# 欧盟的《网络韧性法案》

2022年9月15日，欧洲委员会发布了数字产品网络安全法规草案——《网络韧性法案》（Cyber Resilience Act），以增强欧盟数字产品的网络安全性，并解决现有网络安全性监管框架的漏洞。该提议适用于具有数字元素的有形和无形产品，包括连接设备和非嵌入式软件，将网络安全标准强制应用于整个数字供应链。

《网络韧性法案》适用于“任何软件或硬件产品及其远程数据处理解决方案，包括单独上市的软件或硬件组件。”它将在整个生命周期内适用于这些产品——从设计阶段到过时阶段。

《网络韧性法案》涵盖有形数字产品，例如连接设备，以及非有形数字产品，例如嵌入到连接设备中的软件产品。实质上，《网络韧性法案》旨在覆盖连接到互联网的欧盟市场上的数字产品和互联网连接的软件。

为了应对不断增长的网络安全成本和漏洞，委员会指出《网络韧性法案》的四个具体目标：

* 确保制造商在整个生命周期内提高所覆盖产品的网络安全性；To ensure manufacturers improve the cybersecurity of covered products throughout the whole life cycle;
* 为欧盟创建单一、一致的网络安全合规框架；To create a single, coherent framework for cybersecurity compliance in the EU;
* 提高产品及其制造商的网络安全实践和属性的透明度；To increase the transparency of cybersecurity practices and properties of products and their manufacturers;
* 为消费者和企业提供安全的可用产品。To provide consumers and businesses with secure products ready for use.

通过加强欧洲数据驱动经济的网络安全性，《网络韧性法案》增强了欧盟的“塑造欧洲数字未来”战略。《网络韧性法案》通过创建适用于连接设备和服务的制造商、进口商和分销商的必要网络安全性要求列表，强制执行安全设计，并通过认证、报告和符合性评估来实现。

《网络韧性法案》不适用于软件即服务（software-as-a-service），除非该软件即服务是数字元素产品的整体远程数据处理解决方案的一部分。《网络韧性法案》只适用于在商业活动过程中开发或供应的自由开源软件。《网络韧性法案》的附文将商业活动定义为收费的产品或技术支持服务，提供一个软件平台，制造商从中获得其他服务的收益，或出于不改善安全性、兼容性或互操作性的原因使用个人数据。

欧盟的《网络韧性法案》草案主要针对欧盟内部的网络安全问题和网络基础设施的安全保障，涉及到的范围主要是欧盟成员国的公共部门、关键基础设施和数字服务提供商。然而，草案中涉及到的一些规定可能会影响欧盟与中国之间的网络安全合作，例如规定了欧盟成员国禁止使用未经授权的网络设备、禁止从未经授权的网络供应商获取网络设备、服务等。这可能会影响中国企业在欧洲市场的发展。

此外，随着欧盟对网络安全问题的关注程度提高，欧盟对从中国进口的网络设备和技术可能会更加审慎和谨慎。这可能会对中国企业在欧洲市场的进一步扩张和合作带来一定的限制。