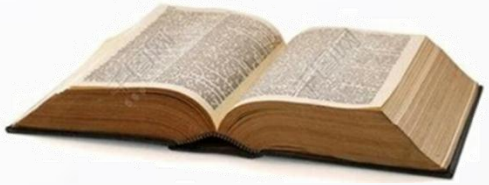
信息安全法律基础

法律遵从，科技向善

——共建网络空间安全

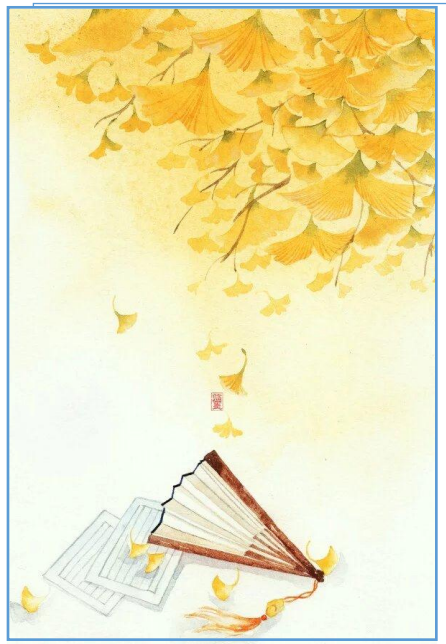


第6章 数据安全治理与法律规制

第6章 数据安全治理与法律规制

- 6.1 数据确权
- 6.2 用户大数据安全治理
- 6.3 数据安全管理与个人信息保护法律规制
- 6.4 数据保护官

第6章 数据安安全治理与法律规制



知识点探究

- 了解和学习《电信和互联网用户个人信息保护规定》、《网络安全法》《电子商务法》《数据安全管理办法（征求意见稿）》、《App违法违规收集使用个人信息行为认定方法（征求意见稿）》等相关法规，探讨数据安全、个人信息保护等方面的法律规制。
- 观看纪录片《互联网时代》第8集（忧虑），探讨互联网企业（网络平台）在大数据安全与隐私保护方面的责任和义务。
- 探讨数据确权（数据权属）、数据问责、AI伦理等问题。

6.1 数据确权

6.1 数据确权

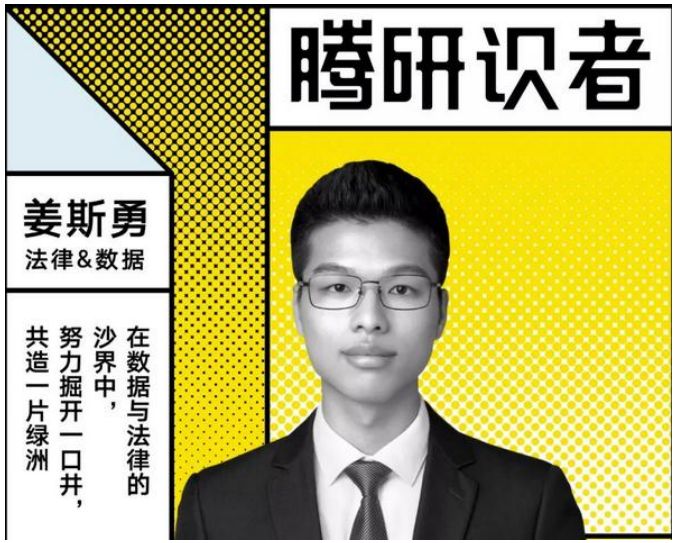
6.1.1 数据确权的现实意义

（1）数据确权已具备经济基础（数据确权收益>数据确权成本）

- 互联网企业的博弈已由流量竞争转向数据竞争。
- 数据的价值变大（数据越多，越贵），具有了财产属性，已成为生产要素。

（2）不确定的数据产权给各方在数据的开发利用环节带来了不可控的风险成本

- 不少企业不乐意将自己的数据共享给其他企业，或者选择自建数据体系，其原因在于权属不清，容易产生纠纷，或者权益被侵犯、想维权却担心无法可依。



姜斯勇，上海明庭律师事务所律师
数据产权：互联网下半场不容回避的竞争焦点

6.1 数据确权

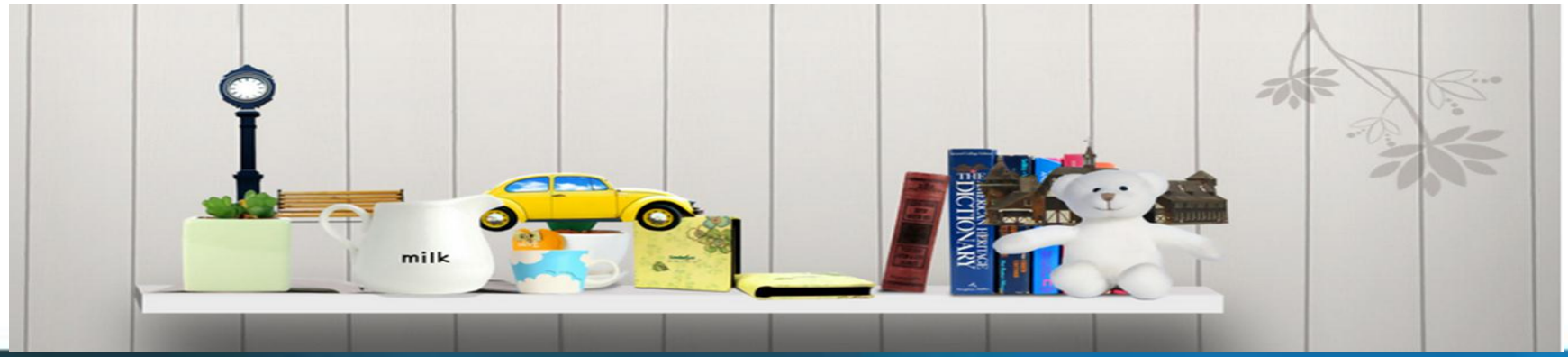
6.1.1 数据确权的现实意义

（3）通过立法确定数据产权以促进各方合作

- 通过构建法律，使私人之间由于协调失败所造成的损失达到最小（雷布斯定理）。
- 数据的收集、挖掘、开发、利用、共享、交易等环节都绕不开对数据产权的认定。

（4）从立法和司法角度，当新生事物在现有法律体系下难以找到合适制度来保护时，可以尝试用数据产权来解决

- AI生成物能否成为著作权法意义上的作品引起了极大争议。
- 将AI生成物确定为数据，进而确定其权属，不仅可以促进AI发展，也使数据问责（算法问责）有法可依。



6.1.2 数据产权及其特性

（1）数据产权

- 数据产权作为权利束（A Bundle of Rights），包含使用权、收益权、占有权、处分权、可携带权、被遗忘权等。
- 数据产权主体包含个人用户、数据收集企业、平台企业、政府机构、数据中介等组织。

（2）数据产权的特性

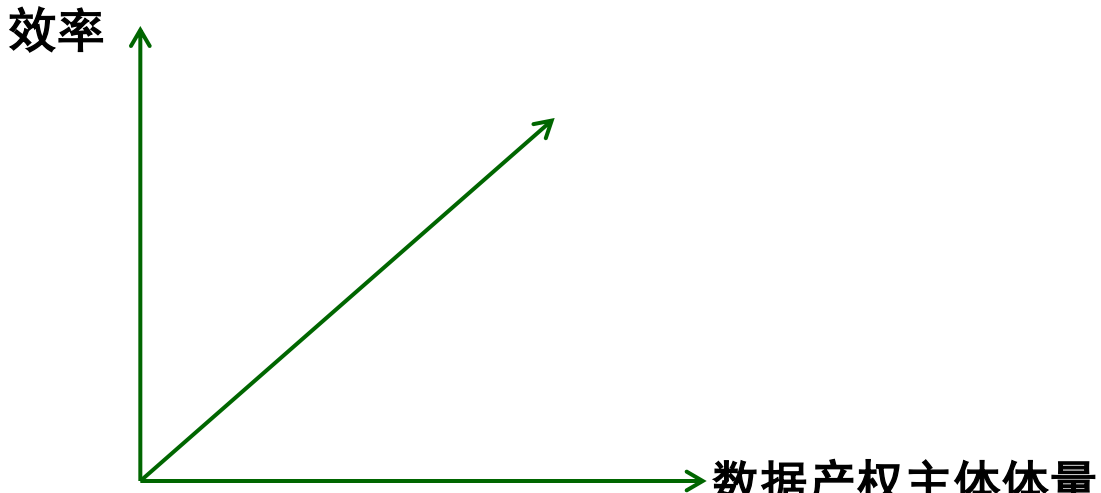
- 多主体性：很多数据可能是由多轮不同主体产生和处理。
- 潜在价值：初始数据不具有很高的直接价值，在不断挖掘和使用中体现其经济 价值和稀缺性。
- 多栖性：因为数据方便复制携带，数据可以同时存在不同的介质中。
- 隐私性：有些能够识别特定个人的数据往往具有隐私性。

6.1 数据确权

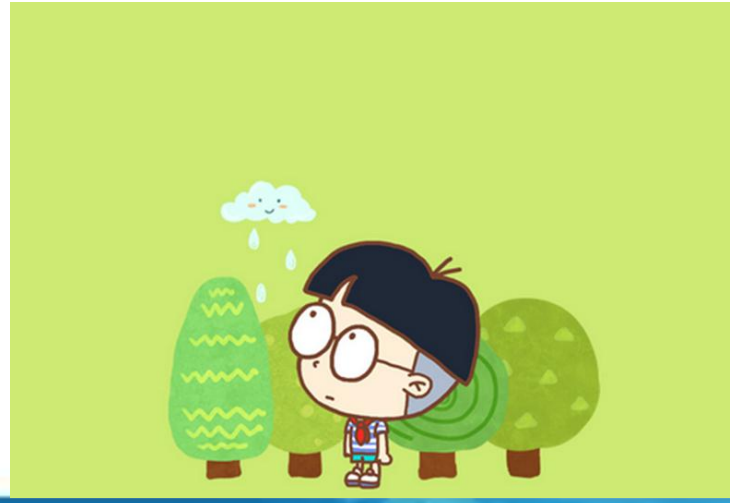
6.1.3 数据确权的多视角思考

（1）经济角度：效率优先

- 数据产权越向大体量级别的主体集中，所产生的价值越大，效率（投入产出比）也越高。
- BAT等超大型平台产生的市场价值和社会价值，是一个较好的例证。



数据产权主体体量与效率的关系



6.1 数据确权

6.1.3 数据确权的多视角思考

（2）公平角度：公正合理优先

- 谁有付出，谁拥有相关权利

数据与生产者关系

数据	数据生产者
初始数据	个人、企业、政府
聚合数据	数据企业
建模数据	平台企业

6.1 数据确权

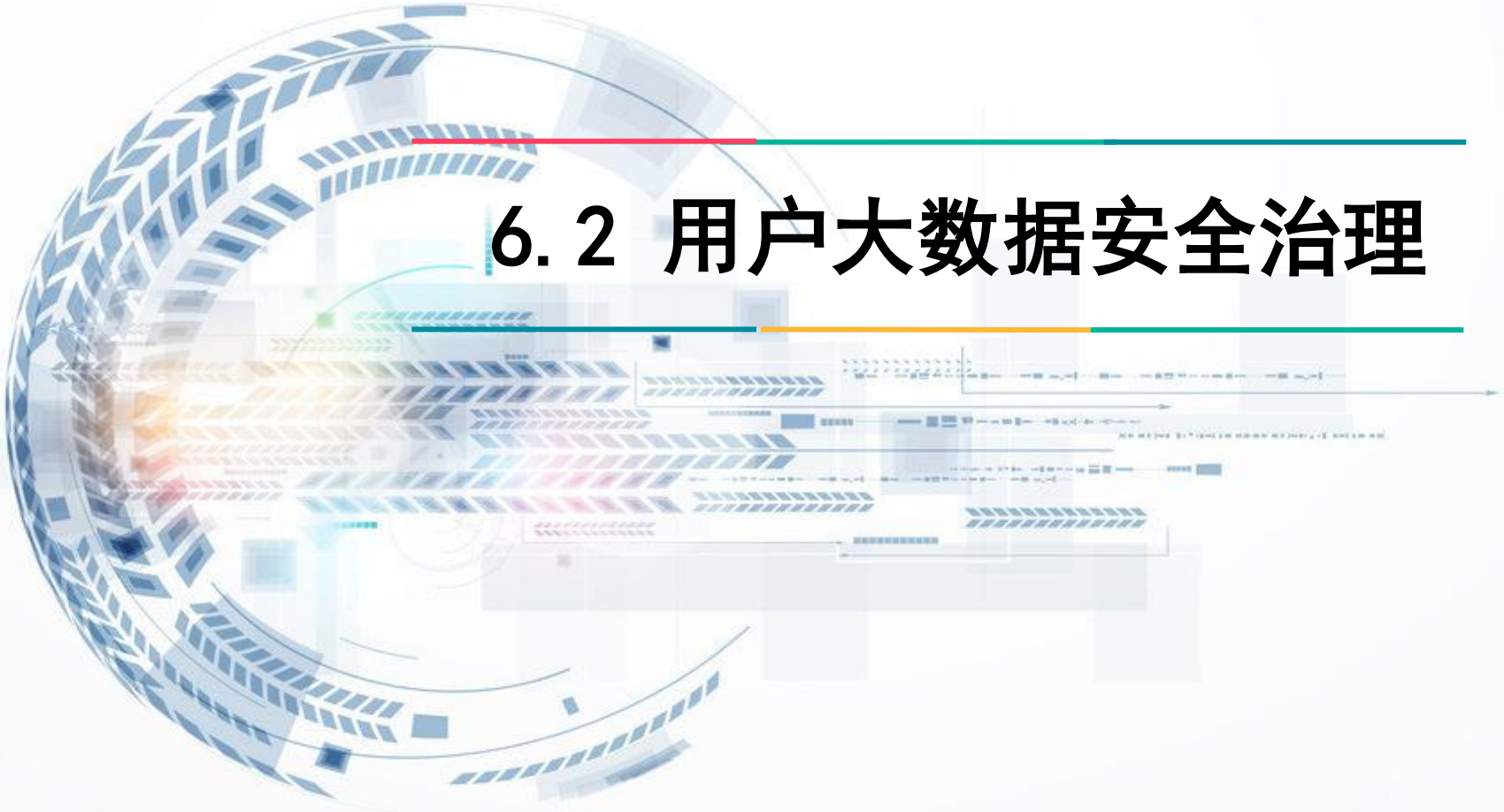
6.1.3 数据确权的多视角思考

（3）法律角度：兼顾公平与效率

数据、生产者与数据产权

数据	数据生产者	关于数据产权的探讨
初始数据	个人	• 个人隐私和敏感信息，其产权归属个人 • 脱敏处理后的衍生数据，其产权归企业
聚合数据	数据企业	
建模数据	平台企业	

《网络安全法》第四十二条规定：“网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。”

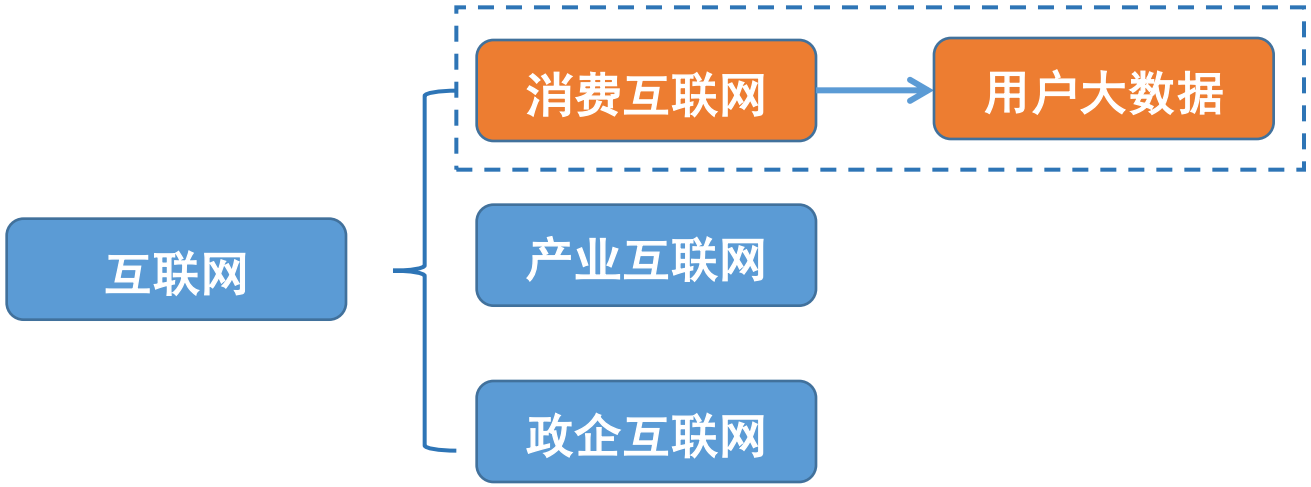


6.2 用户大数据安全治理

6.2 用户大数据安全治理

6.2.1 关于用户大数据

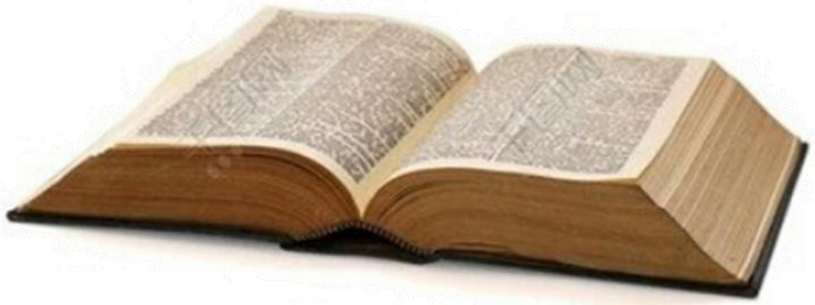
- 用户大数据是指数量非常巨大的复杂的用户数据集，包括静态数据和动态数据。
  - **静态数据**主要来源于用户填写的个人资料。
  - **动态数据**也称为用户行为大数据，是用户大数据的核心部分，主要来源于注册、浏览、点击、购买、签收、评价等用户行为所产生的数据。



6.2 用户大数据安全治理

6.2.2 确立电商平台责任主体的客观性和必要性

- 电商平台既是用户大数据的主要开发者也是最大受益者。从用户大数据的受益者和用户大数据安全治理的技术优势角度，电子商务平台经营者都是用户大数据安全治理的天然主体。
- 《电子商务法》）首次界定了电子商务平台经营者的概念，已对电子商务平台经营者设立了准入门槛，不仅要有更高的技术要求，还要承担平台的管理职责和相应的法律责任。



6.2.3 用户大数据安全治理目标

（1）有效保护用户的个人资产

- 用户大数据来源于用户，属于用户的个人资产，用户对个人数据具有完全的知情权和控制权。
- 对于用户大数据的使用者而言，数据财产权益并非是一种天赋人权，而是法定授权。
- 电子商务平台经营者作为用户大数据的主要使用者，必须在法定授权的情况下使用用户大数据，同时必须有效保护其安全。

6.2.3 用户大数据安全治理目标

（2）有效保障治理过程中权责的基本对等

- 全球领先的信息技术研究和顾问公司Gartner认为，安全和风险管理领导者应该制定适当的数据安全治理框架，避免安全风险可能给企业带来的信誉流失和经济损失。
- 电子商务平台经营者正在担当着用户大数据安全与风险管理领导者的角色，既应该承担相应的管理职责和法律责任，在合法合规的前提下，也应该拥有诸如用户大数据安全自治、参与相关技术标准制定等与其责任相适应的权利。

6.2.3 用户大数据安全治理目标

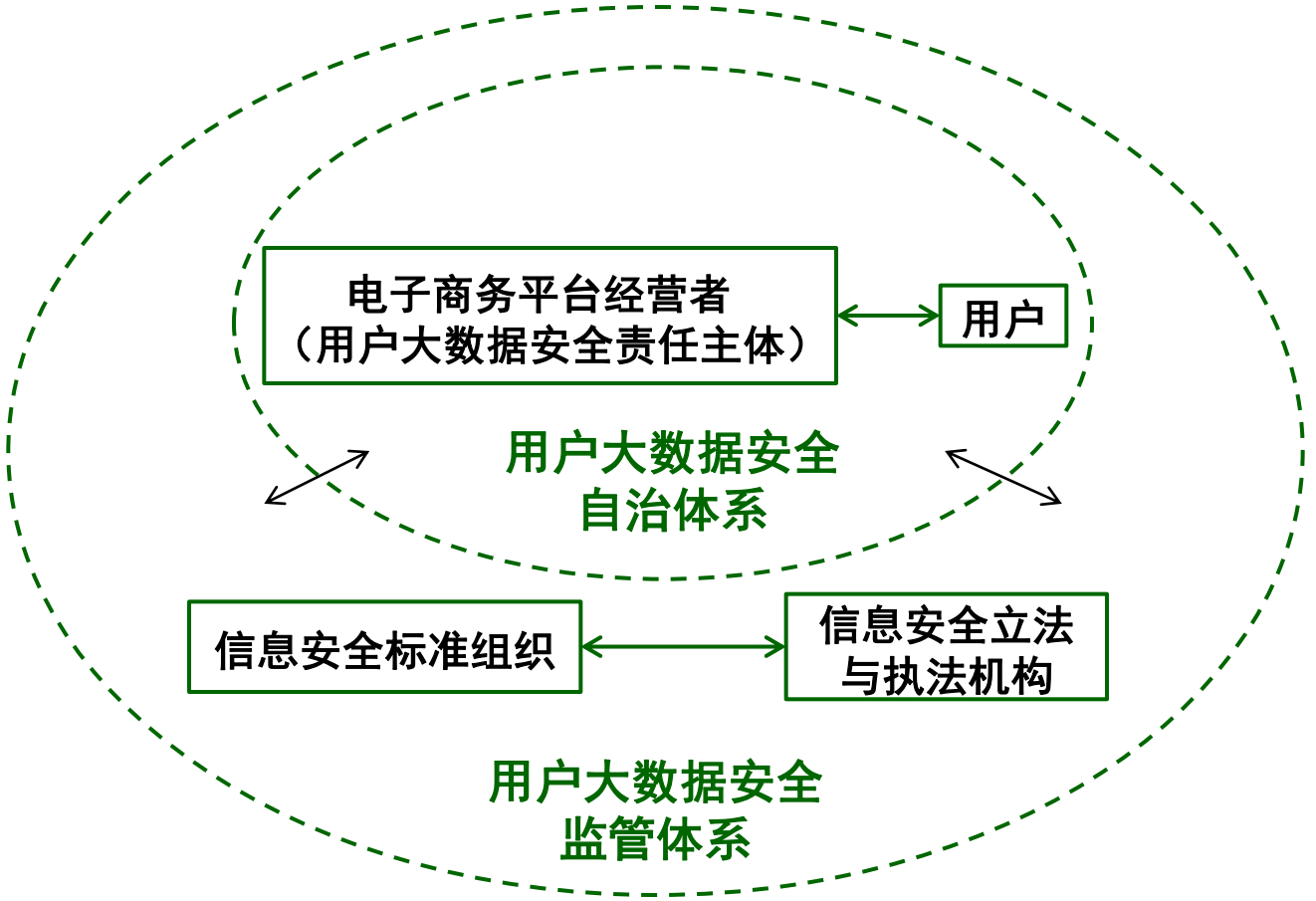
（3）有效降低治理成本、提升治理效率

- 用户大数据的安全治理是一项长期的规模浩大、动态多变的系统工程，既要在短时间内做出成效，又要长期的持续迭代，在人员素质、技术资源等方面都具有较高的要求，需要长期的大量投入和高效运作，必须考虑治理成本和效率问题。
- 电子商务平台经营者在技术方面具有天然禀赋，并且作为企业更加注重效率。

6.2 网络平台大数据治理

6.2.4 用户大数据安全综合治理体系

- 自治体系—电子商务平台经营者作为责任主体应该建立共生理念， 将顾客主义作为企业价值观，利用自身的技术优势实现自治，为用户信息安全提供有效保障。
- 监管体系—实施适度地监管也是非常必要的，并由事后的惩罚机制转变为事前的预警机制，让电子商务平台经营者在法律、制度、标准等框架下实现自我管理、创新发展。



用户大数据安全综合治理体系

6.3 数据安全管理与个人信息保护法律规制

6.3 数据安全管理与个人信息保护法律规制

6.3.1《电信和互联网用户个人信息保护规定》

- 2013年6月28日中华人民共和国工业和信息化部第2次部务会议审议通过
- 2013年7月16日中华人民共和国工业和信息化部第24号令公布
- 自2013年9月1日起施行
- 主要内容包括：
  - 第一章　总则
  - 第二章　信息收集和使用规范
  - 第三章　安全保障措施
  - 第四章　监督检查
  - 第五章　法律责任

6.3 数据安全管理与个人信息保护法律规制

6.3.1《电信和互联网用户个人信息保护规定》

第一章　总则

第四条　本规定所称用户个人信息，是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息。

第五条　电信业务经营者、互联网信息服务提供者在提供服务的过程中收集、使用用户个人信息，应当遵循合法、正当、必要的原则。

第六条　电信业务经营者、互联网信息服务提供者对其在提供服务过程中收集、使用的用户个人信息的安全负责。

第七条　国家鼓励电信和互联网行业开展用户个人信息保护自律工作。

6.3 数据安全管理与个人信息保护法律规制

6.3.1《电信和互联网用户个人信息保护规定》

第五章　法律责任

第二十二条　电信业务经营者、互联网信息服务提供者违反本规定第八条、第十二条规定的，由电信管理机构依据职权责令限期改正，予以警告，可以并处一万元以下的罚款。

第二十三条　电信业务经营者、互联网信息服务提供者违反本规定第九条至第十一条、第十三条至第十六条、第十七条第二款规定的，由电信管理机构依据职权责令限期改正，予以警告，可以并处一万元以上三万元以下的罚款，向社会公告；构成犯罪的，依法追究刑事责任。

第二十四条　电信管理机构工作人员在对用户个人信息保护工作实施监督管理的过程中玩忽职守、滥用职权、徇私舞弊的，依法给予处理；构成犯罪的，依法追究刑事责任。

6.3 数据安全管理与个人信息保护法律规制

6.3.2《数据安全管理办法（征求意见稿）》

- 国家互联网信息办公室，2019年5月28日
- 意见反馈截止时间为2019年6月28日
- 主要内容包括
  - 第一章 总 则
  - 第二章 数据收集
  - 第三章 数据处理使用
  - 第四章 数据安全监督管理
  - 第五章 附 则

6.3 数据安全管理与个人信息保护法律规制

6.3.2《数据安全管理办法（征求意见稿）》

第一章 总 则

第一条 为了维护国家安全、社会公共利益，保护公民、法人和其他组织在网络空间的合法权益，保障个人信息和重要数据安全，根据《中华人民共和国网络安全法》等法律法规，制定本办法。

第六条 网络运营者应当按照有关法律、行政法规的规定，参照国家网络安全标准，履行数据安全保护义务，建立数据安全管理责任和评价考核制度，制定数据安全计划，实施数据安全技术防护，开展数据安全风险评估，制定网络安全事件应急预案，及时处置安全事件，组织数据安全教育、培训。

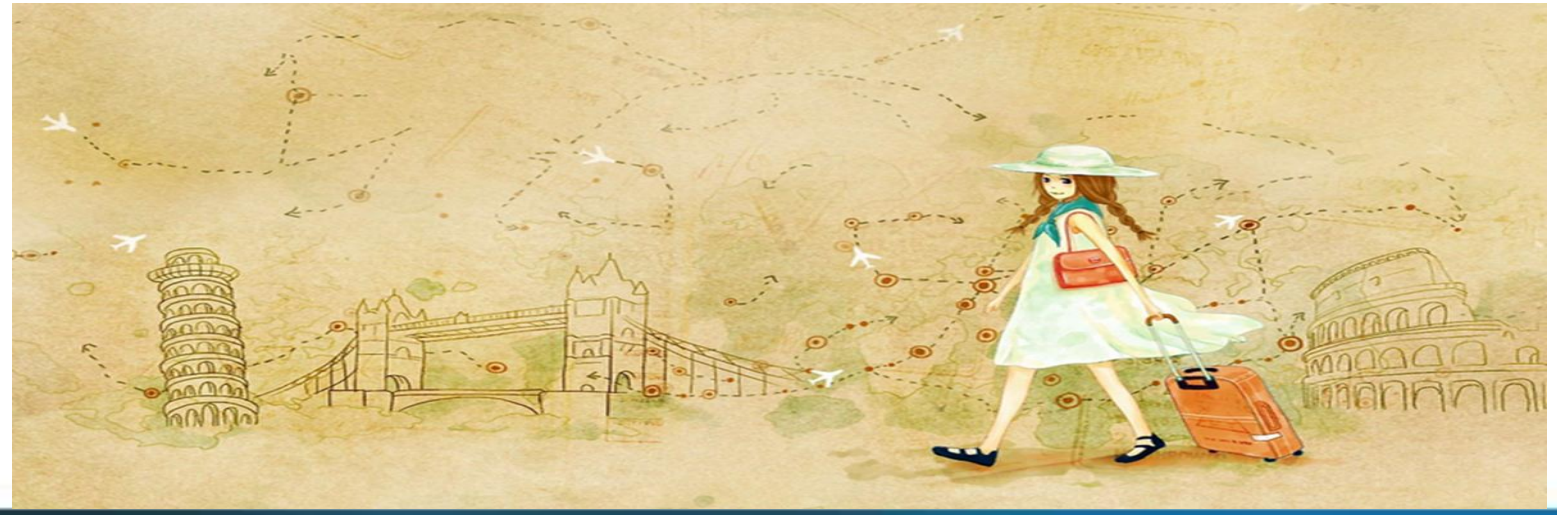
6.3 数据安全管理与个人信息保护法律规制

6.3.2《数据安全管理办法（征求意见稿）》

第二章 数据收集

第十七条 网络运营者以经营为目的收集重要数据或个人敏感信息的，应当明确数据安全责任人。

数据安全责任人由具有相关管理工作经历和数据安全专业知识的人员担任，参与有关数据活动的重要决策，直接向网络运营者的主要负责人报告工作。



6.3 数据安全管理与个人信息保护法律规制

6.3.2《数据安全管理办法（征求意见稿）》

第二章 数据收集

第十七条 网络运营者以经营为目的收集重要数据或个人敏感信息的，应当明确数据安全责任人。

数据安全责任人由具有相关管理工作经历和数据安全专业知识的人员担任，参与有关数据活动的重要决策，直接向网络运营者的主要负责人报告工作。

6.4 数据保护官

6. 4 数据保护官

6.4.1 关于数据保护官

- 数据保护官（Data Protection Officer，DPO）：一种新的岗位角色
- 欧盟《通用数据保护条例》（GDPR）（2018年5月25日生效）以法律形式明确规定DPO的任命要求和职责。
- 在我国现行法律中，虽然没有明确与DPO名称上相对应的角色，但是，GDPR中的DPO的职责与《中华人民共和国网络安全法》等法规中的网络安全负责人，在设立目的上存在相似性，都是为了个人信息保护和隐私数据合规而设立。
- 从合规的角度，对DPO的任命对于符合条件的企业是强制性要求。

6.4 数据保护官

6.4.2 DPO岗位基本能力要求

- 法律解读能力
- 基本技术能力
- 1. 数据主体权利梳理
  - 必须履行七项数据主体权利的要求，包括知情权、访问权、修正权、删除权（被遗忘权）、限制处理权（反对权）、可携带权和拒绝权（GDPR）
  - 通常会用到Data Mapping、Data flow等技术帮助更高效地完成梳理工作。
- 2. 数据保护方案设计
  - 熟知各类数据保护技术的基本技术原理，具备将不同数据保护技术合理应用及组合的能力，为不同场景设计合适的数据保护方案，确保企业隐私保护实践达到最佳效果。

6.4 数据保护官

6.4.2 DPO岗位基本能力要求

- 3. 隐私影响评估
  - 常见的评估内容有隐私影响评估（Privacy Impact Assessment，PIA）、数据保护影响评估（Data Protection Impact Assessments，DPIA）以及隐私风险评估（Privacy Risk Assessment，PRA）。
- 4. 参与产品设计和研发流程
  - 在产品设计环节尽量采取不涉及或少涉及个人数据的方式实现产品功能。
  - 将数据合规有机融入设计中，并实现全生命周期的保护。

感谢聆听