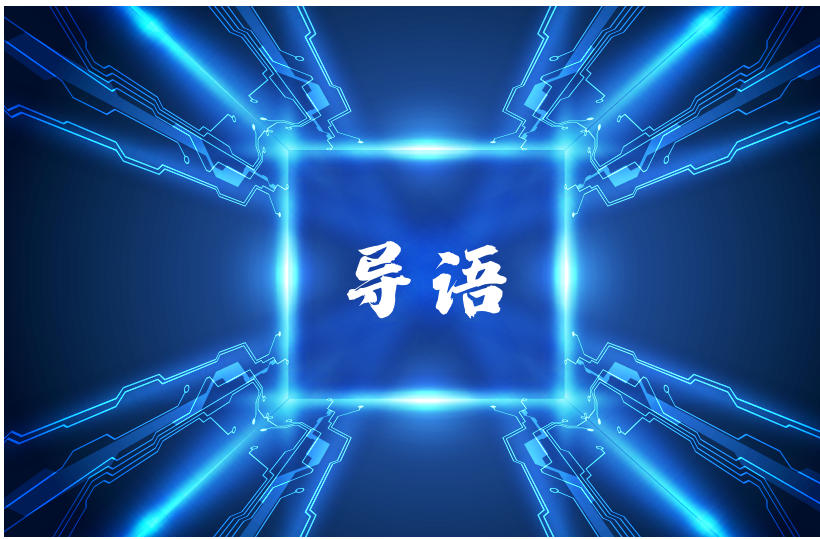
云鑫众
YUN XIN ZHONG

口袋秘籍

网络安全政策法律解读

网络安全，
人人有责。
提高网络安全意识，
拒绝做网络世界的『透明人』！

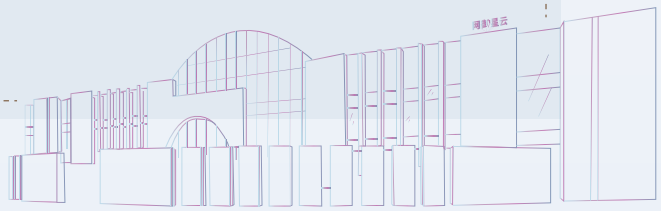

导语

互联网时代下，信息技术已经成为经济社会发展的重要推动力之一，但随之而来的野蛮生长问题不容忽视。近年来，在国家总体安全观的指引下，我国国家安全法律体系不断完善，陆续推出了《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等一系列基础性法律，构筑起我国互联网时代下信息保护的法律屏障。

其中，《中华人民共和国数据安全法》强调数据安全的保护，进一步明确了数据安全相关者的保护义务与职责；《中华人民共和国个人信息保护法》则集中于个人信息的保护，对个人信息保护的全生命周期作出了全面规定。

“十四五”时期，“加快数字化发展，建设数字中国”成为了战略发展目标，在国家战略和政策法规的双轮驱动下，网御星云结合网络安全全领域场景化实践经验，针对《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》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等做出专业解读，为数字时代下政企如何践行法律法规提供借鉴思路，推进数字经济与安全共生创新。

目录



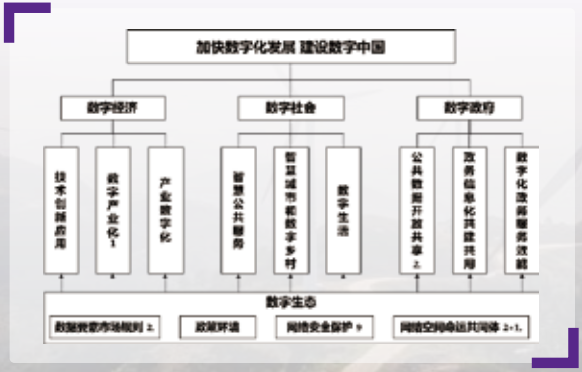
“十四五”规划中的网络安全

2021年3月13日，《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》（以下简称《规划纲要》）正式公布。《规划纲要》明确了发展目标、量化指标和工程任务，具化描摹了未来我国发展的蓝图路线。

《规划纲要》网络安全要点解读

从《规划纲要》全文出现的14次“网络安全”和5次“数据安全”主题词分布看，多达12次的“网络安全”和5次的“数据安全”，都出现在第五篇“加快数字化发展 建设数字中国”内容中。

第五篇的主要内容逻辑梳理，以及主题词出现的位置如下图所示。（“网络安全”主题词用数字表示，“数据安全”主题词用数字加点表示）



网络安全已融入数字化发展的方方面面

由上图可见，数字化发展和数字中国的建设，重点集中在数字经济、数字社会和数字政府三个领域，并且受到数字生态的规范化管理约束。网络安全与数据安全，已经不再是传统的外围加固、松散整合模式，而是深深融入到数字化发展的方方面面。

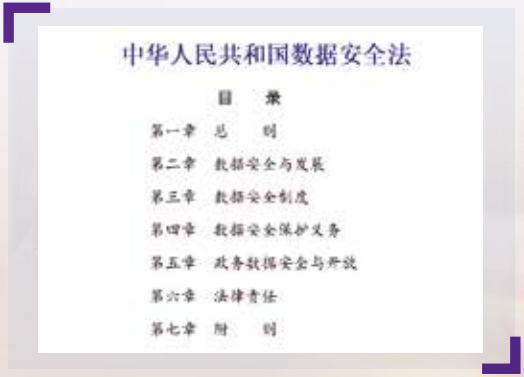
除了对数字化发展进行安全赋能保障外，在网络安全保护章节中，还提出了要提升“网络安全威胁发现、监测预警、应急指挥、攻击溯源能力”，构成了网络安全发现、预警、指挥、行动、溯源的多环节动态闭环管理，为网络安全统筹管理能力建设指明了方向。

明确数字经济的重点发力领域

另外，《规划纲要》还明确了7个数字经济重点领域，包括：云计算、大数据、物联网、工业互联网、区块链、人工智能、虚拟现实和增强现实；以及10个数字化应用场景，包括：智能交通、智慧能源、智能制造、智慧农业及水利、智慧教育、智慧医疗、智慧文旅、智慧社区、智慧家居、智慧政务。这7个领域和10个场景中的网络安全和数据安全，必将成为未来安全产业发展的重中之重。

《中华人民共和国数据安全法》解读

2021年6月10日，十三届全国人大常委会第二十九次会议通过了《中华人民共和国数据安全法》（以下简称：数据安全法），自2021年9月1日起施行。《数据安全法》的出台，把数据安全上升到了国家安全层面，基于总体国家安全观，将数据要素的发展与安全统筹起来，为我国的数字化转型，构建数字经济、数字政府、数字社会提供法治保障。


中华人民共和国数据安全法

目　录

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

《数据安全法》出台历程

- 2018年10月，全国人大开始组建专班针对《数据安全法》进行研讨，2020年7月，《中华人民共和国数据安全法（草案）》向公众公开征求意见。
- 2021年4月，第十三届全国人大常委会第二十八次会议对《中华人民共和国数据安全法（草案二次审议稿）》进行了审议，并公开向社会征求意见。
- 2021年6月，第十三届全国人大常委会第二十九次会议对草案三次审议稿进行了审议并通过。

《数据安全法》三次修订要点变化

《中华人民共和国数据安全法（草案）》提出了支持促进以数据为关键要素的数字经济发展，确立了决策统筹机制、安全责任主体、协调监管部门、数据安全保护义务、数据安全制度机制、政务数据安全与开放等方面内容。

草案二次审议稿重点对数据安全用语的含义予以完善、完善了数据分级分类和重要数据保护制度、充实数据出境安全管理规定等。

草案三次审议稿主要是加强对数据安全工作统筹；明确对关系国家安全、国民经济命脉、重要民生、重大公共利益等数据实行更严格的管理制度；提出解决老年人、残疾人、儿童等信息弱势群体的“数字鸿沟”问题；完善保障政务数据安全方面的规定；加大对违法行为的处罚力度。

从三次修订过程可以看出，《数据安全法》的内涵和深度在不断完善和发展：

1.相关法律概念范畴逐步精确，首次明确了数据、数据处理和数据安全等法律概念。

2.进一步明确和加强了数据安全统筹工作。

3.提出针对“数字鸿沟”的法律条款，回应了数据安全在社会伦理方面的关切。

4.增加对主管机构法律约束彰显公平。

《数据安全法》要点解读

依据《数据安全法》相关要求，数据相关方在今后的数据安全运营中应重点关注以下方面：

数据分类分级

数据安全首要工作是建立数据分类分级机制，除国家秘密之外，各行业应在本法的规制下，分析本行业业务数据特征，制定数据分类分级标准，解决数据安全保护工作中带来的不均衡性、不适用性难题。

重要数据保护

根据数据重要性程度建立数据资产清单，为针对重要数据实施重点保护工作奠定基础。通过数据分类分级划分为核心数据、重要数据等级别，采取等级化保护，此举和国家网络安全等级保护、国家关键信息基础设施保护相辅相成。

数据开发利用安全

随着数据开发利用的扩展，数据安全也要同步进行发展。数据安全和数据开发利用是一体两翼，数据开发利用产生的隐私保护及更广义的业务安全问题，迫使我们必须重视数据在开发利用过程中的数据安全问题。

数据交易安全

数据交易活动管理成为数据安全工作的焦点问题，数据的来源、交付、使用、传递等环节的合法性问题必须形成有效安全监管手段，培育一个良性数据要素市场。

政务数据安全开放

规定国家机关应建立保障政务数据安全和推动政务数据开放的制度措施，大力推进政务数据资源开放和开发利用。

除此之外，还需进一步完善数据安全管理制度，加强数据安全风险评估、数据安全应急处置、数据安全创新研究等工作，强化数据安全运营能力。

《中华人民共和国个人信息保护法》解读

2021年8月20日，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》（以下简称：个人信息保护法），自2021年11月1日起施行。这表明我国个人信息保护工作已经纳入法制化轨道。

中华人民共和国个人信息保护法

目　录

第一章　总　则
第二章　个人信息处理规则
　第一节　一般规定
　第二节　敏感个人信息的处理规则
　第三节　国家机关处理个人信息的特别规定
第三章　个人信息跨境提供的规则
第四章　个人在个人信息处理活动中的权利
第五章　个人信息处理者的义务
第六章　履行个人信息保护职责的部门
第七章　法律责任
第八章　附　则

《个人信息保护法》出台历程

2020年5月，十三届全国人大常委会第三次会议表决通过了《中华人民共和国民法典》。

意义

首次规定了隐私权和个人信息保护原则，界定了个人信息的概念，规范了个人信息处理者的义务、自然人对其个人信息的权利以及行政机关的职责等，为该领域的未来立法奠定了基础。

2020年10月，《中华人民共和国个人信息保护法（草案）》向公众公开征求意见，2021年4月，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（草案二次审议稿）》进行了审议，并公开向社会征求意见。

意义

体现了个人信息保护立法工作的逐步细化充实。

2021年8月，十三届全国人大常委会第三十次会议上，对个人信息保护法草案三审稿进行了分组审议。

意义

草案三审稿充分吸纳了各方意见建议，在完善个人信息处理规则、加强未成年人个人信息保护等方面作出调整完善，增强了系统性、针对性和可操作性，总体已经比较成熟。

《个人信息保护法》要点解读

《个人信息保护法》是一部保护个人信息的法律条款，对个人信息保护什么、怎么保护、谁来保护等问题进行了全面回应，明确了个人信息保护的适用范围、健全了个人信息的处理规则、完善了个人信息跨境提供的规则、确定了个人信息处理活动中个人的权利和处理者义务、框定了履行个人信息保护职责的部门以及法律责任，为破解个人信息保护中的热点难点问题提供了强有力的法律保障。

探索个人信息保护与数字经济发展的平衡点

我国在数字经济领域走在世界前列，同样也面临一些新情况、新问题，正视个人信息保护的多元化诉求，探索一条与数字时代相适应的数据隐私保护路径，关键在于以保护个人权益和促进信息合理流通为准绳，找到信息利用和安全的平衡点。

收集个人信息，限于实现处理目的的最小范围

《个人信息保护法》明确，处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围。

事前进行个人信息保护影响评估

在个人信息处理行为日益复杂化、泛在化、链条化的今天，个人信息处理者应当具备一个完整的风险评估流程，通过风险评估的结果得出合适恰当的处理动作，针对性地提出安全保护措施，最终达到动态优化式的个人权益保护效果。

采取措施有效避免个人信息泄露、篡改、丢失

个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，对个人信息分类管理，采取加密、去标识化等安全技术措施，确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失。

健全个人信息保护合规制度体系

处理个人信息达到国家网信部门规定数量的个人信息处理者，应当指定个人信息保护负责人，成立主要由外部成员组成的独立机构，负责对个人信息处理活动以及采取的保护措施等进行全流程安全监督。

《个人信息保护法》下的网络安全能力思考

安全方案场景化

个人信息保护面临的新型挑战十分复杂，新形势下需要贯彻“场景化”安全思维，针对一个个的具体安全问题，转换原有以合规为目的的设备堆砌方法，提出场景化的个人信息保护安全解决方案。

安全能力体系化

个人信息保护体系构建是一个复杂系统工程，在设计实现个人信息保护安全能力时，不能再像传统网络安全那样事后介入、外围加固，而是应事前统筹规划，采用体系结构方法，科学合理设计各类安全能力组件，通过能力抽象、标准接口和业务编排等，使单点的功能连接起来，形成协同联动的安全体系，以灵活应对新型安全威胁。

安全交付运营化

个人信息保护安全能力形成不是一次性安全资源投入，而是持续的安全运营。这就要求个人信息处理者面向真实安全需求，建立起完备的技术“一体化”、管理“一条龙”服务型安全运营体系，既解决以人为核心的个人信息窃取与反窃取的对抗，又平衡数字经济发展与个人信息保护之间的矛盾。

网络安全为人民，网络安全靠人民

树立网络安全观，全民共筑安全线