引用格式：郗蕊，柳经纬. 网络安全法律引用标准：现状、问题与建议[J]. 标准化学报，2026(5): 16-24.
XI Rui, LIU Jingwei. The Reference to Standards in Cybersecurity Laws: Current Status, Issues, and Recommendations[J].Journal of Standardization, 2026(5): 16-24.

网络安全法律引用标准：现状、问题与建议

郗 蕊[1]　柳经纬[2*]

（1.北京警察学院；2.中国政法大学）

摘　要：【目的】网络安全规范体系由法律规范（法律、法规、规章）与技术标准构成，二者通过法律对技术标准的“引用”形成关联，共同发挥规制网络活动、防范网络安全风险的重要作用。本文旨在明确当前我国网络安全法律引用技术标准的现状与问题，提出针对性优化路径，以强化法律与技术标准之间的协同。【方法】采用法律文本分析法，系统梳理网络安全领域不同位阶法律文件（法律、行政法规、部门规章）中引用技术标准的数量、方式、范围等核心要素，归纳总结引用现状。【结果】网络安全法律引用技术标准存在四大突出问题：一是标准总引用率偏低，引用范围集中于少数强制性国家标准，大量推荐性标准、行业标准等未被充分纳入；二是在普遍性引用方式下，部分法律条文所指标准缺失或不配套，导致条文“虚置”；三是直接引用中存在法律与标准更新不同步的情况，既包括注日期引用未跟进标准修订，也包括无日期引用存在标准滞后制定的问题；四是引用标准的表述模糊不准确，未能清晰界定标准的制定主体、属性及范围。【结论】为破解上述问题，应构建分级引用规则，明确标准引用的层级与优先级；完善标准清单目录及公共查询渠道，提升标准可获得性；优先采用不注日期的直接引用方式，实现法律与标准的动态适配；统一引用表述规范，明确所引标准的类型与范围，从而提升网络安全法律引用标准的科学性、规范性与可操作性，完善网络安全治理体系。

关键词：网络安全法律；技术标准；引用；标准清单

DOI编码：10.3969/j.issn.2097-857X.2026.05.002

The Reference to Standards in Cybersecurity Laws: Current Status, Issues, and Recommendations

XI Rui[1]　LIU Jingwei[2*]

(1. Beijing Police College; 2. China University of Political Science and Law)

Abstract: [Objective] The cybersecurity regulatory framework comprises legal norms (laws, administrative regulations, and departmental rules) and technical standards. These two components establish connections through the “reference” of technical standards by laws, jointly undertaking the important responsibility of regulating network activities and preventing cybersecurity risks. This paper aims to clarify the current status and existing issues of technical standard references in China’s cybersecurity laws, and propose targeted optimization paths to enhance the synergy between laws and technical standards. [Methods] Adopting the legal text analysis method, this paper systematically sorts out core elements

基金项目：本文受国家社会科学基金重大项目“基于法治、国家治理和全球治理的技术法规研究”（项目编号：21&ZD192）资助。
作者简介：郗蕊，博士，讲师，研究方向为行政法、标准化法治、技术法规、网络安全法。
柳经纬，通信作者，教授，博士生导师，研究方向为民商法、标准化法治、技术法规。

such as the quantity, methods, and scope of technical standards cited in legal documents of different hierarchical levels (laws, administrative regulations, and departmental rules) in the field of cybersecurity, and summarizes the current situation of citations. [Results] The research identifies four prominent problems in the citation of technical standards by cybersecurity laws: firstly, the overall citation rate of standards is low, with the citation scope concentrated on a small number of mandatory national standards, while a large number of voluntary standards, industry standards, and other types of standards are not fully incorporated; secondly, under the general citation method, the standards referred to in some legal provisions are missing or incompatible, rendering the provisions "in a state of inaction"; thirdly, there is an asynchrony between laws and standards in direct citations, including dated citations failing to keep up with standard revisions and undated citations facing the problem of delayed standard development; fourthly, the expression of cited standards is vague and inaccurate, failing to clearly define the development entities, attributes, and scope of the standards. [Conclusion] To address the above issues, it is necessary to construct hierarchical referencing rules to clarify the hierarchy and priorities of standard citations; improve standard catalogs and public inquiry channels to enhance standard accessibility; prioritize the use of undated direct referencing methods to achieve dynamic adaptation between laws and standards; unify the norms for citation expressions to clarify the type and scope of cited standards. In this way, the scientificity, standardization, and operability of technical standard references in cybersecurity laws can be improved, and the cybersecurity governance system can be refined.

Keywords: cybersecurity laws; technical standards; reference; standard catalog

0 引言

网络安全（本文网络安全指的是狭义的网络空间安全，主要是网络信息系统、设备、通信等技术方面的安全，而非网络意识形态等内容方面的安全）是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。网络安全关涉政治安全、经济安全、军事安全等多领域，是构建国家安全体系的基础性要素[1]，因此被法律列为专项监管的对象；以网络安全为监管对象的法律即网络安全法律。同时，网络是否安全，是否存在危及国家安全、私人权利的风险，是一个技术问题，须依据有关网络安全的技术标准判定。网络安全法律（法律法规、规章）与网络安全技术标准通过前者"引用"后者的方式，形成网络安全的规范体系，共同发挥着规制网络活动，预防网络安全风险，维护国家安全、社会公益、个人隐私及财产安全的作用。

1 网络安全法律

网络安全法律是专门规制网络建设、运营、维护、使用以及网络安全监督管理活动的法律规范，旨在"保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展"。在我国，它主要指关于网络安全的法律、行政法规、部门规章。

法律层面：全国人民代表大会常务委员会2016年通过、2025年通过修改决定，2026年1月1日起施行的《中华人民共和国网络安全法》（以下简称《网络安全法》）是网络安全领域的基础性法律，其明确了网络安全的基本原则、网络运行安全、网络信息安全、监测预警与应急处置等内容。

行政法规层面：国务院1994年颁布、2011年修订的《计算机信息系统安全保护条例》（国务院令第147号）以及2021年颁布的《关键信息基础设施安全保护条例》（国务院令第745号）致力于细化网络安全的监管要求。《计算机信息系统安全保护条例》是我国第一部关于计算机信息系统安全的综

合性行政法规，规定了计算机信息系统使用单位的安全义务、计算机病毒防治管理以及网络安全事件报告等网络安全保护的基本制度框架。《关键信息基础设施安全保护条例》在《网络安全法》基础上，要求关键信息基础设施安全保护措施应与系统建设同步规划、同步建设、同步使用，定期进行安全检测和风险评估，优先采购安全可信的网络产品和服务；重要数据出境的，应按照国家网信部门会同国务院有关部门制定的办法进行安全评估。

部门规章层面：公安部、国家保密局、国家密码管理局、国务院信息化工作办公室四部门2007年制定的《信息安全等级保护管理办法》确立了网络安全等级保护制度，要求运营者按等级实施技术保护并接受监管。工业和信息化部、国家互联网信息办公室、公安部三部门2021年制定的《网络产品安全漏洞管理规定》要求产品提供者2日内向工业和信息化部报送漏洞信息，并限制漏洞披露行为。国家互联网信息办公室2021年修订、2022年发布的《网络安全审查办法》确立了关键信息基础设施运营者采购网络产品及开展数据处理活动的国家安全风险审查机制。国家密码管理局、国家互联网信息办公室、公安部三部门2025年制定的《关键信息基础设施商用密码使用管理规定》对关键信息基础设施商用密码的使用范围、使用要求、使用管理等方面作出了详细规定。

2　网络安全标准

网络安全标准是指基于网络空间的技术层，为确保网络信息系统与设备的安全、稳定和可靠运行，所制定的一系列技术规范和管理要求。网络安全标准从早期零散制定基础标准，发展到覆盖网络安全管理、技术、产品、评估、数据、个人信息等全方位领域，形成了网络安全标准体系，奠定了网络安全法律中网络安全等级保护制度、关键信息基础设施保护等制度实施的基础[2]。

从制定主体上看，网络安全标准有国家标准、行业标准、地方标准和团体标准、企业标准。一是国家标准，系属网络安全的基础性规范。例如，网络安全等级保护方面，GB 17859—1999《计算机信息系统安全保护等级划分准则》是强制性国家标准；GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》等推荐性标准和GB/Z 41288—2022《信息安全技术 重要工业控制系统网络安全防护导则》等指导性文件细化了网络安全等级保护的具体要求。二是行业标准，由公安部、工业和信息化部等行业主管部门制定，结合行业特点，对国家标准进行了补充和细化，增强了网络安全标准在特定行业的可适用性。例如，公安部归口管理的GA/T 2182—2024《信息安全技术 关键信息基础设施安全测评要求》。三是地方标准，由地方各级政府标准化行政主管部门根据本地实际情况制定，旨在解决区域性网络安全问题，填补国家标准和行业标准的空白。例如，北京市发布的DB11/T 1654—2019《信息安全技术 网络安全事件应急处置规范》。四是团体标准，由社会团体或产业技术联盟根据市场需求共同制定。具有灵活性强等特点，能快速响应新兴技术需求，为企业和市场提供更多选择。例如，中国电子学会发布的T/CIE 216—2024《信息安全技术 信息系统网络安全免疫框架 第1部分：概述》。五是企业标准，由企业自行制定，主要针对企业自身的业务特点和安全需求，具有较强的针对性和适应性。例如，深圳市永达电子信息股份有限公司编写的Q/YD 016—2020《网络安全检测系统》。

通过全国标准信息公共服务平台，按照关键词“网络安全”“信息安全”搜索，检索到国家标准568项，行业标准338项，地方标准108项，团体标准超400项，合计可达1 488项。国家标准分为强制性标准、推荐性标准，行业标准一般属于推荐性标准，但特定的行业标准因涉及人体健康、人身财产安全等因素而被纳入强制性标准的范畴，而地方标准均为推荐性标准。其中，

强制性国家标准有5项，分别为GB 17859—1999《计算机信息系统安全保护等级划分准则》、GB 42250—2022《信息安全技术网络安全专用产品安全技术要求》、GB 35114—2017《公共安全视频监控联网信息安全技术要求》、GB 45438—2025《网络安全技术 人工智能生成合成内容标识方法》、GB 44495—2024《汽车整车信息安全技术要求》。

国家标准设有标准清单目录，有《信息安全国家标准目录》（2018版）和《网络安全国家标准清单》（2024年版）2个版本。按照《信息安全国家标准目录》（2018版），信息安全国家标准分为九大类，分别为基础标准、技术与机制标准、安全管理标准、安全测评标准、产品与服务标准、网络与系统标准、数据安全标准、组织管理标准和新技术新应用安全标准。

3 网络安全法律引用标准现状

网络安全法律与网络安全标准通过“引用”建立联系，将两种规范连接在一起，构成统一的网络安全规范体系。网络安全法律引用标准，使得法律的强制性效力延伸到所引技术规范，确保人们在遵守法律的同时负有遵守法律所引技术规范的义务[3]。法律通过义务性规范规定了网络运营者的各项具体责任和要求，通过引用标准为保障网络安全提供了技术支撑[4]。“引用”揭示了网络安全标准法律效力的来源。

3.1 《网络安全法》引用标准

《网络安全法》中引用标准3次3条，即第十一条、第二十四条和第二十五条；采用普遍性引用方式，指明特定机构或具体领域内所有标准，不逐个列举标准名称；主要表述为“国家标准的强制性要求”。该法将标准纳入法律体系，作为网络建设、运营、产品和服务的技术准则，形成三类义务框架：第十一条以“国家标准的强制性要求”作为采取建设运营服务技术措施的基本准则；第二十四条将“国家标准的强制性要求”确立为网络产品与服务合格销售的市场准入条件；第二十五条进一步将“国家标准的强制性要求”作为网络关键设备和网络安全专用产品的安全认证检测依据。为落实第二十五条（《网络安全法》修订前第二十三条），国家网信办等部门联合发布《网络关键设备和网络安全专用产品目录》，并制定强制性国家标准GB 42250—2022《信息安全技术 网络安全专用产品安全技术要求》。该标准与配套的系列产品类别标准（如GB/T 20281—2020《信息安全技术 防火墙安全技术要求和测试评价方法》、GB/T 20275—2021《信息安全技术 网络入侵检测系统技术要求和测试评价方法》等）共同构成产品准入的技术门槛。

3.2 网络安全行政法规引用标准

《计算机信息系统安全保护条例》中引用标准2次2条，即第十条和第二十一条采用普遍性引用方式，指向计算机机房相关国家标准，形成义务性规范要求。《关键信息基础设施安全保护条例》中引用标准1次1条，即第六条采用普遍性引用方式，通过引用“国家标准的强制性要求”，为运营者在网络安全等级保护基础上采取技术保护措施和其他必要措施提供依据。其中，网络安全等级保护依据GB 17859—1999《计算机信息系统 安全保护等级划分准则》等强制性标准，而具体技术保护措施则需参照其他相关国家标准。

3.3 网络安全部门规章引用标准

公安部制定的部门规章《信息安全等级保护管理办法》引用标准20次11条，采用普遍性引用和直接引用2种方式。

采用普遍性引用方式的有4次4条，即第八、第十一、第二十、第二十四条，主要内容是要求运营、使用单位应当按照国家信息安全等级保护管理规范和技术标准，使用符合规定满足等级需求的信息技术产品，开展信息系统安全建设或者改建工作；同时公安机关依据有关标准发出整改通知。

采用直接引用方式的有16次7条，即第九、十、十二、十三、十四、二十五、二十九条。直接引用又分为2种。一是注明日期引用，引用标准时给出标

准名称，同时标出标准代号、顺序号和发布日期或版次；第十二、十三、二十五、二十九条采用注明日期引用。例如，第十二条采用注日期直接引用方式规定，在信息系统建设过程中，运营、使用单位应当按照GB 17859—1999《计算机信息系统 安全保护等级划分准则》等技术标准，参照GB/T 20271—2006《信息安全技术 信息系统通用安全技术要求》、GB/T 20270—2006《信息安全技术 网络基础安全技术要求》、GB/T 20272—2006《信息安全技术 操作系统安全技术要求》、GB/T 20273—2006《信息安全技术 数据库管理系统安全技术要求》、GA/T 671—2006《信息安全技术 终端计算机系统安全等级技术要求》等技术标准同步建设符合该等级要求的信息安全设施。二是不注明日期引用，引用标准时给出标准名称，但仅标出标准代号和顺序号，不标出发布日期或版次。第九、第十条和第十四条采用不注日期直接引用方式，第九条规定信息系统运营、使用单位应当按照《信息系统安全等级保护实施指南》具体实施等级保护工作，第十条规定信息系统运营、使用单位应当依据本办法和《信息系统安全等级保护定级指南》确定信息系统的安全保护等级。

综上所述，网络安全法律中引用标准的现象已日渐普遍，对网络安全监管和合规工作起到了有效的支撑作用。然而，不同位阶的法律在引用标准的规范上存在差异。由于直接面对监管实践，低位阶的部门规章在引用标准的数量上更多，且方式更为直接。

4　网络安全法律引用标准存在的问题

网络安全法律通过引用标准实现了法律规范与技术规范的衔接[5]，并使标准嵌入到法律规范范畴。按照法律规范的本质属性，引用标准的法律条文应该具备形式体系性、概念统一性、操作明确性等特征。但当前网络安全法律引用标准的条文尚存在标准的总应用率不高、普遍性引用标准与法律不配套、直接引用标准与法律不同步、引用标准的内涵表述不准确等问题，导致现行引用条文陷入“虚置”的状态。

4.1 标准总引用率低

从前文数据统计来看，虽然网络安全标准数量众多且体系逐渐完善，但在《网络安全法》、网络安全行政法规和网络安全部门规章等各位阶法律文件的引用中，与庞大的标准库相比，标准的实际引用数量占比极为有限，引用范围也未覆盖全面。

从制定主体看，网络安全法律主要引用的是国家标准，特别是强制性国家标准，大量推荐性国家标准、行业标准、地方标准和团体标准均不在引用范围内。以法律层面的《网络安全法》和行政法规层面的《关键信息基础设施安全保护条例》为例，所引标准表述为“国家标准的强制性要求”，实质指的是强制性国家标准。据全国标准信息公共服务平台搜索关键词统计，总标准合计超1 488项，强制性国家标准为5项，推荐性国家标准、行业标准（包括强制性行业标准）、地方标准及团体标准等1 483项不属于被引标准；据《信息安全国家标准目录》（2018年版）统计，总标准数为268项，仅GB 17859—1999为强制性国家标准，267项推荐性国家标准不属于被引标准；《网络安全国家标准清单》（2024年版）378项国家标准中，仅GB 17859—1999为强制性国家标准，377项推荐性国家标准不属于被引标准。推算可知，法律引用标准的范围只有强制性国家标准，总引用率约为0.3%。至于引用标准数量较多的部门规章，以《信息安全等级保护管理办法》为例，以《网络安全国家标准清单》（2024年版）378项国家标准为总标准数进行统计，直接引用标准16项，引用的范围为国家标准，总引用率不超4%。

从内容来看，网络安全法律主要引用的是网络安全专用产品、网络安全系统建设与检测等领域标准，众多与网络安全相关的技术、管理、评估等方面的标准未能被充分涵盖。《网络安全法》第二十四条和第二十五条的法律条文内容涉及网络

服务、网络产品、网络关键设备和网络安全专用产品，但在该领域所引用标准限于强制性国家标准，故实际引用标准为GB 42250—2022《信息安全技术 网络安全专用产品安全技术要求》这1项，且只涉及网络安全专用产品这一类，其他类别标准未被涉及；部门规章层级的《信息安全等级保护管理办法》直接引用的16项标准主要针对网络信息系统建设、运营、保护等专业领域。就网络安全法律整体而言，除网络安全专用产品和网络安全等级保护之外的其他领域标准未被引用。

这种引用数量低、引用范围窄的情况，使得网络安全法律在实施过程中，无法全面借助现有的标准体系来保障网络安全。众多先进的网络安全技术标准、管理标准等不能及时、有效地转化为法律实施的技术支撑，影响了网络安全法律的全面性和有效性。同时，这也限制了网络安全治理能力的进一步提升，无法充分发挥标准在网络安全领域的技术规制作用，不利于国家网络安全战略的全面实施和网络安全治理体系的完善。

4.2 普遍性引用下标准与法律不配套

网络安全法律采用普遍性引用方式引用标准时，法律条文引用标准的指向不明晰，标准不能与法律适配，致使法律条文“虚置”。例如，在法律层面，《网络安全法》第二十四条规定“网络产品、服务应当符合相关国家标准的强制性要求”，第二十五条规定“网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求”，这里引用的标准应解释为网络产品、网络服务、网络关键设备和网络安全专用产品的强制性国家标准。但实际上，在《信息安全国家标准目录》（2018年版）分类中，第五部分“产品和服务标准”涵盖网络关键设备、网络安全专用产品、网络服务等标准，序号为125至176条，共计52项标准，全部为推荐性标准，并非第二十四条与第二十五条所引用的强制性国家标准；在《网络安全国家标准清单》（2024年版）中，没有专门指向网络产品、网络服务、网络关键设备和网络安全专用产品的标准；目前，只有公安部负责归口管理的GB 42250—2022《信息安全技术 网络安全专用产品安全技术要求》与之对应，该标准并非由全国信息安全标准化技术委员会（TC 260）制定，因此尚未收录于网络安全国家标准清单目录。即使GB 42250—2022《信息安全技术 网络安全专用产品安全技术要求》符合法律条文引用的标准范围，且在其“前言”中明确表示：“本文件为贯彻《网络安全法》第二十三条（现为《网络安全法》第二十五条）而制定……”，但该标准仅解决了第二十三条中关于“安全专用产品”的引用问题，只覆盖条文的一半内容，另一半内容则因网络关键设备无对应标准可引用，致使第二十五条缺乏完整标准支撑而“虚置”；同理，第二十四条因网络产品、网络服务无对应标准可引用而“虚置”。

在行政法规层面，《计算机信息系统安全保护条例》也存在类似问题。其中，第十条明确规定计算机机房应符合国家标准及国家相关规定；第二十一条规定，若计算机机房不符合国家标准和其他国家相关规定，或者在计算机机房周边施工对计算机信息系统安全造成危害时，由公安机关协同有关单位进行处理。第十条和第二十一条相互对应，所引用标准应解释为关于“计算机机房”的“国家标准”，既涵盖强制性国家标准，也包括推荐性国家标准。然而，在相关目录和清单中均无专门针对“计算机机房建设的国家标准”。故而，第十条和第二十一条因缺乏对应标准支撑而“虚置”。

4.3 直接引用下法律与标准不同步

在网络安全法律引用标准时，直接引用存在法律与标准不同步的问题。首先表现为，采用注日期直接引用方式下，法律所引标准一旦有更新版本，若法律规范不及时修订则无法与最新版本标准保持同步，致使法律适用不规范。例如，《信息安全等级保护管理办法》第十二条在引用标准条款时采用注日期直接引用方式，要求在信息系统建设过程中，运营、使用单位应当参照GB/T 20272—2006《信息安全技术 操作系统安全技术要求》、GB/T

20273—2006《信息安全技术 数据库管理系统安全技术要求》。然而,《信息安全技术 操作系统安全技术要求》的GB/T 20272—2006版本已被GB/T 20272—2019版本替代、《信息安全技术 数据库管理系统安全技术要求》的GB/T 20273—2006版本已被GB/T 20273—2019版本替代,但《信息安全等级保护管理办法》却一直未修订,这就导致执法部门在指导检查计算机信息系统安全等级管理时适用法律不规范。

其次表现为,采用未注明日期的直接引用方式时,若法律颁布之际,其所引用标准尚未制定,则会致使法律适用出现标准空缺。例如,《信息安全等级保护管理办法》(公通字〔2007〕43号)是2007年6月22日发布,第九条引用的《信息系统安全等级保护实施指南》,最早版本GB/T 25058—2010《信息安全技术 信息系统安全等级保护实施指南》是2010年发布;第十条引用的《信息系统安全等级保护定级指南》,最早版本GB/T 22240—2008《信息安全技术 信息系统安全等级保护定级指南》是2008年发布;第十四条引用的《信息系统安全等级保护测评要求》,最早版本GB/T 28448—2012《信息安全技术 信息系统安全等级保护测评要求》是2012年发布。可以看到,在2007年6月至对应标准版本发布的时间段中,第九、第十条和第十四条并没有可供支撑的标准,法律条文处于"虚置"状态。

4.4 引用标准的表述不准确

法的本质属性要求法律概念具备明确性与统一性,这是法律规范体系逻辑自洽的基础要件。因此,网络安全法律规范中的关键概念须具有明确的内容指向,避免出现法律概念定义偏差导致适用冲突。但是,当前网络安全法律引用标准的条文中,标准类型表述较为模糊,既不能从制定主体上区分所引用的是国家标准、行业标准、地方标准还是团体标准,也不能从属性上区分是强制性标准还是推荐性标准。例如,《网络安全法》中引用标准的3项条文表述为"国家标准的强制性要求",不能清晰指明到底是强制性国家标准全文,还是国家标准中的强制性要求部分。这里涉及标准化界的"条文强制"问题。2000年2月,原国家技术监督局《关于强制性标准实行条文强制的若干规定》"二、强制性标准的形式,强制性标准可分为全文强制和条文强制两种形式:标准的全部技术内容需要强制时,为全文强制形式;标准中部分技术内容需要强制时,为条文强制形式"。2020年国家市场监督管理总局发布《强制性国家标准管理办法》(国家市场监督管理总局令第25号),第十九条规定"强制性国家标准的技术要求应当全部强制,并且可验证、可操作",第五十五条规定"有关部门规章中涉及强制性国家标准管理的内容与本办法规定不一致的,以本办法规定为准"。也就是说"国家标准的强制性要求"这一表述,在2000年实行"条文强制"的时期是有意义的;但在2020年《强制性国家标准管理办法》后,强制性国家标准的技术要求只能全文强制,不能条文强制。所以,《网络安全法》中的"国家标准的强制性要求"表述,应该指的就是强制性国家标准[6],且是全文强制。但这样的模糊表述致使法律与标准无法契合,法律条文处于"虚置"状态。

5 网络安全法律引用标准的优化建议

为提升网络安全法律引用标准的规范性、协同性与适用性,针对现有问题,提出以下优化路径。

5.1 建立分级引用规则,促进法律与标准有效联动

为解决法律引用标准范围不清、效力不明及更新脱节等问题,首先建议在网络安全法律体系内建立系统化的分级引用规则[7]。该规则可通过在法律中增设"技术规范引用"专章,或制定配套的实施细则的方式予以明确。具体而言,应依据标准的技术权威性、强制效力及适用范围,确立清晰的引用层级秩序:优先引用强制性国家标准与推荐性国家标准;补充引用推荐性行业标准;审慎引用技术内容成熟、确属必需的地方标准与团体标准。此分级规则旨在确保法律优先依托国家层面的权威标准,同时为特定行业或领域的特殊技术需求提

供必要的规范补充。

为实现法律与标准的长期协调，须同步建立联动修订机制。明确标准更新触发法律文本或引用清单评估修订的程序，确保法律所引用的标准体系能够与技术发展同步演进，从制度层面系统性化解因标准迭代而产生的适用滞后问题。

5.2 完善标准清单目录，提升标准可获得性

设置引用标准清单目录，系统列明法律所引技术规范的名称与编号，是明确被引标准范围、增强法律可操作性的关键举措。网络安全法律在引用标准时，应建立统一、权威的标准清单发布机制，系统梳理并持续更新网络安全相关标准的分类目录，涵盖国家标准、行业标准等主要类型，清晰标注其属性、效力状态与适用范围，以实现法律条文与技术规范之间的准确对应。

标准清单目录建议采用分层设置、协同配合的模式。例如，在法律层面确立核心标准清单，保障基础权威性。建议在《网络安全法》等基础性法律中，以附录形式设置一个相对稳定的核心强制性标准清单。该清单应列明支撑法律中最关键义务（如产品准入、关键信息基础设施保护）的少量强制性国家标准的名称与编号。在部门规章层面建立动态标准清单，确保灵活与全面。建议通过国家网信办、工业和信息化部等主管部门的规章或规范性文件，建立并维护一个全面、动态的引用标准清单。此清单应广泛涵盖法律授权引用的各类推荐性国家标准、行业标准等，并及时更新。

同时，通过建设权威的标准化公共查询平台，将此类清单及其对应的标准全文向社会公开，可显著提升标准信息的透明度与可获得性，确保监管机构、企业及社会公众在适用法律过程中能够及时、准确地获取所需技术依据，从源头上增强法律实施的有效性。

5.3 优先采用不注日期的直接引用方式，增强法律适应性

与普遍性引用方式易导致所引标准范围模糊、存在性难以确认不同，直接引用通过在法律条文中明确标注技术规范的具体名称与编号，能够确保被引标准的实际存在及其内容确定性。因此，在网络安全法律法规起草或修订过程中，建议优先采用不标注具体日期的直接引用方式，并注明这种方式所引标准指向的是最新版本，以解决法律的稳定性与标准更新之间的矛盾，保持法律与技术发展之间的动态协调。

例如，《网络安全法》第二十五条关于“网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求”之规定，虽意图引用具体技术标准，但因未列明标准编号，导致对应标准难以锁定。如能在法律规范附录中直接列明GB 42250—2022《信息安全技术 网络安全专用产品安全技术要求》等标准名称与编号，将显著增强条款的可执行性与法律指引的明确性。

5.4 统一法律引用表述，明确所引标准的类型与范围

针对《网络安全法》表述中存在的问题，建议修订关于“国家标准的强制性要求”的法条表述，减少使用“国家标准的强制性要求”等笼统表述，统一表述为“国家标准”，清晰表述所引标准的类型为国家标准，包括强制性国家标准和推荐性国家标准，实现法律与标准之间语义对齐。此外，在法律允许范围内，适度拓展对强制性行业标准等的引用，以扩大法律依托的技术依据范围，增强条文的可执行性，从而扩大标准引用范围和数量，提升总体引用率。

6 结 语

网络安全法律对技术标准的有效引用，是构建科学、完备的网络安全治理体系的制度基石。当前，我国已在法律引用标准方面形成初步框架，但在引用准确性、覆盖范围、表述规范与动态协调等方面仍存在明显短板，制约了法律实施效能与标准技术价值的充分发挥。通过建立分级引用标准规则、完善标准清单目录及获取渠道、采用不注日期的直接引用方式、规范引用范围表述等优化路

径，可以有效提升网络安全法律引用标准的科学性和合理性。

未来，随着网络技术的不断发展和网络安全形势的日益复杂，网络安全法律引用标准的机制也需要持续优化和完善。法律与标准的制定部门应加强协作，不断探索更加有效的引用机制和方法，以适应不断变化的网络安全需求，为网络空间的安全和稳定提供坚实的治理保障。

参考文献

[1] 曹诗权.习近平关于网络安全法治的重要论述研究[J].公安学研究,2018(1):1–23,122.

[2] 王秉政,上官晓丽.新时期网络安全国家标准化工作综述[J].中国信息安全,2021(2):65–66.

[3] 柳经纬.法律引用标准的三重意义[J].电子知识产权,2023(6):4–16.

[4] 柳经纬.论标准对法律的支撑作用[J].厦门大学学报（哲学社会科学版）,2020(6):152–162.

[5] 柳经纬.“法规引用标准”解释论:以关键词为中心[J].浙江大学学报(人文社会科学版),2024(5):59–70.

[6] 李佳,逄征虎.强制性国家标准的内涵和管理机制研究[J].标准科学,2021(11):10–15.

[7] 许林波,柳经纬.技术法规的规范性及其实现路径[J].甘肃社会科学,2024(5):175–187.