中国关于个人信息的在法律上的确认以及立法相对西方国家比较晚，也比较不成熟。我国在诸多方面有对隐私信息的保护，但并没有一套独立的法典。参考发达国家在网络与个人信息上的立法有助于我们结合国情研究出更成熟完善的法律体系。

现在普遍认可的有三种保护模式：

**1  美国保护模式**

**2  欧盟保护模式**

**3  日本保护模式**

**1、美国模式：**

美国模式遵从两个原则：  
   a.告知原则：收集公民个人信息时，会对公民进行告知  
   b.选择权原则：公民对于自己个人信息的处理拥有足够的选择权。   
  美国网络信息安全的保护采用自律模式，同时它是自律模式的领导者。

美国的行业自律模式包含两个层次：  
   a.建议性行业指导，为行业内成员提供网络隐私保护的广为接受的指导建议

b.网络隐私认证计划（Online Privacy Seal Program）。网络隐私认证计划，要 求许可张贴隐私认证标示的网站，必须遵守网上在线收集、利用个人信息的行为规 则，并接受某种形式的监督管理。  
  1998年，美国联邦贸易委员会（FTC）抽查了1400个网站，只有14％的网站告知用户采集的个人信息将被如何使用。造成这一现象的主要原因是缺乏有力的法律约束。FTC据此认为有必要立法以确保网络隐私权得到保护，美国联邦贸易委员会提出了四项基本原则：  
 1.知会原则：收集和处理个人信息时，应将收集、利用的目的、用途、内容，明确 告知个人信息主体。  
 2.选择权原则：个人信息主体对被收集个人信息的使用目的、使用方式、二次开发 等享有完全的决定和选择权利。  
 3.通道与参与原则：个人信息主体有权查看所收集的本人的个人信息，并有权质疑 个人信息的准确性和完整性。  
 4.完全与完整性原则：应采取足够的管理、技术措施，防止未经授权的查看、损毁、 使用、披露个人信息。作为实施自律模式保护个人信息时的指导原则，以便与采取 立法模式的国家和地区保持一致。  
 自律模式的自我约束机制，在保护网络隐私权中发挥了一定作用。但是，自律模式也存在一些明显的缺陷：获得隐私认证，并不能保证不会侵犯个人隐私；当个人信息主体与网络经营者利益不一致，特别是个人信息用于商业用途可获得丰厚的商业利益时，很难保证会遵守认证协议；没有加入隐私认证计划的大多数公司，不会受到认证规则的约束和规范等。

**2、欧盟保护模式**

欧盟保护模式是由国家主导的立法模式。

与美国实行的行业自律模式不同，欧盟各国普遍认为，人格权是法律赋予自然人的基本权利，个人信息体现了自然人的人格利益，应当采取相应的法律手段加以保护。

欧盟采用立法模式保护个人信息，是基于保障基本的人格权益。

**3、日本保护模式**

欧盟和美国在国际政治、经济中的重要地位和作用，为个人信息安全提供了保护模式范本。与美国保护个人隐私的发生、发展类似，日本个人信息保护的发生、发展亦自地方公共团体和非政府的民间团体始。在现今日本相对完善的个人信息安全保障体系中，个人信息保护模式，参考了欧盟的立法模式，更多采纳了美国的保护规制，通过政府立法和行业自律实现个人信息安全。

**4、其它国家和地区立法模式**

德国个人数据保护法是比较有代表性的，采取统一立法模式，以信息自决权为宪法基础，以人格权为民法基础，统一规范、保护所有个人数据。

德国个人数据保护法规范了立法原则、监督机构、损害赔偿等机制，已经成为个人数据保护的一种立法范本。

下面主要分析一下美国出台的一个典型法案《网络安全信息共享法》。

【2015年12月，美国通过了《网络安全信息共享法》（CISA）】

六个方面：

1. **规定了联邦政府的网络安全信息共享**

机构之间共享非机密的“网络威胁指标”和“防御措施”，不仅是联邦机构之间的共享，也包括和其他民间机构的共享，然后，比较机密的内容只与拥有足够安全指标的外界共享，同时，政府发布“网络安全最佳实践”，用于帮助企业与民众保护自己的网络安全。

所以，网络安全信息共享，不是和其他人分享一些具体的个人隐私之类的内容，而是共享保护隐私信息方式的内容。

1. **规定了非联邦主体的网络安全信息共享**

《网络安全信息共享法》授权非联邦主体以网络安全目的可以与联邦机构和其他非联邦主体共享“网络威胁指标”和“防御措施”。国土安全部建立程序来帮助联邦主体和非联邦主体之间网络安全信息共享与交流，同时，CISA要求非联邦主体采取足够的措施保护共享的网络安全信息。

1. **规定私主体的责任豁免以鼓励信息共享**

私主体有权对自身的信息安全进行监视，同时，在获得其他主体的授权下，也可以对其他信息系统进行监视，并且拥有在这些信息系统中传送，存储，和处理消息的权利。同时，在获得授权的情况下，为了自身信息安全，私主体也可以对其他信息系统进行防御措施。另外，联邦主体和非联邦主体有义务进行网络安全信息共享，但是私主体不被强迫进行网络安全信息共享。同时，如果两个或多个私主体，为了网络安全目的提供防止、调查或减轻网络安全的协助，并不构成对反垄断法的违反。比如亚马逊的技术人员发现淘宝具有网络信息安全问题，并迫使淘宝倒闭，这种行为，在以前可能会触犯到反垄断法，但在这个法律中可以得到豁免。

1. **规定了隐私，自由和私权利的保护**

在共享网络安全信息系统中，如果发现了个人隐私信息内容，必须立刻进行移除，同时，保证系统中的内容都在合法且严谨的情况下进行使用。共享网络安全信息，并不意味着企业失去法定特权和保护，比如商业机密之类，网络安全信息共享的目的，是创建更加完善的信息保护系统，所以企业的商业性，财产性依旧得到法律的保护。如果在系统中，发现上述的信息，将立刻被提醒并移除。

1. **限制政府所获网络安全信息的用途**

政府所得到的网络安全信息只能用于网络安全目的比如对网络安全威胁与漏洞的披露，对恐怖分子等内容的追踪，不可以用于对非联邦机构正常行为的监控，同时州及地方政府的行为监控是在法律范围内的。比如之前的棱镜门，政府表示监控个人信息是为了防止恐怖分子的系列行为，虽然这个理由符合政府所得到的安全信息可使用范围，但违反了不可以用于对非联邦机构正产行为的监控，更何况是私主体。

1. **规定了联邦机构向国会定期报告制**

就是每年对网络安全信息系统的总结报告：信息共享措施的实施情况，政策、程序、指南遵从情况，将个人信息移除以保护个人隐私安全的情况，保护措施的充分性，以及面临的问题与威胁。

这个法律虽然重点是信息的共享，但共享的目的是使得个人信息得到更好的保障，同时其中展现的公私合作方式，使得这个信息共享模式也更加灵活和公开。以共享的方式来达到保护隐私方式的这种思考模式，值得我们进行借鉴。