教育信息化安全及证据意识探讨

陈 龙　教授

重庆邮电大学 网络空间安全与信息法 学院

chenlong@cqupt.edu.cn

2021年 7月 · 四川 ·资阳

重庆邮电大学
两个B+ 学科 / 博士点 招生

国家布点设立并重点建设的邮电高校之一，是工业和信息化部与重庆市共建的一所特色鲜明、优势突出，在信息通信领域具有重要影响的高水平教学研究型大学。

个人简介

陈龙，博士，三级教授，博士生/硕士生导师。

重庆市学术技术带头人（网络空间安全学科）；
重庆市级教学团队——“网络与信息安全教学团队”带头人；
重庆市司法鉴定协会声像资料专委会主任委员；
CNAS技术评审员、电子数据司法鉴定人；
从事电子数据取证、智能安全等方向研究。

主持国家、省部级等项目10多项，获国家授权发明专利6项，出版著作（教材）6部（含参编），获重庆市科技进步一等奖1项，教学成果奖1项，获软件著作权1项。

重庆邮电大学司法鉴定中心

目前，中心具有 声像资料 类别的司法鉴定资质

包括：电子数据、声音、图像（视频）领域的数据提取、固定、发现、恢复，目标检材功能性、真实性、同一性、相似性分析，内容分析等。

提 纲

- 网络空间安全
- 教育信息化安全
- 教育信息化中的证据意识
- 教育行业安全（鉴定）案例

重庆邮电大学
CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

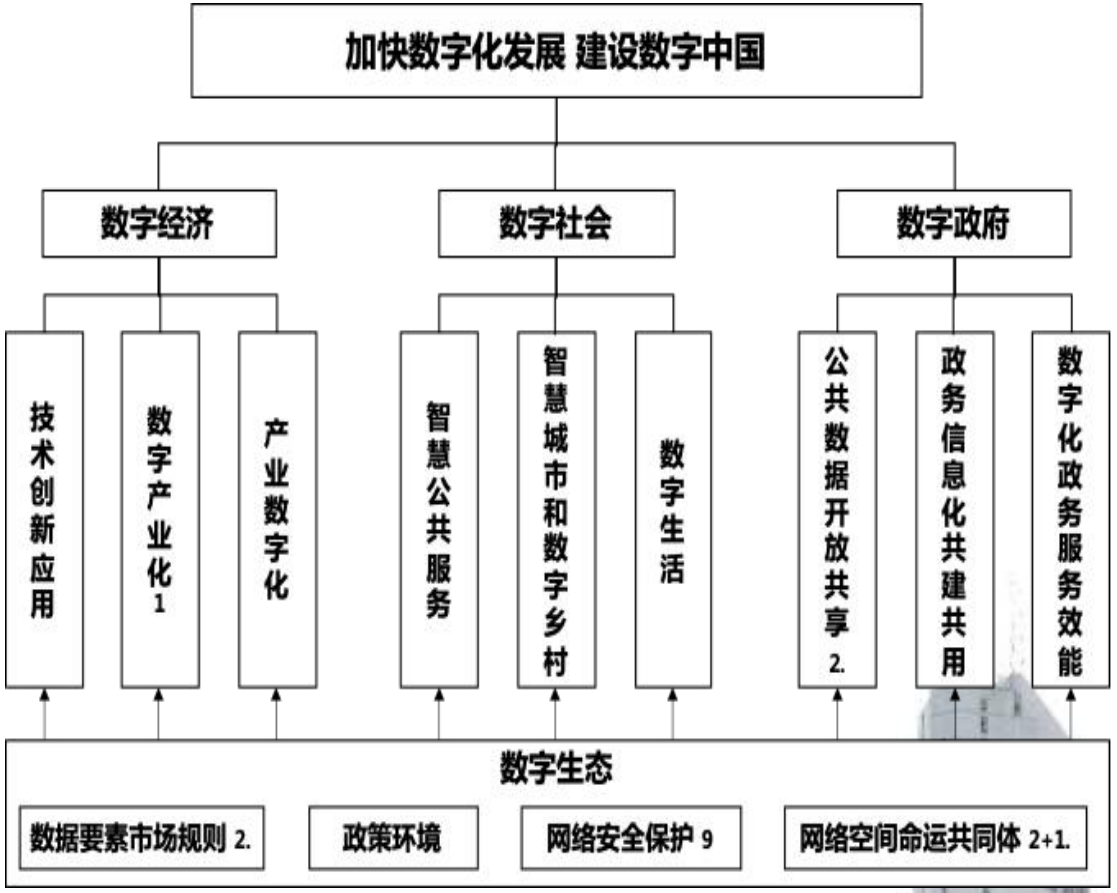
01

网络空间安全

--- 形势与需求

1.0 网络空间 -- 第五空间

- 网络空间安全 -- 国家主权
- 网络空间安全 学科设置
- 《网络安全法》
- 《网络空间安全战略》
- 《网络安全审查办法》
- 《密码法》《数据安全法》
- 《十四五规划和2035远景目标纲要》



1.1领导讲话　2018.4.23 习近平总书记
全国网信工作会议重要讲话

- 重庆日报：**构建网上网下同心圆**
  - 用新理念指导新实践，开启建设网络强国的新征程

- “没有网络安全就没有国家安全”
- “要树立正确的**网络安全观**，加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然”。

1.2 滴滴出行 等面临的安全审查

国家网信办7月4日晚间通报，经检测核实，“滴滴出行”App存在严重违法违规收集使用个人信息问题，已通知应用商店下架该APP，要求滴滴出行认真整改。

BOSS直聘、货运帮以及运满满

网络安全 有法可依！

网络安全 有法必依！ 动真格的！

1.3 教育行业 数据泄漏

今年4月，珠海网警在“净网2021”专项行动中破获一个侵犯公民个人信息的犯罪案件，抓获6名嫌疑人，查获泄露的中小学生个人信息10万余条。经警方调查，涉案的教育培训公司是通过一家维护“校讯通”系统的信息技术有限公司获得数据的，警方继而对该“校讯通”系统维护公司泄露数据的行为展开了深入调查。

今年5月，某大学两位学生的不雅视频在网络广泛传播，引起社会各界的高度关注。学生行为由校规、校纪度量.....；视频泄露事件、一系列安全环节更值得关注。

1.4 学生成绩修改案例

早前，普渡大学的一学生通过盗取教授校园网账号密码给自己修改成绩，未被发现，甚至于以优秀学生在普渡大学毕业。其最终因为教授发现账号出问题而被查处，最后该学生获刑4年。

2017年底，某学院软件工程专业大四学生周某某，因五门考试挂科，担心考试成绩影响毕业，遂通过技术手段获取老师的工作账号及密码，入侵学校的教务管理系统，并修改自己的成绩为合格。.....给予该生留校察看处分...。

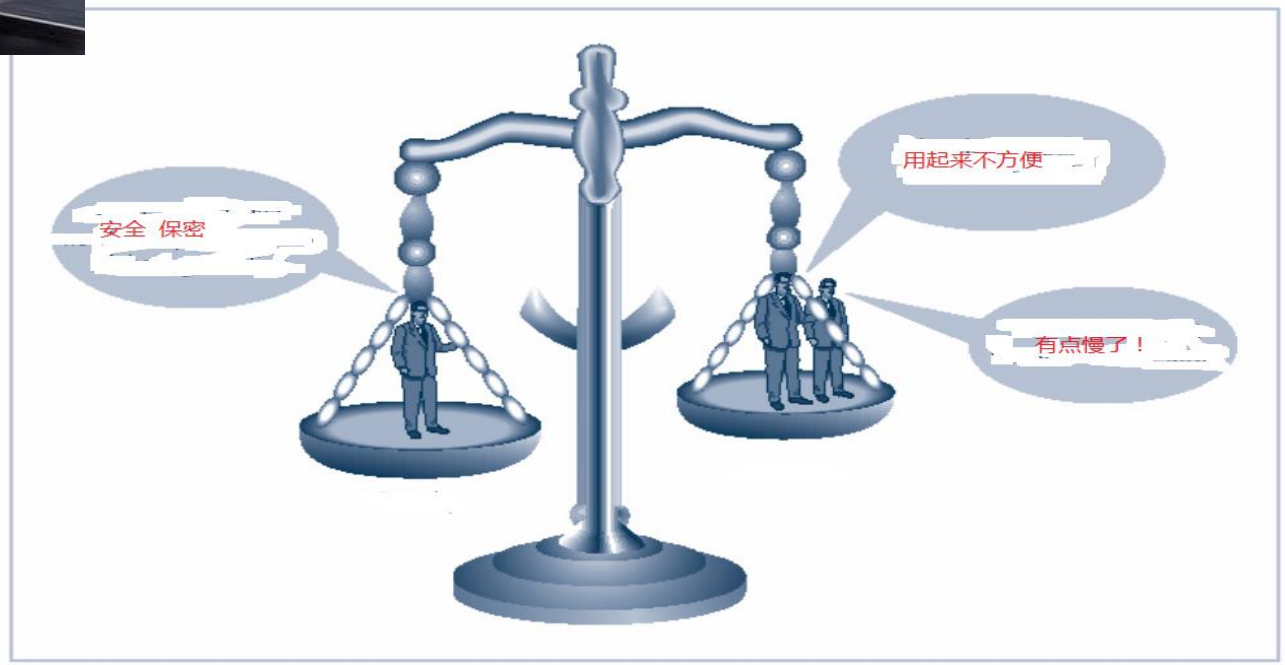
1.5 回归/回顾 信息安全属性

- 对信息的**保密性**、**完整性**和**可用性**的保持。
  - 不可否认性+可控性

Confidentiality
Integrity
Availability

1.6 网络安全与信息化发展需求

- 数字化
- 赋能 （全域)
- 智慧化 教育、校园
- 安全机制 -- 平衡



02 教育信息化安全

——体系化安全
细粒度访问控制
大数据与隐私
可证明安全
零信任安全

2.1a 体系化安全

- 安全木桶理论

  安全短板！

安全链条？

弱口令 （密码）
始终存在

个别人士多半存在

2.1b 新木桶理论

“安全”短板理论——→长板理论（优势）

→杨义先老师的新木桶理论

系统观、系统论、体系化

2.2 教育信息化 -- 新技术与安全

内生安全：

安全性分析、功能脆弱性

赋能 应用便利性

攻击 ？

防御 ？

衍生安全

争议/证据

2.3 细粒度访问控制

- 某高校财务/劳务发放系统

  ---- 可查询专家/教工 详细财务信息

用户共享教工信息

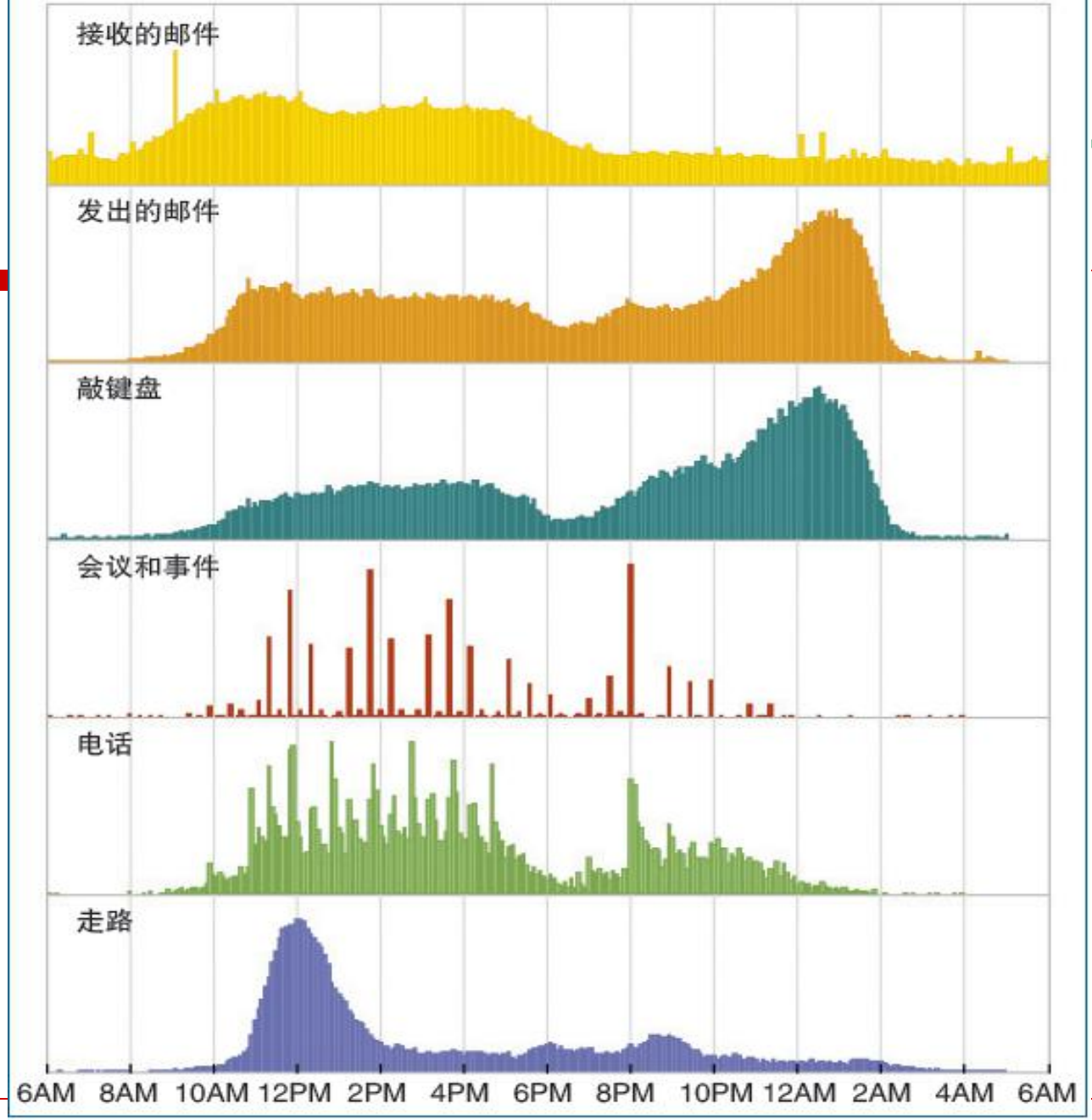
用户共享专家信息 --> 不共享

个别人士

2.4 校园 大数据分析与隐私

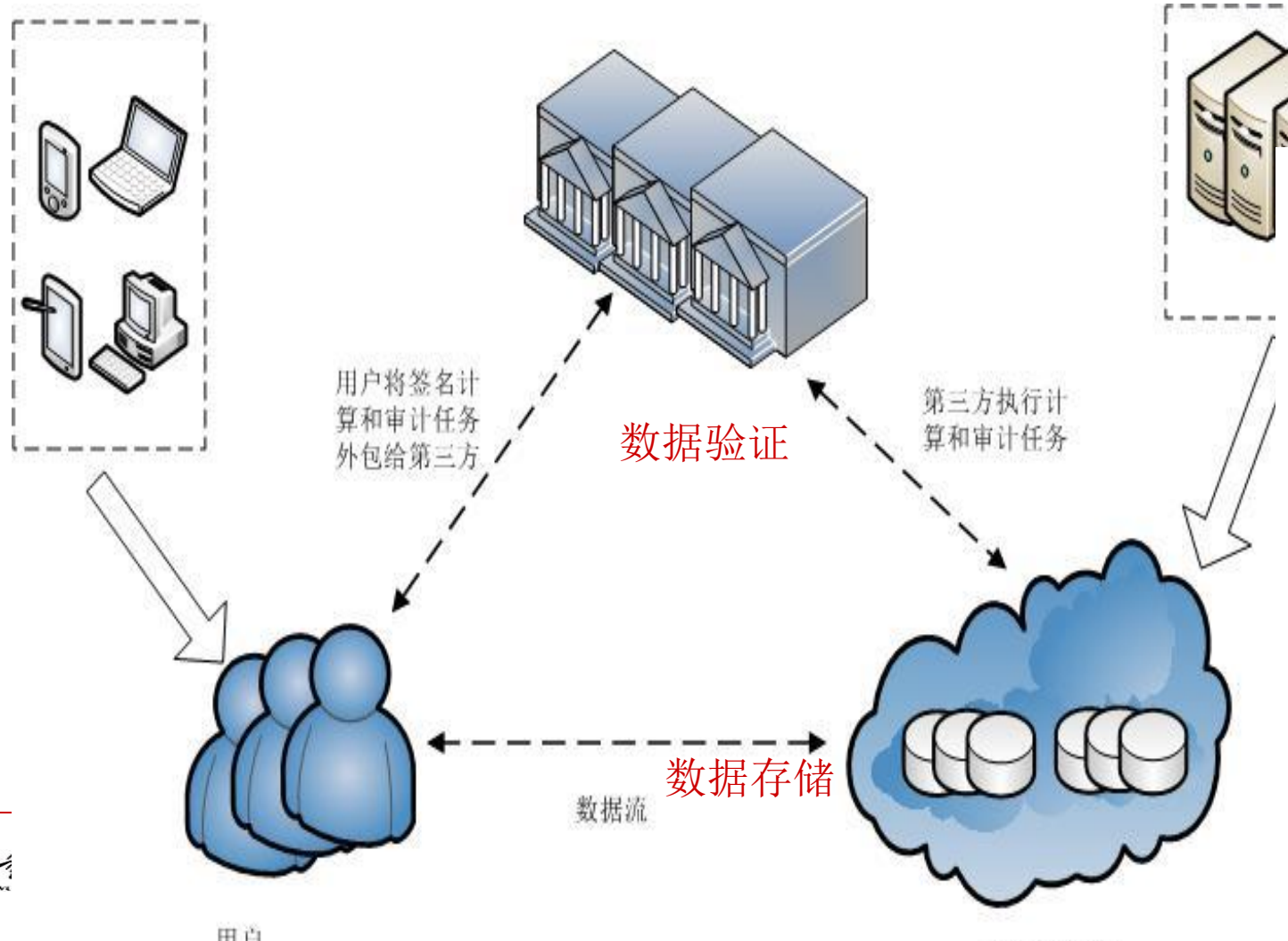
个人行为分析 示例

抽象数据



2.5 存储数据安全——可证明安全

□ 服务器存储 数据可验证



验证方法

应用性、安全性需求：

数据安全（完整性）有保障

隐私保护

容错处理（备份、纠错码）

2.6 零信任安全 -- 理念、方法、证据

不信任

1. 以资源（数据、设备、服务）保护为中心

2. 以身份（人、设备、应用、API等）为基础支撑

3. 以上下文、情报、信任评估、策略等为数据驱动

4. 以智能算法、大数据为催化剂和生产力

重庆邮电大学
CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

03

教育信息化中的证据意识

——取证、法规

应急响应

内部调查

案例： 家居管理APP 妙用

- S女士怀疑家里有外人，其与丈夫的关系可疑
- S女士计划出差一个月，丈夫嘱咐让她照顾好自己
- 出差的时间里，S女士不时地看手机 .....
- 终于在一个周末的晚上，她收到了一条消息，也正是这条消息确认了自己的猜测.....
- S女士在出差前买了一个电子体重计，这个体重计可以连接网络，体重计称重的数字会发到手机上。
- 这天她就收到的体重信息：55公斤
- 谁的体重？周末晚上，不是***，不是^^^，那么真相只有一个.....

电子数据　证据意识/要求

- 合法性、关联性、真实性

- 法庭 证据运用的经验法则
  - 综合评判

3.2 法规 -- 证据留存义务

- 第二十一条　国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：
- （一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；
- （二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的**技术措施**；
- （三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定**留存**相关的网络日志不少于**六个月**；
- （四）采取**数据分类、重要数据备份和加密**等措施；
- （五）法律、行政法规规定的其他义务。

案例：

重庆一网络公司未留存用户登录日志被网安查处

- 重庆公安局网安总队在日常检查中发现，重庆市某科技发展有限公司自《网络安全法》正式实施以来，在提供互联网数据中心服务时，存在未依法留存用户登录相关网络日志的违法行为。公安机关根据《网络安全法》相关规定，决定给予该公司警告处罚，并责令限期15日内进行整改。
- 执法机构：重庆公安局网安总队
- 处罚行为：未依法留存用户登录相关网络日志
- 处罚措施：警告并责令其改正
- 法律依据：《网络安全法》第21、第59条

3.3 网络运行安全--应急预案

- 网络安全法 第二十五条
- 网络运营者应当制定**网络安全事件应急预案**，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的**补救措施**，并按照规定向有关主管部门报告。
- 数据安全法 第二十三条
- 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

3.4 网络安全法 供应链安全--服务

- 第三十五条
- 关键信息基础设施的运营者采购网络产品和服务，可能影响**国家安全**的，应当通过国家网信部门会同国务院有关部门组织的**国家安全审查**。
- 第三十六条
- 关键信息基础设施的运营者**采购网络产品和服务**，应当按照规定与提供者签订**安全保密**协议，明确安全和保密义务与责任。

3.5 技术协助义务--取证支持

- 网络安全法 第二十八条
- 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。
- 数据安全法 第四十八条
- 违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

3.6 安全 管理义务

- 《刑法》 第二百八十六条之一 【拒不履行信息网络安全管理义务罪】网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金。
- 数据安全法 第四十五条 开展数据处理活动的组织、个人不履行****规定的数据安全保护义务的，***
- 数据安全法 第四十九条

国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。

3.6 案例：南京某研究院等网络运营单位不履行网络安全保护义务案

- 一、案件基本情况
- 南京某研究院、无锡某图书馆因安全责任意识淡薄、网络安全等级保护制度落实不到位、管理制度和技术防护措施严重缺失，导致网站遭受攻击破坏。
- 二、处理情况
- 南京、无锡警方依据《网络安全法》第21条、第59条规定，对上述单位分别予以5万元罚款，对相关责任人予以5千元、2万元不等罚款，同时责令限期整改安全隐患，落实网络安全等级保护制度。

04

教育行业安全（鉴定）案例

电子数据取证 运用广泛 --> 内部调查

- 公安行业
- 行政执法
- 政府部门
- 企事业单位
- 学校 （多个相关职能部门）

4.2 电子数据鉴定

➢ 电子数据存在性鉴定：

包括电子数据的提取、固定与恢复及电子数据的形成与关联分析。其中电子数据的提取、固定与恢复包括对存储介质（硬盘、光盘、优盘、磁带、存储卡、存储芯片等）和电子设备（手机、平板电脑、可穿戴设备、考勤机、车载系统等）中电子数据的提取、固定与恢复，以及对公开发布的或经所有权人授权的网络数据的提取和固定；电子数据的形成与关联分析包括对计算机信息系统的数据生成、用户操作、内容关联等进行分析。

电子数据鉴定

- **电子数据真实性鉴定：**

包括对特定形式的电子数据，如电子邮件、即时通信、电子文档、数据库数据等的真实性或修改情况进行鉴定；依据相应验证算法对特定形式的电子签章，如电子签名、电子印章等进行验证。

电子数据鉴定

- **电子数据功能性鉴定：**

  包括对软件、**电子设备**、计算机信息系统和破坏性程序的功能进行鉴定。

- **电子数据相似性鉴定：**

  包括对软件（含代码）、数据库、电子文档等的相似程度进行鉴定；对集成电路布图设计的相似程度进行鉴定。

4.3 案例：某机构投标标书相似性案件——电子文档相似性鉴定

- **委托人陈述：**

  评标组认为标书有相似，怀疑A、B、C三家公司串标，委托对标书文档进行相似性鉴定。

- **鉴定分析**

  1） 目标 目录结构、命名方式分析

  2）目标 文件属性对比分析

  3）目标文件 特殊标识性信息分析

检验结果表明： A公司U盘中存在一个其他文件含有B公司信息；

- 部分标书文档有一定相似性，不足以判定实质相似；
- 三份表格文档同一时间修改完成！

结 论

- 教育信息化与安全，大有可为！任重道远！
- 信息系统生命周期、数据生命周期

  ——伴随证据意识

  ——保密、公正、公开、平衡
- 团队技术能力建设与专业化服务 平衡

重庆邮电大学
CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS

致谢！

- 电子数据鉴定咨询
- 司法鉴定意见书解析
- 电子数据证据运用
- CNAS认可评审

陈龙　电话：13648443661　Email：chenlong@cqupt.edu.cn