第三章课后作业及答案

3.1 数据隐私及安全

1. 案例分析：某电商平台未加密用户数据被攻击，违反哪些安全原则？

（1）保密性：

未加密用户数据直接暴露敏感信息（如姓名、手机号、地址等），导致攻击者可直接获取数据，严重违反“数据应仅对授权用户可见”的保密性原则。

（2）数据最小化原则

平台可能存储了超出必要范围的用户数据（如过度收集个人信息），增加了数据泄露后的风险敞口。

（3）纵深防御

未通过加密构建多层防护，仅依赖单一安全措施（如防火墙），导致攻击者突破后可直接获取明文数据。

（4）合规性原则

违反《个人信息保护法》《数据安全法》等法规要求（如未履行加密义务、未通过安全评估），可能面临法律追责。

（5）责任原则

建立数据泄露后的追溯与问责机制，未能证明已采取合理技术措施保护数据。

2. 模拟练习：用记事本对手机号“13812341234”做脱敏处理。

步骤说明（以保留前 3 位和后 4 位为例,展示其中三种方式）：

打开记事本，输入原始手机号：13812341234 手动替换中间 4 位为****，

结果为：138****1234

其他常见脱敏方式：

随机替换：138***41234（保留部分真实信息，其余随机填充）

哈希处理（需编程实现）：对手机号哈希后存储（如 MD5/SHA-256），但需结合盐值防止逆向破解。

3. 辩论：数据共享是否必然侵害隐私？如何兼顾两者？

班级自行开展组织。

3.2 技术应用的可持续发展

1. 物联网如何帮助节能环保？请结合实际案例说明。

物联网（IoT）通过设备互联、数据采集与智能分析，在节能环保领域发挥关键作用。以下是具体应用场景及案例：

（1）智能能源管理

案例：西门子智能楼宇系统 西门子通过物联网传感器实时监测建筑内的温湿度、光照、人流量等数据，动态调节空调、照明和电梯运行。例如，德国慕尼黑某办公楼部署该系统后，能耗降低 30%，碳排放减少 25%。

原理：通过预测性维护避免能源浪费，结合机器学习优化设备运行策略。

（2）工业节能优化

案例：海尔卡奥斯工业互联网平台 在中国，海尔利用物联网技术对工厂生产线进行实时监控，通过分析设备运行数据识别能耗异常。某家电工厂实施后，年节电约 120 万千瓦时，相当于减少 960 吨二氧化碳排放。

原理：边缘计算与云计算协同，实现秒级能耗异常检测。

（3）智慧农业节水

案例：以色列 Netafim 智能灌溉系统 通过土壤湿度传感器和气象数据，物联网精准控制灌溉量与时间。加州葡萄园采用该系统后，用水量减少 40%，同时提高作物产量 20%。

原理：结合 AI 预测模型，避免过度灌溉导致的资源浪费。

2. 如何设计一款适合老年人的智能健康设备？

需围绕“易用性、安全性、健康监测、社交连接”四大核心需求设计.

（1）硬件设计

（2）软件功能

（3）服务生态

（4）社区互助

3. 若不同国家对数据安全要求不一，会产生哪些问题？如何解决？

（1）核心问题

合规成本激增：跨国企业需为欧盟、中国、美国等市场建立独立数据存储与处理系统，开发成本增加 40%-60%（参考 IBM 研究）。

数据流动受阻：GDPR 禁止向未通过“充分性认定”国家传输数据，导致全球数据共享效率下降 30%（欧盟委员会数据）。

法律风险：违反《数据安全法》的中国企业可能面临年营收5%的罚款，欧盟则高达4%或2000万欧元。

（2）解决方案

技术层面：

数据匿名化：采用差分隐私技术（如苹果iOS系统），使数据无法追溯至个人。

联邦学习：模型训练在本地设备完成，仅共享加密后的参数（如谷歌Gboard输入法）。

制度层面：

认证互认：推动APEC跨境隐私规则（CBPR）与GDPR互认，减少重复审核。

数据信托:由第三方机构托管数据使用权,平衡商业需求与隐私保护(如英国MyData模式）。

法律层面：

标准合同条款（SCC）：欧盟已更新SCC模板，企业签署后可合法跨境传输数据。

本地化存储+全球治理:如TikTok在美国建立数据安全中心,同时接受第三方审计。

（3）行业实践

医疗领域：飞利浦HealthSuite平台采用“数据不动、模型动”策略，AI模型在各国数据中心本地化训练。

金融领域：SWIFT支付系统通过Tokenization技术，将卡号替换为随机令牌，满足PCI DSS与GDPR双重标准。

3.3 辩论活动

1. 请绘制一份属于你自己的“数据使用地图”，列出日常生活中你在哪些平台或设备上留下了哪些数据，它们可能被谁收集？是否安全？

举例说明：

平台/设备	收集的数据类型	收集方/潜在接收方	安全性评估
微信	昵称、手机号、设备信息、位置、朋友圈内容、步数、声纹等	腾讯公司及第三方服务提供方（需用户授权）	数据加密存储,用户可删除,但法律授权下可能共享（如犯罪调查）
支付宝	支付信息、银行账户、交易记录	蚂蚁金服及合作金融机构,受金融监管部门监督	金融级加密,但用户增长带来的监管挑战增

			加

2. 模拟设计一款“环保又安全”的智能家居产品。你会如何兼顾技术功能与隐私保护？

案例：节能家居监控系统

核心功能：

智能能源管理：通过 AI 学习用户习惯，自动调节家电能耗（如空调、照明），减少浪费。

太阳能集成：支持屋顶太阳能板供电，多余电量存入家庭储能电池。 水质监测：实时检测自来水质量，过滤杂质并提醒更换滤芯。

垃圾分类助手：通过摄像头识别垃圾类型，指导用户正确分类。

隐私保护设计：

本地数据处理：所有用户数据（如能耗模式、使用习惯）在本地设备处理，不上传云端。

差分隐私技术：若需共享数据至第三方（如能源公司），添加随机噪声保护个体隐私。

物理隐私开关：摄像头、麦克风配备物理关闭按钮，LED 指示灯提示工作状态。

区块链日志：所有设备操作记录在区块链上，用户可追溯数据访问历史。

环保材料：

外壳采用回收塑料与竹纤维复合材料，减少碳排放。 包装使用可降解材料，内置可拆卸电池方便回收。

3. 观看一个关于未来城市或 AI 发展的短视频或纪录片，记录你认为其中涉及的伦理问题。

要点：

引言:简要介绍视频/纪录片名称、核心主题（如智慧城市、AI 医疗、自动驾驶等）。

提出观察视角：技术发展与伦理冲突的平衡点。

核心伦理问题梳理

数据滥用与监控

就业剥夺与社会分化

现实映射与反思

结论

4. 课堂小调查：问 10 位同学“你最担心哪种信息被泄露？”，统计结果并讨论原因。

以下为调研提纲，逻辑合理即可。

调查目的：了解同学对个人信息泄露的担忧程度及类型偏好；探讨担忧背后的原因（如隐私意识、社会新闻影响等）。

调查设计

问题

数据收集与统计：在课堂上发放问卷，或通过口头提问记录答案。 统计各选项票数，整理开放式回答的共性原因。

结果分析

数据可视化：用柱状图展示各信息类型的担忧比例。

原因归类：财产安全：银行账户、身份证号。

隐私侵犯：聊天记录、健康数据。

现实安全：家庭住址、手机号。

讨论点： 为何健康数据担忧度低？是否因医疗信息化普及不足？00 后对聊天记录的担忧是否高于其他群体？

结论与建议：总结主要担忧类型及其社会心理背景。

提出个人防护建议（如开启应用加密、定期修改密码）；呼吁加强隐私教育，推动企业透明化数据使用政策。