个人信息安全保护的民事制度研究

徐洁

华东政法大学，上海市，200042；

摘要：数字经济时代，以人工智能、大数据、云计算为代表的新一代信息技术不断取得新突破。在信息产业快速发展的同时，如果个人信息保护不足，可能带来风险，不仅会损害个人权益与人身安全，还有破坏社会信用体系的隐患。尽管《个人信息保护法》、《数据安全法》等法律已出台，但配套实施细则仍不健全。本文结合现行立法、司法实践与学术前沿，首先梳理个人信息保护的法律框架；其次，从技术标准脱节、预防性机制缺失、维权成本与收益失衡等制度困境进行分析；再次，有针对性地提出相应的完善路径；最后，总结制度创新对数字经济与法治社会的意义。

关键词：个人信息；数据安全；数字经济；数字技术

DOI：10.69979/3041-0673.25.08.079

引言

近年来，国内以人工智能、大数据、云计算为代表的新一代信息技术不断取得新突破，推动了数字产业的快速发展。在信息产业快速发展的同时，如果个人信息保护不足，可能带来风险，不仅会损害个人权益与人身安全，还有破坏社会信用体系的隐患。为充分保障个人信息安全，维护公民在网络空间的合法权益，有必要加强对个人信息安全保护的民事制度研究。

1 个人信息安全保护的现状

1.1 个人信息的界定

美国将个人信息表述为“个人隐私”，欧盟将个人信息称为“个人数据”，我国 2021 年正式实施的《个人信息保护法》第四条对“个人信息”的概念加以阐述：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。从“个人信息”的一般规定来看，个人信息包括但不限于：姓名、性别、联系方式、出生年月、家庭住址以及生物学性信息如身高、指纹、血型、脸型、虹膜等。

1.2 个人信息安全保护的立法概况

1994 年，国务院发布的《中华人民共和国计算机信息系统安全保护条例》首次提到个人信息保护问题。此后互联网快速发展，有关的法律法规不断出台：2017 年正式施行《中华人民共和国网络安全法》；2019 年正式出台《中华人民共和国密码法》；2020 年正式施行《个人信息安全规范》，同年，《民法典》正式颁布，在民事基本法中进一步明确了个人信息保护的基本原则和规则；2021 年正式公布施行《中华人民共和国数据安全法》，同年，《个人信息保护法》正式颁行，全面系统规定了个人信息的处理规则，开启了我国个人信息保护法治新篇章。

1.3 个人信息安全保护的民事法律规定

《民法典》第 1034-1039 条，明确个人信息权益的民事权利属性，强调“合法、正当、必要”的处理原则，并将信息安全纳入人格权保护范畴。

《个人信息保护法》第 9 条、第 51 条进一步要求处理者采取技术措施和管理制度以保障信息安全，同时通过第 69 条过错推定原则强化民事赔偿责任。

2025 年 5 月 1 日起实施的《个人信息保护合规审计管理办法》进一步细化企业合规要求，要求处理超千万用户信息的企业每两年至少开展一次合规审计，并引入第三方独立评估机制。

2 现行民事制度的实践困境

2.1 技术标准与法律规则的脱节

2.1.1 标准制定与法律效力的衔接不足

技术标准作为法律规则的技术支撑，其制定主体多元，而法律规则的制定主体具有法定性，两者在程序规范上存在差异。实践中，技术标准常滞后于技术发展，且缺乏法律强制力。

例如，虽然《个人信息保护法》援引了部分个人信息安全技术标准（如数据加密、匿名化处理），但未明确其法律属性，导致其司法裁判中技术标准的适用效力模糊。此外，技术标准与法律规则在“合规性”要求上可能存在冲突。

2.1.2 司法实践中标准适用的不确定性

技术标准在司法裁判中常作为“参考依据”而非“裁

判依据”，法官因技术理解能力不足，难以对标准的具体适用进行实质性审查。在个人信息泄露案件中，法院往往依赖第三方检测机构的标准评估结果，可能引发裁判偏差。同时，部分标准因缺乏强制约束力，企业合规动力不足，进一步加剧法律规则与行业实践的割裂。

2.1.3 标准更新与法律稳定性的矛盾

技术迭代速度远超法律修订周期，导致标准内容与法律规则动态脱节。例如，《个人信息保护法》要求数据处理者采取“必要措施”，但具体措施的技术标准（如数据存储期限、跨境传输安全要求）因技术变迁频繁调整，法律条文难以同步细化，造成企业合规成本高企与法律预期不稳定。

2.2 预防性责任机制的缺失

2.2.1 风险预防责任的立法空白

现行民事制度以“损害填补”为核心，对个人信息安全风险的预防性责任缺乏系统规定。例如，《民法典》第 1038 条虽规定信息处理者的安全保障义务，但未明确“风险预防”的具体内涵（如风险评估、实时监控等），导致司法实践中对“未履行预防义务”的认定标准模糊。

2.2.2 归责要件与因果关系的模糊性

个人信息侵权的隐蔽性和技术性使得传统侵权责任要件（过错、因果关系）难以适用。例如，算法歧视或数据泄露可能涉及多方主体（开发者、运营者、第三方服务商），但现有法律未明确预防性责任的分配规则，导致责任主体难以界定。此外风险预防责任要求对“潜在损害可能性”进行证明，但个人用户往往缺乏技术能力举证，形成维权障碍。

2.2.3 企业合规激励机制不足

现行制度对企业主动采取预防措施（如隐私设计、数据加密）缺乏正向激励，依赖事后惩罚。例如，欧盟《通用数据保护条例》（GDPR）通过“数据保护影响评估”制度推动企业事前合规，而我国《个人信息保护法》第 55 条虽引入类似机制，但缺乏实施细则和配套标准，企业合规成本与收益失衡，执行效果有限。

2.3 维权成本与收益失衡

2.3.1 举证责任分配不合理

个人信息侵权案件中，个人需证明信息处理者存在过错及损害后果，但技术壁垒使得用户难以获取关键证据。尽管《个人信息保护法》第 69 条采用过错推定原则，但实践中法院对“过错”的认定仍依赖技术鉴定，鉴定费用高昂且周期长，加重原告负担。

2.3.2 损害赔偿计算困难

个人信息侵权的损害多为精神损害或潜在风险，难以量化。例如，数据泄露可能导致身份盗用、名誉损失，但现行法律未规定精神损害赔偿的具体标准，法院常以象征性赔偿结案，无法弥补实际损失，也无法震慑侵权方。

2.3.3 集体诉讼与公益诉讼机制不完善

我国虽在消费领域引入集体诉讼制度，但个人信息侵权案件因涉及人数多、地域分散，仍面临立案难、协调难问题。此外，检察机关提起的公益诉讼多集中于环境与食品安全领域，个人信息保护公益诉讼的受案范围与赔偿规则尚不明确，制约了规模化维权的可行性。

3 制度完善路径的建议

3.1 技术标准的法律化：强化标准与规则的协同治理

3.1.1 明确技术标准的司法适用效力

建议通过司法解释，将《个人信息安全规范》（GB/T 35273）等国家标准明确为司法裁判中过错认定的“法定依据”。例如，规定信息处理者若未达到标准中的技术要求（如数据加密等级、访问控制措施），可直接推定其存在过错（《个人信息保护法》第 69 条过错推定原则的延伸适用）。

另外，建议由网信部门联合标准化委员会定期评估技术标准的时效性，通过“法律授权+技术目录”形式（如《数据安全法》第 21 条数据分级分类制度）将核心标准纳入法律强制性规范进行联动更新，避免标准滞后导致的规则僵化。

3.1.2 细化技术门槛的法定标准

建议参考《个人信息安全规范》附录 A，明确匿名化处理需满足“无法通过额外信息识别特定自然人的技术标准，并将“可复原性测试”作为司法鉴定依据。例如，若企业宣称采用匿名化技术但未通过测试，则认定其未履行法定义务（参考《数据安全法》第 51 条）。

借鉴欧盟 GDPR 第 25 条“通过设计保护数据”原则，要求企业证明其技术措施已达到法定标准，否则承担不利后果。例如，在算法歧视案件中，企业需提交代码审计报告以自证合规。

3.1.3 未达标准的法律后果强化

扩张适用“推定过失”，比如在个人信息侵权案件中，若信息处理者未达到强制性技术标准，可直接推定其存在过失，减轻原告举证负担。例如，某 APP 因未按《个人信息安全规范》要求进行权限最小化设计导致数据泄露，法院可直接认定其过错。

建议形成行政处罚与民事责任的联动，将违反技术标准的行为纳入《个人信息保护法》第 66 条“情节严

重”的处罚范围，允许受害者在民事诉讼中援引行政处罚决定作为依据，形成“行政认定—民事追责”的衔接机制。

3.2 构建“预防+救济”双层机制：平衡风险控制与权益保障

3.2.1 预防性责任机制的法定化

建议在《民法典》侵权责任编中增设专门条款如“信息安全缺陷排除请求权”，赋予个人或检察机关在发现信息系统存在漏洞时，请求法院强制企业采取修复措施的实体权利。

建议由法院委托第三方技术机构评估系统风险等级并制定修复方案，企业未按期履行则按日处以罚款（如 GDPR 第 58 条行政强制措施）。同时，将未履行修复义务作为后续侵权责任中“故意或重大过失”的加重情节。

数据处理者应承担“强制警示义务”，在发现数据泄露或系统风险后，除向监管部门报告外，必须通过短信、弹窗等显著方式向用户披露风险内容及应对建议。未履行警示义务的，可在后续诉讼中直接适用惩罚性赔偿（参考《消费者权益保护法》第 55 条）。

3.2.2 分层赔偿标准的量化设计

（1）基础赔偿：按信息条数与敏感度系数计算

基数的确定，参考《民法典》第 1182 条“实际损失难以确定”条款，设定单条个人信息的基础赔偿额（如普通信息 10 元/条，敏感信息 50 元/条）。敏感度系数根据信息类型动态调整（如生物识别信息系数为 2.0，行踪轨迹为 1.5）。

在此基础上，可参考《最高人民法院关于审理人身损害赔偿案件适用法律若干问题的解释》第 22 条，授权省级高院根据地区经济水平发布年度赔偿基准，采用动态调整机制，避免“一刀切”导致的地区不公。

（2）惩罚性赔偿：引入“风险扩散倍数”

根据信息泄露规模（如涉及 10 万人以上）或企业隐瞒风险的主观恶意（如明知漏洞未修复），在基础赔偿上叠加 1-3 倍惩罚性赔偿。例如，参考 GDPR 第 83 条“全球营业额 4%”的处罚逻辑，假如某企业违规收集 100 万条人脸信息未警示，按敏感系数 2.0 计算，总赔偿额=100 万*50 元*2.0*2=2 亿元。

（3）集体诉讼与公益诉讼的赔偿金分配

可以借鉴美国加州 CCPA 集体诉讼制度，将赔偿金的 30%用于原告个体分配，70%纳入“个人信息保护基金”，支持技术研发、法律援助等公共利益项目。

4 结论

本文提出的技术标准法律化与“预防+救济”双层机制，旨在破解现行民事制度中技术规则滞后、风险控制薄弱与维权激励不足的实践困境。核心价值在于：

（1）推动数字经济的可信化发展，通过技术标准的法律化，降低企业合规的不确定性，增强数据流通的信任基础。引入分层赔偿标准与惩罚性赔偿机制，既可以遏制企业“侵权逐利”的冲动，又避免过度威慑抑制技术创新，符合数字经济“包容审慎”的治理需求。

（2）夯实法治社会的权利保障根基，预防性责任机制将权利保护节点前移，体现“风险社会”中法律对人格尊严的主动维护，呼应《民法典》第 111 条“个人信息受法律保护”的价值导向。技术标准与法律规则的协同治理，推动法治从“文本规范”向“技术赋能”转型，弥合法官技术认知鸿沟，提升法律适用的科学性与公信力。

从实践意义的角度，技术标准联动更新与风险警示制度将法律规制嵌入技术运行全周期，形成“标准制定—合规审查—风险预警—侵权追责”的闭环链条，实现从原来的“事后救济”变革为“全程控制”，是对治理范式的革新。

个人信息安全保护的民事制度创新，既是数字经济高质量发展的制度底座，也是法治社会实现“技术向善”的关键路径。本文试图通过技术规则与法律价值的深度融合、风险预防与权利救济的功能互补，构建兼具包容性与威慑力的治理体系，提供可行的数字治理方案。

参考文献

[1]吴丽洁：《大数据时代背景下基层社区公众个人信息安全保护路径研究》，载《法制博览》2022 年 6 月
[2]方媛 衡亮:《公民个人信息安全的法律保护研究》，载《文化学刊》2024 年 2 月
[3]洪延青：《数字司法中的个人信息保护》，载《学习与探索》2024 年第 10 期
[4]孙诗丹：《技术标准的法治逻辑与实现路径》，载《标准科学》2024 年第 5 期
[5]毛艳辉：《工程建设标准的法治化现状、成因及对策》，载《标准科学》2024 年第 7 期
[6]冷罗生 韩康宁：《环境民事公益诉讼中预防性责任之限缩适用》，载《中国政法大学学报》2024 年第 5 期

作者简介：徐洁（1985.8—），女，汉族，江苏无锡，中级经济师，本科，华东政法大学，研究方向：民商法方向。