**解读《中华人民共和国网络安全法》**

《中华人民共和国网络安全法》是为了保障网络安全，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，制定的法规。

信息时代使得人类站在了新时代的前沿，然而在享受互联网的红利和便捷时，开放的、共享的环境也使得我们常常暴露在危险之中。《网安法》在第一条就明确指出，“为了保障网络安全，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，制定本法”。要真正读懂这番话，必然离不开深入了解我国网络安全的现状。据《2016中国网民网络安全诉求洞察报告》显示，2016年十大网络安全事件，不论国内国外，都集中表现为数据泄露，具体手段包括但不限于非法出售、安全入侵等。据统计，2015年互联网应急中心共接收境内外报告的网络安全事件126916起，同比增长125.9%；威胁主要来自于境内，有126424起，同比增长128.6%。相比之下，来自境外的威胁逐渐减少，同比减少了43.9%。就网络威胁的渠道来看，PC端占比约为73%，是移动端的3倍，这在很大程度上也是因为电信、交通、金融等重要行业的信息存储，都主要依赖于PC端，而这些机构又极易受到网络入侵和攻击。此外，从2016年起，接连发生的大学生遭电信诈骗致死事件，公民个人隐私泄露案件，更突出了网络安全保护的刻不容缓。基于上述种种背景，作为名副其实的网络大国，我国的《网络安全法》及其配套文件应运而生。归结来说，《网络安全法》主要围绕以下三个方面：1. 加强关键信息基础设施的安全保障；2. 加强对个人和企业的权益保护；3. 维护国家安全和社会公共利益。

《网络安全法》全面设定网络运营者的安全保护义务，在《网络安全法》中关于义务性规定的数量远远大于禁止性规定，并详细列明了违反义务性规定所要承担的行政责任，这也反映出我国针对网络侵权甚至犯罪，“预防大于追究”的原则。

《网络安全法》明确举报危害网络安全行为的主体。网络安全法明确了公民对危害网络安全行为的举报权利，政府部门受理、处置公民举报的责任，保障了公民通过网络举报参与网络空间治理的有效性，让民间力量与官方机构一同努力，共筑网络安全防线。

同时，《网络安全法》着重保护个人信息，与民刑法相衔接。对用户个人信息数据的收集、存储、使用都给出了非常严格的规定，说其严格，不仅仅是因为设定的义务多而全，也是因为设定了较高的法律责任。

综上所述，《网络安全法》是我国网络安全领域的基础性法律，是我国网络治理体系的重要组成部分，也是我国参与国际网络治理合作的重要依据。《网络安全法》从网络安全的角度，对数据的定义、分类、保护、利用、监管等方面作出了系统规范，为我国网络安全治理提供了法律依据和制度保障。《网络安全法》的实施将有助于提升我国在数字经济时代的竞争力和话语权，保障我国在网络领域的主权和利益。