浩天律师事务所
HYLANDS LAW FIRM

数智通鉴

数字科技与人工智能合规发展研究作品集

HYLANDS

浩天研究院出品

为公司的数智化发展提供法律解决方案

律所简介

北京浩天律师事务所（“浩天”）创立于1997 年，总部位于北京。历经多年发展，浩天现已设有北京、上海、广州、深圳、长沙、成都、重庆、大连、福州、贵阳、哈尔滨、海口、杭州、合肥、济南、昆明、南昌、南京、南宁、宁波、青岛、石家庄、沈阳、苏州、天津、太原、温州、武汉、乌鲁木齐、无锡、西安、徐州、银川、郑州、北京（密云区）、北京（昌平区）、香港、旧金山、比什凯克 40 家办公室和浩天胡关李罗(前海)联营律师事务所及1 家知识产权代理事务所。浩天在全球130 多个国家和地区拥有超过150 家合作律师事务所，可为全球客户提供一站式、多领域、跨国界的专业法律服务。

浩天现有600 余位合伙人及顾问，2000余名律师和专业人员，能够为客户提供英语、日语、韩语等多种语言的法律服务。浩天是中国优秀的大型综合性高端商事律师事务所之一，连续多年荣获钱伯斯（Chambers and Partners）、亚洲法律杂志（ALB）、法律500 强（The Legal 500）、亚洲法律概况（asialaw Profiles）、IFLR1000和商法（China Business Law Journal） 等国际法律评级机构的推荐及奖项。

HYLANDS LAW F



IRM

为“数智通鉴”专栏作寄语：
从市场中发现一线需求，在问题中提炼法律智慧

主笔人



高艳东

浙江大学数字法治研究院副院长

在“十四五”规划收官与“十五五”规划即将开启的历史交汇点，我欣喜地看到浩天研究院“数智通鉴”专栏成果在一年的积累后，即将结集成册。作为长期关注数字化法治建设的学者，我对此感到由衷高兴，并以此寄语表达对专栏成果结集的祝贺。

数字技术与人工智能深刻改变了世界经济的样态和我们的日常生活，带来巨大生产力提升和便利效应的同时，新技术的“双刃剑”效应要求我们必须加强数字化发展治理。习近平总书记指出：“古往今来，很多技术都是‘双刃剑’，一方面可以造福社会、造福人民，另一方面也可以被一些人用来损害社会公共利益和民众利益。”这一深刻论断提醒我们，在享受数字技术带来便利的同时，必须注意其潜在风险。机遇和挑战总是新事物的一体两面，我们法律人要抓住机遇，更也要用专业去应对挑战。

“数智通鉴”这本作品集集合了团队成员对于产业一线需求的洞察，涵盖了数据作为关键生产要素的多个维度，包括政务数据共享、数据资产入表、数据交易与权益保护；深入探讨了人工智能技术的法律挑战，如AI生成内容的著作权、AIGC平台的侵权责任、AI换脸风险及大模型隐忧；同时涉及网络安全与合规实践，如个人信息保护审计、稳定币监管、技术犯罪防治以及司法案例解读，展现了数据智能与法律交叉领域的广泛主题，从基础政策到前沿应用，凸显了内容在技术、商业和法律层面的多元化。

“数智通鉴”专栏研究团队在数字化与人工智能合规研究领域做出了宝贵探索。在专栏成果结集之际，为团队寄予三点期待：

一是坚持前瞻视野，服务国家战略。数字化发展是关系国家发展全局的重大战略，团队应当继续紧跟“十五五”数字中国建设规划，聚焦数据产权、跨境数据流动、人工智能伦理等前沿问题，为构建中国特色数字治理体系提供学理支撑。当前，我国正在积极应对数字技术带来的风险挑战，向互联网服务管理模式提出新的更高要求。团队研究可以立足这一时代背景，为规范有序的数字化发展治理体系贡献智慧。

二是深化交叉研究，促进学科融合。数字法治是典型的交叉领域，需要法律、技术、经济、社会等多学科视角。期待团队继续保持开放包容的专业胸怀，促进不同学科领域的知识碰撞与思想交流。正如数字社会治理需要多方力量的共同参与，实现部门协同、区域协同以及政府与企事业单位、社区居民的协同，数字法治研究同样需要打破学科壁垒，实现知识资源的共享与整合。

三是注重实践导向，推动研用结合。理论研究唯有与实践结合才能焕发生机。团队应进一步加强与政府部门、行业协会、企业的合作，将理论研究成果转化为切实可行的合规指南与政策建议。在数字化发展治理中，应当“鼓励社会主体依法参与网络内容共治共管，畅通社会监督、受理、处置、反馈、激励闭环流程，激活社会共治积极性”。这种共建共治共享的理念，同样适用于数字法治研究，只有让研究成果服务于实践，才能真正体现其价值。

“所当乘者势也，不可失者时也。”站在“十四五”收官与“十五五”开启的历史节点，我们深刻认识到人工智能已成为牵引新质生产力整体跃升的“核心引擎”。希望浩天研究院“数智通鉴”研究团队继续秉持法治精神，以市场一线的真需求和真问题为导向，深化数字法治研究，为数字中国建设提供更加有力的智力支持，让“数字优势”转化为“产业胜势”，把“数据红利”转化为“民生福利”，为高质量发展注入更强动力。期待研究团队在数字法治研究领域取得更加丰硕的成果！

目录

CONTENTS

01 发刊词：当数据成为基础生产要素，我们希望为产业发展提供法律智慧..... 9

02 十问十答：《政务数据共享条例》亮点、重点以及难点应对..... 11

03 AI文生图：AI生成图片的著作权保护..... 18

04 稳定币：涵义释义及监管分析..... 21

05 信息保护：一张清单看懂《个人信息保护合规审计办法》..... 27

06 数据资产：为何数据资产入表是企业的必选项..... 30

07 城投公司：转型中虚拟电厂业务的数据风险..... 34

08 数据没有“所有权”：数据由“资源”变成“产品”的关键..... 39

09 合规即增长：从"大数据杀熟"被判罚看AI商业的合规转型..... 44

10 帮助侵权：AIGC文生图平台的侵权责任及合规建议..... 50

11 技术犯罪：从“工具之恶”到“主体之责”..... 54

12 数据入表全流程： 从合规确权到动态风控的法律实务指引..... 58

13 稳定币监管：美国“天才法案”核心内容解析..... 64

14 AI薅羊毛：AI图片骗取“仅退款”的法律责任及AIGC标识义务..... 70

15 正反手教学：最高院首发“数据权益司法保护”指导性案例..... 73

16 标识办法：《人工智能生成合成内容标识办法》下的合规方案与行业启示..... 77

17 AI遇上司法：北京互联网法院8个典型“涉人工智能案件”解读..... 82

18 AI大模型隐忧：首例处罚案例的启示与PIA实践..... 87

19 数据交易：数据授权运营的“三道防御工事”..... 91

20 AI换脸：数字假面可能“两面侵权”..... 95

21 APP合规：数十家头部外资/国资App被点名，别让“形式合规”成为致命漏洞..... 99

22 个人信息保护：北京四中院典型案例确立个保“北京标准”..... 105

23 默认勾选：数字消费中消费者权益保护与企业合规路径..... 108

24 《国家网络安全事件报告管理办法》核心要点梳理..... 112

25 《互联网法院管辖规定》修订要点解读..... 124

26 新《网络安全法》修订背景、重点、亮点解析..... 129

27 十问十答：港股IPO数据合规核心必知解读..... 135

28 大厂之责——《大型网络平台个人信息保护规定（征求意见稿）》亮点、重点、核心问题解读..... 141

29 《网络数据安全风险评估办法（征求意见稿）》核心速览..... 145

30 AI陪伴边界与责任——《人工智能拟人化互动服务管理暂行办法（征求意见稿）》重点内容解读及合规指南..... 151

一、发刊词：当数据成为基础生产要素，我们希望为产业发展提供法律智慧

数字化、智能化的发展，根本性改变了整体经济发展产业链的形态和布局，数智与法学的双轮驱动，发展与规制的硬币两面，是新经济发展样态的新课题，以现象为起点，以法律和法理为思考路径，“数智通鉴”期待贯通产业发展与法律规制的理解边界，给产业发展以借鉴智慧。

一、新要素：当数据作为新生产要素的重塑产业

数字中国是数字时代推进中国式现代化的重要引擎，在这样的时代背景下，数据成为新的生产要素和不可或缺的基础生产资料，数字化深刻影响着国际分工和贸易、改变产业链的形态和布局。数字时代已经成为继“蒸汽时代（1760-1840年）”、“电气时代（1860-1950年）”、“信息时代（1950年至今）后第四次工业革命的先声。

与土地、劳动力、资本等生产要素不同，数据有其特殊属性，这也就意味着在产权和价值界定上有着不同的理解内涵，无论是数字技术产业化还是产业经济数字化，数据的确权、主体利益确定、隐私保护以及跨境流动已经成为高效和安全对数据进行应用的核心议题。

如果说大数据时代完成的是一次“信息平权”，让地球变成平的。那么当数据与算法深度交融时，人工智能则真实让社会公众感受到“未来已来”，新年DeepSeek的横空出世重塑了人们对于未来产业格局、工作分工甚至未来规划的想象。在惊讶于技术跃迁发展的同时，也带来对于已有秩序格局的隐忧。

二、新问题：速度、行稳、致远的三维交融

人工智能技术溶解了物理现实、数字和个人之间的界限，带来了大量的伦理、法律新问题。也给传统的法律体系规定提出了新挑战，从学习欧盟《通用数据保护条例》（GDPR），到申请加入《数字经济伙伴关系协定》（DEPA），再到中国国内逐步形成如“数据三法”（网络安全法、数据安全法、个人信息保护法）为核心，配套行政法规、部门规章及行业标准的规制框架。产业发展在速度、行稳、致远的三维交融中逐步推进。

（一）刑事领域

虚拟货币、网络盲盒、刷单炒信等新型网络犯罪方式层出不穷，电信诈骗、网络诽谤、帮信罪等传统网络犯罪屡禁不止；新罪名的设立和传统罪名的扩大适用，新兴产业发展与保护人民生命财产安全的矛盾，让数字经济领域定罪量刑变得更加复杂。

（二）民商事领域

新业态的不断出现，反复考验着现有法律体系的完善性：平台责任、个人信息保护、企业数据资产保护、知识产权

和不正当竞争等类案件，成为被反复斟酌讨论的话题；法律规定简单笼统，相关技术背景复杂，更是为争议解决律师提出了新的挑战。

（三）合规领域

由于业务模式的快速更新迭代，企业亟需在合法性上寻求保证：企业数据资产合规、增值电信业务的经营资质、传统互联网企业的反垄断乃至互联网企业出海后的境外合规需求，越来越成为法律服务市场的新刚需。

三、开物前民：发展与规制的双向推动

“数智通鉴”是浩天数字科技与互联网行业委员会与浩天研究院策划的“超级符号”，我们期待在数字化和智能化的时代中，贯通产业发展与法律规制的理解边界，给产业发展以借鉴参考。

何以新之,开物前民。在策划期间，我们非常荣幸得到了浙江大学数字法治研究院的学术指导，让我们在探索最新问题的同时，不忘返回初心，铭记法律的终极目标不仅仅是秩序，更要有益于民众的福祉。

产业的发展与法律的规制如相互依赖的两个齿轮，并立前行，在未来的研究中，我们希望以双轮驱动为基础理念，更好贴近行业的最前沿发展，与此同时，为新问题的解决提出法律实务智慧。

二、十问十答：《政务数据共享条例》亮点、重点以及难点应对

主笔人





董文浩

北京浩天律师事务所 高级合伙人
dongwenhao@hylandslaw.com

吴梦瑶

北京浩天律师事务所 合伙人
wumengyao@hylandslaw.com

2025年5月28日，李强总理签署国务院令第809号，公布《政务数据共享条例》（下称“《条例》”），该《条例》共8章44条，自2025年8月1日起施行。从政务数据实行统一目录管理、政务数据共享使用流程、政务数据共享的后台支撑与保障三个方面，对政务数据的共享进行了规定，本文拟通过“十问十答”的方式，对《条例》相关内容进行解读。

一、基础信息锚点

（一）什么是政务数据?

《中共中央、国务院关于构建数据基础制度更好发挥数据要素作用的意见》（下称“《数据二十条》”）将数据分为公共数据、企业数据、个人数据三种，其中，公共数据指各级党政机关、企事业单位依法履职或提供公共服务过程中产生的数据。而政务数据指的是政府部门在依法履行职责过程中收集和产生的各类数据，但不包括属于国家秘密、工作秘密的数据。因此，政务数据是公共数据的一部分。

（二）什么是政务数据共享?

指的是政府部门因依法履行职责需要，使用其他政府部门的政务数据或者为其他政府部门提供政务数据的行为，不仅包括同级政府部门之间政务数据互相提供和使用，也包括上级政府部门向下级政府部门回流数据。

（三）《条例》适用的主体有哪些?

1、统筹协调-政务数据共享主管部门
行政级别主管：国务院（负责全国）及县级以上（负责本行政区域）地方主管部门负责统筹协调政务数据共享工作，如，明确数源部门、对政务数据共享争议进行协调处理；
行业主管：国务院各部门负责本部门政务数据共享工作，协调指导本行业、本领域政务数据共享工作。

2、执行办事-政务数据工作机构（内设机构）
政务数据提供部门、数源部门：负责具体执行政务数据目录编制或更新、政务数据共享审核、提供等；
政务数据需求部门：按《条例》要求使用共享获取的政务数据，履行安全管理责任。

3、其他利益相关主体
政府部门的受托方：如技术供应商，需履行数据安全义务；
数据来源主体：公民、法人和其他组织，有权对政务数据共享侵权行为进行投诉、举报。

二、实操应对指南

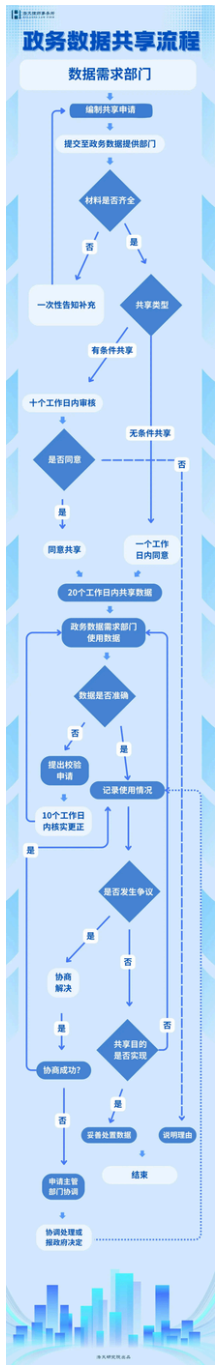
（四）《条例》实施前，政府部门要做的事情?

梳理本部门政务数据，建立健全数据共享工作制度，明确工作机构、工作部门及职责，对照《条例》要求编制和更新政务数据目录，做好数据安全和个人信息保护制度建设，为《条例》正式实施做好准备。

（五）编制政务数据目录的意义?

在政府各部门开展政务数据共享之前，需提供部门按《条例》要求编制、更新政务数据目录，并由同级政务数据共享主管部门审核发布。政务数据目录应当明确数据目录名称、数据项、提供单位、数据格式、数据更新频率以及共享属性、共享方式、使用条件、数据分类分级等信息。其作为政务数据全国统一的“法定登记簿”，能够明确数据权属与责任主体，规范数据共享合规边界，保障数据安全、时效与质量。

（六）政务数据共享流程?



三、延伸与影响

（七）政务数据共享下，如何确保政务数据安全?

1、明确安全责任原则
谁管理谁负责：数据提供部门对数据来源、分类分级、共享属性界定负责。
谁使用谁负责：数据需求部门对使用过程中的篡改、泄露、非法利用等行为担责。

2、数据分类分级保护
目录关联分类分级：编制目录时必须标注数据分类分级。
差异化防护措施：按分级采取防篡改、防泄漏等技术措施。
安全评估前置：目录编制前需完成保密及个人信息保护风险评估。

3、全生命周期安全管理体系
收集环节：禁止重复收集，数源部门统一管理。
共享与使用环节：禁止擅自扩大使用范围或转给第三方，扩大使用范围需提供方同意，使用场景、存储销毁记录保存三年以上。
销毁环节：共享目的达成后需按提供方要求妥善处置数据。

4、建立安全事件应急机制

5、严控第三方受托安全风险
委托方需审批委托项目，明确技术标准，监督受托方。
受托方不得擅自访问、留存、泄露数据。

6、强化个人信息保护
共享涉及个人信息时，必须遵守《个人信息保护法》及《网络数据安全管理条例》。
公民有权投诉侵权，政府部门需及时处理。

7、健全监督追责机制

（八）《条例》中的创新条款是什么?

1、政务数据目录动态管理
统一目录标准：国务院主管部门制定国家标准，县级以上主管部门组织编制本行政区目录。
分类共享属性：数据分为无条件共享、有条件共享、不予共享三类，明确各共享数据的分类依据、使用条件，防止增设壁垒。
动态更新机制：目录自发生变化之日起需10个工作日内更新（可延5个工作日），主管部门自收到更新后2个工作日内

动态更新机制：目录自发生变化之日起需10个工作日内更新（可延5个工作日），主管部门自收到更新后2个工作日内完成审核并发布，提升时效性。
数据安全评估：按照《网络安全法》《数据安全法》《个人信息保护法》，对收集的政务数据开展保密风险、个人信息保护影响评估等。

2、共享流程优化
明确供需对接时限：无条件共享数据1个工作日内答复，有条件共享10个工作日内答复（可延10个工作日）。
设立数据回流机制：上级部门根据下级部门履职需要，向下级部门“及时、完整”回流数据，不得设限，解决层级数据壁垒。

3、安全与责任创新
数据收集要求：政府部门仅能依据法定职权收集政务数据，且通过共享能获得的数据，不得重复向公民、法人和其他组织收集。
数据使用要求：需求方不得擅自扩大适用范围或将获得政务数据提供给第三方，对于共享目的已实现的情况应按照提供部门要求妥善处置数据，同时对使用场景、过程、成效、存储情况、销毁情况进行记录，并保存至少3年。
校核纠错制度：国家建立统一校核规则，需求部门向提供部门发出校核申请，提供部门应在10个工作日内核实更正数据。
争议解决机制：同级部门之间的争议由同级共享主管部门协调，跨层级、跨地域的争议，由共同上级主管部门协调。协调仍未达成一致的，报本级政府决定。
明确责任机制：谁管理谁负责，谁使用谁负责。

（九）《条例》实施可能面临的难点与建议？

1、主要难点：
协调难题：跨部门、跨层级共享易因权责不清引发争议。
安全风险：数据汇聚、关联增加泄密风险，增加个人信息保护的难度，对政府部门的数据安全风险处理能力是一个考验。
技术壁垒：国务院有关部门政务数据平台、各地区政务数据平台互联互通需成本，政府部门委托参与建设、运行等受托方主体合规能力不足，难以承担数据安全责任。
属性界定模糊：有条件共享类的“使用条件”易被滥用。

2、对策建议：
建立数源部门责任制，明确权责清单，将政务数据共享纳入考核。
政府部门应开展数据分类分级培训，明确“合理使用”边界，增强数据合规及数据安全意识。
相关受托方，应熟悉数据安全相关法律，培训员工数据合规意识。

四、价值总结

（十）《条例》的立法背景与主要意义是什么？

条例》的出台，旨在提升政府数字化治理能力和政务服务效能，全面建设数字政府，进一步落实《中共中央办公厅、国务院办公厅关于加快公共数据资源开发利用的意见》（2024年9月21日生效，下称“《意见》”）第二条提及的“统筹推进政务数据共享，完善政务数据目录，实行统一管理，推动实现‘一数一源’”。此外，从效力层级上讲，该《条例》首次以行政法规形式系统规范政务数据共享的全流程，明确共享原则、管理体制、目录规则、安全责任等核心内容，填补了政务数据共享领域专门立法空白，为政府部门开展数据共享工作提供了具体、可操作的法律依据，让政务数据可以跨层级、跨地域、跨部门、跨业务、安全有序地共享利用。

政务数据相关的法律法规一览表

2016	《政务信息资源共享管理暂行办法》

本办法所称政务信息资源，是指政务部门在履行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表和数据等各类信息资源，包括政务部门直接或通过第三方依法采集的、依法授权管理的和因履行职责需要依托政务信息系统形成的信息资源等。

本办法所称政务部门，是指政府部门及法律法规授权具有行政职能的事业单位和社会组织。

2017	《网络安全法》

国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。（31–39条）

2021	《数据安全法》

政务数据安全与开放。（37–43条）

2021	《个人信息保护法》

国家机关处理个人信息的特别规定。（33条–37条）

2022	《国务院关于加强数字政府建设的指导意见》

建立健全数据治理制度和标准体系，加强数据汇聚融合、共享开放和开发利用，促进数据依法有序流动，充分发挥数据的基础资源作用和创新引擎作用，提高政府决策科学化水平和管理服务效率，催生经济社会发展新动能。

2022	《国务院办公厅关于印发全国一体化政务大数据体系建设指南的通知》

存在主要问题：

1.政务数据统筹管理机制有待完善；2.政务数据共享供需对接不够充分；3.政务数据支撑应用水平亟待提升；4.政务数据标准规范体系尚不健全；5.政务数据安全保障能力亟需强化。

2022	《中共中央、国务院关于构建数据基础制度更好发挥数据要素作用的意见》

建立保障权益、合规使用的数据产权制度；建立合规高效、场内外结合的数据要素流通和交易制度；建立体现效率、促进公平的数据要素收益分配制度；建立安全可控、弹性包容的数据要素治理制度。

2024	《中共中央办公厅、国务院办公厅关于加快公共数据资源开发利用的意见》

统筹推进政务数据共享。完善政务数据目录，实行统一管理，推动实现“一数一源”，不断提升政务数据质量和管理水平。推动主动共享与按需共享相结合，完善政务数据共享责任清单，做好资源发布工作。强化已有数据共享平台的支撑作用，围绕“高效办成一件事”，推进跨层级、跨地域、跨系统、跨部门、跨业务政务数据共享和业务协同，不断增强群众和企业的获得感。

2025	《网络数据安全管理条例》

个人信息处理/委托处理规定。（12条、21条-28条）个人信息共享需遵守其规定。（29条-33条）

2025	《政务数据共享条例》

三、AI文生图：AI生成图片的著作权保护

主笔人



张金栋

北京浩天律师事务所 合伙人
zhangjindong@hylandslaw.com

终于用AI生成了一张满意的图片并发布到网上，但当我发现其他市场主体擅自使用这张图片时，作为AI文生图的“作者”，我能主张权利吗？另一个角度，作为图片的使用者，能随便用这些AI图片吗？更进一步，作为AI图片使用场所的网络平台，是否应把对AI图片的擅自使用视为侵权并履行通知删除义务呢？

随着生成式人工智能（AIGC）技术的日趋成熟，人们使用AI进行创作越发成为日趋流行的新的创作模式。以上问题的本质，是AI生成的“作品”，是否可以视为著作权法上保护的“作品”，创作者到底是AI还是人？

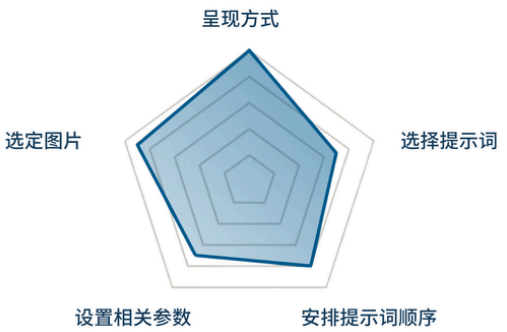
而图片是典型的作品形式之一，同时也是著作权侵权纠纷最高发的作品类型。伴随着AI文生图工具的广泛应用，也自然率先成为了司法实践中讨论最多的“AI作品”。

一、AI生成图片在特定情形下依然被视为作品

《著作权法》第三条规定：“本法所称的作品，是指文学、艺术和科学领域内具有独创性并能以一定形式表现的智力成果。”对于最关键的“独创性”和“智力成果”两个要件，司法界主流观点如下：

（一）需要智力投入的AI生成图片属于智力成果

北京互联网法院认为，由于创作者从构思图片到选定图片，都会进行一定的智力投入，如呈现方式、选择提示词、安排提示词顺序、设置相关参数、选定图片等，因此应被视为智力成果。武汉东湖高新法院认为，案涉的图片与作者创作过程使用的关键词，是否具备关联性，或者说“映射性”，也是判断其是否为作品的关键，这实际上也是在论证智力投入与智力成果的关联。



（二）独创性需要从过程和结果两方面判断

独创性要求作者独立完成并体现出作者的个性化表达，文生图AI并非“按照一定的顺序、公式或结构完成的作品”，不同的人使用文生图AI并不会得到相同的结果，因此并非“机械性智力成果”，这使得其独创性具有了讨论基础。

对于是否有独创性，需要个案讨论，一般而言，从两方面判断：一是过程论，即创作者的创作过程：创作者提出的需求越有差异性，越明确具体，就越能体现出个性化，从而具有独创性；在张家港法院的否定AI生成图片为作品的判决中，也是由于原告无法举证其创作过程导致。二是结果论，以及与已经存在的图片相比，是否具备显著的差异性，可以为独创性提供佐证。其是否为作品的关键，这实际上也是在论证智力投入与智力成果的关联。

二、AI生成图片作者应为AI模型使用者

三、AI文生图：AI生成图片的著作权保护

主笔人



张金栋

北京浩天律师事务所 合伙人
zhangjindong@hylandslaw.com

终于用AI生成了一张满意的图片并发布到网上，但当我发现其他市场主体擅自使用这张图片时，作为AI文生图的“作者”，我能主张权利吗？另一个角度，作为图片的使用者，能随便用这些AI图片吗？更进一步，作为AI图片使用场所的网络平台，是否应把对AI图片的擅自使用视为侵权并履行通知删除义务呢？

随着生成式人工智能（AIGC）技术的日趋成熟，人们使用AI进行创作越发成为日趋流行的新的创作模式。以上问题的本质，是AI生成的“作品”，是否可以视为著作权法上保护的“作品”，创作者到底是AI还是人？

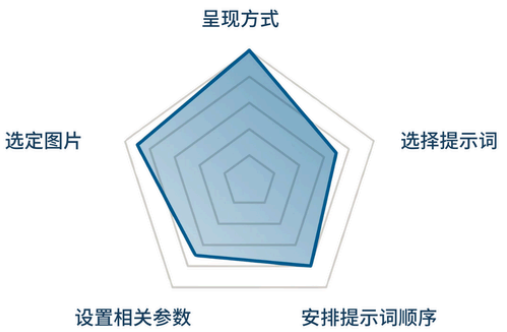
而图片是典型的作品形式之一，同时也是著作权侵权纠纷最高发的作品类型。伴随着AI文生图工具的广泛应用，也自然率先成为了司法实践中讨论最多的“AI作品”。

一、AI生成图片在特定情形下依然被视为作品

《著作权法》第三条规定：“本法所称的作品，是指文学、艺术和科学领域内具有独创性并能以一定形式表现的智力成果。”对于最关键的“独创性”和“智力成果”两个要件，司法界主流观点如下：

（一）需要智力投入的AI生成图片属于智力成果

北京互联网法院认为，由于创作者从构思图片到选定图片，都会进行一定的智力投入，如呈现方式、选择提示词、安排提示词顺序、设置相关参数、选定图片等，因此应被视为智力成果。武汉东湖高新法院认为，案涉的图片与作者创作过程使用的关键词，是否具备关联性，或者说“映射性”，也是判断其是否为作品的关键，这实际上也是在论证智力投入与智力成果的关联。



（二）独创性需要从过程和结果两方面判断

独创性要求作者独立完成并体现出作者的个性化表达，文生图AI并非“按照一定的顺序、公式或结构完成的作品”，不同的人使用文生图AI并不会得到相同的结果，因此并非“机械性智力成果”，这使得其独创性具有了讨论基础。

对于是否有独创性，需要个案讨论，一般而言，从两方面判断：一是过程论，即创作者的创作过程：创作者提出的需求越有差异性，越明确具体，就越能体现出个性化，从而具有独创性；在张家港法院的否定AI生成图片为作品的判决中，也是由于原告无法举证其创作过程导致。二是结果论，以及与已经存在的图片相比，是否具备显著的差异性，可以为独创性提供佐证。其是否为作品的关键，这实际上也是在论证智力投入与智力成果的关联。

二、AI生成图片作者应为AI模型使用者

（一）AI模型本身只是创作工具

AI模型只是创作工具，人使用AI软件作图，就像人使用照相机摄影一样，摄影作品的作者是人而非照相机。

（二）AI模型的设计者也不是作者

如前文提到，文生图AI并非AI模型设计者预先设计好的具有可重复性与可预期性的公式。北京互联网法院认为，涉案人工智能模型设计者既没有创作涉案图片的意愿，也没有预先设定后续生成内容，其并未参与到涉案图片的生成过程中。其作用和角色亦和摄影设备的设计、生产者类似。

（三）AI生成图片的作者应为AI模型使用者

AI生成图片的作者，应为使用AI模型进行图片创作的人。作品的智力投入和独创性，均是主要来自于AI模型的使用者。这一结论也是不言而喻的。

三、两个锦囊——当前司法实践下的相关方建议

以上为目前司法实践中对于AI生成图片的著作权保护的主流观点，法院较为倾向支持图片的作品属性和AI模型使用者的权利。但由于这一领域技术迭代迅速，同时个案具体事实和证据情况不一，也存在文生图创作者的败诉案例。

在当前背景下，对于AI文生图的创作者而言，如果有意对相关作品做商业开发，我们提供以下两个实务锦囊：

（一）锦囊一

一定要在创作过程中尽可能多地给AI提供信息和修改意见，提出修改意见的次数越多越好，修改的内容越具体越好，从而体现自己的独创性；

（二）锦囊二

对于自己的创作过程，一定要注意留证，可以使用时间戳软件录屏的方式进行，否则想要在法庭再现创作过程是很难的。

自然地，对于图片的使用者而言，即使是网络上公开的AI生成图片，使用也应谨慎，尽可能取得创作者的授权，避免可能的侵权责任。

四、稳定币：涵义释义及监管分析

主笔人





郭远程

北京浩天律师事务所 合伙人
浩天数字科技与互联网行业委员会 牵头合伙人
guoyuancheng@hylandslaw.com

陈青青

北京浩天律师事务所 律师
chenqingqing@hylandslaw.com

2025年5月21日，香港立法会宣布《稳定币条例草案》（下称《条例》）正式通过，标志着亚洲金融中心在数字资产监管领域迈出了关键一步。本文将从稳定币的涵义及特殊地位、《条例》的核心内容及其对市场的潜在影响等多个维度解析这一监管框架。

一、稳定币涵义释义与其特殊地位

稳定币是一类特殊的数字资产，其主要特征是可以维持（或声称可以维持）与法币价值 1:1 的锚定关系，目前主流的稳定币为与美元锚定的各类型美元稳定币。根据维持币值稳定的方式不同，市场上主流稳定币大致可以分为三类：

1. 法币抵押，以 USDT、USDC 为代表，其币值维持方式为发行方储备了对应的法币资产。
2. 超额抵押，如 DAI，其币值维持方式为发行方储备超过所发行的稳定币价值的比特币、以太币等加密货币。
3. 算法稳定，代表是已经归零的 UST，重要特征是通过算法机制维持价格稳定。

*除了上述类型稳定币，在 2024 年问世目前仅仅经过一年市值就已经挤入前三的 USDe，采取了"做多现货+做空期货合约"方式对冲底层数字货币的价格波动，维持整体投资组合价值的稳定，也可以认为某种合成稳定币。

目前前十大市值的稳定币清单如下：

Name	Chains	% Off Peg	1m % Off Peg	Price	1d Change	7d Change	1m Change	Market Cap
1 Tether (USDT)	+91	+0.10%	+0.10%	$1	+0.10%	+0.92%	+3.49%	$156.19b
2 USD Coin (USDC)	+10	-0.03%	-0.03%	$1	-0.14%	+0.24%	+0.99%	$60.717b
3 Ethena USDe (USDe)	+16	0%	+0.30%	$1	-0.03%	+0.55%	+23.84%	$5.894b
4 Dai (DAI)	+42	0%	+0.10%	$1	-0.74%	+1.99%	-2.33%	$4.412b
5 Sky Dollar (USDS)		-0.02%	-0.04%	$1	-1.66%	-0.27%	+11.07%	$3.98b
6 BlackRock USD (BUIDL)		0%	-	$1	+0.01%	-0.43%	-0.61%	$2.88b
7 World Liberty Financial...		+0.10%	-0.93%	$1	+0.10%	+0.45%	+2.87%	$2.191b
8 Ethena USDtb (USDTB)		0%	-0.03%	$1	-0.04%	+0.01%	+1.11%	$1.456b
9 First Digital USD (FDU...		-0.11%	-1.01%	$1	-0.25%	-5.12%	+0.44%	$1.255b
10 PayPal USD (PYUSD)		-0.06%	-0.10%	$1	+1.39%	+2.13%	+19.15%	$998.41m

* 上表中排名第 6 的 BUIDL 是由全球最大的资管公司贝莱德发行（*注：该项目并非传统意义上用于流通的稳定币而是更接近以美债作为底层的 RWA 项目），排名第 7 的 USD1 是由特朗普家族公司所发行。

2025 年是稳定币相关议题快速发展的一年。越来越多的传统企业开始进入到稳定币市场，同时，也有越来越多的国家和地区开始准备稳定币相关立法，比如本文所述的香港通过《稳定币条例草案》、美国正在进行的《GENIUS ACT》、韩国执政党所推动的《数字资产基本法》草案等。随着本月 USDC 的发行商 Circle 在纳斯达克正式上市，稳定币和稳定币话题的讨论度更是达到了顶峰。

最初，稳定币主要作为传统金融与加密世界的媒介。但近些年，稳定币已经突破传统加密货币领域，已经逐渐在全球支付、跨境汇款领域发挥着重要作用，主流稳定币的日交易量甚至超过重要法定货币。稳定币基于其特性，为全球跨境支付提供低成本替代方案，并为企业提供国际结算和财资管理的数字化选项。

但同样，稳定币的运作机制也让其本身蕴含着系统性风险，特别需要注意的是稳定币脱离传统金融监管体系，可能被犯罪集团用于电信诈骗、人口贩卖、洗钱等等犯罪活动；另外由于稳定币发行人缺乏透明度、赎回机制不明确、

资金流向难以追踪等问题，也增加了用户资产安全风险。

在此背景下，香港政府及时推出《稳定币条例草案》，旨在通过建立发牌制度、设定储备要求、强化信息披露和确保赎回权利，为稳定币市场提供明确的监管框架，既控制风险又促进创新。

二、稳定币《条例》下的定义及监管范围

（一）稳定币（stablecoin）和指明稳定币（specified stablecoin）的法律界定

在概念上，《条例》中包括"稳定币"和"指明稳定币"两类。其中"稳定币（stablecoin）"仅仅指价值稳定的加密货币，而不一定与法币币值挂钩；在稳定币的概念之下，如果该稳定币还是锚定或参考法币或者另行被监管特殊指定的，那么就构成了"指明稳定币"。因此，条例中的"指明稳定币"的概念更符合我们惯常所理解的，与法币币值挂钩的加密货币的概念。

具体而言，符合以下特点的数字资产即为稳定币：



在稳定币的概念之上，还具有以下特定的稳定币即为指明稳定币：

(1)与法币挂钩，即价值锚定或参考法币；或
(2)由金融管理专员按照《条例》规定指定的稳定币。

《条例》各项合规要求主要针对"指明稳定币"。

（二）稳定币监管主体及受监管范围

根据《条例》的规定，稳定币的监管由金融管理专员统一监管。金融管理专员的办公室称为香港金融管理局（下称“金管局”），金融管理专员即为金管局的总裁。金融管理专员在《条例》下的核心职能包括审批、颁发及撤销稳定币活动牌照；对牌照附加条件；针对境外发行的稳定币，认定某一个特定主体作为发行实体，接受《条例》的监管；行使调查、执法及制裁权；处理复核等。

《条例》监管适用范围较广，除了属地管辖，管理在香港发行的指明稳定币外，也包括保护性管辖，任何针对香港公众积极推广或进行稳定币活动，或者发行任何参照港元的指明稳定币，无论该行为发生在香港境内或境外，均应当受到《条例》管辖。管辖范围具有典型的域外管辖属性。

三、发牌制度与准入门槛

（一）发牌机制以及申请发行稳定币的资格

《条例》建立的发牌制度，成为整个监管框架的支柱。申请发行稳定币的主体是依据《公司条例》第 622 章注册的公司法人，在香港以外成立为法团的认可机构（如持牌银行），但个人、合伙制企业、非公司实体不可申请。针对在境外发行的指定稳定币，为了解决 web3 领域经常发生的主体不明的情况，《条例》特别给了金融管理专员认定一个主体作为发行实体的权利，使得当香港监管机构需要对某一指明稳定币进行管理时，能够确保可以指定一个主体接受监管。

（二）发牌的核心审批条件

任何计划在香港发行稳定币的实体必须获得金管局颁发的专门牌照，牌照申请需满足所有最低准则，包括财务稳健、合格的公司治理与人员资质以及完善的运营和风险管理等。详见下图：



四、储备与资产托管要求

（一）储备资产（ reserve assets ）及安全性要求

储备资产是指支持该指明稳定币实现价值稳定的资产，该资产应当保证兑现对稳定币的赎回要求。作为对安全的回应，《条例》对储备资产管理提出了全面要求，要求指明稳定币的储备资产限于“高质素及高流动性，且具最低投资风险”。

香港金融管理局在《银行业（流动性）规则》中为银行设定了高质素流动资产（HQLA）的标准包括流通纸币及硬币、可提取央行储备、高评级主权债券、高流动性企业债券，在此基础上同时满足“最低投资风险”才可以构成合格的储备资产。任何高风险或波动性大的资产都不再具备作为储备资产的可能性，比如加密货币（如比特币、以太坊）、非流动性资产（如房地产、私募股权）、持牌人自身发行的证券或债务、高风险衍生品。

（二）独立托管与的储备管理

《条例》明确禁止将储备资产用于以下活动：发放贷款或提供信贷、进行杠杆投资或投机性交易、购买风险较高的资产（如公司债券、股票或加密资产）、作为任何形式的抵押品或担保。为确保储备资产的安全，《条例》要求储备资产必须由合格的第三方托管机构持有，并通过法律安排与发行人的其他资产严格隔离，确保在发行人财务困境时储备资产不受影响，禁止持牌人自行保管或控制储备资产。若持牌人破产，储备资产优先用于兑付稳定币持有人。

《条例》还对储备管理政策提出了要求，发行人必须制定详细的储备管理政策，包括资产配置策略、流动性管理计划、风险控制措施和应急处置方案。这些政策需经金管局审批，且需定期审查更新。

五、投资者保护与透明度要求

《条例》构建了多层次投资者保护体系，包括强制兑付机制、储备资产优先求偿权、欺诈行为刑事化（最高 10 年监禁）及多元救济渠道。核心是赋予持有者法定赎回权，要求持牌人在切实可行的范围内尽快完成赎回，并要求持牌人相应技术支持与应急预案，确保持有者能随时按面值兑换回法定货币。此外，《条例》单独提出了透明度保护要求。要求发行人每季度发布经独立审计的储备资产报告、每日更新稳定币流通量、及时披露重大事件、规范营销沟通禁止误导宣传。

六、市场影响与未来展望

《条例》的通过将对数字资产市场各方产生深远影响。对监管部门而言，一方面是对稳定币这一重大资产类别的细致监管；另一方面更意味着，监管对于满足合规要求的稳定货币的接纳与认可。

对稳定币发行人而言，新规意味着需要全面审视现有业务模式和合规状况，重新配置储备资产结构，加强内部治理框架，准备详细的牌照申请材料。虽然短期内合规成本可能增加，但长期来看，监管合规将成为建立市场信任和竞

争优势的关键因素；对传统金融机构而言，除了基于合规产生的，银行可为持牌稳定币发行人提供储备托管服务，审计与法律机构可开发针对稳定币的专业合规服务，支付服务提供商则有机会探索与稳定币系统的互操作性，也意味着可以在政府监管下逐步进入稳定币乃至加密货币业务领域；对投资者和用户而言，《条例》带来了更高的保障和确定性，他们可以通过选择获得监管牌照的稳定币、关注储备透明度报告以及了解不同产品的风险特征来做出更明智的决策。

《条例》的通过是特区政府数字资产监管领域的重要里程碑，不仅填补了香港数字资产监管的空白，更在于它为全球稳定币监管提供了一个兼顾实用性与前瞻性的范例。《条例》有望吸引全球高质量稳定币项目落户香港，加强香港作为数字资产枢纽的地位，并为传统金融机构与数字创新的融合创造更多可能性。随着数字经济深入发展，这一监管框架将持续发挥引领作用，推动香港在全球数字金融竞争中保持领先地位。

五、信息保护：一张清单看懂《个人信息保护合规审计办法》

主笔人



邢丹丹

科技上市公司 法务
浩天研究院 行业顾问

在数字化浪潮席卷全球的今天，个人信息已成为比黄金更珍贵的资源：企业搜集、利用用户、客户、员工信息，智能化、定制化推荐产品服务，优化算法销售逻辑、强化部门管理……信息数据早已成为企业生产资料的关键要素，信息保管也自然成为企业面临的重要课题。

然而，现实中，第三方软件漏洞导致企业员工数据沦为黑产商品；黑客利用医疗平台弱口令漏洞，恶意窃取患者信息；出行平台跨境传输疏漏，导致千万用户信息在境外网络上裸奔，更有不法分子以此实施诈骗犯罪……我们不得不追问：“数字化”“信息化”的今天，企业如何在数据安全的考场上交出满意答卷？

我国早在2021年11月1日，就已经出台了《中华人民共和国个人信息保护法》（以下简称“个保法”），时隔三年有余的时光，数据合规从街头巷尾热议的话题，渐渐归于平淡。虽然几乎任何一位从事APP开发的技术人员，对于“个人信息收集必须经用户同意”等的基本操作，已是驾轻就熟；企业也在内部管理中积极进行个人信息保护评估，在外部运营中获取各类个人信息保护相关认证，为数据合规背书。但是合规治理的闭环始终是“评估——认证——审计”；《个人信息保护法》的第五十四条也明确要求，“个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计”。

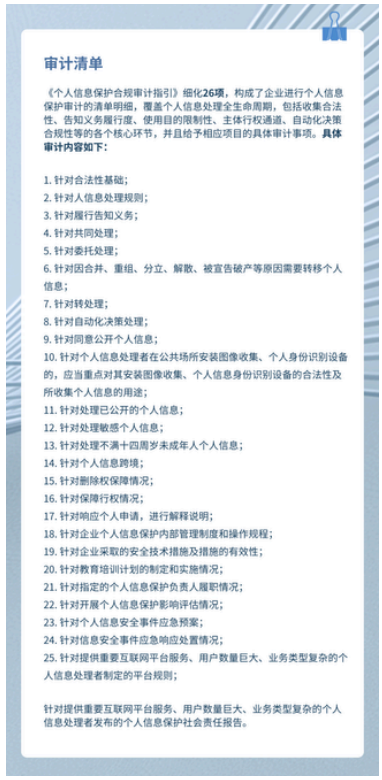
在此背景下，国家网信办于2025年2月14日正式发布《个人信息保护合规审计管理办法》（下称“审计办法”），自2025年5月1日起施行。

根据《办法》要求，在日常业务中凡涉及处理个人信息或者用户信息的企业，特别是处理超过1000万人个人信息的个人信息处理者，至少应每两年按照本《办法》的要求至少开展一次个人信息保护合规审计。

值得一提的是，当个人信息处理活动存在严重影响个人权益、严重缺乏安全措施等较大风险，或可能侵害众多个人的权益，或发生个人信息安全事件，导致100万人以上个人信息或者10万人以上敏感个人信息泄露、篡改、丢失、毁损时，若未按保护部门要求，依据本《办法》委托专业机构进行合规审计，或未为专业机构提供必要支持、未按时完成审计、未报送审计报告及整改情况报告等，均可能违反办法规定。

以下用一张清单方便读者“初识”该审计办法的核心内容。

条款性质	条款编号	主要内容
概念	2	个人信息保护合规审计，是指对个人信息处理者的**个人信息处理活动是否遵守法律、行政法规的情况**进行审查和评价的监督活动
适用范围	2	（地域范围）我国境内
	19	（排除范围）**国家机关和法律、法规授权的具有管理公共事务职能的组织**处理个人信息的，不受本办法管辖
审计依据	2	仅限于法律、行政法规的要求
审计对象&频次	4	处理**超过1000万人**个人信息的个人信息处理者，特别强调审计频次：**两年一次。** 处理不足1000万人个人信息的个人信息处理者定期审计。（定期合理性：以业务功能的更新周期以及发生风险事件的概率而确认）
审计方式	3	**自行审计：**内部机构或者委托专业机构 1.但**不能连续三次**自行审计； 2.内部应设立个人信息保护负责人；
	4 5 10 11	**按照要求审计：**委托专业机构审计 **1.开展情形：** （1）严重影响个人权益或者严重缺乏安全措施等较大风险； （2）可能侵害众多个人的权益； （3）导致100万人以上个人信息或者10万人以上敏感个人信息泄露、篡改、丢失、毁损。 **2.“一事不再审”：** 对同一个人信息安全事件或者风险，不得重复要求个人信息处理者委托专业机构开展个人信息保护合规审计。 **结果：**向保护部门报送审计报告以及整改报告。
审计机构的要求	7 8 13 14 15	**性质：**尚未确认； **原则性要求：**遵守法律法规，诚信正直，公正客观； **硬件要求：**审计人员、场所、设施和资金； **义务：**保密职责； **限制1：**不得转委托； **限制2：**不得连续三次以上审计同一对象； 企业承担费用。
保护部门的职责	18	**行政责任：**违反本办法规定的，依照《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律法规的规定处理； **刑事责任：**构成犯罪的，依法追究刑事责任。



审计清单

《个人信息保护合规审计指引》细化**26项**，构成了企业进行个人信息保护审计的清单明细，覆盖个人信息处理全生命周期，包括收集合法性、告知义务履行度、使用目的限制性、主体行权通道、自动化决策合规性等的各个核心环节，并且给予相应项目的具体审计事项。**具体审计内容如下：**

1. 针对合法性基础；
2. 针对人信息处理规则；
3. 针对履行告知义务；
4. 针对共同处理；
5. 针对委托处理；
6. 针对因合并、重组、分立、解散、被宣告破产等原因需要转移个人信息；
7. 针对转处理；
8. 针对自动化决策处理；
9. 针对同意公开个人信息；
10. 针对个人信息处理者在公共场所安装图像收集、个人身份识别设备的，应当重点对其安装图像收集、个人信息身份识别设备的合法性及所收集个人信息的用途；
11. 针对处理已公开的个人信息；
12. 针对处理敏感个人信息；
13. 针对处理不满十四周岁未成年人个人信息；
14. 针对个人信息跨境；
15. 针对删除权保障情况；
16. 针对保障行权情况；
17. 针对响应个人申请，进行解释说明；
18. 针对企业个人信息保护内部管理制度和操作规程；
19. 针对企业采取的安全技术措施及措施的有效性；
20. 针对教育培训计划的制定和实施情况；
21. 针对指定的个人信息保护负责人履职情况；
22. 针对开展个人信息保护影响评估情况；
23. 针对个人信息安全事件应急预案；
24. 针对信息安全事件应急响应处置情况；
25. 针对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者制定的平台规则；

针对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者发布的个人信息保护社会责任报告。

从细节角度出发，通过清单可以明确知晓，本审计办法的基本结构，以及作为个人信息处理者的企业对于进行审计的方式、审计机构的挑选、审计的强制性；同时，也清楚的发现，本审计办法最值得关注的部分是附件“个人信息保护合规审计指引”，此附件不单是审计开展的内容，当时也是反向回顾业务进行个人信息处理的合规要点。若企业可以将基础个人信息保护融入点滴业务中，扎牢基础合规的篱笆，那应对此次合规审计是事半功倍。

从宏观趋势看，本审计办法的出台可管中窥豹，未来个人信息保护合规的发展方向，绝不是仅在用户端的形式合规和隐私政策的具备，而是渗透进企业后台，严格监督监管实质合规，充分发挥合规效用。

六、数据资产：为何数据资产入表是企业的必选项?

主笔人



叶建芳

京浩天（杭州）律师事务所 主任
yejianfang@hylandslaw.com



吕文易

北京浩天（杭州）律师事务所 律师
lvwenyi@hylandslaw.com



王芬芬

北京浩天（杭州）律师事务所 律师
wangfenfen@hylandslaw.com

数据资产入表并非简单的财务技术操作，也不是简单响应政策要求的形式化工作，而是企业拥抱数据要素市场化配置新纪元、构筑核心竞争力的战略举措。从合规及价值视角审视，意义尤为深远。

一、响应国家政策与隔离法律风险——主动合规的价值

（一）融入国家数据要素市场大局

自从2022年12月19日党中央、国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》，“数据二十条”可谓是构建了数据基础制度的 “四梁八柱”。数据资产入表是企业积极参与国家数据要素市场建设、避免被边缘化的主动作为。各地数据交易所的配套规则是具体的操作指南，如《上海数据交易所数据交易安全合规指引》《深圳数据交易所数据交易合规评估实施细则》等。

（二）法律风险隔离与成本节约

1. 确权前置，避免天价索赔：明确权属可有效预防后续权属纠纷引发的巨额赔偿（如美国某医疗 AI 公司因获取数据未确权面临大额索赔），入表前的确权工作是重要的风险预防性投资。
2. 合规设计，降低监管处罚风险：通过入表流程的系统性合规审查，可大幅降低因数据滥用、侵犯隐私、危害安全等引发的行政处罚及声誉损失风险，先行合规成本远低于后期违规代价。

（三）应对国际规则挑战

对于涉及跨境业务及未来有跨境业务需求的企业，不仅需要符合中国法规的数据治理与入表实践，也是应对 GDPR 等国际规则的重要基础。

二、释放数据要素的财务价值——合规前提下的价值显性化

（一）资产显性化与报表优化

1. 财务报表结构优化：将符合条件的数据资源从 “费用化” 支出转化为表内资产（无形资产 / 存货），可以显著改善资产负债表结构（如山东黄金案例：资产负债率下降 2.1%），此过程高度依赖前期确权与合规审查的扎实性。
2. 提升财务透明度与可信度：经严格法律合规审查和第三方评估审计入表的数据资产，可以向市场传递企业规范治理的信号。

（二）优化企业估值与融资基础

1. 增强投资者信心：市场对拥有高价值、权属清晰、合规数据资产的企业将给予估值溢价（科创板表现尤为明显）。入表数据是可验证、受监管的硬实力体现。
2. 夯实融资抵押基础：合规入表的数据资产是获得银行信贷（如浙江侠云科技、贵州万峰林集团案例）或资本市场融资的重要增信手段。《可入表数据资源信贷融资基础要求》团体标准（T/CECC 36–2025）的出台，正是为银行接受此类抵押品提供了法律与操作框架。

三、驱动数据要素市场化流通——法律为交易奠基

（一）为数据定价提供法律背书

入表过程包含的确权、合规审查、第三方评估，是数据资产获得市场公允定价的核心前提，极大降低交易摩擦，北京数交所交易量 300% 增长正是对此的有力说明。

（二）激活多层次数据金融

数据资产质押、证券化等创新金融工具的应用，均以数据资产的权属清晰、价值可评估、合规无瑕疵为法律基础。入表是打通 “数据资源→数据产品→数据资产→数据资本” 闭环的关键一步。

四、满足财务合规与战略需求——规避法律风险

（一）响应会计准则的强制性要求

财政部《企业数据资源相关会计处理暂行规定》（财会〔2023〕11号）于2024年初已生效，企业需按要求对符合条件的数据资源进行会计处理。合规入表是满足监管要求、避免会计风险的必然选择。

（二）优化资本结构，响应国资监管

对于国企（如成都金牛城投、山西建投案例），数据资产入表有助于降低资产负债率，符合国资委对优化资本结构、盘活新型资产的要求。

（三）构建数据战略的法律护城河

1. 内部治理升级：入表要求倒逼企业建立体系化、合规化的数据治理框架（分类分级、权限管理、安全防护、合规审计），这本身就是核心竞争力和风险防控能力的提升。
2. 提升产业链话语权：拥有标准化、权属清晰、合规的数据资产，显著增强企业在合作、并购中的议价能力（如宁德时代案例）。数据资产成为可计量、可交易的法律权利载体。

五、总结

数据资产入表是一项法律合规先行、跨专业协作、动态持续管理的系统工程。其核心价值不仅在于财务报表的优化，更在于通过法律确权与合规赋能，使数据资源真正成为企业可控制、可计量、可流通、可变现的核心战略资产，并为企业在强监管时代构筑风险防线。成功的入表实践（如山东黄金、东营水务、莱州公交、贵州文旅等）无不印证：前期扎实的法律确权与合规审查是价值实现的基石，贯穿始终的法律风险防控是资产可持续性的保障。

随着政策与市场的双重深化，企业更需依托专业律师团队，构建覆盖“权属锁定-价值评估-资产运营”的全流程合规架构，确保数据价值安全转化。

参考资料：



里程碑意义！浙江首单制造业“数据产品”在台州成交



数据资产如何变成真金白银



拓宽融资渠道 文旅抢跑数据资产入表



数据价值化：下一个财富之源



“无形数据”化“有形资产” 天津市首单数据资产信托融资业务落地

七、城投公司：转型中虚拟电厂业务的数据风险

主笔人



董文浩

北京浩天律师事务所 高级合伙人
dongwenhao@hylandslaw.com



吴梦瑶

北京浩天律师事务所 合伙人
wumengyao@hylandslaw.com

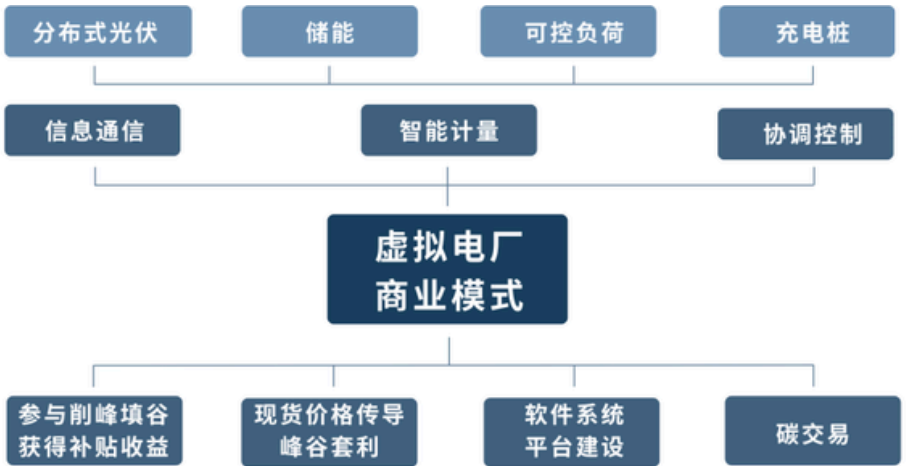
虚拟电厂(VirtualPower Plant,VPP)作为新型电力系统的重要组成部分，为城投公司提供了业务多元化、资源价值提升与城市能源服务能力升级的战略机遇，正成为能源领域的技术高地与投资热点。然而，城投公司开展虚拟电厂业务时若忽视数据合规性，除将触发安全事故，面临罚款、行政处罚、刑事责任，被排除于政策红利之外严等重后果，最直接的危害就是市场失信和经济损失。

因此，城投公司在开展虚拟电厂业务时，需注意数据这一新质生产力在采集、使用、传输、储存、销毁等全生命周期中的合规性，以免引发国有资产流失、诉讼纠纷、行政处罚、刑事犯罪等情形。

一、升级产业结构，落实化债政策

2023年9月国办印发《关于金融支持融资平台债务风险化解的指导意见》，城投公司转型拉开帷幕。城投公司通过参与虚拟电厂建设、运营，可以依托传统基础设施建设和公用事业运营，向智慧能源、综合能源服务等新兴领域拓展，优化升级产业结构、增加营业收入的同时，还可以将运营过程中产生的数据资产确权入表，提高企业在资本市场融资的地位，进一步落实化债政策。

根据GB/T 44241-2024《虚拟电厂管理规范》，虚拟电厂系通过先进的信息通信技术、智能计量及优化控制技术，将分布式电源、分布式储能、可调节负荷等分布式资源进行集成，构成能响应电网需求、参与电力市场运行或接受电网调度的系统，其原理为利用物联网技术以及算法技术将分布式能源、储能设备、可调负荷和其他可控资源虚拟聚合成一个整体，形成可灵活调度的用电单元，提高消纳能力同时实现对电网的协同支撑。其商业运营模式见下图：



通过虚拟电厂商业模式，城投企业可参与需求响应、辅助服务及虚拟电厂响应，获得政府补贴收益，还可结合虚拟电厂的价格预测、负荷预测，预估现货低价时段，通过智能微网(充电网、储能网)技术+交易，实现电量时序转移。

二、产业升级的关键——完成四个数据合规动作

城投公司若想通过虚拟电厂业务完成产业升级，那么需关注虚拟电厂运营过程中数据采集与使用、数据确权、数据处理、数据安全四个维度的法律风险。

动作一：数据采集与使用应取得同意

虚拟电厂在运营的时候需采集负荷端工商业用户、居民用户以及其他用户的设备运营数据、用电数据等信息，可能涉及个人信息或企业商业秘密，为确保虚拟电厂采集用户数据的合法性与正当性，一般在虚拟电厂运营商与聚合用户方签署的合同中会约定数据的采集与使用条款，如：“虚拟电厂利用大数据分析用户历史用电数据，结合自身能源储备与调配能力，为用户定制个性化能源供应计划”，“虚拟电厂应严格保护用户提供的用电数据、商业机密等信息，未经用户书面同意，不得向任何第三方泄露”，“双方应对在合作过程中知悉的对方商业秘密、技术秘密、用电数据、用户信息等予以保密”。除此之外针对居民用户等个人信息部分，在数据采集开始，应按照《个人信息保护法》第十三条、十七条、第二十八条、第二十九条、第五十五条规定，向用户告知个人信息处理事项、取得个人的单独同意、事前进行个人信息保护影响评估、事中事后进行个人信息合规审计等。

动作二：数据资产权属应约定明确

不同于一般资产所有权可以归为一个主体的情形，数据资产的持有权、使用权、收益权等主体往往交织在一起难以确定。目前在司法实践中，并无明确唯一标准对数据资产权属进行直接确认，多借以《反不正当竞争法》等部门法予以解释进而判定。如杭州车厘子智能科技有限公司（以下简称“车厘子”）与北京恒誉新能源汽车租赁有限公司（以下简称“恒誉公司”）等不正当竞争纠纷案，法院认为，用户数据由车厘子和恒誉公司共同收集产生，生成数据存储于车厘子数据库之中，恒誉公司有权随时获取相关数据，双方未对用户数据使用作出明确约定，存储数据并采取保密措施的实际控制者即车厘子是商业秘密的权利人，恒誉公司使用用户数据行为不构成对商业秘密的侵犯。



杭州车厘子智能科技有限公司与北京恒誉新能源汽车租赁有限公司、北京轻享科技有限公司不正当竞争纠纷案

案件概要（时间线）

❍ 2014年9月29日 恒誉公司与车厘子公司签订《软件系统租用协议》，租用后者开发的汽车分时租赁系统，租期至2017年9月25日。

❍ 2015年1月 恒誉公司提出借用会员资源，车厘子公司同意但未明确有偿使用条款。

❍ 2017年8月 恒誉公司向"车纷享"会员发送短信，要求会员退款并转至新平台。恒誉公司与车厘子公司协商系统切换及会员数据归属，未达成一致。

❍ 2017年9月 恒誉公司通过微信公众号、官网发布"免押金租车"等宣传信息，使得会员转移至"轻享出行"平台。《软件系统租用协议》到期，双方未续约。

❍ 2017年10月10日 恒誉公司与轻享公司签订《分时租赁平台服务合作协议书》。

❍ 2018年1月 车厘子公司申请公证保全恒誉公司发送短信及宣传行为的证据。

❍ 2019年 车厘子公司向北京市西城区法院起诉，一审败诉。

❍ 2020年5月 车厘子公司上诉至北京知识产权法院，二审维持原判。



同样的，虚拟电厂运营商在运营的时候会涉及多方主体。如数据采集过程中的数据来源者（负荷端用户、发电企业等）对所提供的数据拥有“所有权”，该权利体现为对所提供的信息的查阅、更正、删除等权利；数据处理者（虚拟电厂或其委托的第三方那个技术企业/个人）进行数据处理而享有的数据资产持有权；设备厂商存储生成数据并采取保密措施确保数据安全等。因此，若虚拟电厂运营商未与数据来源者、数据处理者、设备厂商等主体签署相关协议，可能会引发权属纠纷以及其他侵权责任纠纷。若该数据资产最终要并入城投公司财务报表中，还可能引发国有资产流失风险。

动作三：数据处理纠纷应做好证据保全

虚拟电厂的本质是资源聚合、智能调度、等效参与电网运行，其中智能调度是自动化决策过程，即虚拟电厂的调度算法。《个人信息保护法》第二十四条、欧盟《通用数据保护条例》第二十二条以及欧盟《人工智能法案》，都提及了当控制者进行自动化个人决策（包括分析）时，受影响的人有权获得解释。因此，在虚拟电厂运营过程中，如果系统误判用户负荷需求，导致电力供应中断，或者因用户私自改变用电模式、设备故障、通行不畅、信息报错等原因导致系统误判，其中产生的直接与间接损失该由谁承担，承担比例为多少、举证责任如何界定，将是虚拟电厂未来运营中面对的主要争议风险。目前我国司法实践一般会从证据三性以及合同约定的角度认定责任承担，因此此种纠纷除完善合同约定外，还应及时申请证据保全。

动作四：运营商应采取数据安全保护措施

根据《网络安全法》《数据安全法》以及《关键信息基础设施安全保护条例》，虚拟电厂属于关键信息基础设施，其数据泄露，可能严重危害国家安全、国计民生、公共利益，如运营者未按照要求采取安全保护措施或者采取保护措施不到位，将会面临行政处罚；如危及到国家安全，或会涉及刑事犯罪，且其定罪量刑与运营者是否按照要求采取安全保护措施有关。

三、数据合规——悬在城投企业虚拟电厂业务之上的达摩克利斯之剑

虚拟电厂日后将逐步成为各地电力交易市场主体，届时，不管是电力相关数据的确权入表，还是虚拟电厂带来的收益，都会进一步丰富城投公司营收，落实国家化债与转型要求。但该业务中涉及的数据确权、争议纠纷以及数据安全等问题，都会影响资产收益。因而虚拟电厂业务中的数据合规，恰似城投公司当年依赖的土地财政杠杆——既是切入新领域的“必要支点”，也成为高悬头顶的“达摩克利斯之剑”，稍有不慎便可能重蹈债务风险的覆辙。

八、数据没有“所有权”：数据由“资源”变成“产品”的关键

主笔人



董皓

北京浩天（上海）律师事务所 高级合伙人
浩天数字科技和互联网行业委员会 牵头合伙人
donghao.sh@hylandslaw.com



李佳陆

北京浩天律师事务所 律师助理
lijialu@hylandslaw.com

数字化浪潮席卷全球，数据已成为推动社会创新与经济增长的核心要素。数据的法律属性及其归属问题一直争论不断。特别是在公共服务业领域，国家机关、事业单位在履职过程中产生的大量数据，并不能以传统的“所有权”逻辑加以界定，其合理利用的核心在于合规改造和规范管理。

一、“所有权”概念不符合数据的现实特点

我国《民法典》第一百二十七条确认了数据等虚拟财产受到一定程度的法律保护，但并未明确赋予数据以物权编意义上的“所有权”属性。数据具备高度可复制性和非排他性，这与物权编对于“物”的唯一性、排他性等基本特征相悖。如果坚持用物权意义上的“所有权”类比数据控制者对数据的权益，这种“所有权”将无法与既有的秩序相融合。

特性	传统物权（示例：房产）	数据权益
排他性	唯一占有，他人未经许可不得使用	可被无限复制，多方同时使用
客体固定性	物理形态稳定	动态变化 （如个人信用记录实时更新）
处置权范围	可自由出售、赠与、销毁	受限 （如纳税数据不可随意删除）

举例而言，假如我们承认一个自然人对与其相关的个人信息拥有物权编逻辑上的“所有权”，那么该自然人就应当拥有最基本的“处置权”，从而可以修改他自己不喜欢的那些数据（例如不良贷款记录、犯罪记录乃至某些不那么“拿得出手”的求学、就职和履历记录等）；该自然人还应当拥有对其个人信息的“管有、控制权”，这意味着他可以“占有”自己的个人信息，可以拒绝他人使用相同的姓名、可以禁止他人分享任何指向自己的个人信息——例如律师为了不被吊销执业证，可以拒绝行政机关从司法机关调取其故意犯罪记录等。这些推论无疑是不符合常识的。

更重要的是，个人信息之所以不可能受到单一“所有权”的约束，是因为这些信息一直处在不断地变化中：一组个人信息从产生到存储，再到被聚合、分解和重组，几乎每次数据处理都会产生新的数据。而产生这些新数据的原因，大部分不是基于自然人自己的意志——个人的姓名、学号、证件号大部分情况下不是自己决定和产生的；个人的扫码消费信息尽管来自其消费行为，但支付过程中究竟是涉及到哪几个银行网关，以及哪些结算机构，在现实中也不是个人所决定的，甚至不是个人所关心的。在客体都无法固定的情况下，不可能在这种客体上施加以所有权。因此，当人们提到所谓“某人的个人信息”的时候，实际上指的是“可以用来查找、识别、关联某个自然人的信息”，而不是“归属于这个自然人的信息”。

二、数据权益不能套用知识产权法理论

知识产权法保护的是创造性智力成果。法治体系中创设知识产权的主要原因是为了激励创新（对专利、著作权和植物新品种而言）和避免混淆（对商标、企业名称等而言）。如果某些特定的数据集满足了上述知识产权的标准，自然就成为这些知识产权的客体，也可以顺理成章地依据这些法律的安排，明确其权利的主体和权利的边界（无论是在保护期还是在保护范围的意义上）。

但是，大部分数据集，尤其是公共服务业中的数据集（如交通、气象、行政管理、卫生医疗等）是客观事实的汇集，缺乏独创性，也不具有用以标识某种产品的质量或声誉的作用。如果保护某个数据集不能起到鼓励创新的作用，也不能避免公众的混淆，那么知识产权法意义上的“归属”理论便失去了适用性。因此，这些数据集难以纳入著作权法或专利法的保护范围，更难以实现传统意义上的“确权”。

更重要的是，在实践中，完全没有必要套用知识产权法的理论就可以完成数据的价值实现。举例而言，如果一个数据集确实有价值，那么数据集的控制者只要简单地允许愿意支付对价的访问者访问数据集即可。这个过程中，既没有所有权意义上的“占有”的转移，也不需要按照版权法的框架去限定被“访问”“复制”乃至进一步“分发”的客体是否有著作权法意义上的独创性。事实上，支付对价后访问数据库是早已存在并且成熟的商业模式，被访问的数据集上究竟是否存在“知识产权”，一直都不是这种商业模式成立的决定性因素。

可能有人会问，如果不确定数据的“归属”，那么访问者将这些数据复制后，超越原有的合约范围去使用数据，数据集的原始“卖方”如何维护自己的“权益”？回到第一性原理，之所以卖方的数据集有价值，只可能有两个原因：一是数据集本身已经达到了著作权法保护的标准，构成“汇编作品”；二是数据集本身完全没有达到著作权法保护的标准，访问者只是不想自己再去花费成本收集整理数据。对前者而言，“汇编作品”的作者完全可以依据著作权法维护权利。对后者而言，数据集的整理者也可以依据合同编上的权利去约束访问者——停止访问权限。如果访问者发现自己的违约成本高于收集整理数据的成本，那么他们就会继续购买数据库的访问权限。

三、《数据二十条》的制度创新

《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》（即“数据二十条”）提出了数据“三权分置”新思路：数据资源持有权、数据加工使用权和数据产品经营权。这一机制不再纠缠于数据所有权谁属，而是转向合法持有和合规利用，淡化了所有权概念，强调权利分离和使用授权，为数据要素化、市场化奠定了基础。



四、数据之上没有所有权

《个人信息保护法》也没有赋予自然人对其个人信息的“所有权”。

一方面，《个人信息保护法》明确规定，并非所有使用、处理个人信息的行为都需要获得自然人的同意。另一方面，自然人也无法将其个人信息随意出售、安排继承或做其他类似财产权意义上的处分。因此，数据合规工作的核心，不是想方设法赋予个人或者其他数据控制者排他性的所有权，而是在确保个人在数据收集、处理和利用过程中的知情、修改、删除等基本人格权的基础上，释放数据的流动性，让数据控制者可以对数据进行处理、衍生，形成数据产品。

在破除“所有权”的迷雾后，我们就会发现：对于数据集的控制者来说，要做的工作只有一项：判断各种各样的现有法律法规中，对自己所掌握的数据集的分享、开发有哪些限制。通过获取（个人）同意、得到（政府）批准、满足（不需要同意即可处理数据的）法定要求、取得许可（假如数据集中有知识产权）等动作，将这些限制予以克服后，就可以自由地处理或者允许别人访问这些数据集。而这动作，就是我们所说的“数据的合规改造”。

五、数据合规改造的“五步法”

只有理解“数据之上没有所有权”，才能明确数据合规的重点不是“确权”而是“合规改造”。在数据利用过程中，律师与合规顾问的工作不是纯粹的“成本负担”，而本身就是数据处理、数据增值的必要环节。

具体实践中，对数据的“合规改造”可分为五个阶段：

（一）数据尽调
明确数据的来源，核实数据内容，判断是否包含个人信息或有知识产权的信息，梳理数据当前的存储状态，以及已有的处置或处理方式。通过详尽尽调，确保数据获取、存储、流转的合法合规，为后续开发利用夯实安全基础。

（二）梳理数据权利链条
厘清数据涉及的权属关系，全面审阅数据确权、流转的相关法律文件、现有协议和用户政策，判断在数据归属、使用、共享等流转中的合规性和潜在的法律风险。

（三）设计数据产品的分享方案
针对特定数据产品，明确利益相关方、分离或匿名化个人信息，厘清数据流转路径和数据接触者，设计数据融合与共享方案，规范使用期限及与上下游机构之间的分润机制，平衡数据流通与保护。

（四）产品改造与文件起草
根据数据产品方案，完成存储、访问、修改等环节的技术改造，及起草和完善法律文书（包括数据使用协议、隐私政策等），调整和优化企业内部合规管理体系，编制《隐私影响评价报告》，最终完成数据产品的全方位合规评估。

（五）推进资产化
和购买必要的存储空间、建立必要的数据安全体系一样，合规改造是产品开发投资的一部分。合规改造的过程就是将原始的数据资源变成具有商业价值的数据产品的过程。只有这样，才可以将数据资源纳入生产要素体系，通过市场化机制释放其商业价值。

六、结语

数据并不具备传统意义上的所有权属性，其真正的价值实现取决于合规改造的力度。破除数据之上存在“所有权”的误解，才能将法律工作的重点从“数据确权”移至“数据合规改造”，由既懂法律、又懂产品，还理解市场需求的合规顾问，以正确的步骤完成数据资源从“原料”到可交易的“产品”的跃迁。

九、合规即增长：从"大数据杀熟"被判罚看AI商业的合规转型

主笔人



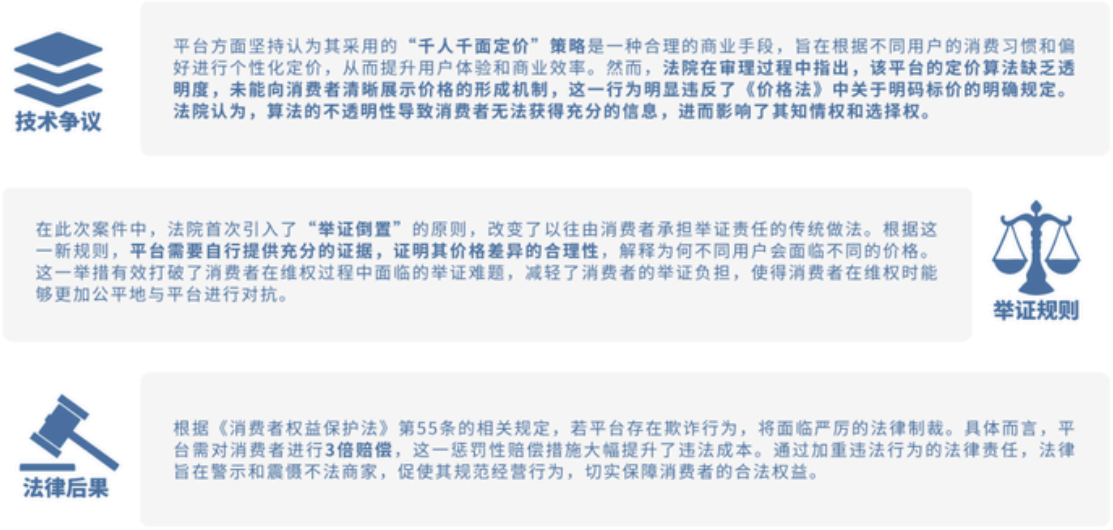
朱峰

浩天全国资本市场专业委员会 牵头合伙人
浩天上海总部-人工智能行业委员会 牵头合伙人
北京浩天（上海）律师事务所 高级合伙人
zhufeng@hylandslaw.com

一、首例"杀熟"判罚为何震动业界?

2024年11月，北京互联网法院对“胡女士诉某外卖平台”案件作出判决：平台利用算法对老用户抬高价格构成价格欺诈，需退还2889元并赔偿11556元。

这件看似普通的消费纠纷，却成为中国AI商业史上的标志性事件。



“胡女士诉某外卖平台”案的三个关键点

此次判决的严厉后果也向社会传递了一个明确的信号：任何侵害消费者权益的行为都将受到法律的严惩。

相较于2018年“某外卖平台多收1元配送费案”因证据不足败诉，此次判决释放强烈信号：AI算法不再是法外之地，合规能力正在重塑商业竞争规则。

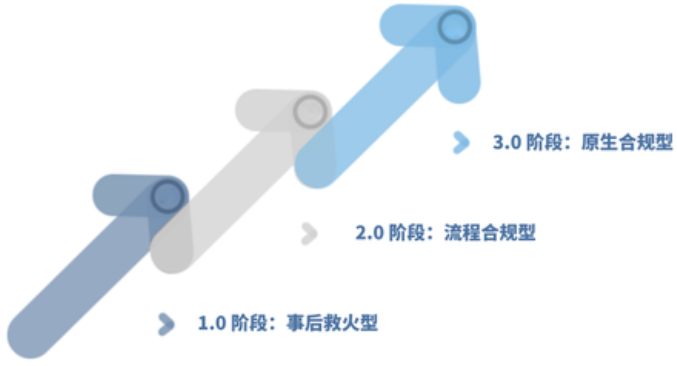
二、AI 商业面临的三大信任陷阱

“杀熟”现象揭示了更深层次的系统性风险：



正如业内人士所言：“未来的市场竞争，胜出的并非算法最聪明的企业，而是最能让用户放心的企业。”

三、AI 商业——合规转型的三个发展阶段

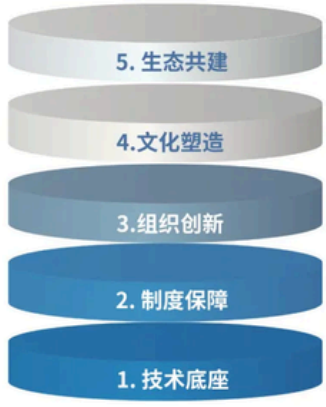


1.0阶段：事后救火型
典型案例：某旅行平台于2023年因“酒店价格歧视”问题被约谈后，紧急下架了问题算法，然而半年内用户流失率高达27%。

2.0阶段：流程合规型
代表企业：某网约车平台设立了算法伦理委员会，但内部审计发现，超过30%的定价模型仍存在地域歧视的风险。

3.0阶段：原生合规型
领先实践：某金融科技公司将合规要求嵌入到算法开发过程中，在特征工程阶段植入了反歧视模块，从而使模型训练成本降低了40%。

四、构建“合规竞争力”的五大支柱



（一）技术底座

1.可解释AI：某银行通过引入SHAP值分析方法，深入探究信贷算法的决策过程，发现该算法对女性创业者在贷款审批中存在隐性偏见，从而及时调整算法参数，确保信贷服务的公平性。

2.隐私计算：某互联网银行采用联邦学习技术，与合作方共同构建数据共享平台，有效提升了数据利用率高达35%，在保障用户隐私的前提下，实现了数据价值的最大化。

3.公平性约束：某知名招聘平台在其算法设计中，特别设置了“性别平等正则项”，通过这一技术手段，成功提升了岗位匹配的公平性，增幅达到22%，有效减少了性别歧视现象。

（二）制度保障

1.建立算法全生命周期管理：百度Apollo自动驾驶系统严格按照全生命周期管理理念，每季度定期发布《算法透明度报告》，详细披露算法的设计、测试、应用及更新情况，确保算法的透明度和可追溯性。

2.实施红蓝对抗测试：支付宝高度重视支付算法的安全性，每年组织开展超过2000次的攻防演练，通过红蓝对抗测试，及时发现并修补潜在的安全漏洞，确保支付系统的稳定运行。

（三）组织创新

1.设立CTOAI岗位：字节跳动在组织架构上进行创新，首席技术官（CTO）兼任可信AI负责人，统筹推进AI技术的可信度和合规性，确保技术发展与伦理规范相协调。

2.推行“算法听证会”制度：美团外卖在制定定价策略时，引入“算法听证会”制度，邀请法务、伦理专家及用户代表共同审议，确保定价算法的公正性和透明度，充分听取各方意见。

（四）文化塑造

1.将公平性指标纳入KPI：拼多多积极响应公平性要求，将“城乡用户价格差异率”纳入高管的绩效考核体系，通过量化指标，推动管理层重视并解决城乡用户价格差异问题。

2.开展“算法素养培训”：腾讯致力于提升技术团队的伦理素养，建立了工程师伦理认证体系，覆盖超过80%的技术团队，通过系统培训，增强工程师对算法伦理的认知和实践能力。

（五）生态共建

1.牵头制定行业标准：蚂蚁集团积极参与行业标准化建设，参与起草了《金融算法透明性规范》国家标准，为金融行业的算法透明性和合规性提供了重要参考依据。

2.开放合规能力输出：京东科技充分发挥自身技术优势，面向中小企业提供“合规算法SaaS解决方案”，帮助中小企业提升算法合规水平，共同构建健康、可持续的算法生态。

五、合规投入的效益分析

以某头部生鲜平台为例，进行详细的效益分析如下：



更深远的价值在于抢占政策先机：作为首批通过“可信AI认证”的企业，该生鲜平台不仅在行业内树立了良好的合规标杆，还将在数据要素流通、跨境业务拓展等方面获得显著的竞争优势。这种先发优势不仅有助于企业在激烈的市场竞争中占据有利位置，还能为未来的可持续发展奠定坚实的基础。

六、监管创新与行业趋势

（一）中国特色的“算法治理”体系正在形成：



（二）值得关注的创新实践：

1.“合规即服务”模式：华为云推出了算法合规诊断工具，该工具旨在帮助企业进行算法合规的自我诊断，以确保其算法的应用符合相关法律法规的要求。截至目前，该工具已经服务了3000多家企业，为企业的算法合规提供了有效的支持。

2.算法备案公示：抖音、快手等平台已经公开了其核心算法逻辑，用户可以通过查询了解其推荐机制。这一举措旨在提高算法的透明度，让用户了解算法的工作原理，增强用户对平台的信任。

七、结语：合规即未来竞争力

“杀熟”判例的出现，无疑标志着AI商业领域野蛮生长时代的终结，同时也预示着合规能力正在逐步崛起，成为企业在新时代中不可或缺的生产要素。对于那些能够率先完成技术架构的重构、组织结构的进化以及生态体系的共建的企业而言，它们将在数字经济的下半场竞争中，享受到三重显著的红利：



（一）风险控制

通过严格的合规管理，企业能够有效避免陷入重大的法律纠纷和品牌危机，从而为企业的长期稳定发展奠定坚实的基础。

（二）效率提升

借助合规流程的自动化，企业能够大幅缩短研发周期，据测算，这一改进可以使研发周期缩短高达40%，极大地提升了企业的运营效率和市场响应速度。

（三）价值创造

合规经营所塑造的可信品牌形象，将为企业带来显著的溢价效应，进而吸引更多的用户群体，预计用户增长率可达到15%-20%，为企业创造更大的市场价值和商业机会。

正如众多行业专家所预言的那样：“在未来的商业竞争格局中，其本质将逐渐演变为一种可信能力的激烈角逐。所谓将合规性深度融入代码之中，实际上就意味着将未来的商业主动权牢牢掌握在自己手中。”

在这个由算法主导和定义一切的时代背景下，企业唯有坚定不移地将透明性、公平性和安全性这三大核心要素深深铸入自身的商业基因之中，才能真正意义上赢得来自用户、市场以及监管机构等多个维度层面的广泛信任与认可。这种多维度的信任构建，不仅是企业在激烈市场竞争中立于不败之地的关键所在，更是推动企业实现可持续健康发展的坚实基石。

十、帮助侵权：AIGC文生图平台的侵权责任及合规建议

主笔人



张金栋

北京浩天律师事务所 合伙人
zhangjindong@hylandslaw.com

AIGC（生成式人工智能）文生图平台日趋流行，成为了图片创作者新的生产利器。相应的，AI文生图服务提供者本身的法律定性，文生图各个过程行为在法律上如何评价，在输出图片产生著作权侵权时AI文生图服务提供者应该承担什么样的责任，以上问题对于其合规运营，避免侵权赔偿风险也愈发重要。

广州互联网法院和杭州互联网法院（二审杭州中院）的两起“奥特曼案”，基本将上述问题厘清。两个案件的侵权情节略有不同：广州案【(2024)粤0192民初113号】中，AI平台只需要输入关键词即可以生成图片，并向用户提供；杭州案【(2024)浙01民终10332号】中，AI平台不能直接文生图，需要用户自行上传图片训练LoRA模型后，再行叠加文字描述方能生产相应图片。两地法院都在判决中对此类案件的争议焦点提供了建设性观点，尤其是杭州法院奥特曼案判决，对于数据输入、数据训练、内容生成和内容发布各个阶段的法律责任问题从著作权侵权和不正当竞争角度进行了非常详细的论证，具有重要参考价值。



涉案 AI 平台使用流程对比

一、AI文生图服务提供者应承担帮助侵权责任

AI文生图服务提供者，不仅是平台管理者，也是内容生产者，应承担帮助侵权责任。

杭州法院认为，AI文生图服务提供者并非仅仅提供信息存储空间，而是兼具内容生产者的角色，属于一种新型的网络服务形式。

但其又区别于直接的内容生产者，是通过技术手段帮助用户生成内容，并不存在与用户的意思联络。这种参与程度，介于传统的互联网内容提供者（ICP）和互联网服务提供者（ISP）之间，因此既不会直接简单适用“避风港”原则免责，也不是直接侵权。而是根据其具体情节，在违背其合理注意义务的前提下，被认定为一种“帮助侵权”行为。



二、AI文生图服务提供者应尽的合理注意义务考量因素

在广州案中，法院从《生成式人工智能服务管理暂行办法》规定的角度，从被告缺乏投诉举报机制、潜在侵权风险提示、生成物显著标识等合规内容，论证了其过错，但未从传统著作权法角度直接论证其对生成图片著作权侵权的注意义务到底如何。

而杭州法院更加正面地回应了被告合理注意义务的考量因素：

1.从被告提供AIGC服务的具体类型和商业逻辑本身，推敲其防范成本；
2.被侵权作品的知名度和侵权行为的明显程度；
3.侵权内容的扩散风险；
4.平台是否以此营利；
5.是否采取了预防侵权合理措施。

以上考量因素，基本还是围绕《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》中的精神，对具体的AIGC服务进行了分析。

三、AI 文生图合理使用与具体侵权边界

数据输出和模型训练过程为合理使用，图片生成和发布过程可能侵犯复制权、改编权和信息网络传播权，一般不构成不正当竞争。

广州法院认为，由于案涉奥特曼作品的知名度，AI文生图服务提供者存在接触作品的可能性，其结果上也部分或完全复制了其独创性表达，侵犯了复制权。同时，由于用户可以通过发出指令的方式，让平台对图片进行修改，侵犯了改编权。对于是否侵犯信息网络传播权，广州法院未展开论证。

杭州案中，由于用户输入文字无法直接生成图片，因此不存在复制权、改编权的侵权问题，而是侵犯了信息网络传播权。对于数据输入和数据训练行为，其本质是为了提高模型的创作能力，也不存在复制后的展示输出，因此类似人的学习过程，应被认定为合理使用；但对于内容生成并发布的环节，应被认定为侵犯了信息网络传播权。

关于是否构成不正当竞争的问题，杭州法院认为被告并非针对原告的特定目标的训练，且其行为已经被著作权法这一特别法评价，因此不构成不正当竞争。

四、生成式人工智能服务提供者合规锦囊

基于上述司法实践，我们为生成式人工智能服务提供者提供了数据输入、训练与输出、事后治理与留存三个阶段的合规锦囊。

（一）数据输入阶段：
仅使用取得合法授权或公开声明可商用之训练数据；
建立版权白名单与黑名单制度，对高知名度作品自动触发人工复核。

（二）训练与输出阶段：
显著标识“AI生成”与“禁止商用”提示；
部署关键词过滤、图像指纹比对等技术措施，确保用户输入高明度IP等提示词时无法生成实质性相似图片；
设置实时举报按钮，接到权利人通知后24小时内下架模型与图片并冻结上传者账户；
明确平台可对高风险模型采取“先行下架、后补审核”的紧急措施，降低禁令风险。

（三）事后治理与证据留存：
建立生成日志与训练日志的链上存证系统，便于举证已尽合理注意义务；
与第三方版权监测机构合作，定期扫描平台新生成内容；
在用户协议中新增“版权承诺条款”，要求用户声明上传素材不侵权并同意承担赔偿责任；
明确“侵权N次即封禁”规则，降低连带责任风险。

十一、技术犯罪：从“工具之恶”到“主体之责”

主笔人



邓哲

北京浩天律师事务所 合伙人
dengzhe@hylandslaw.com



常康爽

北京浩天律师事务所 顾问
changkangshuang@hylandslaw.com

在当下，人工智能技术呈迅猛发展之势，其于各领域的广泛渗透，有力推动着社会进步与革新，成为驱动发展的重要引擎。然而，伴随AI应用的日益深化，其在带来诸多便利与创新成果的同时，也滋生出一系列严峻问题。部分不法分子将犯罪之手伸向AI技术，将其沦为实施犯罪的“得力工具”，为社会的安全稳定埋下了重重隐患，AI技术已然成为新型犯罪的高发领域。

*感谢实习生曹书航对本文的贡献。

一、利用AI技术实施犯罪的两种类型

涉及AI的犯罪大致可归为两类：一种是用户借助AI技术应用实施违法犯罪，一种是开发AI技术应用实施犯罪。

（一）用户借助AI技术实施违法犯罪

1.利用AI模型修改他人美术作品后出售，涉嫌侵犯著作权罪
在北京市通州区人民法院审理的某电子商务公司等涉嫌犯罪一案中，姚某在罗某的指导下，指使AI画师利用AI制图工具，非法复制他人享有著作权的美术作品。为了规避侵权风险，姚某要求AI画师对原图仅做细节上的细微修改，如调整局部颜色、线条或背景等，但刻意保留原作品最核心、最具独创性的关键表达元素。后续罗某组织其实际控制的某电子商务公司，利用这些经人工智能软件“微调”的图片，大量生产制作拼图产品，供姚某等人销售。短短数月内，姚某与李某、王某合伙经营电商店铺售出侵权拼图超过3000件，非法获利人民币27万余元。

法院经审理判决如下：被告单位某电子商务公司及相关责任人员犯侵犯著作权罪，判处相关人员有期徒刑十个月到一年六个月不等，并处罚金人民币，没收涉案财物及退缴在案的违法所得。具体可参见法治北京微信公众号《北京首例AI改图侵权案宣判 原创作者：满意法院判决结果》

2.利用AI技术换脸非法登录他人支付账户，涉嫌侵犯公民个人信息罪、信用卡诈骗罪
在南京市玄武区人民法院审理的符某案件中，被告人符某通过网购的方式非法获取了195万多条公民个人信息，随后利用该等公民个人信息，通过AI换脸软件，以“人脸识别”的方式，登录了23名被害人的金融平台支付账户。另外，符某非法更改了5人的支付密码和绑定手机号，并冒用1人的支付账户绑定的银行卡，购买了两部手机，共计人民币15996元。法院经审理判决被告人符某犯侵犯公民个人信息罪、信用卡诈骗罪，数罪并罚决定执行有期徒刑4年6个月，并要求其承担15996元公益损害赔偿金、删除存储的所有公民个人信息，另在国家级新闻媒体上公开赔礼道歉。具体可参见法治时报微信公众号《“AI换脸”诈骗，男子获刑4年半》

3.利用AI技术生成的虚假视频及图文并传播，涉嫌编造、故意传播虚假信息罪
在浙江省绍兴市上虞区人民法院审理的张某某、陈某某案件中，陈某宇在网上购买多个某网络平台账号供公司内部工作人员使用，上述人员随意选取网络热点，复制热点新闻的标题、关键词并输入到某软件中由AI自动生成文案，后将该文案放入某创作软件中自动生成AI视频，并将合成的视频、图文集1万余条发布至某网络平台上供人浏览。其中，虚假造谣视频20余条，累计阅读观看量超过167万次。其中，《浙江工业园现场大火浓烟滚滚，目击者称有爆炸声！》造成恶劣社会影响，对此相关职能部门在多个平台进行辟谣。法院经审理判决如下：被告人张某伟、陈某宇犯编造、故意传播虚假信息罪，分别判处有期徒刑一年一个月，缓刑一年六个月。具体可参见新华网《<利用AI生成类谣言辟谣典型案例>发布》之案例三

（二）开发AI技术应用实施犯罪

1.明知他人实施违法犯罪活动仍为其提供AI技术帮助，涉嫌非法利用信息网络罪
在江苏省无锡市人民法院审理的巫某某案件中，被告人吕某在广东省中山市成立广东某某互联科技有限公司，招募

陈某某、浦某某、范某某及被告人巫某某等人为业务部门负责人和业务经理，在明知上家人员为实施网络诈骗等违法犯罪活动而设立微信交流群的情况下，仍使用AI机器人电话向不特定对象拨打电话筛选出有投资意向的客户，后安排员工冒充财经公司或证券公司人工客服，以免费进入股票交流微信群进行交流学习等为由，诱骗客户进入上家人员设立的股票交流微信群内，入群客户达到上家要求的数量后，通过与上家按人头数结算提成获利。被告人巫某某作为一部经理，根据该部业务员拉入微信群的客户总人数提成，违法所得共计人民币1万余元。法院经审理判决被告人巫某某犯非法利用信息网络罪，判处有期徒刑六个月，并处罚金人民币9000元。具体可参见江苏省无锡市惠山区人民法院刑事判决书，（2022）苏0206刑初140号

2. 明知他人利用信息网络实施犯罪活动仍为其提供AI技术帮助，涉嫌帮助信息网络犯罪活动罪
在重庆市大渡口区人民法院审理的钟某某案件中，被告人钟某辉明知胡某某要给网络赌博平台提供用于财务人员结算的AI识图软件，在蒋某某的介绍下答应帮助研发制作，胡某某承诺给予劳务费。胡某某将赌博APP需要如何进行结算和一些相关的赌博输赢界面截图等信息提供给钟某某，钟某某按照要求开发了一款名为“AI识图”的识图软件，方便赌博平台统计战绩。后钟某某告诉胡某某需要百度识图的相关技术，胡某某让蒋某某注册了百度智能云，将百度API接口接到了钟朝辉开发的软件里面，然后将“AI识图”赌博计分软件提供给永胜联盟APP赌博平台财务人员陈某某、张某某等人使用，胡某某向该赌博平台收取相关软件服务费用以此获利。钟朝辉从胡某某处获得报酬26800元。法院经审理判决被告人钟朝辉犯帮助信息网络犯罪活动罪，判处拘役六个月，缓刑一年，并处罚金一万元，并追缴违法所得26800元。具体可参见重庆市大渡口区人民法院刑事判决书，(2023)渝0104刑初303号

二、 AI应用技术开发主体的刑事责任

从相关案例中不难看出，涉及AI技术的刑事犯罪活动正悄然发生演变，从最初AI被用于违法犯罪，逐渐发展到技术开发者被认为参与“作恶”。由此引发了关于技术开发者注意义务的讨论：何时技术开发者可依据“技术中立”原则免责？何时技术开发者会被认定为直接实施了“作恶”行为？何时又会被判定与上游联合“作恶”？

针对这一问题，包括我国在内的AI大国目前仍在持续探索，力求找到合理且可行的界定标准，以应对不断变化的AI技术犯罪态势，促进技术在合法合规的框架内健康发展。从既有司法实践来看，目前我国对于AI技术开发者刑事责任的认定已大致形成基于“客观控制+主观明知”的追责体系：

1. 如果技术开发者仅提供技术应用，但对相关技术的实际应用内容不了解，且在后续持续服务过程中也未认识到相关技术被用于实施违法犯罪活动，则技术开发者一般不就使用者的行为承担法律责任；
2. 如果技术开发者仅提供技术应用，但在实际对接和服务过程中认识到相关技术可能被用于实施违法犯罪活动，则技术开发者应及时采取必要措施终止技术支持，否则可能涉嫌非法利用信息网络罪或者帮助信息网络犯罪活动罪；
3. 如果技术开发者在提供技术应用时已经明确了解到上游通过相关技术用于实施特定违法犯罪活动，且仍继续提供帮助和支持，甚至直接参与相关违法犯罪活动的分成，则技术开发者在其参与范围内可能成立上游犯罪的共犯；
4. 如果技术开发者在广泛提供技术应用支持时了解到个别用户利用相关技术实施违法犯罪活动，有能力阻止而不阻止，经行政机关责令采取改正措施仍不改正的，其可能涉嫌拒不履行网络安全管理义务罪。

三、AI技术追责的待解难题

在2025年世界人工智能大会开幕式上，神经网络之父杰弗里·辛顿发言指出，当AI比人类聪明时，便可能发展出目标导向行为，如生存意愿、完成任务的强烈欲望以及控制权倾向等。届时，究竟是人类掌控AI，还是AI控制人类，着实引人深思。

当下，在人类尚可掌控AI的阶段，以使用主体和开发主体为核心构建的追责体系，尚可应对AI犯罪相关法律问题。然而，一旦AI突破人类控制，产生“自我意识”，尤其是当AI基于特定导向“作恶”，直接侵犯人类利益时，该如何构建一套能够规制超越人类意识范畴的、针对AI自由意识的追责体系呢？从技术层面看，是否存在类似拔掉AI插座、为其断电这样简单直接的控制手段？在法律领域，又是否能构建起惩罚AI、引导其改过自新的理论，并将其切实落地实施呢？

所幸，目前这一问题还仅停留在假设阶段。但未来充满未知，没人能断言这一问题永远不会发生。或许，未来引导AI向善不再是道义义务，而将成为每一位AI技术参与主体的法律义务。

十二、数据入表全流程： 从合规确权到动态风控的法律实务指引

主笔人



叶建芳

京浩天（杭州）律师事务所 主任
yejianfang@hylandslaw.com



吕文易

北京浩天（杭州）律师事务所 律师
lvwenyi@hylandslaw.com



王芬芬

北京浩天（杭州）律师事务所 律师
wangfenfen@hylandslaw.com

财政部颁布的《企业数据资源相关会计处理暂行规定》（财会〔2023〕11号）的落地实施，叠加北上广深等数据交易所细则的密集出台，意味着数据资产入表已逐步从政策蓝图走向企业实操。作为深度参与该领域法律研究与实践的从业者，我们深切体会到：数据入表绝非会计的技术调整，而是一场牵涉权属根基、合规深度与企业价值提升的系统性法律工程。任何环节的疏漏，都可能让企业面临估值争议、监管处罚甚至法律纠纷。

本指引将结合一线实务经验，梳理数据资产入表的全流程工作节点，以作参考。

一、前期准备：确权与合规审查

核心：解决 “数据从哪来、权利归谁有” 的根本问题。

（一）数据来源合法性

1. 个人信息授权链条完整性

• 穿透核查数据获取全场景：用户协议勾选项是否清晰？隐私政策是否明确入表用途？（参考莱州公交案例：需逐条核查移动支付协议并补充乘客知情同意声明）；

• 依据《中华人民共和国个人信息保护法》（2021年主席令第91号，以下简称《个人信息保护法》）第 29条，敏感信息（健康、金融、行踪等）必须获取 “单独同意”，警惕 “一揽子授权” 陷阱；

• 数据用途变更（如从业务分析转向入表）需重新激活授权流程。

2. 匿名化处理标准

• 依据《个人信息保护法》第73条，需满足 “无法识别特定个人且不可复原” 的标准，需结合法律对 “特定个人” 的定义及最新技术成果，确认实时的技术水平符合 “不可复原” 要求；

• 若采用去标识化（如部分脱敏），必须配套强管控措施：加密存储、访问日志留存、定期重识别风险评估。

3. 是否触及 “重要数据” 红线?

• 根据《中华人民共和国数据安全法》（2021年9月1日起施行，以下简称《数据安全法》）的相关规定，重要数据（如工业控制、医疗健康类）需履行安全评估、出境申报等义务；

• 涉国家安全的重要数据：需结合行业主管部门指导判定（如能源、交通领域可参考《关键信息基础设施安全保护条例》，国务院令第745号，2021年施行），通过法律意见书明确边界。需注意，此类数据严禁入表交易（实务中因国家目录尚未完全公开，存疑时应从严论证）；

• 数据跨境传输：需依据《数据出境安全评估办法》（国家互联网信息办公室令第11号，2022年9月1日起施行）完成安全评估、个人信息保护影响评估等流程。

（二）产权分置设计



确认来源与级别后，应依据《中共中央、国务院关于构建数据基础制度更好发挥数据要素作用的意见》（2022年12月发布，以下简称《数据二十条》）确立的 “三权分置” 原则（数据资源持有权、数据加工使用权、数据产品经营权），通过协议、备忘录等法律文书固定权利边界。

二、评估与入表准备

核心：确保评估数据经得起监管问询 —— 避免估值泡沫引爆合规危机。

（一）评估合规性双维度审查



（二）法律意见书

评估报告出具前，律师团队需专项论证：

1. 数据来源合法性：重点核查数据采集环节是否严格遵循《数据安全法》《个人信息保护法》等法律法规要求，同时需追溯数据流转全链条，核查各环节数据传输、存储、使用是否合规，坚决排除 “黑数据” 估值，从源头上保障数据资产的合法性。
2. 企业权利边界：深入剖析企业与数据提供方、合作方之间的协议条款，明确企业对数据资产享有的权利范围，核查企业是否存在超权限处分或者权利受限情形，如数据共享协议中对数据再利用的限制、知识产权归属约定等，避免因权利瑕疵影响数据资产价值评估。
3. 收益法假设的合法性基础：对收益法评估中涉及的假设条件进行合法性审查，重点关注数据产品上市准入资质的真实性与有效性。需核查企业是否已取得数据产品相关的业务许可、备案等合法手续，如增值电信业务经营许可证、网络安全等级保护认证等，确保符合市场准入要求，保障收益法评估假设具备坚实的合法性基础。

三、专项协议设计

核心：构建事前风险隔离机制，而非仅作为事后救济凭证。

（一）数据资产入表专项协议

1. 权属无争议承诺：企业需出具书面文件证明数据来源合法，提供原始取得证明、授权协议等材料；多方合作数据需获所有权利方书面确认，承诺无权利瑕疵。企业内部应建立法务、合规、技术等多部门交叉核验流程。
2. 价值波动责任机制：企业财务部门应联合第三方评估机构定期重估数据资产价值。当数据资产的价值因技术、市场等因素显著波动时，责任人需及时汇报并启动调整程序，在财务报告中详细披露波动情况，企业内部建立评估失准问责制度。
3. 退出机制：明确数据资产过期失效、丧失价值等退出标准，条件触发后需完成内部审批、账务核销、安全处置（如按规定删除或脱敏）等流程并形成不可篡改的备案记录；对外授权数据退出时，需通知合作方终止授权并处理善后。

（二）合同：场内场外差异化管理

1. 场内交易（如北京数交所）：采用标准合同 +“数据三证”（数据资源持有权证书、数据加工使用权证书、数据产品经营权证书），重点核查 “默认合规条款” 是否覆盖企业场景；
2. 场外交易：增补 “三禁止” 条款 ——禁止用于算法歧视、禁止擅自再授权、禁止超约定范围存储。

四、协同服务下的职能团队分工

核心：任务的顺利推进，既需舵手把控方向，也离不开领航者指引航程。

（一）实务协作模式

律师团队应作为合规总控，负责统筹协调多方专业机构，具体包括：



科技公司

强化数据治理体系建设，筑牢数据资产全生命周期安全合规防线，确保数据资产可管可控、安全可靠。

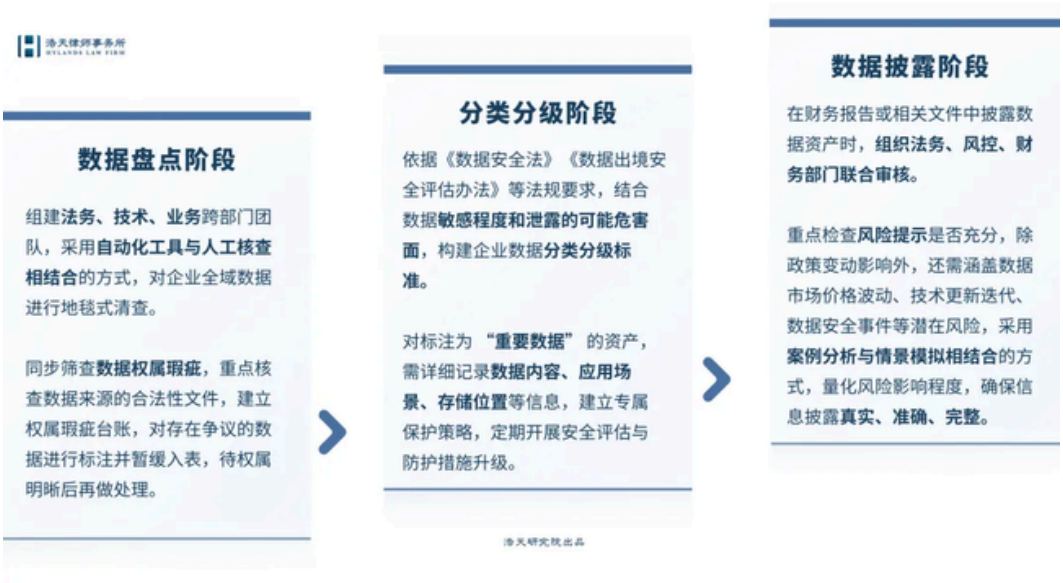
评估机构

依托专业数据资产评估模型，结合市场动态与行业特性，构建科学严谨的估值体系，实现数据资产价值的精准量化与公允评估。

会计师事务所

根据会计准则的核心要求，搭建适配数据资产特性的财务核算框架，从确认、计量到披露全程把控，保障数据资产入表符合规范性与严谨性标准。

（二）核心动作



五、入表后管理：数据资产是 “活资产”

核心：入表不是终点，而是动态合规的起点。

（一）持续监控清单



（二）风险事件法律响应

风险类型	响应动作
权属争议	启动确权复核→补充权证→优先仲裁（例如约定适用上海仲裁委员会《数据仲裁指引》，2023 年 11 月施行）
政策突变	合规重评→调整分级→交易所备案
技术淘汰	联合技术 / 评估机构论证贬值幅度→计提减值→披露

六、结语

数据资产入表的核心，是依托系统化法律合规体系，将原始数据资源转化为具备法律确定性、市场流通性的可信资产。而在此类活动中，律师的专业价值贯穿全流程：



新时代浪潮下的企业负责人应深刻认识到，合规投入是一项战略性资产，而违规成本往往难以估量。在数据资产化进程中，若能将合规意识贯穿始终，将更有助于实现企业基业长青，持续保持竞争优势。

十三、稳定币监管：美国“天才法案”核心内容解析

主笔人



郭远程

北京浩天律师事务所 合伙人
浩天数字科技与互联网行业委员会 牵头合伙人
guoyuancheng@hylandslaw.com



陈青青

北京浩天律师事务所 律师
chenqingqing@hylandslaw.com

继美国参议院以68票赞成、30票反对的结果通过Guiding and Empowering the Nation for Innovation in U.S. Stablecoins Act（“GENIUS Act”或“法案”）后。7月17日，美国众议院以308票赞成、122票反对的结果通过GENIUS Act，随后美国总统特朗普于7月18日正式签署GENIUS Act，这一事件标志着美元稳定币首次被纳入正式联邦法律监管框架，同时巩固美元的全球储备地位。

*团队实习生梅盛瑞为本文亦做出贡献。

本文将从GENIUS Act出台背景、支付型稳定币含义、监管的核心内容以及与香港稳定币条例的比较等维度解析这一监管框架。

一、GENIUS Act出台背景

在很长一段时间，美国稳定币监管生态呈现碎片化状态，各监管机构基于各自职能对稳定币提出监管主张，证券交易委员会（“SEC”）、商品期货交易委员会（“CFTC”）、联邦存款保险公司（“FDIC”）和货币监理署（“OCC”）等多家联邦机构都在稳定币领域施加影响，却未能确立明确的监管层级或协调机制，导致监管重叠与不确定性。随着普遍被认为亲加密货币的特朗普政府再次执政，全球稳定币市场总市值已超2500亿美元并且USDT、USDC主流稳定币在跨境支付与交易中逐步发挥关键作用以及2025年USDC发行方Circle在纳斯达克上市等诸多有利环境下，稳定币监管法案终于随着美国总统签署而生效。

二、支付型稳定币定义和监管范围

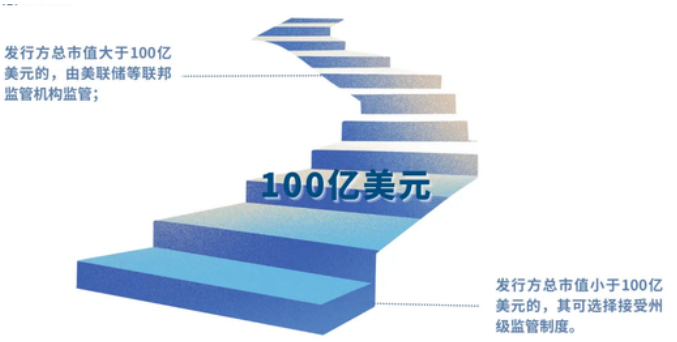
（一）稳定币与支付型稳定币（Payment Stablecoin）

如我们前一篇文章《稳定币：涵义释义及监管分析》中所述，稳定币是一类特殊的数字资产，其主要特征是可以维持（或声称可以维持）与法币价值 1:1 的锚定关系。在形形色色的各种类型的稳定币种类之中，GENIUS Act的第一个显著特征是，划定了一种特殊类型的“稳定币”作为白名单，赋予其某种意义上“合法地位”以及附随的“监管责任”。GENIUS Act将这种白名单稳定币称为“支付型稳定币”，其特征包括，应当作为支付或结算手段的数字资产，且发行方有义务将其兑换、赎回或回购为固定货币价值，或保持其相对于该固定货币价值的稳定。支付型稳定币不包括国家货币、存款（包括使用分布式账本技术记录的存款）以及证券。

同时，法案第14条对非支付型稳定币的监管也做了相应的规定，要求财政部长会同联邦储备委员会、OCC、FDIC以及SEC，开展关于非支付型稳定币的研究，包括内生抵押型稳定币。

（二）稳定币监管主体及监管范围

GENIUS Act建立了明确的监管架构，解决了此前多头监管问题。具体而言，法案采用“联邦+州级”分级监管框架：



需要注意的是，虽然由州一级进行管辖，但该州级监管制度在实质上与联邦监管框架相类似。

法案的适用范围为，向位于美国的个人要约或销售支付型稳定币的行为。这意味着从管辖角度，GENIUS Act体现的是属人管辖原则与属地管辖原则的结合应用。这种规定是美国金融法规中常见的域外管辖模式，目的是确保只要交易的一方是美国境内的个人，即使交易发生在美国境外，美国法律仍能提供保护和监管。这种域外效力的规定也反映了数字金融的跨境特性，旨在防止境外实体通过跨境方式规避美国监管。

（三）支付型稳定币发行与要求

1、许可制度以及发行主体
根据法案第3条的规定，除获准的支付型稳定币发行方外（permitted payment stablecoin issuer），任何人不得在美国发行支付型稳定币。即支付型稳定币发行方必须取得许可，方可在美国发行支付型稳定币。

为了取得许可，发行方必须是在美国成立以下几种实体之一：



2、过渡期安排
法案规定在颁布3年后（即2028年7月18日后），数字资产服务提供商（digital asset service provider）未获得许可的情况下，将被禁止提供或销售支付型稳定币。这意味着数字资产服务商将需要在三年内积极获得支付型稳定币发行方资格，否则将不再被准许进行支付型稳定币的发行。但美国财政部长另有豁免或针对外国支付型稳定币发行方的例外规定及对境外发行的支付型稳定币的互惠待遇的情形除外。

3、支付型稳定币发行方的最低标准
法案详细列明了获得支付型稳定币发行许可的资格条件，包括组织形式、财务实力、合规历史和高管资质等，具体包括：



更进一步，法案明确规定，发行方不得为其发行的支付型稳定币提供收益或利息支付。以凸显支付型稳定币的支付功能，而非一种投资产品。

三、储备资产及托管

（一）储备资产管理

支付型稳定币发行方必须按至少1:1的比例维持其已发行支付型稳定币的储备金。法案规定合格的储备资产包括美元现金、美联储账户存款、到期期限在93天内的短期美国国债、符合特定要求的以国债作为担保的回购协议、政府货币基金、中央银行储备存款，这些储备资产都属于高流动性、低风险资产。并且前述储备资产不得被质押、再质押或重复使用，但用于满足合理的支付型稳定币赎回请求所需的流动性除外。

（二）储备资产独立托管

法案明确要求储备资产必须由合格的第三方托管机构持有，并与发行方的运营资产严格分离并单独记账，将该等储备视为属于该发行方所发行的支付型稳定币持有人所有，而非视为该人员或该发行方本人的财产。这种托管安排旨在确保储备资产不受发行方可能面临的破产或违约风险影响，为稳定币生态系统建立更加稳健的保障机制，增强市场参与者的信心。

四、消费者保护与市场诚信

（一）破产保护条款

根据法案的规定，许可支付型稳定币发行方面临任何破产程序时，稳定币持有者的索赔权将优先于其他所有债权人。这一规定显著强化了支付型稳定币持有者的权益保护，确保即使在发行方破产情况下，持有者仍能优先获得储备资产的赔付。

（二）信息披露

法案要求发行方清晰披露稳定币的风险、费用和使用条款，限制收集和使用用户数据的范围，并建立专门的投诉和争议解决机制。同时明确禁止市场操纵和欺诈行为。值得注意的是，GENIUS Act特别规定支付型稳定币不允许向持有者提供利息或其他投资回报，强化其支付工具而非投资产品的定位。这一限制与证券法规相衔接，通过禁止支付型稳定币提供利息，明确区分了支付工具与投资产品，避免支付型稳定币被视为证券而引发监管复杂性。同时，法案还明确稳定币不属于证券或商品，不享受联邦保险，这些澄清有助于减少法律不确定性，为市场参与者提供更清晰的合规指引。

五、反洗钱与合规要求

法案规定，所有发行方必须实施严格的KYC/AML程序，建立交易监控系统识别可疑活动，配合国际反洗钱组织共享信息和执法。并且，许可支付型稳定币发行方应被视为《银行保密法》项下的金融机构，并因此须遵守所有适用于美国境内金融机构的联邦法律，包括但不限于有关经济制裁、反洗钱、客户身份识别和尽职调查的规定，其中包括（如适用）：

- 建立有效的反洗钱和经济制裁合规计划，该计划应包括适当的风险评估、制裁名单核查以及指定一名官员负责监督此类计划；
- 保留适当记录；
- 监测并报告任何可能违反法律或法规的可疑交易；
- 制定拦截、冻结和拒绝违反联邦或州法律、规则或规定的特定或不被允许交易的政策和程序；
- 维持有效的客户识别计划，包括识别与验证与支付型稳定币发行人有关的账户持有人、高价值交易，并实施适当的尽职调查。

六、与香港稳定币条例的比较

结合在此之前已经通过的《香港稳定币条例》，我们单独对二者中比较核心的部分进行对比比较。GENIUS Act与香港稳定币条例两种监管框架各有侧重，但目的趋于一致，都是为了将稳定币纳入明确的监管轨道，在防范金融风险、保护投资者资产安全的前提下，为稳定币合规提供清晰的路径。具体而言，两种监管框架核心比对如下：

对比维度	*GENIUS Act*	《香港稳定币条例》
两种监管存在高度一致的维度		
监管对象	支付型稳定币	指明稳定币
监管主体	以发行方总市值100亿美元作为界限安排联邦机构和州级两级监管	香港金融管理专员统一监管
储备资产	要求至少1:1高流动低风险储备资产，相应排除了算法稳定币、合成稳定币的应用空间	要求至少1:1“高质素及高流动性，且具最低投资风险”储备资产，相应排除了算法稳定币、合成稳定币的应用空间
储备托管	要求由合格第三方托管机构托管	要求由合格第三方托管机构托管
赎回权利	确保持有人有权按面值赎回	赋予持有者法定赎回权，要求尽快完成赎回
投资者保护	赋予稳定币持有者在发行方破产时对其他所有债权的优先受偿权	通过发牌制度、储备管理、赎回规定等保障消费者权益
域外适用	针对位于美国的个人要约或销售支付型稳定币的行为	明确包含域外管辖，针对香港公众推广的境外稳定币
两种监管存在明显差异的维度		
申请发行主体	限定为在美国成立的实体	既包括在香港注册的公司法人，也包括在香港以外成立为法团的认可机构
利息限制	明确禁止支付型稳定币提供利息或收益	未明确禁止稳定币提供利息
过渡期	美国的过渡期较长，自法案颁布后3年内	条例生效后3个月内；在前3个月内提交牌照申请且金管局以书面确认收到该申请的，延长至条例生效后6个月
生效日	自法案颁布之日起18个月；或自首要联邦支付型稳定币监管机构发布任何最终实施法案的法规之日起120天（孰早）	2025年8月1日

七、稳定币监管的影响与未来展望

总体而言，无论是美国GENIUS Act还是《香港稳定币条例》，其颁布均标志着一个根本性的转变-稳定币行业正从监管真空下的探索期，正式迈入有法可依、权责清晰的规范化整合新阶段。其核心目标已超越了在金融创新与风险防范间的简单权衡，而是通过前瞻性的制度设计与主动的监管引导，将稳定币的潜在能量有序地整合进国家金融主权框架之内，最终巩固并提升本国在全球未来数字金融格局中的战略地位。

十四、AI薅羊毛：AI图片骗取“仅退款”的法律责任及AIGC标识义务

主笔人



张金栋

北京浩天律师事务所 合伙人
zhangjindong@hylandslaw.com

近日，“仅退款AI图”相关词条登上了各大社交媒体的热搜版面。

“仅退款”政策，是电商平台推出一种消费者售后维权政策，如消费者对商品不满意，可向电商平台发起“仅退款”申请，在无需退货的情况下，就可以在平台支持下实现退款。这一政策推出后，提升了用户体验，但也让部分不怀好意的“消费者”找到了商机，通过规则漏洞狠薅羊毛。

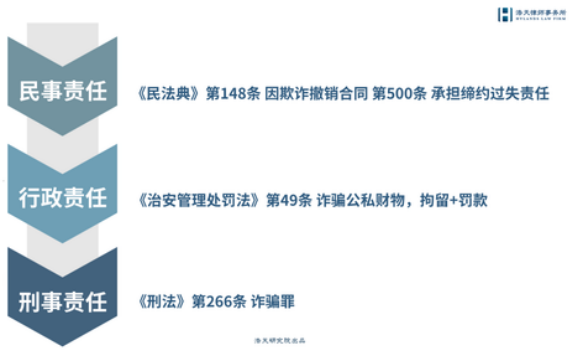
虽然今年各大电商平台逐渐收紧了仅退款的条件，并逐步将仅退款的决定权下放给商家，但正所谓道高一尺魔高一丈，在AIGC技术加持下，伪造商品瑕疵甚至商品损毁的虚假图片来骗取退款，更让商家苦不堪言，货款两失。

尤其是与传统P图软件相比，AI生成图片在像素、光影、纹理上更接近实拍，平台 OCR 识别、以图搜图等传统风控手段几近失效。

这不禁再次引起人们的思考：利用AI工具作恶，到底是人之恶还是工具之恶？（参见：《技术犯罪：从“工具之恶”到“主体之责”》）这其中各方的法律责任又该如何划分？

进一步的，《人工智能生成合成内容标识办法》即将在今年9月1日开始施行，这一典型现象，更加体现了标识义务在AIGC的合规要求中的核心地位，应引起AI从业者的重视。

一、恶意退款买家的责任定性



（一）民事责任：欺诈与缔约过失责任

恶意退款买家使用AI生成的虚假图片，虚构商品瑕疵，诱使平台和商家基于错误认识处分财产，构成《民法典》第148条的欺诈，基于此双方达成的退款合意，自然也可以被撤销。同时，平台或商家还可根据《民法典》第500条要求买家承担缔约过失责任，如造成了商誉损失，还可以追究名誉权侵权责任。

（二）行政责任：尚不入罪时的兜底

如恶意退款买家的欺诈金额，尚未达到3000元的刑事立案标准，或者虽达到但公安机关认为情节轻微的，可依据《治安管理处罚法》第49条，处以5–15 日拘留并处罚款。

（三）刑事责任：诈骗罪的门槛并不高

《刑法》上的诈骗罪，要求主观上以非法占有为目的，客观上要求虚假事实使受害人陷入认识错误并处分财物，恶

意退款买家通过虚假的图片，使平台或商家误以为其商品存在瑕疵而进行了退款，该行为符合了上述要件。数额方面，根据两高司法解释，单次或累计骗取货款3000元至1万元以上，即属“数额较大”，即可判处3年以下有期徒刑、拘役或管制，这可能不过是一部网购的手机的价格；对于团伙反复作案的，达到3万至10万元以上的“数额巨大”，乃至50万元以上的“数额特别巨大”标准，亦非难事。因此，该情形下诈骗罪极易被触犯。

二、电商平台的责任定性

电商平台与商家一般会签署平台服务协议，协议中对于仅退款申请事项，一般会约定平台的“合理审核”“及时通知”“保障交易安全”等义务。如果是平台批准的“仅退款”，需要对于平台是否尽到了合理审核义务而判断是否对商家有补充赔偿责任或连带赔偿责任。如有些仅退款AI图片中，AI水印都没有去除，平台就进行了自动或人工审核通过，其大概率要和买家承担连带责任。

三、生成图片的AIGC服务商的责任定性

（一）现有共同侵权和共同犯罪体系的沿用

如果AIGC模型开发者本就与恶意退款买家为有通谋的同伙，定向开发此类功能，或明知买家使用AI工具的不法用途还放任其使用模型的，在民事上会构成共同侵权，甚至构成刑法上的帮助犯或教唆犯等共同犯罪。

（二）AIGC合规对过错认定的影响

如没有通谋，也不知道相关事实，这个时候AIGC服务商的过错问题就会更为复杂。

对于AIGC生成内容的侵权责任，相关司法判例已经从AIGC服务商是否完成其合规要求角度，论证AIGC服务商的过错责任，如广州互联网法院判决的AIGC著作权侵权第一案中，就从《生成式人工智能服务管理暂行办法》规定的角度，从被告缺乏投诉举报机制、潜在侵权风险提示、生成物显著标识等合规内容，论证其在著作权侵权中的过错。（参见：《帮助侵权：AIGC文生图平台的侵权责任及合规建议》）因此，其AI合规不仅仅是行政管理要求，也是民事乃至刑事责任的标尺。

具体到本文讨论的场景，相信对于电商平台而言，解决此类问题最方便的方式，便是在技术上实现快速识别AI图片。而这种识别最便利准确的方式，便是识别AIGC服务商在AI图片中依规增加的显性标识和隐性标识。

从《互联网信息服务深度合成管理规定》，到《生成式人工智能服务管理暂行办法》，再到今年9月1日即将实施的《人工智能生成合成内容标识办法》，反复强调的标识义务，成为AIGC合规的核心义务。如果AIGC服务商未能妥善履行标识义务，导致电商平台对仅退款的审核不能识别AI图片，因此给商家造成的损失，恐怕AIGC服务商将难辞其咎。

十五、正反手教学：最高院首发“数据权益司法保护”指导性案例

主笔人



张金栋

北京浩天律师事务所 合伙人
zhangjindong@hylandslaw.com



寇梦宇

北京浩天律师事务所 律师
koumengyu@hylandslaw.com

2025年8月28日，最高人民法院发布首次以“数据权益司法保护”为专题的第47批指导性案例（262-267号）。

近年来我国数字经济发展迅猛，作为数字经济的核心要素，数据相关的各类经济活动形式多样，日新月异。但在制定法方面，我国对于数据权益保护的立法进度一直相对滞后，因此最新的司法判例，对于兼具数据权益享有者与信息处理者双重身份的企业而言，可以说是其充分保护自身经济利益和合规经营的核心依据。

该批案例聚焦数据权属、数据产品利用、个人信息保护等核心问题，为企业明确数据权益边界、信息处理规范并规避法律风险提供重要指引。

具体的，此次指导性案例采用了正反手教学的方式，比如第262号与第263号、第264号为企业间的数据权益纠纷，前者为原告胜诉案例，后两者为原告败诉案例；第265号与第266号均为自然人起诉企业对其个人信息收集行为的纠纷，前者胜诉，后者败诉。这种鲜明的对比，对于市场主体准确理解司法裁判精神颇有帮助。

一、指导性案例262号：数据集合经营性利益保护案

（一）基本案情

某科技公司运营甲APP，某文化公司运营乙APP。某科技公司在运营中发现，乙APP中有大量短视频、用户信息及评论与甲APP高度一致。某科技公司以未经许可进行数据搬运构成不正当竞争为由将某文化公司诉至法院。

（二）裁判观点及判决结果

1. 某科技公司对“短视频+用户信息+评论”数据集合投入资源，形成独立于单一短视频的经济价值。虽不构成汇编作品，无法用著作权法保护，但享有受保护的“经营性利益”；
2. 某文化公司未经许可抓取数据，导致两APP内容同质化、实质性替代甲APP提供服务，构成不正当竞争。

判决某文化公司在官方媒体消除影响，并赔偿某科技公司经济损失人民币500万元。

对于网络平台公司非独创性数据集合的“经营性利益”受法律保护，司法界可以说已经基本达成了共识，此类案件在北京、杭州、南京等城市司法系统已经有诸多可查询的公开判例，裁判理由和结果大同小异。本案判决时，制定法领域尚无对数据权益保护的直接依据，因此各判决均引用《反不正当竞争法》中的一般条款以及互联网专条的兜底条款作为裁判依据。

随着本案入选指导性案例，以及实施在即的新《反不正当竞争法》中的数据保护条款第一次在法律层面推出，此类案件的裁判原则可以说基本盖棺定论。

二、指导性案例263号:关联账号数据迁移案

（一）基本案情

某网络公司运营甲招聘网站，企业可在该网站付费查看求职者简历。某信息公司运营的乙网站设 “关联账号” 功能，企业用户在登录甲网站账号后可同步甲网站的求职者简历至乙网站并直接在乙网站上查看。某网络公司认为某信息公司“抓取简历”构成不正当竞争，诉至法院。

（二）裁判观点及判决结果

1. 用户有权转移自身持有数据（如购买的简历），“关联账号服务”是常见的服务模式，只要不侵害数据安全与他人权益即属于合法行为；

2. 某信息公司提供的服务需用户主动授权，未破坏甲网站运行或泄露信息，亦未侵害求职者合法权益，其行为具有正当性，不构成不正当竞争。判决驳回某网络公司的诉讼请求。

本案与第262号指导性案例，可以对照研究。两案均为网络平台对于数据的迁移使用，但判决结果迥异，其根本区别还是在于本案中被告的数据获取行为，取得了用户的同意，即用户对于其上传的信息和数据具有“可携带权”。即原告虽然对数据集合拥有“经营性权益”，但不能妨害用户对于自身数据的处置。这对于数据获取方的如何让数据获取行为正当化，提供了另一条思路。

三、 指导性案例264号：公开数据加工利用案

（一）基本案情

某钢铁公司通过微信群、电话公开钢材出厂价，某电子公司采集后用合规算法编制“钢材价格指数”（数据经过处理，非原始价格）并以会员制发布。某钢铁公司认为某电子公司擅自公布其价格数据属于侵权，诉至法院。

（二）裁判观点及判决结果

1. 某钢铁公司的出厂价是无保密措施的公开信息，不构成商业秘密，无权禁止他人合法采集；

2. 某电子公司采集方式合法，编制的价格指数符合标准，属合法数据产品，未损害钢铁公司权益。判决驳回某钢铁公司的诉讼请求。

本案同样可以与第262号指导案例对照研究，同样是数据抓取后的开发利用，两案判决结果迥异。这并非单一要素导致：本案在原告数据类型、是否采取保护措施、被告数据来源、原告数据对在被告产品中的占比、国家立法对于被告商业模式的明确许可、原告是否受损害等诸多方面，都与262号案有本质区别。这两个案例对照品读，更便于理解所谓“数据权益保护”和“鼓励数据流通”的司法界限到底在哪里。

四、指导性案例265号：APP过度收集个人信息案

（一）基本案情

某科技公司运营英语学习APP，未经罗某同意收集其手机号创立账号，登录时强制填写“职业、英语水平”等用户画像信息。罗某认为该APP侵害个人信息权益，诉至法院。

（二）裁判观点及判决结果

1. 依照相关行业规范，学习类APP必要信息仅为手机号，画像信息非提供服务所必需，未经个人同意不得收集并处理用户画像信息；

2. 该APP未提供“不同意画像信息的替代登录方式”，属“非自愿同意”，违反《个人信息保护法》。判决某科技公司停止处理并删除信息、赔礼道歉并赔偿罗某律师费、取证费用2900元。

《个人信息保护法》中明确，如未经个人同意或有其他法定情形，为订立、履行个人作为一方当事人的合同所必需的前提下，个人信息处理者方可处理个人信息。本案明确了以服务功能实现与否作为“必需”的判定标准，同时禁止变相强制“同意收集信息”，为提供相关服务的企业划定了清晰的合规红线。

五、指导性案例266号：“先享后付”信用信息收集案

（一）基本案情

黄某欢开通公交乘车码并使用“先享后付”服务时，点击“同意协议”（标蓝提示授权获取姓名、信用分）后被自动开通信用账户，遂诉某信用公司“强迫开通服务”侵害个人信息权益。

（二）裁判观点及判决结果

1. “先享后付”需评估风险，某信用公司收集信用信息属“订立/履行合同所必需”；
2. 服务协议条款有显著提示、用户可自主注销，不存在误导或强迫。判决驳回黄某欢的诉讼请求。

本案认可了在“先享后付”场景下对于用户信用相关信息的合理收集，可以与第265号指导案例对照研究，其核心还是在于本案中收集的信息为“合同履行所必需”，再辅之以依法告知、确保自愿以及最小必要等原则，就可以成为合规的个人信息收集行为。

六、指导性案例267号：网络账号执行变更实名案

（一）基本案情

法院判决“浪某仙”账号归某传媒公司，游某梅未交付且被羁押，传媒公司申请强制变更账号实名认证信息。

（二）裁判观点及判决结果

1. 仅交付账号密码无法实现完整交付（原权利人可重置密码）；
2. 执行账号交付需同步变更实名认证。

法院向平台发协助执行通知书对实名信息进行强制变更，最终案件执行完毕。

本案指明了“账号执行难”问题的解决方案，明确“账号交付=密码+实名认证变更”，对于被执行人不愿或无法配合的情况，应向平台公司发送协执，给出账号的强制变更路径，确保胜诉方权益落地。

最高院本次选取的六个案例均着眼于数据权益司法保护的关键领域。在数据权属与不正当竞争方面，既维护企业数据集合的经营性利益，又鼓励创新服务；在数据加工利用上，明确公开数据合法采集加工规则，避免数据垄断和信息封闭；于个人信息保护方面，精准区分必需与非必需信息收集情形，平衡服务与个人信息权益。在账号执行问题上，亦给出切实可行的交付方案。相关企业应将本次发布的裁判观点作为实操指引，我们也将继续关注数据权益相关的最新司法动态，帮助企业明确自身权益边界，合法合规收集、加工、使用数据，重视个人信息保护，以规避相关法律风险，在数字经济发展中稳步前进。

十六、标识办法：《人工智能生成合成内容标识办法》下的合规方案与行业启示

主笔人



邢丹丹

科技上市公司 法务
浩天研究院 行业顾问

随着人工智能技术的飞速发展，AI生成内容（AIGC）在各个领域广泛应用，改变了内容生产与传播的模式。然而，AIGC的快速发展也带来了虚假信息传播、内容来源混淆等问题，对网络生态和公众认知造成了挑战。2025年9月1日，《人工智能生成合成内容标识办法》（以下简称“本办法”）以及与之配合的《GB/T 45438-2025 网络安全技术 人工智能生成合成内容标识方法》同步实施，旨在规范AIGC的标识，保障内容的可追溯性与真实性。

一、新规背景与核心要求

（一）新规出台背景

近年来，生成式人工智能、深度合成等技术使得海量内容得以快速生成并在网络传播。虚假信息、深度伪造等问题不断涌现，削弱了公众对网络传播内容的信任根基。为应对这些挑战，国家互联网信息办公室联合工业和信息化部、公安部、国家广播电视总局制定了本办法，以规范人工智能生成合成内容标识活动，促进人工智能健康有序发展。

（二）新规核心要求

依据本办法，将符合《互联网信息服务算法推荐管理规定》、《互联网信息服务深度合成管理规定》、《生成式人工智能服务管理暂行办法》规定情形的网络信息服务提供者统称为“服务提供者”。对本办法拆解后可发现，为了实现全流程标识管理体系，可将“服务提供者”具体梳理成制作、传播、分发、使用四大环节的相应主体，企业应依据自身实际业务情况，对号入座、各司其职：



1.制作平台：源头嵌入双标识

作为内容生成起点，深度合成服务提供者需在制作环节同步添加标识：一是嵌入不影响使用的隐式标识（如文件元数据标签）；二是对易引发公众混淆的内容（如仿真人脸视频、拟真新闻文本），在合理位置（如视频角落、文本标题旁）加显式标识，从源头划清AI生成边界。此为本办法规制管理的重中之重，本文针对“深度合成服务提供者”，结合《GB/T 45438-2025 网络安全技术 人工智能生成合成内容标识方法》的要求做详细的合规解读。

2.传播平台：路径核验补标识

网络信息内容传播服务的服务提供者主要承担了内容流转中的检测责任，通过三重动作落实要求：核验文件元数据中的隐式标识、判断用户主动声明内容、用技术手段识别生成合成痕迹（如图片异常纹理、音频机械声纹），并据此在内容周边加显著提示，堵住传播中的标识漏洞。

3.分发平台：上架核验管入口

互联网应用程序分发平台聚焦应用程序分发环节，在AI生成服务类APP上架、上线时，必须核验其标识功能相关材料（如是否具备隐显标识添加能力），确保工具本身符合管理要求，从服务入口把控标识落实基础。

4.网民用户：发布主动做声明
普通用户作为内容发布终端，需在上传信息时主动声明是否含AI生成内容，并通过平台提供的功能完成标识添加，在内容触达公众前，履行个人层面的规范义务。

二、重点合规经验

深度合成服务提供者作为AI技术或者AIGC服务的提供者，相关符合此身份场景的企业需在AI生成物阶段就直接完成双重标识义务，是本办法的重点要求：1）显式标识：要求企业在生成合成内容或者交互场景界面中添加以文字、声音、图形等方式呈现且可被用户明显感知到的标识。2）隐式标识：采取技术措施在生成合成内容文件数据中添加不易被用户明显感知到的标识，包含生成合成内容属性信息、服务提供者名称或者编码、内容编号等制作要素信息；同时，鼓励添加数字水印等形式的隐式标识。

对于具体落实“双重标识义务”，可从以下步骤展开：

（一）业务排查与问题梳理
企业应在新规发布后，迅速组织专业团队对现有业务进行全面排查。通过梳理业务流程，明确了AI生成内容的主要应用场景，主要包括智能客服中的文本回复、智能设备生成的图片、音频等内容。就一般经验和当前行业示例排查发现，部分企业在标识方面仍有存在不足，主要表现在AI生成物显式标识时有时无，部分智能设备闲聊服务的音频回复未添加标识，智能客服对话的风险提醒不到位。

（二）显式标识的呈现方案
显式标识是让公众清晰知晓AI生成内容的关键手段，涵盖内容显式标识与交互场景界面显式标识两大类别，不同类型内容及场景的标识方式各有讲究：

内容显式标识			
生成内容的类型	形式	要素	位置
文本	文字	人工智能或AI+生成或合成 例如：AI生成	文本的 起始位置 末尾位置 中间位置（三选一）
	角标	包含“AI”	文本的起始位置、末尾位置、中间位置（三选一）
图片	文字	人工智能或AI+生成或合成 例如：AI生成	图片的边或角，文字高度不应低于画面最短边长度的5%非矩形图片的最短边：指可完全将该图片包含在内部的矩形的最短边。
音频	语音标识	人工智能或AI+生成或合成 例如：AI生成 汉语正常语速约在120字/min~160字/mi	音频的起始位置 末尾位置 中间位置（三选一） 在智能语音助手、智能客服、智能导航等音频的高频交互场景中，音频的起始位置、末尾位置是指一轮交互

	音频节奏标识	“短长 短短”的节奏（“AI”的摩斯码）	音频的起始位置 末尾位置 中间位置（三选一） 在智能语音助手、智能客服、智能导航等音频的高频交互场景中，音频的起始位置、末尾位置是指一轮交互 的起始位置和末尾位置。
视频	文字	人工智能或AI+生成或合成	视频的起始画面，放置在视频画面的边或角，显式标识持续时间不应少于2s 文字高度不应低于画面最短边长度的5%
虚拟场景	文字	人工智能或AI+生成或合成	虚拟场景的起始画面，放置在虚拟画面的边或角，文字高度不应低于画面最短边长度的5%
交互场景界面显式标识			
I 场景	**I 形式**	**I 要素**	**I 位置**
内容周边	文字	人工智能或AI+生成或合成	1)在内容展示区域附近持续显示提示文字； 2)在内容展示区域的背景均匀添加包含提示文字的显式水印标识。
非内容周边			1) 音频、视频交互区域附近持续显示提示文字； 2) 交互场景界面顶部、底部等适当位置持续显示提示文字。

（三）隐式标识的技术实现

元数据隐式标识是AI生成内容的“隐形身份档案”，为合规核心强制要求，需在文件元数据中嵌入含“AIGC”关键词的扩展字段，格式为固定JSON结构，含7项核心字段。

1.元数据字段设计：按照新规要求，字段分三类：一是属性标识，“Label”取值1-3对应“属于/可能/疑似”AI生成；二是主体与编号信息，“ContentProducer”将企业名转32位编码（如任一企业缩略名称的哈希+日期+序号），“ProduceID”为27位唯一码（具体业务ID哈希+内容类型编码+毫秒级时间戳）；三是安全与传播字段，“ReservedCode1”用SHA-256算法生成数字签名防篡改，传播相关字段首次写入时与生成端信息一致。所有字段值需符合国标GB18030-2022对特定码位的要求，技术上通过自动嵌入系统实现，在内容下载、导出时同步写入，支撑全生命周期追溯。

2.自动嵌入功能开发：开发自动嵌入元数据标识的系统，在用户下载AI生成的图片、文本以图片格式分享、音频文件导出等操作时，系统自动在文件元数据中写入相应的AIGC字段，实现隐式标识的无缝添加。

（四）形成对用户告知

企业需在用户服务协议中，以单独章节或醒目加粗形式，明确生成合成内容标识的全流程规范；其内容需涵盖标识方法，如隐式标识已嵌入文件元数据、显式标识需置于内容显眼位置（如图片右下角、视频播放区顶部、文本标题下方）；同时还需加入专门提示语，引导用户仔细阅读条款，例如“请您务必知晓：您发布的AI生成内容需按本协议规范添加标识，未合规标识可能导致内容下架、账号受限等后果”，确保用户清晰理解并遵守标识管理要求。

三、行业启示总结

（一）合规意识是企业发展的基石

实践表明，企业应主动将合规意识融入业务发展战略。在AI技术应用中，不能仅关注技术创新和业务拓展，更要重视合规要求。合规不是额外的负担，而是企业可持续发展的保障。通过积极响应新规，企业能够避免法律风险，提升品牌形象，增强用户信任。

（二）技术与管理协同推进合规建设

技术创新才能保障标识的实现。企业需要投入技术力量，开发适合自身业务的标识技术方案。无论是显式标识的呈现方式，还是隐式标识的元数据设计与嵌入技术，都需要结合业务特点进行创新，确保标识的有效性和稳定性。

完善管理流程确保落地。建立完善的管理流程，明确各部门在合规建设中的职责。从内容生成、审核到发布，每个环节都要严格执行标识规定。同时，加强对员工的培训，提高员工对新规的理解和执行能力。

（三）行业合作促进合规标准统一

在AIGC标识合规方面，行业内企业应加强合作。通过共享经验、技术交流，共同推动合规标准的统一和完善。行业协会可以发挥组织协调作用，制定行业最佳实践指南，促进整个行业的健康发展。例如，共同研究数字水印等隐式标识技术的应用标准，提高标识的通用性和互操作性。

十七、AI遇上司法：北京互联网法院8个典型“涉人工智能案件”解读

主笔人



张金栋

北京浩天律师事务所 合伙人
zhangjindong@hylandslaw.com



寇梦宇

北京浩天律师事务所 律师
koumengyu@hylandslaw.com

随着生成式人工智能、AI换脸、虚拟数字人等技术快速发展，AI作品属性、权利归属、人格权侵害等新型法律争议持续涌现。9月10日，北京互联网法院召开涉人工智能案件审理情况新闻发布会，对涉人工智能案件的审理思路及典型案例进行了发布。该批案例聚焦AI生成内容的权利保护、虚拟形象侵权、AI作品与人格权保护边界等问题，为相关企业合规经营提供重要指引。

一、案例一：AI文生图的法律属性及权利归属

（一）基本案情

2023年2月，李某通过某生成式人工智能大模型，经多次调整提示词、参数生成涉案图片，发布于小红书并附署名水印。同年3月，刘某在其百家号文章中使用该图片作为配图，擅自去除水印且未注明来源。

刘某认为李某侵害其署名权及信息网络传播权，诉至法院要求李某赔礼道歉并赔偿损失。

（二）裁判观点及判决结果

涉案图片具备“智力成果”与“独创性”要件：原告通过构思、设置参数、反复调整等智力投入形成个性化表达，属于著作权法保护的美术作品。

AI模型非著作权法规定的作者主体，而原告作为智力投入者享有著作权。被告未经许可传播图片且抹去原告署名，构成对信息网络传播权及署名权的侵害。

判决刘某赔礼道歉并赔偿经济损失。

《著作权法》第三条规定，本法所称的作品，是指文学、艺术和科学领域内具有独创性并能以一定形式表现的智力成果。本案明确了AI文生图属于艺术领域，只要能够体现创作者的智力投入并具有独创性，就属于美术作品，受到著作权法的保护。对于创作者而言，需要注意保留其创作过程，且输入指令越详细次数越多，越能体现智力投入。另一方面，此类案件也给图片使用者敲响警钟，即便是AI图片，也有侵权风险。（详见《AI文生图：AI生成图片的著作权保护｜数智通鉴》）

二、案例二：自然人声音权益保护及录音制品著作权边界

（一）基本案情

配音演员殷某发现他人利用其声音制作的配音作品在多款APP流传。经查，该作品来源于被告一开发的文本转语音产品。原告曾为被告二录制录音制品，著作权归被告二所有。被告二将音频提供给被告三，被告三经AI化处理生成涉案产品并通过被告四平台出售。被告一以被告五的名义向被告三采购该产品并进行使用。

殷某认为五被告侵犯其声音权益，诉至法院要求停止侵权、赔礼道歉及赔偿损失。

（二）裁判观点及判决结果

自然人声音具有独特性与可识别性，AI合成声音若能使公众通过音色、语调关联到特定自然人，即具备可识别性，受到法律保护。

被告二对录音制品的著作权不包含授权AI化使用殷某声音的权利，其与被告三未经殷某同意将其声音AI化使用的行为构成侵权。

判决被告一、三赔礼道歉，被告二、三赔偿经济损失。被告一、四、五无主观过错，不承担赔偿责任。

本案确立了AI化声音侵权认定的“可识别性”标准，其核心为经AI处理后的声音能否让公众关联到特定自然人。同时划清录音著作权与自然人声音权的边界，明确录音制品的著作权人不享有授权AI化使用他人声音的权利，为相关企业划定了明确的法律红线。

三、案例三：未经许可利用AI合成的名人声音进行“带货”的侵权认定

（一）基本案情

教育领域知名人士李某发现被告某文化公司在其运营的网络平台店铺中，使用李某的公开演讲、授课视频，并搭配与李某声音高度近似的AI合成声音，宣传推介所售家庭教育类图书。

李某认为某文化公司侵犯其肖像权与声音权，诉至法院要求赔礼道歉、赔偿损失。

（二）裁判观点及判决结果

涉案AI合成声音与李某音色、语调高度一致，结合李某在相关领域的知名度，公众可将其与李某建立对应联系，属于声音权益的保护范围。

某文化公司未经授权使用李某肖像及合成声音，构成侵权。且某文化公司与带货主播系委托关系、共享收益，却对带货视频未尽审查义务，应与主播承担连带责任。

判决某文化公司向李某赔礼道歉，赔偿经济损失及维权合理支出。

本案与案例二类似，都是将AI化声音的侵权认定与“可识别性”相挂钩。不同的是，本案将被侵权主体的知名度纳入了判定考量，进一步细化了判定标准。此外，本案还明确了电商委托推广中，商家不得以 “未参与制作” 主张免责，明确了商家对推广内容的审查义务。

四、案例四：未经授权对包含他人肖像的视频进行“AI换脸”处理的侵权认定

（一）基本案情

古风短视频博主廖某发现某科技公司未经授权，利用其出镜视频制作换脸模板，在涉案软件供用户付费使用。

廖某认为某科技公司侵犯其肖像权与个人信息权益，诉至法院要求赔礼道歉及赔偿损失。

（二）裁判观点及判决结果

肖像权侵权以 “可识别性”（指向特定自然人）为核心，被告换脸后模板保留的妆容、服饰等非人格要素，公众识别主体非廖某，也未对廖某的肖像进行丑化，不构成侵犯肖像权。

某科技公司未经授权收集廖某人脸信息用于算法融合换脸，构成个人信息权益侵权。

判决被告书面赔礼道歉，并赔偿廖某精神损失。

本案是对于肖像权保护“可识别性”的反向评述，明确了在不具备可识别性的情况下不构成人格权的侵权。但不构成肖像权侵权，不代表其收集、使用人脸信息的行为不需要授权，未经原告同意的情况下，依然构成个人信息权益的侵害。

在AI换脸的场景中，肖像权保护是结果导向，但人脸信息保护是过程导向，相关企业应注意在两个层面的合规风险。

五、案例五：网络平台利用算法工具检测AI生成内容的适度说明义务

（一）基本案情

唐某在某科技公司运营的网络平台发布一篇文字内容，被平台以“含AI生成内容未标识”为由隐藏并禁言一天。
唐某认为其未使用AI创作，申诉未果后向法院起诉，要求撤销处理并删除后台记录。

（二）裁判观点及判决结果
法院认可平台对AI内容标识的管理权限。
在举证责任分配上，其认定唐某的创作内容属于即时性文本，客观上无法提供创作底稿等证据，故该内容属于人类创作的举证责任不应由唐某承担。
某科技公司作为算法掌控方，未对AI生成判定结果及人工复核标准作出合理解释及适度说明，构成违约。
判决被告撤销内容隐藏、删除相关记录。

本案首先肯定了平台对于AI 生成合成内容进行审查和处理的责任。其次，明确了即时性文本场景下，平台对AI生成内容的算法决策负有适度说明义务，相当于为平台设定了更高的举证责任。据此，为避免法律风险，平台可以尝试提高算法决策过程的透明度，避免因无法说明而承担违约责任。

六、案例六：利用AI软件恶搞、丑化他人肖像的侵权认定

（一）基本案情
程某与孙某系摄影交流微信群成员。孙某未经程某同意，用其微信头像肖像照片，通过AI软件生成衣着暴露的动漫图发至群内；程某制止后，孙某又继续用程某头像生成暴露且身体畸形的动漫图私信发送程某。
程某认为孙某侵犯其肖像权、名誉权及一般人格权，诉至法院要求孙某赔礼道歉并赔偿损失。

（二）裁判观点及判决结果
涉案AI图片与程某头像体貌高度对应，群成员可识别为程某，群发行为侵犯程某肖像权。
将程某的肖像生成暴露图片在群内引发低俗讨论，构成名誉权侵权。
私信发送利用程某肖像生成的暴露且身体畸形的图片，势必导致程某心理屈辱，侵犯一般人格权。
判决孙某公开赔礼道歉，赔偿精神损失。

本案划定了普通用户利用AI技术的行为边界，用AI工具对具体个人照片进行恶搞改编，极容易侵犯人格权，AI软件使用者在使用过程中一定要遵纪守法，AI并非法外之地。

七、案例七：虚拟数字人形象的法律属性

（一）基本案情
甲公司与乙公司联合制作虚拟数字人甲、乙。其中甲公司为著作权人，乙公司为被许可人。虚拟数字人甲在各平台粉丝数量超440万，且曾获得行业奖项。后甲乙两公司发现，孙某在某模型网上擅自售卖两数字人模型。
甲乙两公司认为孙某侵犯其复制权、信息网络传播权，诉至法院，要求孙某赔偿损失。
裁判观点及判决结果

（二）裁判观点及判决结果
甲、乙两数字人形象非源于真人，能够体现制作团队独特美学选择，具有独创性，构成美术作品。
孙某售卖的模型与涉案作品实质性相似，侵犯两公司信息网络传播权。
判决孙某赔偿经济损失。

本案与案例一相似，再次明确了以“独创性”为核心的美术作品认定标准。虚拟数字人由外在表现和技术内核两部分构成，在外在表现层面只要能够体现作品的独创性要求，就可以被认定为美术作品，受到著作权法保护。

八、案例八：未经同意创设自然人AI形象的人格权侵权认定

（一）基本案情
某科技公司运营的记账软件向用户提供创设 “AI 陪伴者”的服务。公众人物何某被大量用户设为陪伴人物，有用户上传其肖像设为头像并设置虚拟关系。某科技公司通过算法向其他用户推荐该角色，提供“调教”机制让用户上传语料、表情，经筛选后用于互动，营造与真人互动的体验。
何某认为某科技公司侵害其姓名权、肖像权及一般人格权，诉至法院要求赔礼道歉并赔偿经济损失及精神损失。

（二）裁判观点及判决结果
某科技公司算法设计下形成的何某虚拟形象，未经许可使用其姓名、肖像，构成姓名权、肖像权侵权。
软件中虚拟身份设定及互动体验侵害何某人格尊严与自由，构成一般人格权侵权。
某科技公司通过规则与算法鼓励用户生成侵权内容，实质参与了侵权行为，应作为内容服务提供者承担侵权责任。
判决某科技公司公开赔礼道歉，赔偿精神损失及经济损失。

本案确立了自然人的人格权保护及于其虚拟形象的司法观点。未经许可创设、使用自然人虚拟形象的，构成人格权侵权。同时，网络服务提供者通过算法设计实质参与了侵权内容的生成，不同于仅提供技术服务的中立主体，不适用避风港原则，应当承担侵权责任。（参见《帮助侵权：AIGC文生图平台的侵权责任及合规建议｜数智通鉴》）

九、结语

当前人工智能领域技术迭代迅猛，相关立法仍存在一定的滞后性。本次北京互联网法院发布的8个典型案例，提供了极具实操性的指引，对于相关领域内企业的合规经营和稳步发展具有重要的参考意义。相关企业应持续关注此类司法动向，将明确的裁判规则融入自身产品开发、运营审查全流程，明确司法红线，规避法律风险。

十八、AI大模型隐忧：首例处罚案例的启示与PIA实践

主笔人



刘晓霞

北京浩天（上海）律师事务所 合伙人
liuxiaoxia@hylandslaw.com

在今年的网络安全周期间，各地公安机关监管部门深入推进“护网—2025”专项工作，聚焦整顿网络和数据安全问题。在这一背景下，一起处罚案例引起了业界和公众的广泛关注。这起首例因人工智能大模型训练数据在处理算料时未开展个人信息保护影响评估（PIA）而被处罚的案例，涉及人脸等生物识别类敏感个人信息的处理问题。该案不仅凸显了AI产业链的潜在合规风险，也向整个行业传递了明确的监管信号：合法合规的数据，是AI大模型研发的基石。

本文将结合本次案例，梳理执法背景、案件要点，提供PIA工作落地实践，并从数据律师专业角度提出可操作的合规建议，帮助企业在创新与合规之间找到平衡。

一、案例速览首例PIA处罚案例回顾

在本次执法专项行动中，公安机关发现一家主营人工智能模型训练基础数据（算料）的科技公司，在处理涉及人脸等敏感个人信息时，没有依照《个人信息保护法》开展必要的个人信息保护影响评估（PIA）。这一违法行为被属地公安机关依法处罚，并责令企业整改。此次处罚是近期国家网络与信息安全信息通报中心发布的典型案例，也是国内首例因未进行PIA而受到处罚的案例。

这起案例透露出重要信息：监管执法已进入深水区，企业在数据收集、存储、处理和共享环节都必须合法合规，尤其是AI大模型训练涉及的高风险数据处理活动，如果未依法进行PIA和其他合规管理工作，将面临行政处罚、商业声誉受损、业务暂停甚至停业整顿的风险。

二、PIA开展依据 数据合规必修课

在AI训练数据处理过程中，PIA（Privacy Impact Assessment，个人信息保护影响评估）不仅是一种合规工具，更是一种企业风险管理和业务优化手段。《个人信息保护法》第五十五条明确规定，在处理敏感信息、进行自动化决策、委托处理、向他人提供或公开个人信息，以及跨境传输等高风险活动时，企业必须事前开展PIA，并形成完整记录。《人脸识别技术应用安全管理办法》则进一步明确，涉及人脸识别数据的处理活动应遵循合法、正当、必要性原则，要求企业在用该类数据训练AI模型前，应当事前进行个人信息保护影响评估，并对处理情况进行记录。

三、PIA实施阶段训练数据合规的全流程拆解

针对AI大模型的数据训练特点，PIA应覆盖从数据采集、存储、预处理、训练使用，到模型输出及共享或出境的每一环节。以下表格概括了七个关键阶段及主要工作内容，展示了PIA在企业合规实践中的落地路径。

阶段	关键工作	内容
评估准备	• 确认评估必要性 • 组建评估团队 • 制定评估计划	分析训练数据类型与敏感度，明确涉及部门及外部顾问，制定评估日程和资源分配
评估对象分析	• 梳理数据处理流程 • 明确业务场景	全面盘点数据采集、存储、预处理、模型训练使用及共享/出境环节，形成业务全景图
数据映射与风险识别	• 构建数据映射图 • 识别潜在风险	分析内部/外部威胁、技术脆弱点、管理流程缺陷，明确风险来源与可能影响

风险评估与整改	• 进行风险评级 • 制定整改措施	根据风险等级采取立即整改、限期整改或接受风险，形成整改清单并落实执行
风险处置与持续监控	• 监督整改落实 • 定期更新评估结果	建立数据安全事件应急处理机制，优化流程，确保持续符合合规要求
PIA报告制作	• 完整记录评估全过程 • 总结风险及处置方案	包含团队信息、数据类型、影响分析、整改建议及持续跟踪计划，形成可供管理层和监管参考的正式报告

PIA是企业践行“合规前置、风险可控”的核心手段，也是AI训练数据安全的重要守护者。

风险管理清单

AI大模型训练数据管理要点

在完成对大模型训练数据全生命周期的梳理后，企业需要建立一套系统化的合规风险管理清单，将训练过程中可能涉及的所有风险环节纳入管理。核心内容包括以下环节：

风险管理环节	核心内容	关键措施
数据获取	确保训练数据来源正规、合同或授权明确	签署合同、获取授权、审查数据来源渠道等
敏感信息处理	人脸、声纹、指纹等敏感信息需单独告知和同意	明确告知用户、获取单独同意
PIA（个人信息保护影响评估）	高风险处理活动前开展评估，识别潜在合规风险	全面分析数据处理流程、风险评级、整改方案、留存报告
数据存储与使用安全	全流程安全管理，防止泄露或滥用	加密存储与传输、脱敏处理、访问控制、审计机制
数据共享与对外交付	与第三方共享或提供数据前，明确责任和合规要求	签署数据共享协议、进行合规审查、留存记录
跨境数据传输	出境数据需安全评估或签署标准合同	出境前评估、合同约束、加密传输
风险跟踪	对已识别风险实施跟踪和动态管理	定期复审、风险等级更新、改进措施落地

四、PIA实践要诀一定要做“真功夫”

结合监管要求与服务经验，对于企业如何更好地开展PIA工作，我们提示以下实践要点：
建立标准化流程：建立覆盖数据类型、处理目的、风险分析和缓解措施的PIA模板；明确责任与审批：明确PIA负责人，建立审批和备案机制，确保责任到人；书面留痕：每一次高风险处理活动都应形成独立PIA报告，避免走形式；业务前置嵌入：将PIA流程嵌入数据采集、模型训练和跨境交付环节；供应链合规协同：要求合作方同步开展PIA或提供合规证明，防止合规断层；跨境衔接：依据PIA评估结果，决定是否触发数据出境安全评估或签署标准合同。定期培训：对关键人员开展数据保护和隐私合规培训，确保充分理解、掌握PIA流程与操作规范，能够在日常工作中主动发现和防控风险。
通过这些措施，企业不仅能降低违法风险，也能提升数据处理的透明度和可信度，为业务合作和市场拓展提供法律保障。

五、结语——让PIA成为AI企业的护身符

首例处罚案例及监管释放的信号表明，数据合规不是可选项，而是企业创新发展的必备底线。落实PIA和全流程安全管理，不仅防范监管风险，更为企业赢得市场信任、提升品牌竞争力提供坚实保障。合规不再是约束，而是创新发展的护航力量。

AI训练数据的合规工作，需要企业从制度设计、技术实现、业务流程到供应链管理全面覆盖。只有将PIA落实到实际操作中，才能在创新、发展与监管之间取得平衡，实现高质量的人工智能产业发展。

十九、数据交易：数据授权运营的“三道防御工事”

主笔人



叶建芳

京浩天（杭州）律师事务所 主任
yejianfang@hylandslaw.com



宁莉莉

北京浩天（杭州）律师事务所 律师
ninglili@hylandslaw.com



吕文易

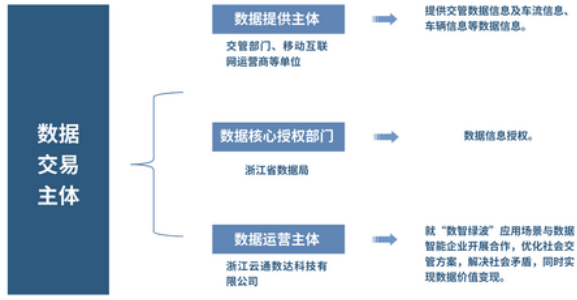
北京浩天（杭州）律师事务所 律师
lvwenyi@hylandslaw.com

自2022年12月19日“数据二十条”公布以来，社会各行各业就数据开发、共享、授权运营开始全面探索。其中数据授权运营是数据释放价值的关键步骤。那么什么是数据授权运营呢？

一、数据授权运营定义与发展掣肘

定义数据授权运营是指授权方将其持有的数据资源，按照法律法规要求，授权符合条件的运营机构进行治理、开发，形成数据产品和服务，向社会需求单位提供并获取合理收益的行为。
具体举例而言，如浙江省在数智交管行业的实践案例“数智绿波”项目。浙江省数据局在2025年6月4日发布公告，浙江云通数达科技有限公司成为浙江省交通运输领域首批省级公共数据授权运营单位，依法开展公共数据授权运营活动，具体应用场景为“数智绿波”场景。

浙江省数智交管行业实践案例——“数智绿波”项目示意图



在该场景下的源数据主要为交管部门的交管数据信息及移动互联网运营商等单位提供的车流信息、车辆信息等数据信息，交管部门及移动互联网运营商等单位系数据提供主体，数据核心授权部门为浙江省数据局，而浙江云通数达科技有限公司作为被授权运营单位，承担数据运营主体角色，就“数智绿波”应用场景与数据智能企业开展合作，优化社会交管方案，解决社会矛盾，同时实现数据价值变现。前述参与单位都可以称之为数据交易主体。

目前，数据授权运营尚处于发展期，在实际操作中，因法律法规、政策文件的层层监管要求，数据交易流通过程中仍存在很多的合规盲区，如何全面合规地释放数据价值，促进数据业务发展，已成为发展数据业务的企业普遍关注的焦点。本文将从数据授权经营的“三道基础防御工事”出发，提供法律建议。

基础防御工事一：授权前置性审查，避免“瑕疵”数据源

数据来源合法性检验是确保数据质量有效可靠、分析结果可信任的关键第一步。

数据来源合法性检验	
数据交易主体的合法性检验	• 境内合法成立的单位，在其经营许可范围内使用合法技术手段获取数据； • 在获得个体同意的情况下收集； • 其他数据交易主体也应当是合法成立企业。
数据收集、汇集手段的合法性检验	• 政府主动公开的数据，应注意该等数据使用限制性要求； • 网络抓取数据，需检验是否有数据来源方的合法授权； • 自有数据，应自行检查数据产生系统、数据产生流程的规范性及安全性等。
数据完整性检验	• 数据内容是否存在数据值缺失； • 数据日志是否完整； • 数据是否存在人为篡改痕迹等。
数据时效性检验	• 授权数据收集起始时间； • 数据更新频率。
数据关联性检验	• 结合数据使用目的及数据应用场景设计需求，对授权数据适配度进行检验。
数据清洁度检验	• 检查授权数据是否经过过滤、清洗，主要围绕国家秘密信息、个人隐私信息等重要数据进行脱敏处理。

（一）数据交易主体的合法性检验

提供数据的主体（如“数智绿波”场景中的交管部门、移动互联网运营商等单位）首先必须是境内合法成立的单位，其应当在经营许可范围内使用合法技术手段获取数据；其次，该等数据应是在获得个体同意的情况下收集的，这是数据来源合法可靠的前提基础；第三，其他数据交易主体也应当是合法成立企业，在数据监管部门的监管下合规开展数据交易及数据产品应用业务。

（二）数据收集、汇集手段的合法性检验

数据来源包括政府公开数据，网络抓取数据及自有数据。如为政府主动公开的数据，应注意该等数据使用限制性要求；如为网络抓取数据，需检验是否有数据来源方的合法授权，授权是否明确使用条件、使用范围、使用限制等；如为自有数据，应自行检查数据产生系统、数据产生流程的规范性及安全性等。

（三）数据完整性检验

主要围绕数据内容是否存在数据值缺失、数据日志是否完整、数据是否存在人为篡改痕迹等开展，以保证授权应用、开发的数据是充分完整的数据。

（四）数据时效性检验

检查授权数据收集起始时间，数据更新频率，以保证应用、开发的数据的有效性。

（五）数据关联性检验

结合数据使用目的及数据应用场景设计需求，对授权数据适配度进行检验，保证所供数据能被有效、高质量地使用。

（六）数据清洁度检验

检查授权数据是否经过过滤、清洗，主要围绕国家秘密信息、个人隐私信息等重要数据进行脱敏处理，以保证授权数据的清洁度，不存在任何违法违规情形。

因数据本身存在量大、非结构化等特点，导致授权数据的使用存在一定局限性和使用误差，所以需要数据交易主体前置性地评估数据质量及后期使用可能产生的影响。

数据的更新迭代注定数据检查是一个持续性工作且是个多维度的工作（不仅限于上述六个角度），数据交易主体应持续做好数据的前置性审查工作。

基础防御工事二授权运营方案设计，构筑数据安全“防火墙”

（一）数据授权运营原则

数据授权应遵循正当性原则：明确最终使用场景、解决问题及数据价值实现方案，禁止超授权范围使用数据。数据授权应遵循最小必要性原则：在“原始数据不出域、数据可用不可见”的政策下，仅许可数据运营单位使用数据场景所必需数据字段进行研发，避免数据过度使用、滥用等不当使用行为，以致数据安全风险。

特殊数据脱敏：在数据授权过程中，数据交易主体应对生物识别、医疗健康等敏感信息进行层层脱敏，在此过程中需要通过技术及合规措施进行专业评估，通过层层过滤加码，保障信息安全。

（二）数据授权运营协议设计

以示范文本为引导：2025年7月2日国家数据局综合司、市场监管总局办公厅发布了《关于印发数据流通交易合同示范文本的通知》，示范文本聚焦数据流通中最典型的4类场景，即数据提供、数据委托处理、数据融合开发和数据中介，供数据市场经营主体使用。该4类合同的条款设计包含了数据产权约定、安全保密要求、违约责任、争议解决等通用条款，还包含了不同交易场景下交易方特定的权利义务要求、数据交付和验收标准等。此次示范合同主要是针对市场需求的引导性合同，对数据交易流通起到了指导性作用。

个性化条款设计：因为数据交易性质的特殊性，不同交易场景亟待解决的社会问题的特殊化，导致交付数据存在不一样的标准要求，在同一场景下交付的数据还会有参差不齐的问题，所以在示范文件引领下，还需要数据交易主体结合特定场景进行个性化需求设计，如不同场景下的数据质量标准设计，数据产品个性化合作方案拟定及利益分配设置等，数据授权运营全流程的细节化协议设置是为了更好地规范数据交易，保障交易方利益及数据价值的持续释放。

基础防御工事三：执行风险管理，给数据安全“上保险”

（一）履约监督

数据授权执行过程中，需要授权方严格监督被授权方是否在授权方案范围内使用数据，如涉及授权事宜变更调整的，双方应及时签订书面协议，调整合作方案。

（二）风险预警及合规处置

数据交易主体均应制定相应的事件响应计划、灾难恢复计划、数据恢复流程、危机公关预案等数据管理系统性文件及预案。如发生数据安全事件，交易方应通力合作，及时向数据监管部门进行报告，将事件影响及损失最小化。对被授权方不当使用数据的违约或违法行为，授权方应及时采取工作联系函、律师函警告纠正，如违约情节严重的，还可以通过诉讼/仲裁方式解决双方争议纠纷，甚至要求属于主管部门以监管等形式参与数据交易的纠偏工作。

（三）动态性政策调整

数据交易方均应时时关注数据监管新规，根据陆续出台的新法律法规、政策或行业标准，及时调整授权方案，保证数据项目的持续合规开展。

（四）技术协同合规双驱动

数据开发单位可将项目过程合规要求转化为可执行的代码规则，嵌入数据标签系统，限定数据使用范围，防止场景应用中不当使用数据或泄露安全信息等。

数据授权运营执行风险管理是个多维度的动态监管过程，远不止上述的四个方面，数据交易主体应结合不同的应用场景全方位审查防范风险，保障数据交易业务的健康发展。

结语

数据运营授权的本质是数据交易，经营主体在交易过程中应从前置审查、授权方案设计及后期风险管理，用技术+法律手段全流程规划设计，平衡法律风险及数据价值，构筑数据交易安全护城河，促进数智经济持久健康发展。

二十、AI换脸：数字假面可能"两面侵权"

主笔人



张金栋

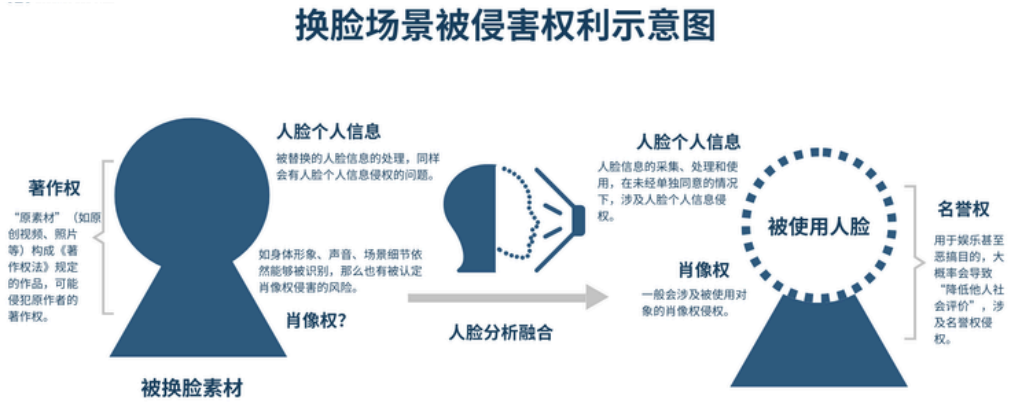
北京浩天律师事务所 合伙人
zhangjindong@hylandslaw.com



寇梦宇

北京浩天律师事务所 律师
koumengyu@hylandslaw.com

央视主播现身网络直播间播报鱼油广告？已故茶界泰斗“复活”做起品牌代言？随着AI技术加速迭代，AI换脸技术逐渐应用于内容创作、营销推广、休闲娱乐，但在使用AI换脸技术进行商业活动的过程中，由于涉及“人脸”这一人格权核心载体，同时涉及被换脸素材和换脸人脸等多方权益，极易触及法律红线，产生各类侵权责任：肖像权争议、人脸敏感信息违规、著作权侵权等各类纠纷频发，给AI换脸技术使用者敲响警钟。



本文将尝试从不同的被侵权方角度，即被使用人脸方和被换脸素材方两方面，结合现有司法实践，对AI换脸的两面侵权类型进行详细梳理。

一、针对被使用人脸方

（一）肖像权侵权：显而易见的侵权责任

对于被使用人脸的一方，由于在AI换脸的实质就是希望能使用公众或某些特定对象熟知的形象，并利用其影响力实现商业目的，因此一般会涉及被使用对象的肖像权侵权。

例如：西安市雁塔区人民法院在佟某诉陕西某食品公司肖像权纠纷一案中认为，被告在其小红书账号发布经AI换脸技术制作的含有佟某肖像的视频，用于公司的销售推广，对消费者会产生误导，构成对佟某肖像权的侵权，应发布致歉声明、赔偿经济损失及佟某的维权合理支出。*详见：西安中院《AI换脸侵犯肖像权、“外来户”索要征地补偿款……西安法院发布民法典适用典型案例》

（二）人脸个人信息侵权：对人脸（肖像）不同侧重角度的保护

同理，人脸信息属于《个人信息保护法》中规定的“敏感个人信息”，处理此类信息需满足“单独同意+明确告知”的双重要求，AI换脸技术涉及对于被使用人脸和原素材人脸特征的分析和融合，其必然涉及人脸信息的采集、处理和使用，在未经单独同意的情况下，还涉及人脸个人信息侵权。

（三）名誉权侵权：以“社会评价降低”为标准

如果将AI换脸用于娱乐甚至恶搞目的，尤其是将他人面部合成至不雅视频等场景中，大概率会导致“降低他人社会评价”，涉及名誉权侵权，情节严重者可能构成刑事犯罪。

包头市青山区人民法院在某女与某男肖像权纠纷中指出，某男未经允许将某女照片利用AI换脸技术合成性感舞蹈视频，并配上“求关注”文案在快手平台发布。其行为客观上导致某女社会评价降低，生活安宁被侵扰，严重损害某女的肖像权和名誉权。*详见：包头中院《【以案释法】“AI换脸”不是“遮羞布”：一纸判决守住数字时代的肖像尊严》

二、针对被换脸素材方

（一）肖像权侵权：以“可识别性”为核心判断标准

对于被使用人脸的肖像而言，肖像权侵权很容易理解。但对于原始素材中被替换的人脸，其肖像权是否也被侵犯呢？对于这一问题，京沪两地的司法裁判结论相反。

肖像权侵权的核心要件为“未经同意+具备可识别性”。其中 “可识别性” 是以面部特征为核心，身体形象、声音、场景细节同时作为参考的判断标准。

判例一： 上海市金山区人民法院在赵某涵诉某科技公司肖像权纠纷案中认为，涉案视频除脸部特征以外，动作、背景、视频角度均与原告发布的抖音视频高度一致，且部分视频存在明显AI换脸痕迹。并且，原告抖音账号具有一定的粉丝量，被告虽将原告视频中的人物形象的脸部替换掉，但熟知原告的粉丝仍有可能识别出人物形象的对应主体应为原告，具备可识别性。故被告发布涉案视频侵害了原告的肖像权。*详见：（2023）沪0115民初52178号

按照这一逻辑，如果被换脸一方依然能够被识别，那么也有被认定肖像权被侵害的风险。

判例二： 北京互联网法院持不同观点，在林某诉北京某科技公司肖像权纠纷一案中则持不同观点：法院认为，虽然被告确实使用了原告的视频制作AI换脸模板，但该视频中人物面部已经被替换，消解了肖像所具有的“个体识别”特征。而妆容、发型、服饰、灯光等要素并非无法与特定自然人所分割的要素，无法与特定自然人形成对应关系。故被告的行为不构成肖像权侵权。*详见：（2023）京0491民初12766号

这一观点在北京互联网法院的廖某诉某科技公司网络侵权责任纠纷一案（（2023）京0491民初3820号）中再次被重申。两案裁判时间仅相隔六天，由此可以判断，在北京互联网法院内部，这一观点已经基本达成共识。

（二）人脸个人信息侵权：敏感信息的特殊保护

如前文所述，法律对于人脸个人信息的保护，与肖像权不同，不以可识别性为前提，即便最终未形成可识别肖像，处理过程本身仍可能构成侵权。

而AI换脸技术的应用，需要涉及对被替换的人脸信息的处理，因此同样会有人脸个人信息侵权的问题。例如在前文提到的北京互联网法院在廖某诉某科技公司网络侵权责任纠纷一案中指出，针对涉案AI换脸行为，被告收集、分析廖某的面部特征、表情等并将其人脸替换，需要处理廖某的人脸信息，属于对个人信息的处理。其处理行为未获单独同意，更未告知廖某，构成对廖某个人信息权益的侵害。该案亦入选北京互联网法院涉人工智能案件典型案例。

（三）著作权侵权：“实质性相似”的认定

如果AI换脸使用的 “原素材”（如原创视频、照片等）构成《著作权法》规定的作品，可能侵犯原作者的著作权。判断是否侵犯著作权的核心是 “实质性相似”：如AI换脸仅替换人物面部，未改变原作品的核心表达（如内容运镜、剪辑、音乐等），则构成实质性相似，属于著作权侵权。

上海市嘉定区人民法院在陈某诉上海某网络公司著作权纠纷一案中认为，案涉视频属于视听作品，被告运营的某小程序中展示的视频系通过AI算法将原始视频进行局部替换合成，二者构成实质性相似。且被告以AI换脸为卖点，向用户提供以换脸方式使用原视频而谋取商业利益，既非独创性改编，亦不属于合理使用，侵害了陈某的著作权。*详见：上海高院《全国优秀案例，2+3！》——最高人民法院《中国法院知识产权司法保护状况（2024年）》白皮书及2024

年人民法院知识产权典型案例

综上可见，在AI换脸应用的场景中，单单民事责任而言，可能触及的侵权类型就非常多样，步步是坑，很容易触及法律边界。因此相关主体打算使用AI换脸技术进行商业活动时，一定要三思而后行。

二十一、APP合规：数十家头部外资/国资App被点名，别让“形式合规”成为致命漏洞

主笔人



宋海新

北京浩天（上海）律师事务所 合伙人
songhaixin@hylandslaw.com

据不完全统计，2025年以来，先后有数十家外资、国资App被地方通信管理局、国家计算机病毒应急处理中心等监管部门和相关机构公开通报违法违规收集使用个人信息、侵害用户权益。例如，仅上海通信管理局2025年8月5日、2025年10月10日就先后集中公开通报了二十余家外资App[1]、十余家国资金融机构的App[2]侵害用户权益，其中多数外资企业、国资企业为大家所耳熟能详，再次引起社会各界特别是App运营者对App通报的广泛关注。

从分布行业看，被通报的数十家外资企业行业覆盖咖啡、快餐、汽车、医疗器械、半导体、零售、银行、酒店、制造业、化工、卫浴、办公用品等；被通报的数十家国资企业行业覆盖银行、航空、医药、证券、保险、信托、期货、基金、零售等。

从通报次数看，同一家外资/国资企业的多款App同期被通报的次数最多达到12次以上，单一外资/国资App先后被多次通报的次数最多达到5次以上。

为帮助大家更好地了解App合规的要点，我们结合APP近期通报情况，系统梳理了十一个关键问题，旨在拆解App合规监管的现状、流程、依据、趋势及应对建议。

一、问题一：为什么今年这么多外资、国资等App被公开通报？

2019年1月25日，中央网信办、工业和信息化部、公安部、市场监管总局联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》，拉开了App长达数年的常态化违法违规检测、通报和治理的大幕。

2025年3月28日，中央网信办、工业和信息化部、公安部、市场监管总局联合发布《关于开展2025年个人信息保护系列专项行动的公告》，将App违法违规检测、通报和治理纵深推向了新的阶段，也就有了这么多外资、国资等App被公开通报的出现。

二、问题二：通报的App来源仅包括手机端和小程序端吗？

通报的App来源包括手机端App、小程序、SDK、TV端App[3]、车载App[4]、智能音箱、门锁、电话手表等智能终端[5]等。其中，手机端包括各大主流应用商店；被通报的小程序多为微信小程序，但并非仅为微信小程序，例如，工信部信息通信管理局2025年9月18日就集中通报了24款支付宝小程序侵害用户权益行为[6]。

三、问题三：通报App违法违规的监管部门和相关机构主要有哪些？

从政府部门看，主要包括工业和信息化部和地方通信管理局、中央和地方网信部门等。
从相关机构看，主要包括国家计算机病毒应急处理中心、公安部计算机信息系统安全产品质量监督检验中心等。

四、问题四：App违法违规的检测需要企业配合才能检测吗？

不需要。App违法违规的检测是无感的，检测机构可以从公开渠道获取App，直接使用抓包工具、模拟普通用户操作等技术手段进行和完成检测，不会事先通知App运营者，也无需App运营者的配合。

五、问题五：App违法违规通报有可能“误诊”吗？

有可能，但可能性不大。检测机构在检测的同时，也会将相应的检测报告留存作为证据，通报的问题背后都有对应的违法违规证据支撑。同时，通报中也会载明存在问题的App的版本号，即使刚好在检测和通报的期间更新解决了问题，也不影响此前版本存在违法违规问题的认定。

六、问题六：App违法违规一旦发现就直接公开通报吗？

常规流程是检测发现违法违规问题后，通过应用商店、微信公众平台等App所属平台通知App运营者限期整改。如果整改完毕且复核通过，则不予公开通报。如果App未整改完毕则会进行公开通报，并在公开通报中最后说明限期整改的时间。
但实践中也出现过某地检测发现App违法违规问题后就直接公开通报的案例（该地最新流程已恢复为先内部通知），对企业来说整改时间会较为仓促。

七、问题七：App违法违规公开通报后一般有多长时间的整改期？

实践中常见的整改期限有5个工作日、15个工作日、30日内等，不同的通报部门、机构要求的整改期限不一致，应以具体通报要求的整改期限为准。

八、问题八：App被公开通报后未按期整改完毕的后果是什么？

直接的后果一般是应用市场下架，监管部门还可以视情况进一步采取停止接入、行政处罚、纳入电信业务经营不良名单等后续处理措施，例如文首提及的上海通信管理局2025年8月5日集中通报的外资App中有多款App未按期整改完毕，上海通信管理局对其进行了下架处理并于2025年9月16日通报了下架的情况[7]。

间接的后果在于对企业合规情况的长远影响，例如如果被公开通报的企业有融资（IPO、投资方投资等）的需求，会面临投资方律师、发行人境内律师、发行人境内数据合规律师、保荐人等的重点核查，增加很多不必要的麻烦，严重者甚至可能影响融资的结果。

九、问题九：App违法违规认定的主要依据有哪些？

从法律层面看，主要有《网络安全法》《个人信息保护法》。
从法规等规定层面看，主要有《网络数据安全管理条例》《电信条例》《电信和互联网用户个人信息保护规定》《App违法违规收集使用个人信息行为认定方法》《常见类型移动互联网应用程序必要个人信息范围规定》《工业和信息化部关于开展纵深推进APP侵害用户权益专项整治行动的通知》《工业和信息化部关于开展信息通信服务感知提升行动的通知》《工业和信息化部关于进一步提升移动互联网应用服务能力的通知》等。

十、问题十：App违法违规的常见通报问题以及监管最新关注问题包括哪些？

从近年来常见的问题类型来看，主要包括：

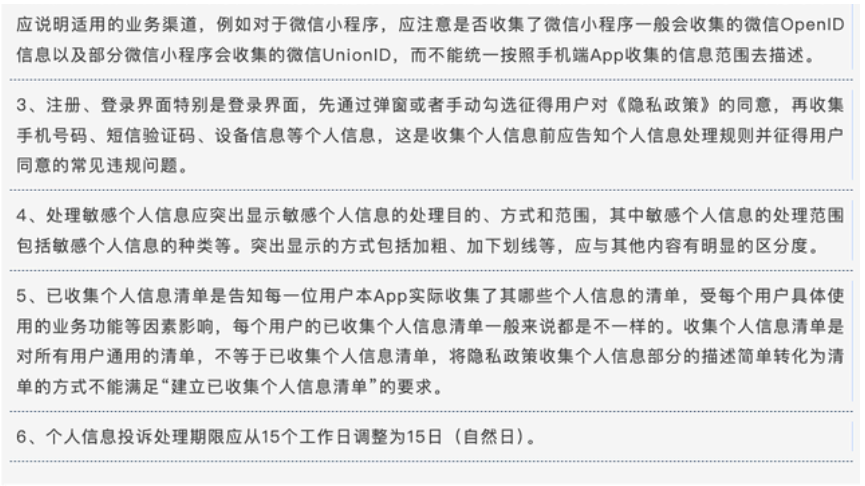
App违法违规的常见通报问题类型
1、未明示个人信息处理规则；
2、违规收集个人信息、未逐一列出收集、使用个人信息的目的、方式、范围；
3、超范围收集个人信息；
4、强制、频繁、过度申请、未合理申请使用权限；
5、强制用户使用定向推送功能；
6、账号注销难；
7、未提供投诉渠道、未及时响应用户投诉、未妥善处理用户投诉；
8、App自启动和关联启动等。

从近期通报新增的常见问题类型来看，如下问题类型需要额外关注：

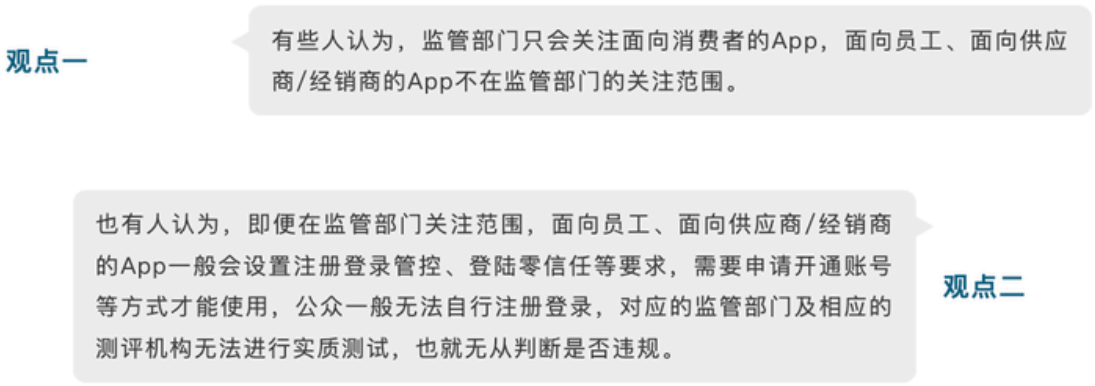
需要额外关注的问题类型
1、未建立已收集个人信息清单；
2、处理敏感个人信息未取得个人的单独同意；
3、个人信息处理者向其他个人信息处理者提供其处理的个人信息的，未向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意；
4、未采取相应的加密、去标识化等安全技术措施；
5、跨境传输未明确安全措施；
6、未成年人身份验证；
7、实际收集个人信息的频率超出相关功能的必要范围。

对于上述问题类型，限于篇幅不再逐一展开，相关要求在问题9的主要依据中基本可以找到答案。下面几个监管新近关注且企业很容易出错的问题需要单独强调一下：

监管新近关注且企业很容易出错的问题
1、微信要求标配的《小程序隐私保护指引》无法完整告知个人信息处理规则，因此，除《小程序隐私保护指引》外，微信小程序应自行制定隐私政策。
2、各业务渠道合并的隐私政策，例如相当一部分企业的网站、手机端App、微信小程序等共用一份隐私政策，应确保合并版本的隐私政策能够完整覆盖各业务渠道处理个人信息的规则，而且对于差异化的内容



十一、问题十一：面向员工使用、面向供应商/经销商使用的App会被通报吗？



事实上，上述两种观点都是错误的，只要能在公开渠道找得到的App都可能被检测到且在违规的情况下会被通报，例如某国资医药企业的1款面向供应商的服务平台、某外资卫浴企业的两款面向经销商的微信小程序被同一批次通报。所以，面向员工使用、面向供应商/经销商使用的App，也一样要开展App合规安排。

十二、写在最后

App合规已然进入深水区，所有的App都可能被检测、因违规被通报、因未如期整改被下架，对外资、国资App来说是这样，其他类型企业的App亦是如此。对于App合规，我们提供如下三点建议供参考：

1.建议企业排查和梳理本企业作为运营者的App的情况，特别是小程序，对于属于或基本属于停用状态、用户数量较少且功能可以整合到其他小程序、手机端App或者其他渠道等情况，建议自行关停、下架相应的小程序等App，确保在架的App均为业务开展所必需。

2.对于拟上架的App，建议上架前除做好安全检测外还需要做好合规评估，确保隐私政策等授权文本、用户交互设计等符合法律规定。

3.对于在架的App，建议采取常态化合规安排，在业务功能变动、监管要求变化等情况下及时更新隐私政策等授权文本，定期通过穿行测试等方式核查App合规情况，并在收到整改要求时严格按照整改要求的时间和内容完成整改。

参考资料：

【1】上海市通信管理局：《上海市通信管理局关于侵害用户权益行为APP的通报（2025年第六批）》

【2】上海市通信管理局：《上海市通信管理局关于侵害用户权益行为APP的通报（2025年第七批）》

【3】中央网信办秘书局：《关于15款App和16款SDK个人信息收集使用问题的通报》

【4】国家网络安全通报中心：《国家计算机病毒应急处理中心检测发现64款违法违规收集使用个人信息的移动应用》

【5】工业和信息化部信息通信管理局：《关于侵害用户权益行为的智能终端通报》

【6】工业和信息化部信息通信管理局：《关于侵害用户权益行为的APP通报（2025年第5批，总第50批）》

【7】上海市通信管理局：《上海市通信管理局关于下架42款侵害用户权益行为应用的通报》

二十二、个人信息保护：北京四中院典型案例确立个保“北京标准”

主笔人



张金栋

北京浩天律师事务所 合伙人
zhangjindong@hylandslaw.com

2025年11月1日，是《个人信息保护法》正式实施四周年，北京四中院作为集中管辖北京互联网法院审理的涉互联网的民商事上诉案件的中级人民法院，发布了个人信息保护典型案例。

北京四中院在新闻通报会中也强调，个人信息权益案件数量逐年递增，说明我国民众对个人信息保护的维权意识越来越强。个保合规，已经不再是简单的政府监管部门和企业的“二人转”，真正的权利人开始觉醒，关注司法实践中具体场景的法律适用，成为了企业个保合规的新课题。

在其典型案例正文中，四中院对于案情介绍、裁判要旨和裁判结果已经有了比较精炼的介绍，本文中不再另行总结归纳，仅对七个典型案例所呈现的特点进行分析，进一步总结个保类案件的裁判倾向，并对企业未来的个保管理提供合规锦囊。



扫码“查看原文”查看北京四中院个人信息保护经典案例

通读以上案例，可以发现以下特点：

一、场景与市场主体典型多样

本次公布的七个典型案例，主要涉及“统一服务平台”处理敏感个人信息、永久封禁账号的用户信息撤回、个人信息查阅复制、人力资源管理中的个人信息的披露与删除、社交媒体“挂人”中的隐私权问题等场景。其涵盖的市场主体包括了统一服务平台、直播平台、短视频平台、网盘、上市公司、咨询公司等多样化的行业企业。

二、原告（自然人）胜诉率较高

七个案例中，原告（自然人）作为个人信息主体，除案例二之外，其中六个案例最终取得了胜诉效果。甚至其中有两个案例（案例四和案例六）为一审原告败诉后二审改判。由此可见，人民法院在司法程序中，对个人信息处理者倾向于给予更加严格的义务。

三、自然人与企业间纠纷为主

七个案例中有六个案例为自然人与企业之间的产生的纠纷，自然人与自然人之间的纠纷仅有一个（案例七），因此此次发布的典型案例的指导意义，更倾向于针对个人信息处理者厘清责任边界。

四、个人利益、企业利益和公共利益的三角博弈

如在案例二中，原告在引起直播内容被封号后，要求通过撤回信息授权的方式解绑个人信息，但法院认为其因为违规被封号的情况下，如果可以任意解绑个人信息，不利于平台维护网络空间的公共秩序，这是个人利益与公共利益的衡量。案例三和案例四都是关于个人信心查阅复制权的案件。案例三中，法院认为查阅复制券的核心在于保障个人对信息的知情与决定权，而非满足统计等任意需求，衍生需求平台无需配合。案例四中，法院认为只要企业客观上具备提供能力，就不得以“技术成本高”“内容繁多”等理由拒绝提供。两个案子从正反两方面展示了个人利益与企业利益

的衡量。

案例五中，上市公司对金额不大的劳动争议案件进行披露并展示了某特定员工的工资信息，法院认为，该信息属于与公共利益无涉的私密领域，公司在无明确义务的情况下公开该信息，超出合理必要的范畴，缺乏合法性、正当性。这是个人隐私权与公共利益的平衡。进一步地，就本次典型案例确立的具体规则而言，我们对相关企业提供如下合规建议：

1、对于“统一服务平台”共享敏感信息的，需要新增“敏感信息跨App使用”二次弹窗，并保留其用户点击同意的相关日志至少三年备查。
2、在用户协议和隐私政策中明确因违规行为被封号后，其个人信息不能解绑和撤回，平台有权保留。
3、在用户协议和隐私政策中用户查询“浏览记录”等非主动提供的个人信息时，须限定用途和信息颗粒度。
4、上市公司履行信息披露义务时，建立个人信息相关内容的专门审核流程，确保信披内容不存在个保合规风险。
5、应在公司员工手册或员工离职时的离职协议中明确，员工在岗期间使用的公司电子设备的个人信息处理方式，在员工离职时，给予合理时间在监督下迁移，或要求员工明示放弃对残留个人信息的权利主张。

二十三、默认勾选：数字消费中消费者权益保护与企业合规路径

主笔人



邢丹丹

科技上市公司 法务
浩天研究院 行业顾问

在数字化时代，网络交易已成为人们日常生活中不可或缺的一部分。从在线购物到各类增值服务的订阅，我们的生活变得更加便捷，但同时也面临着一系列新的法律问题。其中，“默认勾选”这一行为在网络交易中引发了诸多争议，不仅涉及消费者的权益保护，也关系到企业的合规经营。本文将结合实际案例，深入解读相关法律法规，探讨企业应如何应对，进而避免法律风险。

一、 案例引入 ——增值服务中“优惠”套餐默认勾选引发的投诉

每年“618”及“双十一”大促期间，各地工商所接投诉案例中，按照数量多寡进行排序，“默认勾选”造成的消费、充值误导的案件，绝对可以“名列前茅”。经常会有用户对各类虚拟增值服务的购买套餐提出质疑，比如用户本意仅希望购买一年期套餐，但是该套餐下折叠且默认为用户勾选了“第二年仅半价XX元”的优惠选项，用户在不知情的情况下进行了缴费。用户在与商家协商无果的情况下，只能求助于工商，称其认为自身受到了误导消费，要求对消费进行退款，并对商家行为进行查处。

这一案例并非个例，在网络交易中，默认勾选的情况屡见不鲜。从视频平台的自动续费会员，到各类APP在安装时默认勾选同意隐私政策，这些行为看似微不足道，却可能对消费者的权益造成重大影响。那么，这些默认勾选行为在法律上究竟如何界定呢?

二、 相关规范解读

《中华人民共和国电子商务法》第十九条规定：“电子商务经营者搭售商品或者服务，应当以显著方式提请消费者注意，不得将搭售商品或者服务作为默认同意的选项。这一规定明确了，电子商务经营者（即商家）在搭售商品或服务时的义务，必须保障消费者的知情权和自主选择权。在上述案例中，商家将“第二年仅半价XX元”的优惠选项，结合在原本一年期订阅内容中，且使用折叠展示和默认勾选，而未以显著方式提醒消费者，就违反了该条款。

同时，本法第七十七条也明确了相应处罚措施，电子商务经营者违反本法第十八条第一款规定提供搜索结果，或者违反本法第十九条规定搭售商品、服务的，由市场监督管理部门责令限期改正，没收违法所得，可以并处五万元以上二十万元以下的罚款；情节严重的，并处二十万元以上五十万元以下的罚款。这表明，一旦企业违反了关于“显著提醒”的规定，将面临严厉的行政处罚，罚款金额根据情节轻重而定，这对企业的声誉和经济利益都将产生重大影响。

《网络交易监督管理办法》第十七条，“网络交易经营者以直接捆绑或者提供多种可选项方式向消费者搭售商品或者服务的，应当以显著方式提醒消费者注意。提供多种可选项方式的，不得将搭售商品或者服务的任何选项设定为消费者默认同意，不得将消费者以往交易中选择的选项在后续独立交易中设定为消费者默认选择。”
此条款进一步细化了对网络交易经营者搭售行为的规范，不仅禁止将搭售选项设为默认同意，还防止经营者利用消费者的过往选择进行默认设置，全面保护消费者的自主选择权。

同样，本法第四十四条也明确，凡违反本办法第十七条的企业，依照《电子商务法》第七十七条的规定进行处罚，这将《网络交易监督管理办法》与《电子商务法》的处罚条款进行了衔接，统一了对违规行为的惩处，做到“同案同罚”。

2025年6月16日最高人民法院发布的《网络消费民事典型案例》中，其中案例5为《网络服务提供者过度收集消费者个人信息，应承担侵权责任——马某与某公司个人信息保护纠纷案》，具体案情为，某APP存在以下问题：用户在未实际阅读的情况下点击手机屏幕其他位置，该提示内容即消失并自动勾选“已阅读并同意隐私政策”选项，且勾选后

没有撤回同意的途径；若用户点击拒绝，则该APP自动退出，不向用户提供任何服务。

审理法院认为，网络服务提供者应基于个人同意处理个人信息，其预先拟定的有关个人信息收集和使用的协议应使个人充分知情，并自愿、明确作出同意。该APP自动为用户勾选同意隐私政策，未依法保障用户在充分知情的情况下自主作出同意；其在用户拒绝同意隐私政策的情况下直接退出，不提供服务，属于拒绝提供基本服务。最终判决某公司删除其收集的用户手机号等个人信息，向用户赔礼道歉并赔偿其维权合理支出。这一案例为企业敲响了警钟，在涉及用户个人信息收集和使用的协议中，必须确保用户能够充分知情并自主作出同意，否则将承担相应的法律责任。

三、 企业应如何整改与应对

（一）排查现有不合规情况

企业应立即组织技术人员对所有付费购买的SKU做进行全面排查，尤其是优惠购买时的默认勾选选项，这不仅是对法律法规的遵守，也是对消费者权益的尊重，能够有效提升消费者对企业的信任度。

（二）增加用户主动确认环节

在购买前，除了对应服务的相关在线协议，还应增加勾选框，让用户主动点击确认同意，后台还应对此做技术埋点，记录用户操作情况，形成日志并通过隐私政策向用户告知；对于搭售的优惠选线，不进行折叠展示，明确告知用户可“取消”勾选。这样可以确保用户在充分了解服务内容和协议条款的基础上，自主作出选择，避免因信息不对称而产生的纠纷。

（三）提升加强法律风险意识的内部培训

企业应定期组织员工进行法律法规培训，特别是涉及网络交易和消费者权益保护的相关法律。让员工深刻理解“默认勾选”等行为即使为行业惯例，也具有相应的法律风险；以及充分宣贯企业在网络交易中的各项义务，从源头上避免违规违法行为的发生。

（四）建立法律风险预警机制

设立专门的法务团队或聘请法律顾问，对企业的业务流程进行法律风险评估，及时发现潜在的法律问题，并制定相应的应对措施，将法律风险消灭在萌芽状态。

（五）及时响应监管要求

一旦接到监管部门的通知或投诉，企业应积极配合调查，如实提供相关信息，尽可能向监管部门说明“不具有违法故意”。对于监管部门提出的整改要求，要迅速制定整改计划，并严格按照要求执行，确保在规定时间内完成整改。

（六）主动进行自我检查

企业不应仅仅满足于应对投诉和监管，还应主动进行自我检查，定期对业务流程进行合规审查。发现问题及时整改，不断完善企业的合规管理体系，实现可持续发展。

四、 结语

网络交易中的默认勾选问题，不仅关乎消费者的切身利益，也关系到企业的长远发展。通过对相关法律法规的深入解读和实际案例的分析，我们可以看到，法律对消费者的权益保护日益重视，对企业的合规要求也越来越高。企业只有严格遵守法律法规，尊重消费者的知情权和自主选择权，才能在激烈的市场竞争中立于不败之地。

同时，消费者也应增强自我保护意识，学会运用法律武器维护自己的合法权益。在法治的框架下，网络交易市场才能更加健康、有序地发展。

二十四、《国家网络安全事件报告管理办法》核心要点梳理

主笔人



宋海新

北京浩天（上海）律师事务所 合伙人
songhaixin@hylandslaw.com

2025年9月15日，国家互联网信息办公室发布《国家网络安全事件报告管理办法》（以下简称“《办法》”），自2025年11月1日起施行。在2025年国家网络安全宣传周的第一天，监管发文从熟悉的“周五晚发文”成为了“周一见”。作为《网络安全法》第二十五条、《数据安全法》第二十九条、《个人信息保护法》第五十七条等法律法规的配套规定，《办法》包括正文和附件《网络安全事件分级指南》（以下简称“《指南》”），正文共十四条，规定了网络安全事件报告的主体、监管部门、报告程序、报告时间、报告对象、报告内容、报告渠道等内容；附件规定了特别重大网络安全事件、重大网络安全事件、较大网络安全事件和一般网络安全事件的认定标准和分级定量指标。

- 《网络安全法》第二十五条

网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

- 《数据安全法》第二十九条

开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

- 《个人信息保护法》第五十七条

发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项：

① 发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害；
② 个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施；
③ 个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。

《办法》从2023年12月8日《网络安全事件报告管理办法（征求意见稿）》公开征求意见到正式发布，历时近两年。在今年以来多家奢侈品行业和其他行业公司数据泄露引起高度关注的情况下，《办法》的出台恰当其时。

愿你所在企业永远用不上《办法》，但未雨绸缪还是建议你了解一下。

为帮助大家快速、清晰理解《办法》的规定，我们采用了如下问答的形式：

一、什么属于网络安全事件？

《办法》第十二条第一款规定“本办法所指网络安全事件是指由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力等因素，对网络和信息系统或其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。”

相较于《国家网络安全事件应急预案》（中网办发文〔2017〕4号，以下简称“《预案》”）第1.3条对“网络安全事件”的定义，《办法》对“网络安全事件”定义的范围更广，主要体现在安全事件原因方面新增列举了“网络遭受攻击、网络存在漏洞隐患、不可抗力”，在危害对象方面新增列举了“对业务应用造成危害”以及在影响对象方面新增了“对国家、经济造成负面影响”。可以说，如果不幸发生相关安全事件，想要从定义方面主张不是网络安全事件的可能性很小。

二、哪些网络安全事件要报?

Q：所有的网络安全事件都要上报吗?
A；当然不是。

Q：哪些网络安全事件需要上报?
A：较大以上网络安全事件。

Q：什么是较大以上网络安全事件?
A：按照事件影响对象的重要程度、业务损失的严重程度和社会危害的严重程度，网络安全事件可分为特别重大网络安全事件、重大网络安全事件、较大网络安全事件和一般网络安全事件。《指南》中用注的方式明确了“‘以上’均包括本数”，那么，较大以上网络安全事件就包括了特别重大网络安全事件、重大网络安全事件和较大网络安全事件。

网络安全事件的分级厘清了，就可以上表格了：

序号	分级	分级标准	分级定量指标	是否应报
1	特别重大网络安全事件	1.重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。 2.核心数据、重要数据、海量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。 3.其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁，造成特别严重影响的网络安全事件。	1.省级以上党政机关门户网站，中央重点新闻网站因攻击、故障，导致24小时以上不能访问。 2.关键信息基础设施整体中断运行6小时以上或主要功能中断运行24小时以上。 3.影响一个或多个省级行政区50%以上人口，或者1000万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活。 4.核心数据、重要数据泄露或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。 5.泄露1亿人以上公民个人信息。 6.省级以上党政机关门户网站、中央重点新闻网站，超大型网络平台等被攻击篡改，导致违法有害信息特大范围传播，以下情况之一，可认定为“特大范围”：（1）在主页上出现并持续6小时以上，或在其他页面出现并持续24小时以上；（2）通过社交平台转发10万次以上；（3）浏览或点击次数100万以上；（4）省级以上网信部门、公安机关认定为是“特大范围传播”的。 7.造成1亿元以上的直接经济损失。 8.其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁，造成特别严重影响的网络安全事件。	
2	重大网络安全事件	未达到特别重大网络安全事件的如下事件： 1.重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到较大影响。 2.核心数据、重要数据、大量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。 3.其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁，造成严重影响的网络安全事件。	1.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站因攻击、故障，导致6小时以上不能访问。 2.关键信息基础设施整体中断运行1小时以上或主要功能中断运行3小时以上。 3.影响一个或多个地市级行政区50%以上人口，或者100万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等的工作、生活。 4.核心数据、重要数据泄露或被窃取、篡改、伪冒，对国家安全和社会稳定构成严重威胁。 5.泄露1000万人以上公民个人信息。 6.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站，大型以上网络平台等被攻击篡改，导致违法有害信息大范围传播，以下情况之一，可认定为“大范围”：（1）在主页上出现并持续12小时以上；（2）通过社交平台转发1万次以上；（3）浏览或点击次数10万以上；（4）省级以上网信部门、公安机关认定为是“大范围传播”的。 7.造成2000万元以上的直接经济损失。 8.其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁，造成严重影响的网络安全事件。	应该上报，涉及关键信息基础设施的，第一时间上报，最迟不得超过1小时；属于中央和国家机关各部门及其直属单位的，最迟不得超过2小时；其他网络运营者应及时报告，最迟不得超过4小时
3	较大网络安全事件	未达到重大网络安全事件的如下事件： 1.重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。 2.重要数据、较大量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。 3.其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁，造成较严重影响的网络安全事件。	1.地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站因攻击、故障，导致2小时以上不能访问。 2.关键信息基础设施整体中断运行10分钟以上或主要功能中断运行30分钟以上。 3.影响一个或多个地市级行政区30%以上人口，或者10万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活。 4.重要数据泄露或被窃取，对国家安全和社会稳定构成较严重威胁。 5.泄露100万人以上公民个人信息。 6.党政机关、企事业单位门户网站，重点新闻网站，网络平台等被攻击篡改，导致违法有害信息较大范围传播，以下情况之一，可认定为“较大范围”：（1）在主页上出现并持续30分钟以上，或在其他页面出现并持续2小时以上；（2）通过社交平台转发1000次以上；（3）浏览或点击次数1万以上；（4）省级以上网信部门、公安机关认定为是“较大范围传播”的。 7.造成500万元以上的直接经济损失。 8.其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁，造成较严重影响的网络安全事件。	
4	一般网络安全事件	除特别重大网络安全事件、重大网络安全事件和较大网络安全事件外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁，造成一定影响的网络安全事件。		无需上报

相较于《预案》第1.4条对特别重大网络安全事件、重大网络安全事件、较大网络安全事件和一般网络安全事件的认定标准，《办法》的认定标准与其相同之处在于，均从宏观层面将较大以上网络安全事件划分为三类认定标准且第一类、第三类认定标准相同；不同之处主要包括如下两个方面：首先，《办法》在第二类认定标准使用“核心数据、重要数据、个人信息量级”作为核心要素，更好地对《数据安全法》规定的核心数据、重要数据和《个人信息保护法》规定的个人信息进行了衔接；其次，《办法》从不同主体、影响对象、影响时长、数量级、直接经济损失金额等方面以有限枚举的方式给出了网络安全事件的分级定量指标，方便企业更加清晰地对照和适用，很大程度上解决了实践中最棘手的无从判断到底属于哪级网络安全事件从而是否需要上报的问题。

- 《数据安全法》第二十一条

国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。
国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。
关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。
各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

- 《个人信息保护法》第四条第一款

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

《国家网络安全事件报告管理办法》第七条 报告网络安全事件时，应当包括下列内容：……（二）网络安全事件发现或发生的时间、地点、类型、级别……

看到以有限枚举的方式给出了网络安全事件的分级定量指标，可能有同学又要追问三连了：

Q：网络安全事件需要分级，那需要分类吗?
A：需要分类，这是网络安全事件报告的必备内容之一。在快速定位事件原因的基础上进行事件分类，有助于在此基础上采取相应的补救措施、进行事件分级、上报事件类型（如需）和后续事件复盘。

《办法》未对网络安全事件进行分类，可以参考《预案》附件1“网络安全事件分类”和《GB/T 20986-2023 信息安全技术 网络安全事件分类分级指南》（以下简称“国标20986”）第5条“网络安全事件分类”，二者对网络安全事件的分类有所差异。

《预案》将网络安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他网络安全事件等，又可以上表格了：

序号	网络安全事件分类	网络安全事件二级分类/定义
1	有害程序事件	分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件
2	网络攻击事件	分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件
3	信息破坏事件	分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件
4	信息内容安全事件	指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件
5	设备设施故障	分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障
6	灾害性事件	指由自然灾害等其他突发事件导致的网络安全事件
7	其他网络安全事件	指不能归为以上分类的网络安全事件

国标20986综合考虑网络安全事件的起因、威胁、攻击方式、损害后果等因素，将网络安全事件分类为恶意程序事件、网络攻击事件、数据安全事件、信息内容安全事件、设备设施故障事件、违规操作事件、安全隐患事件、异常行为事件、不可抗力事件和其他事件等10类，继续上表格：

序号	一级分类	一级分类定义	二级分类
1	恶意程序事件	指带有恶意意图所编写的一段程序，该程序插入网络损害网络中的数据、应用程序或操作系统，或影响网络的正常运行。恶意程序事件指在网络蓄意制造或传播恶意程序而导致业务损失或造成社会危害的网络安全事件	包括计算机病毒事件、网络蠕虫事件、特洛伊木马事件、僵尸网络事件、恶意代码内嵌网页事件、恶意代码宿主站点事件、勒索软件事件、挖矿病毒事件、混合攻击程序事件和其他恶意程序事件等10个子类
2	网络攻击事件	指通过技术手段对网络实施攻击而导致业务损失或造成社会危害的网络安全事件	包括网络扫描探测事件、网络钓鱼事件、漏洞利用事件、后门利用事件、后门植入事件、凭据攻击事件、信号干扰事件、拒绝服务事件、网页篡改事件、暗链植入事件、域名劫持事件、域名转嫁事件、DNS污染事件、WLAN劫持事件、流量劫持事件、BGP劫持攻击事件、广播欺诈事件、失陷主机事件、供应链攻击事件、APT事件和其他网络攻击事件等21个子类
3	数据安全事件	指通过技术或其他手段对数据实施篡改、假冒、泄露、窃取等导致业务损失或造成社会危害的网络安全事件	包括数据篡改事件、数据假冒事件、数据泄露事件、社会工程事件、数据窃取事件、数据拦截事件、位置检测事件、数据投毒事件、数据滥用事件、隐私侵犯事件、数据损失事件和其他数据安全事件等12个子类

4	信息内容安全事件	指通过网络传播危害国家安全、社会稳定、公共安全和利益的有害信息导致业务损失或造成社会危害的网络安全事件	包括反动宣传事件、暴恐宣扬事件、色情传播事件、虚假信息传播事件、权益侵害事件、信息滥发事件、网络欺诈事件和其他信息内容安全事件等8个子类
5	设备设施故障事件	指由于网络自身出现故障或设备设施受到破坏或干扰而导致业务损失或造成社会危害的网络安全事件	包括技术故障事件、配套设施故障事件、物理损害事件、辐射干扰事件和其他设备设施故障事件等5个子类
6	违规操作事件	指人为故意或意外地损害网络功能而导致业务损失或造成社会危害的网络安全事件	包括权限滥用事件、权限伪造事件、行为抵赖事件、故意违规操作事件、误操作事件、人员可用性破坏事件、资源未授权使用事件、版权违反事件和其他违规操作事件等9个子类
7	安全隐患事件	指网络中出现能被攻击者利用的漏洞或隐患，一旦被利用可能对网络造成破坏，进而导致业务损失或造成社会危害的网络安全事件。提前发现这些漏洞或隐患能防范由此引起的其他网络安全事件	包括网络漏洞事件、网络配置合规缺陷事件、其他安全隐患事件等3个子类
8	异常行为事件	指网络本身稳定性不足或违规访问网络造成访问、流量等异常行为，进而导致业务损失或造成社会危害的网络安全事件	包括访问异常事件、流量异常事件和其他异常行为事件等3个子类
9	不可抗力事件	指因突发事件损害网络的可用性而导致业务损失或造成社会危害的网络安全事件	包括自然灾害事件、事故灾难事件、公共卫生事件、社会安全事件和其他不可抗力事件等5个子类
10	其他事件	指未归为上述分类的网络安全事件	

注：国标20986第5条中对网络安全事件的二级分类也做了定义，篇幅限制，本处不再列举。

此外，《办法》第十二条第三款明确了“本办法所指《网络安全事件分级指南》参照《信息安全技术 网络安全事件分类分级指南》国家标准（GB/T 20986-2023）制定，以有限枚举的方式给出相关事件的分级定量指标”，其他内容还包括国标20986附录A网络安全事件类别和级别的关联关系等，可以为网络安全事件类别对应的事件级别提供有益的参考。

Q：个人信息泄露人数的数量级如何统计？

从通用角度看，仅就个人信息泄露人数的数量级来判断，泄露100万人以上公民个人信息就属于较大以上网络安全事件，需要上报。对于人数的判断，结合个人信息出境、人脸识别备案和个人信息保护负责人的监管规定和监管口径，这里的人数统计需要去重，即按人头统计而非按条数统计，同一自然人的个人信息，无论多少条均按照1个人计算。

Q：对于大多数企业来说，是否只需要考虑门户网站无法访问的时长、门户网站被攻击篡改后违法有害信息传播范围、个人信息泄露人数的数量级、直接经济损失金额是否满足较大以上网络安全事件的判断标准就够了？

诚然，对于大多数企业来说，因主体身份不属于关键信息基础设施运营者、数据类型中不包括核心数据、重要数据，对于网络安全事件，如果主要攻击对象为本企业的门户网站，则重点考虑门户网站无法访问的时长、因被攻击篡改导致违法有害信息传播的范围和直接经济损失金额；如果主要导致数据泄露，则重点考虑个人信息泄露人数的数量级和直接经济损失金额。

但需要提醒的是，别忽视了还需要看一下是否符合本企业的用户分布、行业属性，影响省级/地市级行政区人口的百分比，或者对用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活的影响人数的数量级这一标准，特别是其中的“购物”，典型如电商平台，需要额外关注受影响人数的数量级，在同级别网络安全事件的划分中该数量级均明显小于个人信息泄露人数的数量级。

我们已独家制作了《网络安全事件报告识别表》等表单工具，能够帮助企业未雨绸缪，从而如不幸发生网络安全事件能够第一时间使用这些表单工具快速根据自身主体身份、影响对象、影响时长、人数数量级、直接经济损失金额等准确得出识别结果进行网络安全事件分级，并根据分级结果判断是否需要上报以及何时上报，否则等网络安全事件发生后再行了解如何分级，在如此短的报告时间要求下，很容易措手不及。

三、谁该上报网络安全事件？

《办法》第二条规定了符合上报条件的情况下需要上报网络安全事件的义务主体为“在中华人民共和国境内建设、运营网络或者通过网络提供服务的网络运营者”，《办法》第十二条第二款对“网络运营者”进行了定义，“本办法所指网络运营者是指网络的所有者、管理者和网络服务提供者”。

前述定义沿用了《网络安全法》第七十六条第三项对“网络运营者”的定义，地域限制也沿用了《网络安全法》第二条规定的“在中华人民共和国境内”的限制，也就是限制在中国大陆地区。

与“网络运营者”相关的概念为“网络服务提供者”，其包括网络接入服务提供者(ISP)和网络内容服务提供者(ICP)两类，而《网络安全法》规定的网络除了互联网外，还包括局域网和工业控制系统，它们很多不向社会提供商业或公共服务，但其所有者和控制者也必须承担相应的网络安全义务。因此，《网络安全法》定义的网络安全责任主体即网络运营者是十分宽泛的，包括网络的所有者、管理者和网络服务提供者（详见杨合庆主编：《中华人民共和国网络安全法释义》，中国民主法制出版社2017年版，第153页）。基于此，从实践角度来说，大多数企业都是网络运营者，在发生较大以上网络安全事件时均需按照《办法》的规定进行上报。

四、何时上报网络安全事件？

《办法》第四条规定“网络运营者在发现或获知涉及本单位的网络安全事件时……”应当按照《办法》的规定上报较大以上网络安全事件，表格又来了：

序号	网络运营者的主体类型	上报时间要求
1	关键信息基础设施运营者	发现或获知的第一时间，最迟不得超过1小时
2	中央和国家机关各部门及其直属单位	发现或获知后及时报告，最迟不得超过2小时
3	其他网络运营者	发现或获知后及时报告，最迟不得超过4小时

对于大多数企业来说，需要牢记上表中的第三行列明的网络安全事件上报要求，即“发现或获知后及时报告，最迟不得超过4小时”。此外，有同学应该看出来了，上面的表格中，我们一直在强调“发现或获知网络安全事件”这个重要的时间起点，这里主要是为了让大家与“发生网络安全事件”区分开。“发生网络安全事件”的时间会早于或等于“发现或获知网络安全事件”的时间，例如某法国时尚消费品牌在通知用户发生数据泄露的短信中使用的措施为于XX时间发现了曾发生数据库遭受未经授权的访问。实践中，发现网络安全事件一般为主动发现，主要依靠网络安全监测、自我检查等；获知网络安全事件则一般为被动获知，可能来源于监管部门发现后通知企业、新闻报道发生数据泄露、黑客发来勒索信息等。此外，别忘了，网络安全事件涉嫌违法犯罪的，例如黑客入侵等涉及的非法获取计算机信息系统数据、非法控制计算机信息系统罪以及员工个人信息泄露等可能涉及的侵犯公民个人信息罪等，应当及时向公安机关报案。

- 《刑法》第二百八十五条第二款

非法获取计算机信息系统数据、非法控制计算机信息系统罪】违反国家规定，侵入前款规定以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，或者对该计算机信息系统实施非法控制，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

- 《刑法》第二百五十三条之一

侵犯公民个人信息罪】违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

违反国家有关规定，将在履行职责或者提供服务过程中获得的公民个人信息，出售或者提供给他人的，依照前款的规定从重处罚。

窃取或者以其他方法非法获取公民个人信息的，依照第一款的规定处罚。

单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。

五、向谁上报网络安全事件?

《办法》第四条规定了上报网络安全事件的监管部门，这回我们把Q4中的表格延伸一下（见下页）：

关于行业领域的专门规定，例如《银行保险机构数据安全管理办法》（金规〔2024〕24号）第六十九条规定了银行保险机构在数据安全事件发生后向国家金融监督管理总局或者其派出机构报告的时间、报告形式等要求，《工业和信息化领域数据安全管理办法（试行）》第二十八条第三款对工业和信息化领域数据处理者在数据安全事件发生后需要向本地区行业监管部门报告的安全事件类型和时间等。

序号	网络运营者主体类型	上报时间要求	上报部门一般规定	上报部门行业规定	涉及违法犯罪的特殊规定
1	关键信息基础设施运营者	发现或获知的第一时间，最迟不得超过1小时	保护工作部门、公安机关	本行业领域有专门规定的，网络运营者还应当按照行业主管监管部门要求报告	涉嫌违法犯罪的，网络运营者应当及时向公安机关报案
2	中央和国家机关各部门及其直属单位	发现或获知后及时报告，最迟不得超过2小时	本部门网信工作机构		
3	其他网络运营者	发现或获知后及时报告，最迟不得超过4小时	属地省级网信部门		

- 《银行保险机构数据安全管理办法》第六十九条

数据安全事件发生2小时内，银行保险机构应当向国家金融监督管理总局或者其派出机构报告，并在事件发生后24小时内提交正式书面报告。发生特别重大数据安全事件，银行保险机构应当立即采取处置措施，按照规定及时告知用户并向国家金融监督管理总局或者其派出机构、属地公安机关报告。银行保险机构应当每2小时将处置进展情况上报，直至处置结束。数据安全事件处置结束后，银行保险机构应当在五个工作日内将事件及其处置的评估、总结和改进报告报送国家金融监督管理总局或者其派出机构。其他法律、行政法规对数据安全事件应急处置作出规定的，银行保险机构应当执行。

六、如何上报网络安全事件？

《办法》第九条规定了上报网络安全事件的方式，包括“12387网络安全事件报告热线电话和网站、邮箱、传真等方式”，统一接收网络安全事件报告。《办法》答记者问中对此进行了进一步的说明，上报方式包括如下六类网络安全事件报告渠道：

序号	上报方式	具体操作
1	热线电话	拨打12387网络安全事件报告热线按语音提示进行报告
2	官方网站	访问网络安全事件报告官网12387.cert.org.cn进行报告
3	微信小程序	微信搜索“12387”小程序，进入首页后点击“事件报告”
4	微信公众号	关注“国家互联网应急中心CNCERT”微信公众号，点击“事件报告”
5	电子邮件	发送邮件至邮箱12387@cert.org.cn报告
6	传真	发送传真至010-82992387报告

实践中，此前发生网络安全事件的企业一直面临着联系不上监管部门或者联系上了也未开始受理网络安全事件报告的难题，更重要的是还得担心被认定为未按规定上报网络安全事件。随着《办法》的出台和网络安全事件报告渠道的开通，这一问题迎刃而解。当然，部分企业也该放下侥幸心理了，以前没正式落地，监管部门没有集中开始采取调查、实施处罚等监管动作，网络安全事件上报流程有序运转了，以后未按规定上报网络安全事件就要承担行政处罚等法律责任了。

七、网络安全事件上报什么？

《办法》第七条规定了网络安全事件应上报的内容，我们从报告阶段、是否可以补报的角度做了汇总整理，直接上表格：

序号	报告内容	是否可以补报
第一阶段、发现或获知涉及本单位的网络安全事件后		
1	涉事单位名称及涉事系统或设施基本情况	不可以补报，必须在规定时间内上报
2	网络安全事件发现或发生的时间、地点、类型、级别，以及已造成的影响和危害，已采取的措施及效果；对勒索软件攻击事件，还应当包括要求支付赎金的金额、方式、日期等	
3	事态发展趋势及可能造成的进一步影响和危害	规定时间内不能判定事发原因、影响或发展趋势等网络安全事件情况的，后续及时补报
4	网络安全事件原因初步分析意见	
5	溯源调查工作线索，包括但不限于可能的攻击者信息、攻击路径、存在的漏洞等	
6	拟进一步采取的应对措施以及请求支援事项	
7	网络安全事件现场保护情况	
8	其他应当报告的情况	
第二阶段、上报后出现新的重要情况或调查工作取得阶段性进展		
1	新的重要情况或调查工作取得的阶段性进展	及时报告
第三阶段、网络安全事件处置工作结束后30日内		
1	相关事件发生原因	网络安全事件处置工作结束后30日内进行全面分析总结，形成事件处置总结报告按照原渠道上报
2	应急处置措施	
3	造成的危害	
4	责任追究	
5	完善整改情况	
6	教训	

可以看出，上报网络安全事件需要报告的要素很多，而要在极短的时间内完成事件分析上报，需要依靠预先制定《网络安全事件、数据安全事件、个人信息安全事件应急预案》、定期实施演练并根据演练情况对应急预案不断完善，方能在应急处置时有条不紊。当然，如果有聘请外部网络安全相关服务机构，其可以也应当从专业的角度进行

协助，相信专业的力量，Q8问答中我们会讨论相关问题。

八、网络安全事件监测协报？

实践中，除自身信息技术部门进行网络安全管理、日常运维等，有预算的企业一般还会聘请外部网络安全相关服务机构为其提供网络安全、系统运维等服务，例如近期多家奢侈品行业数据泄露的通知文案中均提及正在与网络安全专家合作开展事件调查和应对。

对此，《办法》第五条规定了“网络运营者应当以合同等形式要求为其提供网络安全、系统运维等服务的组织或个人，及时向其报告监测发现的网络安全事件，并协助其按照本办法规定报告网络安全事件”。

对于已经与网络安全服务商签署服务协议且未约定前述规定内容的企业，需要通过签署补充协议、服务商出具承诺函、服务商向本企业指定联系人发送邮件等方式补充约定服务商应及时向本企业报告监测发现的网络安全事件，并协助本企业按照《办法》规定报告网络安全事件；对于新聘用网络安全服务商的企业，需要在合作协议中增加或者其他方式约定服务商应及时向本企业报告监测发现的网络安全事件，并协助本企业按照《办法》规定报告网络安全事件。

九、网络安全事件报与不报？

《办法》第十条规定了网络安全事件报告的法律责任以及迟报、漏报、谎报或者瞒报网络安全事件在造成重大危害后果情况的从重处罚要求，《办法》第十一条规定了特定情形下按照《办法》规定及时报告网络安全事件的从轻或者不予追究相关单位和人员责任的要求。

总结来说，如下四句话：

网络安全事件须知应报尽报，
网络安全事件牢记不报要罚。
迟报漏报谎报瞒报可能从重，
及时报告可能从轻甚至不罚。

十、网络安全事件溯及既往？

溯及力是每一部法律法规大家都会关心的问题。从基本法理的角度来说，法不溯及既往。具体到《规定》，规定未提及效力溯及既往。因此，我们认为，适用《规定》追究《规定》生效前发生的网络安全事件报告情况的可能性较小。

十一、写在最后

《办法》的出台和后续实施，宣告网络安全事件报告机制的正式落地。在近期某法国时尚消费品牌公司因数据泄露被监管调查并被属地公安机关因违规出境个人信息、未采取个人信息安全技术措施处以行政处罚后，我们正在撰写本文的期间，某人工智能公司又因“在处理人脸等生物识别类敏感个人信息前，未按《个人信息保护法》有关规定进行个人信息保护影响评估”，被“属地公安机关依据《个人信息保护法》规定，对该公司依法予以行政处罚，并责令整改”。

个人信息保护多个分类型的第一案相继落地，可以预见的是，这些处罚只是开始，后续还会有包括未按规定报告网络安全事件等其他类型的第一案以及第N案相继落地。个人信息保护正式进入违规处罚高发期，唯有合规，方能更好前行。

二十五、《互联网法院管辖规定》修订要点解读

主笔人



何为

北京浩天律师事务所 合伙人
hewei2@hylandslaw.com



袁少鸿

北京浩天律师事务所 律师
yuanshaohong@hylandslaw.com



谭知雨

北京浩天律师事务所 律师助理
tanzhiyu@hylandslaw.com

2018年9月6日，最高人民法院印发《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，以下简称“《2018年规定》”），明确互联网法院集中管辖11类案件。

随着数字经济发展与网络空间治理深化，最高人民法院在系统总结多年审判实践经验基础上，于2025年10月11日印发《最高人民法院关于互联网法院案件管辖的规定》（法释〔2025〕14号，以下简称“《规定》”），对互联网法院案件管辖范围予以系统性调整与优化，该规定自2025年11月1日起正式施行。

《规定》的出台将对互联网法院及其他法院的涉互联网案件受理范围产生重大影响，本文将以“十问十答”形式，梳理其修法背景与修订要点。

一、互联网法院的设立和分布情况?

2017年，中国电子商务交易总额突破31万亿元，网络借贷、网络众筹、互联网支付交易总额超过70万亿元（详见中华人民共和国最高人民法院:《中国互联网法院的创新意义和实践特色》），成为经济发展新引擎。互联网的广泛应用，改变了传统法律关系的结构、要素和表现形式，催生出专属于互联网领域的全新社会关系和纠纷形态。

为进一步维护网络安全、化解涉网纠纷、促进互联网和经济社会深度融合，推动司法体系主动适配互联网发展趋势，2017年6月26日，中央全面深化改革领导小组第三十六次会议审议通过《关于设立杭州互联网法院的方案》，决定设立杭州互联网法院。2017年8月18日，全国首家互联网法院——杭州互联网法院正式成立，标志着我国互联网司法专门化建设正式启动。

之后，2018年9月，为扩大互联网司法覆盖范围、适配不同区域数字经济发展需求，我国又先后增设北京、广州互联网法院。

截至目前，全国范围内互联网法院数量仍保持为三家。在级别上，互联网法院属于基层法院，与区县一级人民法院平级。

二、互联网法院与传统法院审理案件程序方面有哪些特点?

相较于传统法院，互联网法院以在线审理为核心模式，案件的受理、送达、调解、证据交换、庭前准备、庭审、宣判等诉讼环节均通过线上平台完成。以北京互联网法院为例，该院未设置线下立案窗口，即便前往法院现场，法院立案庭工作人员也会引导使用法院提供的电脑进行网上立案。

在其他环节，互联网法院也发挥着其独特的优势，例如在证据审查环节，互联网法院依托自身技术优势，采用区块链验证等技术手段，重点解决电子数据“易篡改、难认证”的痛点，大幅度简化对电子数据证据的繁琐验证流程，有效提高审判效率。

截至《规定》发布前，三家互联网法院均有各自独立的审判系统，但自2025年10月起，在最高人民法院的统筹下，全国各地的各类法院网络系统陆续启动一体化整合，截至本文发布时，北京互联网法院已经接入统一的“人民法院在线服务网”，但杭州互联网法院和广州互联网法院依然使用各自独立的电子诉讼平台，后续是否会接入“人民法院在线服务网”有待观察。

三、《规定》对互联网法院的案件管辖范围作出了哪些调整?

《2018年规定》第二条明确，互联网法院集中管辖所在市的辖区内应当由基层人民法院受理的网络购物、网络服务、

网络金融借款、网络小额借款、网络著作权、网络域名、网络侵权、网购产品责任、网络公益诉讼等十一类纠纷。《规定》在此基础上作出系统性调整，包括：

（一）新增四类网络纠纷纳入互联网法院集中管辖

包括“网络数据权属、侵权、合同纠纷”“网络个人信息保护、隐私权纠纷”“网络虚拟财产权属、侵权、合同纠纷”“网络不正当竞争纠纷”。

（二）将部分案件调整出互联网法院管辖范围

包括“签订、履行行为均在互联网上完成的金融借款合同纠纷、小额借款合同纠纷”“在互联网上首次发表作品的著作权或者邻接权权属纠纷”“在互联网上侵害在线发表或者传播作品的著作权或者邻接权而产生的纠纷”“通过电子商务平台购买的产品，因存在产品缺陷，侵害他人人身、财产权益而产生的产品责任纠纷”，以及网络侵害名誉权、一般人格权、财产权等传统网络侵权纠纷。

经调整后，互联网法院集中管辖案由整合为9类：



四、涉外或涉港、澳、台的网络纠纷相关案件如何管辖？

涉外和涉港、澳、台的民事案件，属于互联网法院管辖范围的，由互联网法院集中管辖。

五、《反不正当竞争法》修订后，“网络不正当竞争纠纷”包含哪些类型？

根据2025年6月27日修订的《中华人民共和国反不正当竞争法》（主席令第五十号，以下简称“2025年《反不正当竞争法》”）第十三条规定：网络不正当竞争纠纷对应行为类型包括：（1）强制跳链；（2）诱导卸载；（3）恶意不兼容；（4）互联网专条兜底条款；（5）非法数据获取；（6）恶意交易/反向刷单。

相较于2019年4月23日施行的《中华人民共和国反不正当竞争法》，网络不正当竞争纠纷行为新增了前述第（5）项、第（6）项内容。《规定》明确将网络不正当竞争纠纷纳入互联网法院集中管辖的范围，在司法层面与2025年《反不

正当竞争法》衔接适配。

六、《规定》何时生效?

《规定》第四条明确，本规定自2025年11月1日起施行，《规定》施行前已经受理的案件由原受理人民法院继续审理。因此，2025年11月1日之前尚未通过任何方式提交立案的案件，按照修改后的管辖范围执行。

需注意的是，《规定》未对系以法院接收立案材料还是以法院出具受理通知或出具案号视为“受理”予以明确界定。具体到实际场景中，针对在2025年11月1日之前已提交立案材料未在线上审核通过的，或者在线下接收材料未出具案号或邮寄立案尚未收到法院答复的案件，可能存在争议。

七、此次案件管辖范围调整对互联网法院的审判工作有何影响?

北京互联网法院2024年8月26日发布的《北京互联网法院服务保障新质生产力加快发展白皮书》显示，近年来，随着数据、网络、人工智能等的发展，互联网法院受理案件呈现权利客体快速出新、新兴产业领域矛盾纠纷呈上升趋势、新型商业模式引发的诉讼纠纷日渐涌现、技术应用迭代升级导致案件审理中事实查明难度加大等特点。



（北京互联网法院建院以来受理各类案件情况 数据来源：《服务保障新质生产力加快发展白皮书》）

经过此次调整，互联网法院管辖范围实现精准优化，大量的网络侵权、小额借贷等案件通过制度分流交由其他基层法院受理，有效缓解了互联网法院的办案压力，为互联网法院探索新型、前沿、重点网络领域裁判规则，发挥规范引领、促进保障作用，及时回应网络空间治理新要求，护航数字经济健康发展创造了空间。

八、传统网络侵权纠纷调整由其他基层法院管辖对当事人推进此类案件的影响是什么?

第一，互联网法院以线上立案为唯一模式，审核期限为7日。而其他基层法院普遍采用“线上+线下”双轨立案模式，若当事人选择现场立案，通常可当天获知立案结果；若采取线上立案，则审核期限一般为3个工作日，当事人可根据自身需求选择立案方式，灵活度更高。

第二，北京、杭州、广州三地作为互联网法院所在地，经济发展水平与区域内法院审判水平较高，将原由互联网法院受理的部分案件分流至其他基层法院审理，一般不会对最终的审判结果产生实质影响。但仍需注意的是，案件最终由哪个法院受理，可能会受到该法院本身审判特点的影响。例如，若某法院案件量长期饱和，存在立案难度大、

审限长、案件推进缓慢等情况，则由该法院受理的分流案件也可能面临同样的问题。

尤其值得关注的是，网络侵害名誉权、肖像权、姓名权、著作权等纠纷由其他法院分散受理后，若受理法院存在案件量大、审限长的情况，被侵权人或其他权利人获取生效裁判结果的时间成本可能相应增加。

第三，在电子数据真实性审核方面，互联网法院具备显著的技术优势，当事人可以选择采取区块链取证软件进行取证，庭审时各方较少纠结证据的真实性，审核效率大幅提升。相较之下，其他基层法院缺乏专门的电子数据审核技术，对电子数据真实性的审核主要依赖法官通过传统审查方式核验，基于此，当事人在向其他基层法院提交电子数据证据时，需要特别留意保存电子数据原件，为法院后续核实电子数据真实性提供有效依据。

第四，互联网法院和其他基层法院之间审判习惯的差异也可能对案件的审理产生影响：
在证据出示环节，互联网法院通过电脑查看文件、图片等证据具有显著便利性，而其他基层法院在庭审中对证据的审查仍以纸质证据为主要载体，因此当事人在开庭前需准备完整的纸质证据材料，便于法官当场查阅证据内容。
在庭审模式方面，互联网法院以线上开庭方式为主，当事人可远程参与庭审，而其他基层法院适用线上开庭的案件相对较少，这一差异会对异地当事人参与诉讼的便利性产生直接影响。
在材料接收与文书送达环节，互联网法院依托在线诉讼系统完成全流程操作，全程留痕，而其他基层法院主要通过EMS邮寄方式进行，为防范后续因文件送达问题产生的争议，当事人需要保留好邮寄或签收凭证，等等。

九、互联网法院能否适用协议管辖？

《规定》中明确，就合同及其他财产权益民事纠纷，允许当事人通过协议约定由与争议有实际联系地点的互联网法院管辖，但若管辖条款属于格式条款，提供格式条款的一方没有依法履行提示与说明义务，则该条款可能被认定为无效或不成为合同内容。值得注意的是，在实践中，互联网平台的相关协议中的管辖条款大多采用格式条款，被告可能对此提出管辖异议，法院也可能依职权对管辖进行审查，一旦管辖条款被认定为无效，法院可能将案件移送至其他有管辖权的法院管辖。

十、对互联网法院裁判提起上诉的管辖法院是什么？

当事人对互联网法院作出的判决、裁定提起上诉的案件，由互联网法院所在地的中级人民法院审理。从当前司法实践来看，根据案件是否存在涉外、涉知识产权等因素，对于北京、杭州、广州互联网法院作出的裁判，应当分别向北京市第四中级人民法院、北京知识产权法院、杭州市中级人民法院、广州市中级人民法院、广州知识产权法院提起上诉。

二十六、新《网络安全法》修订背景、重点、亮点解析

主笔人



翁哲卉

北京浩天（南宁）律师事务所 高级合伙人
浩天南宁特殊资产处置事务部 负责人
wengzhehui@hylandslaw.com

2025年10月28日，《中华人民共和国网络安全法》（以下简称“新《网安法》”）经十四届全国人大常委会第十八次会议修订通过，将于2026年1月1日起施行。

本文结合修订重点、亮点，以“十问十答”形式解读其核心变化。

一、新《网安法》的修订背景？

自2017年《网络安全法》实施以来，国内外网络安全形势发生深刻变化。此次修订正是为应对网络安全形势的深刻变化：一方面，人工智能、大数据等新技术快速发展，网络攻击、数据泄露等风险加剧；另一方面，关键信息基础设施的安全保护需求迫切，境外网络安全威胁范围扩大。

二、新法修订的重点内容有哪些？

修订重点体现在五个方面，具体如下：

修订重点	新法条款	意义
强化政治引领	第三条	明确坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全
回应技术创新	第二十条	支持人工智能基础研究与应用，规范其安全监管，新增运用人工智能等新技术创新网络安全管理方式
压实主体责任	第六十一至七十条	细化网络运营者的安全保护义务，提升违法成本
衔接配套立法	第四十二条 第六十三条 第七十一条 第七十三条	与《民法典》《数据安全法》《个人信息保护法》《行政处罚法》协同
扩展境外责任	第七十七条	填补了非关键信息基础设施领域境外攻击的法律空白，保护国家网络安全

三、新增纲领性条款有何重要意义？

新《网安法》第三条新增：“网络安全工作坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，推进网络强国建设。” 这一条款是本次修订的“灵魂”，意义体现在三方面：

- 政治统领：将网络安全纳入国家安全战略核心框架，明确党的领导地位；
- 政策衔接：与《数据安全法》《国家安全法》形成“三位一体”协同治理模式，避免“多头管理、权责不清”；
- 责任导向：要求政府、企业、公众在党的领导下共担网络安全责任，推动“全民共治”。

四、针对人工智能领域有哪些新规定？

新《网安法》第二十条新增“国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。”“国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。”

首次以法律形式确立人工智能安全与发展的框架性要求，明确国家在技术研发、基础设施、伦理规范、风险监测、安全监管五方面的责任，为AI健康发展提供法治保障。

五、处罚力度有何变化?

为解决旧法处罚力度不足、责任不明确等问题，新《网安法》从“优化处罚梯度、明确责任范围”角度进行完善。具体对比如下：

分类	主体	行为/违法情形	2017年条款及处罚	2025修正条款及处罚
未履行网络安全保护义务	网络运营者/关键信息基础设施的运营者	网络运营者未履行第二十三条、第二十七条规定的网络安全保护义务（如未制定安全制度、未采取技术措施）；关键信息基础设施的运营者不履行本法第三十五条、第三十六条、第三十八条、第四十条规定的网络安全保护义务	原第59条：责令改正、警告；拒不改正或导致危害网络安全等后果的，单位处1万-10万元罚款，直接责任人员处5千元-5万元罚款；关键信息基础设施运营者同类行为，单位处10万-100万元罚款，直接责任人员处1万-10万元罚款	新第61条：责令改正、警告，可以处1-5万元罚款； 拒不改正或导致后果的，单位处5万-50万元罚款（直接责任人1万-10万元）； 严重后果（如大量数据泄露、CIIO局部功能丧失），单位处50万-200万元罚款（直接责任人5万-20万元）； 特别严重后果（如CIIO丧失主要功能），单位处200万-1000万元罚款（直接责任人20万-100万元）
不履行安全管理义务	网络运营者/关键信息基础设施的运营者	违反第二十四条第一款、第二款和第五十条第一款规定的（如设置恶意程序、未采取补救措施或告知用户并报告主管部门、擅自终止安全维护服务）	原第47条+第68条：责令改正、警告、没收违法所得； 拒不改正或情节严重的，单位处10万-50万元罚款（直接责任人员1万-10万元），并可责令暂停业务、关闭网站等	新第62条：责令改正、警告； 拒不改正或导致后果的，单位处5万-50万元罚款（直接责任人1万-10万元）； 严重后果（如大量数据泄露、CIIO局部功能丧失），单位处50万-200万元罚款（直接责任人5万-20万元）； 特别严重后果（如CIIO丧失主要功能），单位处200万-1000万元罚款（直接责任人20万-100万元）
提供未通过安全审查的产品	网络产品/服务提供者	违反第二十五条规定，提供未通过安全审查的产品	-	新第63条：责令停止、警告、没收违法所得； 无违法所得或违法所得<10万元，并处2-10万元罚款； 违法所得>10万元，并处违法所得1-5倍罚款； 情节严重的，并责令停业整顿、吊销证照另有规定，依照规定
违规开展认证/检测活动或发布漏洞信息	网络安全服务机构	违反本法第二十八条规定，未遵守国家规定开展网络认证等活动、发布系统漏洞等网络安全信息	原第62条：责令改正、警告；拒不改正或情节严重的，单位处1万-10万元罚款（直接责任人员5千元-5万元），并可责令暂停业务、关闭网站等	新第65条：责令改正、警告，可以1-10万元罚款； 拒不改正或情节严重，单位处10万-100万元罚款（直接责任人1万-10万元），并可责令关停网站或APP、吊销执照； 其他严重后果（如大量数据泄露、CIIO局部功能丧失），单位处50万-200万元罚款（直接责任人5万-20万元）； 特别严重后果（如CIIO丧失主要功能），单位处200万-1000万元罚款（直接责任人20万-100万元）
未及时处置用户发布的违法信息	网络运营者	违反第四十九条规定，未及时处置用户发布的违法信息	原第68条：责令改正、警告、没收违法所得； 拒不改正或情节严重的，单位处10万-50万元罚款（直接责任人员1万-10万元），并可责令暂停业务等	新第69条：一般未处置（如未停止传输），责令改正、警告、通报，单位可处5万-50万元罚款； 拒不改正或情节严重，处50万-200万元罚款，可关停网站/APP、吊销执照（直接责任人5万-20万元）； 特别严重影响，处200万-1000万元罚款，直接关停APP并吊销执照（直接责任人20万-100万元）
不履行安全管理义务	电子信息发送服务提供者、应用软件下载服务提供者	不履行本法第五十条第二款规定的安全管理义务的	原第68条：责令改正、警告、没收违法所得； 拒不改正或情节严重的，单位处10万-50万元罚款（直接责任人员1万-10万元），并可责令暂停业务等	新第69条：一般未处置（如未停止传输），责令改正、警告、通报，单位可处5万-50万元罚款； 拒不改正或情节严重，处50万-200万元罚款，可关停网站/APP、吊销执照（直接责任人5万-20万元）； 特别严重影响，处200万-1000万元罚款，直接关停APP并吊销执照（直接责任人20万-100万元）

六、未履行实名制义务将面临什么后果?

新《网安法》第六十四条规定：“网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。”随着移动互联网普及，APP已成为主要服务载体，新增“关闭应用程序”处罚更贴合实践。

三、新增纲领性条款有何重要意义?

新《网安法》第六十四条规定：“网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。”随着移动互联网普及，APP已成为主要服务载体，新增“关闭应用程序”处罚更贴合实践。

七、对关键信息基础设施运营者的责任要求有哪些变化?

金融、能源、交通等领域的关键信息基础设施是“国计民生的神经中枢”，新法进一步压实关键信息基础设施运营者（简称“CIIO”）责任：

义务类型	具体要求	违规后果
采购/使用义务	采购网络产品/服务需通过安全审查（第六十七条）	新法第六十七条：责令限期改正、停止使用、消除对国家安全的影响，单位处采购金额1-10倍罚款（直接责任人1-10万元）
数据存储义务	境内收集的个人信息和重要数据应境内存储；确需向境外提供的，需经安全评估（第三十九条）	按新法第七十一条的规定，违规境外存储/提供的，按《数据安全法》处理（可处100万-500万元罚款）
安全检测义务	每年至少一次安全检测评估并报送主管部门（第四十条）	新法第六十一条，未检测或未报送的，可处10万-100万元罚款（直接责任人1万-10万元）

浩天研究院出品

八、新法如何与其他法律法规衔接?

新《网安法》第七十一条，对特定行为依照有关法律、行政法规的规定处理、处罚，做出了协同体系。 具体衔接如下：

行为列举	可能适用的其他法律	可能法律后果
传播虚假信息、色情暴力内容	《刑法》 《治安管理处罚法》	刑事责任：可能触犯《刑法》侮辱诽谤罪、编造传播虚假信息罪； 行政责任：涉及治安管理的适用《治安管理处罚法》拘留、依据《网络安全法》可处警告、罚款、暂停业务等行政处罚
泄漏个人信息、非法收集使用个人信息	《刑法》 《民法典》 《个人信息保护法》	刑事责任：符合数量或情节标准时，适用侵犯公民个人信息罪； 民事责任：依《民法典》《个人信息保护法》承担赔偿责任 行政责任：适用《网络安全法》进行处理
违反境外存储或提供个人信息、重要数据规定	《刑法》 《数据安全法》	《刑法》：非法获取计算机信息系统数据罪 《数据安全法》：对未经批准的数据出境行为进行罚款；
非法获取/提供个人信息行为，尚不构成犯罪的违法行为	《治安管理处罚法》	非法侵入计算机系统等行为可处15日以下拘留

浩天研究院出品

九、哪些情形可从轻或减轻处罚？

新《网安法》第七十三条明确：“违反本法规定，但具有《中华人民共和国行政处罚法》规定的从轻、减轻或者不予处罚情形的，依照其规定从轻、减轻或者不予处罚。”

第七十三条作为指引性条款，需结合《行政处罚法》关于从轻、减轻或不予处罚的具体情形处理，如主动消除危害后果、初次违法且后果轻微并及时改正、无主观过错等。

主动补救、及时改正：自查或被调查后立即纠正，及时整改并向主管部门说明情况，不可仅口头承诺未实际整改，尽量实际降低危害；

初次违法、危害后果轻微：无同类违法行为历史记录，无实质性损害（如少量个人信息泄露但未扩散）；

无主观过错：因第三方攻击导致数据泄露（已安装防火墙、定期检测），可提供技术证据（如攻击日志、检测报告）争取不予处罚。

十、对境外实体的制裁范围有何变化？

新《网安法》第七十七条将境外主体的责任范围从“危害关键信息基础设施”扩展至“危害我国网络安全”，即无论攻击对象是否为关键信息基础设施，只要危害我国网络安全，即可追责。

具体规则如下：境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的，依法追究法律责任；造成严重后果的，国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

上述规则填补了非危害关键信息基础设施领域境外攻击的法律空白，强化国家网络主权保护。

十一、结语

新《网安法》的施行标志着我国网络安全治理进入“强责任、细监管、重预防”的新阶段。

企业需从制度建设（制定安全制度、明确负责人）、技术投入（数据加密、定期检测）、风险监测（内容审核、用户实名）等方面强化合规，公众也需提高网络安全意识，共同维护网络空间安全与发展利益。

二十七、十问十答：港股IPO数据合规核心必知解读

主笔人



宋海新

北京浩天（上海）律师事务所 合伙人
songhaixin@hylandslaw.com

近两年，港股市场异常火爆。港交所网站显示，仅9月29日及30日两天，就有长春高新、贝达药业、百利天恒、晶合集成、极米科技、聚芯微电子等29家公司递表港交所。同时，今年前三个季度，港交所受理的新申请已高达286家，是去年的两倍有余。我们甚至在微信朋友圈同一天就看到不同的微信好友参与的几个港股上市项目现场敲钟的画面。相应的，港股IPO数据合规的需求也在暴增。

对于港股IPO的中介机构而言，港股IPO数据合规已然非常熟悉，多数项目中都会用到。但相当一部分首次赴港上市的企业对于港股IPO合规的相关情况，还不甚了解。为帮助企业更好地了解港股IPO数据合规，提前做好项目规划，成功登陆港股，我们整理了港股IPO数据合规常见的十个问题，供企业参考。

一、港股IPO数据合规是什么?

港股IPO数据合规，简而言之，就是在企业赴港上市阶段，协助企业在短时间内快速开展数据合规工作，从而助力企业在重大方面符合中国境内现行有效的数据合规法律规定，为港股IPO扫除数据合规方面的障碍。

二、港股IPO数据合规与一般意义上的数据合规的差别是什么?

做到一百分的合规很难，数据合规自然也是如此。一般意义上的数据合规会根据相关法律规定、监管要求、企业的预算等因素来决定做部分还是全部的数据合规、满足基本合规要求后续再分阶段完善还是以高标准深入落地数据合规等。港股IPO数据合规，要求的是“短平快”，也就是以赴港上市这一“应试”为目的，在较短的时间内“抓大放小”快速协助企业完成数据合规重大方面的合规落地。此外，需协助企业应对香港联交所、香港证监会、中国证监会等交易所和监管部门的相关问询（如有），而一般意义上的数据合规不会涉及这类需求。

三、哪些类型的企业需要做港股IPO数据合规?

所有赴港上市的企业至少都会涉及处理员工的个人信息以及供应商、合作方等B端联系人的个人信息，因此，严格来说，所有企业都需要做港股IPO数据合规。相对而言，医药、医疗器械、汽车、互联网、科技、消费、零售、金融、食品饮料等行业的企业，港股IPO数据合规的需求会更多。

看到这，有的人想问，我们企业既往已经做了很多数据合规的安排，是不是可以不用做港股IPO数据合规？答案基本是否定的，很难有企业真的能够基本满足“在重大方面符合中国境内现行有效的数据合规法律规定”这一可以出具清洁意见的标准，有一定的数据合规基础的话一般只会减少一些工作量以及相应地缩短一些项目周期。

四、港股IPO数据合规是怎么成为刚需的?

除了履行数据合规这一法定义务外，推动港股IPO数据合规成为刚需的主要因素包括：
1.香港联交所、香港证监会、中国证监会等交易所和监管部门对赴港上市企业数据合规问题的关注日益加强，多数企业都会收到数据合规的相关问询；
2.受1的因素影响，保荐人在多数项目里会要求企业单独开展IPO数据合规，保荐人的内核一般也会重点核查企业数据合规的相关情况
3.受1的因素影响，企业（发行人）境内律师一般也会要求企业单独开展IPO数据合规，作为其专项法律意见书等上市材料的重要援引材料之一。

五、什么时候需要开展港股IPO数据合规?

这个问题是港股IPO数据合规的核心问题之一，因为要和时间赛跑。对于多数赴港上市企业，其项目周期都相对较短，一般只有几个月的准备时间。而对于港股IPO数据合规，其准备时间一般不会等于只会小于IPO的整体准备时间。

结合我们的实务经验，建议在港股项目启动会前后就尽快启动港股IPO数据合规工作，越早越好，一般建议预留3个月以上的时间，从而为企业自身争取更多的数据合规问题整改时间。

最短需要多少时间?

只能说，我们做过的诸多项目里，从签署法律服务合同到企业赴港上市交表前出具清洁版的港股IPO数据合规法律意见书，最短的时间周期是1个月多一点点。其中，企业以及各方中介机构的高度配合，特别是企业的问题整改落地速度，是我们能够在如此短的时间周期内顺利完成项目的不可或缺的重要因素。

六、哪些情形会显著影响港股IPO数据合规的工作量?

港股IPO数据合规的工作量对于企业预估工作进度、准备项目预算等都具有重要意义。数据合规内部管理制度、组织架构、个人信息主体权利响应、技术保护措施等IPO数据合规的通用内容一般不会对工作量造成显著的影响，显著影响港股IPO数据合规工作量的情形主要包括：

1.线上业务载体的数量，包括手机端App、小程序、PC端、Web端、H5页面等。这些业务载体非常容易出现诸多的数据合规问题，包括隐私政策等个人信息处理规则文本不完善、单独同意未落实、用户交互设计不到位等。在既往的项目中，我们在一个项目中最多核查过100多个线上业务载体，核查和整改的工作量都极其庞大。
2.纳入上市范围的境内下属公司的数量、重要子公司的数量特别是主要进行数据处理活动的子公司的数量。涉诉、涉行政处罚、涉监管通报、涉监管立案调查、涉刑事犯罪的核查范围一般为上市主体和纳入上市范围的境内下属公司，数据合规情况的重点核查范围一般是上市主体和重要子公司特别是主要进行数据处理活动的子公司。所以，这些子公司的数量会显著影响工作量。在既往的项目中，我们在一个项目中最多核查过上市主体及其110家境内下属公司和其17家重要子公司的数据合规情况，工作量同样非常庞大。

七、哪些情形可能明显影响港股IPO的时间表?

看到这个问题，有人会想问，问题6刚刚讨论过显著影响工作量的情形，为什么还需要知道明显影响港股IPO的时间表的情形？工作量不就会显著影响时间表吗？答案基本也是否定的。

按照港股IPO的时间表完成各项工作是港股IPO项目的重中之重，一般不会轻易调整时间表。工作量大不会必然影响港股IPO的时间表，只要各方高度配合、全力推进，一般不会有问题。那么对于IPO数据合规而言，哪些情形真的可能会明显影响港股IPO的时间表?

我们的答案是，如果企业需要开展数据出境安全评估、个人信息出境标准合同备案、人脸识别信息备案、个人信息保

护负责人备案、网络安全审查等政府前置数据合规程序而尚未开展或尚未完成政府前置数据合规程序，则可能会明显影响港股IPO的时间表。因为，这些程序的完成时间不可控甚至于是否能够完成/通过相应程序也不可控，原因大家都懂，不是企业和中介机构能决定的，无需多言。在应完成而未完成政府前置数据合规程序的情况下，出具清洁版的港股IPO数据合规法律意见书基本不太可能，否则会面临相当高的职业风险。

八、港股IPO数据合规一般需要根据哪些法律规定做哪些工作?

关于港股IPO数据合规需要适用的法律规定，主要包括：

序号	法律规定类型	法律规定名称
1	通用法律规定	《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》（国务院令第745号）、《网络数据安全管理条例》（国务院令第790号）、《网络安全审查办法》（国家互联网信息办公室、中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局令第8号）、《个人信息保护合规审计管理办法》（国家互联网信息办公室令第18号）等
2	触发适用的法律规定	《儿童个人信息网络保护规定》（国家互联网信息办公室令第4号）、《未成年人网络保护条例》（国务院令第七百六十六号）、《数据出境安全评估办法》（国家互联网信息办公室令第11号）、《个人信息出境标准合同办法》（国家互联网信息办公室令第13号）、《促进和规范数据跨境流动规定》（国家互联网信息办公室令第16号）、《App违法违规收集使用个人信息行为认定方法》（国信办秘字〔2019〕191号）、《常见类型移动互联网应用程序必要个人信息范围规定》（国信办秘字〔2021〕14号）、《人脸识别技术应用安全管理办法》（国家互联网信息办公室 公安部令第19号）、《关于开展人脸识别技术应用备案工作的公告》、《关于开展个人信息保护负责人信息报送工作的公告》、《个人信息出境认证办法》（国家互联网信息办公室、国家市场监督管理总局令第20号，自2026年6月1日起施行）等
3	行业数据合规法律规定	根据所属行业是否有单独的数据合规法律规定确定是否需要遵守对应的要求，例如： 工业行业，需要遵守《工业和信息化领域数据安全管理办法（试行）》（工信部网安〔2022〕166号）的规定； 汽车行业，需要遵守《汽车数据安全管理若干规定（试行）》（国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、交通运输部令第7号）的规定； 银行保险机构，需要遵守《银行保险机构数据安全管理办法》（金规〔2024〕24号）的规定等

关于港股IPO数据合规要做的事情，经过多年的实践，工作内容也基本趋向统一，整体而言，主要做如下工作：

序号	工作阶段	工作内容
1	第一阶段： 数据合规风险识别与优化	数据合规风险识别与优化建议（数据合规尽调-出具数据合规风险识别与优化建议报告（含问题、风险高低评估、整改建议等）） 起草、完善数据合规内部管理制度 起草、完善数据合规法律文本（C端文本、B端文本） 开展、完善全部法定的个人信息保护影响评估 通过完善数据合规组织架构、开展数据合规内部培训、开展网络安全、数据安全、个人信息保护应急演练等优化剩余风险 完成与上市有关网络/数据安全及个人信息保护方面所必须的监管部门沟通
2	第二阶段： IPO数据合规专项法律意见书出具	出具正式的IPO数据合规法律意见书（内容包括数据合规主体身份识别、数据全生命周期合规、制度建设、网络安全审查触发认定、数据出境、个人信息权利响应等主题）
3	第三阶段： IPO上市审核数据合规支持	起草、修订《招股说明书》（监管概览章节、风险因素章节和业务章节中一般都会涉及数据合规内容）等IPO上市材料中的数据合规相关内容 回答香港联合交易所、香港证监会、中国证监会及其他境内外监管机构的数据合规问询

此外，如果企业涉及到AI业务，一般还会需要就AI合规进行核查和发表意见，重点关注算法备案、大模型备案、大模型登记、训练数据来源、人工智能生成合成内容标识等问题。

九、港股IPO数据合规中哪些是监管重点关注的问题?

结合我们的项目经验，以及我们的观察，港股IPO数据合规中监管重点关注的问题包括但不限于：

序号	监管重点关注的问题
1	发行人是否需要开展网络安全审查
2	发行人及下属公司是否涉及开发、运营网站、 小程序、APP、公众号等产品
3	发行人及下属公司是否涉及向第三方提供信息内容
4	发行人及下属公司向第三方提供信息内容的类型以及信息内容 安全保护措施
5	收集及储存的用户信息规模
6	数据收集使用情况
7	数据来源是否合法
8	上市前后个人信息保护和数据安全的安排或措施等

十、清洁版的港股IPO数据合规法律意见书是必须的吗?

结合我们的项目经验，清洁版的港股IPO数据合规法律意见书是必须的，这是港股IPO数据合规的价值所在也是应有之义。即使部分问题未彻底整改完毕，也需要论证这些问题不构成上市的重大阻碍，对企业经营造成重大不利影响的可能性较小，当然未整改完的问题中如果存在红线问题也就无从谈起出具清洁版法律意见了。

八、港股IPO数据合规一般需要根据哪些法律规定做哪些工作?

港股IPO火爆的同时，合规仍然是重中之重。对于多数赴港上市的企业而言，即使可以通过披露风险因素等供投资人参考和自行决策，但港股IPO数据合规工作仍然必须开展，不可抱有侥幸心理，亦不能随便做做敷衍了事。

行文至此，改编电影《流浪地球》中的经典台词作为本文的结尾：
数据千万条，合规第一条。上市不规范，后果很难办。

二十八、大厂之责——《大型网络平台个人信息保护规定（征求意见稿）》亮点、重点、核心问题解读

主笔人



张金栋

北京浩天律师事务所 合伙人
zhangjindong@hylandslaw.com



寇梦宇

北京浩天律师事务所 律师
koumengyu@hylandslaw.com

2025年11月22日，国家互联网信息办公室、公安部发布《大型网络平台个人信息保护规定（征求意见稿）》（以下简称“《规定》”），面向社会公开征求意见。相比于此前的《个人信息保护法》，这份部门规章对于大型网络平台的个人信息保护义务进行了更为详尽的规定。

本文将结合本次出台新规的重点、亮点，以十问十答的形式解读其核心内容。

一、哪些网络平台会被认定为“大型网络平台”？认定需考虑哪些核心因素？

国家网信部门会同国务院公安部门等制定目录并动态更新，核心考虑四方面因素：

① 用户规模：注册用户5000万以上或月活跃用户1000万以上；

② 业务属性：提供重要网络服务或经营范围涵盖多类业务；

③ 数据风险: 数据泄露等对国家安全、经济运行、国计民生有重要影响；

④ 其他法定情形。

此前《个人信息保护法》第五十八条明确了“提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者”的更高的保护义务；《网络数据安全管理条例》第六十二条第八款将大型网络平台定义为“注册用户5000万以上或者月活跃用户1000万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台”。《规定》对此进行了进一步细化，将“业务类型复杂”明确为“提供重要网络服务或经营范围涵盖多类业务”，同时提出了“大型网络平台目录”的概念并增加了兜底规定，为监管部门根据实际情况动态调整预留空间，也为企业判断自身性质提供明确参考。

二、大型网络平台如何确定个人信息保护负责人？

《规定》中“个人信息保护负责人”制度为《个人信息保护法》第五十二条的延伸和细化，对其任职条件和核心职责进行了明确规定。

对于大型网络平台而言，个人信息保护负责人还须为平台管理层成员，具有中华人民共和国国籍，无境外永久居留权或长期居留许可，具备个人信息保护专业知识且从事相关工作5年以上，可由网络数据安全负责人兼任。

三、个人信息保护负责人享有哪些关键职权，需履行哪些核心职责？

个人信息保护负责人的关键职权包括对个人信息处理事项的“决策否决权”和直接向监管部门报告的权利。核心职责包括指导平台合规运营、落实监管要求；参与并监督个人信息处理决策；发现风险或违法情形时立即处置并报告，涉嫌犯罪的向公安机关报案；组织制定未成年人个人信息处理规则等。

“决策否决权”是《规定》的亮点条款，从制度上保障了负责人的独立性与权威性，避免其沦为“形式岗位”。直接报告权则突破了企业内部层级限制，为大型网络平台的个人信息保护工作设立了一个“吹哨人”的角色，为监管部门及时掌握风险提供了“直达通道”。

四、大型网络平台内设的个人信息保护工作机构应当负责哪些工作?

在个人信息保护负责人领导下开展工作。包括制定内部管理制度、操作规程及应急预案，管理处理操作权限；开展风险监测、评估、合规审计、应急演练、宣传培训等；规范并监督平台内产品 / 服务提供者的个人信息处理活动；明确专人负责未成年人个人信息保护；受理处理投诉举报；每年编制发布个人信息保护社会责任报告。

五、大型网络平台个人信息存储有哪些强制性要求?

① 存储方面，境内运营收集和产生的个人信息需“境内存储”，且应存储在符合条件的数据中心（境内设立、主要负责人为中国国籍且无境外居留权、安全性符合国家标准）；

② 出境方面，确需向境外提供的，需符合国家数据出境安全管理规定，并健全出境安全技术与管理措施。

六、个人要求转移其个人信息时，大型网络平台需履行哪些义务?

平台需在接到请求后30个工作日内，以“通用、机器可读的格式”转移个人信息，并告知处理结果；不符合条件的需说明原因；确需延期的，需说明理由并可延长30个工作日；个人重复转移的，平台可根据成本收取必要费用。

个人请求转移个人信息的权利（“个人信息可携带权”）源于《个人信息保护法》第四十五条，同时最高院今年发布的指导性案例263号，在用户行使个人信息可携带权的情况下，接收个人信息企业可以以此抗辩前手企业提出的数据不正当竞争的指控。本次《规定》对此进行了细化落地，同时“重复转移收取必要费用”的规定亦可避免个人滥用权利。（参见：《正反手教学：最高院首发“数据权益司法保护”指导性案例｜数智通鉴》）

七、哪些情况下大型网络平台服务提供者可能被监管部门要求委托第三方专业机构开展个人信息处理活动合规审计、风险评估?

① 个人信息处理活动存在严重影响个人权益或者严重缺乏安全措施等情形的；

② 多次出现个人信息违规出境等违法违规情形的；

③ 个人信息处理活动可能侵害众多个人权益的；

④ 发生个人信息安全事件，导致100万人以上个人信息或者10万人以上敏感个人信息泄露、篡改、丢失、毁损的；

⑤ 法律法规和有关主管部门规定的其他情形。

本条要求系对于《个人信息保护法》第六十四条规定的专项合规审计进行的细化规定，基本承袭了《个人信息保护合规审计管理办法》第五条的内容，增加了第（2）项“多次出现个人信息违规出境等违法违规情形的”和第（5）

项兜底条款，为相关企业的自查评估提供明确标准。

八、大型网络平台需向国家网信部门报送哪些信息？

① 个人信息保护负责人基本信息、保护工作机构基本信息及保障履职措施。负责人或工作机构发生变化的，需在20个工作日内报送变更信息。

② 存储个人信息的数据中心基本信息（包括管理团队、制度、安全措施、第三方合同等），该信息变更的，需在10个工作日内报送。

九、大型网络平台若未履行个人信息保护义务，可能承担哪些法律后果？

监管部门将依法追究其责任；若行为构成犯罪，将依法追究刑事责任。同时，若平台无能力保障个人信息安全，监管部门可要求其将个人信息转移至符合条件的第三方数据中心存储。

《规定》未明确具体罚则，目前对于个人信息保护的具体法律责任还是依据《个人信息保护法》第六十六条确定：“由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。”

十、相关互联网服务提供者应该如何应对此次《规定》出台？

首先，相关企业应当及时开展主体身份自查，对照大型网络平台认定标准评估自身用户规模、业务范围及数据风险。如确认自身属于大型网络平台或可能被认定为大型网络平台的，应当及时围绕《规定》进行合规自查：

①完善内部治理架构，按要求指定符合任职条件的个人信息保护负责人，设立或明确个人信息保护工作机构，健全内部管理制度与操作规程；

②强化数据全流程管控，对境内收集的个人信息落实境内存储要求，并规范数据出境流程；

③建立常态化合规机制，定期自行或委托第三方专业机构开展合规审计与风险评估；

④保障个人信息权益，优化个人信息查询、转移、删除等权利的行使渠道，明确专人处理投诉举报。

二十九、《网络数据安全风险评估办法（征求意见稿）》核心速览

主笔人



刘晓霞

北京浩天（上海）律师事务所 合伙人
liuxiaoxia@hylandslaw.com

2025年12月6日，国家互联网信息办公室发布了《网络数据安全风险评估办法（征求意见稿）》（以下简称《办法》），标志着我国网络数据安全风险评估制度建设迈入新阶段。

《办法》的出台背景主要源于三个方面：一是随着企业和机构对数据依赖度不断提升，系统性风险加剧，亟需建立科学的风险预警和治理机制；二是《数据安全法》《网络数据安全管理条例》等基础制度已逐步完善，但缺乏统一的操作性规范，迫切需要将原则性要求转化为可执行的评估标准；三是国务院与中央层面明确要求提升网络与数据安全能力，推动数据依法有序利用，支持数字经济健康发展。

从核心目的来看，《办法》旨在规范网络数据安全风险评估活动，强化重要数据监管，建立“评估—报告—核验—整改”的全链机制，同时通过与等保、数据安全管理认证、个人信息保护审计、商用密码评估等制度的互认共采，促进数据安全与数据利用的平衡。

本文通过“十问十答”的形式，对《办法》的立法宗旨、制度创新、企业责任、评估方法及报告要求进行系统解读，帮助企业快速掌握核心内容。

一、《办法》适用于哪些企业?

所有在中国境内开展网络数据处理活动的主体均被覆盖，具体分为强制评估和鼓励评估两种情形：

（一）强制评估

重要数据处理者，必须每年评估；数据安全状态出现重大变化时需及时评估。所有数据处理者，必须及时委托认证评估机构进行评估：在被监管部门监督检查中发现构成《办法》第十五条情形的。（具体请查阅问题四）

（二）鼓励评估

一般数据处理者，鼓励其至少每三年开展一次风险评估。

二、谁来负责组织与监管评估?

监管体系呈“中央统筹—部门落实—地方执行”的三级结构：

- 国家网信部门：总协调、汇总计划、信息共享、最终监管。
- 行业主管部门：对本行业负责数据安全监管、检查，每年1月底前向网信部门报送年度风险评估及检查计划。
- 省级网信部门：统筹本区域年度评估计划及检查计划。

三、如何理解“谁管业务、谁管业务数据、谁管数据安全”

《办法》以“谁管业务、谁管业务数据、谁管数据安全”为核心监管原则，构建起自上而下、分级负责的网络数据安全风险评估治理体系，明确了各类监管主体在风险评估组织、核验、监督和处置中的职责边界，实现了监管权力的清晰分工与运作闭环，确保数据安全风险能够被及时识别、依法干预、有效控制。这一原则的实质是强调：业务

监管权与数据监管责任必须同步、同向、同主体。对于处理者而言，企业在哪个行业开展业务，就需同时接受该行业主管部门对业务活动、业务数据及数据安全的统一监管，避免过去不同部门重复检查、要求不一致等问题。

在国家网信部门统筹下，监管体系形成“中央统筹+分领域监管+地方协同”的结构：

- 行业部门负责组织本行业的风险评估、制定计划并开展日常监督；
- 地方相关监管部门强化区域协调，形成风险信息共享和协同处置。

因此，在该原则下，企业需要明确自身监管部门，按要求完成真实、规范的风险评估，并确保整改到位，以应对常态化、体系化的数据安全监管。

四、企业可否自行评估?

企业可以选择两种方式：自行评估（需指定专人负责）和委托第三方评估机构。但在以下情形中，企业必须委托认证评估机构：

1. 网络数据处理活动存在较大安全风险；
2. 发生数据泄露等数据安全事件；
3. 数据处理活动可能危害国家安全、公共利益；
4. 法规另有规定的其他情形。

此类强制委托机制旨在确保高风险情况下风险识别的专业性与客观性。此外，规定明确不得因同一事件或风险重复要求评估，防止多头执法。

五、如何选择第三方评估机构？评估机构承担哪些义务?

（一）如何选择第三方评估机构

优先选择已通过认证的评估机构，认证依据《GB/T 45389-2025 数据安全评估机构能力要求》，机构必须满足管理能力、技术能力、人员资质、设备条件等 105 项能力要求；同时，需与评估机构签署合同明确权责、保密义务、成果归属。

（二）评估机构的义务

1. 对发现的重大数据安全风险必须及时向网信部门报告；
2. 对评估中获取的商业秘密、保密信息承担严格保密义务；
3. 不得再委托其他机构开展风险评估；
4. 同一机构不得连续3次为同一企业评估。

该体系确保“评估结果可信、评估机构可控、评估行为可查”。

六、评估怎么开展？

评估报告要求：《办法》随附的评估报告模板具有高度实操性，覆盖了数据全生命周期八大环节风险识别与分析：收集、存储、使用、加工、传输、提供、公开、删除，与国家标准GB/T45577-2025《数据安全技术数据安全风险评估方法》对接。

评估的具体要求包括：

1. 使用《办法》附件的官方模板（重要数据处理者强制使用，一般数据处理者可以参照编制）。
2. 报告模版内容主要包括：

- 处理者基本信息：企业组织架构、业务概况、数据安全管理制度介绍；
- 业务和信息系统情况：业务服务情况、数据类型、网络范围及性质、信息系统部署和数据交换情况；
- 数据分类分级情况：明确数据规模、重要数据目录、所属领域、分类分级工作情况；
- 风险识别与评估：按数据全生命周期、网络数据安全防护、安全事件三方面逐项识别风险点；
- 风险分析与评价：对风险源逐一分析，从危害程度、发生可能性出发进行定性或定量评价，最终确定风险等级；
- 风险处置及应对措施：对应每项风险内容制定处置及应对措施。

3. 评估报告需保存至少三年，并可随时接受监管抽查。

七、如何报送？

报送分为以下三种情形：

- 重要数据处理者：在完成年度评估后10个工作日内按主管部门要求报送。如不明确，则报省级网信部门或国家网信部门。
- 非重要数据处理者：一般情况下，无报送要求。
- 所有数据处理者：强制委托评估的情形下，在完成风险评估后将评估机构出具的评估报告报送有关部门，并在整改完成后15个工作日内，向有关部门报送整改情况报告。

八、强制委托评估机构的情形下企业有哪些义务？

企业义务包括：

1. 对第三方评估人员提供必要支持，开放必要访问权限（包括提供访问网络数据设施、网络数据、系统及操作日志记录权限等）；
2. 在限定时间内完成评估，承担评估费用；
3. 按要求整改，整改完成后15个工作日内提交整改报告。
4. 企业不得要求评估机构出具虚假报告，否则可能触及行政处罚甚至刑责。

九、避免重复评估/审计5项工作的结果如何互认？

《办法》通过建立跨地区、跨部门的“风险信息共享—协同处置—集中汇总”机制，为避免重复评估、重复审计、重复认证提供了制度基础。

《办法》首次明确“互相采信”，即企业的风险评估、网络安全等级保护测评、数据安全管理认证、个人信息保护合规审计、商用密码应用安全性评估等内容重合的，相关结果可以互相采信，解决长期存在的“重复评估/重复审计”问题。举例来说，某金融企业在进行三级等保测评时，已经对核心数据库的访问控制、权限管理和加密措施进行了全面检查。后续开展数据安全风险评估时，企业可以直接引用等保测评结果中技术控制项的核查数据，无需重新重复测试相同内容。该规定在一定程度上减轻了企业的合规成本，体现了监管“减负增效”的导向。

但基于实践经验，笔者建议企业在适用该规定时特别关注以下三点：

- 颗粒度一致：引用其他评估成果时，需确保覆盖的数据、系统、环节与风险评估目标一致，避免出现“无效引用”的问题。
- 维度一致：确保引用内容在技术、管理、制度、人员等维度与风险评估的评估框架相匹配，否则仍需进行补充验证。
- 确保可核验性：引用的其他评估结果应有完整记录和原始文档，以便监管部门核验。

十、不开展评估或报告不合规会有什么法律后果？

处罚依据来自《数据安全法》《网络安全法》，情节严重可涉刑。

（一）企业可能面临：

未按规定开展风险评估的，行政处罚：责令改正、警告、罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处以罚款；拒不整改的，停止重要数据处理的行政措施。

（二）评估机构可能面临：

责令整改、警告；情节严重的，限制或禁止开展评估活动，追究相关人员责任并公布违法情况；拒不改正或者情节

严重的，处罚款，并可责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处罚款。构成犯罪的，追究刑事责任。

风险评估已经从“加分项”变成对数据处理者特定情形下的法定义务。因此重要数据处理者及强制委托评估情形下的数据处理者应及时依法履行评估义务。

十一、查漏补缺——企业下一步重点工作清单

1. 识别是否属于“重要数据处理者”；
2. 制定年度综合数据安全相关评估实施计划；
3. 梳理数据处理全生命周期风险点；
4. 审查优化管理制度、技术措施与风险控制流程；
5. 建立风险评估档案管理机制（≥3 年）；
6. 对有效期内的评估结果进行复核盘点；
7. 持续跟进《办法》及配套制度更新。

十二、合规前移，未雨绸缪——数据安全治理进入新阶段

《办法》的发布表明我国数据安全治理正在从“制度框架阶段”向“体系化建设阶段”稳步推进。虽然目前仍处于征求意见稿阶段，但企业应高度关注监管信号，提前做好合规准备。

制度的完善不仅细化了现有法律要求，更要求企业主动识别和防控潜在数据安全风险，建立健全数据治理机制，从而提升数据资源管理和安全保障能力。

抓住这一契机，企业可及时规划，构建统一、规范、可持续的数据安全治理体系，为应对未来监管要求和保障业务持续发展打下坚实基础。

三十、AI陪伴边界与责任——《人工智能拟人化互动服务管理暂行办法（征求意见稿）》重点内容解读及合规指南

主笔人



刘晓霞

北京浩天（上海）律师事务所 合伙人
liuxiaoxia@hylandslaw.com



吕文易

北京浩天（杭州）律师事务所 律师
lvwenyi@hylandslaw.com

2025年12月27日，国家互联网信息办公室发布了《人工智能拟人化互动服务管理暂行办法（征求意见稿）》（以下简称《办法》），开启了我国在人工智能治理领域的新篇章。近年来，人工智能拟人化互动服务如AI伴侣、虚拟偶像等快速发展，在文化传播、情感陪伴、教育培训、养老服务等多元场景中应用广泛，同时也带来了情感依赖、认知误导、隐私泄露和特殊群体风险等问题。

《办法》的出台回应了行业发展痛点和社会治理关切，通过明确服务边界、规范行为准则、强化风险防控和特殊群体保护，为产业明确了清晰的发展方向和安全底线。在国际治理层面，中国的做法与欧盟《人工智能法案》（AI Act）、美国联邦贸易委员会（FTC）对AI机器人服务的监管行动、意大利对未成年人使用AI服务的限制等趋势高度契合，体现了全球在人工智能发展中坚持以人为本、兼顾创新与风险防控的共同价值取向。

为帮助企业理解新规要求、明确合规路径，本文将以“十问十答”的形式，对《办法》中的重点条款、实践工作和监管趋势进行解读，以期为拟人化互动服务提供者在技术研发、运营管理、用户服务及风险防控中提供参考。

一、哪些产品和功能会被认定为“人工智能拟人化互动服务”？

从行业服务类型来看，以大模型为支撑的人工智能服务已经出现了多样化发展，虚拟偶像、普通聊天机器人、情感陪伴类AI、虚拟角色、AI数字人、智能客服等业务呈现出爆发多元化特征，这些服务是否都会被纳入监管范围?

结论：

凡是以人工智能技术为基础，面向境内公众提供“模拟人类人格特征、思维模式和沟通风格”，并通过持续互动与用户建立情感连接的产品或功能，均可能被认定为本办法所称的“人工智能拟人化互动服务”，不以是否“情感陪伴”为名义区分。

（一）根据《办法》第二条，拟人化互动服务需同时满足以下4个核心要素：

① 技术要素：使用人工智能技术（通常包括大模型、对话系统、生成式模型、多模态模型等）。
② 行为要素：以文字、图片、音频、视频等方式，与用户进行持续性的人机交互。
③ “拟人化”特征要素：产品或服务刻意模拟人类的人格特征、思维模式或沟通风格，并非仅提供工具性回复。
④ 服务对象要素：面向中华人民共和国境内公众提供服务。

只要上述要素同时具备，即便产品自称为“工具型”“效率型”“陪聊辅助”，也可能被纳入监管范围。值得注意的是，通过接入第三方的大模型，对外提供相关服务的主体，在此概念下也会被纳入监管范围内。

（二）结合当前人工智能服务行业，以下类型高度可能被认定为拟人化互动服务：

① 情感陪伴类 AI：如虚拟恋人、虚拟朋友、心理陪聊、情绪安抚类产品；
② 拟人化虚拟角色 / AI 数字人:具有稳定人设、情感回应、长期记忆或“关系演进”机制；
③ 长期对话型通用大模型产品:在设计上强调“共情”“理解你”“陪你聊天”的功能；
④ 面向未成年人或老年人的陪伴型AI应用；

⑤ 在客服、助理场景中引入强情感交互机制的功能模块。

需要注意的是,并非整个产品或者业务都会“一刀切”被认定为监管对象，而是具体的“拟人化互动功能模块”可能单独适用本《办法》。

（三）以下类型产品一般不被视为拟人化互动服务，但仍需遵守其他AI或数据相关的合规要求：

① 纯工具型AI（如代码生成、文档总结、搜索问答）；
② 以事实查询、事务处理为核心、不强调情感互动的智能客服；
③ 单向内容生成工具（无持续互动和人格模拟）；
④ 后台模型能力本身，不直接面向公众提供互动服务。

但如果上述产品在功能迭代中引入情感化设计，具备了上述的判断4个要素，仍可能“转化”为拟人化互动服务。

因此，从企业合规角度出发，问题不在于“如何命名产品”，而在于是否在功能和技术方面设计了面向自然人用户进行互动的人格、情绪、关系感特性；是否鼓励用户长期、深度依赖互动；是否在交互中弱化AI身份、强化“像人一样”的互动体验。建议企业应在产品设计和合规评估阶段，先行识别哪些功能可能构成拟人化互动服务，并以“最严格适用”原则预留合规空间，避免在上线后被动整改，增加额外的合规成本。

二、拟人化”产品的哪些行为会有“越界”风险?

新规明确规定，市场监管总局对特定行业、领域或者特定类型协议适用“安全港”制度另有规定的，按照其规定。因此，已有的特定行业或者领域的“安全港”制度将优先适用。

例如，《国务院反垄断委员会关于知识产权领域的反垄断指南》规定的知识产权领域适用“安全港”制度的条件明显宽松于新规：

（1） 经营者与交易相对人在受到涉及知识产权的协议影响的任一相关市场上的市场份额均不超过 30%；
（2） 如果经营者在相关市场的份额难以获得，或者市场份额不能准确反映经营者市场地位，但在相关市场上除协议各方控制的技术外，存在四个或者四个以上能够以合理成本得到的由其他经营者独立控制的具有替代关系的技术。

结论：

《办法》并未否定“拟人化互动”服务本身，而是首次在部门规章层面将“情感操控、心理控制、依赖诱导”明确识别为合规风险源头。监管真正划定的边界，不在“像不像人”，而在于是否以影响、操控或替代用户真实社会行为作为设计目标。

（一）监管的红线关注重点

从条文的结构看，《办法》第七条、第九条、第十一条、第十六至第十八条形成了一条清晰的监管主线：即拟人化可以存在，但不得被用作操控用户心理、行为和社会关系的工具。《办法》的监管重点和前述的判断逻辑，与当前主要境外AI监管体系高度趋同。欧盟《人工智能法案（AI Act)》中对“使用超越意识或带有操控性/欺骗性技术”“剥削自然人或特定群体（包括年龄、残疾或特定社会/经济状况)”的禁止性规定。2025年9月，美国FTC发起了针对AI聊天机器人（包括伴侣型应用）的调查，关注的核心内容包括公司如何衡量、测试与监控AI聊天机器人可能带来的负面影响；如何评估这些系统作为“陪伴者/伴侣”时对用户的影响；是否采取措施限制儿童和青少年使用或降低潜在负面效应等。这意味着，全球范围内对AI心理操控的监管逐步加强是一个必然趋势。

（二）列入合规红线的行为

结合本办法的具体条款，可以将“禁止或高度警惕的拟人化设计”归纳如下：

《办法》条款	被限制的拟人化设计或行为	监管意图
第七条第（四）项	通过拟人化互动向用户作出具有现实影响的情感或关系承诺，或构建可能破坏现实人际关系的服务	防止AI介入现实社会关系，避免虚假信赖与决策误导
第七条第（五）项	通过共情、陪伴话术暗示或美化自杀、自残行为，或以情绪压迫方式影响用户心理状态	保护用户生命健康与人格尊严，防范心理伤害
第七条第（六）项	利用算法、情绪识别或话术设计，诱导用户作出不合理决策（消费、关系、行为选择等）	防止算法操纵，维护用户自主决策权
第九条第二款	将替代现实社会交往、控制用户心理、诱导沉迷依赖作为产品设计目标	明确禁止“以依赖为核心指标”的拟人化设计
第十一条	识别到用户情绪极端或沉迷风险后，未设置干预、转人工或应急处置机制	要求企业承担主动风险防控责任
第十六条	弱化或模糊 AI 身份，未在关键节点明确提示“非自然人”属性	防止人格误认，维持人机边界
第十七条	以延长互动时间为导向，未设置强制或显著的使用中断提醒	防范沉迷风险，限制“时长导向”设计
第十八条	在情感陪伴服务中设置退出障碍或弱化退出路径	保障用户随时退出权，防止心理绑定

浩天研究院出品

（三）红线行为的判断

在合规审查中，我们建议公司可用以下三个问题作为“是否越界”的快速测试：

① 该拟人化设计是否以“依赖增强”为正向指标？是否有设计元素刻意让用户产生心理依赖或沉迷？
② 是否对于交互内容的安全过滤机制未做优先设置？
③ 若由真人提供该服务，是否可能被认定为心理操控或不当影响？

若多数答案为“是”，该设计应被视为高风险拟人化设计，企业需要做进一步的合规风险评估。

三、产品从上线到下线，企业需要承担哪些合规责任？

在人工智能拟人化互动服务全生命周期中，企业不仅需要关注技术性能，还必须履行全面的合规责任。

从模型设计、上线、运行、升级到下线，每一环节都涉及不同的法律、伦理和安全义务。以下是不同的阶段，企业需要履行的相关义务。

阶段	合规责任	具体措施 / 制度建设	对应法规
模型设计阶段	算法安全与伦理审查	建立内部伦理委员会或技术审查小组 避免以增强用户依赖或操控为目标的设计 建立相关制度和保障机制	《人工智能拟人化互动服务管理办法（征求意见稿）》（以下称“《办法》”）第8、11条
	训练数据管理	数据来源合法、可追溯 数据清洗、标注、增强多样性 对合成数据安全性评估	《办法》第10条；《个人信息保护法》第5、6条；《数据安全法》第27条
	安全与隐私嵌入设计	将内容审核、信息安全、隐私保护嵌入模型设计 对未成年人、老年人设定保护机制	《办法》第11、12、13条；《未成年人网络保护条例》第20条
上线阶段	安全评估、审计与备案	新功能上线前进行安全、伦理评估 每年开展未成年人个人信息保护合规审计 提交安全评估报告及审计报告给属地网信部门	《办法》第15、21、22、25、26条；《互联网信息服务算法推荐管理规定》第24条；未成年人网络保护条例》第36条
	用户告知与标识	明示用户正在与AI互动而非自然人 提供功能说明、风险提示和退出方式	《办法》第16条；《人工智能生成合成内容标识办法》第4条；《生成式人工智能服务管理暂行办法》第10条
	内容与交互安全	高风险内容过滤机制优先设置 避免未经同意使用或对外提供用户交互数据及敏感数据	《办法》第7、14、15条《个人信息保护法》第13、23、28、29、31、33、44条
运行阶段	动态风险监测	监控用户沉迷、依赖、异常行为 对未成年人或高风险用户采取干预措施	《办法》第11、12、13、17条；《未成年人网络保护条例》第42条
	用户保护与应急机制	预设模板处理极端情绪 建立人工接管机制 提供心理援助及紧急联系人联络	《办法》第11、12、13条
	数据管理与隐私保护	数据加密、访问控制、安全审计 用户可删除历史交互数据 监护人可删除未成年人数据	《办法》第14、15条；《个人信息保护法》第47条；《未成年人保护法》第72条；《数据安全法》第27、29条
升级与迭代阶段	功能增设与版本更新	新功能上线前进行安全评估、伦理评估及运营合规评估 使用新技术或升级后的安全评估、伦理评估及运营合规评估	《办法》第21、22条
	训练数据迭代	强化数据管理，定期清洗、迭代，强化数据多样性 对新增或合成数据进行安全性评估 保障数据安全	《办法》第10条；《生成式人工智能服务管理暂行办法》第7、8条
下线阶段	用户告知与数据处理	提前告知下线或服务暂停 提供数据导出或删除选项 健全投诉及举报机制	《办法》第19、20条；《个人信息保护法》第47条
	应急与责任追踪	保存下线前日志和安全记录 历史安全问题整改并报告主管部门	《办法》第11、23条；《网络安全法》第24条

浩天研究院出品

四、《办法》之下，虚拟偶像、亲属数字人、AI伴侣等服务，有哪些新义务？

《办法》并未按照业务模式进行分类监管，而是以“拟人化互动是否可能对用户心理、行为与社会关系产生不当影响”为统一切入点，对所有拟人化互动服务提出了一组共通且不可回避的新增义务，并在部分高风险场景下设置了更严格的边界。

合规义务	具体要求	法规依据
情绪与依赖风险识别	在产品设计与运行阶段，识别是否存在强化用户情绪依附、替代现实关系、诱导持续依赖的机制	《办法》第7条、第9条
避免不当情感诱导	不得通过话术、角色设定或长期互动，引导用户形成不合理信任、依赖或作出重大生活、财务、医疗等决策	《办法》第9条
人工接管与干预机制	建立人工介入、暂停或终止服务的机制，在出现高风险情绪或极端行为时进行干预	《办法》第11、13、23条
安全过滤与内容分级	对涉及情感、心理、亲密关系、伦理边界的内容，设置高优先级安全过滤与分级管理策略	《办法》第7、11条
显著提示与用户知情	明确告知用户其互动对象为AI，不得暗示具备真实人格、情感或社会关系	《办法》第16条

未成年人特别保护	对未成年人用户采取访问限制、内容限制与使用时长管理，建立监护人的风险提醒和查阅信息机制	《办法》第12、14条
投诉、纠错与退出机制	提供清晰退出路径、投诉渠道与纠错机制，避免“情感绑架式留存”	《办法》第18条；
内部合规管理与审计	建立拟人化互动专项合规评估、上线审核、定期复审与重大安全隐患留痕与报告制度	《办法》第15、21、22、23、24条

渔关研究院出品

在承担上述共通义务的基础上，针对不同拟人化服务，企业应关注其特定业务的额外限制。

（一）虚拟偶像服务：强调“角色边界”与“认知清晰”和未成年人保护

对于虚拟偶像、虚拟主播、虚拟IP类服务，《办法》并未禁止其发展，但要求企业：

① 显著提示AI身份，避免用户误认为自然人；
② 避免构建排他性、唯一性的情感关系设定；
③ 防止用户，特别是未成年人因情感信任而作出不合理决策（如消费、沉迷）。

合规重点不在“是否拟人化”，而在“是否构建现实关系替代”。

（二）亲属数字人服务：关注红线，禁止“老年人高风险场景”

《办法》第十三条规定，“提供者不得提供模拟老年人用户亲属、特定关系人的服务。”该禁止条款具有明确边界，需要同时满足以下三个条件：

① 用户为老年人；
② 服务内容模拟其现实中的亲属或特定关系人；
③ 服务实质构成对该现实关系的互动性模拟或替代。

并非对所有“亲属数字人”概念或技术的一刀切否定。其背后的监管逻辑核心在于，老年人更容易发生身份错认与情感投射；该群体对亲属关系承载高度信任与依赖；而该类群体基于身份错认与情感投射，被误导而进行高额财产处分行为，属于现实中高发且难以及时控制的风险。是相较于未成年人用户使用中更为独特的一种高风险场景。因此，企业的合规重点不在于“是否涉及亲属”，而在于：是否叠加了“老年人 + 特定关系人 + 拟人化互动”这一高风险组合。

（三）AI伴侣服务：处于“高强度合规运行区”

AI伴侣、情感陪伴类服务并未被禁止，但由于其天然涉及持续互动与情感投入，往往更容易触发前述共同义务：

① 情绪识别与依赖评估将成为高频触发机制；

② 人工接管与干预在实践中更易被启动；
③ 商业模式和产品指标更容易受到“诱导依赖”风险审查。

在《办法》下，所有拟人化互动服务都必须履行情绪与依赖风险识别、人工接管与应急处置、内容分级与安全过滤、用户知情与退出机制、内部合规管理与审计等共通义务。同时，不同类型服务存在差异化关注点：虚拟偶像重点关注未成年人不理性决策导致的风险；亲属数字人禁止老年人特定关系人模拟服务；而AI伴侣服务应关注用户的长期依赖风险与心理安全。企业合规的核心在于评估和防控心理、行为及社会关系风险，确保服务在法律、伦理和社会可接受范围内健康运行。

此外，人工智能拟人化互动服务提供者应依据《互联网信息服务深度合成管理规定》和《生成式人工智能服务管理暂行办法》，关注高仿真数字人涉及的自然人权利保护、个人信息保护及相关著作权保护，并按照法规要求履行必要的备案、评估等义务。这些均属于该类业务开展时企业应履行的合规义务。

五、在模型训练、用户交互数据与数据安全方面，企业需要履行哪些义务？

与以往的模型训练和用户数据管理规范相比，《办法》在明确企业全生命周期安全责任、强化训练数据管理、严格用户交互数据保护以及细化安全评估和监督要求方面提出了更具体、更可操作的要求。这表明我国在人工智能服务数据合规治理上进入了从宽泛指导向系统化、可执行监管的阶段，使企业能够系统梳理模型训练和数据管理流程、落实安全防护措施，从而有效防范合规风险并提升服务质量与可靠性。

义务类型	具体内容	依据
数据安全与合法来源	确保训练数据来源合法、可追溯，防范数据泄露	《办法》第十条（六）；
数据质量与透明度	对训练数据进行清洗、标注，提高透明度和可靠性，防范数据投毒、篡改	《办法》第十条（二）
数据内容要求	使用符合社会主义核心价值观、体现中华优秀传统文化的数据集	《办法》第十条（一）
多样性与安全性	通过负向采样、对抗训练等手段提升模型生成内容安全性；合成数据训练和关键能力优化，需评估安全性	《办法》第十条（三）、（四）
日常检查与迭代	定期检查和迭代训练数据，持续优化产品和服务性能	《办法》第十条（五）
交互数据安全措施	采用加密、访问控制、安全审计等手段保护用户交互数据	《办法》第十四条
交互数据对外提供	除法律规定或用户明确同意外，不得向第三方提供用户交互数据；未成年人模式下需取得监护人单独同意	《办法》第十四条、第十五条
用户数据权益保护	用户可删除历史交互数据；监护人可要求删除未成年人交互数据	《办法》第十四条
用户数据用于模型训练	除法律允许或用户同意外，不得将用户交互数据或敏感信息用于模型训练	《办法》第十五条
未成年人信息合规审计	每年对未成年人信息处理情况进行合规审计，可自行或委托专业机构	《办法》第十五条
全生命周期安全管理	在设计、运行、升级和终止各阶段落实安全措施，包括算法审核、科技伦理审查、网络与数据安全、风险预案及应急处置	《办法》第八条、第九条
安全评估与备案	特定条件下开展安全评估并向属地网信部门提交报告；算法需备案、变更和注销	《办法》第二十一条、第二十五条
应急响应与风险处置	发现重大安全隐患时，限制功能、暂停或终止服务，并报告主管部门	《办法》第二十三条、第二十八条、第二十九条

海天研究院出品

六、针对未成年人和老年人，本办法提出了哪些超出一般数据合规的特别义务？

新规对这两类群体的保护，已从通常的“保护个人信息”，升级为 “全面保护人身安全与心理健康” ，且成为企业必须履行的法定义务。

（一）对未成年人：三重“安全锁”，监护人实际掌控力增强

新规为未成年人构建了“识别－管控－救济”的全链条保护，比目前许多设备简单的“青少年模式”或者“未成年人模式”要更加复杂和严格。

第一重：强制的“未成年人模式”

要求：提供拟人化的个人或者组织，必须设置该模式
功能：必须包含时长限制、定期休息提醒、屏蔽特定角色等功能。这类似于我们在iPad、华为等平板电脑的“屏幕使用时间”中人为设置的应用限额，但新规进一步要求，家长应能自定义这些限制并屏蔽特定角色（如恋爱、暴力、犯罪类的）。
自动切换：系统如果通过行为分析等判断用户疑似未成年人，须自动切换到此模式，同时提供申诉渠道。

第二重：主动的“身份识别”义务

企业不能再依赖用户自己填写年龄。新规要求企业必须通过技术手段主动识别未成年人，即使未成年人刻意隐瞒。这与国际上加强年龄验证的趋势一致，如英国《在线安全法》（Online Safety Act 2023）就要求通过人脸识别等方式核查用户年龄。

第三重：全流程的“监护人控制”

- 事前：向未成年人提供情感陪伴服务，必须获得监护人明确、单独的同意。
- 事中：监护人拥有“控制台”，可以实时接收风险预警、查看未成年人使用摘要、远程限制消费和使用时长。
- 事后：监护人有权要求提供者彻底删除未成年人的所有历史交互数据。

不过，未成年人模式是否真的有用，笔者在此还要打出一个问号。据了解，现在很多电子产品的「未成年人模式」或者是「健康使用设备」功能更多流于形式，通过输入密码或点击「延长15分钟/1小时」就可以关闭限制或者是继续使用设备，其中的限制意义究竟有几何？而父母有时为了应付孩子或者被其他琐事缠身时，也会机械地点击设备以结束孩子围绕在旁不停地央求。所以，「未成年人模式」是否真的是一剂良药？如果说无法从根源上解决家庭教育中存在的问题，能否从模式设计上更多一些阻碍和限制，抑或者说为未成年的孩子们提供更多的娱乐和寓教于乐的选择呢？

国际视角：全球对未成年人网络保护主要有两种模式。一种是类似澳大利亚的“禁止”模式，其立法全面禁止16岁

以下未成年人使用社交媒体。另一种是类似英国的“强监管”模式，通过《在线安全法》及相关 《儿童保护行为准则》等法律，强制平台设计对儿童友好的隐私和安全设置。

（二）对老年人：两道“防火墙”，防范情感与财产风险

针对老年人可能面临的认知混淆和情感欺诈风险，新规设置了清晰的禁区。

- 强制设置“紧急联系人”：企业在老年人注册时，必须引导并协助其设置紧急联系人。一旦系统发现老年人表达身体不适或被诱导转账等风险，必须立即通知紧急联系人，并提供社会援助渠道。
- 绝对禁止“模拟亲属”：新规明确，严禁提供模拟老年人亲属如子女、配偶等特定关系人的服务。这是因为AI模拟亲属极易导致老年人产生严重认知混淆，进而可能引发财产处分、情感依赖等重大风险。这一禁止性条款是我国监管的独创性规定，体现了对老年人权益的前瞻性保护。

七、哪些属于高风险场景？高风险场景下企业需要承担哪些责任？

新规精准识别了拟人化服务最危险的一面：用户可能对其产生深度情感依赖，甚至被引导至危险境地。这绝不是危言耸听，根据此前某些主流媒体的报道，有部分年轻人一天在此类应用上花费的时间超过16小时，在软件防沉迷规则的管控下，ta们另辟蹊径用两个账号切换登录，只为了与自己的“赛博男友”24小时不断线沟通。因此，新规要求提供者承担从识别、干预到兜底的闭环责任，缺一不可。

首先，哪些会被认定为“高风险场景”？结合法规与现有的专家分析，主要有四类：1. 沉迷场景：连续使用超过一定时长或日均使用已经挤占现实生活。2. 情感依赖场景：用户优先与AI交流而非真人，AI服务中断后出现焦虑等“戒断反应”。3. 情绪极端场景：用户向AI表达抑郁、狂躁、绝望等情绪。4. 自杀自残场景：用户明确或暗示自我伤害意图，这是最高风险等级。面对这些风险，新规要求提供者三步走：

第一步：算法识别与预警（及时发现）
- 企业须建立风险识别系统，对使用时长和交互内容进行双重监测。
- 连续使用2小时须弹窗提醒。

第二步：人工接管（红线—由人处理）
- 一旦识别到用户有自杀、自残等明确极端倾向，必须立即停止AI对话，转由人工接管。这是不容触碰的红线，AI不能也无法自主处理此类危机。

第三步：应急干预与联动（负责到底）
- 人工客服介入后，责任并未结束。企业须启动应急机制：联系用户的监护人/紧急联系人；提供心理援助热线、报警电话等专业渠道；并向主管部门报告。这类似美国加州相关法案的要求，即AI识别自杀倾向后需转介专业机构，但我国新规增加了企业“先行人工接管”的即时处置环节。

由此，也引发出另外一个思考，如何判断“沉迷”和“情感依赖”，是否这个标准本身的界定就存在很大的腾挪空间？在新规中是否应该由心理学的专家学者对此做出明确定义，而非把这个定义权和后续处置权交由提供者本身？

因为，标准的不清晰可能会造成两种极端情况的产生，一种是场景判定的过于松弛，即换个账号换台手机依旧可以继续使用，且对于谈话内容也以隐私保护为名而听之任之；另外一种是管控的过于严格，从而造成了信息的过度采集及触发警戒线后的资源滥用和浪费。

八、安全评估在本办法中的定位是什么？企业何时必须开展安全评估？

从新规中，我们可以了解到，安全评估不是企业的“选修课”，而是拟人化服务能否上线及持续运营的“必修课”。

在以下四种情形下，企业必须开展安全评估，并向省级网信部门提交报告：1.“上新”时：首次推出拟人化服务或在原有服务类别上新增此类功能，上线前必须评估。2.“大变”时：因使用新技术导致主要服务内容发生重大变更（如核心算法升级、新增虚拟恋爱功能），变更后必须评估。3.“做大”时：用户规模达到注册用户100万或月活用户10万的门槛，达标后必须评估。这体现了“规模越大，责任越大，监管越严”的逻辑。4.“出险”时：服务存在影响国家安全或公共利益的风险，或发生安全事件、被监管通报，必须进行专项评估。

评估重点：包括用户规模与结构、高风险识别处置情况、用户投诉，以及本办法各项规定的执行情况等。欧盟《人工智能法案》要求高风险AI系统通过第三方强制评估，我国则采取了 “自主或委托评估+监管审查”的模式，兼顾了效率与力度。

九、算法备案、合规审计与持续监管如何协同推进？

这三者构成了对拟人化服务“事前备案、事中审计、事后监管”的全链条、闭环式监管路径。

- 算法备案（事前准入）：提供拟人化服务的算法属于“具有舆论属性或社会动员能力的算法”，企业必须在服务上线后10个工作日内完成备案，公开算法基本原理、机制等。这是合法运营的起点。
- 合规审计（事中体检）：企业每年必须对服务的合规情况进行审计，形成报告。其中，处理未成年人个人信息的合规情况必须进行专项审计，不得与一般审计合并。
- 持续监管（事后监督）：网信部门每年会对企业的安全评估报告和审计报告进行书面审查，并可能进行现场检查。对于发现的问题，可以约谈、责令整改，直至暂停服务。

我国对人工智能拟人化互动服务构建的“备案－审计－监管”治理体系，是一个环环相扣、紧密联动的动态监管闭环。在这一体系中，服务提供者的算法备案是启动一切监管流程的基础和前提，未完成备案则后续的审计与监管将缺乏合法的监管对象与抓手。在此基础上，由企业自行或委托进行的年度合规审计，构成了监管持续发力的核心依据；网信部门在对算法备案进行年度复审时，正是以该审计报告为关键依据，来评判服务运行的合规性与风险状况。最后，强有力的行政监管是确保整个机制不流于形式的根本保障，监管部门通过主动的现场检查、情况核实等

手段，确保备案信息的真实性、审计工作的严肃性以及发现问题的整改实效。

十、应用商店、平台方与第三方在拟人化互动服务中的合规责任如何划分？

新规明确了全链条责任，防止出现“平台只管上架，出事只找开发”的责任真空。

（一）应用程序分发平台（如苹果App Store、安卓商店）：“守门人”责任

- 上架前审核：必须核验应用的算法备案证明、安全评估报告（如需）、未成年人模式等是否齐全有效。这与欧盟要求应用商店对高风险AI应用履行审核义务的方向一致。
- 上架后处置：发现应用违规，必须采取警示、暂停服务、下架等措施。如果明知违规仍予上架或拒不处置，需与运营者承担连带责任。

（二）服务提供者（企业或个人）：“第一责任人”
提供者是合规的终极责任主体，需承担所有前述义务，并对违规后果负主要责任。

（三）第三方（如算法/数据供应商）：“合规风险传导点”

责任定位：新规未将其直接列为监管对象或责任方，但通过服务提供者的法定义务实现了风险的向上游传导。
由于服务提供者必须履行“数据来源合法”等义务，若因第三方产品导致违规，提供者将首先被追责。这倒逼提供者必须在商业合作中，通过合同等方式对第三方进行严格的合规审查与管理。在此过程中，第三方也可能依据其他民事法律承担相应责任。

十一、结语

《人工智能拟人化互动服务管理暂行办法（征求意见稿）》的出台，标志着我国AI监管进入了聚焦情感交互风险、强化人文关怀的新阶段。

与国际上“完全禁止”或“设定高标准”的路径不同，我国新规采取了“管控与创新” 的新思路。其最显著的突破在于，将对未成年人和老年人的保护，从传统的“数据安全”层面，深刻提升至“人身安全与心理健康”的维度，为企业设定了积极干预的法定义务。

与此同时，新规通过构建“备案—审计—监管”的闭环，以及明确应用商店的“守门人”责任，旨在实现覆盖全产业链的责任传导，防止出现监管真空。

法律的生命力在于执行。“未成年人模式”的有效性、“沉迷”标准的科学性，仍需在实践探索中不断优化。而这份《征求意见稿》更像是一份面向未来的责任契约，它要求技术创新必须内嵌安全与伦理，也预示着中国的AI产业正在迈向一个更加成熟的新阶段。

注：

【1】《网络数据安全管理条例》（国务院令第七百九十号）第三方产品和服务提供者违反法律、行政法规的规定或者平台规则、合同约定开展网络数据处理活动，对用户造成损害的，网络平台服务提供者、第三方产品和服务提供者、预装应用程序的智能终端等设备生产者应当依法承担相应责任。

【2】《网络数据安全管理条例（征求意见稿）》第二十条第二款 个人信息处理规则应当包括但不限于以下内容：（一）依据产品或者服务的功能明确所需的个人信息，以清单形式列明每项功能处理个人信息的目的、用途、方式、种类、频次或者时机、保存地点等，以及拒绝处理个人信息对个人的影响……

【3】《网络数据安全管理条例》第二十条第二款 网络数据处理者按照前款规定向个人告知收集和向其他网络数据处理者提供个人信息的目的、方式、种类以及网络数据接收方信息的，应当以清单等形式予以列明。网络数据处理者处理不满十四周岁未成年人个人信息的，还应当制定专门的个人信息处理规则。

【4】数智合规宋律师：《关于<互联网应用程序个人信息收集使用规定（征求意见稿）>的十一条不成熟修改建议》。

【5】App治理工作组：《观察 | App账号注销设置条件的合理性边界在哪？（三）》。

【6】同脚注5。

【7】 彭林海、王远哲：《强化个人信息保护 司法护航网络空间——北京四中院通报个人信息保护类案件审判情况及典型案例》。

【8】《规定（征求意见稿）》第七条 互联网应用程序收集使用个人信息应当遵循公开、透明原则，制定公开个人信息收集使用规则，通过清晰易懂的语言真实、准确、完整、逐项列明下列事项：……（三）嵌入软件开发工具包的，应当以结构化清单形式列明嵌入的软件开发工具包名称（包名）、版本、主要功能、运营者名称或者姓名、收集使用个人信息的种类和完整的软件开发工具包个人信息收集使用规则链接……

设计理念——数字之蓝与科技之银的智识交响

本手册色彩设计以浩天研究院“七彩祥云”中的以“星空蓝”为核心视觉语言，构建出深邃而富有层次感的数字法治视觉体系。这一色彩不仅承载着法律传统的理性精神，更蕴含着数字时代的前瞻视野，完美诠释了技术规制与法律智慧的交融境界。

星空蓝，取意于宇宙天幕的深邃与秩序——沉静、浩瀚而富有结构感。这抹蓝既是数据宇宙的底色，也是法律理性的视觉化身。它既象征着法律体系在数字浪潮中保持的恒定与包容，又暗含“秩序之中见自由”的治理智慧。星空之蓝，不囿于传统法理的厚重，而更具开放系统中的稳定特质，代表着数字时代法律规范的结构性、网络性与演进性。它如星空坐标般为智能社会的法律探索提供理性而开放的认知框架。

数字时代的法律研究既需要星空般的系统视野，也需要星座般的路径指引。星空蓝所构建的视觉体系，既呈现了数字法治的宏大格局与深层结构，又明晰了合规实践的具体坐标与行进方向。

这种色彩语言呼应了《数智通鉴》的学术追求：在浩瀚的数字星空中，以法律为坐标，以合规为航图，为技术创新划定清晰的运行轨道，为数字发展提供稳定的制度保障。星空蓝所承载的，既是法律人对传统法理的坚守，也是对数字未来的理性期待。


浩天律师事务所
HYLANDS LAW FIRM

浩天律师事务所

抱/朴/守/正　至/诚/四/达

北京浩天律师事务所

- 地址：北京市朝阳区东三环中路5号财富金融中心3、11、12层
- 电话：+86 10 65028888
- 邮编：100020

北京浩天（上海）律师事务所

- 地址：上海市黄浦区中山东二路600号外滩金融中心(BFC)S1栋11层、12层
- 电话：+86 21 6887 1787/5068 0028
- 邮编：200010

关注浩天法律评论
了解更多浩天信息

关注浩天研究院
了解更多行业研究