



公安部第三研究所

网络安全法律研究中心



全球网络安全政策法律发展年度报告

(2023)

公安部第三研究所网络安全法律研究中心

360 集团法务中心

2023 年 12 月



执行概要

信息技术革命的成就令人印象深刻，这并不仅仅是指生产力和生产关系的跃迁，而是触及社会运行底层逻辑的系统性变化。很少有法律议题像网络安全这般复杂且具有挑战性——这几乎涉及到过去、现在和未来人类想象力能够覆盖到的所有领域和场景——在任何语境下，能够被称之为“安全”的问题无疑最为核心且优先，其隐含了关于“生存和发展”的终极阐释，但“安全”本身的“主体间性”却往往令与此相关的法律议题陷于困惑，网络安全尤为如此。其中最为艰难的部分可能不仅仅在于找到某种可行的“安全”途径或方法，而且包括促进这种途径和方法在尽可能多的价值层面上形成共识或达成妥协。

基于后工业时代“风险社会”中那些显著“现代性特征”所揭示的经验和教训，网络安全几乎从一开始就成为与信息技术革命同步考虑的问题。在过去的三年中，人类社会向信息系统迁移的速度明显加快，新技术新应用不断出现。其中，尽管大部分的技术“外观”可能是陈旧的，但其技术“体验”绝对是全新的。站在实用主义的角度，由“人机交互”向“人机融合”的过渡已经渐成现实，“虚拟”与“现实”之间产生了几乎可以“触碰”到的紧密联系，这也导致全球网络安全政策立法整体态势在 2023 年出现了两个方面的显著变化。其一，社会公众对政策法律的“工具性价值”更为认同，这进一步强化了政府持续塑造和改良规范体系的内驱动力，促进全球网络安全政策立法的全面繁荣。其二，全球网络安全政策立法在表现出高度技术敏感性的同时，也开始修正早期为迅速填补规范空白而略带盲目性的“扩张”思路，对于技术利用与限制的平衡被更多的予以考虑。类似于在数据问题上全面复刻欧盟 GDPR 蓝本的情况已经很少出现，这可能预示了一个更为多元而审慎的网络安全政策立法态势。此外，鉴于技术自身的高速发展，“出台即过时”也成为决策者必须纳入考量的影响因素，这要求制度设计必须足够弹性，网络安全政策立法无疑将变得更为复杂。

回顾 2023 年，面对全球网络安全传统风险更加复杂多变与新兴风险多面出现相互交织的局面，各国政策立法总体呈现出优化调整、细化落实现有立法要求，使其适应新形势下风险防御新特点的同时，针对新兴风险提出突破性、前瞻性立法，并引入其他治理理念和工具，试图预判风险、提前规避。本报告全面回顾

2023 年全球网络安全政策立法与典型执法情况，将 2023 年全球网络安全政策法律发展总结为十大特点：（1）全球网络空间治理区域合作加强，共同安全成为关键词；（2）关键信息基础设施保护重者恒重，且向着细分领域下沉；（3）内生安全风险与外界政府干预共同加剧全球供应链安全风险；（4）漏洞资源价值持续凸显，激励漏洞披露与发现仍是关键环节；（5）数据精细化、场景化立法蓬勃发展，数据跨境成为关注焦点；（6）信任成为信息内容治理核心，未成年人保护与网络暴力为重点关切；（7）基于风险的人工智能法治趋于理性，软硬法协同推进向善包容治理；（8）监管行动持续推进，聚焦平台与规模效应的网络执法效能日渐突出；（9）安全与发展辩证关系在量子技术推进与后量子密码迁移中深刻诠释；（10）网络犯罪预防、打击、治理一体化基本共识形成，防治相关立法加速推进。

展望 2024 年，信息技术发展与风险迭代升级相伴而生，技术利用与风险防范并行不悖，安全与发展的辩证统一将始终是各国网络安全对内治理和对外合作的底层逻辑。报告研判出 2024 年全球网络安全政策法律的六大趋势：（1）网络空间大国博弈背景下局部和暂时性妥协有望达成和延续；（2）数据赋能发展的制度保障仍需加强，跨境流动面临不确定性；（3）网络执法的精细化、专业化、智慧化水平将大幅提升；（4）人工智能包容性、参与式治理纵深发展；（5）新型网络犯罪治理趋向生态化、预防化、智能化；（6）后量子密码标准化将加速“特定重要”领域后量子密码迁移进程。



出品单位

公安部第三研究所网络安全法律研究中心

360 集团法务中心



指导单位

中国信息安全法律大会专家委员会

密码法治实践创新基地

中国计算机学会计算机安全专业委员会



参编单位

中国人民公安大学

西交苏州信息安全法学所

网络安全等级保护与安全保卫技术国家工程研究中心

信息网络安全公安部重点实验室

数字丝路安全智库

西交科教院网络安全法治研究所

上海市信息网络安全管理协会互联网安全法律服务专家委员会

江苏竹辉律师事务所

北京中企数安咨询有限公司



课题支持

2020 年度国家社会科学基金项目《网络安全新业态视角下的关键技术风险分析及防控对策研究》（20AZD114）



专家指导组

马民虎 密码法治实践创新基地 主任
严 明 中国计算机学会计算机安全专业委员会 主任
宋燕妮 全国人大常委会法工委经济室 原副巡视员
金 波 公安部第三研究所 副所长
张 薇 情报杂志 主编
焦 娇 360 集团副总裁/董事/法务部总法律顾问
吴松洋 公安部第三研究所 研究员
孙艳玲 360 集团 高级法务总监
吴佳丽 360 集团 法务总监
王斌君 中国人民公安大学 教授
鲍 亮 公安部第三研究所 副研究员
于月霞 宁夏公安厅网安总队 总工程师
朱莉欣 西交苏州信息安全法学所执行所长
尹鹏翎 励讯集团 数据战略官
赵 艳 华为中国区网络安全与隐私保护 总监
刘春梅 上海市信息网络安全管理协会 秘书长



总负责人

黄道丽 公安部第三研究所 研究员



执行负责人

梁思雨 公安部第三研究所 助理研究员
何治乐 公安部第三研究所 副研究员



报告撰写组

原 浩 马 宁 王彩玉 胡文华 胡柯洋
俞少华 王明一 洪慧英 方 婷 谢永红

目录



一、2023 年全球网络安全政策法律发展回顾 - 1 -

- (一) 全球网络空间治理区域合作加强，共同安全成为关键词 - 3 -
- (二) 关键信息基础设施保护重者恒重，且向着细分领域下沉 - 5 -
- (三) 内生安全风险与外界政府干预共同加剧全球供应链安全风险 - 7 -
- (四) 漏洞资源价值持续凸显，激励漏洞披露与发现仍是关键环节 - 9 -
- (五) 数据精细化、场景化立法蓬勃发展，数据跨境成为关注焦点 - 12 -
- (六) 信任成为信息内容治理核心，未成年人保护与网络暴力为重点关切 .. - 14 -
- (七) 基于风险的人工智能法治趋于理性，软硬法协同推进向善包容治理 .. - 16 -
- (八) 监管行动持续推进，聚焦平台与规模效应的网络执法效能日渐突出 .. - 18 -
- (九) 安全与发展辩证关系在量子技术推进与后量子密码迁移中深刻诠释 .. - 21 -
- (十) 网络犯罪预防、打击、治理一体化基本共识形成，防治相关立法加速推进 - 23 -

二、2024 年全球网络安全政策法律趋势展望 -26-

- (一) 趋势一：网络空间大国博弈背景下局部和暂时性妥协有望达成和延续 - 27 -
- (二) 趋势二：数据赋能发展的制度保障仍需加强，跨境流动面临不确定性 - 28 -
- (三) 趋势三：网络执法的精细化、专业化、智慧化水平将大幅提升 - 29 -
- (四) 趋势四：人工智能包容性、参与式治理纵深发展 - 31 -
- (五) 趋势五：新型网络犯罪治理趋向生态化、预防化、智能化 - 32 -
- (六) 趋势六：后量子密码标准化将加速“特定重要”领域后量子密码迁移进程 - 33 -

—

2023 年全球网络安全政策法律发展回顾

2023 年世界进入经济复苏的重要时期，全球新一轮科技和产业变革加速升级，以 ChatGPT、量子计算等为代表的颠覆性技术迭代更新，信息技术创新发展、数据价值最大化利用、人工智能通用化等技术带来的产业动能成为经济社会发展过程中的重要引擎，引发各国对其予以前所未有的关注。与此同时，随着不稳定、不确定、难预料因素的显著增多，新旧问题与复杂矛盾叠加碰撞，安全风险变得不总是“可见的”、可以预测的，未知来源、未知类型、未知后果风险的难以捉摸使得安全的内涵更加深刻。如果说防入侵、防泄露、防篡改等是网络安全的初期目标，那么在遭遇不论是内在风险，还是因政治、外交、贸易等外部风险时能够保持稳定、及时从风险中恢复则成为网络安全的长期目标。因此，韧性成为 2023 年网络安全领域的高频词汇。无论是关键基础设施韧性、产业链供应链韧性，还是《G20 领导人新德里宣言》提出“在数字经济中构建安全、保障、韧性和信任”，美国《国家网络安全战略》的“建立可防御性、有韧性的数字生态环境”目标，均致力于确保网络安全各环节在面对内生和外部风险时能够保持动态稳定。

作为固根本、利长远、稳预期的重要治理工具，法治在 2023 年仍然是各国强化网络安全的关注重点，通过立法引导、规范、支持信息技术发展和数据价值利用，保障网络安全。复杂多变的外部环境、法治建设的内在驱动与未来技术的迭代升级，推动全球网络安全领域政策立法和监管实践不断加强，采取的政策不仅寻求更佳的社会秩序，同时赋予法律更强的政策导向和工具属性。

回顾 2023 年，面对全球网络安全传统风险更加复杂多变与新兴风险多面出现相互交织的局面，各国政策立法总体呈现出优化调整、细化落实现有立法要求，使其适应新形势下风险防御新特点的同时，针对新兴风险提出突破性、前瞻性立法，并引入其他治理理念和工具，试图预判风险、提前规避。本报告将其总结为十大特点。

（一）全球网络空间治理区域合作加强，共同安全成为关键词

2023年是习近平主席提出构建人类命运共同体理念的十周年。网络空间命运共同体是网络强国重要思想的重大理论创新，为全球网络空间治理贡献“中国方案”。如《携手构建人类命运共同体：中国的倡议与行动》白皮书中所说“站在历史的十字路口，是团结还是分裂，是开放还是封闭，是合作还是对抗？如何抉择，关乎人类整体利益，也考验着各国的智慧。”2023年，尽管地缘政治变化所引发的国家间战略竞争仍然十分激烈，但越来越多的区域性合作开始被观察到，特别是诸如“集体安全”“共同安全”等一些极具“示范”意义的话语力量开始广泛出现。这意味着在信息技术和数字经济成为国家发展基本条件的大背景下，基于特定利益、信任或价值关系的国际合作的深度和广度都在持续加深。这也似乎建立了一种可预期的良好开端，或将为网络空间治理的各方参与者提供更多的机会。

联合国发布极具代表性的政策简报《全球数字契约》，旨在为全人类构建一个开放、自由和安全的数字未来，其中的一项关键目标就是弥合各国数字鸿沟并推进可持续发展。中俄发布《关于深化新时代全面战略协作伙伴关系的联合声明》，深刻指出应秉持普遍、开放、包容、非歧视和兼顾各方利益的原则，实现世界多极化和各国可持续发展。中俄呼吁各国弘扬和平、发展、公平、正义、民主、自由的全人类共同价值，对话而不对抗，包容而不排他，和睦相处，合作共赢，促进世界的和平与发展。美国在新版《国家网络安全战略》中明确提出建立网络空间国际伙伴关系，促进网络空间负责任的国家行为，重点包括共同应对数字生态系统威胁、提高合作伙伴抵御网络威胁能力、打造安全可靠和值得信赖的全球供应链。新西兰发布首份国家安全战略《共同安全》，其强调的优先事项就包括加强国内和国际伙伴之间的信任理解，共同合作应对挑战。澳大利亚、印度、日本、美国在《四方伙伴关系领导人联合声明》中指出，面对数字化世界中复杂的网络威胁，迫切需要共同加强集体网络安全。

此外，各国网络安全区域合作开始通过更为丰富而多元化的方式加以呈现，具有共识性的联合声明成为塑造国际规则和主张国家立场的重要渠道。例如，美欧就

加强网络弹性领域合作发表联合声明，拟在欧美网络对话框架下深化网络安全治理合作。美国和印度签署《美印关键和新兴技术倡议》，提出双方政府、企业界和学术界将致力于在加强两国间创新生态系统（人工智能、量子技术等）、建立有韧性的半导体供应链等领域展开密切合作。美国、日本发布联合声明，就可信数据自由流动和跨境数据流达成共识。美国、加拿大发布联合声明，寻求共同改善半导体供应链和关键基础设施安全。欧盟、拉丁美洲和加勒比发布《数字联盟联合声明》，旨在提升公民基本数字能力，缩小数字鸿沟。

需要承认的是，现有的网络安全国际合作具有强烈的地缘政治属性，合作各方通常具有明显的互信关系，某种意义上来说合作范围内的信任意味着对范围外的不信任，这可能引发更为激烈的区域冲突和对抗。个别国家将互联网作为维护霸权的工具，用集团性“帮规”破坏全球性互联网治理原则。典型如美国在全球范围内寻求合作伙伴共同限制芯片、半导体出口，这无疑将导致全球网络空间的主体间关系变得不再稳定，“进攻性”的政策法律会越来越多的出现，需要引起警醒。“信任”将在相当长的时间内作为全球网络空间治理的核心议题，这可能并不是单纯通过技术方案能够解决的。对此，我国持续致力于为动荡变化的时代注入更多稳定性和确定性，倡导通过对话达成安全共识。我国提出《全球安全倡议概念文件》，重申共同、综合、合作、可持续的安全观，提出战争和制裁不是解决争端的根本之道，对话协商才是化解分歧的有效途径。发布《中国关于全球数字治理有关问题的立场（就制定“全球数字契约”向联合国提交的意见）》提出面对数字化带来的机遇和挑战，各方应坚持多边主义，坚守公平正义，统筹发展和安全，深化对话合作，完善全球数字治理体系，构建网络空间命运共同体。中国-中亚峰会西安宣言发布，提出中国同中亚五国支持在《全球数据安全倡议》框架内构建和平、开放、安全、合作、有序的网络空间，共同落实好《“中国—中亚五国”数据安全合作倡议》，共同推进在联合国主导下谈判制定关于打击为犯罪目的使用信息和通信技术全面国际公约，合力应对全球信息安全面临的威胁和挑战。这些努力不仅体现了区域信任，更为如何寻求和搭建信任树立了典范。

（二）关键信息基础设施保护重者恒重，且向着细分领域下沉

2023 年，俄乌冲突、混合攻击激增以及北溪天然气管道破坏等不稳定因素对关键基础设施安全稳定运行带来挑战。欧盟网络安全局基于 2022 年 1 月至 2023 年 8 月期间发生的经验证的 310 起 DoS 事件分析发现，受此类事件影响最大的是政府行政部门，政府基础设施已经成为威胁行为者的首选目标，且 66% 的攻击事件是出于政治动因。美国网络安全和基础设施安全局（CISA）在 2022 年应要求对某大型关键基础设施组织进行红队评估，并最终获得了该组织敏感业务系统相邻系统的访问权限。CISA 表示尽管该组织拥有成熟的网络态势感知能力，但并未在整个评估过程中检测到红队行动。这使得**关键基础设施保护在 2023 年发布的国家战略中仍占据重要地位，各国普遍认识到关键基础设施面临着重大威胁，关基保护需要在立法、公私合作等方面进一步推进。**美国《国家网络安全战略》将“保护关键基础设施”列为战略确立的五大支柱之首，明确关键基础设施保护的目標是“运作持久且有效的协作防御模式，公平分配风险和责任，为美国数字生态提供基本安全和韧性。”对此，美国将创新机制，使关键基础设施所有者和经营者、联邦机构、产品和服务供应商以及其他利益相关方能够在速度和规模上有效地协作。美国国防部《2023 年网络战略》也表示将借助现有所有合法可用的合同机制、资源和业务安排来改善美国关键基础设施网络安全。欧盟 NIS 2 指令、《关键实体弹性指令》正式生效，为欧盟现代化网络安全保障提供制度基础。受北溪管道事件驱动，欧盟提出《关于〈协调联盟应对重大跨境关键基础设施中断的蓝图〉的理事会建议提案》，旨在提高对关键基础设施重大事件的态势感知、信息共享和有效响应。我国修订《反间谍法》，将间谍组织针对关键信息基础设施实施的网络攻击定义为间谍行为，进一步充实关键信息基础设施保护制度体系。

在总体战略指引和安全形势驱动下，各国关键基础设施保护开始走向精细化、行业化和专业化。近两年澳大利亚关键基础设施保护立法取得重大进展，2023 年进入细化立法要求阶段，发布《关键基础设施安全（关键基础设施风险管理计划）规则》《关键基础设施资产类别定义指南》等文件，明晰关键基础设施资产类别及其责任主体的安全保护义务。《2023-2030 年澳大利亚网络安全战略》将

“保护关键基础设施”列为保障网络安全的六大盾牌之一，旨在确保关键基础设施和政府基础系统能够抵御网络攻击并从中恢复。同时也表示尽管《2018 年关键基础设施法》提供了法律框架，但监管仍存在差距，没有充分覆盖特定的部门、实体或者资产，存在多个监管框架覆盖同类型实体造成冗余的情形，为此，战略表示将进一步确保监管针对的是正确的实体和正确的资产。美国《国家网络安全战略》指出“战略环境需要现代灵活的网络安全监管框架，根据每个部门的风险状况量身定制。行业和监管机构之间的协作将促成运营和商业上可行的监管要求，确保关键基础设施安全与韧性。”2023 年，美国供水、航空、海洋运输、证券、液化天然气等领域发布细化的网络安全要求，其中“风险评估”成为行业要求普遍选择，通过自我评估、委托第三方评估、监管部门评估等方式判断风险管理措施的有效性，发现网络安全差距。

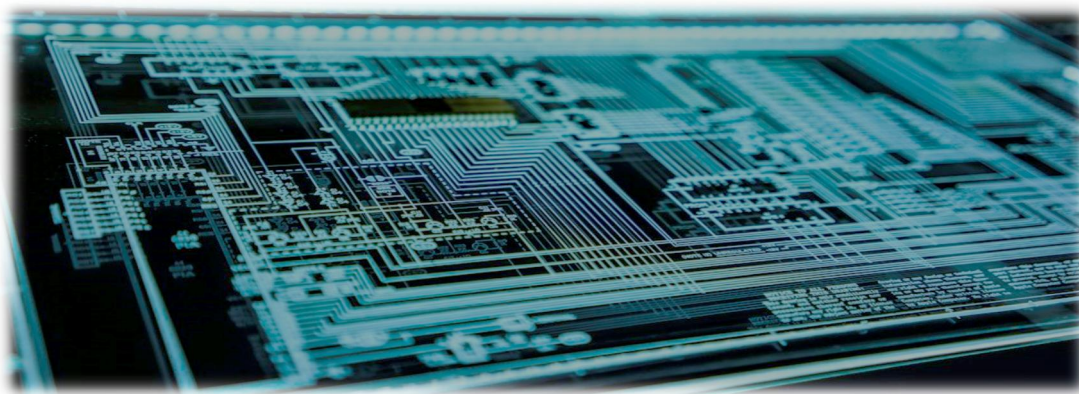
我国在《关键信息基础设施安全保护条例》生效之后，同样积极推动其在重要行业、领域的细化和下沉工作。首个相关国家标准《信息安全技术 关键信息基础设施安全保护要求》正式施行，成为支撑《关键信息基础设施安全保护条例》的基础性核心标准，并从分析识别、安全防护、检测评估、监测预警、主动防御和事件处置六方面提出 111 项安全保护要求。此外，证券期货业、公路水路、铁路等领域出台专门的关键信息基础安全保护管理办法或将其作为重要内容一并写入行业网络安全管理办法中，并提出行业特殊要求，如证券期货业要求本行业关键信息基础设施运营者定期开展压力测试，公路水路领域将关键信息基础设施分为部级设施和省级设施，并在检测评估和事件报告等方面提出差异化要求。

（三）内生安全风险与外界政府干预共同加剧全球供应链安全风险

《全球网络安全政策法律发展年度报告（2022）》的前瞻展望部分，我们曾提出供应链安全问题将强势“扩张”，成为网络安全的主线之一。2023年，供应链安全风险愈加凸显。如澳大利亚发布的《关键基础设施年度风险评估报告》中指出，供应链不再是线性的，即从A到B到C，而是演变为由上游、下游和相互联结的服务共同构成的涉及多重供应商的供应链网络，这使得供应链更加暴露在地缘政治、环境、社会和经济领域的各类潜在破坏性风险中。欧盟网络安全局发布的《2030年威胁预见》中更是将“软件依赖导致的供应链妥协”认定为2030年可能出现的头号网络安全威胁。

一方面，供应链自身面临的安全风险更加突出，供应链的扩张增加网络攻击暴露面，特别是当供应链上不同主体的网络安全成熟度参差不齐时。因此，提高供应链风险感知能力，提高网络产品安全性成为各国立法重点。美国、加拿大、新加坡等国17个政府机构联合发布《改变网络安全风险的平衡：软件安全设计原则和方法指南》，强化软件制造商网络安全责任，要求软件制造商优先考虑产品的安全性，保障产品功能安全运行，减少被攻击的可能性。同时，对于面向广大消费者提供的网络产品，通过打标签、添加信任标识等方式佐证产品安全性。欧盟近年来持续推动的《网络弹性法案》着眼于提供安全的数字产品，该法案为数字产品制造商和零售商引入强制性网络安全要求，并将这种保护延伸到整个产品生命周期。法案生效后，此类产品将带有CE标志，以表明它们符合安全标准。美国白宫宣布“美国网络信任标识计划”，零售商和制造商提供的符合网络安全标准的智能设备将获得“网络信任”标签，帮助消费者更轻松地选择不易受到网络攻击的设备。澳大利亚《2023-2030年澳大利亚网络安全战略》提出将网络安全嵌入软件开发过程中，将为应用商店和应用开发者设计自愿性的实践指引，明确软件开发的网络安全要求。对于开源软件，美国发布《开源软件安全路线图》《提高运营技术和工业控制系统中开源软件安全性的说明书》，表示将提高对开源软件使用和风险的可见性，评估开源软件在联邦政府和关键基础设施中的普及情况，加强开源软件生态系统安全性。

另一方面，个别国家泛化国家安全风险，在芯片、半导体、人工智能技术等领域滥用出口管制措施，人为设置网络空间和信息技术发展障碍，加剧全球供应链中断风险。美国在与英国、加拿大、澳大利亚、日本、荷兰、印度等



国发布的联合声明中，大多涉及共同构建半导体供应链。美国总统拜登签署《关于处理美国在受关切国家的特定国家安全技术 and 产品领域投资的行政令》，限制或禁止美国实体及其控制的境外实体对中国大陆、香港特别行政区以及澳门特别行政区的半导体和微电子、量子信息、人工智能领域的投资。美国商务部产业与安全局公布《实施额外出口管制：特定先进计算物项；超级计算机和半导体最终用途；更新和更正临时最终规则》，在 2022 年 10 月 7 日出台的临时规则基础上，进一步加严人工智能相关芯片、半导体制造设备的对华出口限制。此外，为发展本国芯片产业，美国持续推动《2022 年芯片和科学法》落实，商务部就该法发布“国家安全护栏”最终规则。商务部部长雷蒙多对此称，这些“护栏”将确保美国的每一分钱都不被中国利用去发展技术、赶超美国¹。

¹ 商务部。美国收紧半导体出口管制损人不利己。
<http://exportcontrol.mofcom.gov.cn/article/zjsj/202311/923.html>

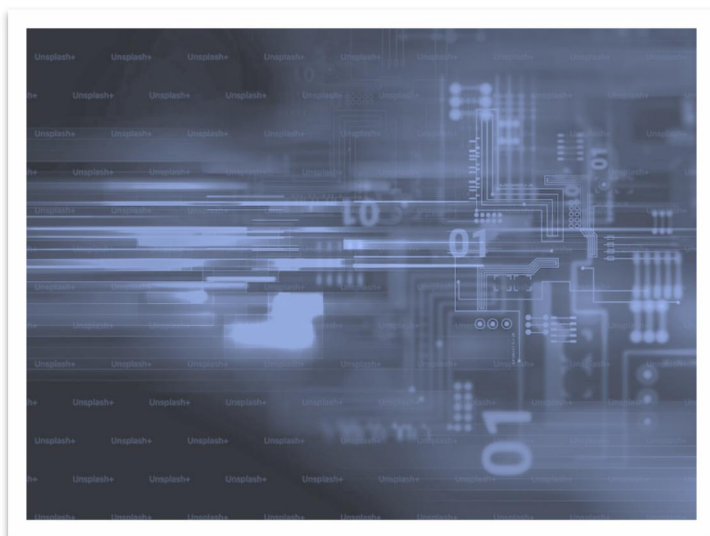
（四）漏洞资源价值持续凸显，激励漏洞披露与发现仍是关键环节

漏洞的有效治理仍是各国关注的重点内容。一方面，漏洞的武器化演变仍在持续，成为个别国家实现政治目的工具。如英国、韩国发布联合警报《朝鲜行为者进行软件供应链攻击》，指控朝鲜国家黑客持续利用流行软件应用程序中的零日漏洞，借此发起全球供应链攻击，以进行间谍活动和金融盗窃。我国国家计算机病毒应急处理中心发布的《“黑客帝国”调查报告——美国中央情报局（CIA）（之一）》指出，在规模庞大的全球性网络攻击行动中，CIA 大量使用零日漏洞，其中包括一大批至今未被公开披露的后门和漏洞，在世界各地建立僵尸网络和攻击跳板网络，针对网络服务器、网络终端、交换机和路由器，以及数量众多的工业控制设备分阶段实施攻击入侵行动。另一方面，漏洞成为从事网络违法犯罪、实施恶意网络活动的重要工具。澳大利亚信号局指出五分之一的漏洞在发布补丁或缓解建议后 48 小时内被利用，一半的漏洞在两周内被利用。我国 2023 年公开披露的行政执法案件中，涉及大量由于网络存在安全漏洞，未及时进行处置，导致网络或数据存在安全风险而被行政处罚的案件。公安部将“系统防护能力欠缺、用户防护意识不足。部分责任单位对网络安全重视程度不够，未及时升级维护相关系统，致使大量高危漏洞和高危端口长期存在，给黑客可乘之机”列为导致当前黑客类犯罪多发频发的三大原因之一，提示企业高度重视“两高一弱”问题，即高危漏洞、高危端口与弱口令²。2023 年全球发生的部分大规模网络安全事件都与漏洞存在千丝万缕的联系，如 6 月亚马逊网络服务遭遇数小时中断，亚马逊事后表示已对导致问题的漏洞进行修复³；10 月有黑客利用满分严重漏洞（CVE-2023-20198），成功侵入超过四万台运行 IOS XE 操作系统的思科设备⁴。鉴于此，**强制性漏洞披露要求、建立漏洞披**

² 公安部. 公安部新闻发布会：通报公安机关打击黑客类违法犯罪工作举措及总体成效情况，公布十大典型案例. <https://www.mps.gov.cn/n2254536/n2254544/n2254552/n9309244/index.html>

³ 安全内参. 不止阿里云！2023 年全球规模最大的 15 起云中断事件盘点. <https://mp.weixin.qq.com/s/W7BtGPPo2FpeOvLLShBkPQ>

⁴ 安全内参. 超过 4 万台思科设备被植入后门账号：零日漏洞攻击，暴露即被黑. <https://mp.weixin.qq.com/s/EKfMqB8fR31oYPGuVy0Fxf>



露计划、发布漏洞早期预警、鼓励安全研究人员善意发现并报告成为各国有效缓解漏洞风险，保障网络安全主要路径。

欧盟发布《制定国家漏洞计划》报告认为，欧盟协调漏洞披露（CVD）生态系统仍然

支离破碎，成员国中仅比利时、法国、立陶宛和荷兰制定了完整的国家CVD政策。报告指出尽管成员国和行业组织已经采取部分措施，但行业的最大期望是建立国家或欧盟层面的CVD政策，以帮助组织和公共部门将漏洞管理作为优先事项。欧盟《网络弹性法案》为数字产品制造商引入强制性漏洞披露要求，规定制造商应在得知漏洞后 24 小时内毫不拖延地通知ENISA其数字产品中包含的任何被积极利用的漏洞，通知内容应包括漏洞详细信息以及所采取的缓解措施。对于此要求，来自谷歌、电子前沿基金会等多个组织的 56 位网络安全专家签署联名信，认为该规定会催生情报、监视等方面新的威胁，破坏数字产品和使用者的安全。联名信建议删除此条款或进一步完善，明确禁止国家机构通过根据该法案披露的漏洞信息实施情报监视或发起网络攻击；只有在补丁等有效的漏洞缓解措施公开可用 72 小时后再向机构报告漏洞信息等提议。

美国持续加强漏洞披露环节，致力于在被恶意利用前进行修复。CISA 根据《关键基础设施网络事件报告法》授权建立勒索软件漏洞警告试点。通过该试点，CISA 将确定与已知勒索软件利用相关的漏洞，就此向关键基础设施实体发出漏洞警报，从而在勒索攻击事件发生前进行缓解。CISA 也持续根据掌握的信息在其已知漏洞利用目录中添加新的漏洞信息，并强烈敦促所有组织及时修复目录中的漏洞。CISA 还发布其首份《漏洞披露政策（VDP）平台年度报告（2022）》，指出美国许多联邦文职行政机构既缺乏从第三方接收漏洞信息的正式机制，也缺乏处理此类信息的明确策略。为帮助各机构满足约束性操作指令 BOD20-01 的要求，CISA 于 2021 年 7

月建立 VDP 平台。截至 2022 年 12 月，该平台已收到超过 1300 份有效漏洞信息披露，其中约 85% 已被修复。



一直以来，安全研究人员在漏洞发现和修复方面发挥着重要作用，漏洞赏金计划是安全研究人员参与漏洞治理的有效途径之一。2023 年，美国防部发起“黑掉五角大楼 3.0”漏洞赏金计划；谷歌推出漏洞赏金计划，以勘察 Google AI 的系统漏洞，提高生成式人工智能安全性。与此同时，安全研究人员漏洞发现行为在法律上的认可始终存在模糊性，成为阻碍研究人员上报漏洞的主要原因之一。欧盟《制定国家漏洞计划》报告认可研究人员在漏洞披露方面的重要作用，认为从研究人员角度来看声誉仍是其合法报告漏洞的关键激励因素之一，然而从立法层面进行保护也需要给予高度重视。比利时网络安全中心（CCB）发布新法律框架《向 CCB 报告 IT 漏洞》，指出虽然诸多国家或组织制定协同漏洞披露政策和发起漏洞赏金计划，但善意发现漏洞的主体仍可能面临被诉的风险。这种对法律风险的担忧通常会抑制善意主体寻找或报告漏洞的意愿。为解决这个问题，该框架允许任何自然人或法人在没有欺诈或恶意情况下发现和报告位于比利时的网络信息系统中的现存漏洞，前提是严格遵守框架规定的特定要求。框架规定了数项基本原则，包括研究人员验证漏洞存在的行为应严格遵循必要性和适当性要求，发现漏洞后必须尽快报告 IT 系统负责人，按照规定程序报告给 CCB 等。

（五）数据精细化、场景化立法蓬勃发展，数据跨境成为关注焦点

2023 年，全球主要经济体数据治理持续发展并逐渐进入规则的细化、完善及调整期。欧盟方面，继《数字市场法》《数字服务法》《数据治理法》后又通过《数据法》，为数字欧洲建设提供制度保障。美国探索联邦层面个人数据保护统一立法，试图在联邦立法层面对个人数据保护、数据经纪人制度做出完善。我国进入《数据安全法》《个人信息保护法》常态化执法阶段，两大数据立法下的重要制度规范正在加紧研制。印度历经五年的讨论及修改终于出台《2023 年数字个人数据保护法》。英国积极开展数据保护制度改革，酝酿制定《数据保护和数字信息法案》。日本最新修订的《个人信息保护法》正式施行。特殊类型数据、特殊场景、特殊主体的数据保护问题受到监管特别关注，数据规则精细化、场景化趋势明显。日本、欧盟、韩国、英国、挪威、加拿大等国围绕热像仪、执法领域面部识别技术、人事劳务、员工监控、青少年隐私等出台细化要求。我国针对个人信息与数据安全问题多发高发领域或环节相继出台诸多细化规范。《证券期货业网络和信息安全管理规定》《关于规范货币经纪公司数据服务有关事项的通知》《关于加强第三方合作中网络和数据安全管理的通知》《寄递服务用户个人信息安全管理规定》聚焦不同领域，细化制度要求。



作为数据法治的重点议题，数据跨境流动治理方面的冲突与融合在 2023 年更加凸显。欧盟及其成员国针对中美大型平台的执法力度持续加大。爱尔兰数据保护委员会因 Meta 公司违规向美国传输数据对其处 12 亿欧元罚款，并责令其在

未来五个月内暂停将个人数据传输至美国的行为，并在六个月内删除已非法传输并储存的数据。同时，数据跨境流动的双边合作取得重要进展。欧盟与美国、日本，



美国与英国、日本间的数据跨境流动取得突破。欧盟委员会通过《欧盟—美国数据隐私框架的充分性决定》，个人数据据此可以从欧盟的控制者和处理者转移到美国经认证的组织，而无需获得任何进一步的授权。欧盟与日本达成《欧盟—日本跨境数据流动协议》，取消数据本地化要求，确保企业在无需应对繁琐行政或存储要求的情况下有效处理数据。“英美数据桥”正式确定，英国企业和组织可根据数据桥安全可靠地将个人数据传输至美国认证组织。我国在《网络安全法》《数据安全法》《个人信息保护法》构筑的数据出境基本规则下，不断完善配套制度措施。《个人信息出

境标准合同办法》《个人信息出境标准合同备案指南（第一版）》《规范和促进数据跨境流动规定（征求意见稿）》发布，推动个人信息出境标准合同制度正式落地，调整现有数据出境规则，减轻企业数据出境合规义务。

数据流通利用成为国际数据治理又一重点关注。欧盟《数据法案》对企业—用户（B2C）、企业—企业（B2B）、企业—公共部门（B2G）等场景的数据共享进行具体规定，旨在促进欧洲数据共享与再利用。英国《数据保护和数字信息法案》采取多项举措减轻企业数据合规成本为产业发展松绑。国内，国家全面布局数据要素市场发展。中共中央、国务院印发《数字中国建设整体布局规划》，将数据资源体系与数字基础设施并列为数字中国建设的“两大基础”。北京、上海、福建、江西等多省份均发布地方性文件，发挥数据要素作用，推动数据要素产业创新发展。

（六）信任成为信息内容治理核心，未成年人保护与网络暴力为重点关切

客观而言，基于信息技术的所有应用和场景最终都要以“信息”为载体形式加以呈现。现代社会以信息为基础，对信息的整合和利用构成社会运行核心内容。信息社会的一切表征都可以泛化为信息，而社会的基本功能及其运行本质也开始转向对信息本身的产生、获取、处理和利用。正如欧盟委员会在《数字服务法》序言中所指出的那样，信息社会服务，尤其是中介服务，已经成为欧盟经济和欧盟公民日常生活的重要组成部分。这一客观的社会进程导致互联网信息服务成为足以影响社会福祉的公共性服务，并与国家安全、社会稳定、产业发展和公民保障密切相关。世界经济论坛《未来网络安全 2030：新基础》白皮书中认为“信任加固是未来十年网络安全努力的关键目标之一。错误和虚假信息的在线传播已经成为网络安全的核心关切。网络安全对于信息机密性和可用性的关注将有所减少，反之对于信息完整性和来源的关注将有所增加。”

一是未成年人保护与网络暴力治理成为重要关注。英国《在线安全法》在经历争议后正式获批成为法律，通过对社交媒体平台赋予严格的内容安全义务，明确其承担阻止和立即移除非法内容的法定责任，采取零容忍态度保护儿童免受网络伤害，旨在使英国成为世界上最安全的上网场所。新加坡《在线安全（杂项修正案）法》生效，规定信息通信媒体发展局可以向在线通信服务提供者发布指令，要求其删除、屏蔽特定的负面内容。在全球范围内，我国是较早制定专门的信息内容安全法律制度的国家之一，在长期的法治实践中逐步形成了颇具中国特色的制度结构。2023年聚焦未成年人保护与网络暴力、网络谣言治理。我国第一部专门性未成年人网络保护综合立法《未成年人网络保护条例》公布，将网络信息内容规范作为重要内容写入。国家网信办发布《网络暴力信息治理规定（征求意见稿）》，两高一部印发《关于依法惩治网络暴力违法犯罪的指导意见》，从强化网络信息服务提供者治理责任，加强违法犯罪惩治力度等方面全面提升网络暴力治理效能。国家网信办发布《关于加强“自媒体”管理的通知》，要求加强“自媒体”管理，压实网站平台信息内容管理主体责任，健全常态化管理制度机制，推动形成良好网络舆论生态。

二是生成式人工智能、深度伪造等技术在信息内容方面的不当利用使得信息内容治理难度持续加大。对于 ChatGPT “一本正经胡说八道”的担忧似乎仍然萦绕在耳畔，不论是个体利用人工智能生成虚假信息，还是国家行为体借此实

现政治企图，均使得信息内容治理难度持续加大，公众对于所见所闻的信息内容的信任正在接受校验。美国国土安全部发布的《国土威胁评估 2024》中指出“新兴网络和人工智能工具的扩散和可访问可能会帮助国家行动者通过创建低成本、高质量的文本、图像和音频合成内容来支持他们的恶意信息活动”。兰德公司发布的《生成式人工智能兴起和即将到来的社交媒体操纵 3.0 时代》报告中认为“可以肯定的是，生成式人工智能可以被用来制造更高质量的虚假或欺骗性信息。无处不在、功能强大的生成式人工智能的出现，通过扩大和实现对社交媒体的恶意影响操作，对国家安全构成潜在威胁。”EPIC 发布的《危害产生：生成式人工智能的影响与未来之路》报告认为“人工智能生成内容涉及到更宽泛的法律问题，即公众对于所见所听内容的信任。随着人工智能生成媒介的日渐普遍，假亦是真、真亦是假的情况也将越来越多”。考虑到此类内容在竞选等政治活动中可能造成的危害，EPIC 等组织向美国联邦选举委员会提交请愿书，要求应对 2024 年选举前虚假信息的持续威胁，包括由人工智能生成的虚假信息。美国、德国、日本、加拿大等国发布的相关声明或指南文件中均关注到人工智能引入的信息安全风险问题。我国在《生成式人工智能服务管理暂行办法》中要求生成式人工智能服务提供者承担网络信息内容生产者责任，履行网络信息安全义务；美国白宫召集 OpenAI、谷歌等七家人工智能领先企业作出自愿承诺，开发包括水印系统在内的技术机制，确保用户知晓哪些内容是由人工智能产生的，以获取公众信任，均是国家对于信息内容领域新技术安全应用的回应。

（七）基于风险的人工智能法治趋于理性，软硬法协同推进向善包容治理

目前人工智能技术仍处于“社会试验”状态，法律也是这一社会试验的重要组成部分。各国对人工智能发展和应用而引致的现实性和潜在性安全风险都有关注，试图厘清算法和模型背后的逻辑与法律逻辑之间的关系，在具体的监管方式与规制重点上各有特色，但基于风险的分分类分级管理已然成为基本共识。欧盟以风险水平为导向，希望通过《人工智能法案》全面监管人工智能。高票通过的《关于制定〈人工智能法案〉和修订某些欧盟立法的提案的修正案》一是完善基于风险识别的监管体系，将人工智能应用的风险分为四类，尤其对“高风险”系统的提供者规定全流程风险管理措施；二是新增对类 CHATGPT 基础模型的特别监管措施，要求生成式人工智能的基础模型提供者采取风险控制、数据治理、质量管理等措施，模型投放市场前应在欧盟数据库中登记备案。这些举措反映了欧盟欲抢占人工智能领域制高点的战略意图。美国也支持基于风险的人工智能监管方法，但更侧重于商业发展优先，鼓励人工智能技术创新发展。美国总统拜登签署《关于安全、稳定和可信的人工智能行政令》，在保护美国用户隐私、促进公平和公民权利、维护消费者和工人权益、促进创新竞争等方面做出规定。聚焦内容安全、平台责任、公开透明、问责框架等方面，美国国会引入《要求曝光人工智能主导的政治广告法案》《监督新兴技术法案》《数字平台委员会法案》《人工智能测试法案》《联邦人工智能风险管理法案》等多项立法案，其中《2023 年人工智能研究、创新和问责法案》明确人工智能系统分类分级和安全管理要求，针对“关键影响”“高影响”人工智能系统设定相应的风险管理评估与报告要求。此外，加拿大《人工智能和数据法案》、巴西第 2338 号法案《提供人工智能使用规则》等取得实质性进展。当前，中国在人工智能领域的规定采用区分业务领域、区分技术方向的措施，针对人脸识别、深度合成、自动化推荐等应用场景制定专门监管规则。国家网信办等七部门联合发布的《生成式人工智能服务管理暂行办法》是我国首个针对生成式人工智能的部门规章，旨在平衡创新推动和风险管控。

鉴于人工智能技术、行业发展具有不可预知性，以新加坡、韩国、新西兰等为代表的国家对人工智能安全治理与监管采取“温和干预”的思路，在更具实质性监管的硬法规制之外，重点推进生成式人工智能指南制定。为应对类 ChatGPT 生成式

人工智能带来的数据安全风险,新加坡通信和信息部宣布将根据《个人数据保护法》发布《在人工智能系统中使用个人数据的咨询指南》,支持生成式人工智能技术负责任开发和部署;韩国个人信息保护委员会发布《人工智能时代个人信息安全使用指南》,强调机器学习阶段要对个人信息进行匿名化处理并强化隐私增强技术等个人信息保护技术应用;新西兰隐私专员发布《人工智能与信息隐私原则》指南,鼓励在人工智能工具实施的每个阶段,从数据收集和模型训练到用户使用,都考虑信息隐私原则。

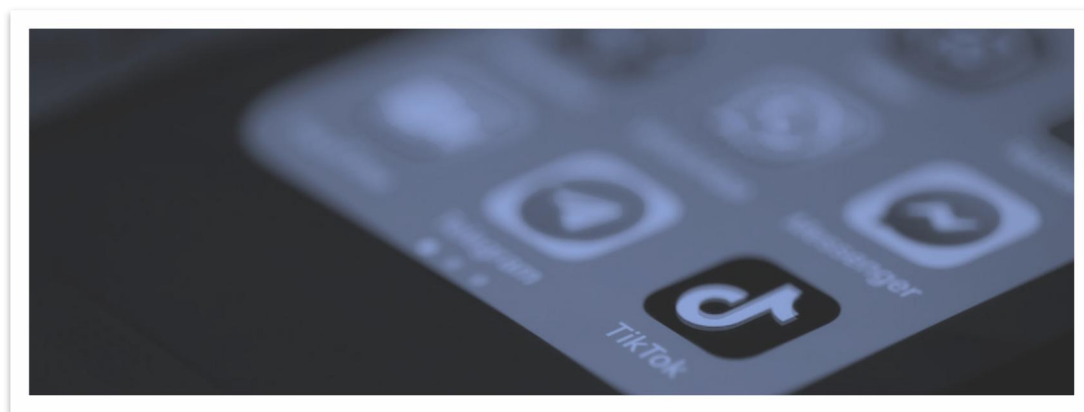
法律之外,还有伦理、信念、教育等引导人工智能向善发展,设计和发展“有道德”的人工智能是全人类共同追求。德治是适用范围最广泛的社会行为调节机制,2023年以来,各国在人工智能技术伦理规范方面深入推进,重点关注人工智能系统设计和建造背后“人”的价值取向、伦理抉择、行为规范,探索建立以人为本的价值体系。政府间机构、国际组织成为引导人工智能向善治理重要力量,经济合作与发展组织关注人工智能大语言模型的“稳健性、安全性”原则;七国集团就《人工智能指导原则》《人工智能开发者自愿行为准则》达成一致,呼吁各组织在开发高级人工智能过程中,采取适当安全措施,监测投放市场后滥用行为,识别、评估并降低人工智能全生命周期安全风险,并实施负责任的信息共享和事件报告制度;欧洲委员会人工智能委员会发布《经修订的零草案框架:人工智能、人权、民主和法治框架公约》,概述平等和反歧视、隐私和个人数据保护、问责制与法律责任、透明度和监督、安全创新等人工智能管理基本原则;北约数据和人工智能审查委员会提出制定用户友好且负责任的人工智能认证标准。此外,中国发布《全球人工智能治理倡议》并参与签署《布莱切利宣言》,伦理先行的理念贯穿人工智能开发、设计和使用过程,反对技术滥用,维护人类尊严。

（八）监管行动持续推进，聚焦平台与规模效应的网络执法效能日渐突出

网络执法是落实立法要求，确保制度落地的重要手段，细化规范指引、明确监管对象、督促引导落实安全保护义务、惩治违法犯罪行为均是网络执法的有机组成部分。站在当前的历史节点，仅从立法角度看待网络安全治理已不能满足需求，评估立法实施效能，总结立法执法情况，理清主要违法行为和聚焦的违法对象，思考从个案争议到立法完善的距离很有必要。

2023 年，欧盟 GDPR、我国《网络安全法》《数据安全法》《个人信息保护法》等网络安全重要立法均已施行多年，相应的监管行动进入常态化阶段，在保障网络与数据安全方面取得显著成效。欧盟数据保护委员会近期表示 GDPR 在前 5 年半的应用是成功的，充分加强、现代化和协调了整个欧盟的数据保护原则。

从观察到的 2023 年全球网络执法情况来看，**互联网巨头及大型平台是重点监管对象**，如 meta、TikTok、X(前身 Twitter)、谷歌、苹果、新浪、百度、腾讯、网易等在 2023 年均遭遇不同类型的执法行动。从针对的违法行为来看，**数据安全、个人信息保护、信息内容治理、供应链安全、类 ChatGPT 生成式人工智能、反电信网络诈骗**构成网络执法核心关注。



具体来说，TikTok 因违规处理儿童数据、数据保护措施薄弱、违反广告 cookie 链接相关规定等违法行为，在爱尔兰、土耳其、英国、法国均被处罚。因未经用户同意擅自收集、存储和使用用户位置信息，谷歌支付 9300 万美元和解金。因多次拒绝将俄罗斯用户数据存储于俄罗斯境内的服务器，俄罗斯莫斯科一家法院对谷歌

处以 1500 万卢布的罚款。针对抖音、新浪微博等网站平台存在法律、法规禁止发布或者传输的信息问题,我国国家网信办指导属地网信办分别依法约谈相关网站负责人,责令其限期整改,处置相关账号,从严处理责任人,并分别给予罚款行政处罚。针对快手、百度、腾讯微信、网易等网络平台履行主体责任不力,对其用户发布的信息未尽管理义务,造成淫秽色情、封建迷信、诱导充值、为劣迹艺人辩护等有害信息在网上传播问题,国家网信办指导属地网信办分别依法约谈相关网站负责人,责令其限期整改,处置相关账号,从严处理责任人,并分别给予罚款行政处罚⁵。除持续针对大型平台开展监管行动以外,中小型甚至微型组织同样进入执法视野,表明网络执法逐步全面化、精细化的同时,也引发社会对于执法尺度与温度的思考。

我国 2023 年在数据安全、个人信息保护、供应链安全、网络谣言和网络暴力治理方面持续发力。公安、网信、通信管理等部门依据《网络安全法》《数据安全法》《个人信息保护法》开展大量执法行为,综合运用监督检查、行政指导、行政处罚等手段,引导督促组织落实网络安全保护义务。首例公开披露的针对关键信息基础设施供应链的网络安全审查结果发布,审查发现美光公司产品存在较严重网络安全问题隐患,对我国关键信息基础设施供应链造成重大安全风险,影响我国国家安全。为此,网络安全审查办公室依法作出不予通过网络安全审查的结论。网信部门、公安机关持续开展晴朗、净网等专项行动,依据《网络安全法》《关键信息基础设施安全保护条例》开展的执法活动向纵深化、精细化推进,关键信息基础设施、供应链、“两高一弱”、LED 大屏等重点对象和重点环节的执法全面深入。依据《数据安全法》《个人信息保护法》《反电信网络诈骗法》开展的执法活动显著增加。树立法律权威、严格执法、高额处罚案件不断出现的同时,寻求执法温度、柔性执法的探索也稳步向前。

与此同时,网络执法本身的规范性水平持续提升。国务院办公厅印发《提升行政执法质量三年行动计划(2023—2025 年)》,指出行政执法是行政机关履行政府职能、管理经济社会事务的重要方式,行政执法质量直接关系法治政府建设成效。行动计划围绕全面推进严格规范公正文明执法等六项重点任务提出 17 项具体工作举措,要求综合运用多种方式督促引导受处罚企业加强合规管理、及时整改违法问

⁵ 中国网信网. 聚焦违法违规 加大执法力度. http://www.cac.gov.cn/2023-07/31/c_1692460653560853.htm

题，防止以罚代管。公安机关将行政执法规范化建设作为重要任务之一，国家互联网信息办公室发布《网信部门行政执法程序规定》，工信部发布《工业和信息化行政处罚程序规定》，对执法活动提出规范化要求。

此外，部分重要立法虽施行不久，但对监管对象产生重要影响的监管举措已正式启动。2023 年，欧盟委员会《数字市场法》《数字服务法》相继生效。《数字服务法》下的超大型在线平台已完成两批认定，超大型在线搜索引擎、《数字市场法》下的“守门人”及其提供的核心平台服务均已完成首批认定，主要针对谷歌、亚马逊、苹果、字节跳动、Meta、微软等大型互联网公司。部分经认定的互联网公司表示已着手开始合规工作，以符合《数字市场法》《数字服务法》要求。但该认定结果并未取得一致认可，部分互联网公司表示异议，如 Meta 对其提供的 Messenger 和 Marketplace 服务、字节跳动对 TikTok 被认定为“守门人”核心平台服务存在异议，已起诉至欧盟普通法院进行裁决。欧盟委员会近日表示已启动针对社交媒体平台“X”的“正式诉讼”程序，以评估其在风险管理、内容审核等方面是否违反《数字服务法》⁶。



⁶ 光明网，欧盟宣布启动对社交媒体平台“X”的“正式诉讼”。
https://news.gmw.cn/2023-12/20/content_37039396.htm

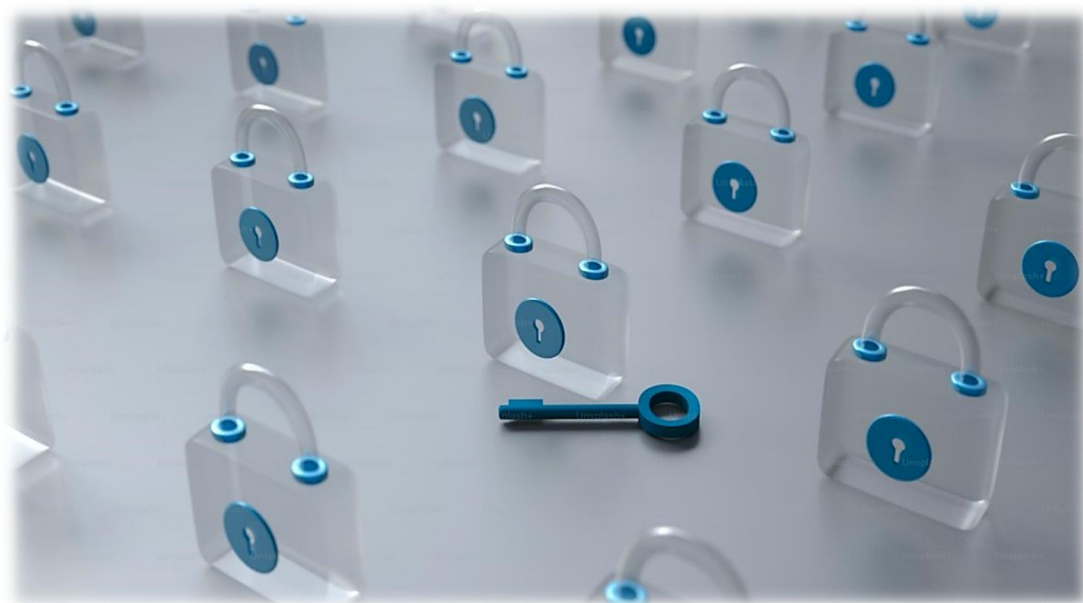
（九）安全与发展辩证关系在量子技术推进与后量子密码迁移中深刻诠释

量子计算的巨大潜力引发新一轮技术变革和激烈竞争，量子信息技术及其产业链已成为国家安全的新内容。正如《数字中国发展报告（2022年）》指出，量子计算等为代表的新技术加快实现从研究探索到商业落地的跨越，在此过程中进一步放大和凸显了隐私泄露、技术滥用、价值渗透等科技法律、伦理和哲学价值问题。量子计算能力的跃升对现代密码学的安全风险正以一种前所未有的方式显现，并从底层“瓦解”现代密码学的数学和工程基础。与利用量子力学保护数据的量子密码不同，后量子密码是基于新的数学问题，在经典计算机上定义和执行算法，研究量子计算机和经典计算机都无法破解的新密码系统。

2023年，加拿大、英国分别发布《国家量子战略》，推动本国量子技术发展。英国将量子视为英国未来发展的五大优先技术之一，认为其对经济增长、国家安全和国防建设均至关重要，提出用十年时间，到2033年使英国成为世界领先的量子赋能经济体的愿景，将自2024年开始投入25亿英镑用于开发量子技术。加拿大表示将致力于在量子计算机软硬件开发、部署和使用方面成为世界领导者，造福加拿大工业、政府和公民。

一直以来，密码安全问题就是算法构筑的“难解性”与计算能力之间的博弈。但这一传统的攻防关系随着量子计算的成熟而变得不再稳定，量子计算提供的强大计算能力将使现有的绝大部分公钥密码算法被攻破，迄今为止最为有效的“安全屏障”可能不再可靠。因此，尽管量子技术发展将带来新的契机，但各国在加快发展量子技术，试图借此抢占网络安全优势地位的同时，也超前布局量子技术风险防范措施，推动向后量子密码迁移，以保障本国免受量子技术威胁。欧洲政策中心发布的《欧洲量子网络安全议程》指出“具有密码价值的量子计算机的出现只是时间问题。这已经改变了威胁格局，一旦技术可用，对手就会用来下载加密信息进行解密。”该中心认为有必要制定新的欧盟协调行动计划，以确保协调过渡到后量子密码。英国在《国家量子战略》中表示政府自身已经对关键信息和服务采取相应风险缓解措施，并提出任何能够管理自己的加密基础设施的组织都应当将量子安全过渡纳入长期计划，开展调查工作，确定当迁移标准可用时哪些系统应优先过渡。加拿大在《国家量子战略》中同样表示加拿大政府已经在安全通

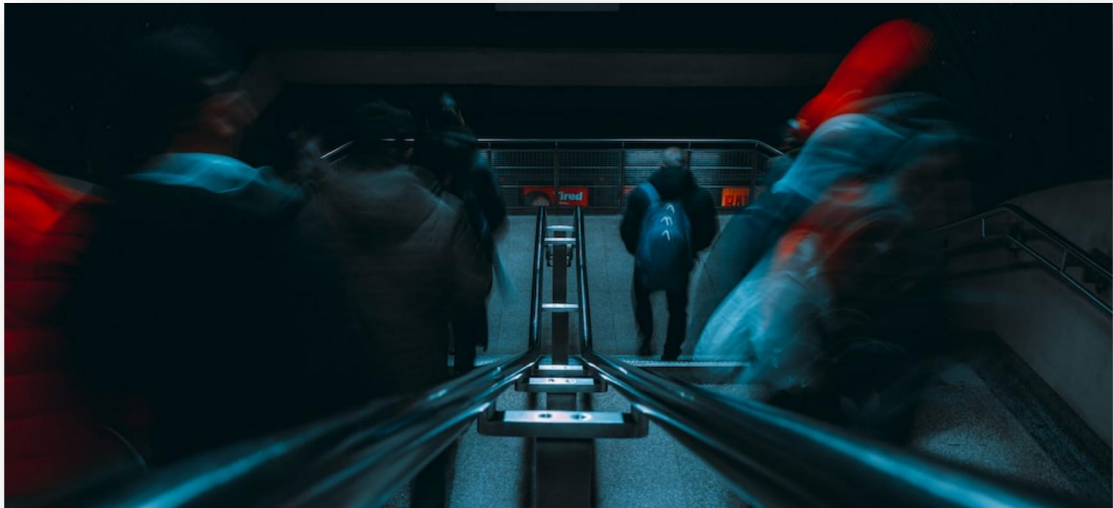
信机构的领导下开展工作，确保高度敏感数据免受量子威胁，后续将与加拿大研究人员和工业界合作，支持在易受量子威胁的技术中部署后量子密码。



2023 年，美国仍在主导后量子密码迁移标准的制定。NIST 作为负责制定后量子密码标准的机构，继多轮次算法筛选后，连续发布《FIPS 203：基于模块格的密钥封装机制标准》《FIPS 204：基于模块格的数字签名标准》《FIPS 205：基于哈希的无状态数字签名标准》初始公开草案。在推进标准制定的同时，美国三部门联合发布《量子准备：向后量子密码迁移》指南，为各组织着手开展后量子密码迁移工作进行指导，要求组织成立专门的项目管理团队，梳理并形成本组织易受量子攻击的系统和资产清单，摸清当前使用的加密技术，并重视供应链安全，加强与包括云服务商在内的技术供应商的合作。NIST 发布《迁移到后量子密码：为考虑实施和采用量子安全密码做准备》指南草稿，帮助实体确定公钥算法在加密方案中的位置和方式，制定将这些算法迁移到量子密码的策略，以及执行互操作性和性能测试。

（十）网络犯罪预防、打击、治理一体化基本共识形成，防治相关立法加速推进

与传统犯罪不同，网络犯罪具有高度可复制性，一旦开发，网络技术可共享、复制、出售甚至外包，实现犯罪技术市场化或提供“犯罪即服务”。在互联网、物联网、大数据、云计算、元宇宙、人工智能等各种网络技术迭代升级背景下，犯罪分子利用 ChatGPT、加密货币等进行犯罪辅助，犯罪纵向精细切割，横向分工细化，交错而成利益链条，形成复杂的网络犯罪生态，呈现泛罪名化、泛技术化、泛组织化、泛产业化、泛地域化等特点，给社会安全治理带来诸多挑战。2023 年，勒索攻击仍是最具破坏性的网络犯罪类型之一。同时，网络犯罪给国家、组织和个人产生的影响也持续增长。澳大利亚信号局（ASD）发布的《2022-2023 年 ASD 网络威胁报告》⁷中指出网络犯罪对澳大利亚企业的打击成本正以每年高达 14% 的速度增长。



鉴于此，各国网络犯罪治理思路从“回应型”趋向“预防型”。有效治理因误用、滥用新型网络技术导致的网络犯罪新业态的关键并不是从法律上否定技术本身的合法性，而是顺应新型网络技术被用于犯罪的进化趋势，转变犯罪治理逻辑，在规制流程上从下游犯罪穿透至源头规制。互联网服务提供者等多元主体都是网络犯罪前端治理的重要环节。个别国家最初期待企业通过自律行为治理平台上违法犯罪内容，但见效甚微，后来也开始通过立法赋予其一定的

⁷ ASD Cyber Threat Report 2022-2023.

<https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>

强制性义务，并结合比例原则，根据主体规模和业务影响程度动态调整私主体的犯罪防治义务。英国《在线安全法》要求社交媒体平台对其网站和应用程序上的内容和行为所产生的儿童性虐待、恐怖主义、诈骗等犯罪风险进行评估和管理。新加坡议会积极推动《网络刑事危害法案》，规定若主管当局确信网络服务是或极有可能是用于实施、协助网络犯罪活动，且新加坡人可使用该服务进行网络活动，则主管当局可将该

服务认定为

“与网络犯罪相关的网络服务”；同时，主管当局可对该网络服务提供者发布行为守则，提供者必



须采取所有合理可行措施遵守守则。欧盟《数字服务法》针对小微企业和超大型平台技术反制义务采取“阶梯式分配”。小微企业仅需履行最低程度合规义务，而超大型平台则被要求更加主动参与到非法内容治理活动之中，对系统性风险进行有效预见及防范。新加坡《在线安全（杂项修正案）法》将具有重大影响的在线通信服务指定为“受监管的在线通信服务”（ROCSs），要求遵守专门行为守则。我国将网络犯罪防治法列入十四届全国人大常委会立法规划，拟全面加强电信、互联网服务提供者等主体在网络犯罪防治方面的法定义务。

除对内强化犯罪防治制度建设外，对外优化执法合作也是跨境网络犯罪治理的内生要求。网络犯罪的跨国性和复杂性的特征日趋凸显，依赖传统的国家治理机制难以抵御各类新型网络犯罪带来的风险和安全隐患，“建立国际合作快速反应机制，逐步建立全球性网络犯罪治理模式”是现实之需。2023年，联合国作为网络犯罪治理的主平台作用凸显。《联合国打击网络犯罪公约》谈判稳步开展，谈判期间，各国普遍支持在尊重国家司法主权基础上，针对打击网络犯罪

的现实需要，构建高效的司法合作机制，包括搭建“7天24小时联络点”、便利电子证据合作等。区域性网络犯罪治理国际合作机制健全发展，跨境电子证据调取、犯罪信息共享、网安能力建设仍是焦点。欧盟理事会通过决议，授权成员国出于欧盟利益签署《〈网络犯罪公约〉加强合作和披露电子证据的第二项附加议定书》，涵盖域名注册信息调取、用户信息披露、流量数据获取、紧急情况即时合作、互助工具与个人信息保护措施等内容。欧洲议会通过《电子证据条例》《刑事诉讼中的电子证据：法律代表指令》，明确取证国当局可从服务提供商处调取订阅者数据、仅出于识别用户身份而请求的数据、流量数据、内容数据等四种类型的电子证据。欧洲刑警组织发布《欧洲刑警组织战略——通过伙伴关系提供安全保障》，旨在构建欧盟犯罪信息中心，促进即时通信、数据存储库的跨国迅速传输，支持加密货币追踪和网络犯罪调查。东盟部长级会议发布主席声明《东盟部长级会议10+1与对话伙伴会议及三边会议主席声明》，提出加强东盟与欧盟、澳大利亚、日本等在广泛的传统和非传统安全问题方面的合作，加强网络安全能力建设，商定网络犯罪共同应对措施。非洲联盟《关于网络安全和个人数据保护的马拉博公约》正式施行，促进非洲国家在调查和起诉网络犯罪方面与其他国家以及国际组织加强合作，共同打击网络犯罪并促进网络安全。特定类型犯罪打击方面，国际反勒索软件倡议（CRI）成员达成《国际反勒索软件倡议2023年度联合声明》，强调不向勒索犯罪团伙支付赎金；探索共同反制措施，创建“共同钱包黑名单”，所有成员共享勒索软件行为者使用的非法钱包数据；若某一成员的政府机关或关键部门遭受勒索攻击，承诺共同协助其进行响应。

二

2024 年全球网络安全政策法律趋势展望

当前,信息技术发展与风险迭代升级相伴而生,技术利用与风险防范并行不悖,安全与发展的辩证统一始终是各国网络安全对内治理和对外合作的底层逻辑。正如世界经济论坛在《未来网络安全 2030: 新基础》白皮书中所指出的,“技术和商业模式创新(包括合法和非法)的加速将为 2030 年的新数字安全格局奠定基础。社会必须从根本上重新调整应对数字安全长期挑战的方式。”本报告认为,本轮数字革命带来法律治理工具的蓬勃发展,同时也在一定程度上导致单一工具供给透支和暂时枯竭。未来网络安全治理除立法、执法、司法等手段外,伦理、社会学、哲学底座等治理工具将发挥重要作用。2024 年全球网络安全政策法律发展将呈现以下六大趋势。

(一) 趋势一：网络空间大国博弈背景下局部和暂时性妥协有望达成和延续

全球主要经济体对网络空间治理规则制定的主导权争夺将进一步激化,地缘政治等因素仍将成为影响网络空间大国博弈的关键因素。但本报告认为在关系前沿技术、军民两用、共同语境的数字、网络安全议题上,各国仍有极大可能达成妥协和一致。2023 年 11 月全球人工智能安全峰会达成的《布莱切利宣言》和对中国《全球人工智能治理倡议》的部分重合已经体现了这一趋势,而未来量子计算安全、拟制公共场所的扩张认定、数据安全标准化应用等问题上,都可以预见各国会在包括双边、多边以及联合国等机构层面上建立一种包容性的妥协。

（二）趋势二：数据赋能发展的制度保障仍需加强，跨境流动面临不确定性

数据作为数字经济的底层支撑，如何释放数据价值促进数字经济发展已成为全球经济复苏背景下的强烈政策导向。尽管各国出于多重价值考虑的数据治理规则存在差异、分歧和博弈，但整体经济态势仍在基础性上影响并最终决定了数据政策、法律的基调。下一阶段，如何深化完善数据治理机制，细化重要数据认定、数据权属等底层问题，推进执法司法走深走实，通过法治促动数字经济，通过数字经济激活实体将是数据法治工作重点和时代使命。

作为全球互联互通、数字经济全球化发展的重要支撑，全球主要经济体在数据跨境流动治理方面冲突与融合进一步凸显，表明数据跨境流动的规制分歧将在相当长一段时间内持续存在且难以弥合。同时，数据在全球范围内持续流动的现实需要对国家间开展数据跨境流动合作提出要求，各国基于双边或多边共同利益诉求，在数据跨境流动方面的共同体建设将持续加强。而此种合作与博弈之间的辩证关系的发展，将使得数据跨境流动面临更大的复杂性与不确定性。就我国而言，数据出境安全评估、个人信息出境标准合同等数据出境制度的相继落地后，针对数据出境的监管活动逐渐展开并呈现严格监管态势，但随着数据出境制度实践的推进与数字经济发展需求，更加便捷、高效的数据跨境流动多元管理机制加速探索，国家互联网信息办公室发布的《规范和促进数据跨境流动的规定（征求意见稿）》，国务院发布的《关于进一步优化外商投资环境 加大吸引外商投资力度的意见》《全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案》等均是优化营商环境的制度探索，以期在数据安全保障与数据价值利用之间寻求更大平衡。未来，我国在数据出境安全与发展之间的辩证关系之间侧重发展的趋势将进一步明确，数据跨境安全有序便利流动的政策法律保障将进一步完善。但其中，由于关涉国家安全、公共利益、经济发展等重要方面，国家在重要数据出境安全与便利之间的权衡将更为谨慎。对于《规范和促进数据跨境流动的规定（征求意见稿）》所明确的“未被相关部门、地

区告知或者公开发布为重要数据的,数据处理者不需要作为重要数据申报数据出境安全评估”的规定,在正式稿中或将重新进行调整,以强化重要数据处理者责任,进而落实重要数据重点保护制度要求。

（三）趋势三：网络执法的精细化、专业化、智慧化水平将大幅提升

坚持严格规范公正文明执法是《法治中国建设规划(2020—2025年)》《法治政府建设实施纲要(2021—2025年)》的共同要求,也是落实网络安全法治体系的必然要求。随着法律实施的不断深入,网络执法更加精细化,使得多法并行背景下执法的细节问题开始显现,如供应链中网络运营者和网络产品、服务提供者认定、云计算等新技术中的责任划分、涉案虚拟货币处置、执法管辖权等问题,均需在法理、法律研究、实践指引的共同推动下寻求破解之道。

同时,网信、公安、工信等部门已开展大量执法行动,取得显著成效。执法进入常态化阶段对执法本身的规范性要求将更加凸显。多法并行如何准确适用法律,如何实现不同执法部门、不同层级、不同地域执法的一致性、协调性、规范性,提升执法的程序化、专业化、精细化、智慧化亟待思考。此外,《法治中国建设规划(2020—2025年)》《法治政府建设实施纲要(2021—2025年)》均要求改进和创新执法方式,加强行政指导等非强制行政手段的运用,广泛运用说服教育、劝导示范、警示告诫、指导约谈等方式,努力做到宽严相济、法理相融,让执法既有力度又有温度。如何在海量的个案中实现执法效果最大化,达到政治效果、社会效果、法律效果、舆论效果的统一需要监管部门、学术界、产业界的共同思考。



值得一提的是，在执法领域，报告义务将持续凸显。近年来，“报告义务”是各国强化网络安全，特别是关键信息基础设施安全保护立法中的重点关注。虽然报告义务置于网络安全整体治理体系中只是一个小的环节，却是要求组织主动向监管部门上报自身存在漏洞等风险隐患或发生安全事件，确保国家及时掌握安全形势的有效途径。因此，事件报告的立法动向，以及具体报告情形、时间、程序等制度细节以及政府将在接收报告后提供何种帮助、采取哪些措施一直受到监管部门和组织的关注。继 2022 年美国、欧盟通过多项立法涉及事件报告要求外，2023 年国内外仍有诸多相关立法动向，以建立或细化义务细节。如临近年末，我国网信、工信部门发布的《网络安全事件报告管理办法（征求意见稿）》《工业和信息化领域数据安全事件应急预案（试行）（征求意见稿）》中对于“1 小时”“立即报告”的表述再次凸显监管部门对于报告环节的重视。

可以预见的是，我国公安、网信、工信等监管部门已充分意识到强化报告要求的重要性，除了继续通过制度文件要求网络运营者、数据处理者、个人信息处理者上报安全风险和安全事件外，在行政执法过程中也将进一步提高对于报告义务落实情况的重视程度，将其列为监督检查、专项行动重要检查内容之一。

（四）趋势四：人工智能包容性、参与式治理纵深发展



人工智能是引领新一轮科技革命和产业变革的战略性技术，全球主要国家和组织加快人工智能治理进程，从“风险管理”、“风险控制”走向“风险治理”。人工智能法律 3.0 带来的思考，是规则的适用性和技术修正的可能性。在正确认识并协调“破坏性创新”与“试验性监管”的基础上，未来人工智能法治有望进一步推动软法与硬法有机结合，关注价值观、治理体系、治理对象、治理技术以及效果评价，形成一个持续优化、修复、完善的包容性体系。

虽然各国有模式路线之争，却并未影响全球人工智能监管共识的凝聚，减轻并缓释技术应用的不利影响、基于风险的人工智能分类分级监管已然成为全球性发展趋势。如何对不同类型的人工智能进行全面性风险评估和影响分析、如何制定分类分级标准、如何实现动态化管控、如何优化类型化治理而非“一刀切”监管，是未来人工智能法立法过程中亟需探讨且不可回避的问题。同时，人工智能带来的风险具有全球性特征，伴随政府间机构、国际组织、行业组织成为引导人工智能向善的重要力量，以伦理、标准为代表的软法有望承担起防范化解人工智能风险的历史使命。

此外，人工智能的治理问题也需借助人工智能本身来共同解决。在人工智能法律 3.0 视域下，代码、人工智能等技术不再只是法律规制的对象，而是成为支持、补充法律规则的治理工具。数字水印、价值对齐等技术治理方案已然融入各国立法，大模型技术及产品评测逐步落地展开，未来对抗生成网络技术、安全增强学习技术、检测与过滤机制、隐私保护技术、区块链技术可进一步赋能安全可信人工智能生态。如何以法治标尺衡量治理技术，如何实现“技术法律化”是人工智能法治下一步要考虑的重要问题。

（五）趋势五：新型网络犯罪治理趋向生态化、预防化、智能化

新时代全球网络犯罪呈现出传统犯罪网络化、网络犯罪链条化、跨地隐蔽打击难、技术更新迭代快等新的变化特点，对传统、单一的回应型打击模式提出新的挑战。在此背景之下，对网络犯罪的规制局限于任何一个环节，都难达到预期效果，以生态治理应对网络犯罪生态化是必然趋势。可以预见，**下一步我国网络犯罪生态治理与立法探索和实践，将向主动化、生态化、预防化、智能化、精准化方向发展，从单个环节的惩治转向全链条、全流程规制，落实网络实名制，加强黑灰产打击治理，消除网络犯罪赖以生存的环境。**同时，伴随国际社会各方参与犯罪治理的积极性凸显，跨境电子证据调取、信息共享、犯罪打击与反制的规则之治有望进一步完善，网络犯罪治理的生态塑造将从国内治理、双边条约、单项合作进一步走向国际治理、国际公约、综合合作。

在微观层面来看，国际社会已然意识到链条化的网络犯罪在很大程度上是可预防的，企业是网络犯罪防治中的重要环节，但各国现行法律大多仅规定企业对犯罪的事后发现报告义务，事前预防、发现、处置的义务较为薄弱。**伴随网络犯罪预防与治理逐步进入各国立法者视野，针对互联网服务提供者的内容审核、安全防控、信息披露、警示引导、及时处置、未成年人保护等义务将进一步明晰。**但如何根据企业主体规模和业务影响程度动态调整犯罪防治义务边界，如何推动企业主体责任、公民自律责任、政府监督责任有机融合是下一步网络犯罪防治立法中要探讨的重要问题。

（六）趋势六：后量子密码标准化将加速“特定重要”领域后量子密码迁移进程

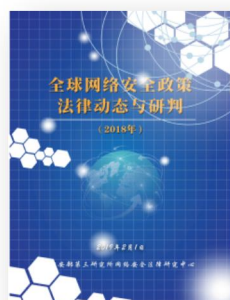
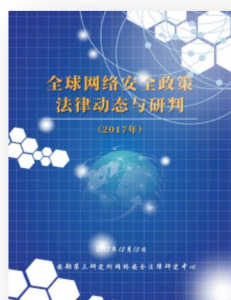
后量子密码已进入到第一个发展鼎盛期，成为保障国家数字经济安全、助力数字经济高质量发展的前瞻性技术与核心竞争力。按照计划，美国 NIST 将于 2024 年正式发布第一批 PQC 标准，为向后量子密码迁移提供标准指引，如何构建兼容和弹性的国际化标准体系将成为标准化工作的下一步难点。近年来，尽管美国、英国、加拿大等国发布战略、指南等文件提醒组织重视量子安全威胁，并为后量子密码迁移做好准备，但多为准备性工作，如提前识别本系统中可能受到量子计算安全威胁的信息系统，列好迁移优先级等，但普遍性和基于“生产”网络和差异化的开展后量子密码迁移工作的较少。可以预见的是，随着 PQC 标准的正式发布和各种兼容、安全问题的进一步研究披露，将推动全球后量子密码迁移工作进行新的阶段。

面对后量子密码迁移带来的机遇与挑战，中国也将从战略、政策、法律和标准层面做好后量子密码迁移的研判与部署。受限于特定时限内的资源和能力，政府需要优先框定具有迫切迁移需求的对象，并保障其迁移资源的合理分配和有效供给。国际层面已形成电力、能源、基础运营商、银行金融机构等具有“特定重要”的关键信息基础设施应优先迁移的共识。“特定重要”的关键信息基础设施领域不仅自身重要，也是其他关键信息基础设施运行的重点保障支撑，更是其他关键信息基础设施迁移的基础。

沿革



作为网络安全领域的专业智库，自 2017 年起公安部第三研究所网络安全法律研究中心整理网络安全政策法律要闻（月度），持续跟进全球相关动态，连续六年编制并向社会公开发布《全球网络安全政策法律发展年度报告》，为产学研各界提供研究素材、指明研究方向、勘定研究前沿，以期为促进我国网络与数据安全法治建设提供助力。



—— 声明 ——



公安部第三研究所网络安全法律研究中心和 360 集团法务中心对本报告全部内容拥有相关版权权利。本报告部分材料来源于网络，若有侵权请联系删除。

未经书面许可授权，任何单位及个人不得以任何方式或理由对本报告进行使用、复制、修改、抄录或传播。

本报告倾注编写团队大量心血，希望每位读者能从中收获知识和见解。在撰稿过程中，编写团队力求尽善尽美，经专家指导组倾力指导、精准把脉，编写团队人员反复琢磨修改最终定稿。由于时间仓促等局限性，难免存在纰漏，请读者朋友们批评、斧正。