# 第一章

# 信息安全的法律法规及产业政策

## 1.1 《国家网络空间安全战略》概要

《国家网络空间安全战略》是为了贯彻落实习近平主席关于推进全球互联网治理体系变革的“四项原则”和构建网络空间命运共同体的“五点主张”，阐明中国关于网络空间发展和安全的重大立场，指导中国网络安全工作，维护国家在网络空间的主权、安全、发展利益而制定的。

《国家网络空间安全战略》经中央网络安全和信息化领导小组批准，由国家互联网信息办公室于 2016 年 12 月 27 日发布并实施。（全文参见附录一）

《国家网络空间安全战略》在以下几个方面值得特别关注：

（1）《国家网络空间安全战略》指出，互联网等信息网络已经成为信息传播的新渠道、生产生活的新空间、经济发展的新引擎、文化繁荣的新载体、社会治理的新平台、交流合作的新纽带、国家主权的新疆域。随着信息技术深入发展，网络安全形势日益严峻，利用网络干涉他国内政以及大规模网络监控、窃密等活动严重危害国家政治安全和用户信息安全，关键信息基础设施遭受攻击破坏、发生重大安全事件严重危害国家经济安全和公共利益，网络谣言、颓废文化和淫秽、暴力、迷信等有害信息侵蚀文化安全和青少年身心健康，网络恐怖和违法犯罪的大量存在直接威胁人民生命财产安全、社会秩序，围绕网络空间资源控制权、规则制定权、战略主动权的国际竞争日趋激烈，网络空间军备竞赛挑战世界和平。

（2）《国家网络空间安全战略》强调，一个安全、稳定、繁荣的网络空间，对各国乃至全世界都具有重大意义。中国愿与各国一道，坚持尊重维护网络空间主权、和平利用网络空间、依法治理网络空间、统筹网络安全与发展，加强沟通，扩大共识，深化合作，积极推进全球互联网治理体系变革，共同维护网络空间的和平安全。中国致力于维护国家网络空间主权、安全、发展利益，推动互联网造福人类，推动网络空间的和平利用与共同治理。

（3）《国家网络空间安全战略》明确，当前和今后一个时期，国家网络空间安全工作的战略任务是坚定捍卫网络空间主权、坚决维护国家安全、保护关键信息基础设施、加强网络文化建设、打击网络恐怖和违法犯罪、完善网络治理体系、夯实网络安全基础、提升网络空间防护能力和强化网络空间国际合作 9 个方面。

## 1.2 《中华人民共和国网络安全法》概要

《中华人民共和国网络安全法》于 2017 年 6 月 1 日起正式实施，成为我国第一部规范网络空间秩序的基础性法律，是我国网络空间法治建设的重要里程碑，是依法治网、化解网络风险的法律重器，是让互联网在法治轨道上健康运行的重要保障。《中华人民共和国网络安全法》将近年来一些成熟的好做法制度化，并为将来可能的制度创新做了原则性规定，为网络安全工作提供切实法律保障。（全文参见附录二）

《中华人民共和国网络安全法》在以下几个方面值得特别关注：

（1）《中华人民共和国网络安全法》明确对公民个人信息安全进行保护，提出了个人信息保护的基本原则和要求，并对加强个人信息保护和惩治非法买卖个人信息等做出了明确规定。例如，第四十四条中规定任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息；第四十三条中规定个人信息被冒用有权要求网络运营者删除；第四十七条中规定网络运营者应当加强对其用户发布的信息的管理。

（2）《中华人民共和国网络安全法》进一步明确了政府各部门的职责权限，完善了网络安全监管体制，将现行有效的网络安全监管体制

法制化，明确了网信部门与其他相关网络监管部门的职责分工。例如，第八条规定，国家网信部门负责统筹协调网络安全工作和相关监督管理工作，国务院电信主管部门、公安部门和其他有关机关依法在各自职责范围内负责网络安全保护和监督管理工作。这种“ 1+$X$ ”的监管体制，符合当前互联网与现实社会全面融合的特点和我国监管需要。

（3）《中华人民共和国网络安全法》第三章用了近三分之一的篇幅规范网络运行安全，特别强调要保障关键信息基础设施的运行安全。关键信息基础设施是指那些一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的系统和设施。网络运行安全是网络安全的重心，关键信息基础设施安全则是重中之重，与国家安全和社会公共利益息息相关。为此，《中华人民共和国网络安全法》强调在网络安全等级保护制度的基础上，对关键信息基础设施实行重点保护，明确关键信息基础设施的运营者负有更多的安全保护义务，并配以国家安全审查、重要数据强制本地存储等法律措施，确保关键信息基础设施的运行安全。

（4）《中华人民共和国网络安全法》第五章将监测预警与应急处置工作制度化、法制化，明确国家建立网络安全监测预警和信息通报制度，建立网络安全风险评估和应急工作机制，制定网络安全事件应急预案并定期演练。

## 1.3 《公共互联网网络安全突发事件应急预案》概要

2017 年 11 月 14 日，工业和信息化部印发《公共互联网网络安全突发事件应急预案》，要求部应急办和各省（自治区、直辖市）通信管理局应当及时汇总分析突发事件隐患和预警信息，发布预警信息时，应当包括预警级别、起始时间、可能的影响范围和造成的危害、应采取的防范措施、时限要求和发布机关等，并公布咨询电话。（全文参见附录三）

《公共互联网网络安全突发事件应急预案》在以下几个方面值得特别关注：

（1）《公共互联网网络安全突发事件应急预案》中，根据社会影响

范围和危害程度，将公共互联网网络安全突发事件分为四级：特别重大事件、重大事件、较大事件、一般事件。其中，特别重大事件包括：全国范围大量互联网用户无法正常上网，.cn 国家顶级域名系统解析效率大幅下降，1 亿以上互联网用户信息泄露，网络病毒在全国范围大面积爆发，以及其他造成或可能造成特别重大危害或影响的网络安全事件。

（2）《公共互联网网络安全突发事件应急预案》中，要求基础电信企业、域名机构、互联网企业、网络安全专业机构、网络安全企业应当通过多种途径监测、收集漏洞、病毒、网络攻击最新动向等网络安全隐患和预警信息，对发生突发事件的可能性及其可能造成的影响进行分析评估；认为可能发生特别重大或重大突发事件的，应当立即向部应急办报告；认为可能发生较大或一般突发事件的，应当立即向相关省（自治区、直辖市）通信管理局报告。

（3）《公共互联网网络安全突发事件应急预案》中，要求建立公共互联网网络突发事件预警制度，并按照紧急程度、发展态势和可能造成的危害程度，将公共互联网网络突发事件预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色标示，分别对应可能发生特别重大、重大、较大和一般网络安全突发事件。发布预警信息时，应当包括预警级别、起始时间、可能的影响范围和造成的危害、应采取的防范措施、时限要求和发布机关等，并公布咨询电话。面向社会发布预警信息可通过网站、短信、微信等多种形式。

## 1.4 信息安全产业政策

### 1.4.1 国内信息安全产业现状

近年来，随着互联网、通信、物联网、人工智能等技术的迅猛发展，我国信息安全产业进入了高速发展期。与此同时，由于国家、企业和个人信息安全意识的不断提升，以及每年计算机及网络犯罪活动带来的巨额损失与巨大威胁，信息安全的需求范围及层次也在不断拓展。

#### 1.4.1.1 重磅政策加速落地，行业成长再上新台阶

近年来，随着国内网络安全事件频繁发生，我国政府对于信息安全防护体系的建设意识逐渐加强，政策支持力度不断上升。2016 年年初，网络安全被正式划入“十三五”规划重点建设方向，在政府未来 5 年的 100 项重大建设项目中排在第 6 位，政府重视程度达到前所未有的高度。随着顶层设计的明确，2016 年下半年开始，相关支持政策出台速度明显加快，包括《中华人民共和国网络安全法》《国家网络空间安全战略》《战略性新兴产业重点产品和服务指导目录》在内的多个重磅政策文件密集出台，加速推动信息安全产品需求释放。从政策趋势来看，未来政府对信息安全建设的支持力度有望继续提升。

信息安全防护体系建设的政策支持力度自2016年下半年起逐步提升。政策驱动下各领域安全防护投资力度不断加大，行业市场规模快速增长。随着近年政策扶持力度的提升，政府、军队、电信、银行等关键领域对于信息安全建设的力度明显加大，带动我国信息安全市场呈现快速发展的态势。根据数据显示，2012 年我国信息安全产业规模仅为 157.26 亿元，2016 年这一市场规模已升至 341.72 亿元。而且随着政策的加快推动，云计算对于 IT 基础设施的重构，以及物联网设备的迅速增长，我国网络信息安全行业迎来全新的发展阶段，预计 2017—2021 年的行业复合增速为 23.2%，2021 年行业整体规模将达到千亿元级，行业景气度将持续走高。

#### 1.4.1.2 信息安全领域资本热度不降反增，行业集中度持续提升

我国信息安全细分领域众多且厂商集中度差，行业集中度提升是必然趋势。主要基于以下几方面考虑：① 由于信息安全单一子行业规模都相对较小且不同子行业间的技术壁垒较高，而信息安全又是一个 360 度全方位的防护建设工程，拥有完整软硬件解决方案及系统集成能力的厂商必将拥有更强的竞争优势，因此行业龙头厂商在布局综合安全产品阶段势必加大在不同子领域的兼并收购。② 随着云计算、大数据等新兴领域的快速发展，具有深厚攻防等核心技术积累及完整解

决方案的龙头公司在处理云安全等相关问题方面将拥有更为成熟可信的综合实力，市场份额将自然地向龙头集中。

资本市场热情不减反增，助力信息安全领域的投资并购数目不断增多。虽然从 2016 年开始，整体资本市场环境逐渐趋冷，但对于信息安全领域的热度却不降反增。数据显示，2016 年第三季度风险投资网络安全交易共 19 宗，是自 2014 年第二季度以来投资交易数量最多的一个季度，而且过去 6 个季度网络安全领域风险投资交易数量都在 12 宗以上。资本热情的提升显示市场热度显著升温，资本的持续投入将助力产业整合加速发展。

#### 1.4.1.3 工控信息安全等保障制度出台在即，行业临近爆发点

国内工业领域加速进入智能制造新时代，工控设备联网成为必然趋势。2016 年开始，各国相继将战略核心聚焦智能制造领域：德国提出“工业 4.0”；英国提出“高值制造”；美国提出“先进制造”；我国也于 2015 年 5 月 8 日提出“中国制造 2025”战略，其内涵核心是把信息互联技术与传统工业制造相结合，形成生产智能化，提高资源利用率，以此来提升整个国家竞争力。由此可见，未来随着“中国制造 2025”战略的推进，工业领域设备联网实现智能化将成为必然的趋势。

随着工业联网的深入，包括电力、烟草、轨道交通、冶金、石油石化、钢铁、煤炭、燃气等多个行业的工控设备对于互联网、办公网、控制网、设备网等的连接变得更加紧密。其安全方面所面临的威胁也逐渐从传统的断网、宕机等非攻击事件转变为来自互联网领域病毒、漏洞、恶意代码等攻击导致的安全问题。且从工控领域被攻击所可能导致的后果来看，其潜在威胁极大。例如，2014 年出现的 Havex 漏洞，不仅可以禁用水电大坝、使核电站过载，甚至还有能力关闭一个国家的电网。因此，工控安全深刻地影响着工业控制网络产业的发展，是智能制造顺利推进的前提保障。

传统的信息安全主要针对管理网和办公网的安全防护，而针对工控系统的安全防护市场总体规模较小。我国工业信息安全行业发展具有三大特点，分别是核心技术自主可控度偏低、相关技术落后依赖国外以及产业生态体系不完整。为改变我国工业信息安全行业存在的这

些问题，国家不断出台相关政策调整产业结构，促进产业发展，鼓励工业信息化创新自主发展。

2016 年 10 月 13 日，国家质检总局、国家标准委发布中华人民共和国国家标准公告（2016 年第 17 号），其中包括了由全国工业过程测量控制和自动化标准化技术委员会（SAC/TC124）秘书处组织国内自动化领军企业、科研院所专家以及来自钢铁、化工、石油、石化、电力、核设施等领域的行业用户，结合 DCS 和 PLC 核心技术及工程实践，自主制定的 6 项有关工业控制系统信息安全的国家标准。此后，国内各行各业对工控系统安全建设的认识逐步提升，包括电力、烟草、石化、制造等多个行业陆续制定了相应的指导性文件，指导落实相应行业的工控安全检查及整改活动。近年来，有关工控安全的国家标准和政策法规参见表 1.1 和表 1.2。

表 1.1　近年来有关工控安全的国家标准

| 序号 | 标准号 | 标准名称 |
|---|---|---|
| 1 | GB/T 33007-2016 | 《工业通信网络 网络和系统安全 建立工业自动化和控制系统安全程序》 |
| 2 | GB/T 33008.1-2016 | 《工业自动化和控制系统网络安全 可编程序控制器（PLC）第 1 部分：系统要求》 |
| 3 | GB/T 33009.1-2016 | 《工业自动化和控制系统网络安全 集散控制系统（DCS）第 1 部分：防护要求》 |
| 4 | GB/T 33009.2-2016 | 《工业自动化和控制系统网络安全 集散控制系统（DCS）第 2 部分：管理要求》 |
| 5 | GB/T 33009.3-2016 | 《工业自动化和控制系统网络安全 集散控制系统（DCS）第 3 部分：评估指南》 |
| 6 | GB/T 33009.4-2016 | 《工业自动化和控制系统网络安全 集散控制系统（DCS）第 4 部分：风险与脆弱性检测要求》 |
| 7 | GB/T 36323-2018 | 《信息安全技术 工业控制系统信息安全管理基本要求》 |
| 8 | GB/T 36324-2018 | 《信息安全技术 工业控制系统信息安全分级规范》 |
| 9 | GB/T 37980-2019 | 《信息安全技术 工业控制系统安全检查指南》 |

表 1.2　近年来有关工控安全的政策法规

| 序号 | 发文机关 | 发文字号 | 政策标题 |
|---|---|---|---|
| 1 | 国务院 | 国发〔2016〕28 号 | 《国务院关于深化制造业与互联网融合发展的指导意见》 |
| 2 | 工业和信息化部 | 工信部信软〔2016〕338 号 | 《工业控制系统信息安全防护指南》 |
| 3 | 工业和信息化部 | — | 《信息安全技术工业控制系统信息安全检查指南》 |

### 1.4.2　国家级信息安全产业政策

#### 1.4.2.1　《国家网络安全产业发展规划》正式发布

2019 年 6 月 30 日，在中国软件产业发展情况新闻发布会上，《国家网络安全产业发展规划》正式发布，工业和信息化部与北京市人民政府决定建设国家网络安全产业园区。这是继“等保 2.0”之后又一网络安全领域国家顶层规划政策，信息安全的国家战略地位进一步得到肯定。信息安全下游客户以政府、金融和电信等行业为主，整体发展受政策影响较大，预计该规划对未来信息安全产业的发展有巨大的指导意义。

根据规划，到 2020 年，依托产业园带动北京市网络安全产业规模超过 1000 亿元，拉动 GDP 增长超过 3300 亿元，打造不少于 3 家年收入超过 100 亿元的骨干企业。到 2025 年，依托产业园建成我国网络安全产业“五个基地”：一是国家安全战略支撑基地；二是国际领先的网络安全研发基地；三是网络安全高端产业集聚示范基地；四是网络安全领军人才培育基地；五是网络安全产业制度创新基地。该产业园是继国家网络安全产业园区（长沙）之后又一国家级网络安全产业园，位于政府部门和央企集中的北京，战略地位更加突出；相比于现有的网络安全市场体量，该产业园规划的产业规模巨大，预计相关部门对网络安全领域的支持力度和投入将进一步加大。

#### 1.4.2.2　“促进网络安全产业发展的指导意见”拟加快出台

2019 年 8 月 19 日—20 日，第七届互联网安全大会（ISC）在北京雁栖湖国际会议中心举行。来自中国、美国、以色列、俄罗斯等国家

的专家学者，以“应对网络战、共筑大生态、同筑大安全”为主题，共同探讨大安全时代网络安全生态建设的发展之路。

2019 年 8 月 21 日，2019 北京网络安全大会（BCS）在北京国家会议中心召开。工业和信息化部副部长陈肇雄为大会致辞，宣布我国将进一步优化产业政策环境，加快出台促进网络安全产业发展的指导意见，推进国家网络安全产业园区建设，完善 5G、工业互联网、车联网等领域的网络安全产品和服务将成为下一步部署重点。

陈肇雄强调，面对网络安全新形势、新挑战，要坚持总体国家安全观，树立正确的网络安全观，加快推进我国网络安全产业高质量发展，有效支撑网络空间安全保障，服务制造强国和网络强国建设。一是坚持创新引领。加强基础性、通用性、前瞻性技术创新，积极利用人工智能、大数据等技术赋能网络安全。充分发挥企业主体作用，激发创新活力，推广创新应用，构建多领域、多层次的网络安全技术创新体系。二是坚持需求导向。面向 5G、工业互联网、车联网等融合领域安全需求，加快完善网络安全产品和服务支撑体系，建设网络安全防护体系，提升态势感知、监测预警、应急响应能力。三是坚持科学布局。优化产业政策环境，加快出台促进网络安全产业发展的指导意见，扎实推进国家网络安全产业园区建设，加强人才队伍建设，全力打造“政、产、学、研、用”一体化的产业生态。四是坚持合作共赢。发挥政府、国际组织、企业、科研院所等各方作用，加强与“一带一路”沿线国家在网络安全领域开展交流合作，共同应对网络安全威胁与挑战，共同维护网络空间安全秩序。

#### 1.4.2.3 《中国工业信息安全产业发展白皮书（2018—2019）》重磅发布

2019 年 6 月 22 日，由工业和信息化部指导、国家工业信息安全发展研究中心和工业信息安全产业发展联盟共同主办的 2019 年中国工业信息安全大会在北京国际会议中心召开。国家工业信息安全发展研究中心副主任、工业信息安全产业发展联盟秘书长何小龙出席大会并发布《中国工业信息安全产业发展白皮书（2018—2019）》。白皮书深入阐述了工业信息安全产业的内涵和范畴，围绕工业信息安全产业的几

个关键要素，重点从产业规模结构、政策环境、技术发展、行业应用、人才培养及市场竞争格局等进行了梳理，深度剖析了现阶段我国工业信息安全产业发展面临的挑战，对产业发展趋势进行了科学预测。白皮书显示，2018 年我国工业信息安全产业规模为 70.32 亿元，市场增长率达 33.55%，工业信息安全产业规模加速扩容，预计 2019 年市场整体规模增长至 93.91 亿元。

### 1.4.3 重庆市信息安全产业现状

#### 1.4.3.1 重庆掀起信息安全产业技术新革命，成立重庆信息安全产业技术创新联盟

2017 年 11 月 2 日，重庆信息安全产业技术创新联盟正式成立。联盟是在重庆市经济和信息化委员会、重庆市科委的支持和指导下，由重庆信息安全产业研究院牵头发起的技术创新合作组织。

重庆信息安全产业技术创新联盟成立后落户重庆市合川区，在毗邻两江新区的草街新城规划建设 22 平方公里的信息安全产业园。联盟创建时共有 39 个市内外会员单位，汇集了信息安全产业各领域的众多骨干企业、科研院所、企事业单位和高等院校。

重庆信息安全产业技术创新联盟是一个融合“政、产、学、研、用、资”的资源整合共享平台，围绕信息安全产业，以市场为导向，以企业为主体，促进成员间资源共享和互惠互利，提升联盟成员的群体竞争力。联盟还将进一步加强创新联动，将更多高校、企业、研究所等聚集到一起，整合优势资源，加快突破核心技术，加强技术创新成果转化应用，努力培育同行业、同领域更多标杆性企业。同时，搭建更多合作平台，推动信息安全产业领域人才、信息、资源等方面互联互通，为重庆市实施创新驱动战略、信息安全产业持续健康发展作出更大的贡献。

#### 1.4.3.2 重庆信息安全产业基地

2018 年 1 月 10 日，重庆信息安全产业基地项目在重庆市合川区草街街道开工建设。项目规划面积 1000 余亩，生产基地建设规模 10 万

平方米，计划 2019 年竣工。

项目主要由北京赛普星通投资管理有限公司牵头出资组建的重庆恒芯天际科技有限公司为龙头，建设通信技术产业总部、研发基地、实验楼、交易展示区及生产基地等；并在新的安全形势下，推动移动互联网、云计算、物联网、大数据、工业软件等新一代信息技术领域信息安全技术和产品的研发和产业化。

### 1.4.4 重庆市级信息安全产业政策

#### 1.4.4.1 将合川信息安全产业基地纳入《重庆市以大数据智能化为引领的创新驱动发展战略行动计划（2018—2020 年）》

合川区地处成渝经济区核心地带，是重庆市新型工业化的主战场之一，拥有较好的区位优势和良好的电子信息制造业、汽摩制造业、现代服务业等产业基础优势。近年来，合川区以打造信息安全产业基地为目标，通过市区联合推进机制，以恒芯天际、中兴通讯等为代表的信息安全相关企业持续快速发展，信息安全产业基地加速建设，招商引资取得实效，产业供给要素加速聚集，为加快培育以信息安全为主的信息产业奠定了坚实的基础。

目前，在市区共同推进下，基地的规划、生产、建设、研发、产业招商、培训等板块，通过工作任务清单的方式有序推进：一是《重庆市合川区信息安全产业发展规划》于 2018 年 2 月通过专家评审，为合川信息安全产业发展提供了“长远规划”和“发展蓝图”；二是基地龙头企业——重庆恒芯天际科技有限公司生产经营正常，2017 年实现产值 50 亿元；三是生产基地于 2018 年 1 月举行开工仪式，各项前期工作有序开展，计划 2019 年底建成投产，项目纳入 2018 年重庆市百项重点关注项目；四是信息安全产业研究院、合川区信息安全产业专家委员会和重庆信息安全产业技术创新联盟已组建完毕，积极汇聚行业创新资源；五是产业招商工作取得实效，上海星地通通信科技有限公司、上海赢联信息技术有限公司等 10 多个项目落地，德国 MiNaCon 公司、工信部软促中心智能制造紧缺人才培养工程等培训项目积极推进。

在总体上，合川的信息安全产业仍处于起步阶段，存在产业基础

相对薄弱、配套体系建设不够完善、产业高端人才支撑不足等问题，为加快推进合川信息安全产业发展，重庆市还将着力做好以下工作：

一是将合川信息安全产业基地列入《工业和信息化部与重庆市人民政府合作框架协议》，力争部市共建。积极对接工信部软促中心、工信部电子一所（国家工业信息安全发展研究中心）等机构，引进人才、平台、项目等资源，形成良好产业发展氛围。

二是将合川信息安全产业基地纳入《重庆市以大数据智能化为引领的创新驱动发展战略行动计划（2018—2020 年）》，利用市区联合推进机制加速推进，重点在招商引资、项目布局、创新资源聚集等方面取得进展。

三是积极借鉴成都、上海、杭州等信息安全产业发达地区成功经验，会同合川区制定针对信息安全产业的人才、土地、税收等优惠政策，积极扶持龙头企业发展和产业集聚，构建产业生态，打造产业高地。

四是在重庆市工业和信息化专项资金项目安排上进行倾斜，促进恒芯天际等龙头企业快速成长，带动合川信息安全产业基地产业发展。

#### 1.4.4.2　加快发展工业互联网平台

工业互联网是新一代信息通信技术与制造业深度融合的关键基础设施、新型应用模式和全新工业生态，是互联网从消费领域向生产领域、从虚拟经济向实体经济拓展的核心载体。抢抓数字革命重要窗口期，加快发展工业互联网平台企业，加速产业集聚融合，对于推动大数据智能化为引领的科技创新，推进数字产业化、产业数字化，促进制造业高质量发展，建设现代化经济体系具有重要意义。

重庆市就加快发展工业互联网平台企业赋能制造业转型升级提出了具体的指导意见（全文参见附录四）。意见提出：到 2022 年，初步构建起工业互联网平台赋能制造业的发展格局，形成工业互联网平台生态和支撑体系；推动工业互联网平台和标识解析协同发展，力争形成工业互联网标识解析体系区域核心，争创国家级工业大数据制造业创新中心；引进一批第三方服务平台，培育 3～5 家具有国内竞争力的平台；发展一批制造业开放服务平台，建设 20 个以上个性化定制、网络化协同、服务化转型的平台。