大数据存在两面性：价值与风险并存（下）

（来源：普华永道微信公众号，2021-07-21）

大数据是一把**“双刃剑”——价值与风险并存。一方面，它的价值体现在**能为企业的生产活动提供决策，公众的日常生活提供便利；**另一方面，它的风险体现在**因大数据被恶意利用，导致个人隐私的泄露事件频发，对社会秩序造成严重侵害。

【国企改革观象台】专栏将针对**大数据的价值与风险**，从国家政策和国有企业数字化转型落地两个角度，分两期探讨**国内对于数据安全及隐私保护的合规要求，和如何应对数据合规挑战、保护数据安全。**

上期文章从国家政策方面，以价值瞭望和守护安全的视角，重点探讨了国内对于数据安全及隐私保护的合规要求，**本期将继续介绍国有企业在数字化转型落地的过程中，如何应对数据合规挑战，保护数据安全。**

01 数字化转型中的国有企业，如何应对数据合规挑战？

2020 年 9 月 21 日，国资委发布《关于加快推进国有企业数字化转型工作的通知》。值得注意的是，该份文件明确要求实行数字化转型一把手负责制，管理层中明确专人分管，统筹规划、科技、信息化、流程等管控条线，优化体制机制、管控模式和组织方式，协调解决重大问题。

这意味着，国有企业数字化转型从组织架构上是自上而下推动的，伴随着数字化转型进程，国有企业的运行与管控机制也会发生一系列变化。

同时，监管部门要求，国有企业在数字化转型中应发挥引领示范和辐射带动作用，激活数据要素潜能，并切实保障数据安全。由此可见，从外部监管视角，不管企业围绕数据进行何种变革，数据安全始终是重点。普华永道建议国企从以下方面着手进行数据合规建设。

数据安全能力评估

企业应树立“知己知彼，百战不殆”的意识，通过数据安全能力评估，在合规框架实施前了解自身的数据安全管理现状，明确存在的问题以及潜在的挑战，规划数据安全能力成熟度的提升方案。

国家标准《信息安全技术 大数据安全管理指南》明确大数据安全管理的基本原则，对大数据平台提出了**保密性、完整性、可用性**方面的安全需求，具体重要原则如下：

保密性：

- 数据传输过程中使用不同的安全协议保障数据采集、分发等操作中的传输保密要求；
- 数据存储过程中使用访问控制和加密机制；
- 使用同态加密等算法进行加密数据运算；
- 通过数据隔离等机制确保汇聚大量数据时不暴露敏感信息；
- 针对个人信息采取匿名化、去标识化处理；
- 建立密钥管理系统。

完整性：

- 确保数据来自于已认证的数据源；
- 确保只对数据执行了期望的计算；
- 确保分布式存储的数据及其副本的完整性；
- 建立数据的细粒度审计机制。

可用性：

- 提升大数据平台抗攻击能力；
- 通过安全情报分析、数据驱动的误用检测、安全事件检测等手段进行风险监测；
- 提升大数据平台的容灾能力。

梳理数据资产

大数据应用合规的第一步是梳理数据资产，通过梳理数据资产，可以形成统一的数据地图，构建基于元数据的安全隐私保护框架。在过程中需要对相关元数据及其相关属性，如数据域、字段类型、表结构、逻辑存储和物理存储结构进行梳理，同时识别出其中的个人信息与重要数据，因为相比于其他类型的数据，这两类数据的合规要求更加严格。

梳理数据流转情况及系统映射

数字化转型往往会涉及数据中台的建立，以及系统间数据的交流共享与融合，而且随着多年的信息化建设，大型企业内部的系统架构及数据流转通常较为复杂，除了部门间数据流转之外，还有可能涉及集团公司与子公司之间的数据流转。梳理数据流转场景及系统映射，有助于企业管理层了解掌握数据风险。

识别适用法律法规

在数据梳理的基础上，企业应对照数据安全相关的法律法规，同步识别相关数据资产适用的合规要求，包括但不限于《网络安全法》、《数据安全法（草案）》、《个人信息保护法（草案）》、《数据安全管理办法（征求意见稿）》及大数据相关的信息安全技术国家标准等。同时，还应特别关注垂直领域的相关合规要求，例如以金融行业为例，

2018年银保监会将数据治理与监管评级挂钩后，监管要求愈发严格。

中国金融行业数据安全及隐私保护重点法规

中国人民银行：

- 《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》
- 《中国人民银行关于金融机构进一步做好客户个人金融信息保护工作的通知》
- 《金融数据安全 数据安全分级指南》（JR/T 0197—2020）
- 《金融行业态势感知与信息共享平台数据接入标准说明（试点）》
- 《金融业数据能力建设指引》

银保监会

- 《银行业金融机构数据治理指引》
- 《关于开展监管数据质量专项治理工作的通知》
- 《银行业金融机构信息科技风险监管现场检查手册》
- 《关于加强非银行金融机构信息科技建设和管理的指导意见》
- 《中国银监会办公厅关于加强网络信息安全与客户信息保护有关事项的通知》

02 国有企业如何在合规框架内，保护数据安全？

国企的数字化转型可能会涉及大数据提供方、技术服务提供方、大数据运营方、大数据需求方、大数据平台等若干种角色。基于数据全生命周期，国企在合规框架内，在**数据采集、存储、加工和应用、传输、和销毁**方面保护数据安全。

数据采集

目前，大数据采集主要有以下几种方式：

- 网络数据收集（如，通过爬虫收集公开数据）；
- 从其他方获取数据（如，获取其他组织的数据）；
- 通过机器或传感器获取（如，摄像头、GPS 等公共或个人智能设备）；
- 系统数据（如，企业信息系统、移动应用、小程序等）。

数据采集阶段，企业应关注的主要合规问题有：

- 个人信息保护
  - 企业收集、处理个人信息的，应当遵循合法、正当、必要原则；
  - 收集个人信息，应向个人信息主体告知收集、使用个人信息的目的、方式和范围等规则，并获得个人信息主体的授权同意；
  - 收集个人敏感信息、生物识别信息、未成年人的个人信息之前，需根据相关法规的要求获得个人信息主体或其监护人的明示同意。
- 不正当竞争风险

目前，以下数据抓取行为可能会涉嫌违反《反不正当竞争法》：

  - 超出协议范围的、违背行业内公认准则的，以及采取违法手段的数据抓取行为可能会涉嫌违反《反不正当竞争法》；
  - 采用技术手段抓取商业秘密数据。
- 知识产权侵权风险

以下类型的数据可能会存在知识产权侵权风险：

  - 用户制作和提供的内容（UGC），如互联网用户的原创性文章、评论等；
  - 互联网平台或平台商户创作的内容，如文字介绍、图片等。

在数据采集阶段，建议企业从以下方面保护数据安全：

- 梳理公司的业务场景，确定需收集的个人信息与使用范围；
- 按照相关法规的规定，在收集个人信息前获取用户的授权同意；
- 间接收集个人信息时，应对个人信息提供方的个人信息来源合法性进行确认，并确保业务活动不超过个人信息提供方已获得的个人信息处理的授权同意范围；
- 确保收集的其他数据类型不会引起不正当竞争或知识产权侵权的风险。

数据存储

在数据存储过程中，企业应当关注数据分类分级与数据存储期限的要求。

- 数据分类分级

《网络安全法》第二十一条明确要求网络运营者采取数据分类、重要数据备份和加密等措施，《个人信息保护法（草案）》也要求对个人信息实行分级分类管理。企业应关注相关法规的要求，对数据进行分类分级，尤其关注与国家安全、经济发展以及公共利益密切相关的重要数据，以及个人信息。

- 数据存储期限

企业应当关注个人信息存储期限的合规要求，个人信息存储期限应为实现个人信息主体授权使用的目的所必需的最短时间，超出存储期限后，应对个人信息进行删除或匿名化处理。

在数据存储过程中，建议企业采取以下措施保护数据安全：

- 对数据进行分类分级，将不同类别和级别的数据分开存储，并采取物理或逻辑隔离机制；
- 关键信息基础设施运营者应按照相关法规贯彻数据本地化存储的

要求；

- 根据国家法律法规，并结合自身行业监管要求，明确不同类型数据的存储期限；
- 采用技术手段和其他必要手段确保存储安全；
- 建立数据存储冗余策略和管理制度，及数据备份与恢复操作过程规范；
- 按照网络安全等级保护制度的要求，履行网络安全保护义务。

数据加工和应用

大数据加工和应用，同时会伴随着数据存储、传输，是大数据生命周期中最复杂的阶段，而且大数据应用可能涉及自用、他用（共享）、数据交易等多种模式。

大数据加工及应用过程中除关注数据存储、传输等阶段的合规要求外，还应关注以下方面风险：

- 数据使用范围与授权或合同约定的一致性；
- 数据使用中的技术风险，如数据脱敏、个人信息去标识化措施的有效性。

在大数据应用过程中，建议企业采取以下措施保护数据安全：

- 涉及个人信息使用的，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围；
- 涉及通过界面展示个人信息的，应通过去标识化处理等措施降低泄露风险；
- 建立最小授权的访问控制策略；
- 采取技术措施对数据进行加密、脱敏等处理，并对其效果进行评估；

- 若存在数据委托处理、共享、转让的行为，应进行风险评估，并通过合同等方式规定对方的数据安全保护责任和义务。

数据传输

大数据传输场景包括企业内部部门间、与关联方、与合作伙伴和供应商之间，部分国企可能会存在与政府部门进行数据传输的场景。

在数据传输阶段，企业应关注的合规问题主要有：

- 数据传输是否安全；
- 是否涉及禁止传输的情形；
- 是否涉及跨境传输。

具体来说，建议企业采取以下数据安全保护措施：

- 遵循责任不随数据转移原则，建立有效的数据安全共享机制；
- 在数据交换前进行风险评估，并通过合同明确数据接收方的数据保护责任；
- 通过数据加密传输、数据脱敏等措施确保传输安全；
- 建立数据跨境传输合规评估机制。

数据销毁

数据需要被销毁的原因可能有以下方面：

- 主动销毁数据以减少数据泄露的风险；
- 删除无价值、不正确、不相关的数据；
- 应用户要求删除数据等。

数据销毁阶段，企业应注意的合规风险主要有：

- 是否实现全部数据副本的同步删除；
- 是否存在相关法规要求在一定时期内不得删除的数据。

建议企业从以下方面完善数据销毁阶段的安全控制：

- 通过数据分级分类，明确不同数据的留存期限；
- 在销毁前，明确需要销毁的数据范围、流程、销毁方式和销毁要求，明确销毁数据范围和流程，删除超出数据留存期限的相关数据。

数字化转型及大数据技术的发展和应用影响着国有企业的决策架构、业务模式、管理方式，同时也间接影响了个人生活方式和社会经济发展模式。目前我国的数字化转型及大数据技术仍处在初期发展阶段，国有企业作为中国经济发展的中流砥柱，应当积极推进大数据应用，同时加强大数据平台、应用及处理活动中的数据安全和隐私保护合规建设，从管理和技术上做好保护数据，有效、安全地应用大数据，起到示范作用。

原文链接：https://mp.weixin.qq.com/s/lRXfsj9_zYglQ2_G3qVZqw ，转载请注明。