Atitit 关于安全方面的法律法规

目录

[1. 信息安全保障立法体系介绍及思考 1 1](#_Toc29413)

[1.1. 一、保护信息安全立法情况 3 1](#_Toc24922)

[1.2. 二、打击计算机犯罪立法情况 4 1](#_Toc5726)

[1.3. 三、保护个人隐私立法情况 4 1](#_Toc14937)

[1.4. 四、保护关键基础设施立法情况 5 1](#_Toc30916)

[2. 法律方面的 1](#_Toc9244)

[2.1. rpc密码法 1](#_Toc32063)

[2.2. 国家安全法 1](#_Toc29571)

[2.3. 《网络安全法》 2](#_Toc4634)

[2.4.](#_Toc24284) [欧盟](#_Toc24284)[通用数据保护条例](#_Toc24284)[GDPR 2](#_Toc24284)

[2.5. 欧盟在1995年制定的《计算机数据保护法》。 2](#_Toc14581)

[2.6. 海外其他立法 2](#_Toc31679)

[2.7. 目前，美国信息安全方面的法律主要有： 2](#_Toc18838)

[3. Other 5](#_Toc16672)

[3.1. 我国的信息安全法的相关法规主要有八部： [4]  6](#_Toc3138)

[3.2. 其他 6](#_Toc22223)

[3.3. 我国信息安全法的相关规章主要有以下15部： [4]  6](#_Toc28602)

[4. 2.1 我国个人信息保护相关法律法规 7](#_Toc1521)

[4.1. 【表1：个人信息保护相关的重要法规及规范性文件汇总目录】 8](#_Toc88)

# 信息安全保障立法体系介绍及思考 1

## 一、保护信息安全立法情况 3

## 二、打击计算机犯罪立法情况 4

## 三、保护个人隐私立法情况 4

## 四、保护关键基础设施立法情况 5

# 法律方面的

## rpc密码法

## 国家安全法

## 《网络安全法》

网络安全法》于2016年11月6日由全国人大正式通过并将于2017年6月1日正式生效

## 欧盟通用数据保护条例GDPR

[编辑](https://baike.baidu.com/item/%E9%80%9A%E7%94%A8%E6%95%B0%E6%8D%AE%E4%BF%9D%E6%8A%A4%E6%9D%A1%E4%BE%8B/javascript:;)

[同义词](https://baike.baidu.com/subview/71844/10028254.htm" \o "同义词" \t "https://baike.baidu.com/item/%E9%80%9A%E7%94%A8%E6%95%B0%E6%8D%AE%E4%BF%9D%E6%8A%A4%E6%9D%A1%E4%BE%8B/_blank) GDPR一般指通用数据保护条例

《通用数据保护条例》（General Data Protection Regulation，简称GDPR）为欧洲联盟的条例，前身是

## 欧盟在1995年制定的《计算机数据保护法》。

## 海外其他立法

计算机安全法 ，信息自由法案，数据保护法，计算机犯罪法，软件保护法，保密法，个人隐私法

外的计真机信息安全立法在国际上,由于发达国家的计算机应用己非常普及,因此,其计算机安全立法工作也早己进行。不同形式的法律,如《计算机安全法》、《信息自由法》叭伪造访问设备和计算机欺骗与滥用法》、《数据保护法》、《计算机犯罪法

，2017年2月澳大利亚通过强制性数据泄露通知法案。此外日本的《个人信息保护法》（Personal Information Protection Act）修订版也于2017年5月30日起全面生效

## 目前，美国信息安全方面的法律主要有：

1966年，美国制定《信息自由法》，并且分别于1974年、1986年和1996年进行了修订，主要内容涉及对政府信息的获取、公开方式、可分割性，以及相关的诉讼事宜等。

1987年制定的《计算机安全法》，规定NIST负责开发联邦计算机系统的安全标准。除了国家安全系统被用于国防和情报任务外，商务部负责公布安全标准，加强联邦计算机系统安全保护的培训的责任，以提高联邦计算机系统的安全性和保密性。

1996年发布的《克林格-科恩法》，又名《信息技术管理改革法》，规定设立首席信息官(CIO)职位;授予商务部发布安全标准的权利，要求各个机构开发和维护信息技术架构;要求政府预算办公室(OMB)监督主要信息技术的收购，并且与国土安全部长协商，公布国家标准与技术研究院(NIST)制定的强制性联邦计算机安全标准。

2000年发布的《政府信息安全改革法》，规定联邦政府部门在保护信息安全方面的责任, 此法明确了商务部、国防部、司法部、总务管理局、人事管理局等部门维护信息安全的具体职责，建立了联邦政府部门信息安全监督机制。

2002年发布的《联邦信息安全管理法》，为联邦信息系统创建了一个安全框架。该法案强调风险管理，规定了OMB、NIST、CIOs、CISOs(首席信息安全官)、IGs(联邦机构监察长)的具体责任。倡导建立由OMB监督的中央联邦事件中心，负责分析安全事件并且提供技术帮助，通知机构运营商当前和潜在的安全威胁及漏洞。

2009年奥巴马总统签署《网络空间政策评估报告》，强调保障美国政府的网络系统安全。

美国打击计算机犯罪立法情况

1958年，世界上第一例计算机犯罪在美国硅谷发生，但是直至8年后才被发现，随后计算机犯罪引起了美国的高度重视。1970年美国颁布了《金融秘密权利法》，对金融业务计算机中存储的数据进行限制。到1984年美国制定了规范计算机犯罪的专门性法律《联邦计算机安全处罚条例》，并在1987年颁布。在1988年美国就成立了由计算机安全专家组成的行动小组，对违法犯罪程序和计算机病毒的防范进行研究。同年，美国国防部高级研究计划署成立计算机应急响应小组，负责计算机安全问题。美国有关计算机犯罪的法律主要有：

1984年的《伪造连接装置及计算机欺诈与滥用法》。这是美国通过的第一部关于计算机安全与犯罪的法案，规定了禁止对联邦计算机系统、银行系统、各州及对外贸易的各种攻击。

1986年签署的《计算机欺诈与滥用法》，扩展了1984年《伪造连接装置及计算机欺诈与滥用法》的范围，并对1986年《电子通讯隐私法》进行了补充，宣告未经授权访问“联邦利益”计算机(指被牵涉进某个刑事案件的两台或多台计算机，且它们位于不同的州)，及未经授权破解计算机口令为犯罪行为，以及交易盗窃的计算机密码为违法行为。在1994年的修正案中，对传播病毒和其他有害代码行为也作了规定。

《计算机欺诈与滥用法》颁布以后，网络技术的发展导致计算机犯罪出现新的形式，尤其是业内人士的犯罪行为增加，但该法并没有对内部人员犯罪做出规定，加上近些年计算机犯罪的产业化趋势，使得计算机犯罪立法更为急迫。

中国信息安全认证中心 宋扬

美国的国家信息安全保障体系由来已久，从“二战”期间对国家信息的保护，到“冷战”期间与前苏联之间的信息战，再到“911”事件发生之后，对信息安全保障的重视进入到一个新的阶段，时至今日美国的信息安全的保障体系已经逐步健全。美国信息安全保障框架形成了由安全技术、安全管理与政策法规三个层次统一协调的立体化框架。三个层次之间形成了一个有机整体。总体而言，美国现在的信息安全战略属于“扩张型”的信息安全战略，在关键基础设施、信息安全等级保护等相关领域制定了一系列的相关立法，形成了比较完善的信息安全保障体系。本文对美国信息安全保障立法体系进行介绍，并根据我国情况提出几点思考。

一、美国保护政府信息安全立法情况

美国对计算机网络高度依赖，从联邦政府到州政府，再到公民个人的大量信息几乎全部存储在计算机系统中，由于政府信息安全事关国家安全及政治稳定，一旦遭到破坏，产生的后果将更为深远和不可逆。因此，美国极为重视对政府信息的保护。

目前，美国有关政府信息安全方面的法律主要有：

1966年，美国制定《信息自由法》，并且分别于1974年、1986年和1996年进行了修订，主要内容涉及对政府信息的获取、公开方式、可分割性，以及相关的诉讼事宜等。

1987年制定的《计算机安全法》，规定NIST负责开发联邦计算机系统的安全标准。除了国家安全系统被用于国防和情报任务外，商务部负责公布安全标准，加强联邦计算机系统安全保护的培训的责任，以提高联邦计算机系统的安全性和保密性。

1991年发布的《高性能计算法》，规定建立满足安全需求的联邦高性能计算程序，此程序应当提供跨部门之间协调并向国会递交年度执行报告。此外，此法还要求NIST为联邦系统建立高性能计算的安全与隐私标准。

1996年发布的《克林格-科恩法》，又名《信息技术管理改革法》，规定设立首席信息官(CIO)职位;授予商务部发布安全标准的权利，要求各个机构开发和维护信息技术架构;要求政府预算办公室(OMB)监督主要信息技术的收购，并且与国土安全部长协商，公布国家标准与技术研究院(NIST)制定的强制性联邦计算机安全标准。

2000年发布的《政府信息安全改革法》，规定联邦政府部门在保护信息安全方面的责任, 此法明确了商务部、国防部、司法部、总务管理局、人事管理局等部门维护信息安全的具体职责，建立了联邦政府部门信息安全监督机制。

2002年发布的《联邦信息安全管理法》，为联邦信息系统创建了一个安全框架。该法案强调风险管理，规定了OMB、NIST、CIOs、CISOs(首席信息安全官)、IGs(联邦机构监察长)的具体责任。倡导建立由OMB监督的中央联邦事件中心，负责分析安全事件并且提供技术帮助，通知机构运营商当前和潜在的安全威胁及漏洞。

2009年奥巴马总统签署《网络空间政策评估报告》，强调保障美国政府的网络系统安全。

二、美国打击计算机犯罪立法情况

1958年，世界上第一例计算机犯罪在美国硅谷发生，但是直至8年后才被发现，随后计算机犯罪引起了美国的高度重视。1970年美国颁布了《金融秘密权利法》，对金融业务计算机中存储的数据进行限制。到1984年美国制定了规范计算机犯罪的专门性法律《联邦计算机安全处罚条例》，并在1987年颁布。在1988年美国就成立了由计算机安全专家组成的行动小组，对违法犯罪程序和计算机病毒的防范进行研究。同年，美国国防部高级研究计划署成立计算机应急响应小组，负责计算机安全问题。美国有关计算机犯罪的法律主要有：

1984年的《伪造连接装置及计算机欺诈与滥用法》。这是美国通过的第一部关于计算机安全与犯罪的法案，规定了禁止对联邦计算机系统、银行系统、各州及对外贸易的各种攻击。

1986年签署的《计算机欺诈与滥用法》，扩展了1984年《伪造连接装置及计算机欺诈与滥用法》的范围，并对1986年《电子通讯隐私法》进行了补充，宣告未经授权访问“联邦利益”计算机(指被牵涉进某个刑事案件的两台或多台计算机，且它们位于不同的州)，及未经授权破解计算机口令为犯罪行为，以及交易盗窃的计算机密码为违法行为。在1994年的修正案中，对传播病毒和其他有害代码行为也作了规定。

《计算机欺诈与滥用法》颁布以后，网络技术的发展导致计算机犯罪出现新的形式，尤其是业内人士的犯罪行为增加，但该法并没有对内部人员犯罪做出规定，加上近些年计算机犯罪的产业化趋势，使得计算机犯罪立法更为急迫。

三、美国保护个人隐私立法情况

美国的电子商务迅速发展,收集和分析个人信息的软件行业纷纷建立，给用户的个人隐私安全带来极大隐患。为了降低个人隐私因使用电脑等高科技过程中被侵犯的可能性，美国从法律层面加强对隐私的保护。美国有关隐私保护的法律落后于欧盟，尤其是2001《爱国者法》的出台，扩大了警察机关的权限，为政府更多涉入公民私生活创造了条件，违反确保公民私生活隐秘的宪法原则，引起很大的争议，美国应该考虑制定适应当今时代的新的隐私保护法律。美国有关信息安全的隐私保护法律有：

1974年的《隐私权法》，规定联邦机构限制个人可识别信息的披露，要求机构提供访问个人信息记录的权利。

1986年通过的《电子通信隐私法》主要禁止未经授权的电子窃听，对信息传输安全、存储安全和监视合法性进行的规定。

1998年美国通过了《儿童网上隐私保护法》，该法规定了网站经营者必须披露其隐私保护政策，声明寻求儿童监护人同意的时间及方式，以及违法儿童隐私保护应承担的责任。该法适用于美国管辖之下的自然人或单位对13岁以下儿童在线个人信息的收集。

2001的《医治保险携带和责任法》(HIPAA)修正案，目标之一就是保护病人的电子健康记录，并提出保护的具体标准。该法详细规定了行政保障措施、物理保障措施、技术保障措施及安全责任的分配

# Other

## 我国的信息安全法的相关法规主要有八部： [4]

(1)国务院《中华人民共和国计算机信息系统安全保护条例》(1994．02．18)

(2)国务院《中华人民共和国计算机信息网络国际联网管理暂行规定(修正)》(1997．05．20)

(3)国务院《计算机信息网络国际联网管理暂行规定实施办法》(1997．12．11)

(4)国务院《中华人民共和国计算机信息网络国际联网安全保护管理办法》(1997．12．11)

(5)国务院《互联网上网服务营业场所管理条例》(2002．09．29)

(6)国务院《中华人民共和国电信条例》(2000．09．25)

(7)国务院《互联网信息服务管理办法》(2000．09．25)

(8)国务院《信息网络传播权保护条例》(2006．05．18)

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》(国务院147号令)，这是一件具有重要意义的事情，这是我国第一部保护计算机信息系统安全的专门条例。

## 其他

例如2012年全国人大《关于加强网络信息保护的决定》

[编辑](https://baike.baidu.com/item/javascript:;)《个人信息安全规范》为我国个人信息保护工作的开展提供了详实的实务指南，该标准是国家推荐性标准，将于2018年5月1日正式实施。

随着国家标准《个人信息安全规范》（GB/T 35273-2017）的正式发布

## 我国信息安全法的相关规章主要有以下15部： [4]

(1)农业部《计算机信息网络系统安全保密管理暂行规定》(1997．04．02)

(2)公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》(1997．12．12)

(3)公安部中国人民银行《金融机构计算机信息系统安全保护工作暂行规定》(1998．08．31)

(4)公安部《计算机病毒防治产品评级准则》(2000．03．20)

(5)公安部《计算机病毒防治管理办法》(2000．04．26)

(6)邮电部《中国公用计算机互联网国际联网管理办法》(2000．05．25)

(7)教育部《教育网站和网校暂行管理办法》(2000．06．29)

(8)信息产业部《互联网电子公告服务管理规定》(2000．10．08)

(9)国务院新闻办公室，信息产业部《互联网站从事登载新闻业务管理暂行规定》(2000．11．07)

(10)信息产业部《非经营性互联网信息服务备案管理办法》(2005．02．08)

(11)信息产业部《电子认证服务管理办法》(2005．02．08)

(12)信息产业部《互联网IP地址备案管理办法》(2005．02．08)

(13)公安部《互联网安全保护技术措施规定》(2005．12．13)

(14)公安部国家保密局国家密码管理局国务院信息化工作办公室《信息安全等级一保护管理办法(试行)》(2006．01．17)

(15)公安部《网吧安全管理软件检测规范》

# ****2.1 我国个人信息保护相关法律法规****

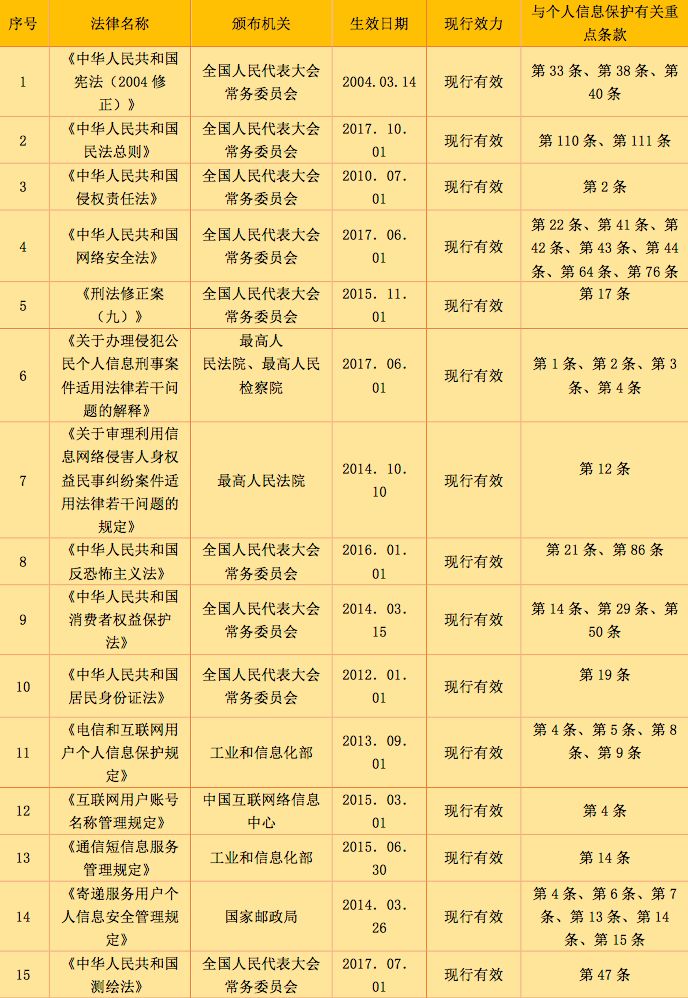
****国家根本大法层面，《宪法》****（1982年，2004修正）中关于“公民的人格尊严不受侵犯，公民享有通信自由和通信秘密的权利，国家尊重和保障人权”等相关条款是个人信息应当受到法律保护的《宪法》依据。

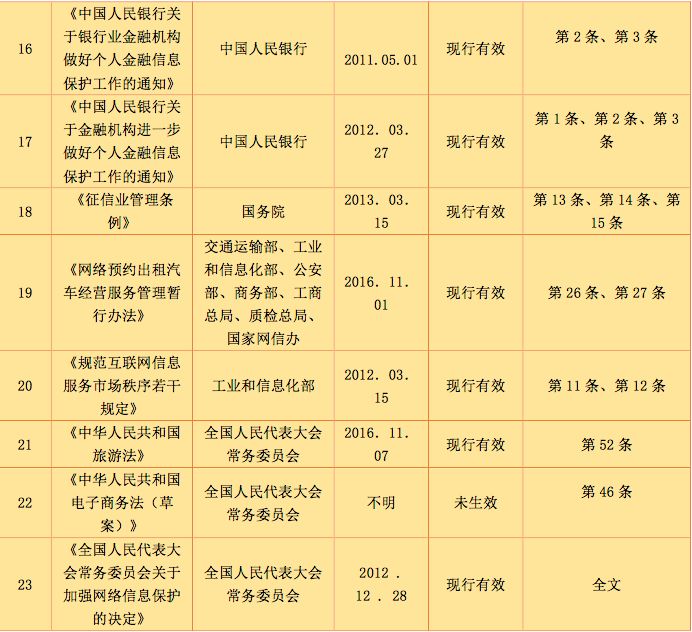
****民事法律层面，《民法总则》****（2017年）首次对隐私权和个人信息采取“二元论”保护模式[②]。《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（2014年）****首次从司法解释层面，明确了个人信息的法律内涵及侵权责任承担方式。《侵权责任法》（2010年）首次将隐私权纳入民事权益的范畴。****

****行政监管法律层面，《网安法》****（2017年）延续了《全国人民代表大会常务委员会关于加强网络信息保护的决定》（2012年）、《电信和互联网用户个人信息保护规定》（2013年）、《消费者权益保护法》（2014年）等关于个人信息保护的思路，明确了“个人信息”的概念，对个人信息保护提出了更为严格的要求。

****刑事法律层面，《刑法修正案七》****（2009年）新设“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”。《刑法修正案九》（2015年）对《刑法修正案七》进行了修改，将“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”整合为“侵犯公民个人信息罪”，明确放宽了侵犯公民个人信息罪的主体范围。

## ****【表1：个人信息保护相关的重要法规及规范性文件汇总目录】****





美国信息安全保障立法体系介绍及思考.html

重磅全文 \_ 美国新罕布什尔州签署《保险数据安全法案》\_ DataLaws - 链闻 ChainNews.html