OECD publishing

人工智能、数据治理和隐私

国际合作

OECD人工智能论文

2024年6月 第22

OECD

BETTER POLICIES FOR BETTER LIVES

前言

报告报告强调了关键的调查结果和建议，以加强人工智能，数据治理和隐私方面的协同作用和国际合作领域

本文件于2024年6月20日由经合组织数字政策委员会（DPC）通过书面程序批准和解密，并由经合组织秘书处准备出版。本文参考了经合组织人工智能专家网络的人工智能、数据和隐私问题专家组（以下简称"专家组"）的贡献它是在经合组织人工智能治理工作组（AIGO）和经合组织数据治理和隐私工作组的主持下编写的，这两个工作组都是

在发布时，专家组由Israeli Privacy Protection Authority（以色列隐私保护局），Denise Wong（新加坡信息技术媒体发展局（IMDA））和Clara Neppel（IEEE欧洲业务运营）共同主持专家组还受益于由Yordanka Ivanova（欧盟委员会），Kari Laumann（挪威数据保护局），Winston Maxwell（巴黎电信-巴黎综合理工学院）和Marc Rotenberg（人工智能和数字政策中心）组成的指导小组的投入和指导

报告的编写和起草工作由经合组织秘书处成员领导，关与该报告的主要贡献者Winston Maxwell（巴黎电信-巴黎理工学院）合作：数据治理和隐私部门负责人Clarisse Girot和人工智能部门负责人Karine Perset认可了两个工作组和相关政策社区共同努力的价值，并提供了资源，投入和监督。数字经济政策司的Gallia Daor和科学、技术和创新司副司长Audrey Plonk提供了建议和监督。

作者感谢那些抽出时间参加向专家组介绍情况的个人和机构所作的贡献。

最后，作者感谢Andreia Furtado、Marion Barclay和Shellie Phillips提供的行政和沟通支持，报告的整体质量得益于他们的参与。

人工智能、数据治理隐私：协同效应和国际合作**领域3**

各代表团注意

本文件也可在O.N.E上查阅，参考代码为：

DSTI/CDEP/AIGO/DGP（2023）1/FINAL

目录

表

缩略语和简称

AI	人工智能
DPA	数据保护机构
DPC	数字政策委员会
GPU	图形处理单元
HPC	高性能计算
信通技术	信息和通信技术
IGO	政府间组织
ML	机器学习
NGO	非政府组织
NLP	自然语言处理
经合组织	经济合作与发展组织
一个al	经合组织人工智能专家网络
豌豆	隐私执行机构
研发	研发
SDG	可持续发展目标
中小企业	中小企业
VC	风险投资
WPAIGO	人工智能治理工作组
WPDGP	数据治理和隐私工作组

摘要

最近的人工智能技术进步，特别是生成人工智能的兴起，引发了许多数据治理和隐私问题。然而，人工智能和隐私政策社区通常独立解决这些问题，方法因司法管辖区和法律制度而异。这些孤岛可能会产生误解，增加监管合规和执行的复杂性，并阻止利用国家框架之间的共性。本报告重点关注最近人工智能发展带来它将经合组织隐私准则中规定的原则与经合组织人工智能原则相结合，评估国家和区域举措，并提出潜在的合作领域。该报告支持经合组织隐私准则以及经合组织人工智能原则的实施。通过倡导国际合作，该报告旨在指导尊重和支持隐私的人工智能系统的开发。

缩写

国际审计领域的先进技术，特别是国际审计一般性的研究人员，提出了许多关于捐助者管理和保护私人生活的问题。然而，国际保护法共同体和保护堕胎者隐私的政策也需要采取各种独立的做法，采用不同的司法制度和司法制度。这些国家的主要障碍是遵守和执行规则的复杂性，以及在国家干部之间的共同点上实行资本主义。该报告集中讨论了保护国际法所涉受害者的私人生活所面临的风险和机会。通过比较《保护隐私权法》和《保护投资法》的原则，可以看出国家和区域的倡议以及合作领域的潜力。Le rapport soutient la decisionen Üuvre des Lignes directrices de l'OCDE relatives à la protection de la vie privee parallèlement aux Principes de l'OCDE relatifs à l'IA.在促进国际合作方面，该报告有助于指导建立尊重和支持保护个人生活的国际保障制度。

执行摘要

最近的人工智能技术进步-特别是生成人工智能的兴起-增加了与数据保护和隐私相关的机会和风险。作为一种通用技术，人工智能正在广泛应用并迅速渗透到全球的产品、行业和商业模式中。生成式人工智能的最新进展在很大程度上归功于存储在世界各地的大量训练数据的可用性和使用。与数据一样，人工智能生命周期中的参与者分布在不同的司法管辖区，这强调了全球同步、明确指导和合作努力的必要性，以应对人工智能对隐私的影响所带来的挑战

然而，人工智能和隐私政策社区目前倾向于单独解决挑战，没有太多的合作，因此他们的方法因司法管辖区和法律制度而异。例如，抓取个人数据以训练生成式人工智能的做法引发了重大的隐私问题，并因此引起了越来越多的监管关注。然而，关于使数据抓取实践与隐私准则保持一致的实际解决方案的讨论有限。同样，在生成人工智能的发展中，个人数据保护和隐私权的实际实施还没有成为集体深入反思的主题。随着越来越多的国家开始监管人工智能，这些社区之间缺乏合作可能会导致对数据保护和隐私法的实际范围的误解，以及相互冲突和/或重复的要求，这可能会导致监管合规和执法的额外复杂性。随着两个社区考虑对人工智能的机遇和风险的可能应对措施，他们可以通过加强合作，调整政策反应，提高人工智能政策框架与数据保护和隐私框架之间的互补性和一致性，从彼此的知识，经验和优先事项中受益

由于他们在历史，个人资料和方法上的差异，人工智能和隐私政策社区可以相互学习 近年来，人工智能社区，包括来自学术界、民间社会以及公共和私营部门的人工智能研究人员和开发人员，已经形成了充满活力和强大的网络。人工智能社区中的行为者采取了创新驱动的方法，而隐私社区则普遍采取了更为谨慎的方法，其标志是数十年来实施了长期的隐私和数据保护法。由于长期存在的隐私和数据保护法律，隐私社区通常也具有更成熟的特点，并随着时间的推移而发展，包括各种利益相关者，如监管机构，隐私和数据保护官员，技术专家，律师，公共政策专业人员，民间社会团体和监管技术提供商等。该社区专注于建立隐私保护措施，并在通常复杂和牢固的监管框架内评估风险。尽管存在这些差异，但协同作用仍然存在，合作至关重要。

本报告确定了可以进一步协同增效和互补中受益的领域，包括两个政策界之间的关键术语差异 它将现有的隐私和数据保护考虑因素映射到经合组织2019年关于人工智能的建议中规定的基于人工智能价值观的原则，以确定需要更密切协调的相关领域。这种映射说明了对

隐私和人工智能社区围绕关键概念-包括公平性，透明度和可了解这些差异对于建立可持续的合作行动至关重要。

人工智能和隐私社区的参与者已经在国家、区域和全球层面实施了措施，以应对人工智能带来的机遇和风险。该报告概述了国家和地区在人工智能和隐私方面的发展，包括隐私监管机构就隐私法对人工智能的应用以及相关执法行动提供的指导，特别是关于生成人工智能的指导。它发现，虽然已经采取了许多行动，包括隐私执法机构的政策举措和执法行动，但随着全球范围内出现专门针对人工智能的法律，它们可以从进一步的协调中受益

凭借其在人工智能、数据保护和隐私方面的国际影响力和实质性专业知识，经合组织似乎是加强该领域协同作用和国际合作领域的关键论坛它可以借鉴这两个领域的既定政策工作，包括1980年经合组织隐私指南（2013年更新）和2019年经合组织人工智能建议（2024年更新）此外，经合组织在2024年成立了一个独特的人工智能、数据和隐私专家组

尽管面临挑战，但这项政策工作和专家组内正在进行的活动都表明，广泛而持久的合作以及相互理解是可以实现的。为了为这些合作机会提供一个共同的参考框架，并突出经合组织的独特作用，该报告将经合组织人工智能原则（第一个关于人工智能的政府间标准）与完善的经合组织隐私指南（作为全球数据保护法律的基础）进行了协调。

该报告评估了与人工智能和隐私相关的国家和地区举措，并确定了合作，例如在隐私增强技术（PET）领域，这有助于解决隐私问题，特别是关于人工智能算法的人工智能、数据和隐私联合专家组