2020 年 5 月 12 日

抓紧新基建机遇——企业多面数字化转型的法律指引（一）

前言

“新基建”从 2018 年年底中央经济工作会议[1]首次提出，在受疫情影响的 2020 年年初不断深化并受到市场的热捧和重视。

2020 年 4 月 20 日，国家发展和改革委员会在新闻发布会上首次明确了新型基础设施建设的范围，乃是“以新发展理念为引领，以技术创新为驱动，以信息网络为基础，面向高质量发展需要，提供数字转型、智能升级、融合创新等服务的基础设施体系”[2]。

2020 年 4 月 28 日的国务院常务会议指出[3]，“一要根据发展需要和产业潜力，推进信息网络等新型基础设施建设。创新投资建设模式，坚持以市场投入为主，支持多元主体参与建设，鼓励金融机构创新产品强化服务。加强政府引导和支持，为投资建设提供更多便利。二要着眼国内需求，以应用为导向，挖掘我国市场规模巨大的潜能，积极拓展新型基础设施应用场景。瞄准产业升级和智能制造发展，引导各方合力建设工业互联网。适应群众数字消费新需求，促进网上办公、远程教育、远程医疗、车联网、智慧城市等应用。推动通信与相关行业双向开放与合作，消除行业应用壁垒，为平台经济发展和行业开放融合营造良好环境，构建平台及其参与者互促共赢的生态。保障个人隐私和网络、数据安全。三要深化相关领域国际开放合作，推动互利共赢、共同发展”。

同时，各部委及地方政府纷纷出台对于新基建、数字经济的鼓励措施。例如，2020 年 3 月 6 日，工业和信息化部发布《关于推动工业互联网加快发展的通知》[4]。2020 年 4 月 7 日，国家发展和改革委员会和中共中央网络安全和信息化委员会办公室共同发布了《关于推进“上云用数赋智”行动 培育新经济发展实施方案》[5]。2020 年 4 月 8 日，上海市人民政府办公厅印发了《上海市促进在线新经济发展行动方案（2020-2022 年）》[6]。

这无疑为从事新基建领域的各类运营服务商提供了前所未有的发展机遇。而另一方面，对无数可以利用、依托新基建来发展自身的企业来说，也是可以通过各方面的升级和创新，来实现提升企业运营、产品创新、管理运维、甚至传统产业升级的多面数字化转型的挑战和机会。企业可以基于自身目前的业务和管理特点，结合新基建所提供的不同场景下的新技术，创建新的管理、业务和发展的场景，从而在数字经济的发展之中占据一席之地。

我们结合多年来在涉及数字经济发展不同方面的经验，根据我们对于数字化转型各方面的理解，由

[1] http://www.xinhuanet.com/2018-12/21/c_1123887379.htm
[2] https://news.sina.com.cn/c/2020-04-20/doc-iirczymi7321296.shtml
[3] http://www.gov.cn/premier/2020-04/28/content_5507096.htm
[4] http://www.gov.cn/zhengce/zhengceku/2020-03/20/content_5493549.htm
[5] http://www.gov.cn/zhengce/zhengceku/2020-04/10/content_5501163.htm
[6] http://www.shanghai.gov.cn/nw2/nw2314/nw2319/nw12344/u26aw64687.html

我们的各位律师，通过相对短小浓缩的文章，为大家分享关于数字化转型的一些主要法律问题和值得关注的新动向，以期在企业的多面数字化转型的过程提供法律的支持和指引。

分享将通过三期内容向大家呈现。在第一期之中，我们会跟大家分享机构的内部数字化转型，包括数字合同和电子签名、数字化办公和管理、以及数字化设施的设立和运营三方面内容。后续敬请期待我们第二期：数字化转型的业务拓展。

第一期　机构的内部数字化转型

机构运营的全面数字化：文档管理，财务、业务流程管理和内部操作，与客户、合作方以及供应商的电子化联系与签约、系统上云，都会逐渐精简成本、推动效率升级。与此相关的法律问题及制度建设也刻不容缓。

一、 数字化办公和管理

远程办公并不是一个新话题，此前很多公司已在探讨和实施各种灵活办公的方式，以给予员工更多的自由和选择，但仍然相对“小众”、“前卫”。而在最近的疫情期间，为积极配合防控工作的开展，很多公司都采用了远程办公的方式。远程办公方式虽然便利，但实施的安全性、员工的隐私平衡、及同时提高办公效率，都是公司需要考虑、并逐步完善的。

1、 员工使用第三方服务

员工在远程办公的过程中经常需要使用第三方提供的远程办公服务，例如在线会议、即时通信、文档协作等。第三方服务的使用给企业带来便利的同时，往往给企业带来数据安全、系统安全等潜在的风险。

我们建议，在使用第三方服务前，企业可采取包括确认与区分网络安全责任主体、审核第三方服务资质及确认系统是否符合技术安全要求等措施，预防后期可能产生的与使用第三方服务相关的法律风险；企业在使用第三方服务的过程中，应通过隐私政策征求员工的同意、与第三方服务提供商签署数据处理协议等方式，保护员工的个人信息安全，并与第三方服务提供商签署保密协议，防止商业机密和其他重要数据的泄露。

2、 员工使用自有设备

对于企业而言，允许员工使用自有设备能够减少企业在设备方面的开支，有利于员工更迅速的响应工作要求，但也会带来一系列相应的数据安全和个人隐私问题，特别是允许员工使用自有设备可能构成对企业网络与数据安全的威胁。例如员工在其设备上无意间安装了设置有恶意程序的插件，或点击了带有病毒的邮件或钓鱼邮件，企业内部网络的安全将受到被攻击的威胁。

我们建议，为了尽量规避员工使用自有设备所带来的法律风险，企业可考虑采取包括制定自有设备安全使用制度、建立访问权限制度和数据分级管理制度、制定网络应急预案等方式保障员工安全使用自有设备。

3、 采取适当监控措施

在远程工作的过程中，企业出于对员工进行管理和监督的需要，可能会采取对员工进行远程监控的措施。例如，企业可能通过摄像头监控员工的工作状态，或者通过插件追踪员工的网络浏览记录。如何平衡对员工的远程管理与保护员工隐私之间的关系，是远程工作中企业需要重点关注的议题。

实践中，企业应谨慎考虑是否开通对员工进行远程监控的方式，并确保收集的数据和收集的目的是直接关联的、并且符合比例原则；并通过知情同意书等形式向员工告知为了采取监控措施所需要收集的个人信息的类型和方式，并获得员工的明示同意。

此外，我们建议，企业还应确保不将员工的数据

用于工作监测以外的目的，采取必要措施确保信息在传输和存储过程中的安全，且仅在工作时间内开展监控等。

4、 未来的展望

疫情期间为远程办公的实现提供了大规模的试验期。一方面，为远程办公的相关服务会快速增加和迅猛发展，为企业员工提供更便利的工作渠道。另一方面，由于远程办公带来的信息安全风险、隐私权利的争论也会不可避免的增多。企业只有早做部署，全面、提早考虑各种渠道，通过法律、技术等各方面的机制来保证企业自身的信息安全、权利平衡和措施实施的合规性，才能将远程办公的便利性发挥到极致，也将推动未来更深入的工作方式变革。我们愿意持续与不同企业探讨这些新的方式和挑战，并为这些新问题提供相应的解决方案和建议。

有关“数字化办公与管理”更加详尽的内容请参见君合此前发布的**研究简讯《疫情相关的信息保护和网络问题研究系列之二——常态采用远程办公的注意事项讨论》。**

二、 数字化文档及电子签约

——实现文档协议的全面电子化管理

伴随着电子商务的蓬勃发展，普通人对于数字合同已不再陌生，通过鼠标点击“确认”按钮在网站下订单也已成常态。而在企业数字化转型过程，不少企业已通过境内外的电子签约平台实现企业的业务协议、劳动合同等协议文档的远程签署，各行各业也在积极探索采用可靠电子签名的方式，来签署其对内、对外的合同、文书、单据及其他数字化文件（以下统称“**数字化文档**”），以实现企业协议及文档安全、高效、便捷的全面电子化管理。

1、 电子签名及其效力

根据《电子签名法》[7]第二条的规定，电子签名是指“数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据”。因此，我们理解，电子签名的本质是可以识别签名人身份的特殊数据，签名人可通过向数字合同中加入该等特殊数据，表明签名人身份及其对数字化文档内容的认可，从而完成数字化文档的签署。而根据《电子签名法》的规定，同时满足以下条件的电子签名，即可视为可靠的电子签名，并与手写签名或盖章具有同等的法律效力：

(1) 电子签名制作数据用于电子签名时，属于电子签名人专有；

(2) 签署时电子签名制作数据仅由电子签名人控制；

(3) 签署后对电子签名的任何改动能够被发现；

(4) 签署后对数据电文内容和形式的任何改动能够被发现。

2、 可靠的电子签名的实现方式

实践中，电子签名的实现方式较多，常见类型包括：

(1) 基于数字证书、可信时间戳等实现的电子签名；

(2) 基于生物识别特征（如指纹、虹膜、面部特征等）实现的电子签名；及

(3) 基于签名人独有的密码（如手机验证码、Pin码等）实现的电子签名等。

采用不同的电子签名实现方式，相应的技术流程以及技术成本也往往存在差异。以基于数字证书的电

[7] 2004 年 8 月 28 日起正式施行，2015 年 4 月 24 日第一次修订，2019 年 4 月 23 日第二次修订。

子签名为例，根据相关法规及国家标准的规定[8]，企业采用基于数字证书的电子签名的，需要由具有资质的第三方电子签名认证服务机构颁发数字证书并进行一系列验证和认证后[9]，方可确保该等电子签名满足《电子签名法》项下的可靠性要求。因此，我们建议，企业可以根据待签的数字化文档的重要程度、不同的实现方式下的技术流程及成本的差异，综合考虑、选择性价比更高、更适合企业需求的可靠电子签名实现方式。

3、 电子签名的适用范围

根据《电子签名法》第三条，民事活动中的合同或者其他文件、单证等文书，当事人可以约定使用或者不使用电子签名，但以下情形除外：

(1) 涉及婚姻、收养、继承等人身关系的；

(2) 涉及停止供水、供热、供气等公用事业服务的；

(3) 法律、行政法规规定的不适用电子文书的其他情形。

针对上述例外情形，企业需要注意以下问题：

电子签名不当然适用行政合同。企业与行政主体[10]签署的数字合同或行政管理文件，不属于民事活动中的合同或文件，因此，无法当然适用前述规定，该等情形下，企业需根据相关法律、法规的规定以及行政主体的要求，选择适当的方式签署相应文件。

劳动合同不属于《电子签名法》所禁止的范围。《电子签名法》第三条所列举的“婚姻、收养、继承关系”均属于具有强烈人身属性的法律关系，而劳动合同虽然具有一定的人身属性，但其亦包含一定的财产关系，因而并不属于《电子签名法》第三条项下不适用电子签名的例外情形[11]。对此，人力资源与社会保障部办公厅亦于 2020 年 3 月 4 日发函[12]明确劳动合同可采用电子形式订立，为企业采用电子签名签署劳动合同提供了有力支持。

4、 电子证据保存

根据《最高人民法院关于互联网法院审理案件若干问题的规定》（法释〔2018〕16 号）的具体规定[13]，

---

[8]《电子认证服务管理办法》，工业和信息化部于 2005 年 2 月 8 日颁布施行，2009 年 2 月 18 日第一次修订，2015 年 4 月 29 日第二次修订。《信息安全技术 公钥基础设施 基于数字证书的可靠电子签名生成及技术要求》，国家质量监督检验检疫总局与国家标准化管理委员会于 2017 年 12 月 29 日公布实行。

[9] 实践中，企业可通过具有资质的第三方电子签名认证服务机构搭建的在线平台完成数字证书的颁发、电子签名的认证及签署流程。

[10] 如国家行政机关或法律法规授权行使行政管理职能的其他组织等。

[11] 引自《君合创新-劳动合同电子化管理的法律效力研究》，载于“君合法律评论”公众号，原作者马建军、李明及何婷婷。

[12] 《人力资源社会保障部办公厅关于订立电子劳动合同有关问题的函》（人社厅函〔2020〕33 号）明确“用人单位与劳动者协商一致，可以采用电子形式订立书面劳动合同”。

[13]第十一条当事人对电子数据真实性提出异议的，互联网法院应当结合质证情况，审查判断电子数据生成、收集、存储、传输过程的真实性，并着重审查以下内容：

（一）电子数据生成、收集、存储、传输所依赖的计算机系统等硬件、软件环境是否安全、可靠；

（二）电子数据的生成主体和时间是否明确，表现内容是否清晰、客观、准确；

（三）电子数据的存储、保管介质是否明确，保管方式和手段是否妥当；

（四）电子数据提取和固定的主体、工具和方式是否可靠，提取过程是否可以重现；

（五）电子数据的内容是否存在增加、删除、修改及不完整等情形；

（六）电子数据是否可以通过特定形式得到验证。

当事人提交的电子数据，通过电子签名、可信时间戳、哈希值校验、区块链等证据收集、固定和防篡改的技术手段或者通过电子取证存证平台认证，能够证明其真实性的，互联网法院应当确认。当事人可以申请具有专门知识的人就电子数据技术问题提出意见。互联网法院可以根据当事人申请或者依职权，委托鉴定电子数据的真实性或者调取其他相关证据进行核对。

当事人对电子数据的真实性提出异议时，法院将着重审查电子证据所依赖的计算机软硬件是否可靠、生成时间及主体是否明确、保管方式是否妥当、提取方式是否可靠、内容是否存在修改或不完整以及是否可以对电子证据进行重复验证等多方面内容，从而综合判断电子数据的真实性并决定是否采纳。

因此，我们建议，企业在数字化文档的签署和管理过程中，需要按照前述法院对电子证据真实性及可靠性的审查标准，对数字化文档及其生成、签署及保管有关的电子数据（以下统称“**电子证据**”）予以妥善保存，必要时还可以对相关电子证据的生成及存储过程进行公证，或委托具有资质的第三方（如电子签约平台）对电子证据的原始状态进行存证以供随时调查取用及验证，又或者委托司法鉴定机构对电子证据进行专业司法鉴定，从而确保在发生争议时，相关电子证据的真实性及可靠性能被法院认可。

三、 数字化设施的设立和运营

随着大数据、人工智能、云计算、5G、物联网和区块链等数字技术加速发展，为企业实现数字化转型提供了重要助力支持。未来，互联网、大数据、人工智能和实体经济深度融合，“上云用数赋智”将为企业获得高质量发展提供重要引擎。企业可选择自营方式，或通过寻求外包与合作，实现研发设计、生产加工、经营管理、销售服务等业务转型。同时，对于处于设立阶段或已运营的数字化企业，还需关注与数字化服务相关的合规风险等问题。

1、 运营资质

取得运营的相关资质是数字化设施运转的必要条件。根据《互联网信息服务管理办法》、《电信业务分类目录（2015 年版）》（2019 年修订）（简称“**《电信分类目录》**”），企业在数字化转型过程中，如果涉及通过互联网向上网用户有偿提供信息或者网页制作等服务活动，则需要取得 B25 互联网信息服务增值电信业务经营许可证。某些特定行业还可能对线上运营有特殊资质要求，例如根据《网络预约出租汽车经营服务管理暂行办法》，从事网约车经营需要取得《网络预约出租汽车经营许可证》；从事互联网诊疗，需要依据《互联网诊疗管理办法（试行）》经卫生健康行政部门批准同意后进行。

2、 外包风险防控

企业以外包或合作形式从事数字化转型时，服务提供商数据安全保护能力、服务的连续性和稳定性是保障数字化企业稳定运营的核心要素，服务质量缺陷甚至可能导致企业颠覆性风险。例如，某网络技术公司租用某数据服务公司的服务器从事网站经营，后因数据服务公司服务器损坏，导致网络技术公司网站运营相关的数据永久丢失[14]。

从法律规定的层面，部分行业因其数据敏感性，对数据服务提供商的质量把控提出具体的要求。例如，根据《银行业金融机构信息科技外包风险监管指引》，银行业金融机构需要在签订合同前对服务提供商进行尽职调查，对重要的外包服务进行定期的风险评估，每三年对重要的外包服务进行全面审计，发生外包风险事件后及时开展专项审计。

另外，如果数字化企业需要选择数据中心、云计算平台服务提供商、实现系统和服务上云。则根据《电信分类目录》，经营数据中心业务通常需要取得 B11 互联网数据中心业务许可（简称“**IDC 证**”）；对于云计算服务，需根据具体服务形态，例如是否为依托于云服务平台的 SaaS 服务等，判断服务商是否需要取得 IDC 证。

实践中，越来越多的数字化企业在采购服务供应

[14] 北京亿维视讯网络技术有限公司与北京企商在线数据通信科技有限公司网络服务合同纠纷一审民事判决书

商时着重关注数据服务提供商的数据安全保护能力，建立事前预防、事中控制、事后管理全过程风险监管体系。例如，重视服务合同之中关于服务商的资质、服务水平、数据保护、突发事件的处置等条款的各项安排。

3、 数据权属和数据合规

企业在数字化的过程中可能会打通不同系统之间的数据，进行数据分析、用户画像等，与之相关的个人信息保护问题也应成为数字化企业合规运营的重点关切。例如，某信息咨询公司从事提供数据的服务并收取查询费用，因其所提供信息包括个人学历数据库、手机号在网时长数据库、个人金融征信画像库等个人信息，涉嫌刑事犯罪，被移交公安机关处理[15]。

建议企业在采用涉及数据服务的流程之中，包括在与供应商及合作方之间进行数据流转的过程中，需重点识别是否存在个人信息、对应数据主体的授权链条是否完整、以及相应的数据权属进行风险分析、并作出适当的技术和法律安排。

董　潇　合伙人　电话：86 10 8519 1718　邮箱地址：dongx@junhe.com
董俊杰　律　师　电话：86 10 8540 8722　邮箱地址：dongjj@junhe.com
魏珉籍　律　师　电话：86 10 8540 8641　邮箱地址：weimj@junhe.com
朱　彤　律　师　电话：86 10 8519 1739　邮箱地址：zhutong@junhe.com
岳原州　律　师　申话：86 10 8540 8607　邮箱地址：yueyzh@junhe.com
郭　超　律　师　电话：86 10 8553 7733　邮箱地址：guoch@junhe.com
郭静荷　律　师　电话：86 10 8553 7947　邮箱地址：guojh@junhe.com
袁　琼　律　师　电话：86 10 8553 7663　邮箱地址：yuanq@junhe.com
刘青宇　律　师　电话：86 10 8540 8626　邮箱地址：liuqy@junhe.com
冯毅捷　律　师　电话：86 10 8540 8723　邮箱地址：fengyijie@junhe.com

注：（姓名按主要负责部分顺序排列）

[15] 智慧云游（北京）科技有限公司与北京塔塔信息咨询有限公司合同纠纷一审民事裁定书