕记录、事故报告和高风险人工智能系统评估等机制固化为可核验的执行路径，使责任链条、监管触发条件及后果指向更为明确。由此，有助于在制度起步阶段形成相对稳定的规则预期，降低因口径不明和标准不一带来的合规不确定性。

三是为国际人工智能立法提供可参考的制度样本。该法在制度结构上兼顾风险防控与发展促进，一方面以风险分级、透明度义务和责任追究机制回应人工智能安全与用户权利保护等共性治理议题；另一方面以国家战略、受控试验机制和发展基金等工具完善创新支持体系，形成风险约束与产业激励相互配合的制度组合。这种以国家能力建设为基础、以风险治理为约束条件的发展型立法路径，为其他国家统筹人工智能安全目标与发展目标提供了可观察、可借鉴的制度经验。

【本文系国家社会科学基金重大项目“支持全面创新的知识产权制度体系构建研究”（23&ZD161）的阶段性成果】

（作者单位：中南财经政法大学知识产权研究中心）

人工智能 治理规则

数据跨境流动诉讼中非物质损害的司法认定

——以TB诉欧盟委员会案为视角

□ 徐璟航

近年来，因数据跨境流动中违法行为引发的非物质损害诉讼呈显著上升趋势，其争议焦点集中于诉讼主体的适格性、赔偿范围的界定与量化以及因果关系的认定等。2025年1月8日，欧盟普通法院作出的TB诉欧盟委员会案判决，系该院首次在判例中确认自然人因数据跨境流动违法行为所导致的非物质损害具备可赔偿性，该损害范畴涵盖精神或权利侵害且无需证明实际经济损失。由此明晰了非物质损害范围，为欧盟《通用数据保护条例》第82条第1款中损害范围的界定提供了实践路径。判决中确立的赔偿范围等标准，也为全球司法机关应对数据跨境流动诉讼、强化数据主体权利保障提供了有益参考。

基本案情

2021年至2022年间，德国公民TB多次访问欧盟委员会运营的欧洲未来会议网站，并通过Facebook账户完成GoGreen等活动的注册与登录。访问期间，TB注意到使用Facebook登录的行为导致其个人数据被传输至美国Meta公司，并经由该网站部署的Amazon CloudFront内容分发网络进一步跨境传输至位于美国的亚马逊网络服务器。

鉴于美国当时尚未获得欧盟依据《通用数据保护条例》第45条所作出的充分性决定，TB于2021年11月9日向欧盟委员会提交信息申请，询问其个人数据的处理情况以及可能向第三国传输的情况。同年12月3日，欧盟委员会书面回应称，相关数据由位于卢森堡的AWS欧洲公司处理，未发生向欧盟以外接收方传输的情况。TB对上述回复不予认可，并于2022年4月1日再次提出申请，要求欧盟委员会提供包括Meta公司在内的第三方数据处理者的完整数据副本、数据传输链路的详细技术说明等内容。欧盟委员会于2022年6月30日以“重复性请求”为由复函，主张2022年4月的申请实质重复2021年11月之内容，且先前答复已满足“合理期限内”的法定要求，未进一步提供详细信息。

2022年6月9日，TB向欧盟普通法院提起诉讼，提出三项诉讼请求：一是撤销欧盟委员会将其个人数据传输至缺乏充分保护的第三国的行为；二是认定欧盟委员会侵害了其信息获取请求权；三是责令欧盟委员会向其支付1200欧元的非物质损害赔偿，其中800欧元是对其获取信息权利受到侵害的赔偿，400欧元是对其个人数据受到不当传输的赔偿。

裁判要点

根据欧洲议会和欧盟理事会《关于在欧盟机构、机关、办公室和办事处处理个人数据方面对自然人的保护以及这些数据的自由流动，并废除（EC）第45/2001号条例和（EC）第1247/2002号决定的条例》（以下简称《2018/1725条例》）第65条的规定，因违反该条例而遭受物质或非物质损害的个人有权获得赔偿，但须同时符合《欧盟运作条约》第340条第2款规定的非合同责任条件，即严重违反欧盟法律、实际且确定的损害，以及违约行为与损害结果之间存在直接因果关系，裁判围绕上述三个要素展开了司法认定。

第一，欧盟委员会作为数据控制者是造成非物质损害的责任主体。欧盟委员会通过设置“使用Facebook登录”的超链接，实质性触发了向美国Facebook实体的跨境数据传输行为，直接导致TB的姓名、IP地址等个人数据向第三方传输，若欧盟委员会作为数据控制者未及时切断其与第三方平台的数据流关联，即构成了《2018/1725条例》第46条项下的个人数据传输行为，责任主体明确指向欧盟委员会。由于欧盟委员会“使用Facebook登录”的行为创设了数据主体个人数据被跨境传输至第三方的条件，但其未遵守《2018/1725条例》等规则所设定的“充分性传输”和“适当保障措施约束”等要求，因此该违法行为已构成对欧盟数据跨境保护法律规则的实质性损害，欧盟委员会作为数据控制者应承担主要责任。

第二，TB的信息获取权受损不属于实际且确定的非物质损害情形。根据《欧盟运作条约》，数据主体受到非物质损害必须是实际存在且确定的损害，假设性或不确定的非物质损害不足以获得赔偿，而非合同责任项下的因果关系认定则要求数据控制者的违法行为是造成损害结果的直接且决定性原因。根据《2018/1725条例》第14条第3款和第4款的规定，数据控制者回复信息申请的时限为一个月，如果其决定不对申请采取行动，则应在一个月内告知申请者不采取行动的原因，以及向欧洲数据保护监督员投诉和寻求司法救济的可能性。该案中，欧盟委员会对2022年4月1日的信息申请处理因答复期限超时而违反了前述义务，但该时限延误并未对TB造成实际且确定的非物质损害，加之数据主体在2021年11月9日和2022年4月1日提出的申请基本相同，其在2021年12月已收到了对其信息申请的部分答复，这在客观上减轻了信息获取延误的影响。据此，由于TB未能提供证据证明信息延误导致了直接的损害结果，因此不属于欧盟非合同责任中的实际且确定的非物质损害情形。

第三，因数据跨境造成的个人数据安全风险状态与非物质损害结果存在因果关系。由于在Schrems II案后，美国尚未获得欧盟《通用数据保护条例》有关数据跨境的充分性决定，因此根据《2018/1725条例》第47条和48条的强制性要求，数据控制者需要承担更多的法定保障义务。但在2022年3月30日TB使用Facebook登录时，其IP地址被非法传输至在美国注册的公司，欧盟委员会未对传输过程实施有效管控，其提供的登录链接完全受制于Facebook的通用服务条款，导致TB无法获得《2018/1725条例》所规定的“可执行性权利”与“有效法律救济”，当欧盟委员会将处理权让渡于第三方且未嵌入自主监管机制时，即构成对TB在个人信息处理和个人数据安全领域的“不确定性”风险，其与非物质损害结果之间的因果关系成立。根据UI诉奥地利邮政公司等案例，非物质损害的成立无需满足严重性阈值要求，只要数据主体因不当数据处理而陷入“持续性不安状态”，且该状态具有“实际且确定”的特征，即构成《通用数据保护条例》第82条所指的损害情形。

综上，欧盟普通法院基于公平原则，判定欧盟委员会向TB支付400欧元，作为TB因2022年3月30日登录欧盟网站时遭受违法行为而产生的非物质损害赔偿。

启示思考

在《通用数据保护条例》生效之前，欧盟各成员国法院在数据主体权利受到侵害情形下的损害赔偿范围及量化标准问题上长期存在分歧。其根源在于司法实践中的物质损害赔偿通常具备客观的计算标准，而非物质损害赔偿则通常需要基于主观评估，因此，何种不利影响可构成数据保护权项下的法律损害，以及如何合理确定赔偿数额以实现充分补偿等问题成为欧盟数据保护司法实践中的关键难点。该案所确立的裁判规则为上述争议提供了具有实效性的裁判路径。

一是在数据权利诉讼中对非物质损害的程度认定应避免设定严重性阈值。司法实践在确定个人数据信息的非物质损害程度时不能简单适用统一量化标准，而应综合考量侵权行为的性质、所涉数据的敏感度、数据主体的个体特征及潜在衍生风险，以实现数据保护权与司法救济权的实质平衡。若过度严苛化损害标准，将导致轻微或难以量化的损害情形被排除于司法救济之外，违背《通用数据保护条例》第5条合法、公平、透明原则的立法本意。该案表明，非物质损害的构成要件应为“真实且可证明的身心干扰”，损害程度无需量化，但须通过客观证据予以验证，同时还应考虑所涉数据的性质及其在数据主体生活中的重要性。若数据主体能证明数据控制者的违法行为导致其对个人信息的控制权持续性丧失，可以认定该“不确定性”风险与非物质损害之间的因果关系成立。

二是数据处理违法行为本身并不必然构成可赔偿的非物质损害结果。在欧盟有关非合同责任的法律框架下，损害赔偿责任通常以违法侵权行为或对受保护权利的不法侵害为前提，因此在认定非物质损害责任时，必须对侵权行为与损害结果这两个独立要件进行严格区分，即违法行为是责任前提，损害结果是赔偿基础。此外，《通用数据保护条例》第82条将违法行为、损害结果及因果关系并列为责任成立的要件，进一步表明在司法实践中不能简单将违法行为等同于可获赔偿的损害。欧盟既有判例亦对此予以明确，例如AS公司诉欧洲共同体理事会案指出，若就欧盟机构的侵权或违法行为主张损害赔偿，还需满足“对保护个人的上位法律规则的严重违反”的条件。

三是非物质损害赔偿以过错的可归责性判定为原则，以补偿性数额为限度。《通用数据保护条例》第82条第1款确立了以过错为基础的责任制度，即在确定数据控制者或处理者是否应承担赔偿责任时须考察其是否存在过错，但在计算损害赔偿的具体数额时，过错的严重程度一般不影响对非物质损害的认定与衡量。因此过错仅用于验证违法行为的可归责性，而在赔偿计算阶段则须剥离过错程度的影响，避免将“故意违法”等主观因素异化为损害扩大的理由。但也存在例外情形，根据《通用数据保护条例》第82条第3款的规定，数据控制者或处理者如能证明其对于损害的发生无需负责（例如因不可抗力所致），则应免除赔偿责任。根据损害赔偿中的比例责任原则，《通用数据保护条例》第82条规定的赔偿请求权具备的是补偿性而非惩罚性功能，因此根据该条款判处的赔偿金应严格限于损害补偿范围，而不应扩展至惩罚性或威慑性金额。

（作者单位：浙江省高级人民法院）

案例纵览