大数据时代的数字化转型如何实现数据的安全使用

白一尧

山西省数字化转型促进中心　山西　太原　030000

[摘　要]在大数据时代下，数据成为行业发展较为关注的内容。在此期间出现数据安全和数据治理的概念，相应概念对于从事IT和信息安全管理的人员并不陌生，数据安全治理已成为大数据时代确保数据产业良性发展的重要手段，对于企业和政府部门也有较大的意义。在数据资产保护方面需要推进数据安全治理工作，但是我国在数据安全治理方面并未给出标准化的管理策略，难以在数据安全治理中，编制针对性强的管理方案。在大数据时代下推进数字化转型，有必要基于多元维度给出数据治理方案。本文基于数字化转型时期数据资产保护需要，给出数据安全治理的技术支撑，对数据安全治理未来发展方向进行预测，希望对我国产业数字化转型有积极的推动作用。

[关键词]大数据时代；数据产业；数字化转型；数据安全

【DOI】10.12252/j.issn.2096-627X.2020.03.171

在信息网络时代下数据产生量增加，使用户投资规模也不断扩大，在此过程中大数据安全工作迅速发展。根据目前得到的信息，国际层面应用在大数据安全的投资，在2017年便已突破100亿美元且大数据安全的投资仍以每年递增的形式持续发展，预计在2023年将会超过300亿美元。在我国各行业均引入信息技术开展工作的过程中，数据资产成为各行各业企业较为重要的资源。在此背景下，我国网络安全法的出现，成为资产价值肯定以及保护的手段，在企业与政府机构高度关注数据安全且增加此方面投资，数据脱敏、审计、加密，演变为数字安全投资较为热门的内容。在此期间必须基于数据安全管控需求，给出数据安全治理思路，在数据安全治理环节将数据安全管理和安全技术对接起来，基于网络、安全、业务等多部门在数据安全方面的诉求，给出做好数据安全治理的方案。

一、数据安全治理的基本理念

（一）治理愿景

数据安全使用是数据安全治理设定的目标，在数据成为现代诸多行业推动自身发展关键要素的今天，需要继续推进数据安全工作。数据存在便是为了使用，如果数据安全得不到保证，数据的使用便会失去意义，即便能强行应用数据处理工作，也只能得到差强人意的结果。数据安全治理将工作要点锁定在数据安全使用方面，根据数据使用情况，提出具体的管理方案[1]。

角色授权、分级分类、场景化安全为数据安全治理的核心理念，在数据安全治理中需要做好组织架构构建、资产梳理、工作策略编制，在活动中进行全程控制[2]。

（二）核心理念

数据安全治理以数据分析作为首要内容，在数据分析与理解中做好类别的划分。在数据类别划分同时推进数据密集工作，给出数据的使用原则并进行合理控制，根据数据内容给出针对性防护。在数据管理中，根据使用需求和内容，做好防护方案的设定，提高防护方案工作措施的针对性，在适当保护条件下，保证数据得到合理应用，同时提高数据流动自由程度。在数据分类分级后，根据数据特征进行描述，在数据系统建设中依据特征给出分布方案，由此通过数据的分布，清楚数据被访问情况，还能对数据使用信息进行系统的梳理。在数据梳理基础上，根据数据使用者和数据类型的不同，给出管控方法。数据存储、收集、分发、使用、销毁，均是数据管控包含的内容。在数据管理中，需要对访问行为进行记录到日志中，定期处理收集访问日志内容并进行风险分析，由此对数据使用安全性进行评估，在此基础上给出管控方法[3]。

二、数据安全治理的技术框架

（一）支撑技术

在数据资产梳理时，需要基于企业资产的现状进行管理，了解企业资产安全状况，给出对应的管控方法，确保资产梳理可以高效进行，且能做好资产安全管控。给出数据资产梳理的方案，对资产风险进行异常行为监测，通过风险预估和有效控制，防止后期出现信息泄漏的事件。在数据安全治理中，通过数据状况可视化呈现技术、动态与静态梳理技术，做好数据资产存储系统安全现状评估，基于评估值给出安全治理方案[4]。

（二）安全控制

在数据使用阶段，会根据数据使用需求以及流动性进行划分，向不同的场景提供对应技术手段，从而对场景进行有效的操控，达到场景数据使用风险规避的目的[5]。

（三）安全审计

在数据安全治理中，以安全稽核作为数据安全治理策略可靠执行的保障，快速发现数据在使用期间存在的风险行为并进行控制。在数据安全稽核下，可以根据数据安全使用需要，确定数据防护方向，对现有的防护体系和策略进行完善，促使防护体系拥有较强的适应能力[6]。

三、数字化转型中数据安全治理的发展方向

（一）数据产业深层次发展

在互联网时代，很多企业均基于行业发展环境和自身可持续发展需求，构建“互联网+”的工作模式。在此期间，随着企业运营活动的开展，业务数据量随之增多，数据的价值在社会各企业工作模式改变状态下越加凸显。基于我国2019年中央做出的指示，数据已经和技术、资本、劳动成为生产的重要内容。在十四五时期各地企业均看到数字经济具备的发展潜力，基于政府要求参与到产业布局中。政府也根据时代发展趋势，出台关于数字经济方面的政策，为数字经济发展提供支撑，不会因管控不到位出现行业无序发展的乱象。在我国社会经济快速发展的背景下，已经全面进入数字生产力阶段，数据要素也在数字经济作用加大的过程中，依托规模效应低、边际成本低、可复用性强、流动性高等生产优势，成为推动中国高质量发展的新引擎。我国需要在数字经济发展中，进一步推动数据产业化发展[7]。

在疫情背景下对实体行业造成不小的打击，也为数字化发展提供良好条件，物联网、5G、人工智能等以信息技术为

支撑的现代技术，在国民经济流通、生产、消费等环节得到较好作用，相应技术在国民经济中的作用也较为凸显。直播电商、互联网、医疗、远程办公等新业态，也在疫情特殊时期快速发展，使我国数字经济呈现出新的发展局面。在此期间数据的使用量增加，数据的深度应用对政务、金融等领域发展有较大的作用。数字化发展智能化发展以数据利用为重要事项，通过数据的利用和价值的挖掘，为数字化转型提供支撑。不同行业在数据转型方面，因所持基础存在差异，使相应产业的转型步伐和节奏并不统一[8]。

对于医疗、金融、政务等领域，企业技术密集型基础和数据基础与其他行业相比有较大的优势，此类行业的数字化转型速度较快。此类行业作为数据密集型行业，在数字转型阶段将工作重点集中在数据利用方面，并在数据应用中持续推进数据价值的挖掘。金融行业在数字化转型中，将关注点集中在数据分析，对用户的行为进行判断，相应工作也达到一定高度。金融行业在数据应用下，可以提高服务质量。企业数字化服务仍在不断发展中，且能为行业带来更多的优势和资源。

在国家大力推进经济建设与发展中，数字经济成为我国经济领域新的增长点。在我国信息技术快速发展的过程中，也为数字经济发展提供较好条件。通过对数据的研究发现，在数字经济领域我国和西方发达国家的差距并不明显，且在数字产业配套方面能力较为强健。在5G等领域，我国在国际中也处于领跑状态，为我国数字经济发展提供较好的支持。我国人口有14亿之多，超大的内需市场，也为数字经济发展提供较大的规模。在移动互联网、网络基础设施、信息化深度、网络经济等方面，我国均有一定的基础。目前各行业和产业需要基于自身发展诉求，借助政府政策支撑，加快数据产业的转型速度，通过数据的挖掘与数据技术合理使用，获得支持自身持续发展的可靠信息。

（二）平衡数据孤岛

数字经济时代，加快经济发展速度，但是数字经济有利也有弊，在看到数字经济优势一面，还需要做好数字经济所带来问题的处置。数据孤岛便是目前政府以及企业需要着重关注并处理的问题，我国诸多公司乃至机构，内部均出现数据壁垒，不同机构会因规模或其他因素，使数据壁垒的程度有所差别。数据孤岛会对企业或部门发展造成不小的威胁，还会拖慢数据智能化发展速度。隐私保护、数据安全、数据确权也是数字经济时代，各方需要重点关注的内容。在用户隐私保护方面，必须在满足数据使用需求基础上，合理应用数据创造价值，同时不会出现数据泄漏问题。

在数字经济下推进数字产业发展，应该针对数字资产保护的需求，协调行业、从业者、监管、企业等主体，在各生态良性协作下建立数据安全管理机制，通过安全风险熔断、数据申请审核、违规行为追溯等制度的构建，对个人隐私保护、数据应用伦理进行综合研判。在大数据技术的发展中，应该增加大数据安全技术的研发力度，基于数据产业发展需求，引导数据安全产业根据自身需要和当下的发展情况，做出科学的布局。

在数据孤岛处置方面，需要以数据资源共享互通作为工作首要任务，利用数字技术催生出新业态、新产业、新模式，为数字产业化的发展提供条件。在产业数字化转型阶段，需要从企业数字转型诉求方面锁定目标，为使企业可以持续发展，必须在企业数字转型中激发企业的内生动力，让数字技术可以更好的挖掘数据价值，为企业提供服务。通过数字释放，在实体经济发展中获得较好的推动作用，促使实体经济与数字经济实现深度融合。

（三）加大数据安全控制力度

隐私保护、数据安全、数据确权是目前行业，在数据技术使用中较为关注的内容。对于此类难题，IT行业的工作者提出以技术手段进行处理。在数据安全技术层面为处理数据技术应用带来的隐私安全问题，将隐私安全计算作为关键点，通过技术的合理应用提出问题解决方案。隐私计算关联到联邦学习、安全多方计算、可信执行环境、差分隐私等技术，每个技术在各自领域中独立发展，根据数据技术使用需求，呈现出融合趋势。在数字产业发展中，基于企业数字转型需求，加大数据安全领域技术的创新力度，以安全数据交换协议实现数据的共用，而不享有数据。在该做法下可以解决数字隐私方面的不少问题，将数据安全提升到更高的层级。

在数据安全控制中，需要合理使用安全管控方法。比如智慧金融行业在数字化转型中，对于隐私问题处理，在供应链撮合平台构建后，针对该平台跨越智慧政务场景、智慧金融需要打通税务、政务、企业、银行、个人等主体隐私要求与安全保护异构数据的基础上，在中小微融资扶持平台建设中，以知识联邦的方式做好安全串联工作。在知识联邦的安全管理方法下，为数据安全工作提供标准工具。

结语

技术产品供应商、安全治理咨询服务商、大型数据中心用户等，均是数据安全治理产业的重要成员，在我国产业链环境构建过程中，为更好的推进数据安全治理工作，需要做好产业链的完善，从而为数据安全治理提供条件，将数据安全治理的价值发挥出来，推动IT治理变革发展，将数据使用中业务存在的风险控制在较低水平。

参考文献

[1]唐志荣，康锋，陈丽琼.大数据时代高校科技期刊全程数字化出版及其知识服务转型[J].浙江传媒学院学报，2019，026（006）：21-27.

[2]周小健，鲁梁梁.大数据时代背景下计算机网络安全防范应用与运行[J].网络安全技术与应用，2017（5）：2.

[3]戈晶晶.大数据时代数据安全应如何保障[J].中国信息界，2018（4）：4.

[4]刘李.大数据下的企业数字化转型研究与实践——以MT企业为例[J].中国管理信息化，2019，22（15）：3.

[5]宋雪莹.大数据时代公共管理中信息资源共享问题及对策——数字政府治理中信息孤岛问题研究[J].职业，2019（15）：2.

[6]赵跃.大数据时代档案数据化的前景展望：意义与困境[J].档案学研究，2019（5）：9.

[7]陈宝生.基于大数据时代的图书馆服务转型研究[J].人文天下，2019（18）：4.

[8]艾依.数据洪流中的企业数字化转型引路人[J].互联网周刊，2018（12）：2.