**Data Protection from an International Perspective**

**1. 隐私的法律概念**

**Legal Concepts of Privacy**

* **隐私作为不干扰的权利**  
  **Privacy as the Right to Be Let Alone**  
  隐私的早期定义由 Warren 和 Brandeis 在 1890 年提出，即个人拥有“被独自留下”的权利。这种观点强调隐私是一种个人免受干扰的自由。  
  *The early definition of privacy was proposed by Warren and Brandeis in 1890, asserting that individuals have "the right to be let alone." This perspective emphasizes privacy as a personal freedom from interference.*
* **隐私作为信息控制权**  
  **Privacy as Informational Control**  
  根据 Westin 的定义，隐私是个体对何时、如何以及在多大程度上向他人披露信息的控制权。  
  *According to Westin's definition, privacy is the individual's ability to control when, how, and to what extent information about themselves is disclosed to others.*
* **隐私作为财产权**  
  **Privacy as Property**  
  现代隐私权有时被视为一种财产权，个人数据被看作一种可交易的资产。然而，这一观点遭到批评，因为隐私被认为是不可剥夺的基本人权。  
  *Modern privacy rights are sometimes regarded as a form of property, where personal data is viewed as a tradable asset. However, this perspective has been criticized because privacy is considered an inalienable fundamental human right.*

**2. 隐私与数据保护的关系**

**Relationship Between Privacy and Data Protection**

隐私是个人信息不被他人干扰或滥用的权利，而数据保护则是通过技术和法律手段来保护个人信息安全。这两者相辅相成，数据保护可以视为隐私的技术实现。  
*Privacy is the right of individuals to have their personal information protected from interference or misuse, while data protection is the application of technical and legal measures to safeguard personal data. These two are complementary, with data protection serving as a technical implementation of privacy.*

**3. 欧盟隐私法（GDPR）**

**个人数据的定义**

根据 GDPR，**个人数据**是指与已识别或可识别的自然人相关的任何信息（第4条第1款）。这包括：

* 姓名和地址
* 电子邮件地址（如 name.surname@company.com）
* 身份证号码
* 位置数据（如手机的定位功能）
* IP 地址
* Cookie 标识符
* 手机的广告标识符
* 医院或医生保存的健康信息

**原文（第4条第1款）：**  
*"‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."*

**敏感数据**

GDPR 第9条将以下数据定义为敏感数据：

* 种族或民族信息
* 政治观点
* 宗教或哲学信仰
* 工会会员资格
* 健康数据
* 性取向
* 遗传和生物识别数据（用于唯一识别个人）

**原文（第9条第1款）：**  
*"Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited."*

**数据处理的原则**

GDPR 第5条详细规定了数据处理的核心原则：

1. **合法性、公正性和透明性**  
   数据必须以合法、公正和透明的方式处理。  
   **原文（第5条第1款(a)）：**  
   *"Processed lawfully, fairly and in a transparent manner in relation to the data subject."*
2. **目的限制**  
   个人数据只能用于特定、明确和合法的目的，不得进一步处理与这些目的不相符的数据。  
   **原文（第5条第1款(b)）：**  
   *"Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."*
3. **数据最小化**  
   仅收集处理目的所需的数据。  
   **原文（第5条第1款(c)）：**  
   *"Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."*
4. **数据安全**  
   数据必须通过适当的技术或组织措施保护，以防止未经授权的访问、丢失或损坏。  
   **原文（第5条第1款(f)）：**  
   *"Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."*

**数据主体的权利**

GDPR 为数据主体提供以下关键权利：

1. **被遗忘权（第17条）**  
   数据主体有权要求数据控制者删除其个人数据。  
   **原文（第17条第1款）：**  
   *"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay."*
2. **数据可携权（第20条）**  
   数据主体有权将其数据传输至另一控制者。  
   **原文（第20条第1款）：**  
   *"The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format."*
3. **拒绝自动化决策的权利（第22条）**  
   数据主体有权不受完全基于自动化处理（如算法或人工智能）的决策影响。  
   **原文（第22条第1款）：**  
   *"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."*

**数据控制者与处理者**

* **数据控制者（Data Controller）**：决定数据处理的目的和方式。  
  **原文（第4条第7款）：**  
  *"‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."*
* **数据处理者（Data Processor）**：代表控制者处理数据。  
  **原文（第4条第8款）：**  
  *"‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller."*

**4. 数据传输和法律依据**

**充分性要求（Adequacy Requirement）**

GDPR 第45条规定，只有在欧盟委员会认为第三国的数据保护水平“足够”时，才允许向该国传输个人数据。

**原文（第45条第1款）：**  
*"A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection."*

**保障措施**

若第三国无充分性决定，数据传输需使用以下保障措施之一：

1. **标准合同条款（Standard Contractual Clauses, SCC）**
2. **企业约束规则（Binding Corporate Rules, BCR）**

**原文（第46条第1款）：**  
*"In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards."*

**豁免（Derogations）**

在某些特殊情况下，GDPR 允许在无充分性决定或保障措施的情况下进行数据传输，如数据主体明确同意（第49条）。

**原文（第49条第1款）：**  
*"In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions: (a) the data subject has explicitly consented to the proposed transfer."*

**5. 法律豁免与限制**

**豁免的适用情形**

GDPR 在某些情况下允许限制隐私权和数据保护原则，例如：

* **国家安全**
* **公共安全**
* **犯罪调查与侦查**
* **国防**

这些限制的实施需遵守必要性和比例性原则，以确保数据主体的基本权利不会被过度侵犯。

**相关法律条文（GDPR 第23条第1款）：**  
*"Union or Member State law to which the controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."*

**6. 疫情期间的数据保护问题**

**COVID-19 数据保护挑战**

在 COVID-19 大流行期间，许多涉及个人数据处理的场景引发争议，例如：

1. **对员工进行体温检测**
2. **收集健康状况、旅行史和密切接触信息**
3. **向同事或卫生当局披露感染者的身份**
4. **处理位置数据以追踪可能的病毒暴露**

GDPR 并未禁止为公共健康目的而处理这些数据，但要求：

* 所有处理活动必须**合法**、**必要**且**适当**。
* 数据处理机构应确保**透明度**并采取**信息安全措施**。

**相关法律条文（第5条第1款(f)，第32条）：**  
*"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."*

**GDPR 第9条第2款(i)：**  
*"Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare."*

**7. 执法机制**

**独立数据保护机构（Data Protection Authorities, DPAs）**

GDPR 要求欧盟每个成员国设立独立的数据保护机构，这些机构负责监督和执行 GDPR 的规定。其主要职责包括：

* 处理数据主体的投诉。
* 对违法数据处理行为进行调查。
* 对数据控制者或处理者施加处罚。

**相关法律条文：**

* **第55条：管辖权**  
  *"Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State."*
* **第56条：跨境处理的主要监管机构**  
  *"The supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor."*
* **第57条：任务**  
  *"Each supervisory authority shall: (a) monitor and enforce the application of this Regulation; (b) promote public awareness and understanding of the risks, rules, safeguards, and rights in relation to processing."*
* **第58条：权力**  
  数据保护机构具有调查、纠正和咨询的权力，包括：
  + 要求控制者或处理者提供信息。
  + 进行数据保护审计。
  + 颁布警告或处罚。
* **第59条：报告**  
  *"Each supervisory authority shall draw up an annual report on its activities."*

**8. 美国隐私法**

**缺乏全面的数据保护法**

美国没有类似欧盟《通用数据保护条例》（GDPR）的全面数据保护法。

* 在联邦层面，隐私法是分散的，针对特定行业或数据类型，例如《健康保险可携性和责任法案》（HIPAA）保护健康数据，《儿童在线隐私保护法案》（COPPA）保护儿童数据。
* 没有专门的联邦机构负责全面监督数据保护。

**行业自律模型**

美国主要依赖行业自律，公司制定隐私政策并承诺遵守。

* 联邦贸易委员会（FTC）通过《FTC法》第5条对不公平或欺骗性商业行为进行监管。如果公司未遵守其隐私承诺，FTC 可以介入并采取行动。

**与欧盟的对比**

* 美国的监管以**透明性**为重点，强调消费者应了解数据的使用方式。
* 欧盟则通过 GDPR 强制要求公司获得数据主体的明确同意，并设定严格的隐私保护标准，如数据最小化和数据主体的权利（例如被遗忘权）。

**9. 欧盟与美国数据保护冲突**

**Schrems I 案例**

背景：

* 2000 年，欧盟与美国达成“安全港协议”（Safe Harbor），允许跨大西洋传输个人数据。
* 斯诺登披露了美国国家安全局（NSA）大规模监控项目，Max Schrems 指控 Facebook 向美国传输数据违反了欧盟隐私保护要求。

**欧盟法院判决（C-362/14）：**

* 认为“安全港协议”未能提供足够的隐私保护，因为美国的国家安全例外过于宽泛。
* 2015 年，“安全港协议”被废除。

**Schrems II 案例**

背景：

* Schrems 再次挑战欧盟和美国间的“隐私盾计划”（Privacy Shield）。

**欧盟法院判决（C-311/18）：**

* 认为“隐私盾计划”不足以保护欧盟公民的数据隐私，尤其是美国监控活动不符合 GDPR 的必要性和比例性原则。
* \*\*标准合同条款（SCC）\*\*被确认仍然有效，但数据控制者需评估接受国的数据保护水平，并采取额外保障措施。

**关键影响：**

* 跨大西洋数据传输变得复杂。
* 数据控制者需确保 SCC 提供与 GDPR 等同的数据保护水平。

**10. 人工智能与隐私**

**匿名化与数据最小化原则的挑战**

AI 模型通过处理大规模数据集，可以推断出新信息，如用户的种族、健康状况或政治倾向。这使得：

* **匿名化**变得复杂：即便删除直接身份信息，AI 仍能通过数据关联重新识别个人。
* **数据最小化**难以实现：AI 训练需要大量数据，这与仅处理必要数据的原则相冲突。

**数据主体的权利挑战**

* **被遗忘权**：AI 模型基于大量数据训练，要从模型中删除特定个人数据技术上很困难。
* **数据纠正权**：AI 生成的推断数据可能不准确，但如何修改这些数据尚无明确法律框架。

**AI 相关法律的未来发展**

* 可能需要设计新的法律框架以适应 AI 的特殊性。
* 立法者可能需探索：
  + 透明化算法决策。
  + 加强数据可追溯性和数据删除机制。
  + 解决因 AI 推断数据引发的隐私争议。