

数字虚拟人新规解读和对零售行业的主要影响及合规建议

黄春林

近年来，随着计算机视觉、语音交互、生成式人工智能等技术的持续发展与深度融合，数字虚拟人正快速进入零售行业的营销、客服、直播等场景。然而，其在提升商业效能的同时，也触发了人格权保护、数据安全、算法治理及行业准入等一系列新型法律风险。

为此，2026年4月3日，国家网信办发布了《数字虚拟人信息服务管理办法（征求意见稿）》（下称《办法》）。《办法》详细规定了数字虚拟人服务的适用范围、权利保护、服务规范、标识要求、备案与安全评估等问题。

结合近期立法、执法实践及类似项目经验，汇业律师事务所黄春林律师团队简要介绍零售行业数字虚拟人的典型应用场景、资质要求、供应商审查要点、艺人授权问题以及上线运营中的重点合规义务，以供零售行业参考。

一、零售行业数字虚拟人的主要类型及应用场景

（一）数字虚拟人的主要类型

根据《办法》附则定义，数字虚拟人是指存在于非物理世界，利用图形学、数字图像处理或者人工智能等技术，借助真人驱动或者计算驱动，模拟人类外貌，具备声音、行为、交互能力或者性格等特征的虚拟数字形象。实务中，可从以下几个维度进行分类：

分类维度	主要类型	说明
呈现形式	2D/3D	2D 多用于轻量化营销传播；3D 更常用于沉浸式展示、直播或互动场景
驱动方式	真人驱动/非真人驱动	真人驱动通常通过动作捕捉、语音映射实现实时控制；非真人驱动则更多依赖模型自动生成或预设逻辑
形象来源	真人形象/卡通形象	真人形象通常基于艺人、员工、KOL 等构建；卡通形象多为原创品牌 IP

分类维度	主要类型	说明
交互能力	可交互/不可交互	可交互数字人一般具有语音、视觉、情感反馈等能力；不可交互数字人多用于单向展示

从监管与实务风险角度看，“真人形象+真人驱动+3D+可交互”的数字虚拟人，一般属于风险最高、法律要求最复杂的类型。

（二）零售行业的典型应用场景

根据类似项目经验，零售行业对数字虚拟人的应用，主要为以下三类典型场景：

应用场景	主要形式
数字人直播	平台直播、品牌自播、导购讲解、节庆促销直播
数字人营销素材	短视频、海报、广告片、互动品牌内容
数字人客服	官网、APP、小程序、会员系统中的客服或导购助手

（三）数字虚拟人服务所涉主要法律实体

结合零售行业的实际业务模式，数字虚拟人服务通常涉及以下几类主体：

- (1) **数字虚拟人服务提供者**：即直接向境内公众提供数字虚拟人制作、发布等服务的组织，包括专门的数字人平台或解决方案商承担，也可能是零售企业自身（详见第二部分）。
- (2) **数字虚拟人技术支持者**：即为数字虚拟人服务提供底层技术、算法模型、驱动引擎、语音合成、动作捕捉、多模态识别等技术支持的组织，包括技术供应商或集团科技公司等。
- (3) **网络信息内容传播服务提供者**：如抖音、京东、天猫、微信视频号、小红书等。
- (4) **数字虚拟人服务使用者**：即利用数字虚拟人制作、复制、发布内容信息的组织，品牌方大多数时候属于该类主体。此外经销商、TP、营销公司及MCN机构等可能也会属于这一类主体。
- (5) **主体人（真人）**：即数字虚拟人所对应、映射的自然人，通常是艺人、KOL甚至员工等。

(6) **用户**：即接受数字虚拟人服务的消费者、会员、粉丝等。

二、零售行业应用数字虚拟人的资质要求

零售行业应用数字虚拟人，需根据传播渠道的不同履行相应的审批/备案义务：

（一）通过第三方平台应用数字虚拟人

如果零售企业主要通过抖音、京东、天猫、小红书、微信公众号等第三方平台开展数字人直播、数字人客服，通常可在一定程度上依赖平台既有的资质体系和账号管理框架。但应重点关注平台方的准入规则，确保符合平台对 AI 生成内容的特定要求。

（二）通过自有网络渠道应用数字虚拟人

若零售企业通过官网、APP、小程序等自有网络渠道应用数字虚拟人，则需进一步区分其服务性质。

1. 提供非经营性信息服务

如果企业仅在自有官网、APP 或小程序中使用数字虚拟人介绍自有品牌，或者展示自有产品或提供自有产品的客服服务，原则上属于非经营性互联网信息服务，则企业应重点关注 ICP 备案、算法备案、等保备案等问题。

2. 提供经营性信息服务

如果企业进一步向公众用户开放数字虚拟人的制作、发布或养成等功能，使数字虚拟人成为一种直接或间接经营性的在线服务，则可能属于经营性互联网信息服务属性。在此情形下，企业应重点评估是否涉及增值电信业务许可，以及本文第三部分供应商资质审查部分的其他资质要求。

（三）特殊行业信息服务资质

根据《办法》第三条等规定，对于涉及特殊监管领域，例如医疗医药、文旅、教育、广电、游戏等，即使数字虚拟人本身的技术形态并无特殊性，企业在开展相关信息服务时，仍需同时符合各行业的特别规定。因此，数字虚拟人本身并不当然改变行业监管边界，其应用往往会使既有行业规则与互联网信息服务规则发生叠加适用。

三、数字虚拟人供应商资质审查及产品性能要求

由于数字虚拟人服务通常涉及模型、算法、驱动系统、语音引擎、内容生成、平台接入等多个模块，因此企业应同步审查其基础资质、底层能力与合同责任承担机制。

（一）供应商资质审查

企业对数字虚拟人供应商的资质审查，通常至少应涵盖以下方面：

- （1）**ICP 备案或增值电信业务许可**：大多数情况下需要供应商至少具有 ICP 许可证，少数情况下还可能需 B11、B22 等类型的电信业务许可。
- （2）**算法备案情况**：根据《办法》第二十一条等规定，具有舆论属性或者社会动员能力（各地网信办的认定口径较为宽松）的数字虚拟人服务提供者，应当依法履行算法备案和相关变更、注销手续；数字虚拟人技术支持者亦参照履行。
- （3）**大模型备案或登记情况**：如供应商提供 AIGC 能力，尤其是面向公众（不限于 C 端）提供具有生成能力的服务，则应结合现行生成式人工智能监管规则，核查其备案、登记情况。
- （4）**网络安全等级保护情况**：对于承载用户交互、账号体系、音视频处理和个人信息处理的平台，企业通常还应审查其网络安全等级保护备案和测评情况。

（二）产品性能要求

在零售直播、品牌传播和客服互动场景中，若数字人的真实感、响应性、交互准确率或情感反馈能力存在明显缺陷，极易引发误导宣传、消费者投诉乃至平台处罚。换言之，产品性能并非仅是效果问题，而可能直接外溢为合规问题。例如，口型驱动明显失真、动作与语音严重不匹配、响应明显迟滞，均可能影响消费者对商品宣传内容真实性的判断；而在客服场景中，语音打断失败、情感识别错误，也可能导致用户体验恶化、投诉率上升，甚至在特殊情境下侵犯消费者知情权、公平交易权。

因此，在技术采购及验收阶段，黄春林律师团队建议重点关注包括但不限于以下指标：分辨率、模型面数、视频帧率、穿模率、口型驱动准确率、动作匹配准确率、唤醒正确率、响应速度、端点检测准确率、语音打断成功率、情感交互成功率等指标等。

（三）协议约束

基于数字虚拟人服务的复杂性，企业与供应商签署的合作协议，不宜仅停留在传统的软件采购、技术服务或 SaaS 服务框架，而应当围绕数字虚拟人应用的特殊风险，相关条款及合同至少应涵盖以下内容：

- 主体人授权的真实性和完整性与持续有效性；
- 用于训练、生成或展示的知识产权授权链条完整性；
- 虚拟形象、声音素材及生成内容的知识产权归属；
- 网络安全与信息内容安全责任划分；
- 个人信息处理及数据合规性；
- 相关备案、许可和资质的持续有效性；
- 生成合成内容标识和“数字人”提示义务的分工；
- 用户投诉、侵权通知、应急下线及日志协查机制；
- 供应商违反上述义务时的赔偿、整改及终止责任。

从实务角度看，黄春林律师团队建议零售企业将以下文件作为主合同附件一并签署：

- 《AI 合规专项条款》；
- 《（主体人）授权书》；等等。

四、签约艺人生成数字虚拟人的主要法律问题

在零售品牌营销中，企业常希望基于签约艺人、品牌代言人、KOL、店播主播甚至内部员工等主体人，生成可重复使用的数字虚拟人，以降低主体人出镜成本并提升内容供给效率。但该模式也恰恰是法律争议、监管执法最为集中的领域之一。

（一）肖像、声音及名称等人格权授权

如果数字虚拟人以特定主体人为原型或高度近似，则至少需要关注以下授权基础：

- 肖像权、声音权益授权；
- 姓名、艺名、昵称或具有识别性的名称授权；
- 表演形象及相关衍生形象授权；等等。

即便企业与艺人之间已经存在代言合作协议，也不能当然推定企业有权进一步制作、训练、复制并运营其数字虚拟人。

（二）个人信息授权与撤回限制

根据《办法》第七条，任何组织和个人使用自然人敏感个人信息用于建模、形象生成、场景构建等活动的，应当依法取得自然人的单独同意，并履行充分告知义务。尤其是在MCN机构代理签约的情况，如何实现艺人的单独同意机制，需要重点考虑，尤其是当企业采集艺人的面部特征、声音数据、动作轨迹、语义习惯等信息用于模型训练或数字人生成时，其处理行为很可能已落入敏感个人信息处理范畴。

实务中最值得注意的，是授权稳定性与撤回机制之间的张力。对此，企业应在合法边界内通过合同机制尽量明确授权期限、撤回后果、数据删除路径、数字人下线安排及历史素材处置方式，以降低后续争议。

（三）授权范围的精细化约定

数字虚拟人项目中，主体人格权和个人信息授权范围的模糊，是最常见也是代价最高的风险来源之一。建议企业至少明确以下事项：

- 授权人格权、个人信息等权利类型；
- 授权物理地域、网络渠道范围；
- 授权期限；
- 授权品牌或产品/服务范围；
- 可使用的商业场景；
- 是否允许二次开发、二次训练和内容再生成；
- 明确虚拟形象、声音素材及生成内容的知识产权归属及使用限制；
- 合同终止或授权届满后，历史素材和模型参数如何处理；等等。

五、上线运营数字虚拟人的主要合规要求

根据《办法》及现行相关监管执法，零售行业上线运营数字虚拟人至少应重点关注以下几方面要求。

（一）合规治理要求

根据《办法》第十五条等规定，数字虚拟人服务提供者和服务使用者应建立安全风险监测、预警和应急处置、防沉迷提示等机制，建立完善内容导向管理制度，并配备与经营规

模相适应的技术能力和人员力量，采用技术手段与人工审核相结合的方式开展风险识别、监测与预警，记录并留存日志信息。

（二）信息内容安全责任

根据《办法》第十一条、第十二条及第十八条等规定，数字虚拟人服务不得用于生成、传播违法和不良信息，不得从事虚假宣传、恶意诱导消费、电信诈骗等违法活动，并应采取措施防范和抵制存在性暗示、性挑逗、血腥暴力、歧视煽动等不良内容。

（三）数据安全责任

根据《办法》第十四条等规定，数字虚拟人服务提供者和服务使用者应当在特定目的和范围内开展数据处理活动，使用具有合法来源的数据，并采取相应技术措施和其他必要措施，保障数据存储和传输安全，防止数据泄露或者不当使用。在零售场景下，数字虚拟人相关的数据处理活动通常包括：

- 主体人建模数据；
- 用户交互数据；
- 直播评论、语音输入、咨询记录；
- 会员画像和偏好信息；
- 商品知识库、营销话术库、客服问答库。

（四）标识标注义务

根据《办法》第十三条等规定，自数字虚拟人服务开始，数字虚拟人服务提供者、服务使用者及提供网络信息内容传播服务的服务提供者，应当在数字虚拟人展示区域全程持续显示含有“数字人”字样的显著提示标识，并符合国家人工智能生成合成内容标识有关规定。这一要求对于零售企业尤为重要。因为零售场景中的数字虚拟人，常常被设计得尽可能真实、亲和、可信，以增强消费者的接受度和购买转化率。但也正因为其高度拟真，消费者更容易对其真实身份形成误认。因此，监管部门将可识别性作为底线要求，强调必须通过显著、持续、不可忽视的方式进行标识。

（五）其他重点合规要求

数字人直播同样受《广告法》《反不正当竞争法》《价格法》等约束。虚拟主播、智能客服在推介产品或提供服务时，其话术需符合广告合规、价格合规、竞争合规等要求。

同时，根据《办法》第十五条、第十七条及第二十三条，相关主体需要依法记录并留存日志信息，在监管检查中提供必要协助。

此外，尤其是在拟人化互动场景下，企业应避免通过过度情感化设计诱导用户持续使用或消费；用户取消服务特定功能或退出服务时，不得设置不当障碍或实施过度挽留。

总体而言，数字虚拟人进入零售行业，并不只是带来营销效率的提升，更意味着企业将引入一个兼具人格模拟、内容输出、数据处理和商业转化功能的新型合规对象。其合规审查也不应停留在是否购买了合法产品、是否签了授权合同这样的单点判断，而应上升到围绕业务模式、权利基础、数据处理、技术能力、内容治理与持续运营责任展开的体系化评估。