个人信息安全保护

专 业 课 小 课 堂

主讲：曹阳 陈健

时间：2021年9月

课程目录

第一课 标准制定背景及个人信息保护原则

个人信息保护的立法进程

2015年前

- 《刑法修正案（七）》（2009.2）
- 《全国人大常委会关于加强网络信息保护的决定》（2012.12）
- 《消费者权益保护法》（2013.10修正）
- 《刑法修正案（九）》（2015.08）

2016-2018

- 《网络安全法》（2016.11）
- 《民法总则》（2017.03）
- 最高法、最高检《关于办理侵害公民个人信息刑事案件若干问题的解释》（2017.05）
- 信安标委《信息安全技术个人信息安全规范》（2017.12）

2019-2021

- 网信办《儿童个人信息网络保护规定》（2019.08）
- 信安标委《信息安全技术个人信息安全规范》修订版（2020.03）
- 《民法典》（2020.05）
- 《未成年人保护法》修订（2020.10）
- 《数据安全法》（2021.9.1）
- 《个人信息保护法》（2021.11.1）

第一课 标准制定背景及个人信息保护原则

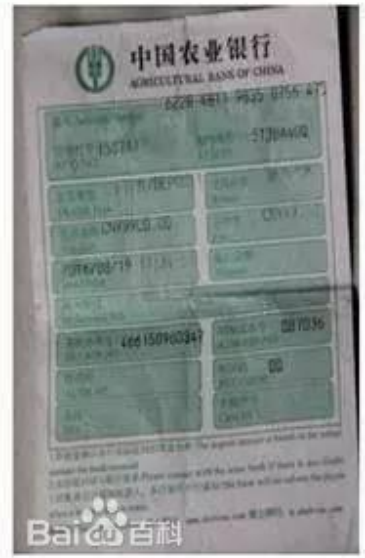
➲ 全球个人信息保护立法（右表）

国家/地区	法律名称	时间/修订历程
美国	《健康保险流通和责任法》 The Health Insurance Portability and Accountability Act,HIPAA	1996年8月美国总统签署生效
	《金融服务现代化法》 Financial Services Modernization Act.又称Gramm-Leach-Bliley Act	1999年11月美国总统签署生效
	《儿童在线隐私保护法》 The Children's Online Privacy Protection Act.,COPPA	1998年10月美国国会通过，2000年4月生效
	《加利福尼亚消费者法》 California Consumer Privacy Act，CCPA	2018年6月加州议会通过，2020年1月生效
欧盟	《通用数据保护条例》 General Data Protection Regulation，GDPR	2016年4月欧洲议会通过，2018年5月生效
德国	《联邦数据保护法》 Federal Data Protection Act，即Bundesdatenschutzgeset，BDSG	1978年1月正式生效，1983年、1990年、2009年、2010年、2016年五次修订
法国	《数据保护法》 Data Protection Act	1978年1月正式生效。1999年、2018年两次修订
英国	《数据保护法》 Data Protection Act，DP	1984年5月英国下院通过，1998年、2018年两次修订
日本	《个人信息保护法》 Act on the Protection of Personal Infomation，APPI	2005年4月日本众议院通过，2017年、2020年两次修订
新加坡	《个人数据保护法》 Personal Data Protection Act，PDP	2012年10月新加坡国会通过，2013年1月正式生效，2020年修订
印度	《个人数据保护法（草案）》 Personal Data Protection Bi	《个人数据保护法（草案）》2018年7月印度高级别委员会发布草案，2019年印度高级别委员会发布送审稿，提交国会审核

第一课 标准制定背景及个人信息保护原则

那些催生个保法出台的案件

2016年8月 山东女孩徐玉玉被南京邮电大学录取，因受电信诈骗损失学费的刺激，溘然离世；



2019年4月 郭兵起诉杭州野生动物世界将其年卡认证识别方式由指纹升级为人脸识别，侵犯其个人隐私信息；

2020年5月 中信银行上海虹口支行在未获授权的情况下擅自将某脱口秀演员的个人账户流水提供给第三方，受到银保监调查。

第一课 标准制定背景及个人信息保护原则

表A.1 个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等
个人财产信息	银行账户、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
个人常用设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/Android ID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

什么是个人信息

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

第一课 标准制定背景及个人信息保护原则

什么是个人敏感信息

表B.1 个人敏感信息举例

个人财产信息	银行账户、鉴别信息（口令）、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息
个人健康生理信息	个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

一旦泄露或者非法使用，可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息，包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。

第一课 标准制定背景及个人信息保护原则

1 合法性

处理个人信息应当采用合法、正当、必要的方式，遵循诚实信用原则，不得通过欺诈、诱骗、误导、强迫等方式处理个人信息，不得通过非法渠道处理个人信息，不得违反法律、行政法规的规定处理个人信息，不得从事危害国家安全、公共利益的个人信息处理活动。

2 权责一致

采取技术和其他必要的措施保障所处理的个人信息安全，并对个人信息处理活动负责，对其个人信息处理活动对受访者或其他个人合法权益造成的损害承担责任。

3 目的明确

具有明确、合理的的个人信息处理目的。

个人信息保护原则

第一课 标准制定背景及个人信息保护原则

4 最小必要

处理个人信息应当限于实现处理目的的最小范围，不得进行与处理目的无关的个人信息处理。

5 公开透明

以明确、易懂和合理的方式明示个人信息处理规则，并接受外部监督。

6 准确性

为实现处理目的，所处理的个人信息应当准确，并及时更新。

个人信息保护原则

谢 谢！

主讲：曹阳 陈健

时间：2021年9月