C

WIPO/ACE/16/15
原文：英文
日期：2024 年 1 月 12 日

执法咨询委员会

第十六届会议
2024 年 1 月 31 日至 2 月 2 日，日内瓦

人工智能和知识产权执法

撰稿：Dennis Collopy 先生、Countercheck 有限公司、环球音乐集团和美卡多公司

1. 在 2022 年 8 月 31 日至 9 月 2 日举行的执法咨询委员会（ACE）第十五届会议上，委员会同意在第十六届会议上审议的议题之一是“就知识产权执法政策和体制等方面的制度性安排交流各国经验信息，其中包括以兼顾各方利益、全面而有效的方式解决知识产权争议的机制”。在这一框架内，本文件介绍了三个私营部门实体（Countercheck 有限公司、环球音乐集团和美卡多公司）关于在人工智能和知识产权执法方面的经验的稿件。

2. Dennis Collopy 先生的稿件概括介绍了《人工智能和知识产权执法》研究报告。稿件明确了关键定义，解释了所使用的方法，并全面概述了研究结果。更具体而言，它指出了利用人工智能进行知识产权执法的机遇，如改进对版权侵权内容的检测、外观设计识别和更快地检测商标滥用。反之，它也指出了一些重大挑战，如成本、缺乏透明度、数据共享问题和伦理方面的考虑。

3. Countercheck 有限公司的稿件讨论了在包裹检查中使用人工智能的情况。稿件重点介绍了 Countercheck 的技术以及实施人工智能的法律挑战，强调了公共和私营部门合力打击知识产权犯罪和完善法律框架的必要性。

4. 环球音乐集团的稿件强调了其对人工智能的看法，重点是在对知识产权侵权深表关切的同时，以负责任的方式使用人工智能。它深入探讨了一些令人担忧的活动，例如利用人工智能模仿艺人并生成欺诈性曲目，以及人工智能系统的训练手段，特别是未经授权获取受版权保护的音乐作品。稿件还强调了音乐产业的权利人如何使用人工智能——既作为创作过程的辅助手段，又作为检测侵权的工具。

5. 美卡多公司的稿件讨论了如何利用人工智能自动检测和删除其电子商务市场上的假冒商品列表。在概述了整个拉丁美洲的监管框架之后，该稿件介绍了美卡多公司在人工智能的协助下积极主动地检测假冒商品的努力，以及在这样使用人工智能时遇到的困难。

6. 稿件的顺序如下：

[后接稿件]

人工智能和知识产权执法：挑战和机遇概述

撰稿：Dennis Collopy 先生，赫特福德大学创意艺术学院高级研究员，联合王国 *

摘　要

本文概述了《人工智能和知识产权执法》研究的结果。在报告研究结果之前，本文明确了关键定义，并解释了所使用的方法。更具体而言，它指出了利用人工智能（AI）进行知识产权执法的机遇，如改进对侵犯版权内容的检测、外观设计识别和更快地检测商标滥用。反之，成本、缺乏透明度、数据共享问题和伦理考虑因素构成了人工智能的一些挑战。稿件最后得出结论，虽然人工智能提供了前景广阔的解决方案，但在更多地采用人工智能之前，必须进行审慎试点并关注伦理、道德和法律界限。

一、导　言

A.　研究的宗旨和目的

1.　此项研究于 2021 年受联合王国知识产权局委托进行，旨在评估是否以及如何利用人工智能（AI）追踪知识产权侵权商品，并评估知识产权侵权者使用人工智能的可能性。

2.　该项目的目的是审查和整理现有文献，并收集具有专门知识和经验的人对现有知识产权执法状况的看法，以便：

- 了解权利人目前如何利用人工智能来保护和执行知识产权，以及
- 评估知识产权侵权者的威胁。

3.　研究涉及五项知识产权：专利、商标、外观设计、版权，以及（尤其是）商业秘密。

B.　方法

4.　该项目分为两个阶段，包括：

- 对政府、学术界和产业界编写的与要审议的五项知识产权相关的人工智能和知识产权执法文献进行批判性审查，以确定核心主题和成果。
- 在此基础上制作了一份调查问卷，对产业界、执法机构、学术界、法律从业人员和司法部门的相关利益攸关方进行了广泛的访谈，以获取对当前问题的最新见解。

C.　定义

5.　鉴于人工智能的定义越来越多，从一开始就必须仔细界定所使用的术语。

6.　这项研究的合著者、人工智能专家 Kevin Curran 教授给人工智能下了一个最清晰、最简洁的定义，即“机器表现出的人类智能”。

7.　我们的研究侧重于人工智能的子集，即机器学习（ML）形式的狭义人工智能。机器学习能够创建“能够从经验中学习，在一组数据中发现模式”的系统，从而能够推断或预测结果，即使过程中存在一些挑战和机遇，而识别这些挑战和机遇正是我们最初研究的重点。文中提到的其他相关表述包括：

---

*　本文件所表达的观点为作者的观点，不一定代表产权组织秘书处或成员国的观点。

- 狭义人工智能是当今存在的唯一一种人工智能形式，它被训练来执行单一任务，与一般人工智能不同，它不能在规定任务之外运行[1]。根据 IBM 的说法，“任何其他形式的人工智能都是理论上的”，甚至 OpenAI 的 ChatGPT 也是狭义人工智能的一种形式，因为它“仅限于基于文本的聊天这一单一任务”[2]。
- NLP（自然语言处理）是指计算机能够像人类一样理解文字和口语。
- 不透明的人工智能（也称黑盒人工智能）无法像有完整审计线索的系统那样接受检查。
- 神经网络是机器学习的一个子集，是深度学习算法的关键，它利用训练数据进行学习，并随着时间的推移不断提高准确性，从而实现高速的数据分类。

二、研究发现

A. 主要机遇

a) 版权

8. 在版权执法中有机会更多地使用人工智能工具，特别是考虑到某些明显取得成功的自动化反盗版系统。

9. 作为一种过滤工具，人工智能有助于识别侵权内容，减少人工工作量，但它需要准确、充分的训练数据。YouTube 的“内容 ID”就是一项明显取得成功的人工智能工具，研究人员发现它“从 YouTube 上删除明显侵权内容的效果相对较好”[3]，尽管其成功率并非百分之百。

b) 外观设计

10. 在外观设计方面，图像识别能力的提高有助于识别潜在的侵权行为。反外观设计抄袭协会（ACID）拥有一个包含 30 多万项外观设计（包括未注册外观设计）的数据库，可以为训练人工智能识别侵权外观设计提供数据。

c) 商标

11. 人工智能工具可以帮助商标执法分析人员，如果能在非常大的数据集上进行培训，就能解放人力资源。与面向消费者的在线平台密切合作，部署人工智能工具监测内容，还可以进一步开发执法解决方案。

12. 例如，欧洲联盟知识产权局（欧盟知识产权局）提供了一系列新工具，包括跟踪和追踪解决方案、风险分析系统，以及利用人工智能/机器学习来检测可疑和潜在的滥用域名注册。

13. 人工智能可以在执行不同类型的网络犯罪所涉及的权利方面发挥作用，也可以在检测假冒伪劣产品方面为人类行为者提供帮助。

---

[1] IBM 数据和人工智能团队（2023 年 10 月 19 日），“了解人工智能的不同类型（Understanding the Different Types of Artificial Intelligence）”，可查阅：https://www.ibm.com/blog/understanding-the-different-types-of-artificial-intelligence/。

[2] 同上。

[3] Joanne E. Gray 和 Nicolas P. Suzor （2020 年），《携手机器：利用机器学习了解大规模自动化版权执法》（Playing with machines：Using machine learning to understand automated copyright enforcement at scale, Big Data & Society），可查阅：https://doi.org/10.1177/20539517209199。

d) 商业秘密

14. 商业机密，尤其是与人工智能相关的发明，需要加强保护，防止被盗用。基于人工智能的技术（包括神经加密技术）等安全措施可以提供更大的保护。

e) 小结

15. 版权侵权检测是人工智能大规模应用于知识产权执法的最常见例子，前提是要有强大的训练数据集。如果采用类似方法，人工智能也可用于识别外观设计和商标侵权行为，从而减少人力资源。

16. 知识产权分析可以更好地发现知识产权侵权的关系、趋势和模式，从而改进执法决策。

17. 人工智能只会不断进步，变得更准确、更快速，以远超人类的方式检测模式。

18. 总之，人工智能是一种有用的过滤工具，可以辅助人工分析，加快识别侵权内容的过程。

B. 主要挑战

a) 版权

19. 存在对使用自动化工具对侵犯版权行为进行执法所涉及的成本和资源的担忧。这些工具可能超出了许多中小企业权利人的能力范围，他/她们主要依靠集体管理组织和行业协会来行使自己的权利。

20. 自动化反盗版系统是不透明的，依赖于使用动态、可能无法预测和不透明算法的硬编码自动规则来进行决策。

b) 外观设计

21. 人工智能工具可以帮助查询已注册外观设计数据库。但是，人工智能可能无助于识别未注册外观设计或依赖于版权的外观设计的侵权行为。

22. 除了现有的数据库（如 ACID 维护的数据库）之外，利用人工智能识别侵权所涉及的成本对拥有外观设计组合的大公司有利。

23. 在执行注册和未注册外观设计时，必须考虑到计算机辅助设计（CAD）和人工智能生成的外观设计的使用，尤其是在未注册外观设计权被用于训练人工智能的情况下。

c) 商标

24. 产业界、政府和执法机构之间的数据共享问题阻碍了自动化工具的大规模使用，从而妨碍了商标执法。

25. 执法部门很难从侵权网站中提取干净的数据，也很难整理出有效的大型数据样本用于人工智能的训练。

d) 专利

26. 人工智能在专利权执法方面的应用需要结合人类知识和技术知识。

27. 申请专利所涉及的语言的复杂性以及采取法律行动的复杂性、成本和精力都是专利权执法所面临的挑战。此外，在英国法庭诉讼中使用反向工程证据的限制也使某些专利权的侵权行为难以证明。

28. 人工智能生成或人工智能辅助的知识产权侵权行为必须与法律意义上的“人”的行为有关，因此可能需要以操作人工智能的人作为执法对象。

29. 由于人工智能“黑箱”[4]，其不确定性使人类无法理解，因此可能会阻碍对人工智能相关专利侵权行为的执法。

30. 人工智能工具被认为不够细致，也不适合专利法，因为专利法需要横向思维和解释。

e) 商业秘密

31. 在法庭诉讼期间，商业秘密执法受公开披露风险的影响，因此侵权问题通常在庭外解决。商业秘密的执法也因法律上构成商业秘密的不确定性而受到影响。

32. 人工智能被视为商业秘密网络盗窃增加的相关因素之一，这反过来又需要新的人工智能和机器学习工具来打击网络攻击。

33. 还有人担心，人工智能可能会被滥用于入侵和掌握商业秘密，而不是保护商业秘密。

34. 商业秘密包括不受专利或其他知识产权保护的有商业价值的信息，但其执行取决于采取合理的保密措施，因为这些信息只有在能够保密的情况下才有用。

35. 在这方面，鉴于商业秘密的细微差别和多样性，以及商业秘密本来就不是面向公众的这一事实，人工智能被认为不那么即刻起作用。

f) 伦理问题

36. 在知识产权执法中使用人工智能的道德局限性包括决策过程中涉及的训练数据集的质量（如不充分或不完整），以及可能导致不公平或不正确决策的系统性和固有的人为偏见。

37. 目前，技术本身也存在不完善之处，包括缺乏透明度（尤其是在“黑箱人工智能”方面）和问责制，以及对人工智能工作原理的不完全了解。

38. 还有人担心人工智能的决策过程不够灵活，可能会导致“过度热心地屏蔽”合法内容。

g) 法律问题

39. 人工智能工具需要重新培训，以满足不同地区不同知识产权法律的需求。当人工智能训练数据涉及使用大量个人或敏感数据时，如何保持 GDPR 合规性也是一个基本挑战。

40. “不良行为者”利用人工智能的危险是存在的，比如在内容被依删除通知删除后重新上传的能力。

h) 小结

41. 主要挑战在于有效利用人工智能进行知识产权执法所需的训练数据的质量和数量，以及所涉及的重要伦理道德问题。

42. 人工智能系统是一个大量耗费资源的过程，人工智能使用的数据量与结果的准确性之间有着明显的联系。

[4] 很不容易了解黑箱人工智能模型是如何产生预测结果的，“因为并不容易获得它的内部运作，而且这种运作在很大程度上是自我指挥的。就像很难看到漆成黑色的箱子内部一样，要了解每个黑箱人工智能模型是如何运作的也是很不容易的”；见 Kinza Yasar 和 Ivy Wigmore，《黑箱人工智能》（Black Box AI），可查阅：https://www.techtarget.com/whatis/definition/black-box-AI。

43. 训练数据的数量、质量和时效是一个普遍关注的问题。显然，训练人工智能工具非常耗时，而且需要不断更新。

44. 考虑到人工智能目前的局限性和伦理担忧，人工智能目前只能作为一种初始工具，用于将内容标记给人工分析师进行验证，而不能独立进行知识产权执法。

三、结论和建议

A. 结论

45. 在使用人工智能/移动终端进行五项知识产权执法中的每一项时，挑战都大于机遇，这主要是由于与使用人工智能进行专利和商业秘密执法有关的基本问题。

46. 在知识产权执法中使用人工智能还存在其他一些问题，其中包括：

- 普林斯顿大学 2022 年的一项研究[5]着重指出了与定量科学中使用机器学习有关的常见方法问题。
- 联合王国邮局 Horizon 软件的长期丑闻凸显了“人类盲目接受自动化系统的输出结果作为可靠证据的危险性”。法律协会前主席 Christina Blacklaws 警告说，邮局事件应该“作为每个组织的警示故事”。减少技术资源、外包关键专业知识和采用不太合适的审计流程的其他组织也可能出现类似问题。[6]
- 澳大利亚政府对 Robodebt 的失败试验，ACS 称其为“人工智能伦理灾难”。[7]
- 对抗机器学习的出现，即坏人可以利用人工智能系统的漏洞，改变其行为以达到恶意的最终目的。这些攻击可能涉及（训练数据）中毒或规避攻击，其中许多攻击在出现人工智能重大故障之前都不会被察觉。

B. 建议

47. 我们仍然相信，人工智能/机器学习有能力提供可扩展的解决方案，协助某些（如果不是所有）我们审议的知识产权的执法。我们还强调，人工智能/机器学习本身也在不断改进。

48. 我们不能不强调前面所述的重要注意事项就建议更多地采用该技术。

49. 因此，我们建议对任何新的基于人工智能的知识产权执法系统进行审慎试点，以确定系统设计是否考虑到上述缺点，以及该技术是否在伦理、道德和法律界限内运行，以实现其主要目的。

[稿件完]

---

[5] Sayash Kapoor 和 Arvind Narayanan（2023 年），《基于机器学习的科学模式中的泄密和可复制性危机》（Leakage and the Reproducibility Crisis in Machine-learning-based Science Patterns），可查阅：https://doi.org/10.1016/j.patter.2023.100804。

[6] John Thornhill（2021 年 4 月 29 日），《邮局丑闻暴露了自动化不公正的风险》（Post Office Scandal Exposes the Risk of Automated Injustice），《金融时报》，可查阅：https://www.ft.com/content/08f485bf-6cea-46d6-962c-46263aaec5f3。

[7] “Robodebt”系统旨在自动匹配税收系统中的收入差异数据，每年的评估数量从 2 万次增加到近 80 万次，几乎增加了 40 倍。2017 年，联邦监察员发现该数字系统在透明度、可用性和公平性方面存在问题。

一种创新的反假冒方法：人工智能驱动的知识产权执法包裹检查

撰稿：Countercheck 有限公司品牌保护和知识产权法律经理 Karolina Zhytnikova 女士，德国柏林 *

摘　要

Countercheck 的防伪解决方案以人工智能技术为基础，有助于保护消费者免受危险商品的侵害，并维护知识产权权利人的权利。

Countercheck 软件直接安装在物流公司分拣中心的现有硬件上，被引入物流链的最中心环节。它可以监控通过分拣中心的所有包裹，检测并拦截可能含有假冒产品的包裹。

过时的法律框架不适应电子商务的迅猛发展，是 Countercheck 在建立其业务模式时遇到的主要挑战。邮政包裹流中扣押和销毁假冒商品的机制僵化，缺乏对在国内市场上运作的假冒者做出高效和迅速反应的权力，这些都损害了反假冒努力的有效性。

物流公司越来越多地对其网络中的假冒商品采取零容忍态度。所有行业参与者内部的公共和私营部门之间的顺畅合作将有助于应对打击假冒产品的新挑战。

一、导　言

1.　电子商务在大流行病期间日益普及，建立了一种新的消费行为模式。这一现象大大增加了消费者直接从电子商务平台和社交网络订购产品的数量。通过邮寄方式运送给客户的不仅有正品，还有假冒商品，这对客户的健康和安全构成了严重威胁。

2.　非正宗商品的批发分销商也在积极利用这一分销渠道囤积假货。邮政运输不仅成本更低，送货更方便，而且由于对运输货物进行抽查，也降低了被执法机关截获的风险。此外，与通常用卡车和集装箱运输的数量相比，即使被截获，造假者的损失也相对较小。这些都是邮政包裹或快件受到造假者青睐的主要原因。

3.　物流业、执法机构和知识产权权利人认识到上述挑战，强调了从整个包裹流中自动处理和智能预选可疑货物的重要性。

二、COUNTERCHECK 在打击假冒商品方面的人工智能技术

A.　帮助实现　供应链正当性

4.　人工智能技术可用于多种途径来解决假冒问题。例如，其中包括在制药、烟草和汽车行业众所周知且广泛使用的方法——可追溯性（跟踪和追溯）解决方案。这些解决方案允许制造商及其合法供应商鉴定正品，并检测供应链各阶段的中断情况。这些技术有助于知识产权权利人实时监控正品的生命周期以及市场上对安全代码可能进行的转移和更改。

5.　Countercheck 解决方案的主要原则是利用人工智能技术，重点不是放在正品上，而是分析整个商业流程。这样做的目的是隔离可能含有假冒产品的高风险包裹，并为知识产权权利人和执法机构提供更广泛的知识产权侵权产品移动的实时情况（即新的路径、入境点、过境国等）。Countercheck 技术有助于确定热点地区，集中执法力量，实现最高效率。

---

*　本文件所表达的观点为作者的观点，不一定代表产权组织秘书处或成员国的观点。

B. 增强反假冒工作的效力

6. Countercheck 的人工智能技术直接引入物流分拣中心的供应链。它可以在减少人工互动的情况下对整个包裹流进行自动控制，并有选择性地只拦截侵犯知识产权的货物，而不拦截所有其他合法产品。

7. 这一检测过程由多个步骤组成：

- 系统提取包裹外部的所有信息，而不分析其内容/内部。
- 人工智能算法在不直接干预包裹的情况下，对 141 多项标准进行分析，并决定是否拦截托运货物以接受进一步检查。
- 如果风险评估系统显示包裹中可能含有假冒商品的概率达到或超过 80%，它就会指示硬件将包裹侧卸到一个单独的专用滑道中。

8. 利用最新的机器学习技术，可以在 0.6 秒内确定通过分拣带的每个包裹的“风险特征”。这样就能有效地检测出潜在的假冒伪劣产品，而不会影响枢纽的运作，也不会造成包裹投递的延误。

三、实施人工智能技术的现行法律框架面临的挑战

A. “国内”包裹流

9. 在欧洲层面，“欧洲议会和欧洲理事会2013年6月12日关于知识产权海关执法和废除理事会第1383/2003号条例的第608/2013号条例”（下称“第608/2013号条例”）赋予海关当局在欧洲联盟边境打击假冒产品的更大权力。

10. 普遍观点认为，大多数假冒商品都是在欧洲联盟之外生产的，并从国外进口到欧盟国家，可与之相反，大量假冒商品都是在欧洲本土生产[8]和/或组装的。

11. 遗憾的是，欧洲各国的国家立法并不总是规定有效的机制和权力，使执法当局能够处理内部市场上的假冒产品，特别是“国内”包裹流。法国是一个正面的例子。[9]

12. 在法国，知识产权权利人不仅可以根据欧盟第608/2013号条例提出行动申请，还可以根据《法国知识产权法典》提出行动申请。通过该行动申请，可以在法国境内对货物进行监控。换言之，即使货物已经通关并自由流通，也可能被扣留。

13. 事实上，这种缺乏控制的情况导致假冒商品批发商倾向于通过邮政物流渠道为当地跳蚤市场、街头小贩、非法商店、仓库和工厂提供货源，以此作为一种B2B模式。

B. 小件货物程序

14. 第608/2013号条例还规定了销毁涉嫌侵犯知识产权货物的简化程序，该程序无需事先获得法院裁决（第26条）。海关在对来自电子商务平台的B2C包裹流进行边境管制时，广泛采用了这一众所周知的销毁小件假冒商品而无需联系知识产权权利人的程序。

15. 然而，一旦这些货物清关完毕，或者如果这些货物在某一欧盟国家生产，然后通过邮政方式加急运往另一个欧盟国家，则不再适用这一小件货物的简化销毁程序。欧盟在这一问题上没有统一的法律框架，只有极少数国家在其国家立法中实施了有关这一问题的先进方法。因此，在大多数情况下，在内部市场拦截可疑货物是警方的特权。为了继续扣押和进一步销毁假冒商品，执法当局（警察）必须开启并遵循普通（即非简化）程序，无论发现的是一双鞋还是一批500件涉嫌假冒产品。

16. 缺乏扣押和简化销毁所有邮寄货物的有效机制，是Countercheck在实施其技术时面临的最大法律挑战之一。

四、物流领域对终端消费者和业务合作伙伴的社会和商业责任新标准

17. 最后，应该说人工智能技术有助于提高我们的工作效率，日常流程的自动化为执法机关节省了大量时间。不过，要想进一步成功打击非法贩运知识产权侵权商品，还应该考虑到另一个非常重要的要素。这个要素就是合作。

---

[8] 例如，法国国家宪兵队查封了一个假冒香烟地下生产基地：https://www.europol.europa.eu/media-press/newsroom/news/counterfeit-tobacco-products-worth-eur-17-million-seized-in-france。

[9] 《法国海关法典》第66条赋予海关当局检查和进入邮政服务提供商和快递货运公司场所的权利：https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071570/LEGISCTA000006138845/。

18. 知名物流公司越来越多地对其网络中的假冒商品采取零容忍的态度，以此作为合规和加强对其物流领域业务合作伙伴的商业责任的一个要素。此外，通过这样做，它们还向社会发出了一个强烈的信息，表明它们对消费者负有社会责任，并愿意保护社会免受危险品的危害。

19. 通过 Countercheck 平台，物流公司、知识产权权利人、海关和执法机构建立了联系，以便对造假者做出迅速有力的回应。通过人工智能技术有效识别可疑货物，知识产权权利人在专用在线平台上快速确认假冒产品（24 小时内），并与海关和执法部门的密切联系，这些都有助于供应链正当性。

20. 展望未来，我们预计公共和私营部门之间的合作会更加密切，因为这是打击知识产权犯罪取得成效的必要因素。值得注意的是，在假冒产品“碎片化”（即假冒产品以小批量、单独货物的方式运输，而不是批量运输）现象的背景下，我们预计可能会更民主地允许私营部门介入相关活动。

21. 我们还期待对过时的法律框架进行调整，减少影响销毁假冒商品时间表的过多预防措施，并为“国内”包裹流建立高效的打击假冒程序。

22. 最后，countercheck 解决方案提供的功能，如整个包裹流的综合风险分析、供应链的实时控制以及进一步调查犯罪网络的丰富情报来源，都是应对打击假冒商品新挑战的必要因素。只有品牌保护业界的所有利益攸关方联合起来，才能产生更强大的影响，以便创造一个安全的生态系统，让造假者无处藏身。

[稿件完]

音乐产业的人工智能：盗版者和权利人对人工智能的使用

撰稿：Graeme Grant 先生，环球音乐集团全球内容保护副总裁，荷兰希尔弗瑟姆 *

摘　要

本文概述了环球音乐集团（UMG）关于人工智能（AI）的看法，聚焦如何在知识产权（IP）侵权备受关注的情况下负责任地使用人工智能。作为音乐产业的领军者，环球音乐集团将人工智能引入各种应用，包括从营销手段到创意工具等各种用途。尽管人工智能具有巨大的创新和扩张潜力，但生成式人工智能不仅对创作者而且对更广泛的社会也构成巨大风险。例如，生成式人工智能的深度伪造和其他骗局也威胁着个人隐私和消费者安全。本文对越来越多的未经授权的活动进行了深入探究，比如，利用人工智能模仿艺人并生成虚假曲目，以及就音乐作品对人工智能平台进行未经许可的训练。数字平台上此类未经授权的使用越来越普遍，对知识产权执法构成挑战，并引发了人们对艺人作品未来完整性的担忧。环球音乐集团的结论是，如果能够负责任地使用，人工智能就能够对艺人的利益和创造性有利，如果不负责任地使用，则是重大威胁。

一、背景

1.　音乐是通过协调情感和表达来讲述的一段故事。词曲作者和艺人用自己的叙事和声音讲述各自的故事。他们借助自己的音乐分享我们大多数人永远也不会有的体验，并带我们去我们永远去不了的地方。他们的创造性对我们的生活而言就是原声音乐。如果没有版权的基本概念，我们可能不曾知道这些音乐。

2.　环球音乐集团拥有一系列广泛的音乐相关业务，其中包括录制音乐、音乐出版、音乐推销和视听内容等，并拥有涵盖每个音乐类型的海量音像录制品和歌曲的产品目录。它发现和培养艺人和词曲作者，并在全球制作和分销备受好评的畅销音乐。

3.　环球音乐集团致力于艺术性、创新和创业精神，推动服务、平台和商业模式的发展，以便为艺人拓展艺术和商业机会，为乐迷创造新的体验。

4.　就像过去几十年里对待其他技术创新那样，环球音乐集团欣然接受人工智能（AI）。它将人工智能用于营销和收集见解以增加艺人的受众数量，助力工作室的创作过程和制作最优化。事实上，环球音乐集团拥有多项人工智能专利。

5.　一些较新的人工智能技术，特别是过去几个月内迅猛发展的“生成式人工智能”技术，为创意界同时带来了机遇和重大风险。人工智能可以为那些渴望使用它的艺人提供增强人类创造性的最前沿工具。但是人工智能的一些用途会带来巨大风险。

6.　如果生成式人工智能技术的应用不尊重艺人的权利，就会给创意界及其创作的内容带来风险。

---

*　本文件所表达的观点为作者的观点，不一定代表产权组织秘书处或成员国的观点。

二、音乐产业内对人工智能的侵权使用

A. 未经许可训练人工智能平台

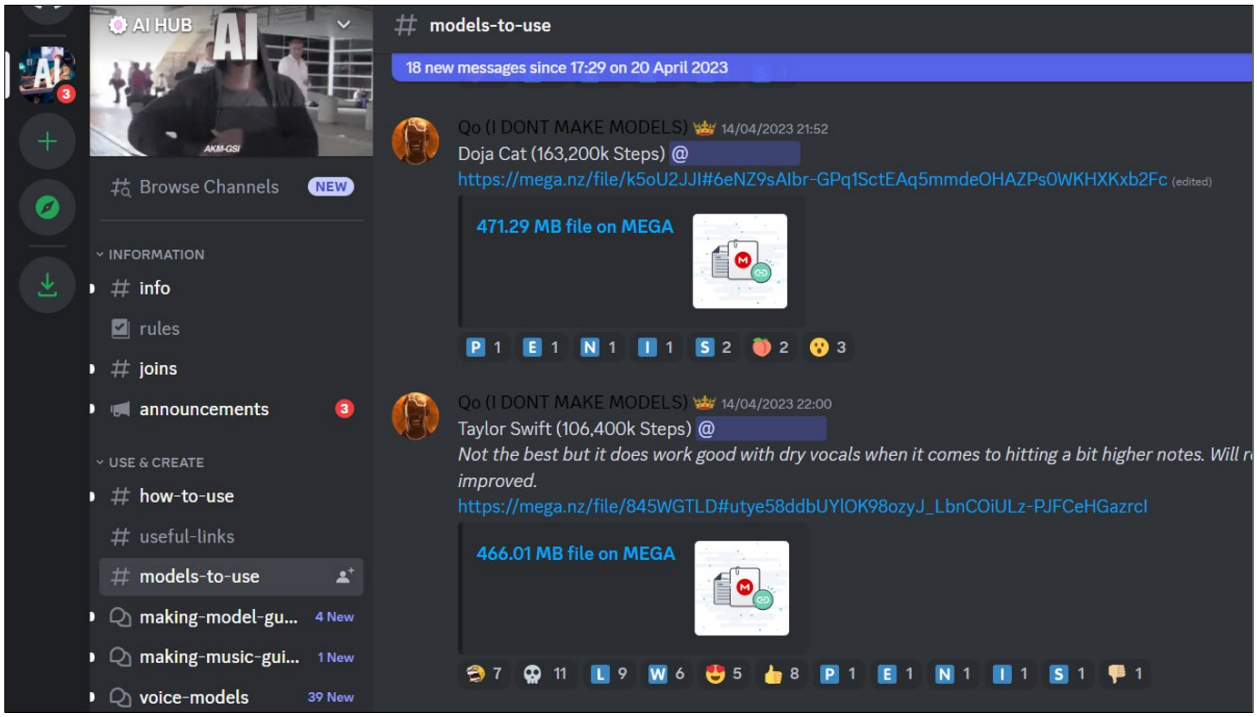
7. 一些人工智能平台正在就受版权保护内容接受非法训练，侵犯了创作者的权利。在接受这种训练之后，这些平台被用于利用这些内容创建作品，进一步侵犯此类权利。几乎在所有情况下，这些平台没有寻求授权，更不用说获得授权了。相反，它们在利用这些侵权行为推进自身业务时通常试图隐瞒自己对音乐作品的使用。

8. 在过去一年里，环球音乐集团注意到利用人工智能技术制作可以模仿艺人独特风格和声音的曲目明显增加。专门的在线社区正在兴起，它们不仅创建和分销这类虚假曲目，而且还提供指导人们完成这种未经授权活动整个过程的全面教程以及自动执行人工智能人声克隆过程的工具（比如机器人）。自 2023 年 8 月以来，用户生成内容平台上涉及我们的权利的人工智能生成内容上传量增加了 175%。截至目前，所发送的大约 47%的提示是由于在底层声乐或器乐中检测到环球音乐集团的原版录音而触发的；其余的则是违反了音乐/文学作品的版权、商标或公开权主张。

9. 被称作“声源分离器”的新兴技术正在利用人工智能技术将人声和器乐子总线从音频原版录音中分离出来（环球音乐集团借此技术为自己的艺人提供支持）。这些被分离出来的元素随后被用于训练复杂的人工智能模型。未经授权或未经许可而全部或部分地使用环球音乐集团的原版录音即为侵犯版权的行为。这种相对较新的侵权形式与流媒体翻录等较旧的做法沆瀣一气。流媒体翻录是将视听作品的音频成分提取出来（通常来自 YouTube 等授权平台）并进行复制。这种做法绕过了经许可的流媒体平台为防止擅自使用内容而采取的技术保护措施，并违反了平台的使用条款。随之而来的“翻录”内容被用作这些声源分离算法的输入项。

10. 人工智能创作者经常利用数字服务提供商（DSP）和用户上传内容（UUC）平台发布自己的作品并套现，这些内容通常包括未经授权使用受版权保护的作品（其中包括专辑封面、原版录音、乐曲、歌词）或者艺人的注册商标（比如艺人的姓名和标识）。尽管一些侵权者可能面临账户暂时停用和销户的情形，但他们时常可以建立新账户以持续开展非法活动。更为严重的是，这些侵权者为了不正当地大规模增加收入，不惜牺牲艺人和合法权利人的利益，通过人为地夸大播放次数和数据流进行流操控和版税欺诈。

11. 在前几个月，环球音乐集团关切地注意到从事知识产权侵权活动的社群通过改变技巧表现出极大灵活性。最初，在生成式人工智能侵权活动的初期增长阶段，如果有人未经授权将人工智能生成的人声混在我们的底层原版录音之上，我们有可能保证删除基于现有版权法所判断的未经授权内容。随着侵权活动的持续增多，人工智能已被用来制作含有某位艺人的人声克隆但在产品里原版录音并不那样明显的内容，从而为删除这种内容带来了更大难题。



B. 人工智能的人声模型

12. 一些人工智能人声模型已经就环球音乐集团受版权保护的音频录音、歌词和封面设计接受非法训练。此外，专门的音乐生成器也利用了环球音乐集团受版权保护的音乐作品。此类未经授权的活动经常依赖流媒体翻录手段。这些模型一旦接受了充分的训练，往往会通过 Discord 和 Reddit 之类的平台上的社交群体以及 GitHub 和 Hugging Face 等资源库进行传播，且经常伴有关于如何利用这些模型生成新的衍生作品的完整而全面的教程。

13. 图 1 显示的是未经授权使用环球音乐集团的一个作品搭建人声模型的情形。请注意歌曲的每一行已被分割成单个的声音文件，目的是将声音映射到具体的单词。

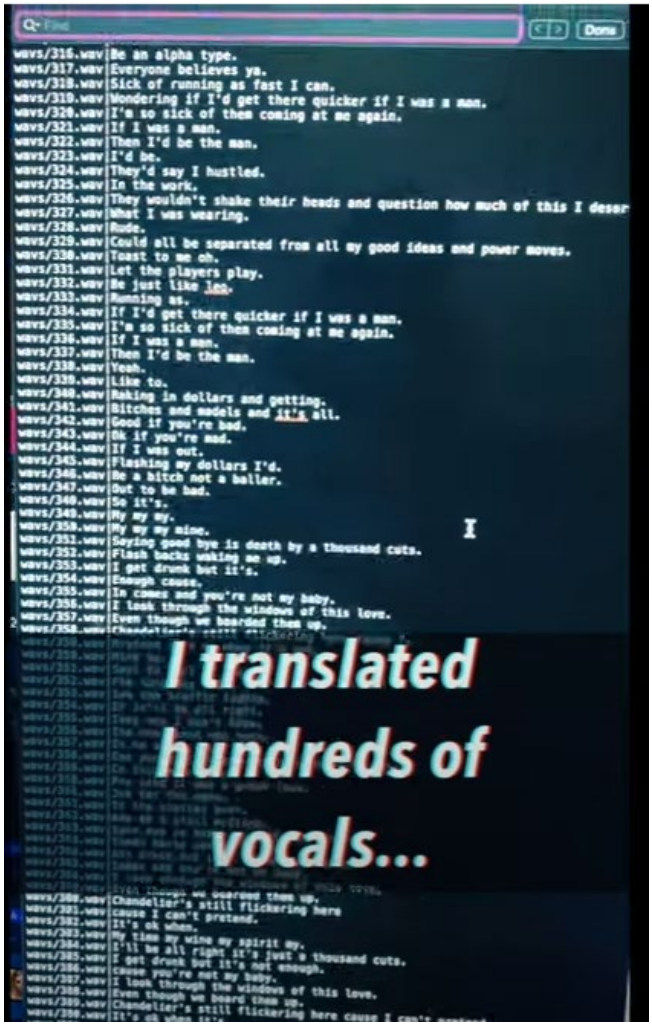


图 1 - 训练人声模型

14. 另举一例，一个在线社区创建了一个与特定艺人相关的、包含 100 多个预训练人声模型的电子数据表，这些模型已被上传到像 Megaupload 和 Google Drive 这样的服务项目中，可供 15,000 名会员中的任何人下载使用。

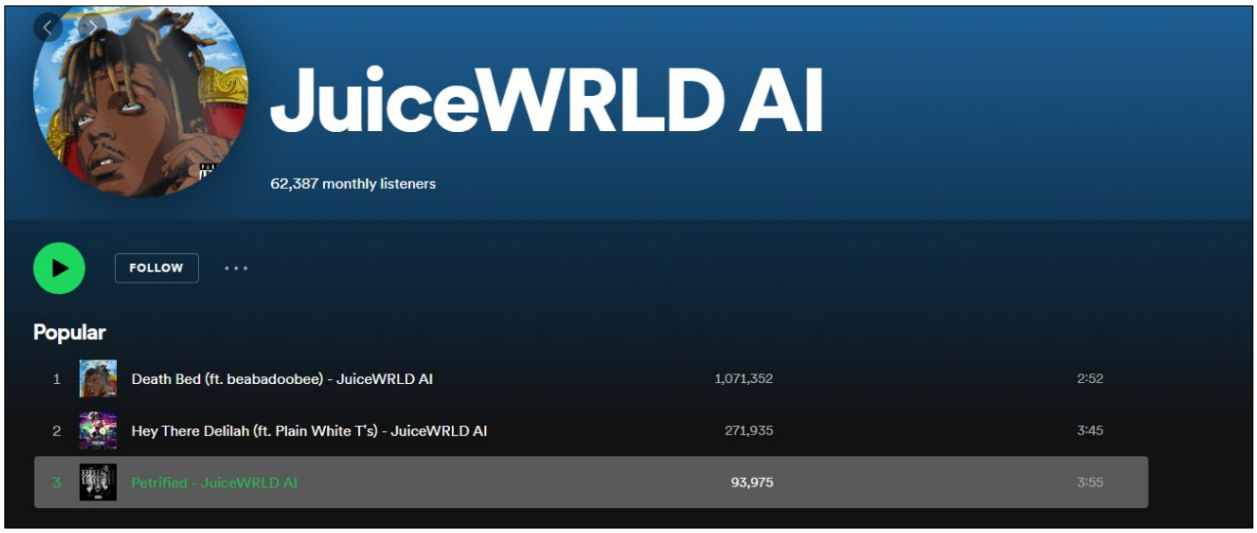
15. 此类人声模型被用来创建一首名为《Heart on My Sleeve》的虚假曲目，曲目模仿 Drake 和 Weeknd 的声音并被上传给数字服务提供商。原版曲目包含了一个由环球音乐集团控制并由 Metro Boomin 演唱的名为《No Complaints》的曲目的样本，该曲目因侵犯版权而被删除。删除了 Metro Boomin 的样本的新版《Heart on My Sleeve》随后被上传给数字服务提供商，但由于存在侵犯商标和名称、图像和肖像而被举报。

C. 虚假的预发行曲目

16. 骗子越来越多地利用人工智能声称他们拥有预发行曲目并随之进行售卖。这些人通常将人工智能生成的模仿环球音乐集团艺人声音的简短曲目片段上传到大众喜欢的泄密网站，并谎称通过黑客攻击、网络钓鱼或虚假陈述等非法手段直接从艺人那里获取了这些曲目。信以为真的用户经常进行“团购”，汇集财力满足骗子高达 5,000 美元到 30,000 美元不等的巨额要价。这些用户往往没有意识到相关曲目并非艺人作品，而是由人工智能创建的。

D. 数字服务提供商平台上的虚假曲目

17. 利用预训练人工智能模型创建虚假曲目的人将会利用 YouTube、Spotify、Deezer 或 Apple Music 等数字服务提供商创收。他们使用聚合服务将虚假曲目上传给数字服务提供商，并声称拥有全部权利，而不承认在已完成的曲目中或用于模仿艺人的人工智能模型中使用了任何受版权保护的内容。曲目在数字服务提供商平台的“播放量”所产生的版税从艺人和权利人处转移到虚假曲目上传者手中（参见下文的 JuiceWRLD 示例）。



18. 为了不让权利人和数字服务提供商发现，通常使用虚假的艺人简介（Juice AI、Drake AI）上传曲目。在 YouTube、TikTok 和 Instagram 等 UUC 网站上，使用真实艺人的姓名和/或标签上传曲目，以产生浏览量，并借此增加广告收入。

19. 在 6 个月内，一个服务提供商的人工智能每日上传量从大约 50 次到 400 多次，表明了问题的严重性。

E. 人工智能促成的网络攻击

20. 人工智能日益成为精心策划网络攻击的有用工具，代表着网络安全威胁的局面发生了转变。利用机器学习算法和其他先进的计算技术，恶意行为者可以将识别唱片公司的系统和网络漏洞的过程自动化，从而减少实施攻击所需时间和专业技能。这些攻击通常是为了获取待售的预发行作品，或者获得接下来用于训练人工智能模型和创建未经授权作品的子总线。

三、权利人对人工智能的使用

21. 在人工智能生成的、模仿环球音乐集团艺人 Drake 和 The Weeknd 的录音走红并引起媒体和政策制定者注意之前很久，环球音乐集团就已经在考虑人工智能的事情了。

22. 11 月份，披头士乐队的新唱片《Now and Then》发行，其中利用人工智能从旧的小样录音中提取出可以用在这张新唱片中的约翰·列侬的声音。

23. 环球音乐集团旗下的 Ingrooves 公司拥有三项与人工智能相关的协助推广独立艺人的专利。长期以来，人工智能也被用作录音室的工具，例如，借助苹果公司的 Logic Pro X 生成鼓轨或使用 Captain Plugins 创建和弦进行。环球音乐集团还经常将人工智能用于协助创建杜比全景声沉浸式音频音乐。

24. 环球音乐集团安保团队使用人工智能保护员工、艺人和利益相关者，使他们免受数量庞大、复杂性日益增加的网络安全威胁。

25. 环球音乐集团内容保护团队使用人工智能模型，基于曲目名称帮助进行侵权分类，基于元数据创建侵权评分，并利用图像识别侦测对我们的品牌和标识进行的实体假冒和未经授权使用。例如，侵权产品的出售者将会使用不同角度、不同尺寸、不同颜色或不同材料的原型图像。人工智能图像识别技术能够发现这些图像均基于相同的基本图像，因而提高了识别率。例如，人工智能具备搜索“Billie Eilish”商标并准确读取以下仿冒品图像中的文字的能力，尽管在示例 1 中存在视觉失真的情况。

示例 1

示例 2

26. 迄今为止，我们已经发现并删除了价值超过 4,500 万美元的 200,000 件假冒或未经授权商品。

27. 环球音乐集团技术团队使用人工智能，使环球音乐集团的产品目录更容易搜索和被发现，从而为内部团队提供支持，并增加环球音乐集团艺人的商业机会。

四、人工智能的监管

28. 如果能够得到负责任的使用，人工智能就是一项了不起的技术，同时它也是环球音乐集团在音乐发展的每个阶段都在使用的技术。

29. 国际上有关人工智能的公共政策仍处于起步阶段。美国、欧盟（EU）和英国正着手对人工智能进行监管。

30. 环球音乐集团赞同七国集团做出的承诺，包括 2023 年 5 月在七国集团广岛峰会领导人公报中做出的承诺。公报和声明强调（1）“多方利益相关者”参与制定优先考虑公平、透明和遵守现有法律的人工智能标准；（2）致力于“以人为本、值得信赖的人工智能”；以及（3）继续讨论和分析如何最大程度地保护知识产权（IP）权利，包括版权。

31. 欧盟《人工智能法案》包括政府在发行前对生成式人工智能模型进行审查、持续评估，以及记录保存条款、透明度和标示义务等方面的有益建议。该法案还承诺遵守七国集团宣布的多数广义原则，包括重点关注，除其他事项外，尊重知识产权权利的创作者主导、公平、透明的人工智能标准。目前，这项欧盟法案的最终版本正在三方磋商（“三方对话”）中讨论，环球音乐集团希望欧洲议会关于簿记和透明度的立场能够被采纳。

32. 生成式人工智能链中的关键机构有必要保留详细的记录，包括所使用的第三方材料、作品或其他受保护的主题内容的详细记录，以及访问的依据，并将这些信息提供给具有合法权益的各方。

33. 一些政策是应当避免的。一个例子是新加坡于 2021 年颁布的版权法的文本与数据挖掘例外条款。此外，日本于 2009 年推行并于 2018 年修订的立法也包含了一个有可能造成混淆的过于宽泛（尽管并非无限制且包括对权利人的某些保护）的例外。在一个生成式人工智能不受控制地吞噬巨量数据的世界，这种性质的例外与公平的基本原则和版权法奖励创造性努力的宗旨背道而驰。环球音乐集团感到高兴的是，去年英国明确拒绝了此类政策，因其承认例外将会对英国的创意产业带来不可挽回的损害。

34. 总之，环球音乐集团认为，现行的版权立法若得到恰当解释、适用和执行，则无需变更。但是，在特定领域可能需要额外的人格权（即声音和肖像）保护。

五、结论

35. 服务于艺人和创意的人工智能可创造出一些奇妙的工具，我们音乐创作中的每一步骤都在使用它们。环球音乐集团与无数负责任地使用人工智能的平台、公司、艺人和创作者携手合作。

36. 人工智能技术一旦被用于破坏对音乐的合理使用，未经许可摄取音乐从而不公平地影响乐迷们希望与现实生活中的艺人和创作者保持的那种关系，或者更糟糕的是，不经授权挪用他们的作品、姓名、形象、肖像或声音，则无助于音乐生态系统。

[稿件完]

美卡多公司使用人工智能检测和终止知识产权侵权

撰稿：美卡多公司机器学习交付与技术部机器学习经理 Gustavo Luis Bertelli 先生和法律与政府关系部品牌保护经理 Guadalupe Garcí a Crespo 女士，阿根廷布宜诺斯艾利斯 *

摘　要

全球有各种法律框架涉及限制互联网中介机构的责任，以及建立举报提供版权或工业产权侵权商品的投诉机制。但在拉丁美洲，只有少数几个国家通过了为此制定的法规。

这意味着，在该区域运营的电子商务平台在寻求防止列示假冒产品并维持高标准服务质量的方法时，必须应对自律和缺乏避风港的挑战。

此外，在这一领域实施行业最佳做法需要用人工智能模型对报告机制进行补充，以便在侵权商品被列示时主动自动检测。这就提出了一个额外的挑战，即分析知识产权权利人提交的报告，以建立一个可靠、持续和最新的侵权知识来源。本文件探讨了拉丁美洲的美卡多平台正在采取的方法。

在拉丁美洲，制定打击电子商务假冒商品列表的解决方案面临特殊挑战。本文无意详尽无遗，而是侧重于介绍美卡多公司开发的从参与成员网站上自动删除假冒商品电子商务列表的机制，并从法律和技术角度对其进行了审查。

一、拉丁美洲的监管框架和美卡多公司开发的报告机制背景简介

1.　关于互联网中介机构知识产权侵权责任的准则框架在拉丁美洲各国的演进方式各不相同。

2.　智利于 2010 年修订了第 17,336 号《知识产权法》，成为此类框架的第一个范例。除了引入删除版权侵权内容的司法通知制度外，该修正案还规定了司法外的申请，要求中介机构在被指控侵权时只有通知卖家的义务。从那时起，巴西、巴拉圭和其他国家都规定了对互联网中介机构责任的限制，主要要求通过司法通知来确定具体有效的信息，以便删除涉嫌侵权的内容。

3.　2020 年，墨西哥根据《美国、墨西哥和加拿大协定》修订了该国《版权法》，以效仿美利坚合众国根据该国 1998 年颁布的《数字千年版权法》（DMCA）建立的司法外私营部门机制。

4.　与此同时，各种司法裁决都采纳了通过识别被控侵权内容获得有效知识的标准，甚至在阿根廷等国，尽管没有关于这一问题的具体立法，但当地最高法院的判例法也承认了这一原则。

5.　在这一动态过程中，拉丁美洲和其他地区电子商务部门形成的良好做法逐渐取代了法律规定，为中介机构实施自愿和自律措施铺平了道路。

6.　这些自愿措施有时是与其他私营部门和政府机构协商制定的，其指导原则是不对中介机构强加一般性的监督义务。相反，这些措施依赖于知识产权权利人的知识和经验，他/她们致力于通过通知-删除机制行使自己的权利。

7.　在这一背景下，一般而言，知识产权侵权行为，尤其是在电子商务平台上列示的商标侵权产品，可以通过通知-删除机制来识别。就美卡多而言，这是通过一个名为“品牌保护计划”（BPP）的独家报告渠道来实现的，该公司向相关知识产权权利人提供这一渠道。

---

*　本文件所表达的观点为作者的观点，不一定代表产权组织秘书处或成员国的观点。

8. 然而，美卡多公司为打击假冒商品列表而开发的解决方案并不局限于这一单一的报告渠道。该公司推出了各种举措，从收到的报告中吸取经验教训，以便在没有具体报告的情况下发现侵权模式和删除欺诈性列表，有时还直接与特定的知识产权权利人合作。

9. 这与行业最佳做法以及所适用的法律和判例法的不断发展有关。从这个意义来说，通知-删除机制现在正得到电子商务平台（包括由美卡多在其运营的国家）主动努力的补充，以检测其网站上侵权行为的趋势和模式。

10. 为知识产权权利人开发这一报告系统的下一步工作，是教育其他平台用户现有知识产权的范围，以及如何在列示所销售产品时避免侵权，如何应对侵权指控，以及如何向知识产权权利人证明所提供的商品是真品。在美卡多平台上，一经提出侵权指控，就会触发立即暂停相关列示信息，卖家的上诉或回应都不足以重新激活这些信息。然后，知识产权权利人会分析卖家的答复，并决定是重新激活还是必须明确删除列示。已确定的删除随后可作为确定侵权趋势或模式以及决定制裁惯犯的依据。

11. 如今，鉴于拉丁美洲普遍缺乏有关互联网中介机构责任的法规，而且中介机构在寻求删除侵权内容的理由时也缺乏避风港，因此，知识产权权利人提交的报告发挥了重要作用，既可以作为作出删除决定的理由，也可以——以吸取的教训的形式——作为采取积极措施的基础。下一部分将探讨为此目的使用人工智能所产生的技术问题。

二、以人工智能作为检测假冒商品的工具

12. 根据世界知识产权组织的说法，“人工智能没有通用定义。它通常被认为是计算机科学中的一门学科，旨在开发各种机器和系统，这些机器和系统能够执行被认为需要人类智能完成的任务。机器学习和深度学习是人工智能的两个子集。近年来，随着新的神经网络技术和硬件的发展，人工智能常被视为‘受到监督的深度机器学习’的同义词。”[10]

13. 伊比利亚-美洲数据保护网引用英国皇家学会的说法，在其《关于人工智能个人数据处理的一般建议》中提供了如下解释：“虽然人工智能没有唯一定义，但可以肯定的是，在其丰富的概念中，人工智能是一个‘总括’术语，包括旨在提高机器开发算法、创建机器学习系统和达到深度学习技术能力的各种计算技术和程序。特别是，人工智能与算法的使用有关，算法是一组规则或一连串逻辑运算，目的是让机器做出决定或以确定的方式行事”[11]。

14. 像美卡多这样的平台所涉及的大量数据为人工智能的应用提供了多种机遇和挑战。如前所述，通过 BPP 收到的知识产权权利人报告不仅为人类用户提供了重要的经验教训，还可用于形成算法，以识别表明违规行为的模式和行为，在此情况下，违规行为包括列示销售的假冒商品。

15. 从数据量的角度来看，在撰写本报告时，美卡多在 18 个拉丁美洲国家运营平台，有 300 多万卖家使用，每秒产生 45 笔销售。

16. 在这样的平台上识别和删除假冒商品列表所需的工作需要多个团队，由具有不同背景和受过不同培训的个人组成，并需要使用多种流程——对这些流程的详细解释不在本文范畴内。在此仅介绍一

[10] 产权组织，人工智能与知识产权，见 https://www.wipo.int/about-ip/zh/frontier_technologies/ai_and_ip.html#accordion__collapse__01。

[11] 伊比利亚-美洲数据保护网（2020 年），《关于人工智能中个人数据处理的一般建议》，可查阅：https://www.redipd.org/sites/default/files/2020-02/guide-general-recommendations-processing-personal-data-ai.pdf。

些相关的标准和流程，以提供背景情况，让人们更好地了解如何利用人工智能和机器学习来检测假冒商品列表。

17. 困难主要来自三个方面。首先，被知识产权权利人认定为假冒商品的数量只占目前美卡多网站上列示商品微不足道的一部分：根据该公司最新的《透明度报告》[12]，2023 年上半年占比仅为 0.11%。这表明，如果知识产权权利人更积极地使用 BPP，从知识产权侵权报告分析中获得的信息水平会更高。

18. 其次，可作为检测假冒商品的过程中额外输入的变量之一是真品的市场价格，它为挑出价格明显偏低的列示商品提供了一个基准。至少作为第一步，与合理基准相比过低的价格通常表明存在假冒行为。不过，价格固然重要，但不能作为发现假冒产品的唯一依据。知识产权权利人有时也会提供临时折扣和/或促销，因此仅依据价格可能会产生误导。假冒商品的销售商也可能会与正品定价保持一致，以避免被发现或被消费者认为是假冒。

19. 最后，侵权者可能会试图通过修改产品描述或其列示商品的其他方面，使其与正品更为相似，从而逃避检测。这表明，在分析通过 BPP 收到的知识产权权利人的报告时，需要持续学习的系统来检测新的侵权趋势。

20. 目前正在构建基于监督式学习的预测分类模型，以应对此类情况，并根据列表标题、图片、产品商标参考、报告最多的产品类别、卖家行为和其他变量，建立具有侵权模式检测功能的算法。

三、结 论

21. 开发基于人工智能的自动流程有助于简化对大量信息的分析，并扩展通过人工修改内容获得的结果。对于在美卡多等电子商务平台上列示的假冒商品，我们的目标是增加删除此类知识产权侵权商品列表的数量。根据该公司的上一份《透明度报告》，通过使用人工智能主动删除的内容占因知识产权侵权而删除的全部内容的 87%，只有 13%的此类内容是根据特定知识产权权利人的报告而删除的。

22. 然而，侵权者不断借助日益复杂的做法，在网上列示假冒产品并冒充是正品。因此，知识产权权利人利用私营部门的侵权举报机制（如 BPP），对于有效打击假冒商品的网上销售仍然至关重要。

[文件完]

[12] 可查阅：https://www.mercadolibre.com.ar/institucional/comunicamos/noticias/transparency-report-first-half-2023。