知识产权和前沿
技术概况介绍

生成式人工智能
知识产权导航

WIPO

生成式人工智能（AI）工具正在快速地被许多企业和组织应用于内容生成。这类工具既为协助企业运营提供了大量机会，又由于当前的各种不确定性而带来重大的法律风险，包括知识产权问题。

许多组织正在寻求制定指导性意见，以帮助员工降低这些风险。尽管每种业务情况和法律背景各不相同，以下指导原则和清单旨在帮助各组织了解知识产权风险，提出恰当的问题，并考虑潜在的保障措施。

生成式人工智能带来众多风险和问题。企业和组织应考虑实施适当的政策，并就此项技术的机遇和局限性向员工提供培训。这种积极主动的方式在应对与使用生成式人工智能相关的挑战中至关重要。

什么是生成式人工智能?

生成式人工智能工具可以根据用户的提示（比如对期望输出的简短书面描述）创建文本、计算机代码、图像、音频、声音和视频等新的内容。目前生成式人工智能工具的实例包括ChatGPT、Midjourney、Copilot和Firefly。

生成式人工智能以机器学习为基础，生成式人工智能工具则使用大量数据进行训练，这类数据通常包括数十亿页的文本或图像。训练数据集可由免费获取且无产权负担的信息（纯数据）、受保护数据（比如受版权保护的作品）或两者混合组成，具体取决于人工智能工具开发人员所采用的方式。

然后，经过训练的人工智能工具受到人工输入的提示，触发通常高达数十亿次的一系列复杂计算，以确定输出。一般来说，无法预测输出，也无法确定训练数据的某些部分是否以及在多大程度上影响所产生的输出。

图：Getty Images / Laurence Dutton

问题概述

开发生成式人工智能的成本可能非常高昂，可达到数千万美元，大多数企业和组织都选择采用第三方生成式人工智能工具，或者使用自己的数据对此类模型进行微调。一般存在的问题和企业风险包括：

确定用例	生成式人工智能可以执行许多任务，最佳用例仍在不断发展中，不同企业和组织的情况将会各不相同。
合同条款的差异	生成式人工智能工具是新生的，商业合同条款的最佳实践和规范仍在发展中。开发人员许可其人工智能工具的条款可能存在相当大的差异，包括商业秘密和其他机密信息的处理方法、输出的所有权、赔偿的可获性以及用户通过实施员工监测和训练来缓解风险的义务。
训练数据问题	一些生成式人工智能工具使用从互联网上抓取的材料进行训练，包括版权作品、个人信息、生物识别数据以及有害的非法内容。关于材料的抓取、下载和处理、受过训练的人工智能模型及其输出是否涉及侵犯知识产权、隐私和合同，这方面的诉讼尚在进行中。有关知识产权所有人和人工智能开发者之间利益平衡的争论仍在继续。
输出问题	生成式人工智能可能会产生不适当或非法的输出，包括不正确的信息、知识产权侵权、深度伪造、个人信息、诽谤性指控以及有偏见的歧视性和有害内容。技术保障措施正在制定，但鉴于相关计算的复杂性，预测人工智能在所有情况下的行为是一件棘手的事情。此外，大多数国家的知识产权法是在人工智能出现之前制定的，导致在人工智能输出的权利归属方面存在不确定性。

改变监管环境	政府和监管机构正在考虑为生成式人工智能制定新的法律、法规、政策和指导方针。这些法律、法规、政策和指导方针可能会对使用生成式人工智能的企业和组织提出要求。中国已出台具体法规，欧盟打算不久也实施相关法规。

该问题清单并非详尽无遗，可能还有许多其他挑战，包括训练和使用生成式人工智能的高耗能特性。

联合国教科文组织、经合组织和人工智能全球伙伴关系等许多国际组织就负责任地使用人工智能的一般原则发布了指导意见。企业和组织应针对生成式人工智能考虑实施员工政策和培训，以鼓励进行负责任的实验和使用。

生成式人工智能和知识产权

生成式人工智能有许多知识产权方面的接触点和不确定性。虽然不可能彻底缓解这些知识产权风险，但以下因素可能有助于在这一不断演变的技术领域中引导知识产权方面的考虑。

机密信息

机密信息是指不能公开获得的、可能具有也可能不具有商业价值，且在私下交流和受到合理保护的信息。它包括商业秘密，这是一种具有（潜在）经济价值或因其秘密性而可以提供竞争优势的机密信息。

如果使用生成式人工智能工具的企业和组织将商业敏感信息用于人工智能工具的训练或提示，则可能会无意中泄露商业秘密或放弃对商业敏感信息的保密。它们应该考虑并用技术、法律和实际保护措施，防止发生这种情况。

风险	缓解办法
生成式人工智能工具可以保存用户提示并基于用户提示进行训练。如果用户提示中包含机密信息，由于人工智能供应商拥有机密信息的副本，且机密信息可能成为与其他用户公开共享的模型和输出的一部分，机密信息就会丧失机密性。	检查生成式人工智能工具的设置，尽量减少供应商存储或利用你的提示进行训练的风险。
当企业和组织从零开始训练生成式人工智能工具或使用其机密信息微调现有工具时，存在着信息被公众获取的风险。	考虑使用在私有云上运行和存储的生成式人工智能工具。
黑客可以使用“提示注入”等技术提取训练数据，包括机密信息。	检查人工智能工具的供应商是否会存储、监测和审查你的提示。就任何机密信息向供应商寻求适当的保护和保证。
私人生成式人工智能工具的供应商可能会监测和存储提示，以检查不当使用的行为。在某些情况下，可能由供应商的员工审查提示。	将使用机密信息的生成式人工智能工具的访问权局限于被授权获取该信息的员工。
	实施员工政策，并就提示中包含机密信息的风险提供培训。
	考虑让信息安全专家审查和监测生成式人工智能工具。

知识产权侵权

许多生成式人工智能工具都是基于大量（有时是数十亿）受知识产权保护的项目进行训练的。现有几起正在进行的法律纠纷，它们指控抓取和使用这些作品来训练人工智能、受过训练的人工智能模型及其输出属于知识产权侵权行为。这些案件主要聚焦于版权和商标，但从理论上讲，也可能涉及其他知识产权权利，比如工业品外观设计、数据库权利和专利发明。

人工智能工具及其训练、使用和输出是否构成知识产权侵权，在法律上存在很大的不确定性。不同司法管辖区可能会给出不同的答案。企业和组织应该考虑通过使用符合知识产权规范的工具，尽可能寻求赔偿，审查数据集，并实施技术和实际措施来减少侵权的可能性，从而降低风险。

风险

对于判定使用受知识产权保护的项目训练人工智能、使用此类受过训练的人工智能模型及其生成的输出是否构成知识产权侵权，世界各地均有未决诉讼。

风险不仅限于人工智能开发人员，还可能延及生成式人工智能工具用户。在许多国家，各种形式的知识产权侵权责任（比如复制版权作品）并非取决于被控侵权人的意图或认知。

法院尚未解决生成式人工智能开发人员、供应商、客户和用户是

缓解办法

考虑使用仅基于许可、公有领域或用户自己的训练数据所训练的生成式人工智能工具。

在选择一款人工智能工具时，要考虑是否有供应商愿意为知识产权侵权（特别是版权侵权）提供赔偿。评估赔偿的范围和适当性。例如，保护可能仅限于第三方赔偿，并以遵守合同限制和实施缓解风险为条件。

在训练或微调生成式人工智能时，彻底审查数据集。核实知识产权所有权、人工智能训练的许

否可对知识产权侵权、赔偿款以及销毁侵权模型或输出承担责任的问题。尚不清楚法院是否会认为下令禁用基于受知识产权保护项目进行训练的人工智能模型是适当的。

关于潜在的版权侵权问题，一些国家的知识产权法包括可能适用于生成式人工智能的例外情况，例如正当使用、文本和数据挖掘以及临时复制。但是，各国之间缺乏协调统一，以及这些例外对生成式人工智能的适用仍是未知数，由此带来了不确定性。

即使法院已作出判决，这些也可能取决于具体的案情以及国家法律的规定。

可范围，以及遵守知识共享许可协议或公有领域地位的情况。确保在预定的司法管辖区采取适当的版权例外。

请注意，监管机构正在考虑对用于模型训练的、受知识产权保护的项目履行细节披露的义务。考虑保存记录，记载人工智能模型是如何接受训练的。

实施员工政策和培训，以尽量减少产生侵权输出的风险。告诫不要使用提及第三方企业名称、商标、版权作品或具体作者/艺术家的提示。

使用输出之前，考虑采取措施检查侵权行为。这些可能包括抄袭检查程序、图片搜索和自由实施审查。

根据具体情况评估缓解措施、相关成本和业务风险。

图：Getty Images / Laurence Dutton

开源义务

人工智能生成的代码可能会受到开源义务的约束。当一个软件应用或代码是开放源代码时，意味着该源代码对公众开放，用户通常被授予使用、修改和分发该软件的特定权利和自由。不过，这些权利和自由伴随着用户必须遵守的义务，例如署名问题，并且这些义务根据管理软件的特定开源许可不尽相同。

企业和组织应考虑这种风险是否与其代码相称，调查潜在的补偿，并实施技术和实际措施，以减少开源义务产生的可能性。

风险	缓解办法
生成式人工智能可基于符合开源要求的代码进行训练，因而可能会违反关于商业使用或署名的限制条件等义务。在美国，一直有这方面的法律纠纷。	考虑从专门基于许可示例进行训练的供应商处获取生成式人工智能工具，或者实施技术保障措施，例如发现相关开源许可。
一些开源许可证规定，含有开源代码的任何代码都要遵守同一个开源许可证的要求。因此，集成人工智能生成代码的用户可能会无意中将开源义务引入其项目。	考虑从提供开源侵权赔偿的供应商处采购生成式人工智能工具。检查保护的范围和适当性以及适用条件。
	在训练或微调生成式人工智能工具时，彻底审查训练数据，以获得足够宽松的许可。
	在编码中使用生成式人工智能时采用风险收益法。如果确保代码不受开源义务的约束至关重要，则应考虑禁止供应商和员工就这些项目使用生成式人工智能。

深度伪造：肖像权和声音权

肖像和声音在许多国家都受到保护，但这种保护并不统一。保护的形式包括一些知识产权权利（比如普通法系国家的假冒）、不正当竞争法、人权、宪法权利和公开权。

生成式人工智能具有模仿特定人物的肖像或声音的潜力，因为有些工具专门为此而设计。企业和组织应该考虑到与这些功能相关的风险。

风险

未经授权使用或模仿某个人的声音或肖像可能导致侵犯知识产权或其他权利，并因各司法管辖区的法律框架不统一而带来挑战。

模仿肖像和声音还可能面临名誉受损或法律诉讼的风险，例如欺诈或诽谤。许多国家正在考虑针对深度伪造制定具体的法律法规。例如，中国已经通过了适用于“深度合成”的法规。

缓解办法

制定员工政策，并提供明确限制使用“深度伪造的”生成式人工智能工具的培训。对于经批准的生成式人工智能工具，实施禁止在提示中提及特定个人的政策。

在有合法的商业理由合成某个人的声音或肖像的情况下，要获得主体的必要同意和许可。

图：Getty Images / SIphotography

人工智能输出的知识产权权利和所有权

尚不明确人工智能工具生成的新内容（比如文本、图像或其他创意作品）是否受到知识产权权利保护，以及如果受到保护，谁拥有这些权利。即使人工智能输出不受知识产权保护，可能还有约束其使用的合同条款。

生成式人工智能输出中的知识产权权利的存在和所有权尚不清楚。企业和组织应该寻求在合同中明确所有权，只有在输出中的知识产权所有权对其业务模式并非至关重要的情况下才考虑使用生成式人工智能。

风险

大多数国家的知识产权法在编写时都没有考虑到生成式人工智能，导致不确定人工智能输出中是否可以有知识产权以及谁将拥有任何此类权利。对于像商标这样的一些知识产权权利来说，这可能不算问题，但对于版权而言，这是一个广泛关注的问题。

最近，将人工智能系统“DABUS”命名为发明人的专利申请，因无法确定人类发明者而在已作出判决的国家被一致驳回。目前尚不清楚生成式人工智能是否可以不依赖人类发明者做出发明，或者这些发明是否可取得专利权。

美国版权局就注册包含人工智能生成材料的作品发布了指导意见，

缓解办法

审查生成式人工智能工具的条款和条件，以了解谁是输出中知识产权（如有）的所有者。

通过纳入品牌名称和标识等知识产权元素，或在修改或创建新版本的输出中引入人类的创意，探索各种途径，加强对输出的控制或权利。

记录人类在发明或创造过程中的作用。

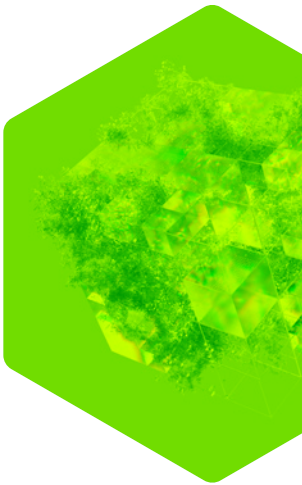
在可能的情况下，就谁拥有计算机生成作品的版权订立协议。不同国家的法律标准不同，可能难以适用，因此协议可增加确定性。

在委托创作时，可考虑寻求获得未使用生成式人工智能的保证。

指出作品中需要有人类的创造性贡献。版权局的裁定表明，仅凭用户的文字提示不能确定版权，因为提示仅仅“影响”输出。然而，北京互联网法院最近裁定，由于用户调整了提示和参数，使图像反映出用户的审美选择和判断，因此用户对人工智能生成的图像拥有版权。这些对人工智能生成作品的版权的不同解释，给全球识别生成式人工智能输出的版权带来了法律上的不确定性。

少数几个国家（比如印度、爱尔兰、新西兰、南非和联合王国）为没有人类作者的“计算机生成的作品”提供版权保护。乌克兰对计算机程序生成的“非原创物品”提供权利。

考虑只在知识产权权利并非必需的情况下使用生成式人工智能，例如供内部使用、创意生成以及（个人）社交媒体帖子等短暂用途。



检查清单

企业和组织可以采取许多措施，促进负责任且合法地使用生成式人工智能。以下检查清单可能有助于希望实施负责任的做法并驾驭这一快速发展领域的企业和组织。

员工政策和培训

- ☐ 实施员工政策和培训，以引导适当的使用，并鼓励对生成式人工智能进行负责任的实验和使用，包括：
  - ☐ 了解与生成式人工智能相关的机会、风险和限制。
  - ☐ 避免在提示中使用机密信息。
  - ☐ 将应用商业秘密训练的生成式人工智能的访问权局限于被授权访问的员工。
  - ☐ 在提示中避免使用第三方知识产权，以尽量减少侵权输出。
  - ☐ 避免使用“深度伪造的”生成式人工智能工具。

风险监测和风险状况管理

- ☐ 监测判例法和法规的变化。
- ☐ 根据不断变化的风险和法院裁决，定期评估和更新政策。
- ☐ 向业务部门明确传达法律风险，以便根据业务风险偏好采取相应措施。
- ☐ 保有一份人工智能工具清单，并根据风险状况对其分类，例如，所有员工均可使用的工具、使用机密信息的受限工具以及禁用工具的白名单。

记录保存

- ☐ 考虑记录如何训练人工智能工具。
- ☐ 让员工给人工智能生成的输出做标记，并对所用提示进行记录保存。
- ☐ 记录创作过程中人的作用。

人工智能工具评估

- 审查外部采购工具的条款、条件和设置（包括基于内部数据进行训练的工具），以便
  - 了解供应商是否储存有你的提示。
  - 了解这些工具基于哪些数据进行了训练。
  - 寻求使用获得适当许可或公有领域训练数据的工具，或者拥有技术保障措施以防范使用受保护数据的工具。
  - 确定供应商是否针对知识产权侵权提供补偿，以及有哪些条件。
- 由信息安全专家审查和监测生成式人工智能工具。
- 探索存储在内部或私有云中的私人生成式人工智能工具，以加强控制和保证。
  - 就机密信息向供应商寻求适当的保护和保证。

数据评估

- 在训练人工智能时检查数据集，并考虑知识产权的所有权和许可范围。

人工智能输出

- 检查生成式人工智能供应商关于输出中的知识产权权利和所有权的条款。
- 在使用输出之前检查知识产权侵权情况。
- 将人工输入和创意与人工智能输出相结合，以保持对输出所有权的控制。
- 就输出的所有权订立协议。
- 记录创作过程中人的作用。
- 获得合成某个人的声音或肖像的必要同意和许可。

延伸阅读

产权组织知识产权和前沿技术对话会是一个促进所有利益攸关方就包括人工智能在内的前沿技术对知识产权的影响进行讨论并分享知识的全球主要论坛。

产权组织对话会第八届会议着重对生成式人工智能和知识产权进行了讨论，以帮助政策制定者了解潜在的政策选择。关于产权组织对话会第八届会议的更多信息，包括日程安排、演示报告和网播，可在该会议网页上查看。

知识产权和前沿技术的更多信息载于产权组织网站：www.wipo.int/ai.

下一步工作

如需了解产权组织对话会下届会议的最新信息，请发送电子邮件至frontier.tech@wipo.int注册订阅知识产权和前沿技术司的新闻通讯。

本文件由产权组织知识产权和前沿技术司参考Matt Hervey（英国高林睿阁律师事务所）的受托作品编写而成。

封面：Getty Images / Laurence Dutton, Just_Super / 产权组织文号：RN2024-8ZH; DOI: 10.34667/tind.49473

wipo.int

WIPO
世界知识产权组织