elastic

如何借助 Elastic 规模化推进 AI 合规工作

执行摘要

随着全球各国政府陆续出台针对人工智能（“AI”）在服务和工具中开发与使用的法律法规，各组织正采取适当措施，确保 AI 系统具备透明性、得到妥善的风险管理，并符合相应的法律要求。Elasticsearch Platform 可帮助企业客户建立全面的管控机制，监测 AI 部署、开展影响评估，并推动构建更值得信赖的生态系统。本白皮书将探讨 AI 治理的关键议题，从理解透明度要求，到以合乎伦理的方式利用数据进行模型训练。我们将提供一份路线图，帮助您的企业应对监管预期，并更有信心地推进创新。我们还将介绍 Elastic 强大的平台如何帮助您跟踪和管理在适用 AI 法律下自身需要满足的合规要求。

请注意：*本白皮书仅供参考，不构成法律建议。*
请咨询您的法律顾问以获取专业法律意见。

全球 AI 法律背景概述

过去几年，全球 AI 监管格局发生了显著变化，世界各地相继出台新法律，对 AI 的开发、应用和监督加以规范。生成式人工智能（GenAI）和大语言模型（LLM）的迅速兴起，让组织和消费者能够以全新且具有变革性的方式利用数据。随着这些技术持续演进，其动态特性也自然引发了人们对其法律、伦理和实际影响的讨论。

尽管世界各地的 AI 法律存在一些关键差异，但它们在许多原则上是相通的。其中较具代表性的例子包括欧盟《AI 法案》、韩国《AI 基本法》、巴西《AI 法案》、科罗拉多州《AI 法案》、加利福尼亚州《AI 透明度法案》、加利福尼亚州基于现行 CCPA 隐私法制定的自动决策技术相关法规，以及犹他州《AI 政策法案》等。除这些现行立法举措外，国际和国家层面的自愿性框架，如《经合组织 AI 原则》、澳大利亚《AI 安全标准》、新加坡《模型 AI 治理框架》，甚至与客户和最终用户签订的合同，也可能对数据使用和处理活动施加额外义务。

为了应对这些要求和期望，组织可以有策略地借助 Elastic，更有效地跟踪、管理并提升 AI 法律合规水平。选择 Elastic 作为合作伙伴，我们将助您打造一个负责任、可持续的 AI 创新未来。

人工智能和机器学习

过去几十年间，AI 取得了长足进步。早期 AI 系统依赖基于规则的程序，按照明确指令执行范围狭窄、定义清晰的任务。随着时间推移，机器学习逐渐兴起。作为 AI 的一个子集，机器学习让计算机系统无需显式编程，便可运用统计技术从数据中“学习”并持续优化性能，从而推动这一领域发展出能够执行自然语言处理、图像识别和自动决策等复杂任务的先进模型。

尽管不同法律和行业指南对 AI 的定义并不完全一致，但欧盟《AI 法案》提供了一个有益的起点。它将 AI 系统描述为：使用机器学习、基于逻辑的方法或统计方法开发的软件，并针对一组由人类设定的目标生成输出——包括预测、建议或决策——而这些输出会对现实或虚拟环境产生影响。这一领域中的一个重要发展就是 GenAI，这是一种通过文本、音频或视觉通信与用户互动，并处理这些通信以生成特定目标输出的系统。从僵化、受规则约束的流程，演变为动态、数据驱动的学习系统，这一变化从根本上重塑了利用数据开展 AI 应用的可能性。

开发者与部署者

在快速演进的 AI 生态系统中，开发者与部署者扮演着不同但彼此关联的角色。监管提案和法定框架（如欧盟《AI 法案》和美国部分州法）通常将“开发者”定义为设计、创建、训练和维护 AI 系统的个人或实体。他们的职责通常涵盖系统的技术和理论基础，包括算法设计和模型训练。

相比之下，“部署者”通常指确定 AI 系统预期用途，并将其集成到产品、服务或运营工作流中的个人或组织。部署者通常负有责任，确保其实施的 AI 系统符合公平性、透明度、安全性和问责制等既定标准。

AI 的生命周期由*开发者与部署者*共同界定，涵盖从概念设计、开发到现实应用的全过程，这也凸显了在 AI 系统实施中明确责任的重要性。

自动化决策与画像

除了专门规制 AI 技术的法律之外，越来越多的法律还禁止以可能导致非法或不公平歧视的方式使用自动化决策技术（包括 AI），即使这种歧视并非有意为之。例如，伊利诺伊州法律对 AI 的使用设置了限制，以防在人员招聘和留任过程中基于受保护特征产生歧视。同样，纽约市第 144 号地方法对某些会显著影响就业决策的“自动化就业决策工具”进行监管，并要求开展偏见审计等。

此外，还有其他拟议中的法律和法规针对那些生成简化输出、用于辅助或替代人类酌情决策的 AI 系统，例如评分、分类或推荐。

另一方面，若此类系统涉及个人数据，欧盟 GDPR 等隐私法律还会对旨在评估、分析或预测个人特征、行为、经济状况、健康、个人偏好或兴趣的自动处理施加限制和义务。

基于风险的 AI 立法路径

许多新的 AI 法律采用基于风险的框架，按照 AI 应用可能造成的潜在危害对其进行分类。例如，欧盟《AI 法案》将 AI 应用划分为不可接受风险、高风险、有限风险和最低风险几类，其中工作场所情绪与情感分析等系统被明令禁止。同样，在科罗拉多州以及美国其他拟议法规中，也强调对特定 AI 部署相关风险的评估。这表明，针对 AI 特定应用进行监管正成为日益明显的趋势，尤其是在相关决策可能对群体或个人产生重大影响的情况下。

AI 基本原则

在人工智能法律颁布之前，行业标准和最佳实践自然而然地出现，用以指导负责任的人工智能开发和部署。这些自律措施由行业参与者、标准制定组织和学术研究人员共同提出，旨在解决人工智能技术及其部署快速发展所带来的伦理和运营问题。从这些早期努力中出现了一些关键原则，以确保 AI 系统以可理解、公平且可问责的方式运作。

1

透明度

这一原则强调应公开 AI 系统的设计与运作方式，包括数据来源、方法和决策过程，以便用户和利益相关者能够理解并信任该系统。

2

可解释性

这意味着 AI 系统需要对其输出或决策给出清晰、可理解且可解释的说明，以便开发者、监管者和用户能够追溯并评估其结论背后的逻辑。

3

防范 AI 偏见和算法歧视

这一原则承认在 AI 系统的数据或设计选择中可能出现的非法或不公平偏见可能导致的不公平结果。它强调了确保技术不会以不公平或非法的方式系统性地使特定群体或个人处于不利地位的重要性。

这些原则通过强调以负责任的方式整合 AI 的伦理要求，为后续法律框架奠定了基础。

企业不遵守 AI 法规的成本

未能遵守日益增多的 AI 法规，不仅仅是合规上的疏漏；它还可能对组织的财务稳定性、市场地位和长期生存能力构成现实威胁。尽管相关法规仍在不断发展演变，但现行法规中的处罚之所以故意设置得较为严厉，正是为了反映未经监管的 AI 系统可能造成的重大社会和经济损害。例如：

- **《欧盟 AI 法案》**规定，对于与高风险或不可接受风险 AI 系统相关的违规行为，最高可处以公司全球营业额 7% 或 3500 万欧元的罚款，以较高者为准。对于营收数十亿欧元的跨国公司而言，这样的罚款可能高达数亿甚至数十亿欧元，并对其盈利能力、投资者信心和市值构成重大威胁。该法案项下的其他违规行为最高可处以 3% 的罚款，提供错误信息的行为最高可处以 1.5% 的罚款。《欧盟 AI 法案》还具有域外效力，这意味着任何在欧盟市场提供 AI 系统的供应商，无论实际所在地在哪里，都必须遵守该法案。

- **巴西《AI 法案》草案**不仅拟规定最高 5000 万雷亚尔（约 900 万美元）的经济处罚，而且还拟赋予监管机构暂停不合规 AI 服务并责令系统整改的权力。

- **《科罗拉多州 AI 法案》**认为，在高风险 AI 系统中未尽“合理注意义务”以避免算法歧视，属于不公平贸易行为；每次违规最高可罚 2 万美元，若针对老年人实施，每次违规最高可罚 5 万美元。

- 《**加州 AI 透明度法案**》对受影响的提供商每日每项违规行为最高可处以 5,000 美元罚款，在某些情况下还可能采取禁令救济措施。“每日”处罚意味着补救延迟或持续不合规可能迅速演变成毁灭性的财务负担。

- **《犹他州 AI 政策法案》**对每次违规行为最高可处以 2500 美元罚款，并允许采取其他救济措施，例如禁令或追缴违法所得。持续性违规可能导致每次违规处以 5000 美元罚款。即使违规输出是由生成式 AI 直接产生，公司仍需对其生成式 AI 应用造成的违规行为负责。这实际上将合规责任完全转移到了部署组织身上。

除了可量化的经济处罚外，不遵守AI监管法律还会带来无形但同样影响深远的代价。品牌声誉受损、客户和利益相关者信任的丧失以及运营效率低下，可能导致长期市场劣势，阻碍增长和创新。

此外，在金钱处罚或禁令不足以应对的情况下，美国联邦贸易委员会（FTC）及其他执法机构还可以采取“算法追缴”措施，要求组织不仅删除非法获取的数据，还必须删除任何依赖这些数据的算法或模型。随着 AI 在业务运营中日益重要，不合规带来的财务和战略影响也在不断加剧。

Elastic 如何助力企业简化 AI 法律合规工作

作为创新 AI 解决方案领域的领导者，Elastic 致力于开放的开发流程，并以透明、直接的方式与社区互动，同时也致力于构建透明、负责任且可解释的系统。这一承诺让客户能够更有信心地管理自身数据，同时稳健满足不断演变的 AI 法律标准。Elastic 提供了一整套全面能力，可直接应对新监管环境带来的核心合规挑战。借助 Elastic，您可以将复杂的合规要求转化为更简洁、更自动化的流程。

从过去几年涌现的 AI 法律中，可以看到一个明显趋势：防范 AI 可能带来的潜在危害，无论这些危害涉及透明度不足、算法中的非法或不公平歧视与偏见，还是更广义的自动化决策问题。尽管许多法律框架早已对 AI 解决方案所处理的底层数据作出规范，但直接规制技术本身，或规制设计和/或使用此类解决方案的公司的法律，却少之又少，甚至几乎没有。

因此，要遵守全球 AI 法律，就必须了解组织数据所处和流转的整个生态系统，以及这些数据还会如何被处理。Elastic 可以帮助客户简化并自动化这些流程，从而为您的合规框架提供支持。

下表梳理了 Elastic 如何帮助组织应对各类 AI 合规场景：

AI 合规性挑战	核心监管需求	Elastic 功能	主要优势
透明度	通知与披露	集中式日志、指标、审计跟踪	展示数据流和决策流程，简化调查
文档和数据清单	数据清单	数据映射与分类	实现数据治理自动化，确保报告的准确性
识别风险	持续监测	实时警报与分析	主动调整风险控制措施，动态实施管控
进行影响评估	算法歧视防范	搜索功能、数据血缘跟踪	简化评估流程，确保基础合规性
AI 素养与政策	培训	全面的培训平台	将 AI 知识转化为实际运营能力，赋能员工开展监督工作
提供用户选择	个人权利请求	数据映射与分类	更快地响应请求，简化个人权利管理

透明度：使用 Elastic 满足通知和披露义务

AI 系统本质复杂，确保透明度（无论是法律、监管还是合同义务）对于建立用户、监管者和利益相关者的信任至关重要。例如，欧盟《AI 法案》等法规要求组织就数据使用情况和模型决策过程提供说明。虽然欧盟《AI 法案》及其他地区的通知要求会因相关行业或 AI 类型而异，但大多数法律都规定了一般性义务：在终端用户与 AI 互动时告知其相关情况，并在特定情形下向用户发出清晰通知，同时维护用于训练模型的数据清单。一般来说，一些新兴框架（如加利福尼亚和科罗拉多州）可能还要求在使用前，甚至在某些情况下，在对最终用户作出重大决定前发出通知。在这套日益复杂的法律拼图中，理解并能够说明相关数据及其处理过程的义务，在美国和欧盟法律中始终是一项共同要求。

Elasticsearch Platform 集中管理各个环境中的日志、指标和审计记录，从而实现实时监控和历史可追溯性。这有助于客户说明数据如何流经其 AI 系统，以及系统如何基于这些数据作出决策。具体而言，客户可以借助 Elastic 实施相关措施，以帮助满足这些透明度义务。

例如，Elastic 客户可以：

- 整合运营、AI 应用和用户交互中的多样化数据源，更好地掌握其数据清单，以便识别、分类并评估用于训练、测试和验证等用途的数据
- 通过维护记录数据沿革和模型活动的日志，形成审计追踪能力，用于取证分析和合规报告
- 利用 Kibana 等工具创建仪表板，帮助用户通过搜索、聚合和可视化分析 AI 如何作出特定决策，从而简化数据调查

Elastic 的客户可以从其 AI 应用中摄取和存储详细日志。这些日志可能包括 LLM 提示、响应以及任何错误或异常。这些数据对于了解 AI 系统的行为至关重要。

Elastic 强大的搜索功能使客户能够索引和搜索大量的结构化和非结构化数据，包括技术文档、培训数据详情和操作日志。

Elastic 客户可以通过 Kibana 中的定制仪表板访问实时监控，以跟踪其 AI 系统的性能。日志分析、异常检测和模式分析等 Kibana 功能可以帮助跟踪 AI 系统行为。这有助于识别可能需要披露的异常或意外行为。

详细了解 Elastic 如何助力 Comcast 将数据趋势和异常可视化，并在团队之间共享洞察。

文档与数据清单：借助 Elastic 推动 AI 系统的合规使用

在透明度方面，欧盟 AI 法案和美国某些州法律（如加利福尼亚州的相关法律）要求维护并发布与特定 AI 系统有关的文件。例如，自 2026 年 1 月 1 日起，加州 AB 2013 要求 AI 开发者在向消费者开放生成式 AI 系统之前，必须在其网站上发布相关文档。根据加利福尼亚州法律，开发者指的是“设计、编码、生产或实质性修改” AI 系统的企业。其中，这些文档需对用于开发生成式 AI 系统的数据集提供高层次概述，包括数据集来源、数据集如何支持实现该 AI 系统的目标，以及数据集是否包含汇总信息或个人信息。

如上所述，Elastic 可通过有效的数据映射帮助您评估自身数据——其中也包括您如何调整我们的搜索体验，以便更好地为终端用户定制解决方案。此外，我们帮助客户集中管理、标记并理解其数据，让他们能够识别适用于特定数据的义务——无论这些义务来自法律、合同、信托责任还是保密要求。

详细了解 Elastic Security 如何助力 Sitecore 集中管理数据，并自动化多达 96% 的安全工作流。

识别与您的数据及潜在 AI 用例相关的风险

由于新兴的 AI 法律会根据数据类型和用例规定不同要求，因此，理解、管理和保护您的数据比以往任何时候都更重要。

借助 Elastic 的持续监控能力，客户能够评估与其数据及其潜在用途相关的风险，从而在风险水平随时间变化时更有效地调整控制措施。例如，根据适用法律，高风险 AI 系统（例如那些用于作出医疗或法律决策的系统）会受到更严格的控制。Elastic 通过提供实时告警、可定制仪表板和详细分析，支持客户落实风险管理框架，让用户能够围绕如何应对（及补救）AI 系统（包括我们的搜索功能）可能带来的潜在危害，设定相应规则和参数。

详细了解 Ernst & Young 如何借助 Elasticsearch Relevance Engine 提高准确性，并加快从非结构化数据中检索对合规和创新至关重要的关键洞察。

进行影响评估

类似于某些隐私法律项下开展数据保护影响评估的既有义务，欧盟和科罗拉多州等地的新兴 AI 法律要求 AI 部署者进行影响评估，这对高风险应用尤为重要。这些评估通常需要记录 AI 用例的关键细节，包括系统情况、用途、所使用的数据、预期收益、算法歧视风险、保障措施以及部署后的监控。

Elastic 帮助客户明确何时以及如何开展这些影响评估。尤其是，了解数据的存储位置、处理方式以及流向，有助于简化影响评估的完成过程，而传统上，完成此类评估往往需要跨业务部门的多职能支持，以便厘清个人数据的使用情况。这些影响评估既能体现基础合规能力，也能帮助组织将数据处理限制在适用法律授权的范围内。

详细了解制药公司如何使用 Elastic，帮助研究人员和合规团队生成从数据摄取到搜索全过程的使用报告，并简化向监管机构履行报告义务的流程。

实施 AI 素养和风险管理政策及程序

根据《欧盟 AI 法案》，AI 提供商和部署者应采取措施，确保参与 AI 运营和使用的员工具备足够的 AI 素养（尤其是那些行使人工监督职能的个人）。此外，AI 素养方面的要求还意味着，组织应开发并实施有针对性的培训计划，确保员工理解所部署 AI 系统带来的机遇、风险和局限性，并进一步具备识别和减轻潜在危害的能力。这一要求与其他地区的相关规定相辅相成，例如科罗拉多州要求实施风险管理政策和计划，以应对潜在的算法歧视问题。

Elastic 帮助客户明确并记录他们认为适合特定用例的 AI 素养要求。Elastic 还可以通过全面的培训平台、技术专长和集成数据解决方案，帮助客户满足这些要求，尤其是通过我们丰富的按需培训资源和虚拟讲师授课课程——涵盖机器学习和 AI 的高级主题。培训订阅提供大量实操练习，让抽象的理论落地，帮助学员更具体地理解 AI 处理流程。

为用户提供选择

许多 AI 法律（以及影响特定 AI 部署的相关法规）要求组织为用户提供清晰的选择，让用户了解其数据如何被使用，以及相关决策如何作出。例如，相关法规可能要求就用户画像和自动化决策过程保持透明，用户也可能有权选择退出或要求人工干预。

Elastic 的数据映射功能是组织处理数据主体请求的核心基础。具体而言，企业可借助 Elastic 的数据映射与分类功能，快速判断此类请求是否有效，并按要求作出适当响应，从而节省宝贵时间，帮助合规团队在法律规定的较短时限内完成处理。

减少算法歧视并开展偏见审计

AI 系统依赖大量训练数据，而这些数据的质量、多样性和来源会直接影响 AI 结果的公平性和可靠性。法规越来越关注训练数据的来源和偏见，以确保 AI 部署符合伦理要求。

Elastic 平台可以从多种来源摄取和索引数据，包括日志、训练数据以及机器学习模型的输出。由于 Elastic 能够在无需移动或重新加载数据的情况下，对各类数据进行搜索和分析，组织就可以在一个平台中汇集完整决策链上的数据——从输入数据一直到最终结果。Elastic 平台允许客户查询、探索并可视化数据集，以评估其构成，并识别可能影响 AI 系统性能和公平性的潜在偏差或数据缺口。

此外，通过使用 Elastic 强大的 查询 DSL，组织可以过滤并深入挖掘数据，以比较不同人口群体之间的结果。例如，客户可以执行聚合查询，以检测算法的决策是否不成比例地影响某些人群。

Elastic 助力客户维护详尽的数据及来源记录，形成对数据的全局视图，让决策过程更加透明、可追溯。

结论

与 Elastic 携手，掌控 AI 合规的未来

理解您的数据以及技术如何作出决策，正日益成为行业最佳实践，也逐渐成为法律层面的要求。能够大规模满足日益增长的 AI 相关要求，预计将成为市场差异化因素，并为组织的战略成功提供支撑。Elastic 简化了这一流程中的关键步骤，让您在合规方面掌握主动权。Elastic 将监管挑战转化为战略优势，帮助组织在降低风险的同时，以更负责任、更有信心的方式推进创新。