

ICS
CCS A 00

团 体 标 准

T/CECC XXXX—XXXX

生成式人工智能知识产权指南

Intellectual Property Guide for Generative Artificial Intelligence

工作组修订稿

【标准三稿完成时间：2025 年 06 月】

XXXX- XX -XX 发布

XXXX- XX-XX 实施

中 国 电 子 商 会 发 布

目 次

前 言	III
引 言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 生成式人工智能著作权合规指南	4
4.1 生成式人工智能大模型开发者的著作权合规要点	4
4.1.1 训练数据收集阶段	4
4.1.2 生成式人工智能大模型开发阶段	4
4.1.3 生成式人工智能大模型发布阶段	4
4.2 生成式人工智能服务提供者的著作权合规要点	5
4.2.1 集成大模型阶段	5
4.2.2 提供服务阶段	5
4.3 生成式人工智能服务使用者的著作权合规要点	5
5 生成式人工智能专利指南	5
5.1 生成式人工智能场景下的专利权取得	6
5.1.1 概述	6
5.1.2 原始取得	6
5.1.3 继受取得	7
5.2 生成式人工智能场景下的专利运营	8
5.2.1 概述	8
5.2.2 专利运营对象管理	8
5.2.3 专利运营方式管理	8
6 生成式人工智能商业标识合规指南	8
6.1 生成式人工智能场景下商业标识的保护对象	8
6.2 生成式人工智能场景下商标和装潢管理	8
6.2.1 标识构成	9
6.2.2 合法性审查	9
6.2.3 真实性审查	9
6.2.4 显著性审查	9
6.2.5 侵权风险审查	9
6.2.6 商标布局	9
6.2.7 商标使用	9
6.3 生成式人工智能场景下显式标识和隐式标识管理	9
6.3.1 标识要求	9
6.3.2 显式标识	9

- 6.3.3 隐式标识 11
- 7 生成式人工智能商业秘密合规指南 11
 - 7.1 生成式人工智能场景下商业秘密的对象 11
 - 7.1.1 涉及生成式人工智能的技术信息 11
 - 7.1.2 涉及生成式人工智能的经营信息 12
 - 7.2 对商业秘密采取的保护措施 12
 - 7.2.1 生成式人工智能大模型开发者的保护措施 12
 - 7.2.2 生成式人工智能服务提供者的保护措施 12
 - 7.2.3 生成式人工智能服务使用者的保护措施 12
 - 7.3 侵害商业秘密场景下的救济措施 12
 - 7.3.1 应急处置 12
 - 7.3.2 证据收集 12
- 8 生成式人工智能场景下的知识产权争议处理 12
 - 8.1 概述 12
 - 8.2 侵权风险防范及应急措施 13
 - 8.2.1 侵权风险防范 13
 - 8.2.2 应急措施 13
 - 8.3 维权 13
 - 8.3.1 侵权评估 13
 - 8.3.2 维权途径——多元纠纷解决机制 13
 - 8.3.3 确定维权方案 14
- 参 考 文 献 15

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由中国电子商会提出并归口。

本文件起草单位：XXXX。

本文件主要起草人：XXXX。

引 言

为应对生成式人工智能带来的知识产权挑战，促进生成式人工智能产业健康发展，引导建议生成式人工智能的应用，使其符合知识产权合规要求，根据《中华人民共和国著作权法》《中华人民共和国专利法》《中华人民共和国商标法》《中华人民共和国反不正当竞争法》《中华人民共和国个人信息保护法》等法律法规，以及《生成式人工智能服务管理暂行办法》和《互联网信息服务深度合成管理规定》等相关部门规章，结合我国生成式人工智能技术和产业发展的实际情况，制定本文件。

生成式人工智能知识产权指南

1 范围

本文件规定了生成式人工智能技术及其应用场景中知识产权管理的基本要求，涵盖著作权、专利、商业标识和商业秘密等方面的获取、保护、应用和风险管理方法。

本文件适用于指导生成式人工智能大模型开发者、生成式人工智能服务提供者、生成式人工智能使用者，面向中华人民共和国境内，使用和提供生成式人工智能产品及内容时，所需要开展的知识产权工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 5271.1-2000 信息技术 词汇 第1部分基本术语
- GB/T 21374-2008 知识产权文献与信息 基本词汇
- GB/T 33251-2016 高等学校知识产权管理规范
- GB/T 35273-2020 信息安全技术 个人信息安全规范
- GB/T 39551-2020 专利导航指南
- GB/T 41867-2022 信息技术 人工智能 术语
- DB31-120/Z 011—2024 企业商业秘密管理规范
- DB46/T 584-2023 商业秘密保护管理规范
- T/CECC 027-2024 生成式人工智能数据应用合规指南
- TC260-003 生成式人工智能服务安全基本要求
- T/PPAC 701-2021 企业商业秘密管理规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

人工智能 artificial intelligence; AI

〈学科〉人工智能系统（3.2）相关机制和应用的研究和开发。

[来源：GB/T 41867-2022，定义 3.1.2]

3.2

生成式人工智能 generative artificial intelligence

具有文本、图片、音频、视频等内容生成能力的模型及相关技术。

3.3

生成式人工智能服务 generative artificial intelligence service

利用生成式人工智能技术向公众提供生成文本、图片、音频、视频等服务。

3.4

生成式人工智能大模型开发者 generative artificial intelligence large model developer

提供通过训练大量数据得到的、用于普适性目标、可优化适配多种下游任务的深度神经网络模型的主体，简称为模型开发者。

3.5

生成式人工智能服务提供者 generative artificial intelligence service provider

利用生成式人工智能技术提供生成式人工智能服务（包括通过提供可编程接口等方式提供生成式人工智能服务）的组织、个人。

3.6

生成式人工智能服务使用者 generative artificial intelligence service user

使用生成式人工智能服务生成内容的组织、个人。

3.7

训练数据 training data

所有直接作为模型训练输入的数据，包括预训练、优化训练过程中的输入数据。

3.8

机器学习 machine learning

通过计算技术优化模型参数的过程，使模型的行为反映数据或经验。

3.9

机器学习算法 machine learning algorithm

依据给定的准则，根据数据确定机器学习模型参数的算法。

3.10

透明性 transparency

人工智能系统与利益相关方交流关于该系统适当信息的特性。

3.11

数据的预训练 data pre-training

使用大规模数据使生成式人工智能获得通用知识的训练过程。

3.12

优化训练 fine-training

使用专门领域数据使生成式人工智能获得一定面向领域服务能力的训练过程。

3.13

生成式人工智能提示词 generative artificial intelligence prompt

在与生成式人工智能进行交互时，用户输入的文本提示，用于引导生成特定的输出。

3.14

创新主体 entity of innovation

从事科技创新活动，并拥有或管理知识产权的组织或个人，包括企业、高校、科研院所等。依据其在产业链中的角色分工、法律责任以及监管要求，分为生成式人工智能大模型开发者、生成式人工智能服务提供者以及生成式人工智能服务使用者。

3.15

专利挖掘 patent mining

在技术研发或产品开发中，对创新主体所取得的技术成果从技术和法律层面进行剖析、整理、拆分和筛选，从而确定用以申请专利的创新点和技术方案。

3.16

专利布局 patent layout

对专利申请时间、地域和途径的选择、专利保护内容的谋划等，对专利申请工作的周密规划和统筹安排，对专利进行有机结合，构建严密高效的专利保护网，形成对创新主体有利的专利格局，是专利挖掘的进一步延伸。

3.17

专利导航 patent navigation

是在宏观决策、产业规划、企业经营和创新活动中，以专利数据为核心深度融合各类数据资源，全景式分析区域发展定位、产业竞争格局、企业经营决策和技术创新方向，服务创新资源有效配置，提高决策精准度和科学性的新型专利信息应用模式。

3.18

显式标识 explicit identification

用于提示用户当前内容由人工智能生成合成的用户可直接感知的信息。

3.19

隐式标识 implicit identification

用于记录生成合成内容，用户不能直接感知且不影响用户正常使用，但通过技术手段能从内容中提取的信息。

3.20

商业秘密 trade secrets

不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

[来源：DB46/T 584-2023，定义3.1]

注：“不为公众所知悉”、“具有商业价值”和“相应保密措施”的具体内容见《中华人民共和国反不正当竞争法》及最高人民法院发布的有关司法解释。

3.21

技术信息 technical information

与技术有关的结构、原料、组分、配方、材料、样品、样式、植物新品种繁殖材料、工艺、方法或其步骤、算法、数据、计算机程序及其有关文档等信息。

3.22

经营信息 commercial information

与经营活动有关的创意、管理、销售、财务、计划、样本、招投标材料、客户信息、数据等信息。

3.23

保密措施 confidentiality measures

商业秘密权利人为防止商业秘密泄露，在被诉侵权行为发生以前所采取的合理保密措施。

3.24

商业价值 commercial value

商业秘密具有的因不为公众所知悉而具有现实的或者潜在的商业价值。

3. 25

装潢 trade dress

用于识别与美化人工智能终端产品而附加其上的文字、图案、色彩及其排列组合。

3. 26

商标 trademark

用于区分人工智能生成物来源的，由文字、图形、颜色、三维标志、声音或其组合而成的标识。

4 生成式人工智能著作权合规指南

4. 1 生成式人工智能大模型开发者的著作权合规要点

4. 1. 1 训练数据收集阶段

相关要求如下：

- a) 应通过合法的来源，收集或采购数据进行训练：
 - 使用开源训练数据时，宜审核并遵循该数据来源的开源许可协议或相关授权文件；
 - 使用自采训练数据时，宜具有采集记录，不宜采集他人已明确不可采集的数据；
 - 使用商业采购训练数据时，宜具有法律效力的交易合同和协议等。交易方或合作方不能提供数据来源的著作权合规承诺或相关证明材料的，不宜使用该数据。
- b) 应通过合法手段收集数据，不可违反爬虫协议、或破解对方的账号密码等妨碍正常业务运营的技术手段收集数据；
- c) 宜采用合法数据进行训练，不宜使用侵害他人著作权的数据进行训练。

4. 1. 2 生成式人工智能大模型开发阶段

相关要求如下：

- a) 应采取措施防控生成物的侵权风险：宜采用技术手段，防止输出与著作权法保护的学习对象实质性相似的生成物；
- b) 训练数据来源可追溯：应对训练数据的来源及训练过程进行留痕记录；
- c) 使用开源代码的，宜对拟采用的开源代码的开源协议条款事先进行审核，并遵循开源协议约定的条件进行使用。

4. 1. 3 生成式人工智能大模型发布阶段

相关要求如下：

- a) 布放用户协议、履行告知义务：开发者宜通过用户协议，向使用者充分告知可能存在的著作权风险，并与使用者约定相关责任和义务；
- b) 建立侵权投诉及举报渠道：开发者应建立著作权投诉途径、投诉机制和反馈方式、以供使用者投诉，并积极响应使用者的投诉、采取应对措施。如发现存在侵犯著作权等情况，应当采取必要措施，如停止生成、停止传输、消除等；
- c) 保持模型透明度：开发者宜向利益相关方提供模型的基本信息、训练数据的来源及内容、为防止侵犯著作权风险所采取的措施等；
- d) 内容标识功能要求：生成式人工智能大模型开发者应当设计并提供标识功能，确保生成式人工智能服务提供者及其服务使用者，能够在生成内容的合理位置、区域、对可能导致公众混淆或者误认的人工智能合成生成内容，进行显著标识，如采用水印等；
- e) 主动进行侵权风险评估：开发者宜对生成内容主动进行侵权风险评估，预防性地采取措施降低侵害著作权风险。

4.2 生成式人工智能服务提供者的著作权合规要点

4.2.1 集成大模型阶段

相关要求如下：

- a) 宜对集成的大模型进行合规性审查：服务提供者宜采用已备案大模型，并对集成的大模型进行著作权合规性审查，以控制侵权风险；如大模型为提供具有舆论属性或者社会动员能力的生成式人工智能服务的，服务提供者应采用已开展安全评估并已备案的大模型；
- b) 宜对生成物的侵权风险进行防控：服务提供者可采用技术手段，防止输出与著作权法保护的学习对象构成实质性相似的生成物，如屏蔽关键词等；
- c) 宜对使用者输入信息进行监测，并在使用者连续输入或一天内累计输入违法信息达到一定次数时，采取暂停服务等处置措施；
- d) 使用开源代码的，宜对拟采用的开源代码的开源协议条款事先进行审核，并遵循开源协议约定的条件进行使用。

4.2.2 提供服务阶段

相关要求如下：

- a) 布放用户协议、履行告知义务：服务提供者宜在用户协议中，充分告知用户可能存在的潜在侵害著作权的风险，积极引导用户在尊重著作权的前提下使用服务，明示对使用者输入信息进行监测的规则、及用户违反规则时采取的处置措施；
- b) 建立侵权投诉及举报渠道：服务提供者应建立便捷的著作权投诉途径、投诉机制和反馈方式，积极响应用户对侵害著作权的投诉，并采取对应措施，如在产品用户界面上设置投诉途径。如发现存在侵犯著作权等情况，应当采取必要措施，如停止生成、停止传输、消除等；
- c) 透明度：服务提供者宜向其用户提供所集成的大模型的基本信息、所提供的服务技术内容、以及为防止侵权采取的措施，以增强透明度；
- d) 内容标识：应在生成内容的合理位置、区域、对可能导致公众混淆或者误认的人工智能合成生成内容，进行显著标识，如采用水印技术等；
- e) 主动进行侵权风险评估：服务提供者宜对生成内容进行侵权风险评估，预防性地采取措施降低风险；
- f) 使用开源代码的，宜对拟采用的开源代码的开源协议条款事先进行审核，并遵循开源协议约定的条件进行使用；
- g) 提供网络信息内容传播服务的服务提供者，应提供必要的标识功能，并提醒用户主动声明发布内容中是否包含生成合成内容。

4.3 生成式人工智能服务使用者的著作权合规要点

相关要求如下：

- a) 服务使用者在使用生成式人工智能服务前，宜主动确认要使用的生成式人工智能服务的基本信息，以控制侵害著作权的潜在风险，如用户协议、使用规则、知识产权条款、技术方案、训练数据来源等相关信息；
- b) 服务使用者宜对使用生成式人工智能时，对输入的生成式人工智能提示词、生成物底稿、生成过程进行留痕记录，确保有迹可查；
- c) 服务使用者宜对生成物是否侵害他人著作权，主动进行风险评估，如核查输入的生成式人工智能提示词中是否具有侵害著作权的内容等；
- d) 服务使用者宜积极采取措施，控制侵权风险。如：建立公司内部使用生成式人工智能的合规制度、健全公司内部使用生成式人工智能的流程、对员工进行使用生成式人工智能场景下著作权合规培训等。发现侵权情况的，应采取停止传播、删除等措施；
- e) 服务使用者使用生成式人工智能服务时，应通过服务提供者提供的标识功能，在生成内容的合理位置、区域、对可能导致公众混淆或者误认的人工智能合成生成内容，进行显著标识，如采用水印技术等。

5 生成式人工智能专利指南

5.1 生成式人工智能场景下的专利权取得

5.1.1 概述

创新主体应根据自身发展状况选择合适的方式来获取专利权，包括原始取得和继受取得。

5.1.2 原始取得

5.1.2.1 专利挖掘

生成式人工智能产业链，一般可分为三层，上游为基础层，中游为模型层，下游为应用层，如图1所示。

在技术图谱层面，将生成式人工智能技术划分为七个技术层级，其中：

- a) 基础层涉及底层技术，包括训练数据的采集和算力的提供；
- b) 模型层涉及模型训练框架、算法、模型架构、模型训练、模型监督微调、模型蒸馏、通用大模型/垂直域大模型相关技术；
- c) 应用层包括功能应用（模型功能）和产业应用。其中，语音识别、自然语言处理、智能感知领域等，可纳入功能应用范畴；金融领域、智慧医疗等，可纳入产业应用范畴。

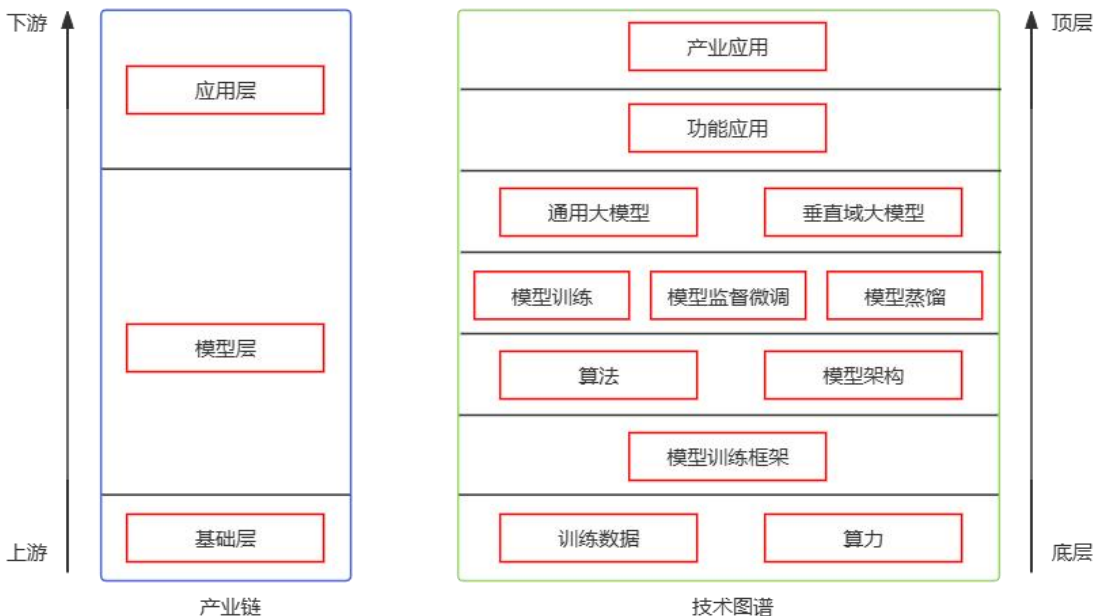


图1 生成式人工智能产业链与技术图谱的对应关系

实施专利挖掘的主体应：

- a) 从技术层面进行定位及开展挖掘：
 - (1) 基于创新主体在生成式人工智能产业链中的位置，定位自身技术在生成式人工智能技术图谱中所处的层级；
 - (2) 基于所定位的技术层级，首先梳理本层级的技术相关成果（技术改进点方案）和非技术相关成果；进一步梳理本层级技术改进引起的其它层级的技术相关成果和非技术相关成果，其中，非技术相关成果，一般包括对生成式人工智能模型进行训练过程中所产生的元数据、配置文件等。
- b) 从法律层面进行客体筛选：
 - (1) 按照现有知识产权法律法规所规定的客体，初步筛选出可能采用专利方式进行保护的成果及明显不适合采用专利方式保护的成果，对于明显不适合采用专利方式保护的成果，考虑采用其它合适的方式进行保护，以获得成果的多重保护，例如数据以商业秘密、著作权或其他方式进行知识产权保护；

(2) 按照现有《专利法》《专利法实施细则》及《专利审查指南》规定的客体，从可能使用专利方式进行保护的成果中进一步筛选，得到符合可专利客体的技术方案，针对生成式人工智能相关成果，可按照如下先后顺序进行判断：《专利法》第五条一款、第二十五条一款二项、第二十五条一款三项（对于生成式人工智能应用于医疗领域，需要特别关注）、第二条二款的规定。

- c) 初步判断符合可专利客体的方案是否满足《专利法》第二十二条二款关于新颖性、第二十二条三款关于创造性、第二十二条四款关于实用性以及第二十六条三款关于公开充分的规定，满足这些条款的方案构成可专利方案；
- d) 基于可专利方案完成交底书的撰写。

5.1.2.2 专利布局

实施专利布局的主体应：

- a) 明确专利布局整体目标，是保护自身技术还是对抗竞争对手：
 - (1) 保护式布局：围绕创新主体自身技术创新展开；
 - (2) 对抗式布局：针对竞争对手的专利，进行对抗式布局。

注：目前生成式人工智能领域专利纠纷尚不多见，创新主体多以保护式布局为主。
- b) 注重时间、地域和时机的把握：
 - (1) 对于创新主体产生的有价值的技术构思，尽快申请专利，避免出现产品或服务推出后才申请专利的情况；
 - (2) 基于技术因素和市场因素确定境外布局的地域；
 - (3) 确定境外布局的途径，包括直接申请途径、巴黎公约途径和PCT申请途径。创新主体需要特别注意的是，根据我国《专利法》的规定，任何单位或者个人将在中国完成的发明或者实用新型向外国申请专利的，应当事先报经国务院专利行政部门进行保密审查。

5.1.2.3 专利导航

实施专利导航的主体应：

- a) 通过企业经营类专利导航，指引企业的创新发展决策；
- b) 通过创新发展决策，进一步指导专利挖掘、专利布局工作，从而培育高价值专利。

5.1.2.4 专利申请

实施专利申请的主体应：

- a) 针对交底书记载的方案是否存在客体问题进行复核；
- b) 针对交底书记载的方案是否满足《专利法》第二十六条三款关于公开充分的规定进行复核；
- c) 针对交底书记载的方案是否满足《专利法》第二十二条二款关于新颖性、第二十二条三款关于创造性的规定进行检索；

注：在申请专利之前，大模型相关算法的投稿甚至在 arXiv 上的预公开构成专利法意义上的“公开”，可能影响新颖性，注意各个国家或地区对于宽限期的规定。
- d) 依照《专利法》《专利法实施细则》《专利审查指南》以及《人工智能相关发明专利申请指引（试行）》进行专利文件的撰写及审查意见的答复，以获得授权，并且在撰写专利文件时应考虑与商业秘密的协调保护。

5.1.3 继受取得

专利的受让人、承继人或被许可人应：

- a) 核查专利的有效性和合法性；
- b) 在转让/许可书面合同中明确约定：
 - (1) 专利基本信息，包括专利名称、专利号、专利类型、专利申请日和授权日等内容；
 - (2) 专利持有者、受让人、被许可人信息；
 - (3) 转让/许可权利范围、许可类型、许可实施范围包括实施方式、地域、期限等内容；
 - (4) 转让/许可费用及支付方式；

- (5) 技术资料清单交付的时间、地点、方式；
- (6) 专利稳定性条款；
- (7) 侵权纠纷处理方式及责任承担条款；
- (8) 后续改进的技术成果的归属与利用；
- (9) 涉及商业秘密和技术信息的，约定保密措施。
- c) 对于转让书面合同，向国家知识产权局登记，专利申请权或者专利权的转让自登记之日起生效；
- d) 对于许可书面合同，自合同生效之日起 3 个月内向国家知识产权局备案。

5.2 生成式人工智能场景下的专利运营

5.2.1 概述

创新主体应建立专利运营对象管理制度以及专利运营方式管理制度，并据此开展专利运营工作。

5.2.2 专利运营对象管理

随着创新主体的专利数量达到一定规模，创新主体应对专利进行分类分级管理，包括：

- a) 分类管理：可根据生成式人工智能行业特点，建立产品和技术的多层级分类体系。分类体系可以按照产品、技术或《国际专利分类表》等标准分别或合并建立；
- b) 分级管理：
 - (1) 可根据生成式人工智能行业特点，建立产品和技术的多层级分级体系。分级体系可以按照专利价值等标准建立。专利的级别以三至五级为宜；
 - (2) 对不同级别的专利进行差异化管理，护航高价值专利，例如可将专利分为战略性专利、基础性专利、改进型专利、一般专利等。

5.2.3 专利运营方式管理

5.2.3.1 专利运营方式的选择

创新主体可以结合自身情况对专利运营方式进行自主选择，包括但不限于：自行实施、许可（包括开放许可）、转让、投融资、作价入股、联合多个创新主体组建专利池、交叉许可、合作开发、维权等。

创新主体宜结合自身专利分类分级标准和/或专利所处的技术层级对运营方式进行选择。

对于许可、转让，应当设定哪些类别和级别的专利可以许可或者转让，并进一步细分许可的类型，例如独占、排他或者普通许可。

对于模型层，存在很多开源、开放大模型，对于相关专利可以考虑采用开放许可方式进行专利运营。

5.2.3.2 具体运营方式中的注意事项

要求如下：

- a) 对于许可和转让，创新主体可参见 5.1.3；
- b) 对于生成式人工智能领域进行融资，创新主体应注意：需要引进外商投资生成式人工智能服务的，应当符合外商投资相关法律、行政法规的规定；
- c) 对于生成式人工智能领域进行投资，创新主体应注意：考虑国家安全及技术出口限制或禁止的规定，在相关交易谈判及交易交割安排中提前做好准备，《中国禁止出口限制出口技术目录》涵盖部分人工智能算法成果，涉及该等技术的对外交流和交易可能受到限制；
- d) 对于联合多个创新主体组建专利池，创新主体应注意：专利筛选与评估、利益分配机制、管理与运营、反垄断合规等方面；
- e) 对于合作开发，创新主体应注意：合作合同签订、知识产权归属、保密措施等方面。

6 生成式人工智能商业标识合规指南

6.1 生成式人工智能场景下商业标识的保护对象

生成式人工智能场景下商业标识的保护对象，一般包括装潢、商标、显式标识、隐式标识等。

6.2 生成式人工智能场景下商标和装潢管理

6.2.1 标识构成

可将文字、图形、三维标志、声音及其组合等作为商标申请注册，确保相关标识在多个维度上得到保护。

6.2.2 合法性审查

商标和装潢应符合法律规定、社会公德和善良风俗。

6.2.3 真实性审查

人工智能终端产品的商标和装潢不得包含虚假或误导性内容，以防对消费者造成欺骗。

6.2.4 显著性审查

商标和装潢宜具有显著性，以便于消费者区分商品或服务的来源。

不宜将含有AI、生成式预训练变换器（GPT）等人工智能领域的通用术语或名称的标识作为商标注册使用，避免商标缺乏显著性。

6.2.5 侵权风险审查

商标和装潢不得侵犯他人姓名权、肖像权、著作权、商标权、专利权、商品化权益等在先权利或在先权益。若系基于现实人物或在先角色形象、声音或他人享有合法权利的标识创建，应取得相应的授权。

6.2.6 商标布局

6.2.6.1 商品/服务

企业可根据其技术应用场景在第9类和第42类“计算机软件”“软件开发”“数据处理”“云计算服务”等核心商品和服务注册商标，亦可根据自身商业发展规划可同时选择相关类别进行商标布局。

6.2.6.2 地域

企业可根据其发展战略提前在目标国家或地区开展商标布局，防止遭受海外抢注。在此基础上建立全球商标监控系统，及时发现并应对商标抢注和侵权行为，积极开展海外维权。

6.2.7 商标使用

确保对注册商标进行真实、持续、合法、有效的商业性使用，避免自行改变注册商标或超出核定范围使用注册商标。

做好商标的跟踪管理，防止商标退化为与人工智能相关的通用术语或名称。

6.3 生成式人工智能场景下显式标识和隐式标识管理

6.3.1 标识要求

人工智能生成内容应根据相关法律规定依法添加显式标识或隐式标识。

6.3.2 显式标识

6.3.2.1 实现方式

显式标识的实现方式主要包括针对文本、图片、音频、视频内容的显式标识以及交互场景界面显式标识。

6.3.2.2 文本内容显式标识

文本内容显式标识方法如下：

- a) 文本内容显式标识应采用文字或角标形式；
- b) 文字形式的文本内容显式标识应同时包含以下要素：
 - (1) 人工智能要素：包含“人工智能”或“AI”，表明使用人工智能技术；
 - (2) 生成合成要素：包含“生成”和/或“合成”，表明内容制作方式为生成和/或合成。
- c) 角标形式的文本内容显式标识应包含“AI”；

- d) 文本内容显式标识应位于以下一个或多个位置：
 - (1) 文本的起始位置；
 - (2) 文本的末尾位置；
 - (3) 文本的中间适当位置。
- e) 文本内容显式标识使用的字型 and 颜色应清晰可辨。

6.3.2.3 图片内容显式标识

图片内容显式标识方法如下：

- a) 图片内容显式标识应采用文字提示；
- b) 图片内容显式标识应同时包含以下要素：
 - (1) 人工智能要素：包含“人工智能”或“AI”，表明使用人工智能技术；
 - (2) 生成合成要素：包含“生成”和/或“合成”，表明内容制作方式为生成和/或合成。
- c) 图片内容显式标识应位于图片的边或角；
- d) 图片内容显式标识使用的字型应清晰可辨；
- e) 图片内容显式标识的文字高度应不低于画面最短边长度的 5%。

6.3.2.4 音频内容显式标识

音频内容显式标识方法如下：

- a) 音频内容显式标识应采用语音标识或音频节奏标识；
- b) 语音标识应同时包含以下要素：
 - (1) 人工智能要素：包含“人工智能”或“AI”，表明使用人工智能技术；
 - (2) 生成合成要素：包含“生成”和/或“合成”，表明内容制作方式为生成和/或合成。
- c) 音频节奏标识应为“短长 短短”的节奏；
- d) 音频内容显式标识应位于以下一个或多个位置：
 - (1) 音频的起始位置；
 - (2) 音频的末尾位置；
 - (3) 音频的中间适当位置。
- e) 语音标识应使用正常语速。

6.3.2.5 视频内容显式标识

视频内容显式标识方法如下：

- a) 视频内容显式标识应采用文字提示；
- b) 视频内容显式标识应同时包含以下要素：
 - (1) 人工智能要素：包含“人工智能”或“AI”，表明使用人工智能技术；
 - (2) 生成合成要素：包含“生成”和/或“合成”，表明内容制作方式为生成和/或合成。
- c) 视频内容显式标识应位于视频起始画面，可位于视频末尾和中间适当位置；
- d) 视频内容显式标识应位于视频画面的边或角；
- e) 视频内容显式标识使用的字型应清晰可辨；
- f) 视频内容显式标识的文字高度应不低于画面最短边长度的 5%。

6.3.2.6 交互场景界面显式标识

交互场景界面显式标识方法如下：

- a) 交互场景界面显式标识应采用文字提示；
- b) 交互场景界面显式标识使用的字型和颜色应清晰可辨；
- c) 交互场景界面显式标识应同时包含以下要素：
 - (1) 人工智能要素：包含“人工智能”或“AI”，表明使用人工智能技术；
 - (2) 生成合成要素：包含“生成”和/或“合成”，表明内容制作方式为生成和/或合成。
- d) 内容周边显式标识应采取以下一种或多种方式：
 - (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。

- e) 非内容周边显式标识应采取以下一种或多种方式：
 - (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。

6.3.3 隐式标识

6.3.3.1 实现方式

隐式标识的实现方式主要包括元数据隐式标识和内容隐式标识。

6.3.3.2 元数据隐式标识

元数据隐式标识应包括以下要素：

- a) 生成合成标签要素：内容的人工智能生成合成属性信息，包括确定、可能、疑似；
- b) 生成合成服务提供者要素：生成合成服务提供者的名称或编码；
- c) 内容制作编号要素：生成合成服务提供者对该内容的唯一编号；
- d) 内容传播服务提供者要素：内容传播服务提供者的名称或编码；
- e) 内容传播编号要素：内容传播服务提供者对该内容的唯一编号。

6.3.3.3 内容隐式标识

人工智能生成合成内容中添加的隐式标识通常为数字水印标识。

数字水印宜明确使用场景(考虑实时性需求、水印嵌入强度限制、提取准确率需求、嵌入位置评估等)、待嵌入信息及载体的基本特性(载体类型、载体结构、内容编码算法、封装格式、空域尺度信息、时序尺度信息等)，评估对应场景下潜在的失真干扰与水印攻击(压缩、裁剪、涂抹、调色、模糊等)，根据前述评估结果对水印嵌入、编码算法进行选型、调参与细节设计。

数字水印在实施过程中宜考虑不可感知性、稳定性、水印容量、可检测性、安全性等基本要求，以及识读方式、防伪力度、识别率、使用环境、识读设备、防伪力度等附加要求，确保数字水印发挥溯源与知识产权保护作用。

7 生成式人工智能商业秘密合规指南

7.1 生成式人工智能场景下商业秘密的对象

7.1.1 涉及生成式人工智能的技术信息

7.1.1.1 数据

在生成式人工智能的研发、训练、运营等过程中，所涉及的具有商业价值且不为公众所知悉，并经权利人采取合理保密措施的数据集合，包括但不限于预训练数据、后训练数据、标注数据、权重数据、模型参数、模型代码等具有独特价值的原始数据及衍生数据等。

7.1.1.2 算法

在生成式人工智能的研发、训练、应用等过程中，所涉及的具有商业价值且不为公众所知悉，并经权利人采取合理保密措施的，用于实现数据处理、模型训练、内容生成等功能的计算步骤、规则和逻辑体系。

7.1.1.3 程序

在生成式人工智能的研发、训练、应用等过程中，为实现特定生成式人工智能相关功能而设计、开发的，由计算机指令、代码、数据结构以及相关文档等构成的，具有商业价值且不为公众所知悉，并经权利人采取合理保密措施的集合体。

7.1.1.4 涉及生成式人工智能的其他技术信息

其他符合商业秘密特征的具有保密性、商业价值并经权利人采取保密措施的材料，包括但不限于详细描述系统架构、工作原理、实现细节和使用方法的技术文档、业务流程、数据标注的规则和方法等。

7.1.2 涉及生成式人工智能的经营信息

生成式人工智能开发、运营管理、使用过程中形成的经营活动有关的创意、管理、销售、财务、计划、样本、招投标材料、客户信息、数据等信息。其中，客户信息包括客户的名称、地址、联系方式以及交易习惯、意向、内容等信息。

7.2 对商业秘密采取的保护措施

7.2.1 生成式人工智能大模型开发者的保护措施

7.2.1.1 使用开源软件工具、开源代码、开源模型等帮助开发的，宜事先评估后续开发中涉及商业秘密保护需求，提前了解开源许可证中对新开发软件、模型的开源要求。

7.2.1.2 对企业的特定数据、算法、程序等，宜采取适当的保密措施，如设立保密区域、设置不同密级并进行分别管理、限制访问范围、限制人员出入和访问、设置访问密码、定期评估与审计等。

7.2.1.3 宜与合作方及员工签订保密协议，着重明确商业秘密范围及保密责任。

7.2.1.4 宜建立企业内部商业秘密保护制度，加强秘密载体管理，注保密标识，保障物理载体安全。

7.2.1.5 宜完善人员管理与培训，落实涉密信息账号管理、处理留痕、使用审批等保护机制。

7.2.1.6 宜采用公证处、行业组织等第三方提供的商业秘密保护、存证平台，对商业秘密采取分发管理、协议签署、电子存证等措施。

7.2.2 生成式人工智能服务提供者的保护措施

7.2.2.1 生成式人工智能服务者在提供服务过程中如涉及开发活动的，相关商业秘密保护措施可参考7.1中的内容。

7.2.2.2 加强保密信息分区、分类、分级管理，使用第三方提供的云服务数据存储、管理技术时，企业宜做好合同审核，约定商业秘密范围，明确相关责任。

7.2.2.3 平衡履行算法解释义务与保护商业秘密两者间的关系，向用户履行算法解释义务时，宜事先充分告知用户保密条款和保密责任；向司法机关提供涉诉算法、程序相关核心内容作为证据时及时提出限制复制等保密请求，避免“二次泄露”等。

7.2.3 生成式人工智能服务使用者的保护措施

人工智能使用者在将相关信息输入生成式人工智能前，宜先行评估其中的涉密信息，提前对相关信息进行匿名化、脱敏化处理。

7.3 侵害商业秘密场景下的救济措施

7.3.1 应急处置

7.3.1.1 制定商业秘密泄密紧急处置预案，建立内部应对流程。

7.3.1.2 出现商业秘密泄露迹象时，及时启动对商业秘密泄露的内部调查取证、评估，查明原因，明确责任。

7.3.1.3 发现访问异常、账号异常等情况及时采取措施，对商业秘密泄露的危害进行控制，减少损失。

7.3.2 证据收集

发现商业秘密涉嫌被侵权时，应搜集并整理下列证据、材料：

- a) 企业是该商业秘密的权利人的证据，如：已采取的相应商业秘密保护措施、以及企业认为是商业秘密的书面证据和证实性材料；
- b) 企业商业秘密被侵犯的初步证据，如：涉嫌侵犯商业秘密的人员与企业的基本信息、相关保密协议与记录、涉嫌侵犯商业秘密的人员能够接触商业秘密的证据等；
- c) 该商业秘密被侵犯的事实，如：侵权行为具体表现（如披露、使用等）、以及企业所受的损失。

8 生成式人工智能场景下的知识产权争议处理

8.1 概述

生成式人工智能大模型开发者、生成式人工智能服务提供者以及生成式人工智能服务使用者应建立侵权风险防范及应急措施、维权措施，并据此开展知识产权争议处理工作。

8.2 侵权风险防范及应急措施

8.2.1 侵权风险防范

- a) 通用知识产权类型防范规则：应注意及时发现并防范侵权的情况，减少被诉风险；
- b) 针对侵害专利权风险防范规则：
 - (1) 开展预警工作：通过收集与分析相关技术领域的专利信息和国内外市场信息，基于图1所示的技术图谱进行专利分类，进而快速对标到创新主体自身产品所使用的技术，以便更有效地进行预警，预判可能产生的风险程度及对策措施；
 - (2) 开展专利侵权尽职调查：进行自由实施尽职调查时，应充分考虑到生成式人工智能技术复杂性、黑箱特性、侵权主体的多样性，防止遗留风险专利；
 - (3) 被诉侵权时的应对：尽快针对涉诉专利提起无效宣告请求。
- c) 针对侵害商标权风险防范规则：
 - (1) 建立监测机制：利用专业的商标监测工具或委托专业机构，对相关商标使用情况进行跟踪，及时发现可能的商标侵权行为；
 - (2) 关注商标动态：定期关注商标注册情况，及时发现他人申请注册与自身商标相同或近似的商标，并在法定期限内提出异议或无效宣告申请。
- d) 针对侵害商业秘密风险防范规则：
 - (1) 商业秘密泄密的预防：可采取保密教育、日常演练、检查监督、日常管理等保密措施，预防商业秘密泄露情况的发生；
 - (2) 对商业秘密采取保密措施：结合7.2章节，可采用分级管理、涉密管理、加注标记、技术措施、保密协议等措施。
 - (3) 发生维权时，企业可结合自身情况，除了结合8.3章节，采用境内维权、同时宜重视在出海场景下的涉外维权。

8.2.2 应急措施

制定涉嫌侵权的应急处理预案，建立紧急应对流程，包括证据保全（数据训练和使用日志、通信记录、数据状态固化等）、应对律师函的措施、应对法院证据保全的措施、诉讼应对策略、行政查处的应对策略等。

8.3 维权

8.3.1 侵权评估

发现知识产权可能被侵害时，分析权利的稳定性、是否受到侵害以及评估受侵害的程度，包括：

- a) 评估权利的稳定性和相关性；
- b) 涉嫌侵权者的情况，应理清所涉及的生成式人工智能技术存在哪些实施主体、各主体的行为模式，以明确侵权者和具体侵权行为，判断是直接侵权还是间接侵权；
- c) 可能造成的损害和影响。

8.3.2 维权途径——多元纠纷解决机制

根据侵权评估结果、诉求及成本确定适当的维权途径，包括：

- a) 与侵权者协商解决；
- b) 请求调解组织解决；
- c) 向第三方平台发起投诉；
- d) 向行政机关申请行政裁决；
- e) 向人民法院诉前禁令、行为保全、民事诉讼等措施；
- f) 仲裁；
- g) 向人民检察院申请法律监督等措施。

8.3.3 确定维权方案

根据确定的维权途径形成维权方案，包括：

- a) 通用知识产权类型维权：
 - (1) 成立专项工作组，确定工作组人员、工作机制和分工；
 - (2) 确定是否聘请外部律师团队；
 - (3) 维权措施，包括取证措施、维权策略等；
 - (4) 时间计划及重要节点；
 - (5) 资金预算。
- b) 特定知识产权类型维权：
 - (1) 对于专利侵权者提起的无效宣告请求的应对策略：创新主体可以针对被挑战的专利，依据5.2.2节中的分级标准确定无效宣告请求所针对的己方专利级别并采取相应的响应措施，进行不同程度的资源投入；
 - (2) 对于商业秘密的维权策略：对于包括生成式人工智能相关的数据泄露、人才流动引发的侵害商业秘密的侵权，权利人可依据7.3节中的应急处置、证据收集、以及8.3.2的维权途径，采取相应措施。
- c) 维权方案可根据案件进展动态调整。

参 考 文 献

- [1] 《中华人民共和国著作权法》（2020 年 11 月 11 日第十三届全国人民代表大会常务委员会第二十三次会议通过）
- [2] 《中华人民共和国专利法》（2020 年 10 月 17 日，第六届全国人民代表大会常务委员会第四次会议通过）
- [3] 《中华人民共和国商标法》（根据 2019 年 4 月 23 日第十三届全国人民代表大会常务委员会第十次会议《关于修改〈中华人民共和国建筑法〉等八部法律的决定》第四次修正）
- [4] 《中华人民共和国广告法》（根据 2021 年 4 月 29 日第十三届全国人民代表大会常务委员会第二十八次会议《关于修改〈中华人民共和国道路交通安全法〉等八部法律的决定》第二次修正）
- [5] 《中华人民共和国反不正当竞争法》（根据 2019 年 4 月 23 日第十三届全国人民代表大会常务委员会第十次会议《关于修改〈中华人民共和国建筑法〉等八部法律的决定》修正）
- [6] 《中华人民共和国著作权法实施条例》（2002 年 8 月 2 日中华人民共和国国务院公布）
- [7] 《中华人民共和国商标法实施条例》（2014 年 4 月 29 日中华人民共和国国务院公布）
- [8] 《中华人民共和国专利法实施细则》（2023 年 12 月 11 日中华人民共和国国务院公布）
- [9] 《专利审查指南》（2023 年 12 月 21 日国家知识产权局公布）
- [10] 《人工智能相关发明专利申请指引（试行）》（2024 年 12 月 31 日国家知识产权局公布）
- [11] 《中国禁止出口限制出口技术目录》（2023 年 12 月 21 日中华人民共和国商务部公布）
- [12] 《互联网广告管理办法》（2023 年 2 月 25 日国家市场监督管理总局公布）
- [13] 《互联网信息服务管理办法》（根据 2024 年 12 月 6 日《国务院关于修改和废止部分行政法规的决定》第二次修订）
- [14] 《计算机软件保护条例》（2013 年 1 月 30 日中华人民共和国国务院公布）
- [15] 《互联网信息服务算法推荐管理规定》（2021 年 12 月 31 日国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局公布）
- [16] 《互联网信息服务深度合成管理规定》（2022 年 11 月 25 日国家互联网信息办公室、工业和信息化部、公安部公布）
- [17] 《生成式人工智能服务管理暂行办法》（2023 年 7 月 10 日国家互联网信息办公室、国家发展和改革委员会、教育部、科学技术部、工业和信息化部、公安部、国家广播电视总局公布）
- [18] 《人工智能生成内容标识办法》（2025 年 3 月 7 日，国家互联网信息办公室、工业和信息化部、公安部、国家广播电视总局发布）
- [19] 《互联网新闻信息服务管理规定》（2017 年 5 月 2 日国家互联网信息办公室发布）
- [20] 《网络音视频信息服务管理规定》（2019 年 11 月 18 日国家互联网信息办公室、文化和旅游部、国家广播电视总局联合发布）
- [21] 《关于禁止仿冒知名商品特有的名称、包装、装潢的不正当竞争行为的若干规定》（1995 年 7 月 6 日国家工商行政管理局发布）
- [22] 《关于加强网络直播营销活动监管的指导意见》（2020 年 11 月 5 日，国家市场监督管理总局发布）
- [23] 《关于审理商标民事纠纷案件适用法律若干问题的解释》（根据 2020 年 12 月 23 日最高人民法院审判委员会第 1823 次会议通过的《最高人民法院关于修改〈最高人民法院关于审理侵犯专利权纠纷案件应用法律若干问题的解释（二）〉等十八件知识产权类司法解释的决定》修正）
- [24] 《关于审理涉及驰名商标保护的民事纠纷案件应用法律若干问题的解释》（根据 2020 年 12 月 23 日最高人民法院审判委员会第 1823 次会议通过的《最高人民法院关于修改〈最高人民法院关于审理侵犯专利权纠纷案件应用法律若干问题的解释（二）〉等十八件知识产权类司法解释的决定》修正）
- [25] 《最高人民法院关于审理侵犯商业秘密民事案件适用法律若干问题的规定》（2020 年 8 月 24 日由最高人民法院审判委员会第 1810 次会议通过）
- [26] 2024 年中国生成式人工智能产业链图谱研究分析（附产业链全景图）
- [27] 王红燕.《中国人工智能合规建设与知识产权法律实务》.北京：中国法制出版社，2023 年.

- [28] NIST AI 100-1 Artificial Intelligence Risk Management Frame(AI RMF 1.0) January 2023
 - [29] NIST AI 600-1 Artificial Intelligence Risk Management Framework:Generative Artificial Intelligence Profile July 2024
 - [30] European Artificial Intelligence Act
 - [31] AI と著作権に関するチェックリスト&ガイダンス 令和 6 年 7 月 3 1 日 文化庁著作権課
 - [32] AI と著作権に関する考え方について 令和 6 年 3 月 1 5 日 文化審議会著作権文科会法制度小委員会
 - [33] AI 時代の知的財産権検討会中間とりまとめ AI 時代の知的財産権検討会 2 0 2 4 年 5 月
 - [34] AI 事業者ガイドライン（第 1.0 版） 総務省 経済産業省 令和 6 年 4 月 19 日
-