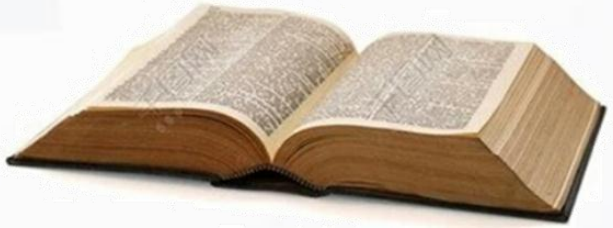
信息安全法律基础

敬畏律法、守法用法

——做网安护法卫士

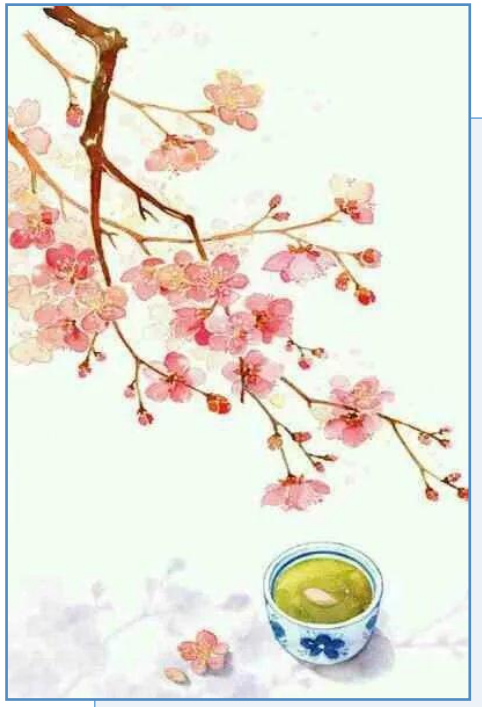


第2章 信息安全与立法

第2章　信息安全与立法

2.1　信息安全概述

2.2　信息安全立法、司法和执法



知识点探究

- 信息安全保障的三大支柱：信息安全技术、信息安全法律、信息安全标准
- 信息安全涉及的法律问题：计算机犯罪、民事问题、隐私问题……
- 网络立法规制的几种方法：实体规制法、程序规制法、类型规制法……
- （以小组为单位搜集相关案例，并进行分析）

和小伙伴们一起
探究更多问题

2. 1信息安全概述

2.1信息安全概述

2.1.1 信息与信息安全

- ISO/IEC的IT安全管理指南（GMITS）对信息(Information）的解释
    - 信息是通过在数据上施加某些约定而赋予这些数据的特殊含义。
- 信息通常表现为消息、信号、数据、情报、知识、智慧等，借助于信息媒体以多种形式存在或传播，可以存储在计算机、磁带、纸张等介质中，也可以记忆在人的大脑里，还可以通过网络、打印机、传真机等方式进行传播。
- 对于现代企业，信息是一种无形资产，尤其是商业数据、专利、论文、标准、管理规章等知识资产，是企业的关键信息资产，是核心竞争力，在知识经济时代，保障其安全已成为企业的一种基本能力。
- 国家层面的信息安全关系到国家安全，个人层面的信息安全关系到个人隐私和财产安全。

2.1信息安全概述

2.1.2信息安全的基本属性和任务

- 信息安全
  - 技术层面的信息安全（狭义的信息安全）—在客观上杜绝对信息安全属性的安全威胁，使信息的主人在主观上对信息的本源性放心。
- 信息安全的基本属性
- 完整性（integrity）
  - 完整性是指信息在存储或传输过程中保持不被修改、不被破坏、不被插入、不延迟、不乱序和不丢失的特性。

  可用性（avaliability）
  - 可用性是指信息可被合法用户访问并能按要求顺序使用的特性，即在需要时就可以取用所需的信息。

2.1信息安全概述

- 保密性（confidentiality）
  - 保密性是指信息不泄露给非授权的个人和实体，或供其使用的特性。
- 可控性（controllability）
  - 可控性是指授权机构可以随时控制信息的机密性。美国政府所提倡的“密钥托管”、“密钥恢复”等措施就是实现信息安全可控性。
- 可靠性（reliability）
  - 可靠性是指信息以用户认可的质量连续服务于用户的特性（包括信息的迅速、准确和连续地转移等）。
- 广义的信息安全—采取一切可能的方法和手段保证信息的“五性”安全。
- 信息安全的任务—采取有效措施（有效的技术、管理手段）让信息资产免遭威胁，或者将威胁带来的后果降到最低程度（风控），维护国家、组织的正常运作以及个人的正常生活。

2. 1信息安全概述

2.1.3信息安全保障的三大支柱

- 保障信息安全对国家、组织、个人而言都是一个复杂的系统工程，需要多管齐下，综合治理。
- 目前普遍认为信息安全技术、法律法规和信息安全标准是保障信息安全的三大支柱。
- 信息安全技术
  - 目前主要采用的信息安全技术有：数据加密技术、防火墙技术、网络入侵检测技术、网络安全扫描技术、黑客诱骗技术、病毒诊断与防治技术等。
  - 尽管信息安全技术的应用在一定程度上对信息的安全起了很好的保护作用，但它并不是万能的，由于疏于管理等原因而引起的安全事故仍然不断发生。

- 近年来，“内鬼”事件多次被曝出
- 除了外来的“黑客”，平台“内鬼”是造成个人信息和数据泄露的另一个主要原因。
- 某银行原信贷部副经理，就是一名“内鬼”，利用职务之便，以每条30块钱的价格卖掉了单位信息系统中3000多个客户的征信信息，其中包括姓名、身份证号码、家庭住址、工作单位等。
- 江苏常州警方曾破获一起特大侵犯公民信息案，案件中内鬼多达48名，涵盖银行、卫生、教育、社保、快递、保险、网购、汽修等多个行业，买卖的信息包括个人征信、车辆信息、开房住宿、收货地址等数十个种类的实时信息。

人性天然具有驱利性、有限理性、自由意志，利已或利他，向善或向恶，需要正向激励和反向约束。

2. 1信息安全概述

2.1.3信息安全保障的三大支柱（续）

- **信息安全法律法规**
  - 从法律层面上规范人们的行为，信息安全工作有法可依，相关违法犯罪能得到处罚，促使组织和个人依法制作、发布、传播和使用信息，从而达到保障信息安全的目的。
  - 目前，我国已建立基本的信息安全法律法规体系，但信息安全立法的任务还非常艰巨，许多相关法规还有待建立或进一步完善。
- **信息安全标准**
  - 建立统一的信息安全标准，为信息安全产品的制造、安全管理体系的构建、安全工作评估等提供统一的科学依据。
  - 目前信息安全标准大致可分为信息安全产品标准、信息安全技术标准和信息安全管理标准三大类，国际标准的制定主要侧重于信息安全管理，而国内标准的制定则主要侧重于信息安全产品和信息安全技术。

- **我国企业在信息安全标准方面的实践**
- 例：阿里巴巴已经成功转型为一家技术公司，拥有近3万名科技工程人员，2016年6月29日，阿里云在云栖大会•成都峰会发布《数据安全白皮书》，首次公开了阿里云在保障用户数据安全方面建立的流程、机制以及具体实践办法，并得到了国际多家标准组织的肯定。
- 支付宝获得“个人信息安全管理体系认证”，成为首批获得国家认证的企业之一。

CCRC

个人信息安全管理体系认证证书

证书编号:CCRC-2018-PISMS-J-104-R0（试点）

兹证明

支付宝（中国）网络技术有限公司

建立的个人信息安全管理体系符合

GB/T 35273-2017

及隐私政策（2018 年 12 月 25 日版）

认证范围包括：

注册地址：中国（上海）自由贸易试验区银城中路 501 号 17 层 1701-1708 室，200120

受审核地址:杭州市西湖区万塘路 18 号黄龙时代广场 B 座，310099

业务范围：

扫码支付、线上支付等网络支付业务服务。

颁证日期：2018 年 12 月 30 日　　有效期至：2019 年 12 月 29 日

2.2信息安全立法、司法和执法

2. 2信息安全立法、司法和执法

2.2.1 信息安全涉及的法律问题

1 计算机犯罪

- 计算机犯罪（Computer Crime）是指行为人通过计算机操作所实施的，危害计算机信息系统（包括内存数据及程序）安全以及其他严重危害社会的，并应当处以刑罚的行为。
  - 从大的犯罪分类来看，计算机犯罪属于妨害社会管理秩序罪中的扰乱公共秩序罪。
  - 计算机犯罪产生于20世纪60年代，随着计算机技术的发展和计算机应用的日益普及，到21世纪初，计算机犯罪已呈猖獗之势，并越来越受到各国的重视。

2. 2信息安全立法、司法和执法

- 《中华人民共和国刑法》中关于计算机犯罪的规定有三个条款:
  - 第285条　违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。
  - 第286条　违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。
  - 第287条　利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。
  - 以上三条分别对应非法侵入计算机信息系统罪、破坏计算机信息系统罪和利用计算机犯罪等三种计算机犯罪的表现形式。第285、286条是1997年新刑法新增加的罪名，并规定了相应的刑罚。第287条是对以计算机为犯罪工具的原则性规定，其刑罚由其他的相关条款规定。

2. 2信息安全立法、司法和执法

- 计算机犯罪的实质特征
  - 从犯罪的实质含义上，刑法第285、286条所规定的犯罪称为狭义的计算机犯罪或单纯的计算机犯罪，加上第287条则称为广义的计算机犯罪。
  - 单纯的计算机犯罪区别于其他犯罪具有以下三个实质特征:

（1）计算机本身的不可或缺性和不可替代性。

（2）明确了计算机犯罪侵害的客体（即计算机信息系统）。

（3）在某种意义上，计算机作为犯罪对象出现的特性。

（参见教材P8案例1、2，请同学谈谈自己的看法）

2. 2信息安全立法、司法和执法

- 计算机犯罪的常用方法
  - 以合法手段为掩护，查询信息系统中不允许访问的文件，或者侵入重要领域的计算机信息系统。
  - 利用技术手段，非法侵入重要的计算机信息系统，破坏或窃取计算机信息系统中的重要数据或程序文件，甚至删除数据文件或者破坏系统功能，直至使整个系统处于瘫痪。
  - 在数据传输或者输入过程中，对数据的内容进行修改，干扰计算机信息系统。
  - 未经计算机软件著作权人授权，复制、发行他人的软件作品，或制作、传播计算机病毒，或制作传播有害信息等。

（以小组为单位搜集相关案例，并进行分析）

2. 2信息安全立法、司法和执法

2.2.1 信息安全涉及的法律问题（续）

2 民事问题

在计算机及网络的使用等方面，不仅存在犯罪问题，也存在民事诉讼问题。人们在使用计算机和网络时有意或无意地侵权，都有可能被提起民事诉讼。（参见教材P9案例4）

3 隐私问题

隐私问题是信息安全和保密中所涉及的一个非常重要的问题， 隐私问题在个人、 组织中都存在，如何利用法律手段有效地保护组织和个人的隐私也是目前法律规制的一个挑战。（参见教材P11案例5）

2. 2信息安全立法、司法和执法

2.2.2 立法、司法和执法组织

1 立法

- 立法权及等级
  - 立法权是一定的国家机关依法享有的制定、修改、废止法律等规范性文件的权力，是国家权力体系中最重要的核心的权力。
  - 我国的立法权根据享有立法权主体和形式的不同，分为国家立法权、地方立法权、行政立法权和授权立法权等，不同级别立法的内容，立法的主体，所立法律的适用范围是不同的。

2. 2信息安全立法、司法和执法

（1）国家立法权

- 国家立法权是由一定的国家权力机关行使，用以调整基本的、带全局性的社会关系，在立法体系中居于基础和主导地位的最高立法权。
- 国家立法权的立法主体是全国人民代表大会及其常务委员会、国务院。

（2）行政立法权

- 行政立法权是源于宪法，由国家行政机关依法行使的，低于国家立法的一种独立的立法权，包括中央行政立法权和地方行政立法权。主要行使行政规章的立法权。

（3） 地方立法权

- 地方立法权是由有权的地方国家权力机关行使的立法权。主要行使地方性法规的立法权。地方立法权的主体一般是省、自治区、直辖市的人民代表大会及其常务委员会和较大市的地方人民代表大会及其常务委员会，另外还有民族自治地方的人民代表大会。

2. 2信息安全立法、司法和执法

- 立法组织与立法程序
  - 享有立法权的组织即立法组织。例如:在我国，国务院、全国和各地区人大是立法组织。其中，全国人大及其常委会是我国的最高立法组织。
  - 目前，我国法律的制定程序主要有以下四个步骤

（1）法律方案的提出。

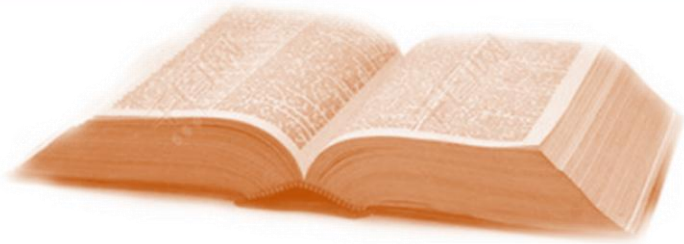
（2）法律草案的审议。

（3）法律草案的表决和通过。

（4）法律的公布。

2. 2信息安全立法、司法和执法

- **我国信息安全法律规范体系**
  - 我国对信息安全的保护主要通过以下三大体系予以保障。
  - 基本法律体系



国家在许多基本法律中都设计了用于保护信息安全的条款，如《宪法》第40条、《刑法》第285、286、287条都作出了相关规定。近年来国家又相继出台了《中华人民共和国电子签名法》、《中华人民共和国网络安全法》等法律。

  - 政策法规体系
    - 政府制定的一系列法规、规章，具体强化了对信息安全保护的力度。如《中华人民共和国计算机信息系统安全保护条例》、《计算机病毒防治管理办法》、《互联网上网服务营业场所管理条例》等。
  - 强制性技术标准体系
    - 国家颁布了一系列技术标准，并且是强制性地执行，如《计算机信息系统安全保护等级划分准则》、《计算机信息系统安全专用产品分类原则》、《计算站场地安全要求》等，从技术上规范了对信息安全的保护。

2. 2信息安全立法、司法和执法

- 网络立法规制的三种方法
  - 在2016年《网络安全法》颁行之后，我国迎来了网络安全相关立法的“井喷期”。这里所说的“立法”是广义概念，既包括制定行政法规和部门规章这些行政性立法，也包括制定技术标准和出台司法解释的“准”立法。
  - 以《网络安全等级保护条例（征求意见稿）》《信息安全技术 个人信息安全规范》及《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》三个规定为例，提出网络立法规制的三种方法，即实体规制法、程序规制法和类型规制法。

谢君泽

中国人民大学网络犯罪与安全研究中心秘书长

中国人民大学物证技术鉴定中心副主任

2. 2信息安全立法、司法和执法

- 实体规制法——传统的立法方法
  - 以《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》为例，先对个人信息这个实体性概念进行界定，然后在此概念基础上形成相关的实体性规则。
  - 《解释》第一条：公民个人信息是指以电子或者其他方式记录的，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。
  - 该解释对公民个人信息的界定采用了“身份指向性”和“行为指向性”双重标准。前者与后者是“质”与“量”的关系。当“行为指向性”信息足够充分明确时，是完全有可能构成“身份指向性”特征的，前提是可以采集到“样本等于全体”的行为信息（个体行为画像）。
  - 在刑法讲究谦抑性原理的情况下，将公民个人信息进行明显不合理的扩大界定，将面临扩张打击的刑事风险。

2. 2信息安全立法、司法和执法

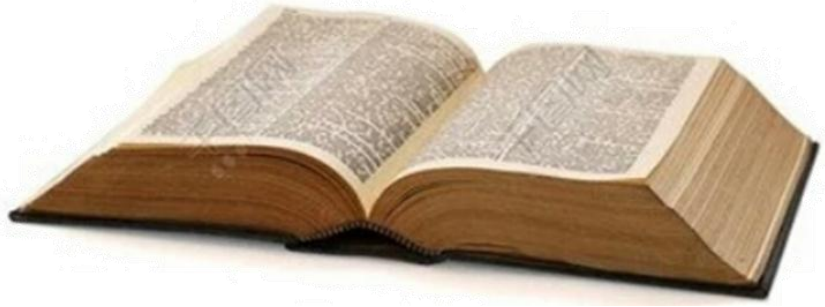
- 程序规制法—时效的立法方法
  - 在实体性规则尚未成熟的情况下，通过程序性指引规制人们的行为方式。
  - 例：2017年的《信息安全技术 个人信息安全规范》，在体例上设计为个人信息的收集、个人信息的保存、个人信息的使用、个人信息的委托处理、共享、转让、公开披露等，并建立相应的具体规则（程序要求）。该规范与欧盟的《通用数据保护条例》（GPDR）一脉相承GPDR的主体部分主要是规定了数据主体、控制者、处理者在不同情形下的权利、义务与行为准则。
  - 程序规制法当下意义较大，能够一定程度解决当前问题，实务指导性较强，该规制方法也往往被务实的英美法系国家所接纳。
  - 采用程序规制法解决信息网络问题，需要归纳网络环境各种行为的可能性，但由于网络具有天然的自由、开放属性，要穷尽各种行为可能性制定规则挑战巨大 。

2. 2信息安全立法、司法和执法

- 类型规制法—实用的立法方法
  - 当抽象一般概念及其逻辑体系不足以掌握某生活现象或意义脉络的多样表现形态时，一种辅助的规制形式是“归类”。
  - 例：正在征求意见的《网络安全等级保护条例（征求意见稿）》，该条例第十五条规定：根据网络在国家安全、经济建设、社会生活中的重要程度，以及其一旦遭到破坏、丧失功能或者数据被篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及相关公民、法人和其他组织的合法权益的危害程度等因素，网络分为五个安全保护等级。（等级规制）

2. 2信息安全立法、司法和执法

2.2.2 立法、司法和执法组织（续）



2 我国的司法组织

- 我国的司法组织主要包括以下两大系统:

（1）人民法院，其中，最高人民法院是最高审判机关；

（2）人民检察院，其中，最高人民检察院是最高检察机关。

- 人民检察院是国家法律监督机关。它独立行使公诉权，同时行使批准逮捕权、逮捕权、抗诉权，对涉及贪污、玩忽职守、侵犯人民选举权等特定犯罪有自行侦查权。检察院实行同级人民代表大会、上级检察院双重领导制度，有县（市）、市（地）、省（自治区、直辖市）、最高四级。

2. 2信息安全立法、司法和执法

2.2.2 立法、司法和执法组织（续）

3 我国的执法组织

- 我国的执法组织包括:人民法院、人民检察院、公安部、安全部、工商行政管理局、税务局等。不同的执法组织在不同的职权范围内行使职权。

（1）对刑事案件的侦查、拘留、执行逮捕、预审，由公安机关负责。

（2）检察、批准逮捕、检察机关直接受理的案件的侦查、提起公诉，由人民检察院负责。

（3）审判由人民法院负责。

（4）国家安全机关依照国家法律规定，办理危害国家安全的刑事案件，行使与公安机关相同的职权。

感谢聆听