**立法背景**

随着智能化社会的迅速发展，全球范围内的国家纷纷加强对人工智能技术的研究与应用布局，人工智能技术已广泛应用于交通、教育、服务等多个领域，但随之而来的安全问题也愈发显著。

当前，人工智能面临着包括数据风险（数据投毒、泄露和异常）、算法风险、网络风险等多种挑战。此外，人工智能在处理复杂问题时可能带入种族和性别歧视的偏见。

例如，COMPAS 是一种在美国广泛使用的算法，通过预测罪犯再次犯罪的可能性来指导判刑，而这个算法或许是最臭名昭著的人工智能偏见。根据美国新闻机构 ProPublica 在 2016 年 5 月的报道，COMPAS 算法存在明显的「偏见」。根据分析， 该系统预测的黑人被告再次犯罪的风险要远远高于白人，甚至达到了后者的两倍。

强化人工智能的安全问题已成为国际间共同关注的重点。全球主要经济体纷纷推出针对人工智能发展的政策和立法措施，以确保这一领域的健康与安全发展。

1. 2017年，中国国务院发布《新一代人工智能发展规划》，强调了建立健全的人工智能相关法律、伦理和社会问题的研究，提出建立一套完善的法律法规和伦理道德框架以及人工智能安全监管和评估体系的必要性，以保障人工智能技术的健康发展。
2. 美国在2016年和2019年分别发布了《国家人工智能研发战略规划》及其更新版，其中将人工智能安全建设作为国家战略的重要方向之一。这些文件体现了美国在确保人工智能技术发展同时，对潜在风险的防控给予高度重视。
3. 欧洲联盟在2021年迈出了更为具体的步骤，发布了《人工智能法案》（Artificial Intelligence Act）。

欧盟意识到单一国家的法规措施可能无法充分应对当下人工智能技术带来的挑战，因为AI的跨界性质和内部市场中产品与服务的自由流通特点使得单一国家的法规可能导致市场碎片化，增加法律不确定性，阻碍技术的均衡发展。

各成员国法规的差异可能会造成AI系统的使用、责任、监管等方面的不一致，给AI提供商和使用者带来合规成本和法律风险。

**立法目的**

1. **建立统一的法律框架**: 通过建立一个统一的法律框架，解决欧盟成员国间在人工智能领域法规的分散性和法律不确定性问题。这一框架的建立旨在促进人工智能技术在整个欧盟范围内的健康发展，确保内部市场的正常运作，并确保人工智能系统相关产品和服务在整个欧盟内的无缝流通。
2. **保护成员国间的基本权利**: 该法律框架保证了在欧盟各成员国之间基本权利的一致尊重和保护。这包括个人数据保护、消费者权利和隐私权等核心价值。
3. **促进AI技术的接受度**: 统一规则的确立使人们和其他用户对基于人工智能的解决方案有更多的信心。这种信任是推动人工智能解决方案广泛接受和应用的关键因素。
4. **激励企业创新与开发**: 统一的法律环境为企业提供了一个更稳定和可预见的法律环境，从而鼓励企业投入资源进行人工智能技术的研发和创新。这不仅有助于技术进步，也促进了新技术的商业化。
5. **增强内部市场的效率与竞争力**: 通过消除内部市场中的法律壁垒，统一法律框架有助于提高市场效率，增强欧盟内部市场的全球竞争力。这样的市场环境有利于吸引更多的投资，推动经济增长。

**监管框架**

* 在AI监管主要存在“横向”监管与“纵向”监管两种主要方式：
  + 在横向监管方式中，监管机构将创建**全面的法规**，以尽可能涵盖AI可能产生的各方面影响；
  + 在纵向监管方式中，政策制定者采取**“定制”**的方法，针对不同应用或类型的 AI 制定不同的法规。
* 《人工智能法》采用横向监管模式。该法案以风险分级的方式将所有 AI 系统纳入监管范围，并允许监管机构随着 AI 的发展不断将新的应用领域纳入现有的风险类别，而没有针对特定AI应用领域制定具体的法律规范。
* 风险分级方式使法案整体处于相对灵活的状态，既能够保持横向监管方式具有的统一性和协调性，同时也弥补了监管方式下对具体 AI 应用场景针对性不高的问题。

对于多AI耦合系统，当较高风险与较低风险的AI系统同时存在时，采用“就高不就低”的原则，对风险进行较严的监管规制。

不同风险级别的AI系统对应不同的监管措施，高风险意味着更严格的监管。这种灵活的分类方法覆盖了所有AI系统，并随技术发展持续更新。该方法针对不同应用场景设定了具体监管措施，避免了规制失焦并为复杂场景提供了清晰的监管框架。

法案对知识产权的保护也给予了充分重视：

第79条：国家监督机构应将其获取的任何信息，包括源代码、软件和数据（如适用）作为机密信息处理，并遵守欧盟关于保护知识产权和商业秘密的相关法律。

第83条：参与该条例应用的所有相关方应致力于确保活动的透明性和公开性，同时也需要保护在执行任务过程中获取的信息和数据的保密性，通过制定技术和组织措施来确保信息的安全性和保密性，包括知识产权以及公共及国家安全利益。

对知识产权的保护不仅是对创新活动的激励，也是推动科技发展和进步的关键因素。《人工智能法》在完善监管措施的同时，基于对个人基本权利的保障，努力实现 AI 技术的可信赖性与 AI 技术发展之间的动态平衡。

**法律责任**

**（一）投放市场前**

**1. 确保高风险AI系统符合相关技术要求的义务：**根据《AI法案》第二章的规定，投放市场或投入使用的高风险AI系统应具备的要件，可进一步细化为基于风险动态变化形成的风险管理体系需求，基于核实验证目的形成的技术文档需求，以及基于减少数据训练引发的算法偏见与歧视等问题形成的数据质量需求。第三章则规定，在相关系统投入使用前，提供者需确保其提供的高风险AI系统已具有上述能力或履行相关要求。

**2. 构建质量管理体系的义务：**《AI法案》2023年折衷草案第17条第（1）款规定，高风险AI系统提供者应建立、实施质量管理体系。具体而言，提供者应通过书面文件的形式（如政策、程序或指令等）系统有序地记录其检测和验证程序、适用的技术规范、数据管理体系、风险管理体系、系统投放市场后监测机制、事故和故障报告、监管配合、问责框架等。

**（二）投放市场时**

**1. 履行符合性评估义务：**《AI法案》对高风险系统采取了事前评估的监管方式，规定在将高风险AI系统投放市场或投入使用前，提供者或第三方评估机构应当进行针对高风险AI系统的符合性评估。2023年《AI法案》折衷草案第43条详细规定了开展符合性评估的规则，其本质是为验证相关条款、对高风险AI系统的有关要求是否得到满足的过程。

**2. 高风险人工智能系统备案义务：**根据《AI法案》提案第51条规定，高风险AI系统投放市场或投入使用前，应在欧盟委员会主导建立的欧盟公共高风险AI系统数据库中备案。折衷草案相较而言，除了新增了特殊部署者的备案义务，还进一步补充了在AI系统发生实质变更时的重新备案义务。

3. CE标识标志义务：对于前述符合性评估的认证，《AI法案》自2021年提案起，即引进了欧盟合格认证（Conformité Européenne, “CE”）机制。对存在高风险的AI产品和服务，经评估程序被认定合格后，可贴上CE标志投入使用。

**（三）投放市场后**

**1. 部署风险监测系统的义务：**根据《AI法案》2023年折衷草案第61条规定，高风险AI系统提供者应采取与AI技术和高风险AI系统相称的方式，建立并执行上市后的监测系统。此监测系统应具有收集、记录和分析由部署者或其他来源提供的有关高风险AI系统在整个生命周期内的性能的相关数据。

**2. 采取纠正措施等义务：**根据2023年《AI法案》折衷草案第21条和22条，如果高风险AI系统的提供者认为或有理由认为其投放市场或投入使用的高风险AI系统不符合《AI法案》的要求，应立即采取必要的纠正措施。

**3. 配合监管部门开展工作的义务：**《AI法案》作为一项欧盟范围内的立法，将对每个欧盟成员国产生法律约束力。在各阶段的草案中，《AI法案》均提出各成员国须建立相应的国家监管机构，以监督《AI法案》的规则在国内的应用和实施。相应的，提供者也设有需要配合上述监管机构开展工作的义务。