第5章 信息素养

信息素养是指在信息技术领域，通过对信息行业相关知识的了解，内化形成的职业素养和行为自律能力。信息素养是当代社会中个体适应信息时代发展、有效参与社会生活和职业活动所必须具备的重要能力。

5.1 信息素养概述

知识目标：

- 了解信息素养的概念、要素、内涵。

能力目标：

- 培养良好的信息素养，用以解决实际问题。

素养目标：

- 将信息意识、信息知识、信息能力和信息道德内化为自身的行为习惯和思维方式。

本节内容思维导图如图 5.1 所示。

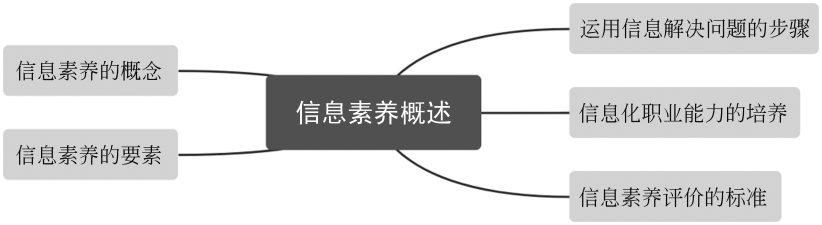

图 5.1 信息素养概述思维导图

近 30 年，得益于互联网技术的快速发展和传播环境的日益开放，人类生产的信息量已超过过去 5000 年信息生产的总和，形成了信息爆炸的现象。同时产生的大量的虚假信息、无用信息甚至有害信息充斥网络，个人在接收信息时面临严重“超载”的问题，具备良好地筛选和利用有效信息的能力就至关重要。以此为核心的信息素养是大学生综合职业素养的重要组成部分，亦是其终身学习的核心能力。

【思考】

问题 1：什么是信息素养？

问题 2：结合自己专业，分析在实际工作 9 岗位中有哪些具体事例体现了信息素养？

5.1.1 信息素养的概念

信息素养是一个综合性的概念，它涵盖了个人在信息社会中获取、理解、评估、创造、使用和交流信息的能力。

信息素养的发展过程是一个不断演进和丰富的过程，它随着信息技术的发展和社会环境的变化而不断变化。

(1) 萌芽阶段(20 世纪 70 年代)，信息素养的概念在这一时期萌芽，主要关注手工检索文献的技能和用户教育。这一时期，信息素养的提出主要是基于图书馆学和情报学的背景，强调如何有效地利用图书馆资源和手工检索工具来获取信息。

(2) 发展阶段(20 世纪 70 年代至 80 年代末)，信息素养中开始融入计算机素养的元素，关注如何利用计算机进行信息检索与评价。这一阶段，信息素养的内涵逐渐扩大，开始重视信息意识的重要性。

(3) 成型阶段(20 世纪 90 年代至 21 世纪初)，信息素养逐渐成为公民的基本素养之一，强调批判和评价信息的能力。这一时期，信息素养的培育开始受到广泛关注，并被纳入教育体系之中。

(4) 新发展阶段(21 世纪 10 年代至今)，信息素养进入了一个全新的发展阶段，强调智能时代的综合素养。随着人工智能、大数据等技术的兴起，信息素养的内涵更加丰富和复杂，除了传统的信息获取、处理和应用能力外，还包括计算思维、信息社会责任等新的元素。强调在新技术环境下的信息获取、理解、评价、交流、使用和创造能力。

5.1.2 信息素养的要素

信息素养的要素是信息素养概念的进一步延伸和细化，主要包括信息意识、信息知识、信息能力和信息道德 4 方面，如图 5.2 所示。

图 5.2 信息素养的要素组成图

1. 信息意识

信息意识是整个信息素养的前提，指人对信息敏锐的感受力、判断力和洞察力，即人的信息敏感程度。信息意识是人们产生信息需求，形成信息动机、信息兴趣，进而自觉寻求信息、利用信息的动力和源泉，是人类所特有的意识。通俗地讲，信息意识就是面对不懂的东西，能积极主动地去寻找答案，并知道到哪里找、如何找才能获得答案的意识。在当下这个“信息爆炸”的时代，具有良好信息意识的人能够以有效的方法和手段对信息去粗取精、去伪存真，自觉地学习、掌握各种现代信息工具，并将其熟练地运用于解决生活、学习和工作中的实际问题，不断提高自己，形成新认知，实现终身学习。

2. 信息知识

信息知识是人们为了获取信息和利用信息而应该掌握的基本知识和技能。这包括了解信息技术的基本概念、原理和发展趋势，掌握信息检索、信息处理和信息传递的基本方法和技巧，以及了解与信息技术相关的法律法规和道德规范等。信息知识是信息素养的基础，它为人们有效地利用信息提供了必要的支持和保障。

(1) 信息理论知识：信息理论包括信息的基本概念，信息系统的结构、工作原理及其原则等。有了对信息本身的认知，就能更好地辨别信息，获取、利用信息。

(2) 信息技术知识：信息技术是指利用计算机、网络等各种硬件设备及软件工具与科学方法，对各种信息进行获取、加工、存储、传输与使用的技术之和。

3. 信息能力

信息能力是指个人利用信息技术解决实际问题的能力。这包括理解信息能力、获取信息能力、处理信息能力、应用信息能力等多方面。

理解信息能力是对信息进行分析、评价和决策的能力，这包括对信息内容和信息来源的分析，鉴别信息质量和评价信息价值，以及决策信息取舍和分析信息成本的能力；获取信息能力就是通过各种途径和方法搜集、查找、提取、记录和存储信息的能力；处理信息能力是指个人对获取的信息进行整理、分析和评价的能力；应用信息能力则是指个人将获取和处理的信息应用于实际问题的解决中的能力。信息能力是信息素养的核心部分，它直接影响个人在信息社会中的生存和发展。

4. 信息道德

信息道德是指在信息领域中用以规范人们相互关系的思想观念与行为准则。它涵盖了信息的采集、加工、存储、传播和利用等各个环节，是这些环节中产生的各种社会关系的道德意识、道德规范和道德行为的总和。具体来说，信息道德通过社会舆论、传统习俗等力量，使人们形成一定的信念、价值观和习惯，从而自觉地规范自己的信息行为。

以上 4 方面相互联系、相互作用，共同构成一个不可分割的统一整体。信息意识是前提，信息知识是基础，信息能力是核心，信息道德是保证。在信息化日益发展的今天，具备良好的信息素养已经成为个人适应信息社会、实现自身发展的重要基础。

5.1.3 运用信息解决问题的步骤

如何用信息技术分析和解决实际问题，是信息素养的核心内涵。运用信息解决问题通常涉及一系列有序的步骤，这些步骤旨在确保问题得以全面、准确和有效地解决。以下是一个典型的流程，分为 6 个关键阶段，如图 5.3 所示。

(1) 明确问题。首先，需要清晰地定义问题的范围、性质和目标。确保对问题的理解是准确且具体的。然后进行需求分析。分析解决问题所需的信息类型和范围，以便后续有针对性地搜集信息。

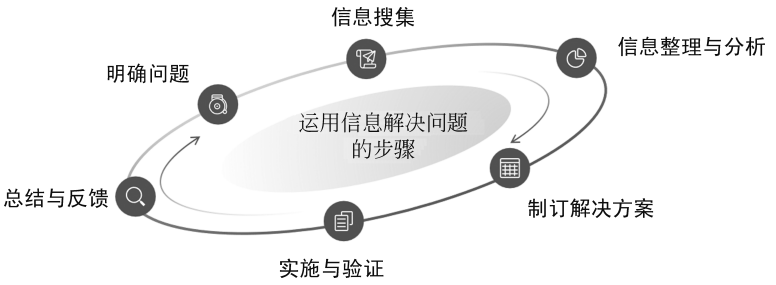

图 5.3　运用信息解决问题的步骤

（2）信息搜集。根据问题的性质和需求，选择合适的信息源。信息源可以包括搜索引擎、专业数据库、行业报告、学术文献、官方网站等，利用多种渠道和工具进行信息搜集，以确保信息的全面性和多样性。在搜集过程中，要注意评估信息的质量，包括信息的真实性、可靠性、时效性和相关性。

（3）信息整理与分析。将搜集到的信息进行分类整理，以便后续分析和处理，这一步骤包括信息筛选和信息分析。信息筛选，去除重复、冗余或无关的信息，保留对解决问题有用的信息。信息分析，运用合适的方法和工具对信息进行分析，如数据分析、趋势分析、对比分析等，以揭示信息背后的规律和趋势。

（4）制订解决方案。根据信息分析的结果，制订解决问题的具体策略或方案。对制订的方案进行可行性评估，包括资源投入、时间成本、预期效果等方面。

（5）实施与验证。按照制订的方案实施，确保各项措施得到有效执行，这一步骤包括监控进展和验证效果。监控进展，在实施过程中，密切关注问题解决的进展情况，及时调整和优化方案。验证效果，通过实际结果来验证解决方案的有效性，评估是否达到了预期的目标。

（6）总结与反馈。对解决问题的过程进行总结，提炼出成功的经验和不足之处。将总结的经验和教训反馈给相关人员或组织，以便在未来的问题解决过程中进行改进和优化。

运用信息解决问题的流程是一个动态循环的过程，可能需要根据实际情况进行多次迭代和调整。同时，不同的问题和情境可能需要采用不同的方法和工具，因此在运用信息解决问题的过程中，需要保持灵活性和创新性，不断适应变化的需求和环境。

信息素养在新时代已经不仅仅局限于信息获取和处理的技能层面，而是涵盖了信息意识、信息获取与检索、信息评估与判断、信息处理与应用、信息交流与协作、信息伦理与责任以及信息创新与创造等多方面。这些新内涵的拓展和丰富使得信息素养成为个体适应新时代发展的重要能力之一。

5.1.4　信息化职业能力的培养

新时代职业教育改革要求深化复合型职业人才培养，开展信息素养教育。一方面是为了让学生更好地适应信息化社会的生活和学习环境，构建终身学习能力。另一方面是使就读于各专业的学生形成信息化职业能力。

各专业学生可以从以下几方面，提高自身信息化职业能力发展水平。

（1）掌握信息技术基础知识和技能。包括掌握计算机基础知识，熟练掌握计算机的基本操作技能，熟练掌握基本的信息处理和信息展示应用软件的操作，掌握因特网的基本应用，掌握计算机安全使用和信息安全基本知识，掌握基本的编程知识，了解新一代信息技术的基本知识和部分应用场景等。

（2）提高自身信息素养。

（3）关注和收集本专业密切相关的信息源。了解并掌握一批本专业密切相关的专业知识库、行业专题网站等，了解本专业信息分类和检索的基本方法。

（4）在所学专业领域努力提升信息化实践水平。

请根据个人信息素养情况，完成个人信息素养自评图，如图 5.4 所示。

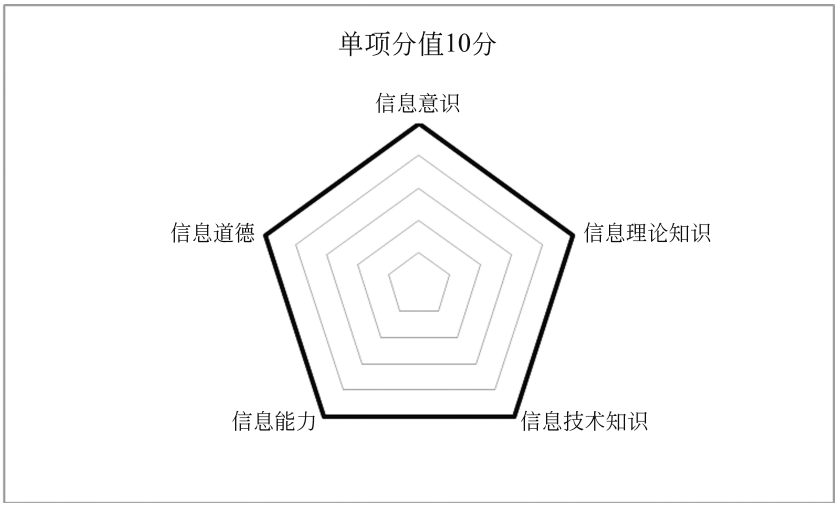

图 5.4　个人信息素养自评图

5.1.5　信息素养评价的标准

2003 年和 2005 年，联合国教科文组织分别召开两次专题性的世界大会，将信息素养界定为一种能力，即“信息素养是人们在信息社会和信息时代生存的前提条件，是终身学习的重要因素，能够帮助个体和组织实现其生存和发展的各类目标，它能够通过确定、查找、评估、组织和有效地生产、使用和交流信息来解决问题”。

2005 年，清华大学孙平教授发布了由他主持研究的“北京地区高校信息素质能力指标体系”。该指标体系由 7 个维度、19 项标准、61 个三级指标组成。该指标体系作为北京市高校学生信息素养评价的重要指标，是我国第一个比较完整、系统的信息素养能力体系。以下为该指标体系的框架。

维度 1：具备信息素质的学生能够了解信息以及信息素质能力在现代社会中的作用、价值与力量。

维度 2：具备信息素质的学生能够确定所需信息的性质与范围。

维度 3：具备信息素质的学生能够有效地获取所需要的信息。

维度 4：具备信息素质的学生能够正确地评价信息及其信息源，并且把选择的信息融入自身的知识体系中，重构新的知识体系。

维度 5：具备信息素质的学生能够有效地管理、组织与交流信息。

维度 6：具备信息素质的学生作为个人或群体的一员能够有效地利用信息来完成一项具体的任务。

维度 7：具备信息素质的学生了解与信息检索、利用相关的法律、伦理和社会经济问题，能够合理、合法地检索和利用信息。

5.2 信息安全与责任

知识目标：

- 了解信息安全、信息责任的概念。

能力目标：

- 通过识别信息安全威胁，提高个人信息安全防护能力。

素养目标：

- 培养信息安全意识、提高信息敏感度，自觉遵守信息道德行为准则。

本节内容思维导图如图 5.5 所示。

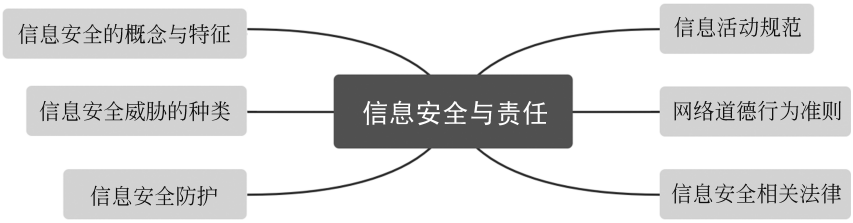

图 5.5 信息安全与责任思维导图

在当今数字化的时代，信息如同空气一般无处不在，渗透到我们生活的每一个角落。从日常的社交互动、在线购物，到重要的金融交易、政务处理，信息的流动和交换支撑着社会的运转。然而，伴随着信息的广泛应用，信息安全问题也日益凸显，成为我们不得不面对的严峻挑战。

【思考】

问题 1：我们在生活中可能遇见哪些信息安全的问题？

问题 2：结合自己所学专业，思考在工作岗位中需要承担哪些信息责任？

5.2.1 信息安全与防护

1. 信息安全的概念与特征

信息安全是对信息系统的硬件、软件以及数据信息实施的安全防护。信息安全对于

保护个人隐私、企业商业秘密、国家机密等至关重要。信息安全具有以下基本特征。

(1) 保密性。信息的保密性是指对于隐私信息,如交易记录、账户密码、社交信息等,未经授权者授权不能获取、阅读或查看。保密性是信息安全的核心特征。例如人们在使用社交媒体时,应当合理设置隐私权限,如个人信息、发布的内容和位置信息等,避免将过多的个人隐私暴露给不相关的人,以防止被骚扰或诈骗。

(2) 完整性。信息的完整性是指信息不被非法更改、篡改或销毁,确保信息的完整性从而有效保证信息的可用性和可信程度。在网络社交平台上,大学生经常分享个人见解、学习心得和生活点滴。信息的完整性要求这些分享的内容在传播过程中不被恶意篡改或曲解,以维护个人的声誉和形象。例如,在社交媒体上发布的时事观点或工作内容,应当确保信息的准确性和完整性,避免被他人断章取义或误导他人。

(3) 可用性。信息的可用性是指被授权的用户在需要时能够便捷、准确地获取到所需信息的程度。它不仅仅关乎信息是否存在,更强调信息能否以用户易于理解、访问和使用的形式呈现。在信息爆炸的时代,大学生需要快速筛选出对自己有用的信息。例如,在寻找实习机会时,一个能根据个人专业、兴趣和地理位置推荐实习岗位的平台,就比一个仅提供大量杂乱无章岗位信息的网站更受大学生欢迎。

(4) 可信度。信息的可信度是信息安全的重要特征之一,它是指信息的真实、准确和可信程度。大学生在注册在线学习平台时,要仔细阅读平台的隐私政策和用户协议,了解平台如何收集、使用和保护个人信息。如果平台的隐私政策模糊不清或存在漏洞,要谨慎考虑是否继续使用该平台。

(5) 不可抵赖性。信息的不可抵赖性,也称作不可否认性,是指在网络信息系统的信息交互过程中,所有参与者都不可能否认或抵赖曾经完成的操作和承诺。在涉及信息安全和隐私保护的场景中,数字签名和身份验证技术是实现信息不可抵赖性的重要手段。大学生在使用各种网络服务时,可能需要提供身份验证信息或签署数字协议。这些操作都确保了信息的真实性和不可抵赖性,保护了用户的合法权益。

(6) 可控性。信息的可控性是指网络系统和信息在传输范围和存放空间内的可控程度,也就是人们对信息的传播路径、范围及其内容所具有的控制能力。在大学校园中,学校通常会通过网络技术手段对校园网络进行管理,以确保网络信息的可控性。例如,学校可以设置网络访问权限,控制哪些网站或资源可以被学生访问。这有助于防止不良信息的传播,维护校园网络的安全和秩序。

2. 信息安全威胁的种类

威胁信息安全的因素很多,主要有以下 4 种,如图 5.6 所示。

(1) 计算机病毒。计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。如今,计算机病毒的威胁变得愈发多元化和复杂化。勒索病毒、二维码病毒、键盘监听病毒等,从数据勒索到系统入侵,对全球网络安全构成严峻挑战。

(2) 网络黑客。在信息安全受到的威胁中,网络黑客通过网络扫描、利用漏洞、暴力破解、篡改攻击、植入后门和恶意软件等技术手段来侵害信息安全,这些手段不仅具有高

图 5.6　信息安全威胁的种类

度的隐蔽性和破坏性，而且往往难以被及时发现和防范。我国法律对黑客攻击行为有明确的制裁措施，不仅规定了刑事责任，还涉及民事责任和行政责任。

（3）垃圾信息。通过垃圾邮件、短信等方式发送的包含恶意链接或附件的信息，一旦用户单击或下载，可能会导致其个人信息（如姓名、电话、地址、账号密码等）被不法分子窃取。垃圾信息充斥着网络空间，使得用户需要花费大量时间和精力去筛选和识别真正有用的信息，降低了信息获取的效率和质量。

（4）隐私泄露。隐私泄露最直接的影响是个人信息被未经授权的第三方获取。这些信息一旦落入不法分子手中，就可能被用于银行卡盗刷、网络诈骗等活动，导致受害者遭受经济损失。隐私泄露事件频发会加剧公众对信息安全的担忧和不信任感，影响社会的和谐稳定。

3. 信息安全防护

有效的硬件与软件信息安全防护是确保计算机系统稳定运行和数据安全的重要措施。包括硬件信息安全、软件信息安全、人员信息安全防护 3 方面。

（1）硬件信息安全防护包括计算机物理安全、设备保护、防止被盗或非法移动、环境控制、网络设备安全等。

（2）软件信息安全防护包括技术层面的数据加密，对敏感数据进行加密存储和传输，以防止数据在存储和传输过程中被未授权访问。

（3）人员信息安全防护包括制定信息安全政策，建立一套符合组织实际情况的信息安全政策；安全培训与教育，定期对相关人员进行网络安全和信息安全培训，提高相关人员的信息安全意识和操作技能。

5.2.2　信息社会责任

信息社会责任是指在信息社会中，个体在文化修养、道德规范和行为自律等方面的综合表现。具备信息社会责任的人具有信息安全意识，能够遵守信息法律法规，信守信息社会的道德与伦理准则，在现实空间和虚拟空间中尊重公共规范，既有效维护信息活动中的

个体合法权益，也积极维护他人合法权益和公共信息安全。

1. 信息活动规范

信息道德(Information Morality)是指在信息的采集、加工、存储、传播和利用等信息活动各个环节中，用来规范其间产生的各种社会关系的道德意识、道德规范和道德行为的总和。信息道德具有巨大的约束力，能够在潜移默化中规范人们的信息行为，是信息政策和信息法律建立和发挥作用的基础。

知识产权(如专利、著作权)通过法律手段保护创新成果，为标准化提供技术基础；标准化可以提高信息活动效率，保障信息质量。信息活动中涉及大量知识产权、标准化的生成、传播与利用。知识产权、标准化也可以激励信息活动中的创新与规范信息使用。

1) 知识产权

知识产权又称为智慧财产权，是指人们对其智力劳动成果所享有的民事权利。知识产权是依照各国法律赋予符合条件的著作者以及发明成果拥有者在一定期限内享有的独占权利，是一种无形的财产。它有两类：一类是版权，另一类是工业产权(专利权)。

版权(Copyright)亦称“著作权”，是指权利人对其创作的文学、科学和艺术作品所享有的独占权。这种专有权未经权利人许可或转让，他人不得行使，否则构成侵权行为(法律另有规定者除外)。

专利权通过权利人向国家专利管理部门申报，经过一定的法律程序获得。版权一般因创作而自动产生，它包括精神权利(发表权、身份权、修改权等)和经济权利(复制权、发行权、公演权、广播权、追偿权等)。前者不可转让、不可剥夺，也无时间限制；后者则可转让、可继承或者许可他人使用。版权期限各国规定不同，少至作者有生之年及其死后 25 年，多至死后 80 年。

2) 标准化

标准是对重复性事物和概念所做的统一规定。规范、规程都是标准的一种形式。标准化的实质是通过制定、发布和实施标准达到统一，其目的是获得最佳秩序和社会效益。

标准化是在经济、技术、科学及管理等社会实践中，以改进产品、过程和服务的适用性，防止贸易壁垒，促进技术合作，以促进最大社会效益为目的，对重复性事物和概念通过制定、发布和实施标准达到统一，获得最佳秩序和社会效益的过程。

2. 网络道德行为准则

网络道德行为准则的核心内容包括遵守法律法规、尊重知识产权、倡导诚实守信、健康上网、不传播有害信息、不侵犯他人权益、保护个人隐私和增强网络安全意识。旨在引导自觉遵守法律法规，维护网络空间的法治秩序，共同营造一个清朗、健康、和谐的网络环境。

具体来说，网络道德行为准则包括以下几方面。

(1) 遵守法律法规。严格遵守《中华人民共和国计算机信息网络国际联网管理暂行规定》《互联网信息服务管理办法》等国家法律法规，不制作、传播违法信息，自觉抵制网络犯罪活动。

（2）尊重知识产权。尊重他人的知识产权，不盗用、不抄袭、不传播未经授权的作品，同时保护自己的知识产权。

（3）倡导诚实守信。在网络交往中，不编造、不传播虚假信息，不参与网络欺诈行为。

（4）健康上网。树立正确的网络观念，合理安排上网时间，不沉迷网络，抵制低俗、暴力等不良信息。

（5）不传播有害信息。自觉抵制网络谣言、淫秽色情、暴力恐怖等有害信息。

（6）不侵犯他人权益。尊重他人的名誉、隐私等合法权益，同时保护自己的合法权益。

（7）保护个人隐私。重视个人隐私保护，不泄露、不传播他人的个人信息。

（8）增强网络安全意识。提高网络安全防范能力，不随意点击不明链接，不下载不明软件，防止网络攻击和个人信息泄露。

3. 信息安全相关法律

1994 年中国通过一条 64kb/s 的国际专线，全功能接入国际互联网，开启了中国互联网时代。1994 年 2 月 18 日，国务院颁布了《中华人民共和国计算机信息系统安全保护条例》，这是我国第一部有关互联网的法律文件，拉开了我国网络立法的序幕。

1997 年底，公安部发布了由国务院批准的《计算机信息网络国际联网安全保护管理办法》，明确了计算机信息网络国际联网的安全保护原则要求，规定了安全保护责任、安全监督、法律责任等。

2000 年底《全国人民代表大会常务委员会关于维护互联网安全的决定》明确了保障互联网的运行安全和信息安全的相关规定，确立了刑事责任、行政责任和民事责任“三位一体”的网络安全责任体系框架。

2012 年以来，随着互联网技术的进一步发展和普及，以及网络安全事件的频发，网络法治建设进入了高质量发展阶段。2016 年发布的《中华人民共和国网络安全法》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，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。

2017 年发布的《信息安全技术　个人信息安全规范》作为国家推荐标准，厘定、阐明了个人信息及其相关术语基本定义，个人信息安全基本原则，个人信息收集、保存、使用和处理等流转环节等，为提升公民意识、企业合规和政府调节水平提供了新的行为指引。

2021 年发布的《中华人民共和国个人信息保护法》进一步细化、完善了个人信息保护应遵循的原则和个人信息处理规则，明确个人信息处理活动中的权利义务边界，健全个人信息保护工作体制机制。

中国互联网立法对普通人维护信息安全具有多方面的意义。它不仅为个人信息保护提供了法律保障和权益维护的途径，还规范了行业行为、提升了公众意识与自我保护能力，并推动了技术创新与产业发展。这些措施共同构成了网络空间安全的重要屏障，为普通人的信息安全保驾护航。