构建安全可信的数字世界
Build A Secure And Credible Digital World

安恒信息
DAS-security 安全中国

科创板：688023

法律法规政策解读

安恒信息
DAS-security 安全中国

安恒信息技术股份有限公司
DBAPPSecurity Co., Ltd.

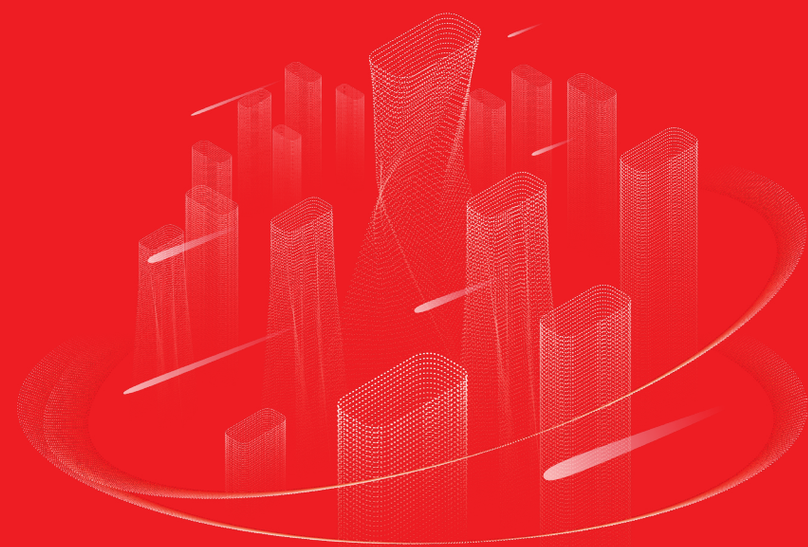
官网：www.dbappsecurity.com.cn
电邮：info@dbappsecurity.com.cn
客服专线：+86-400-6059-110

安恒信息资讯

杭州总部
地址：杭州市滨江区西兴街道联慧街188号安恒大厦
座机：0571-88380999/28860999
传真：0571-28863666

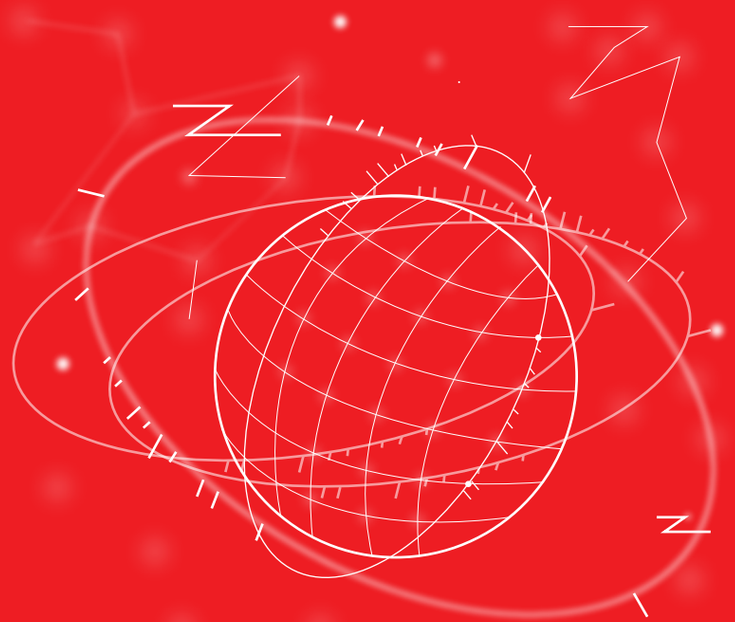
科创板：688023

目录



第一篇

《中华人民共和国网络安全法》解读



★ ★ ★ ★ ★

导入语

数字化云奔潮涌，网络安全牵涉到国家安全和社会稳定。为保障网络安全，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制定，2016年11月7日中华人民共和国第十二届全国人民代表大会常务委员会第二十四次会议审议通过了《中华人民共和国网络安全法》（以下简称《网络安全法》），该法自2017年6月1日起施行。《网络安全法》是我国第一部全面规范网络空间安全管理方面问题的基础性法律，下面我们将带大家一起回顾网络安全法要点内容。

★ ★ ★ ★ ★

★ 法律全文构成 ★

全法共七章七十九条，除常规章节外，《网络安全法》从网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置四个方面展开。

网络安全法

第一章 总则

第二章 网络安全支持与促进

第三章 网络运行安全

第四章 网络信息安全

第五章 监测预警与应急处置

第六章 法律责任

第七章 附则

★ 本法适用范围 ★

在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理。

★ 三大考虑、六大亮点、三个特点 ★

一、制定《网络安全法》的三个考虑

- **制定网络安全法是落实国家总体安全观的重要举措。**

  有利于适应我们国家网络安全工作新形势、新任务，落实中央决策部署，保障网络安全和发展利益。

- **制定网络安全法是维护网络安全的客观需要。**

  中国是面临网络安全威胁最严重的国家之一，制定网络安全法有利于提高全社会的网络安全意识和网络安全的保护水平，使我们的网络更加安全、更加开放、更加便利，也更加充满活力。

- **制定网络安全法是维护国家广大人民群众切身利益的需要。**

  制定网络安全法顺应时代的要求，回应广大人民群众对加强网络空间的法制建设、净化网络环境，使网络空间清朗起来的呼声和期待，把最广大人民群众的切身利益来维护好、发展好、实现好。

二、《网络安全法》六大亮点内容

- 明确了网络空间主权的原则；
- 明确了网络产品和服务提供者的安全义务；
- 明确了网络运营者的安全义务；
- 进一步完善了个人信息保护规则；
- 建立了关键信息基础设施安全保护制度；
- 确立了关键信息基础设施重要数据跨境传输的规则。

三、《网络安全法》三个特点

- **全面性**
  - 比较全面和系统地确立了各个主体在网络安全保护方面的义务和责任；
  - 确立了保障网络的设备设施安全，网络运行安全、网络数据安全，以及网络信息安全等各方面的基本制度。

- **针对性**
  - 从我国的国情出发，坚持问题导向，总结实践经验；
  - 借鉴了其他国家的一些做法，建立保障网络安全的各项制度；
  - 重在管用、重在解决实际问题。

- **协调性**
  - 在立法过程中始终坚持安全与发展并重的原则，协调推进网络安全和发展；
  - 注重保护网络主体的合法权益，保障网络信息依法、有序、自由地流动；
  - 促进网络技术创新，最终实现以安全促发展，以发展来促安全的目的。

★ 首次确立网络空间主权原则 ★

互联网的出现使“地球村”的预言成为现实，高全球化的特性使人类生活、工作与思维均发生了巨大的变革。人类活动空间正在逐步拓展到网络空间，因此国家主权也逐渐从陆地、海洋、天空向网络空间延伸，形成基于国家领土主权“领陆、领空、领海”三维空间延伸出的网络空间主权——“领网权”。“领网权”作为国家主权的第四维空间，将与领土权、领空权、领海权并列成为国际法框架下国家主权的重要组成部分。

“互联网发展是无国界、无边界的，利用好、发展好、治理好互联网必须深化网络空间国际合作，携手构建网络空间命运共同体”“全球互联网治理体系变革进入关键时期，构建网络空间命运共同体日益成为国际社会的广泛共识。”习近平主席多次围绕构建网络空间命运共同体发表重要论述。《网络安全法》首次确立了网络空间主权原则，没有网络安全就没有国家安全，没有网络主权就没有网络空间安全。

《网络安全法》第五条

国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

《网络安全法》第七条

国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

★ 明确主体义务，坚守各方职责 ★

一、主体身份：监督管理部门

- **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**
  - 依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

- **县级以上地方人民政府有关部门**
  - 按照国家有关规定确定网络安全保护和监督管理职责。

- **国务院和省、自治区、直辖市人民政府**
  - 应当统筹规划，加大投入，扶持重点网络安全技术产业和项目；
  - 支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务；
  - 保护网络技术知识产权；
  - 支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

- **省级以上人民政府**
  - 网络安全事件发生的风险增大时应要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测与预测，并向社会发布网络安全风险预警；
  - 发现网络存在较大安全风险或者发生安全事件的，可约谈该网络运营者的法定代表人或者主要负责人；
  - 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

- **各级人民政府及其有关部门**
  - 组织开展经常性的网络安全宣传教育，
  - 指导、督促有关单位做好网络安全宣传教育工作。

二、主体身份：监督管理部门

- 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

- 网络运营者应履行的安全保护义务
  - 制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
  - 采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；
  - 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；
  - 采取数据分类、重要数据备份和加密等措施；
  - 法律、行政法规规定的其他义务。

三、主体身份：网络产品、服务提供者

- 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

- 1.网络产品、服务应当符合相关国家标准的强制性要求；

  2.不得设置恶意程序；

  3.发现其络产品、服务存在安全缺陷、漏洞等风险时，应当立即补救，照规定及时告知用户并向有关主管部门报告；

  4.为其产品、服务持续提供安全维护；

  5.在规定或者当事人约定的期限内，不得终止提供安全维护；

  6.具有收集用户信息功能的，其提供者应当向用户明示并取得同意；

  7.涉及用户个人信息的，应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

★ 网络安全为人民，网络安全靠人民 ★

一、个人、组织的义务

- 任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。
- 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。
- 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。
- 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。
- 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

二、个人、组织的权利

- 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。
- 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息：发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

★ 保护个人信息 ★

- **网络安全监管机构对个人信息、隐私和商业秘密应保密**
- **任何个人和组织不得发布与违法犯罪有关的信息**
- **公民个人有信息删除权和更权**
- **网络运营者**
  - 【原则】收集、使用个人信息，应当遵循合法、正当、必要的原则；
  - 【需经同意】公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。
  - 未经被收集者同意，不得向他人提供个人信息。（经过处理无法识别特定个人且不能复原的除外）
  - 不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集；
  - 不得泄露、篡改、毁损其收集的个人信息；
  - 当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。
- **依法负有网络安全监督管理职责的部门及其工作人员须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密**

★ 保障关键信息基础设施运行安全 ★

一、关键信息基础设施是什么？

- 公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的信息基础设施。

二、除一般安全保护义务外，关键信息基础设施的运营者还应当履行哪些安全保护义务？

- **人员管理**
  - 设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；
  - 定期对从业人员进行网络安全教育、技术培训和技能考核。

- **预防**
  - 对重要系统和数据库进行容灾备份；
  - 制定网络安全事件应急预案，并定期进行演练。

- **评估**
  - 自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估；
  - 将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

- **采购网络产品和服务**
  - 通过国家网信部门会同国务院有关部门组织的国家安全审查；
  - 按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

- **数据存储**
  - 在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储；
  - 因业务需要，确需向境外提供的，应当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。

三、国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

- 对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；
- 定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；
- 促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；
- 对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第二篇

《中华人民共和国数据安全法》解读

★ ★ ★ ★ ★

导入语

2021年6月10日，新华社报道，十三届全国人大常委会第二十九次会议通过了数据安全法。这部法律是数据领域的基础性法律，也是国家安全领域的一部重要法律，将于2021年9月1日起施行。

数字化改革推动我国生产模式的变革，随着经济数字化、政府数字化、企业数字化的建设，数据已经成为我国政府和企业最核心资产。合资企业、跨境贸易、多厂商全球合作的模式变迁，数据开始在企业与企业之间、政府与企业之间以及国与国之间流转、融合、使用。

根据公开报道，2020年全球数据泄露的平均损失成本为1145万美元，2019年数据泄露事件达到7098起，涉及151亿条数据记录，比2018年增幅284%，数据泄漏事件影响大、损失重。

有专家提出，对数据掌控、利用以及保护能力，已成为衡量国家之间竞争力的核心要素。

★ ★ ★ ★ ★

外力驱动和内部需求促使数安法落地

外力驱动

2018年3月23日，时任美国总统特朗普正式签署《澄清域外合法使用数据法》，法案要求对危害美国国家安全的犯罪、严重刑事犯罪等重大案件，无论服务提供者的通信、记录或其他信息是否存储在美国境内，要求服务商根据该法案进行调取并提供相关证据。

2018年5月25日，欧盟《通用数据保护条例》（GDPR）正式实施。GDPR法案要求不论数据控制者、处理者及其处理行为在欧盟境内还是境外，只要处理的是欧盟境内居民的数据，均适用此法案，对数据实施长臂管理。

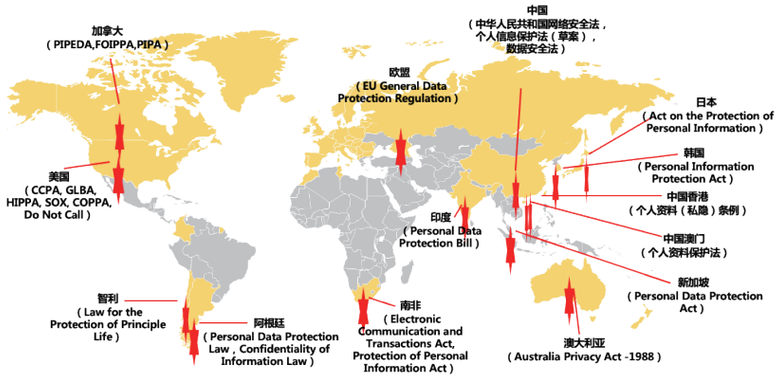


图1 全球数据安全保护立法情况（部分）

目前全球已有近100个国家和地区制定了数据安全保护的法律，数据安全保护专项立法已成为国际惯例。

面对欧美国家将数据主权从物理边界转向技术边界，将会直接影响到第三方国家的主权，在数据跨境流动愈加频繁的今天，必须尽快完善我国相关法律法规，保护我国国家利益、跨国公司以及公民个人利益。

内部需求

当前全球传统经济增长缓慢，尤其是2020年全球“新冠疫情”给经济带来了沉重的打击。迫切需要通过新的经济增长点拉动内需，增加就业，而数字经济正是切入点和发动机，将发展数字经济提升到国家战略高度则水到渠成。

近年来数字经济增速也证明了数字经济发展空间的巨大，中国信息通信研究院发布的《中国数字经济发展白皮书》数据显示，我国数字经济的总体规模已从2005年的2.62万亿元增长至2019年的35.84万亿元;数字经济总体规模占GDP的比重也从2005年的14.2%提升至2019年36.2%。中国信息通信研究院最新发布的数据显示，2020年中国数字经济规模达39.2万亿元，占GDP比重上升至38.6%。

可见，数字经济已成为我国国民经济增长要素的重要一员。从2015年，国务院发布的《促进大数据发展行动纲要》开始，2018年国务院发布《科学数据管理办法》，2020年国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，2021年3月12日，新华社公布了《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》，数据安全政策导向明确，国家数据战略清晰。因此，亟需一部国家的基本法，为中国数字经济的安全发展保驾护航。

上述背景下数安法诞生，恰逢其时，旨在维护我国的数据主权，保障国家的安全、促进经济健康发展。

图2 2005-2020年我国数字经济规模

数安法要点解读和提炼

数安法的发布标志着我国将数据安全保护的政策要求，通过法律文本的形式进行了明确和强化。

本法一共七章五十五条，其中 “总则”、“法律责任”及“附则”三章属于常规章节，另外四个章节围绕着“数据安全与发展、数据安全制度、数据安全保护义务、政务数据安全与开放”展开。

数据安全法

第一章 总则
第二章 数据安全与发展
第三章 数据安全制度
第四章 数据安全保护义务
第五章 政务数据安全与开放
第六章 法律责任
第七章 附则

我们对数安法进行深入解读后，为大家提炼出39个要点。

总则的要点

1 适用范围

在中国境内开展数据活动的组织和个人。

2 定义数据

是指任何以电子或者其他方式对信息的记录。

3 保护要求

采取必要措施，对数据进行有效保护和合法利用，并持续保持其安全能力。

4 责任任务

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主要行业会落地数据保护行业规范，并且落地本部门的数据安全规范。公安机关、国家安全机关等在各自职责范围内承担数据安全监管职责。网信部门负责统筹协调和监管。

5 特别强调

特别的对行业组织提出了制定安全行为规范，加强行业自律，指导会员加强数据安全保护的要求。这项法规有效地消灭了灰色地带，对各行业都形成了法律约束，杜绝了数据的随意共享和流转。

数据安全与发展要点

6 发展原则

国家统筹发展和安全，坚持保障数据安全与促进数据开发利用并重。

7 战略要求

省级以上人民政府应制定数字经济发展规划。进一步细化了国家数据战略的执行主体。

8 标准体系

国家主管部门负责相关标准和体系的制定。

9 评估认证

国家促进数据安全检测评估、认证等服务的发展，支持专业机构依法开展服务。

10 人才培养

要采取率多种方式培养数据开发利用技术和数据安全专业人才。

11 特别强调

特别地，加强了公共服务的要求，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

数据安全制度要点

12 分类分级

国家建立数据分类分级保护制度，对数据实行分类分级保护，并确定重要数据目录，加强对重要数据的保护。

13 风险评估

要建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。

14 **应急处置**

要建立数据安全应急处置机制。

15 **安全审查**

要建立数据安全审查制度。

16 **出口管制**

对属于管制物项的数据依法实施出口管制，可以根据实际情况对该国家或者地区对等采取措施。这项法规进一步明确了国家对中国数据的主权，即我国数据是否在境内，并受到中国法律的保护。

数据安全保护义务要点

17 **管理制度**

在网络安全等级保护制度的基础上，建立健全全流程数据安全管理制度，组织开展教育培训。重要数据的处理者应当明确数据安全负责人和管理机构，进一步落实数据安全保护责任主体。

18 **风险监测**

对出现缺陷、漏洞等风险，要采取补救措施；发生数据安全事件，应当立即采取处置措施，并按规定上报。

19 **风险评估**

定期开展风险评估并上报风评报告。

20 **数据收集**

任何组织、个人收集数据必须采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

21 **数据交易**

数据服务商或交易机构，要提供并说明数据来源证据，要审核相关人员身份并留存记录。

22 **经营备案**

数据服务经营者应当取得行政许可，服务提供者应当依法取得许可。

23 **配合调查**

要求依法配合公安、安全等部门进行犯罪调查。境外执法机构要调取存储在中国的数据，未经批准，不得提供。

24 **特别强调**

特别的，对关基信息基础设施的运营在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

政务数据安全与开放要点

25 **管理制度**

建立健全全流程数据安全管理制度，落实数据安全保护责任。

26 **存储加工**

委托他人存储、加工或提供政务数据，应当经过严格审批，并做好监督。受托方不得擅自留存、使用、泄露或向他人提供政务数据。

27 **数据开放**

构建统一政务数据开放平台，发布数据开放目录，推动政务数据开放利用。

28 **适用主体**

法律、法规授权的具有管理公共事务职能的组织。

法律责任要点

29 不履行规定保护义务

责令改正和警告，给予单位5万至50万元罚款，给予负责人1万至10万元罚款；拒不改正或造成大量数据泄漏等严重后果的，给予单位50万至200万元罚款，最高责令吊销相关业务许可证或者吊销营业执照，给予负责人5万至20万元罚款。

30 危害国家安全和损害合法权益的

给予200万至1000万元罚款，责令停业整顿、吊销相关业务许可证或者吊销营业执照，构成犯罪的，追究刑事责任。

31 未经审批向境外提供重要数据的

违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

32 交易来源不明的数据

没收违法所得，对违法所得一至十倍罚款。没有违法所得或违法所得不足10万元的给予10万至100万元罚款，最高责令吊销营业执照；对主管和直接责任人1万至10万元罚款。

33 拒不配合数据调取的

由有关主管部门责令改正，给予警告，可以并处5万元至50万元罚款，对直接负责的主管人员和其他直接责任人员可以处1万至10万元罚款。

34 国家机关不履行安全保护义务

对负责人和直接责任人员依法处分。

35 国家工作人员违法

因玩忽职守、滥用职权、徇私舞弊，依法给予处分。

36 窃取或非法获取数据的

依照有关法律、行政法规的规定处罚。

37 给他人造成损害

依法承担民事责任，构成犯罪的，依法追究刑事责任。

附则要点

38 涉及国家秘密的数据

依据《中华人民共和国保守国家秘密法》以及相关法律法规执行。

39 涉及军事秘密的数据

由中央军事委员会依据本法另行制定。

数安法是继《网络安全法》提出数据的概念后，国家在数据安全立法层面的一个重大里程碑，是中国数字经济高速发展的压舱石和定海神针。

数据安全建设的几点建议

数安法作为数据安全管理的基本大法，给我们指明了方向并提供法律保障。有关单位和个人收集、存储、使用、加工、传输、提供、公开数据资源，都应当依法建立健全数据安全管理制度，采取相应技术措施保障数据安全。

如何保护数据

数据安全、访问控制和数据保护听起来可能类似，但有一些区别需要注意

数据安全
你是你说的那个人吗

访问控制
证明你是你说的那个人

数据保护
如何确保数据已经被保护

未来如何做好数据安全建设?

政企在进行数据安全能力建设时，考虑数据安全、访问控制以及数据保护三个层面。形象地说，数据安全的首要目标是需要找数据在哪里？数据的主体是谁？访问控制是目前主流的数据安全能力之一，首要目标是数据使用者如何证明具备相应的数据权限？数据保护是更高层面的建设框架，首要目标是组织或个人如何确保数据已经被保护好了？

对于IT和信息安全从业人员来说，数据安全能力建设是最艰巨的任务之一。

关于数据安全能力的建设，安恒信息首席科学家刘博认为：

在业务层面，应当考虑建设包含预防、发现、消除泄密隐患为主的数据安全体系；

在技术层面，应当考虑建设数据风险核查能力、数据梳理能力、数据保护能力以及数据威胁监控预警能力4大核心数据能力；

最终建立“数据安全运营”的全过程自适应安全支撑能力，直至达到整体智治的安全目标。

1、建立健全管理组织体系和组织架构

企业数据安全管理的成败，主要取决主要领导是否重视？意识是否提升？全员是否参与？是否建立了一套完善数据安全管理组织？这是数据安全的重要保障。要形成“管理层重视、一把手负责、全员参与”的管理模式。

数据安全的六大基础

1. 意识到信息安全不仅是首席信息官的工作。
2. 将数据和信息视为业务资产般保护。
3. 保护可移动媒体和移动设备上的重要数据。
4. 知道您组织的重要数字资产的位置。
5. 意识到并非所有数据泄露都是由于外部攻击而发生的。员工也可能有意或无意地导致数据泄露。
6. 认识到满足立法和法规标准只是信息安全战略的起点。

2、建立完善的数据安全技术体系并落地

传统方式已经无法适应新时代数据安全的需要，面临安全的新态势、新要求，在继续做好业务安全的基础之上，通过智能化管理平台，在技术层面实现对风险核查（Check）能力、数据梳理（Assort）能力、数据保护（Protect）能力以及数据威胁监控预警（Examine）能力4大核心能力的建设，在业务层面，实现对数据采集、传输、存储、处理、交换、销毁全生命周期的管理。

3、引进下一代技术，实现流程自动化

人工智能和机器学习将是未来数据安全工作的关键，目前，多数大型企业正在寻求使某些法规遵从流程自动化，包括数据定位和提取，自动化是大型企业保持对大量存储在数据中心和云中的结构化和非结构化数据兼容的唯一方式。

对于数据安全能力建设较为薄弱的企业，建议考虑零信任模式作为一种安全策略，有了“零信任”，企业将着眼于数据管理的整个生命周期，并将关注点从数据安全本身扩展到企业整体信息安全框架。

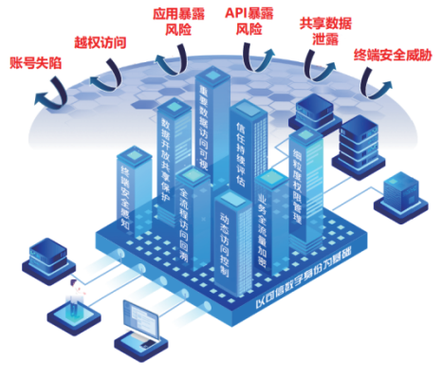


图3 “零信任”模式

灵活的身份安全适配

- 快速引入第三方身份安全设施及能力
- 全面身份认证及多维度身份鉴别

安全的业务访问通道

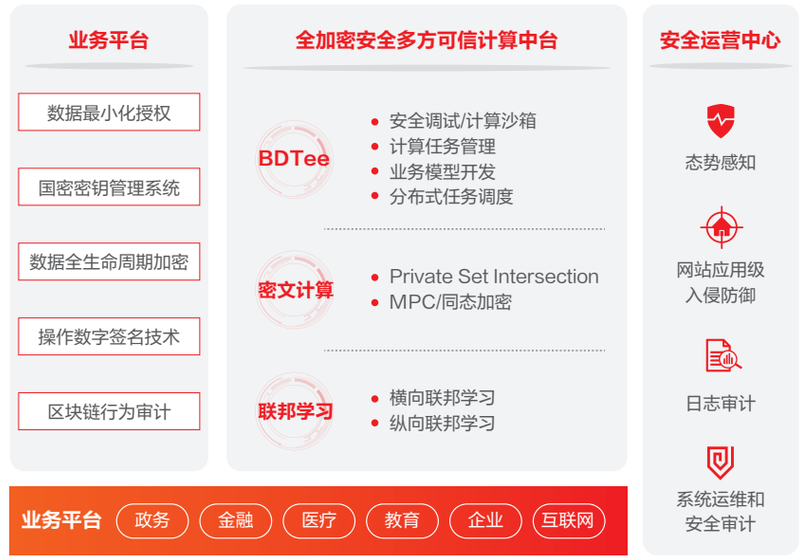
- 细粒度权限管控及访问控制
- 全流量业务加密
- 数据安全能力加持

动态的安全联动响应

- 持续的身份安全评估
- 第三方安全分析、管理平台联动
- 终端环境安全感知及联动

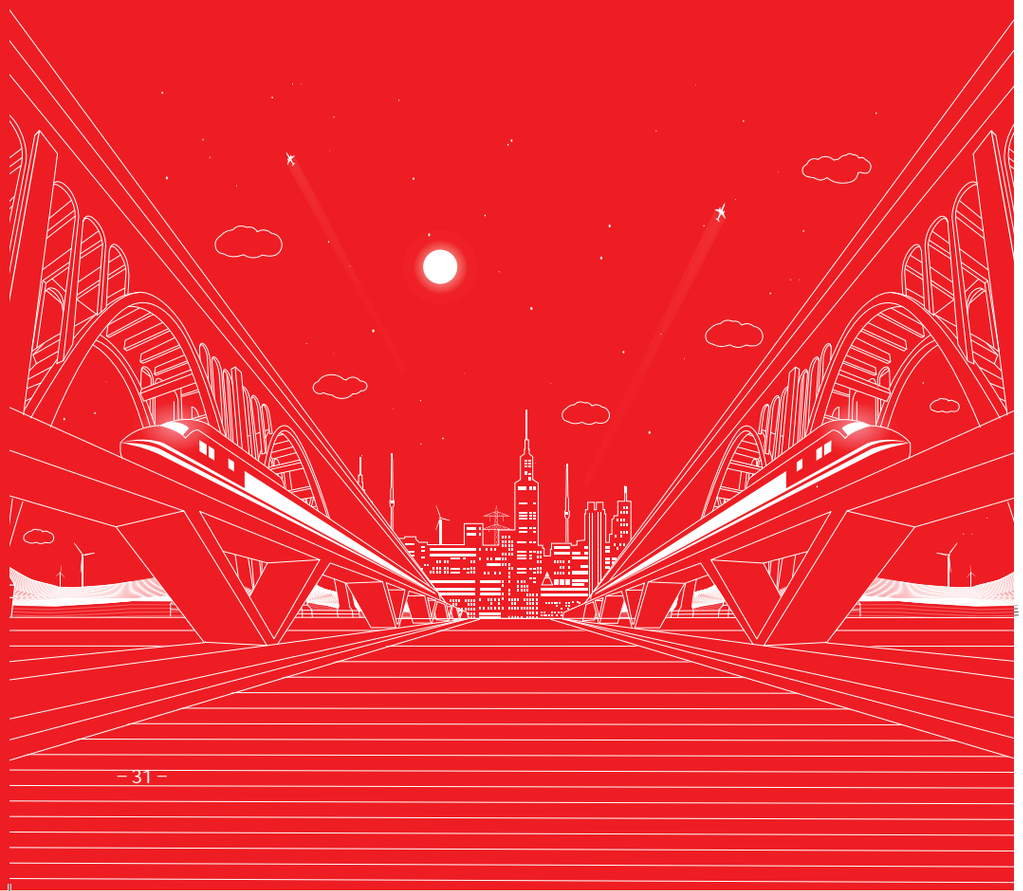
4、政府需落实数据安全保护责任，推动政务数据开放利用

政务数据安全与开发作为数安法的独立章节，要求我国政府在落实数据安全保护责任的同时，推动政务数据开放利用。如何实现数据要素安全、高效的共享开放？个人隐私保护、敏感数据使用、数据确权等难题都成了数据要素市场化的“拦路虎”，我们可以通过引入“数据安全岛”模式，利用安全计算沙箱、安全多方计算、区块链等技术，实现原始数据不出本地，只交换计算结果，做到数据共享的“可用不可见”，解决数据信任和隐私保护、溯源等难题，让流动的数据成为驱动数字经济发展的新动能。



第三篇

《关键信息基础设施安全保护条例》解读



★ ★ ★ ★ ★

导入语

网络安全形势日益严峻，保障关键信息基础设施安全至关重要，这不仅与我国网络安全和国家安全息息相关，也是经济社会稳定发展的基石。2021年7月30日，国务院总理李克强签署国务院令，公布《关键信息基础设施安全保护条例》（以下简称《条例》），自2021年9月1日起施行。《条例》是我国首部专门针对关键信息技术设施安全保护工作的行政法规，《条例》的出台标志着中国网络安全保护进入了新阶段。理解好、落实好、执行好《条例》，对维护国家网络安全、保障关键信息基础设施平稳运行具有重要意义，以下我们对《条例》全文进行了逐条解读。

★ ★ ★ ★ ★

第一章 总则

第一条

为了保障关键信息基础设施安全，维护网络安全，根据《中华人民共和国网络安全法》，制定本条例。

【解读】

对落实《网络安全法》第三章“网络运行安全”中，第二节“关键信息基础设施的运行安全”（第三十一至三十九条）做出的进一步详细规定。

第二条

本条例所称关键信息基础设施（以下称“CII”），是指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域的，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的重要网络设施、信息系统等。

【解读】

用行业分类给出了CII的范围界定，更加详细的关键信息基础设施识别，要依据关键信息基础设施安全主管部门和保护工作部门的识别指南等相关标准规范。

第三条

在国家网信部门统筹协调下，国务院公安部门负责指导监督关键信息基础设施安全保护工作。国务院电信主管部门和其他有关部门依照本条例和有关法律、行政法规的规定，在各自职责范围内负责关键信息基础设施安全保护和监督管理工作。

省级人民政府有关部门依据各自职责对关键信息基础设施实施安全保护和监督管理。

【解读】

与征求意见稿的提法变化较大，给出了中央层面部门的明确分工，明确和强调了网信负责统筹协调，公安负责指导监督，其它部门按各自分管的行业负责保护和监督。省级对应部门履行相应的属地管理责任。

第四条

关键信息基础设施安全保护坚持综合协调、分工负责、依法保护，强化和落实关键信息基础设施运营者（以下简称运营者）主体责任，充分发挥政府及社会各方面的作用，共同保护关键信息基础设施安全。

【解读】

重点强调CII运营者负有主体责任。用了一个章节的篇幅对责任的内容做出了非常具体的表述，具体责任内容参见第12–21条。

第五条

国家对关键信息基础设施实行重点保护，采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治危害关键信息基础设施安全的违法犯罪活动。

任何个人和组织不得实施非法侵入、干扰、破坏关键信息基础设施的活动，不得危害关键信息基础设施安全。

【解读】

与《网络安全法》中的基调一致，强调对CII的重点保护，明确表示对危害CII安全的行为进行严惩。与征求意见稿的提法变化较大。

第六条

运营者依照本条例和有关法律、行政法规的规定以及国家标准的强制性要求，在网络安全等级保护的基础上，采取技术保护措施和其他必要措施，应对网络安全事件，防范网络攻击和违法犯罪活动，保障关键信息基础设施安全稳定运行，维护数据的完整性、保密性和可用性。

【解读】

运营者须确保关基安全稳定运行，CII的防护要在等保的基础之上，采取增强的防护措施，体现CII的重要性。

第七条

对在关键信息基础设施安全保护工作中取得显著成绩或者作出突出贡献的单位和个人，按照国家有关规定给予表彰。

【解读】

鼓励为CII安全保护做出贡献，承诺给予表彰。从鼓励举报违法行为，变为鼓励做出突出贡献。

第二章 关键信息基础设施认定

第八条

本条例第二条涉及的重要行业和领域的主管部门、监督管理部门是负责关键信息基础设施安全保护工作的部门（以下简称保护工作部门）。

【解读】

明确行业主管监管部门是相应重要行业领域的CII保护工作部门，各省级CII的保护工作部门，由各省政府具体明确。

第九条

保护工作部门结合本行业、本领域实际，制定关键信息基础设施认定规则，并报国务院公安部门备案。

制定认定规则应当主要考虑下列因素：

（一）网络设施、信息系统等对于本行业、本领域关键核心业务的重要程度；

（二）网络设施、信息系统等一旦遭到破坏、丧失功能或者数据泄露可能带来的危害程度；

（三）对其他行业和领域的关联性影响。

【解读】

CII的主管和监督部门负责制定CII认定的规则，规则需要上报公安部门备案。认定规则主要考虑的三大因素：“关键核心业务的重要程度”、“遭到破坏后可能带来的危害程度”、“对其他行业和领域的关联性影响”。

第十条

保护工作部门根据认定规则负责组织认定本行业、本领域的关键信息基础设施，及时将认定结果通知运营者，并通报国务院公安部门。

【解读】

保护工作部门负责CII认定，认定后将结果通知运营者，并同步上报公安部门备案。

第十一条

关键信息基础设施发生较大变化，可能影响其认定结果的，运营者应当及时将相关情况报告保护工作部门。保护工作部门自收到报告之日起3个月内完成重新认定，将认定结果通知运营者，并通报国务院公安部门。

【解读】

发生影响认定的较大变化（如新建机房、新建系统等），要上报保护部门，3个月内重新认定并备案。

第三章 运营者责任义务

第十二条

安全保护措施应当与关键信息基础设施同步规划、同步建设、同步使用。

【解读】

CII的防护同样须遵守“三同步”原则。

第十三条

运营者应当建立健全网络安全保护制度和责任制，保障人力、财力、物力投入。运营者的主要负责人对关键信息基础设施安全保护负总责，领导关键信息基础设施安全保护和重大网络安全事件处置工作，组织研究解决重大网络安全问题。

【解读】

明确具体的主体责任，包括：明确责任人为主要负责人（一般理解为单位一把手，除非有明确指定）、保障人，财、物等各方面的投入，领导、决策、事件处置。投入不足有可能构成违反本条例规定的行为。

第十四条

运营者应当设置专门安全管理机构，并对专门安全管理机构负责人和关键岗位人员进行安全背景审查。审查时，公安机关、国家安全机关应当予以协助。

【解读】

继续明确主体责任，包括：设置专门机构、关键人员背景调查（公安机关应予协助）。

第十五条

专门安全管理机构具体负责本单位的关键信息基础设施安全保护工作，履行下列职责：

（一）建立健全网络安全管理、评价考核制度，拟订关键信息基础设施安全保护计划；

（二）组织推动网络安全防护能力建设，开展网络安全监测、检测和风险评估；

（三）按照国家及行业网络安全事件应急预案，制定本单位应急预案，定期开展应急演练，处置网络安全事件；

（四）认定网络安全关键岗位，组织开展网络安全工作考核，提出奖励和惩处建议；

（五）组织网络安全教育、培训；

（六）履行个人信息和数据安全保护责任，建立健全个人信息和数据安全保护制度；

（七）对关键信息基础设施设计、建设、运行、维护等服务实施安全管理；

（八）按照规定报告网络安全事件和重要事项。

【解读】

继续明确主体责任，包括：健全制度、制定计划、定期考核、监测评估、应急预案、应急演练、岗位考核、教育培训、数据防护。其中有些责任也是保卫工作部门的重叠，例如应急演练和应急预案的相关工作，这部分工作需要做好沟通和配合。

第十六条

运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。

【解读】

继续明确主体责任，包括：保障经费、参与决策。

第十七条

运营者应当自行或者委托网络安全服务机构对关键信息基础设施每年至少进行一次网络安全检测和风险评估，对发现的安全问题及时整改，并按照保护工作部门要求报送情况。

【解读】

重复《网络安全法》中的规定，运营者须定期对CII进行风险评估。虽然允许自行评估，但实际执行中最好委托专业安全机构协助完成，在专业性和客观性方面都有保障。

第十八条

关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，运营者应当按照有关规定向保护工作部门、公安机关报告。

发生关键信息基础设施整体中断运行或者主要功能故障、国家基础信息以及其他重要数据泄露、较大规模个人信息泄露、造成较大经济损失、违法信息较大范围传播等特别重大网络安全事件或者发现特别重大网络安全威胁时，保护工作部门应当在收到报告后，及时向国家网信部门、国务院公安部门报告。

【解读】

继续明确运营者主体责任，包括：事件上报、依序上报。

重大事件包括：中断运行、功能故障、数据泄露、经济损失、非法传播、重大威胁。

第十九条

运营者应当优先采购安全可信的网络产品和服务；采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

【解读】

重复《网络安全法》中的规定，明确运营者主体责任，包括：产品采购可信优先、依规进行安全审查。

第二十条

运营者采购网络产品和服务，应当按照国家有关规定与网络产品和服务提供者签订安全保密协议，明确提供者的技术支持和安全保密义务与责任，并对义务与责任履行情况进行监督。

【解读】

重复《网络安全法》中的规定，明确运营者主体责任，包括：签署保密协议，履行保密义务、监督履责情况。

第二十一条

运营者发生合并、分立、解散等情况，应当及时报告保护工作部门，并按照保护工作部门的要求对关键信息基础设施进行处置，确保安全。

【解读】

明确运营者主体责任，包括：机构发生重组时要上报，根据保护工作部门要求处置CII。考虑到深化改革的过程，机构重组的事情会比较常见，本条例给出了遇到类似情况的处置方式。

第四章 保障和促进

第二十二条

保护工作部门应当制定本行业、本领域关键信息基础设施安全规划，明确保护目标、基本要求、工作任务、具体措施。

【解读】

指出了CII保护工作部门履行职责的具体步骤。

明确目标：首先要界定具体的系统，列出清单，明晰底数。

基本要求：明确保护工作的基本要求，把第三章的要求进一步细化。

工作任务：根据要求确定具体任务，可以用具体建设项目的形式明确任务。

具体措施：项目推进的详细举措和实施进度。

第二十三条

国家网信部门统筹协调有关部门建立网络安全信息共享机制，及时汇总、研判、共享、发布网络安全威胁、漏洞、事件等信息，促进有关部门、保护工作部门、运营者以及网络安全服务机构等之间的网络安全信息共享。

【解读】

本条明确了国家网信部门统筹协调CII相关各方，打通网络安全信息共享机制。目前，CII保护工作部门基本已建立各自行业的信息共享平台，通过将情报数据汇总至国家网信部门，由网信部门统筹协调加强各行业之间的工作协同，推进建立安全保障体系，逐步全天候全方位网络安全积极防御态势。

第二十四条

保护工作部门应当建立健全本行业、本领域的关键信息基础设施网络安全监测预警制度，及时掌握本行业、本领域关键信息基础设施运行状况、安全态势，预警通报网络安全威胁和隐患，指导做好安全防范工作。

【解读】

重复《网络安全法》第五章的内容，要求建立健全监测预警机制，及时掌握运行状况和安全态势，落实通报制度。通报工作（业绩排行榜）对网络安全工作具有很明显的督促作用。

第二十五条

保护工作部门应当按照国家网络安全事件应急预案的要求，建立健全本行业、本领域的网络安全事件应急预案，定期组织应急演练；指导运营者做好网络安全事件应对处置，并根据需要组织提供技术支持与协助。

【解读】

重复《网络安全法》的内容，要求制定应急预案，定期应急演练。在实际工作中，应急预案更像应急管理规定，内容普遍不够具体，无法落地。应急演练须用来检验应急预案的完备性。

第二十六条

保护工作部门应当定期组织开展本行业、本领域关键信息基础设施网络安全检查检测，指导监督运营者及时整改安全隐患、完善安全措施。

【解读】

明确保护工作部门负责组织安全检查检测工作，但最好与当地网信和公安部门保持沟通，避免重复检查。

第二十七条

国家网信部门统筹协调国务院公安部门、保护工作部门对关键信息基础设施进行网络安全检查检测，提出改进措施。

有关部门在开展关键信息基础设施网络安全检查时，应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。检查工作不得收取费用，不得要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务。

【解读】

本条进一步明确了相关部门的职责分工和协同增效，明确在实际检查工作开展过程不得收费、指定品牌等动作。

第二十八条

运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作应当予以配合。

【解读】

指出运营者需要配合检查工作的义务，与第13–21条同属运营者义务。

第二十八条

在关键信息基础设施安全保护工作中，国家网信部门和国务院电信主管部门、国务院公安部门等应当根据保护工作部门的需要，及时提供技术支持和协助。

【解读】

国家网信、工信、公安部门需要给CII保护工作部门提供相关技术支持。

第三十条

网信部门、公安机关、保护工作部门等有关部门，网络安全服务机构及其工作人员对于在关键信息基础设施安全保护工作中获取的信息，只能用于维护网络安全，并严格按照有关法律、行政法规的要求确保信息安全，不得泄露、出售或者非法向他人提供。

【解读】

任何部门和服务机构的人员，在履行工作职责过程中所获悉的CII信息（网络拓扑、系统架构、个人数据等等），不得泄露（被动行为）、出售、非法提供（主动行为）。未来网信部门会专门针对类似场景（委托专业安全服务机构提供安全运维服务等），要对工作流程和技术平台等进行风险评估和监督检查。

第三十一条

未经国家网信部门、国务院公安部门批准或者保护工作部门、运营者授权，任何个人和组织不得对关键信息基础设施实施漏洞探测、渗透性测试等可能影响或者危害关键信息基础设施安全的活动。对基础电信网络实施漏洞探测、渗透性测试等活动，应当事先向国务院电信主管部门报告。

【解读】

与《网络安全法》第26条的规定类似，针对CII同样适用。严禁非授权的擅自对CII实施漏洞探测、渗透性测试等活动。授权与审批须同时获得才可以对CII进行相关的探测、渗透。

第三十二条

国家采取措施，优先保障能源、电信等关键信息基础设施安全运行。

能源、电信行业应当采取措施，为其他行业和领域的关键信息基础设施安全运行提供重点保障。

【解读】

能源和电信是更加底层的CII，有义务优先保障其它行业的CII的需求。

第三十三条

公安机关、国家安全机关依据各自职责依法加强关键信息基础设施安全保卫，防范打击针对和利用关键信息基础设施实施的违法犯罪活动。

【解读】

CII中有些属于涉密网络（如国防军工行业的网络），涉密网络的安全保卫，涉及间谍破坏、国家网络战等由国家安全部门负责，非涉密网络由公安部门负责。

第三十四条

国家制定和完善关键信息基础设施安全标准，指导、规范关键信息基础设施安全保护工作。

【解读】

国家层面会制定一系列CII安全的标准，指导CII的安全保护工作。目前，在公安部指导下，在全国信息安全标准化技术委员会的组织下，这个标准体系正在抓紧建立。就安全保护的责任义务而言，其中最基础的两个标准是《关键信息基础设施安全保护要求》和《关键信息基础设施安全控制措施》。

已立项的主要安全标准包括：

关键信息基础设施安全保障指标体系（报批稿）

关键信息基础设施安全检查评估指南（报批稿）

关键信息基础设施安全保护要求（送审稿）

关键信息基础设施安全控制措施（送审稿）

关键信息基础设施要素识别方法（征求意见稿）

关键信息基础设施安全防护能力评价方法（征求意见稿）

关键信息基础设施网络安全应急体系框架（草案）

关键信息基础设施安全测评要求（申报立项）

关键信息基础设施安全监测预警（申报研究）等。

第三十五条

国家采取措施，鼓励网络安全专门人才从事关键信息基础设施安全保护工作；将运营者安全管理人员、安全技术人员培训纳入国家继续教育体系。

【解读】

和第十六条“运营者应当保障专门安全管理机构的运行经费、配备相应的人员，开展与网络安全和信息化有关的决策应当有专门安全管理机构人员参与。”相呼应。CII安全保护工作归根到底还是要靠人才实力，目前我国网络安全人才供不应求，国家层面将推动继续教育体系加大对安全管理人才、安全技术人才的培养力度。

第三十六条

国家支持关键信息基础设施安全防护技术创新和产业发展，组织力量实施关键信息基础设施安全技术攻关。

【解读】

科学技术是第一生产力，CII安全防护工作离不开技术的创新和产业的支持保障，国家层面会通过创新课题、重大项目等形式组织产业和学术力量实施CII安全技术攻关。

第三十七条

国家加强网络安全服务机构建设和管理，制定管理要求并加强监督指导，不断提升服务机构能力水平，充分发挥其在关键信息基础设施安全保护中的作用。

【解读】

CII安全防护必须依赖专业安全服务机构的支撑，国家鼓励网络安全服务机构参与到CII的安全保护工作中，参与对CII的网络安全检测和风险评估等工作。同时，针对网络安全服务机构，国家有关部门会制定管理要求，加强监督指导，提升网络安全服务机构的技术和服务能力。

第三十八条

国家加强网络安全军民融合，军地协同保护关键信息基础设施安全。

【解读】

国家鼓励在CII的安全保护领域开展军民融合、军地协同的合作。既是主观要求（军地双方在人才、资源等很多方面优势互补），也是客观需要（单靠任何一方都无法做好相关工作）。

第五章 法律责任

第三十九条

运营者有下列情形之一的，由有关主管部门依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款：

（一）在关键信息基础设施发生较大变化，可能影响其认定结果时未及时将相关情况报告保护工作部门的；

（二）安全保护措施未与关键信息基础设施同步规划、同步建设、同步使用的；

（三）未建立健全网络安全保护制度和责任制的；

（四）未设置专门安全管理机构的；

（五）未对专门安全管理机构负责人和关键岗位人员进行安全背景审查的；

（六）开展与网络安全和信息化有关的决策没有专门安全管理机构人员参与的；

（七）专门安全管理机构未履行本条例第十五条规定的职责的；

（八）未对关键信息基础设施每年至少进行一次网络安全检测和风险评估，未对发现的安全问题及时整改，或者未按照保护工作部门要求报送情况的；

（九）采购网络产品和服务，未按照国家有关规定与网络产品和服务提供者签订安全保密协议的；

（十）发生合并、分立、解散等情况，未及时报告保护工作部门，或者未按照保护工作部门的要求对关键信息基础设施进行处置的。

【解读】

列出十条红线，这十项要求在前面的条款中都有过明确要求，只要依规办事，一般不会触碰红线。

第四十条

运营者在关键信息基础设施发生重大网络安全事件或者发现重大网络安全威胁时，未按照有关规定向保护工作部门、公安机关报告的，由保护工作部门、公安机关依据职责责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处10万元以上100万元以下罚款，对直接负责的主管人员处1万元以上10万元以下罚款。

【解读】

重大事件上报应该成为一种习惯，一种自觉行为。如果违反，首先收到警告和整改通知，拒不改正才会受到行政处罚。整体基调与《网络安全法》保持一致，还是坚决不要违规。

第四十一条

运营者采购可能影响国家安全的网络产品和服务，未按照国家网络安全规定进行安全审查的，由国家网信部门等有关主管部门依据职责责令改正，处采购金额1倍以上10倍以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款。

【解读】

在产品和服务方面，运营者采购网络产品和服务可能影响国家安全的，应当按照国家网络安全规定通过安全审查。

第四十二条

运营者对保护工作部门开展的关键信息基础设施网络安全检查检测工作，以及公安、国家安全、保密行政管理、密码管理等有关部门依法开展的关键信息基础设施网络安全检查工作不予配合的，由有关主管部门责令改正；拒不改正的，处5万元以上50万元以下罚款，对直接负责的主管人员和其他直接责任人员处1万元以上10万元以下罚款；情节严重的，依法追究相应法律责任。

【解读】

配合相关部门的安全检查工作是运营者必须履行的法律义务，在实际工作中，很少有直接拒绝配合的情况，要注意避免阳奉阴违，暗中设置障碍的做法。否则会受到行政处罚。如果情节严重，受到刑事处罚也是有可能的。

第四十三条

实施非法侵入、干扰、破坏关键信息基础设施，危害其安全的活动尚不构成犯罪的，依照《中华人民共和国网络安全法》有关规定，由公安机关没收违法所得，处5日以下拘留，可以并处5万元以上50万元以下罚款；情节较重的，处5日以上15日以下拘留，可以并处10万元以上100万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处10万元以上100万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本条例第五条第二款和第三十一条规定，受到治安管理处罚的人员，5年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

【解读】

针对CII实施了侵入、干扰、破坏的行为，一般很难不构成犯罪。因此无论是单位还是个人，一定不要心存侥幸，利令智昏。2019年11月1日发布的《最高人民法院最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》与网安法的基调有所不同，相关规定实际上降低了入刑的门槛。

第四十四条

网信部门、公安机关、保护工作部门和其他有关部门及其工作人员未履行关键信息基础设施安全保护和监督管理职责或者玩忽职守、滥用职权、徇私舞弊的，依法对直接负责的主管人员和其他直接责任人员给予处分。

【解读】

督促单位主要负责人重视网络安全工作，加强在网络安全方面的投入。避免因为出现安全事故，承担责任。并非所有事故都需要承担责任，一些零日漏洞的确无法有效防护，但是规定动作都要完成才有机会免责。

第四十五条

公安机关、保护工作部门和其他有关部门在开展关键信息基础设施网络安全检查工作中收取费用，或者要求被检查单位购买指定品牌或者指定生产、销售单位的产品和服务的，由其上级机关责令改正，退还收取的费用；情节严重的，依法对直接负责的主管人员和其他直接责任人员给予处分。

【解读】

第27条中明令禁止乱收费和乱指定的行为，如果出现类似情况则按本条规定进行处理。

第四十六条

网信部门、公安机关、保护工作部门等有关部门、网络安全服务机构及其工作人员将在关键信息基础设施安全保护工作中获取的信息用于其他用途，或者泄露、出售、非法向他人提供的，依法对直接负责的主管人员和其他直接责任人员给予处分。

【解读】

针对违法本条例第30条规定的行为，给出了处罚的方式。这里只涉及行政处罚，通常这类行为还会触犯法律，很大概率会构成犯罪。

第四十七条

关键信息基础设施发生重大和特别重大网络安全事件，经调查确定为责任事故的，除应当查明运营者责任并依法予以追究外，还应查明相关网络安全服务机构及有关部门的责任，对有失职、渎职及其他违法行为的，依法追究责任。

【解读】

只要切实履行相关职责，即使CII出现重大事故，一般也不会认定为责任事故，关键还是切实履行职责，认真落实法律法规的要求。

第四十八条

电子政务关键信息基础设施的运营者不履行本条例规定的网络安全保护义务的，依照《中华人民共和国网络安全法》有关规定予以处理。

【解读】

对于电子政务类CII的运营者的处罚，参照《网络安全法》第72条的规定进行。即先由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分（行政和党纪处理先行）。

第四十九条

违反本条例规定，给他人造成损害的，依法承担民事责任。

违反本条例规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

【解读】

对于违反本条例的行为，如果造成对个人的伤害，需要承担民事责任的，一般为经济赔偿。构成犯罪的会依据刑法中相关规定处罚。

第六章 附则

第五十条

存储、处理涉及国家秘密信息的关键信息基础设施的安全保护，还应当遵守保密法律、行政法规的规定。

关键信息基础设施中的密码使用和管理，还应当遵守相关法律、行政法规的规定。

【解读】

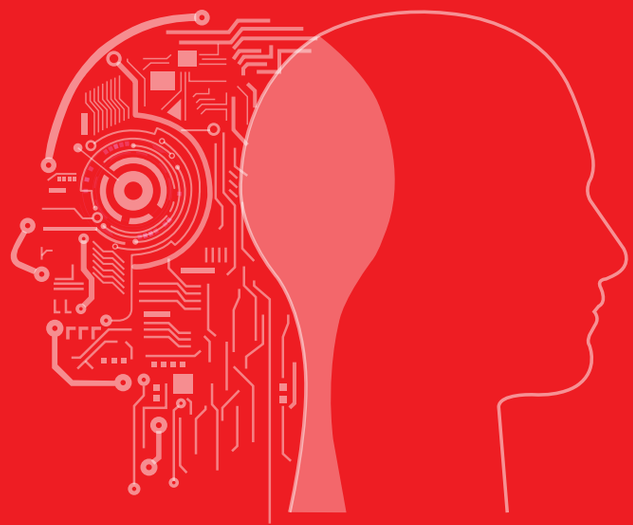
对涉密的CII，还要遵守保密相关法律和法规的要求。

第五十一条

本条例自2021年9月1日起施行。

第四篇

《中华人民共和国个人信息保护法》解读



★ ★ ★ ★ ★

导入语

随着信息化与经济社会持续深度融合，网络已成为生产生活的新空间、经济发展的新引擎、交流合作的新纽带。截至2020年12月，我国互联网用户已达9.89亿，互联网网站超过443万个，应用程序数量超过345万个，个人信息的收集、使用更为广泛。虽然近年来我国个人信息保护力度不断加大，但在现实生活中，一些企业、机构甚至个人，从商业利益等出发，随意收集、违法获取、过度使用、非法买卖个人信息，利用个人信息侵扰人民群众生活安宁、危害人民群众生命健康和财产安全等问题仍十分突出。经营者在数字技术上应用的更加专业、纯熟，消费者就越发的处于弱势地位，个人隐私已成为经营者手中用于交换利益的廉价或免费的筹码。为进一步加强个人信息保护法制保障、维护网络空间良好生态、促进数字经济健康发展，中华人民共和国第十三届全国人民代表大会常务委员会第三十次会议于2021年8月20日通过《中华人民共和国个人信息保护法》（下简称《个人信息保护法》），自2021年11月1日起施行。

作为我国第一部个人信息保护相关的法律，《个人信息保护法》的出台填补了相关空白，规范了社会各行业个人信息的使用途径，做到把个人信息使用权关进法律的笼子里 。《个人信息保护法》对个人信息滥用等社会热点问题有何明确规定？违反《个人信息保护法》有哪些后果？会如何影响我们的工作生活？让我们一起解读该法，用好“个人信息保护”的准绳。

★ ★ ★ ★ ★

★ 立法过程 ★

2019年3月5日

第十三届全国人大常委会第二次会议，将制定《中华人民共和国个人信息保护法》列入本届立法规划。

2020年10月13日

第十三届全国人大常委会第二十二次会议对《中华人民共和国个人信息保护法（草案）》进行了初次审议。

2021年4月26日

第十三届全国人大常委会第二十八次会议对《中华人民共和国个人信息保护法（草案二审稿）》进行了审议，在一审稿的基础上主要修订增加内容如下：

进一步完善明确个人信息处理应遵循的原则；

参照民法典中的规定，增加了对死者的个人信息保护条款；

增加了超大互联网平台特定的个人信息保护义务的要求；

明确了由国家网信部门统筹推进个人信息保护有关工作；

明确了个人信息侵权行为的归责原则为过错推定。

2021年8月20日

第十三届全国人大常委会第三十次会议表决通过《中华人民共和国个人信息保护法》，自2021年11月1日起施行。在二审稿的基础上主要修订增加内容如下：

在第一条中增加规定“根据宪法”制定本法；

进一步完善个人信息处理规则，特别是对应用程序（APP）过度收集个人信息、大数据杀熟以及非法买卖、泄露个人信息等作出针对性规范；

将未成年人的个人信息作为敏感个人信息，并制定专门的处理规则；

完善个人信息跨境提供的规则；

增加个人信息可携带权的规定，完善死者个人信息保护的规定；

完善个人信息保护投诉、举报工作机制及对违法处理个人信息涉嫌犯罪案件的移送提出明确要求。

★ 本法结构 ★

《个人信息保护法》全文涵盖了八章，七十四条内容。分别为总则、个人信息处理规则、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人信息处理者的义务、履行个人信息保护职责的部门、法律责任和附则。

中华人民共和国个人信息保护法

（2021年8月20日第十三届全国人民代表大会常务委员会第三十次会议通过）

第一章 总则（12条）

第二章 个人信息处理规则（25条）

第三章 个人信息跨境提供的规则（6条）

第四章 个人在个人信息处理活动中的权利（7条）

第五章 个人信息处理者的义务（9条）

第六章 履行个人信息保护职责的部门（6条）

第七章 法律责任（6条）

第八章 附则（3条）

★ 要点解读 ★

一、术语界定

- **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。

- **个人信息的处理**

  包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

- **敏感个人信息**

  一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

二、范围界定

- **境内**

  组织、个人在中华人民共和国境内处理自然人个人信息的活动，适用本法。

- **境外**

  在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法：
  以向境内自然人提供产品或者服务为目的；
  分析、评估境内自然人的行为；
  法律、行政法规规定的其他情形。

  * 另：境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

三、个人信息处理规则

- 确立个人信息处理应遵循的原则，强调处理个人信息应当遵循合法、正当、必要和诚信原则，具有明确、合理的目的，限于实现处理目的的最小范围，公开处理规则，保证信息准确，采取安全保护措施等，并将上述原则贯穿于个人信息处理的全过程、各环节。（第五条至第九条）

- 确立以“告知–同意”为核心的个人信息处理一系列规则，要求处理个人信息应当在事先充分告知的前提下取得个人同意，并且个人有权撤回同意；重要事项发生变更的应当重新取得个人同意；不得以个人不同意为由拒绝提供产品或者服务。考虑到经济社会生活的复杂性和个人信息处理的不同情况，本法还对基于个人同意以外合法处理个人信息的情形作了规定。（第十三条至第十九条）

- 根据个人信息处理的不同环节、不同个人信息种类，对个人信息的共同处理、委托处理、向第三方提供、公开、用于自动化决策、处理已公开的个人信息等提出有针对性的要求。（第二十一条至第二十七条）

- 设专节对处理敏感个人信息作出更严格的限制，只有在具有特定的目的和充分的必要性的情形下，方可处理敏感个人信息，并且应当取得个人的单独同意或者书面同意。（第二十八条至第三十二条）

- 设专节规定国家机关处理个人信息的规则，在保障国家机关依法履行职责的同时，要求国家机关处理个人信息应当依照法律、行政法规规定的权限和程序进行。（第三十三条至第三十七条）

四、个人信息跨境提供规则

- 明确关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的处理者，确需向境外提供个人信息的，应当通过国家网信部门组织的安全评估；对于其他需要跨境提供个人信息的，规定了经专业机构认证等途径。（第三十八条、第四十条）

- 对跨境提供个人信息的“告知-同意”作出更严格的要求。（第三十九条，应告知接收方详细信息，并取得单独同意）

- 未经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。（第四十一条）

- 对从事损害我国公民个人信息权益等活动的境外组织、个人，以及在个人信息保护方面对我国采取不合理措施的国家和地区，规定了可以采取的相应措施。（第四十二条、第四十三条，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。）

五、个人信息跨境提供规则

- 与民法典的有关规定相衔接，明确在个人信息处理活动中个人的各项权利，包括知情权、决定权、查询权、更正权、删除权等，并要求个人信息处理者建立个人行使权利的申请受理和处理机制。（第四十四条至第五十条）

- 明确个人信息处理者的合规管理和保障个人信息安全等义务（第五十一条至第五十六条）
  按照规定制定内部管理制度和操作规程，采取相应的安全技术措施，并指定负责人对其个人信息处理活动进行监督；
  定期对其个人信息活动进行合规审计；
  对处理敏感个人信息、向境外提供个人信息等高风险处理活动，事前进行风险评估；
  履行个人信息泄露通知和补救义务等。

- 明确提供基础性互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者的义务（第五十七条）
  建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构，对个人信息处理活动进行监督；
  遵循公开、公平、公正的原则，明确处理个人信息的规范和保护个人信息的义务；
  对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务；
  定期发布个人信息保护社会责任报告，接受社会监督。

六、履行个人信息保护职责的部门

- 个人信息保护职责部门的定义。（第六十条）
  国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。
  国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。
  县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

- 明确个人信息保护部门的职责。(第六十一条)
  开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；
  接受、处理与个人信息保护有关的投诉、举报；
  组织对应用程序等个人信息保护情况进行测评，并公布测评结果；
  调查、处理违法个人信息处理活动；
  法律、行政法规规定的其他职责。

- 个人信息保护部门可以采用的措施，包括询问、查阅、复制资料、现场检查、检查设备及物品、查封或者扣押、约谈主要负责人、进行合规审计等。(第六十三条、第六十四条)

- 对个人信息违法活动的投诉、举报及处置进行规定。(第六十五条)

七、法律责任

- 违反规定。（第六十六条）
  责令改正，给予警告，没收违法所得；
  拒不改正的，并处一百万元以下罚款；
  相关责任人：一万元以上十万元以下罚款；

- 情节严重。（第六十六条）
  责令改正，没收违法所得；
  五千万元以下或者上一年度营业额百分之五以下罚款；
  责令暂停相关业务、停业整顿、吊销相关业务许可或者吊销营业执照；
  相关责任人：十万元以上一百万元以下罚款；

- 存在违法行为的依照有关规定记入信用档案，并予以公示。（第六十七条）

- 国家机关不履行保护义务的处罚进行规定。（第六十八条）

- 个人信息侵权行为的归责原则为过错推定。（第六十九条）

- 个人信息主体可以对侵权行为发起集体诉讼。（第七十条）

- 与治安管理、刑法相衔接。（第七十一条）

★ 热点聚焦 ★

因为涉及面广、影响范围大、发生频率高，广大人民群众苦“个人信息滥用”久矣，因此本法第二十四、第二十六条专门针对个人信息的滥用这一社会热点问题进行了明确规定。

一、针对新技术新引用进行了高度关注

第二十四条

个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。通过自动化决策方式作出对个人权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

针对当前社会各方面对于用户画像、算法推荐等新技术新应用高度关注，对相关产品和服务中存在的信息骚扰、“大数据杀熟”等问题强烈反应。《个人信息保护法》立足于维护广大人民群众的网络空间合法权益，对利用个人信息进行自动化决策作出有针对性规范，明确要求提供个人拒绝的选项。

二、针对公共场所安装摄像头有了明确规定

第二十六条

在公共场所安装图像采集、个人身份识别设备，应当为维护公共安全所必需，遵守国家有关规定，并设置显著的提示标识。所收集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的；取得个人单独同意的除外。

人脸识别是人工智能技术的重要应用，在为社会生活带来便利的同时，其所带来的个人信息保护问题也日益凸显。人脸识别技术滥用乱象频繁曝光、“我国人脸识别第一案”中强制顾客激活人脸识别系统等，体现出人脸识别技术广泛应用与个人信息保护的矛盾日益尖锐。个人信息保护法做了明文规定，只能用于公共安全。

结语

我国“十四五”规划、“新基建”等政策将持续深入推进数据要素安全管控和市场化，提升社会数据资源价值。信息化时代，个人信息保护已成为广大人民群众最关心最直接最现实的利益问题之一。未来，数据安全及个人信息保护能力将成为政企数字化转型成果的“试金石”。随着《数据安全法》、《个人信息保护法》等法律实施，表明我国数据安全保护已进入法制化时代，更是国家安全战略的核心部分。