



REPÚBLICA DE ANGOLA

PROPOSTA DE LEI SOBRE A INTELIGÊNCIA ARTIFICIAL

**PROPONENTE: MINISTÉRIO DAS TELECOMUNICAÇÕES,
TECNOLOGIAS DE INFORMAÇÃO E COMUNICAÇÃO SOCIAL**

Luanda, Setembro de 2025

ÍNDICE

I- INTRODUÇÃO.....	3
II- RAZÕES JUSTIFICATIVAS.....	4
III- PERSPECTIVA DO ESTUDO COMPARADO	6
3.1 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO NORTE-AMERICANO	6
3.2 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO DA UNIÃO EUROPEIA.....	7
3.3 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO CHINÊS	10
3.4 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO JAPONÊS	12
3.5 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO CANADENSE	14
3.6 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO BRASILEIRO	16
3.7 - REGULAÇÃO DA IA EM ÁFRICA	19
3.7.1 - Estratégia Nacional de Inteligência Artificial do Egito	19
3.7.2 - Estratégia Nacional de Inteligência Artificial do Quênia	20
3.7.3 - Estratégia Nacional de Inteligência Artificial da África do Sul	21
3.7.4 - Política Nacional de Inteligência Artificial do Ruanda	21
IV- OBJECTIVOS DA PROPOSTA DE LEI SOBRE INTELIGÊNCIA ARTIFICIAL	22
V- AVALIAÇÃO SUMÁRIA DOS MEIOS FINANCEIROS E HUMANOS NECESSÁRIOS PARA IMPLEMENTAÇÃO DA LEI	23
VI - ÓRGÃOS CONSULTADOS	23
VII - ENQUADRAMENTO PROGRAMÁTICO	23
VIII- CONFORMAÇÃO LEGAL.....	24
IX- FORMA PROPOSTA PARA O DIPLOMA.....	24
X - SUMÁRIO A PUBLICAR EM DIÁRIO DA REPÚBLICA.....	25
XI - LEGISLAÇÃO A REVOGAR.....	25
XII- SÍNTESE DO CONTEÚDO DA PROPOSTA DE LEI	25
XIII - CONCLUSÃO	29
PROPOSTA DE LEI SOBRE A INTELIGÊNCIA ARTIFICIAL	

RELATÓRIO DE FUNDAMENTAÇÃO DA PROPOSTA DE LEI SOBRE A INTELIGÊNCIA ARTIFICIAL

I- INTRODUÇÃO

Ao abrigo da Constituição da República de Angola, nomeadamente dos artigos 40.º, 54.º, 55.º e 210.º, o Estado reconhece e garante direitos fundamentais como a liberdade de expressão, a privacidade e a protecção de dados pessoais, assumindo igualmente o dever de promover o desenvolvimento tecnológico e científico. Neste contexto, a utilização da Inteligência Artificial (IA) no território nacional deve ser orientada por princípios que assegurem a protecção dos direitos e liberdades fundamentais, o respeito pela dignidade da pessoa humana e a promoção do bem comum.

A relevância crescente da IA no plano nacional e internacional, associada ao seu impacto transversal nos sectores económico, social, científico e cultural, impõe a criação de um quadro jurídico específico que regule o seu desenvolvimento, aplicação e utilização. Tal regulação deve conciliar a promoção da inovação e do progresso tecnológico com a salvaguarda dos direitos das pessoas, prevenindo riscos como a discriminação algorítmica, a violação da privacidade, a manipulação de informação e outros potenciais abusos.

A Declaração Africana sobre Inteligência Artificial, assinada em Kigali a 4 de Abril de 2025 por países africanos e organismos regionais, estabelece princípios, objectivos e compromissos para promover uma IA ética, inclusiva e alinhada com a Agenda 2063 e os ODS, com destaque para os seguinte:

- a) Defende soberania digital, diversidade cultural, protecção de dados, transparência e sustentabilidade ambiental;
- b) Define metas como impulsionar inovação, competitividade e liderança africana em IA, com acções concretas: criação de programas de educação e investigação em IA, desenvolvimento de conjuntos de dados abertos e de infra-estruturas de computação soberana, estímulo a *hubs* de inovação e investimentos, incluindo um Fundo Africano de IA;
- c) Prevê ainda governação harmonizada, partilha de conhecimento, cooperação regional e internacional, e a criação do Conselho Africano de IA, visando integrar a África de forma segura e competitiva na economia global da inteligência artificial

Neste sentido, a presente proposta de Lei estabelece os princípios gerais, os direitos e deveres, bem como as normas de funcionamento, fiscalização e responsabilidade aplicáveis às actividades relacionadas com a Inteligência Artificial. O diploma visa assegurar que a adopção desta tecnologia contribua para o desenvolvimento sustentável de Angola, em conformidade com os valores constitucionais e com os objectivos estratégicos de modernização e diversificação da economia, reforçando a soberania digital e a competitividade do país.

II- RAZÕES JUSTIFICATIVAS

A presente Proposta de Lei sobre Inteligência Artificial surge em resposta à rápida evolução tecnológica e à necessidade de Angola se alinhar com as melhores práticas internacionais no domínio da inovação digital. A crescente adopção de sistemas de Inteligência Artificial (IA) traz inúmeros benefícios para a sociedade, como a melhoria da eficiência em serviços públicos e privados, a facilitação de decisões informadas e a promoção do desenvolvimento

económico. No entanto, a utilização desregulada da IA apresenta desafios significativos, incluindo riscos à privacidade, à segurança, à transparência e ao exercício de direitos fundamentais.

A expansão do uso da IA em diversos sectores, como saúde, educação, segurança, justiça e economia, demanda um enquadramento legal que assegure:

- **Transparência:** Garantir que os sistemas de IA funcionem de maneira compreensível para os utilizadores;
- **Responsabilidade:** Definir claramente os agentes responsáveis pelos impactos negativos resultantes do uso de IA;
- **Segurança:** Proteger os cidadãos contra riscos relacionados ao uso indevido da tecnologia, como ciberataques e decisões automatizadas discriminatórias;
- **Protecção de Dados:** Reforçar a segurança e a privacidade dos dados pessoais utilizados por sistemas de IA;
- **Fomento à Inovação:** Estabelecer incentivos para o desenvolvimento e a aplicação de soluções tecnológicas nacionais.

A proposta visa também posicionar Angola como um país que adere aos padrões internacionais de regulação da IA, promovendo a cooperação global e assegurando a competitividade tecnológica no mercado internacional. Legislação semelhante tem sido adoptada em vários ordenamentos jurídicos, como os da União Europeia e da China, o que demonstra a necessidade de Angola acompanhar esta tendência para garantir a protecção de seus cidadãos e o desenvolvimento sustentável através da inovação tecnológica.

III- PERSPECTIVA DO ESTUDO COMPARADO

3.1 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO NORTE-AMERICANO

Tendo em conta a forma republicana dos Estados Unidos da América, a regulação da IA neste país é fragmentada e, principalmente, baseada em regulamentações sectoriais, pois não existe uma legislação federal unificada e, especificamente, virada para IA, mas, sim, várias iniciativas lançadas para guiar o desenvolvimento e o uso responsável da tecnologia.

Não obstante, foi aprovada, em 2020, a **Lei da Iniciativa Nacional de Inteligência Artificial**, *National AI Initiative Act*, com o objectivo de estabelecer uma estrutura coordenada e abrangente para a promoção da pesquisa, desenvolvimento e uso ético e responsável da IA nos Estados Unidos, que reflecte a crescente importância da IA em diversos sectores e busca garantir que o país mantenha uma posição de liderança global na inovação tecnológica. Nos termos do disposto na Secção 101 e 102 da referida Lei, é previsto o **Comité de Iniciativa Nacional de IA**, cuja função é coordenar os esforços federais nesta matéria, reunindo representantes de diversas agências governamentais. Esse comité é responsável por garantir que as iniciativas de IA sejam integradas e colaborativas, evitando duplicidade de esforços e promovendo sinergias entre os diferentes programas e projectos federais. O comité também supervisiona a implementação da estratégia nacional de IA, avalia os progressos feitos e sugere melhorias contínuas para manter a eficácia das políticas neste sector.

No âmbito desta Lei, destaca-se também a norma da Secção 104, que designa o **Instituto Nacional de Padrões e Tecnologia (NIST)**, como a entidade principal para o desenvolvimento de directrizes e padrões para IA, cuja

responsabilidade se consubstancia em criar normas técnicas que garantam que os sistemas de IA sejam seguros, confiáveis e éticos.

Ainda neste domínio, importa referenciar a **Lei de Privacidade do Consumidor da Califórnia**, *California Consumer Privacy Act, CCPA*, que impõe diversas obrigações legais que afectam directamente o uso de tecnologias de Inteligência Artificial (IA), especialmente em relação à colecta, processamento e protecção de dados pessoais. Neste sentido, vários artigos prevêem um conjunto de direitos e garantias dos cidadãos face ao uso de tecnologias de informação.

Por exemplo, o artigo 1798.100 desta Lei garante aos consumidores o direito de saber quais dados estão sendo colectados e para que são utilizados, exigindo que as empresas sejam transparentes sobre como seus sistemas de IA empregam essas informações para treinamento e tomada de decisões automatizadas. Trata-se de um Diploma que, de grosso modo, estabelece uma estrutura legal rigorosa que promove a transparência, segurança e protecção dos direitos dos consumidores, impactando, significativamente, a maneira como as empresas desenvolvem e aplicam a IA.

3.2 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO DA UNIÃO EUROPEIA

A União Europeia está na vanguarda da regulamentação da IA, com uma abordagem mais cautelosa e orientada para os direitos humanos e a protecção de dados. Neste contexto, em 12 de Julho de 2024, foi publicada a **Lei de Inteligência Artificial**, regulamentada pelo **Regulamento (UE) 2024/1689 ("Lei de IA da UE")**, marcando o estabelecimento do primeiro quadro jurídico horizontal e abrangente para a regulamentação de sistemas de IA em

toda a UE. Tendo entrado em vigor, em todos os 27 Estados-Membros, no dia 1 de Agosto de 2024, embora a aplicação da maioria das suas disposições tenha sido preterida para o dia 2 de Agosto de 2026.

Composta, dentre outros aspectos, por 113 artigos, a Lei adopta uma abordagem baseada em risco para regulamentar todo o ciclo de vida de diferentes tipos de sistemas de IA, sendo que a não conformidade com ela pode resultar em uma penalidade financeira de até EUR 35 milhões ou 7% do facturamento anual global, prevalecendo o maior valor.

Nos termos do artigo 2.º, a Lei da IA da UE aplica-se a: (i) provedores que colocam no mercado da UE ou em serviço sistemas de IA ou, ainda, que colocam no mercado da UE modelos de IA de uso geral ("modelos GPAI"); (ii) implantadores de sistemas de IA que têm estabelecimento na UE; (iii) provedores e implantadores de sistemas de IA em países terceiros, se a saída produzida pelo sistema de IA for utilizada na UE. Daí que ela estabelece obrigações para provedores, implantadores, importadores, distribuidores e fabricantes de produtos de sistemas de IA, com conexão ao mercado da UE.

No entanto, ela não aplica a sistemas de IA de código aberto, a menos que sejam proibidos ou classificados como de alto risco ou utilizados exclusivamente para pesquisa e desenvolvimento científico.

A Lei de IA da UE proíbe certas práticas de IA em toda a União, considerando-as prejudiciais, abusivas e em contradição com os valores da UE. As práticas proibidas incluem o uso de técnicas subliminares de IA além da consciência de uma pessoa, ou técnicas deliberadamente manipuladoras ou enganosas, com o objectivo ou efeito de distorcer materialmente o comportamento humano.

A Lei de IA da UE impõe uma ampla gama de obrigações aos diversos actores no ciclo de vida de um sistema de IA de alto risco, incluindo requisitos sobre

treinamento e governação de dados, documentação técnica, manutenção de registos, robustez técnica, transparência, supervisão humana e segurança cibernética. Por exemplo, sistemas de IA de alto risco que utilizam técnicas envolvendo treinamento de modelos com dados devem ser desenvolvidos com base em conjuntos de dados de treinamento, validação e teste que atendam aos critérios de qualidade estabelecidos pelo artigo 10.º.

A Lei de IA da UE dedica um capítulo à classificação e regulamentação de modelos GPAI, definido como "um modelo de IA, incluindo aqueles treinados com grande quantidade de dados usando autos supervisão em escala, que demonstra generalidade significativa e é capaz de realizar uma ampla gama de tarefas distintas, independentemente da forma como é colocado no mercado e que pode ser integrado em diversos sistemas ou aplicativos *downstream*, excepto os modelos de IA usados para actividades de pesquisa, desenvolvimento ou prototipagem antes de serem comercializados".

Conforme mencionado, a Lei da UE sobre IA não se aplica a quaisquer sistemas ou modelos de IA (incluindo modelos GPAI e seus resultados) desenvolvidos e colocados em serviço exclusivamente para pesquisa e desenvolvimento científico (Art. 2 (6) da Lei da UE sobre IA).

Nos termos do artigo 53.º da Lei, todos os provedores de modelos GPAI estão sujeitos a certas obrigações, como: (i) manter documentação técnica actualizada, incluindo o processo de treinamento e teste, ou fornecer informações a provedores de sistemas de IA que pretendem usar o modelo GPAI; (ii) cooperar com a Comissão e autoridades nacionais competentes; e (iii) respeitar as leis nacionais sobre direitos autorais e direitos relacionados.

Os provedores de modelos GPAI com risco sistémico têm obrigações adicionais, incluindo realizar avaliações padronizadas de modelos, avaliar e mitigar riscos sistémicos, rastrear e relatar incidentes e garantir a protecção da segurança cibernética (Art. 55 da Lei de IA da UE).

O artigo 56.º da Lei de IA da UE orienta o Gabinete de IA da UE a incentivar e facilitar a elaboração de códigos de prática no nível da UE para "contribuir para a aplicação adequada" da lei, considerando "abordagens internacionais".

3.3 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO CHINÊS

A República Popular da China não dispõe, ainda, de um Diploma que regula especificamente a Inteligência Artificial, apesar de adoptar uma abordagem centralizada e estratégica para a regulação da IA, alinhada com sua política de se tornar líder global em IA até 2030.

Não obstante, em 2017, aprovou o **Plano de Desenvolvimento da Nova Geração de Inteligência Artificial** da China, vista como a estratégia nacional ambiciosa, elaborada com o objectivo de transformar o país em líder global em Inteligência Artificial (IA) até 2030. Este documento destaca a IA como um motor central para o crescimento económico, inovação tecnológica e segurança nacional, reflectindo o compromisso da China em dominar essa tecnologia emergente.

Dentre outros aspectos o Plano de Desenvolvimento da Nova Geração de Inteligência Artificial da China prevê o seguinte:

- a) Até 2020: O foco inicial consistiu em alcançar avanços significativos em tecnologias de IA, estabelecendo uma base sólida para a indústria de IA e integrando-a aos principais sectores económicos. Isso incluiu o

desenvolvimento de infra-estrutura e plataformas de suporte para pesquisa e aplicação de IA.

- b) Até 2025: O plano prevê que a China lidere o mundo em algumas áreas de tecnologia de IA e que a IA se torne um dos principais motores do crescimento económico do país. Isso implica na integração ainda mais profunda da IA em sectores como manufactura, saúde, educação e serviços públicos.
- c) Até 2030: O objectivo final é que a China se estabeleça como o principal centro de inovação em IA globalmente, com liderança em padrões, teorias e tecnologias de IA. Nessa fase, espera-se que a IA tenha transformado completamente a economia e a sociedade chinesa.

O plano enfatiza a necessidade de inovação em IA, incentivando a pesquisa avançada em áreas como aprendizado de máquina, visão computacional, processamento de linguagem natural e robótica. A China busca não apenas adoptar as tecnologias existentes, mas também liderar a criação de novas soluções e abordagens.

Há um forte investimento em P&D (Pesquisa e Desenvolvimento), com incentivos para universidades, empresas e institutos de pesquisa colaborarem em projectos de IA. O governo chinês apoia activamente esses esforços com financiamentos e políticas que promovem a inovação.

A segurança nacional é uma prioridade central no plano, com a IA vista como uma ferramenta crítica para fortalecer as capacidades militares e de segurança do país. A China planeja usar IA em áreas como defesa cibernética, vigilância e guerra autónoma, garantindo que as inovações tecnológicas também atendam aos objectivos estratégicos do Estado.

Além disso, o plano inclui medidas para proteger a infra-estrutura de IA e dados sensíveis contra ameaças externas, sublinhando a importância da soberania tecnológica.

Reconhecendo a importância de uma força de trabalho qualificada, o plano promove a educação e treinamento em IA. Isso inclui desde a inclusão de IA nos currículos escolares até o apoio a programas avançados de doutorado e pós-doutorado em IA. O objectivo é criar um ecossistema robusto de talentos que possa sustentar o crescimento da indústria de IA na China.

O plano inclui a criação de um quadro regulatório para garantir que o desenvolvimento e a aplicação da IA sejam alinhados com os interesses da sociedade e do Estado. Isso inclui o estabelecimento de normas éticas para o uso de IA, com particular atenção à privacidade, segurança de dados e prevenção de vieses nos sistemas de IA.

O plano promove parcerias entre o governo, a indústria e a academia para acelerar o desenvolvimento e a aplicação de IA. Essas parcerias são vistas como essenciais para criar um ambiente favorável à inovação, onde as empresas privadas desempenham um papel vital na comercialização das tecnologias de IA.

3.4 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO JAPONÊS

A semelhança do que sucede com a República Popular da China, o ordenamento jurídico japonês não prevê ainda um Diploma que, de forma específica, trata da IA, apesar de adoptar, em alguns casos, uma abordagem regulatória flexível e voltada para a promoção da inovação, focando em

directrizes éticas e políticas públicas que incentivam a adoção responsável da IA.

Sem prejuízo do exposto acima, o país dispõe de **Directrizes sobre IA**, aprovadas em 2019, que representa um marco na abordagem ética e responsável do país em relação ao desenvolvimento e aplicação da Inteligência Artificial. Estas directrizes foram criadas com o objectivo de assegurar que a IA seja utilizada de forma transparente, justa e que respeite os direitos humanos.

Um dos principais aspectos dessas directrizes é o foco na transparência e explicabilidade, exigindo que os sistemas de IA sejam compreensíveis e que suas decisões possam ser explicadas de maneira clara aos usuários. Isso é fundamental para evitar o uso indevido de IA em áreas sensíveis como a justiça, finanças e saúde, onde a falta de transparência pode resultar em injustiças ou discriminações.

Além disso, as directrizes destacam a justiça e a não discriminação como pilares essenciais, garantindo que os algoritmos de IA não perpetuem vieses ou prejudiquem grupos vulneráveis. Esta abordagem ética reflecte o compromisso do Japão em promover o uso da IA de forma que beneficie toda a sociedade, minimizando riscos e impactos negativos.

Para além das Directrizes sobre IA, o país adoptou o **Plano Básico de Ciência e Tecnologia** (2021-2025), que, por sua vez, coloca a IA no centro das estratégias de crescimento económico e competitividade global do país. Este plano enfatiza a necessidade de investimentos contínuos em pesquisa e desenvolvimento de IA, incentivando a inovação e o avanço tecnológico em várias indústrias.

Um dos principais objectivos do plano é integrar a IA em sectores-chave como a manufactura, saúde e serviços públicos, onde a tecnologia pode melhorar a eficiência e criar novas oportunidades económicas. O plano também promove a colaboração público-privada, incentivando parcerias entre o governo, a academia e a indústria para acelerar o desenvolvimento e a aplicação da IA. Isso inclui a criação de ambientes de teste e infra-estrutura de apoio que facilitem a implementação de soluções de IA no mundo real. Além disso, o plano sublinha a importância de desenvolver talento humano especializado em IA, através de programas educacionais e de treinamento, para assegurar que o Japão tenha a capacidade de sustentar seu crescimento tecnológico a longo prazo.

3.5 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO CANADENSE

A semelhança do que acontece na República da China e do Japão, o ordenamento jurídico canadense não prevê, ainda, um Diploma que se propõe a regulamentar a IA, embora o país tenha adoptado uma abordagem equilibrada, focando na promoção da inovação em IA enquanto estabelece directrizes claras para o uso ético e responsável da tecnologia.

Não obstante, o país aprovou as **Directrizes de IA**, documento estabelecido para garantir que a IA seja desenvolvida e utilizada de forma transparente, justa e segura, particularmente no contexto de sua aplicação por entidades governamentais. Essas directrizes foram criadas como parte de um esforço mais amplo para garantir que o uso de IA no sector público seja responsável e que os direitos dos cidadãos sejam respeitados.

As directrizes exigem que qualquer sistema de IA usado por entidades governamentais seja transparente em sua operação. Isso significa que os cidadãos têm o direito de saber como e por que uma decisão automatizada foi tomada, e que os algoritmos devem ser auditáveis para assegurar que operam conforme projectado. As decisões baseadas em IA devem ser explicáveis, de modo que os indivíduos afectados possam entender a lógica por trás dessas decisões.

As directrizes também sublinham a necessidade de garantir que os sistemas de IA sejam seguros e protegidos contra ameaças cibernéticas. Isso envolve a implementação de medidas de segurança robustas para proteger os dados e a integridade dos sistemas de IA contra acessos não autorizados, manipulação ou outras formas de comprometimento.

No mesmo contexto, apesar de não existir ainda uma regulamentação específica da IA, a **Lei de Protecção de Informações Pessoais e Documentos Electrónicos** tem sido bastante útil nesta matéria. A propósito, o artigo 4.º desta Lei estabelece que as organizações são responsáveis pela protecção dos dados pessoais que estão sob seu controle. Essa responsabilidade abrange desde a colecta até o processamento e armazenamento das informações pessoais, especialmente no contexto da IA. As organizações devem garantir que os dados utilizados por sistemas de IA sejam tratados com o mais alto nível de protecção, designando indivíduos específicos responsáveis por assegurar a conformidade com os requisitos dessa Lei.

No mesmo sentido, o artigo 8.º garante aos indivíduos o direito de acessar seus dados pessoais mantidos por uma organização e de corrigir qualquer informação incorrecta, norma que, no contexto dos sistemas de IA, requer que as organizações estejam preparadas para fornecer informações detalhadas sobre

os dados pessoais utilizados pelos algoritmos e para permitir que os indivíduos solicitem correcções ou a exclusão desses dados, conforme necessário. Este direito é fundamental para garantir que os sistemas de IA operem com base em dados precisos e actualizados, minimizando erros e distorções nas decisões automatizadas.

Por fim, o artigo 10.º exige que as organizações adoptem salvaguardas adequadas para proteger os dados pessoais contra perda, roubo, acesso não autorizado, divulgação, cópia, uso ou modificação. Isso implica na necessidade de adoptar medidas técnicas, organizacionais e administrativas que garantam a segurança dos dados utilizados nos sistemas de IA, protegendo-os contra ameaças internas e externas. A conformidade com esse artigo é essencial para manter a integridade e a confidencialidade dos dados pessoais, que são críticos para o funcionamento seguro e confiável dos algoritmos de IA.

3.6 - REGULAÇÃO DA IA NO ORDENAMENTO JURÍDICO BRASILEIRO

A semelhança de outros países, a República Federativa do Brasil se encontra em processo de desenvolvimento de uma estrutura regulatória para IA, com um foco crescente na protecção de dados e direitos humanos.

Neste sentido, em 2021 foi aprovada a **Estratégia Brasileira de Inteligência Artificial**, documento que reflecte a visão estratégica do governo brasileiro em posicionar o país como um participante significativo na revolução tecnológica global, ao mesmo tempo em que se assegura que a inovação em IA seja conduzida de maneira ética, responsável e alinhada com os valores e os direitos fundamentais da sociedade.

A estratégia enfatiza a necessidade de promover o desenvolvimento de tecnologias de IA que sejam inovadoras, mas que também respeitem princípios éticos e direitos humanos. A inovação responsável implica em garantir que as soluções de IA não apenas impulsionem o crescimento económico, mas também contribuam para o bem-estar social, mitigando potenciais impactos negativos, como o aumento das desigualdades sociais ou a violação da privacidade.

A estratégia tem como uma das prioridades a capacitação da força de trabalho em IA. Isso inclui iniciativas para fomentar a formação de especialistas em IA, desde o ensino básico até a pós-graduação, além de programas de reciclagem e requalificação para os profissionais já actuates no mercado. O objectivo é assegurar que o Brasil tenha uma base de talentos capaz de sustentar e expandir as capacidades em IA no longo prazo.

A Estratégia também aborda a necessidade de um quadro regulatório adequado para a IA, que seja capaz de acompanhar as rápidas evoluções tecnológicas e de proteger os direitos dos cidadãos. Esse marco regulatório deve contemplar questões como privacidade, segurança cibernética, e a explicabilidade das decisões automatizadas, garantindo que a IA seja desenvolvida e utilizada de forma transparente e justa.

A Estratégia reconhece a importância de investir em pesquisa e desenvolvimento (P&D) para manter a competitividade do Brasil no cenário global de IA. Isso envolve o apoio a iniciativas de pesquisa em universidades, centros de inovação e empresas, além da criação de parcerias público-privadas para acelerar a inovação e a comercialização.

Os marcos estratégicos da IA no Brasil são reforçados pela **Lei Geral de Protecção de Dados Pessoais**, aprovada por via da Lei n.º 13.709/2018, que, apesar de não estar especificamente direccionada para a regulação da IA, possui implicações directas e significativas sobre o desenvolvimento e a aplicação de IA, uma vez que muitos sistemas de IA dependem do uso massivo de dados pessoais para funcionar adequadamente.

Por exemplo, o artigo 7.º define as bases legais para o tratamento de dados pessoais, estabelecendo que o consentimento do titular dos dados é necessário, salvo em casos específicos previstos na lei. No contexto de IA, isso implica que qualquer sistema que utilize dados pessoais deve estar respaldado por uma base legal adequada, como o consentimento explícito do indivíduo, a execução de um contrato ou o cumprimento de uma obrigação legal.

Do mesmo modo, o artigo 18.º garante aos indivíduos diversos direitos em relação aos seus dados pessoais, incluindo o direito de acesso, correcção, exclusão e portabilidade de dados. Para sistemas de IA, isso significa que as organizações devem estar preparadas para responder a solicitações de titulares de dados que desejem exercer esses direitos, o que pode incluir a remoção de seus dados de um sistema de IA ou a correcção de informações imprecisas.

Não menos importante, o artigo 46.º da referida Lei exige que as organizações implementem medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito; essa exigência é relevante no contexto de IA, dado que a segurança dos dados é crucial para garantir a integridade e a confiabilidade dos sistemas de IA.

Por fim, o artigo 52.º prevê sanções severas para organizações que violarem as disposições da lei, incluindo multas que podem chegar a até 2% do facturamento da empresa, limitadas a R\$ 50 milhões por infracção, suspensão ou proibição do tratamento de dados. Essas sanções reforçam a importância da conformidade com a LGPD para qualquer organização que utilize IA, incentivando a adopção de práticas responsáveis e seguras no tratamento de dados pessoais.

3.7 - REGULAÇÃO DA IA EM ÁFRICA

Os ordenamentos jurídicos africanos estudados, ainda não possuem legislação específica sobre a inteligência artificial (IA), mas têm vindo a desenvolver estratégias nacionais para o desenvolvimento da IA. Dentre esses países destacamos o Egipto, Quênia, África do Sul e Ruanda.

3.7.1 - Estratégia Nacional de Inteligência Artificial do Egipto

A Estratégia Nacional de Inteligência Artificial do Egipto 2025-2030 (2ª Edição) visa posicionar o país como líder regional em IA, promovendo uma sociedade digital inclusiva e impulsionando o desenvolvimento socioeconómico.

A Estratégia assenta em seis pilares estratégicos: Governação, Tecnologia, Dados, Infra-estruturas, Ecossistema e Talento – e tem como objectivos centrais criar um quadro ético e de governação robusto, expandir as capacidades tecnológicas, assegurar acessibilidade e partilha segura de dados, desenvolver infra-estruturas de IA a nível nacional, dinamizar um ecossistema saudável com ênfase em *startups* e parcerias, e formar capital humano qualificado através de programas especializados.

Até 2030, pretende-se com ela, aumentar significativamente a contribuição da IA para o PIB e elevar a participação do sector das TIC para 7,7%, estabelecer mais de 250 *startups* de base IA, formar mais de 30 000 especialistas e garantir que 36% da população integre soluções de IA no quotidiano.

A sua implementação está sob coordenação do Conselho Nacional de Inteligência Artificial (NCAI) e seguirá fases progressivas e metas com indicadores de desempenho (KPI's), reforçando a colaboração internacional em ética da IA, atracção de investimento estrangeiro e posicionamento do Egipto como polo de inovação que liga África, o mundo árabe e mercados globais.

3.7.2 - Estratégia Nacional de Inteligência Artificial do Quénia

A Estratégia Nacional de Inteligência Artificial (2025 – 2030) apresenta um plano nacional para posicionar o Quénia como *hub* líder de inovação em modelos de IA em África, impulsionando o desenvolvimento sustentável, o crescimento económico e a inclusão social. Neste sentido, a Estratégia tem uma visão centrada na cidadania, com foco em três pilares estratégicos: Infra-estrutura Digital de IA, Dados e Investigação e Inovação em IA.

A Estratégia está estruturada por quatro eixos transversais, nomeadamente: governação, desenvolvimento de talento, investimento público e privado e equidade/ética/inclusão. A estratégia propõe um processo faseado, desde investimentos fundacionais em políticas, infra-estrutura e capacitação, até à criação de centros de investigação e inovação, projectos-piloto e um sistema de monitorização e avaliação.

Pretende-se, assim, maximizar o contributo da IA para sectores críticos como agricultura, saúde, educação, segurança e serviços públicos, garantindo protecção de dados, respeito pelos direitos humanos e distribuição equitativa de benefícios, enquanto fomenta um ecossistema local robusto de inovação e desenvolvimento (I&D) e *startups*.

3.7.3 - Estratégia Nacional de Inteligência Artificial da África do Sul

A Estratégia Nacional de Inteligência Artificial da África do Sul (2024) visa promover a inovação e o crescimento económico através da IA, assegurando inclusão digital, equidade social e sustentabilidade. A estratégia identifica como motores o avanço tecnológico, a necessidade económica e a pressão social, contrapondo os desafios históricos como desigualdades e fraca infra-estrutura, e define objectivos que alinham o país com padrões globais.

Por outro lado, ela está baseada nos pilares estratégicos: desenvolvimento de talento, infra-estrutura digital, investigação e inovação, aplicação no sector público, ética e transparência, protecção de dados, segurança, redução de preconceitos, controlo humano e promoção de valores culturais e humanos para garantir que a IA seja desenvolvida e utilizada de forma ética, transparente e centrada no ser humano, preparando o caminho para futura legislação específica e consolidando a posição da África do Sul como líder em IA no continente.

3.7.4 - Política Nacional de Inteligência Artificial do Ruanda

A Política Nacional de IA do Ruanda, adoptada em Abril de 2023, visa posicionar o país como um centro africano de inovação em inteligência

artificial, promovendo a inovação responsável e o desenvolvimento inclusivo e sustentável alinhado com a Visão 2050.

A Política Ruandês sobre IA está estruturada em seis áreas prioritárias, nomeadamente: competências do século XXI e literacia em IA, infra-estrutura fiável, estratégia robusta de dados, directrizes éticas, adopção da IA no sector público e estímulo à inovação no sector privado.

A política procura impulsionar o crescimento económico, melhorar os serviços públicos e criar um ecossistema favorável, com destaque para o Conselho Presidencial de IA e a cooperação entre governo, indústria e investigação, consolidando o Ruanda como um “*Laboratório de IA de África*” e fortalecendo a qualidade de vida da população.

IV- OBJECTIVOS DA PROPOSTA DE LEI SOBRE INTELIGÊNCIA ARTIFICIAL

A presente Proposta de Lei pretende:

- Criar um ambiente legal propício ao desenvolvimento de tecnologias baseadas em IA;
- Proteger os direitos fundamentais dos cidadãos face aos riscos inerentes à IA;
- Promover a ética, a transparência e a equidade na utilização da tecnologia;
- Estabelecer mecanismos de fiscalização e sanção para o uso inadequado da IA.

Desta forma, esta proposta de Lei apresenta-se como um instrumento jurídico fundamental para a modernização do Estado e a consolidação de Angola como uma nação preparada para os desafios e oportunidades da era digital.

V- AVALIAÇÃO SUMÁRIA DOS MEIOS FINANCEIROS E HUMANOS NECESSÁRIOS PARA IMPLEMENTAÇÃO DA LEI

Em termos económicos, a proposta de lei produz impacto imediato e directo no Orçamento Geral do Estado.

VI - ÓRGÃOS CONSULTADOS

A elaboração da presente proposta de Lei deve ser submetida à consulta pública, buscando a participação de todas as entidades, públicas e privadas, bem como as individualidades interessadas nas matérias de inteligência artificial.

Além disso, serão igualmente consultadas, entre outros, os seguintes departamentos ministeriais:

- a) Ministério das Finanças;
- b) Ministério do Interior;
- c) Ministério da Administração Pública, Trabalho e Segurança Social;
- d) Ministério do Ensino Superior, Ciência, Tecnologia e Inovação;
- e) Ministério da Educação;
- f) Ministério da Juventude e Desportos;
- g) Ministério da Saúde;
- h) Ministério da Agricultura e Florestas;
- i) Secretária para Reforma do Estado.

VII - ENQUADRAMENTO PROGRAMÁTICO

Do ponto de vista programático, em matéria de Inteligência artificial, a proposta visa também posicionar Angola como um país que adere aos padrões internacionais de regulação da IA, promovendo a cooperação global e

assegurando a competitividade tecnológica no mercado internacional, com efeito, existe expressão ao nível do principal programa do Executivo Angolano, denominado pela Estratégia de Longo Prazo - Angola 2050, aprovado pelo Decreto Presidencial n.º 181/23 de 01 de Setembro, Plano de Desenvolvimento Nacional (PDN - 2023- 2027), aprovado pelo Decreto Presidencial n.º 225/ 23 de 30 de Novembro e pelo Livro Branco das Tecnologias de Informação e Comunicação (LBTIC 2023-2027), aprovado através do Decreto Presidencial n.º 272/24, de 5 de Dezembro.

Neste ínterim, a presente proposta de Lei, encontra-se devidamente alinhada ao quadro programático aludido.

VIII- CONFORMAÇÃO LEGAL

A presente proposta de lei e o respectivo relatório de fundamentação estão em conformidade e harmonizados com o disposto na Lei n.º 7/14, de 26 de Maio, sobre as Publicações Oficiais e Formulários Legais, com o Regimento da Assembleia Nacional, aprovado por via da Lei n.º 13/17, de 6 de Julho com o Decreto Presidencial n.º 251/12, de 27 de Dezembro, que estabelece os Procedimentos para a Materialização das Deliberações do Executivo e com o Regimento do Conselho de Ministros aprovado pelo Decreto Presidencial n.º 357/17, de 28 de Dezembro.

IX- FORMA PROPOSTA PARA O DIPLOMA

A presente proposta de lei reveste a forma de Lei, ao abrigo das disposições combinadas da alínea b) do artigo 161.º, n.º 2 do artigo 165.º e da alínea d) do n.º 1 do artigo 166.º da Constituição da República de Angola (CRA).

X - SUMÁRIO A PUBLICAR EM DIÁRIO DA REPÚBLICA

Eis o sumário que deve constar da Iª Série do Diário da República:

“Lei n.º ____/2025, Lei sobre a Inteligência Artificial.”

XI - LEGISLAÇÃO A REVOGAR

Não existe legislação para efeito de revogação.

XII- SÍNTESE DO CONTEÚDO DA PROPOSTA DE LEI

A presente Proposta conta com 86 artigos, nove capítulos e cinco secções, cujo índice sistemático apresenta-se a seguir:

CAPÍTULO I - DISPOSIÇÕES GERAIS

ARTIGO 1.º (Objecto)

ARTIGO 3.º (Âmbito)

ARTIGO 4.º (Exclusão)

ARTIGO 5.º (Definições)

ARTIGO 6.º (Princípios da IA)

ARTIGO 7.º (Desenvolvimento de Infra-estruturas)

ARTIGO 8.º (Protecção dos Direitos de Propriedade Intelectual)

ARTIGO 9.º (Desenvolvimento Sustentável)

CAPÍTULO II - DESENVOLVIMENTO E PROMOÇÃO DA IA

ARTIGO 10.º (Planeamento do Desenvolvimento da IA)

ARTIGO 11.º (Construção de Infra-estruturas Computacionais)

ARTIGO 12.º (Utilização de Recursos Computacionais)

ARTIGO 13.º (Inovação em Modelos Algorítmicos)

ARTIGO 14.º (Inovação em Tecnologias-Chave)

ARTIGO 15.º (Construção do Ecossistema de Código Aberto)

ARTIGO 16.º (Fornecimento de Factores de Produção de Dados)

ARTIGO 17.º (Utilização de Dados Públicos)

ARTIGO 18.º (Construção de Redes de Informação)

ARTIGO 19.º (Protecção de Direitos de Propriedade Intelectual)

ARTIGO 20.º (Uso Razoável de Dados)

ARTIGO 21.º (Tecnologia e Serviços de Segurança)

ARTIGO 22.º (Contratação de Seguro)

CAPÍTULO III - PROTECÇÃO DOS DIREITOS E INTERESSES DOS USUÁRIOS

ARTIGO 23.º (Direitos Iguais)

ARTIGO 24.º (Direito à Informação)

ARTIGO 25.º (Protecção da Privacidade e das Informações Pessoais)

ARTIGO 26.º (Direito a Esclarecimento e a Recusa de Decisões Baseadas em IA)

ARTIGO 27.º (Direitos de Propriedade Intelectual de Conteúdo Gerado por IA)

ARTIGO 28.º (Direitos e Interesses dos Trabalhadores)

ARTIGO 29.º (Direitos e Interesses de Grupos Digitalmente Desfavorecidos)

ARTIGO 30.º (Direito de Obter Ajuda e Treinamento)

ARTIGO 31.º (Direito de Reclamação e de Acção Judicial)

CAPÍTULO IV - OBRIGAÇÕES E REQUISITOS A OBSERVAR PELOS DESENVOLVEDORES E FORNECEDORES DE IA

SECÇÃO I - DISPOSIÇÕES GERAIS

ARTIGO 32.º (Obrigações de Segurança)

ARTIGO 33.º (Avaliação de Riscos de Segurança)

ARTIGO 34.º (Comunicação de Incidentes de Segurança e Protecção Significativos)

ARTIGO 35.º (Manutenção da Segurança dos Segurados)

ARTIGO 36.º (Qualidade dos Dados)

ARTIGO 37.º (Directrizes de Conformidade)

ARTIGO 38.º (Segurança e Protecção de Conteúdo)

ARTIGO 39.º (Obrigações de Identificação)

ARTIGO 40.º (Requisitos de Acesso)

SECÇÃO II - IA CRÍTICA

ARTIGO 41.º (Abrangência da IA Crítica)

ARTIGO 42.º (Medidas de Protecção para a IA Crítica)

ARTIGO 43.º (Estrutura Organizacional para IA Crítica)

ARTIGO 44.º (Registo da IA Crítica)

ARTIGO 45.º (Avaliação de Riscos de Segurança da IA Crítica)

ARTIGO 46.º (Divulgação de Riscos de Segurança da IA Crítica)

ARTIGO 47.º (Resposta a Emergências de Segurança para IA Crítica)

ARTIGO 48.º (Obrigações de Reportar Alterações nas Entidades de IA Crítica)

CAPÍTULO V - REGIMES ESPECIAIS DE APLICAÇÃO DA IA

ARTIGO 49.º (Uso de IA por Órgãos do Estado e pela Administração Pública)

ARTIGO 50.º (IA Jurisdicional)

ARTIGO 51.º (IA para Notícias)

ARTIGO 52.º (IA Médica)

ARTIGO 53.º (Bots Sociais)

ARTIGO 54.º (Reconhecimento Biométrico)

ARTIGO 55.º (Condução Autónoma)

ARTIGO 56.º (Requisitos Especiais para IA de Propósito Geral)

CAPÍTULO VI - MODELO DE GOVERNAÇÃO DA IA

ARTIGO 57.º (Governança Diversificada e Colaborativa)

ARTIGO 58.º (Mecanismo de Coordenação Geral)

ARTIGO 59.º (Coordenação Diversificada)

ARTIGO 60.º (Comissão de Especialistas)

CAPÍTULO VII - REGULAÇÃO, SUPERVISÃO E FISCALIZAÇÃO

ARTIGO 61.º (Autoridade Competente da IA)

ARTIGO 62.º (Funções de Regulatórias e de Fiscalização)

ARTIGO 63.º (Categorização e Classificação)

ARTIGO 64.º (Fiscalização Especial da IA Crítica)

ARTIGO 65.º (Monitoramento de Riscos e Resposta a Emergências)

ARTIGO 66.º (Avaliação e Certificação)

ARTIGO 67.º (Supervisão, Inspeção e Cooperação)

CAPÍTULO VIII - REGIME DE RESPONSABILIDADE DA IA

SECÇÃO I - RESPONSABILIDADE CONTRA-ORDENACIONAL

ARTIGO 68.º (Contra-ordenação)

ARTIGO 69.º (Contra-ordenações Simples)

ARTIGO 70.º (Contra-ordenações Graves)

ARTIGO 71.º (Responsabilidade contra-ordenacional objectiva)

ARTIGO 72.º (Coimas)

ARTIGO 73.º (Sanções Acessórias)

ARTIGO 74.º (Aplicação das coimas e sanções acessórias)

ARTIGO 75.º (Regime supletivos)

SECÇÃO II RESPONSABILIDADE PENAL

ARTIGO 76.º (Crimes no Âmbito IA)

ARTIGO 77.º (Circunstâncias Agravantes Penais)

ARTIGO 78.º (Suspensão Condicional da Pena)

ARTIGO 79.º (Concurso de Crime e Contra-ordenação)

SECÇÃO III - RESPONSABILIDADE CIVIL

ARTIGO 80.º (Responsabilidade Objectiva)

ARTIGO 81.º (Responsabilidade Civil Conexa com a Penal)

CAPÍTULO IX - DISPOSIÇÕES FINAIS

ARTIGO 82.º (Publicidade das Sanções)

ARTIGO 83.º (Receitas das Sanções)

ARTIGO 84.º (Mecanismo Piloto de Supervisão)

ARTIGO 85.º (Dúvidas e omissões)

ARTIGO 86.º (Entrada em vigor)

XIII - CONCLUSÃO

De acordo com os argumentos aduzidos e depois de realizada a consulta pública, propõe-se que a Proposta de Lei sobre a Inteligência Artificial, anexa ao presente relatório de fundamentação, seja apreciada pelo Conselho de Ministros e, conseqüentemente, remetida para a Assembleia Nacional para os devidos efeitos.

LEI _____/2025

De _____ De _____

Considerando que a Inteligência Artificial (IA) representa um dos mais significativos avanços tecnológicos do século XXI, com impacto transversal nos domínios económico, social, cultural e político;

Reconhecendo o potencial transformador da IA para promover o desenvolvimento sustentável, a inovação e a competitividade económica, bem como para melhorar a qualidade de vida dos cidadãos;

Reconhecendo a importância da colaboração internacional para o desenvolvimento de normas técnicas e padrões éticos que promovam a interoperabilidade e a confiança no uso da IA;

Determinados a estabelecer uma base legal que permita o desenvolvimento, a implementação e a regulação eficazes de sistemas de IA em Angola, promovendo a confiança, a inovação e a competitividade no mercado global;

A Assembleia Nacional aprova, por mandato do povo, nos termos das disposições conjugadas da alínea b) do artigo 161.º, do n.º 2 do artigo 165.º e da alínea d) do n.º 2 do artigo 166.º da Constituição da República de Angola, a seguinte:

LEI SOBRE A INTELIGÊNCIA ARTIFICIAL

CAPÍTULO I

DISPOSIÇÕES GERAIS

ARTIGO 1.º

(Objecto)

A presente Lei tem por objecto o estabelecimento do regime jurídico da inteligência artificial (IA), bem como regular as actividades de desenvolvimento, fornecimento e uso de produtos e serviços de IA, incluindo a sua fiscalização para a salvaguarda do interesse público e reforço da protecção dos direitos dos cidadãos e das pessoas colectivas.

ARTIGO 2.º

(Fins)

São fins da presente Lei:

- a) Promover a inovação tecnológica na área da inteligência artificial (IA);
- b) Facilitar o desenvolvimento saudável da indústria de IA;
- c) Regular as actividades de desenvolvimento, fornecimento e uso de produtos e serviços de IA;
- d) Salvaguardar o interesse público;
- e) Proteger os direitos e interesses legítimos de pessoas singulares e colectivas e demais organizações sociais.

ARTIGO 3.º

(Âmbito)

1. A presente Lei aplica-se às actividades de desenvolvimento, fornecimento e uso de IA realizadas no território da República de Angola.
2. A presente Lei também se aplica às actividades de desenvolvimento, fornecimento e uso de IA realizadas fora do território de Angola que possam afectar os interesses públicos, ou os direitos e interesses legítimos de pessoas singulares e colectivas domiciliadas em Angola.

ARTIGO 4.º

(Exclusão)

1. A presente Lei não se aplica às seguintes situações:
 - a) Uso de IA por uma pessoa singular para assuntos pessoais ou familiares;
 - b) Actividades de pesquisa científica em IA.
2. As actividades de desenvolvimento e utilização militar de IA serão reguladas em diploma próprio.

ARTIGO 5.º

(Definições)

Para efeitos desta Lei, os seguintes termos são definidos:

- a) Inteligência artificial (IA): tecnologia que utiliza computadores para simular comportamentos inteligentes humanos, aplicável em previsão, recomendação, tomada de decisões ou geração de conteúdo, entre outros, para fins especializados ou gerais;
- b) Desenvolvedores de IA: pessoas, singulares ou colectivas, ou outras organizações envolvidas no desenvolvimento de produtos e serviços de IA;
- c) Fornecedores de IA: pessoas, singulares ou colectivas, ou outras organizações que disponibilizam produtos e serviços de IA;

- d) Usuários de IA: pessoas, singulares ou colectivas, ou outras organizações que utilizam produtos e serviços de IA;
- e) Inteligência artificial de propósito geral (AGI): IA com capacidades cognitivas amplas, aplicável em múltiplos campos.

ARTIGO 6.º

(Princípios da IA)

São princípios da IA os seguintes:

- a) Princípio da ética científica e tecnológica: o desenvolvimento de IA deve aderir a uma abordagem centrada nas pessoas, respeitando a liberdade e dignidade individual, promovendo o bem-estar da população e garantindo o interesse público, de forma a orientar e regulamentar o desenvolvimento saudável e ordenado da indústria de IA. Os desenvolvedores, fornecedores e utilizadores de IA devem prevenir e controlar os riscos éticos potenciais da IA, em conformidade com a lei;
- b) Princípio do desenvolvimento inovador: o Estado implementa uma supervisão inclusiva e prudente, incentivando e apoiando o desenvolvimento baseado na inovação da indústria de IA, garantindo a protecção da IA;
- c) Princípio da justiça e imparcialidade: os desenvolvedores, fornecedores e utilizadores de IA devem aderir ao princípio da justiça e imparcialidade, protegendo os direitos e interesses legítimos de indivíduos e organizações, e não devem praticar tratamentos diferenciados de forma injustificada;
- d) Princípio da transparência e explicabilidade: os desenvolvedores, fornecedores e utilizadores de IA devem aderir ao princípio da transparência e explicabilidade e, em conformidade com a lei, fornecer e explicar, de maneira apropriada, as informações básicas, o propósito e a intenção, bem como os principais mecanismos de operação dos produtos e serviços de IA;

- e) Princípio da segurança e responsabilidade: os desenvolvedores, fornecedores e utilizadores de IA devem, em conformidade com a lei, adoptar os meios técnicos e medidas de gestão necessários para garantir a segurança e a confiabilidade dos produtos e serviços de IA. Os desenvolvedores, fornecedores e utilizadores de IA devem, de acordo com a lei, assumir as responsabilidades legais correspondentes pelas actividades de desenvolvimento, fornecimento e uso;
- f) Princípio do uso adequado: os desenvolvedores, fornecedores e utilizadores de IA devem cumprir as leis e regulamentos, respeitar a moralidade e a ética social, observar a ética empresarial e profissional, agir com honestidade e integridade, cumprir sua obrigação de proteger a segurança da IA e assumir sua responsabilidade perante a sociedade. Não devem comprometer o interesse público, nem prejudicar os direitos e interesses legítimos de indivíduos e organizações. É incentivado que os desenvolvedores de IA incorporem restrições de uso nos designs dos produtos para prevenir que os utilizadores empreguem a IA em actividades ilegais;
- g) Princípio da intervenção humana: os desenvolvedores e fornecedores de IA devem avaliar e explicar os riscos de segurança dos produtos e serviços de IA, e estabelecer mecanismos de supervisão e auditoria humana, em conformidade com a lei.

ARTIGO 7.º

(Desenvolvimento de Infra-estruturas)

1. O Estado reforça a construção de infra-estruturas de IA, orienta de forma racional a alocação e o fornecimento de recursos nacionais de capacidade computacional, e promove a interconexão e interoperabilidade de diferentes sistemas de computação.
2. O Estado apoia a construção de plataformas públicas de dados abertos, necessárias para o desenvolvimento da indústria de IA, e encoraja todas

os sectores em todo o território nacional ou circunscrições administrativas, a explorar activamente a disponibilização de dados públicos para uso.

ARTIGO 8.º

(Protecção dos Direitos de Propriedade Intelectual)

O Estado protege os direitos de propriedade intelectual no campo da inteligência artificial (IA), que em conformidade com a lei, explora mecanismos inovadores para a conversão de conquistas científicas em aplicações práticas e aprimora os mecanismos de suporte interactivo para inovação tecnológica, protecção da propriedade intelectual e padronização no campo da IA.

ARTIGO 9.º

(Desenvolvimento Sustentável)

1. O Estado incentiva e apoia a adopção de tecnologias sócio ambientalmente sustentáveis e de economia de energia limpa nas actividades de desenvolvimento, fornecimento e uso de IA, promovendo activamente aplicações inovadoras e de baixo consumo energético das tecnologias de IA.
2. Quando o Estado construir infra-estruturas digitais relacionadas aos recursos computacionais de IA, deverão seguir estritamente o princípio do desenvolvimento sustentável, coordenando e alocando racionalmente os recursos computacionais de acordo com os planos de desenvolvimento e protegendo o ambiente.

CAPÍTULO II

DESENVOLVIMENTO E PROMOÇÃO DA IA

ARTIGO 10.º

(Planeamento do Desenvolvimento da IA)

O Estado formula planos de desenvolvimento da IA, apoia o desenvolvimento de alta qualidade da teoria, tecnologia e aplicações de IA, e promove a integração profunda e a aplicação da IA nos campos económico e social.

ARTIGO 11.º

(Construção de Infra-estruturas Computacionais)

1. O Estado promove a construção de infra-estruturas computacionais, otimizando sua disposição com foco no desenvolvimento da indústria de IA e nas necessidades de desenvolvimento social e económico, reforça a coordenação e integração da cadeia produtiva, apoia a participação dos agentes económicos, promove o desenvolvimento sustentável e de baixo carbono das infra-estruturas computacionais, e avança na construção de um sistema de padrões para computação.
2. Devem ser adoptados *softwares* e *hardwares* básicos seguros e confiáveis para a construção de infra-estruturas computacionais, a fim de garantir a segurança da cadeia de suprimentos.
3. As entidades que operam as infra-estruturas computacionais devem aprimorar sua capacidade de segurança e resposta a emergências, realizando inspecções e verificações regulares.

ARTIGO 12.º

(Utilização de Recursos Computacionais)

1. O Estado estabelece mecanismos para a alocação de recursos de infra-estruturas computacionais, planeja de forma unificada a construção de nós de rede computacional, reforça a disposição científica de recursos diversificados, como computação geral, computação inteligente e supercomputação, e promove activamente a interconexão e interoperabilidade desses recursos.
2. O Estado promove a diversificação da estrutura computacional, orienta diversas indústrias na alocação racional de recursos computacionais,

fomenta o compartilhamento colaborativo e a utilização integrada de recursos computacionais, explora a comercialização orientada pelo mercado desses recursos, aprimora o sistema de alocação de recursos computacionais e aumenta a eficiência de uso das infra-estruturas computacionais.

3. O Estado incentiva a construção e a utilização de plataformas públicas de recursos computacionais, oferecendo suporte público para o desenvolvimento de tecnologias e indústrias de IA, e assegura que pequenas e médias empresas tenham acesso a esses recursos públicos inclusivos.

ARTIGO 13.º

(Inovação em Modelos Algorítmicos)

1. Estado promove a inovação em modelos algorítmicos e sua aplicação, expansão e circulação em conformidade com a lei.
2. As autoridades competentes da IA orientam as organizações industriais na formulação de um catálogo de modelos algorítmicos recomendados e de directrizes de cooperação para melhorar os mecanismos de compartilhamento de benefícios na circulação desses modelos.
3. O Estado apoia entidades relevantes na realização de inovações em modelos fundacionais e no desenvolvimento de um sistema teórico básico para a inteligência artificial de propósito geral.

ARTIGO 14.º

(Inovação em Tecnologias-Chave)

1. O Estado promove a realização de inovações e desenvolvimentos em tecnologias-chave por entidades relevantes, aprimora a capacidade de inovação independente em áreas estratégicas, adere aos princípios de controlo independente, segurança e eficiência, e fomenta o desenvolvimento de alta qualidade da indústria de IA.

2. Para pesquisas de inovação tecnológica em áreas-chave financiadas com recursos públicos, o Estado fornece, de acordo com a lei, suporte financeiro e meios experimentais.

ARTIGO 15.º

(Construção do Ecossistema de Código Aberto)

1. Estado promove a construção do ecossistema de código aberto, apoia entidades relevantes na criação ou operação de plataformas, comunidades e projectos de código aberto, incentiva as empresas a disponibilizarem publicamente código-fonte de *software*, designs de hardware e serviços de aplicação, e fomenta um ecossistema de inovação colaborativa e partilhada em código aberto.
2. O Estado estabelece um sistema de governação de código aberto, incentiva a regulação do licenciamento de produtos de código aberto, a protecção de propriedade intelectual e os mecanismos de alocação de responsabilidades por meio de acordos, e promove a criação de normas industriais para o ecossistema de código aberto.

ARTIGO 16.º

(Fornecimento de Factores de Produção de Dados)

1. O Estado incentiva e apoia a construção de conjuntos de dados e bases de dados de alta qualidade no campo da IA, e no aprimoramento de sua capacidade de fornecimento de dados de alta qualidade.
2. O Estado encoraja a realização de um desenvolvimento colaborativo de tecnologias de *big data* e IA, e o desenvolvimento de ferramentas profissionais e de padrões para rotulagem de dados.
3. As autoridades competentes da IA estabelecem um mecanismo de coordenação de recursos de dados para a indústria de IA e, em conformidade com a lei, promovem a circulação e o compartilhamento

dos factores de produção de dados, a fim de incentivar o desenvolvimento da indústria de IA.

ARTIGO 17.º

(Utilização de Dados Públicos)

O Estado incentiva o estabelecimento de mecanismos de partilha de recursos de dados de IA e promove a disponibilização e o partilha de dados públicos.

ARTIGO 18.º

(Construção de Redes de Informação)

O Estado promove a construção de redes de informação, apoia a participação de agentes económicos, eleva o nível de construção de infra-estruturas de rede, reforça a construção de infra-estruturas críticas de informação, constrói um sistema de infra-estruturas de rede inteligente e eficiente, e mantém a segurança cibernética de acordo com a lei.

ARTIGO 19.º

(Protecção de Direitos de Propriedade Intelectual)

1. O Estado estabelece e aprimora as regras de protecção dos direitos de propriedade intelectual, de dados de treinamento, algoritmos e conteúdos gerados por IA.
2. Os produtos de *software*, patentes de invenção, patentes de modelo de utilidade, segredos comerciais, desenhos de circuitos integrados e outros tipos de direitos de propriedade intelectual formados durante o desenvolvimento e aplicação de IA são protegidos em conformidade com a lei.

3. Os direitos de propriedade intelectual formados pelo uso de IA para criação, invenção, *design* industrial e outras actividades intelectuais também são protegidos, nos termos da legislação aplicável.

ARTIGO 20.º

(Uso Razoável de Dados)

1. O uso de IA é razoável quando o seu desenvolvedor utiliza dados protegidos por direitos de propriedade intelectual de terceiros para treinamento de modelos, nos casos em que o uso seja diferente do propósito ou da função original dos dados e não afecte o uso normal dos dados ou prejudique de forma irrazoável os direitos e interesses legítimos do proprietário dos dados.
2. O uso razoável de dados nos termos do número anterior, isenta o desenvolvedor de IA de pagamento de remuneração ao proprietário dos dados e da permissão deste, mas a fonte dos dados deve ser claramente identificada de maneira visível.

ARTIGO 21.º

(Tecnologia e Serviços de Segurança)

1. O Estado apoia entidades relevantes no desenvolvimento e aplicação de tecnologias de segurança cibernética, segurança de dados e segurança algorítmica, acelerando a inovação em tecnologias de segurança, bem como que organizações profissionais prestem serviços em conformidade com a lei.
2. As actividades de desenvolvimento e utilização de IA pelos serviços de Segurança, serão reguladas em diploma próprio.

ARTIGO 22.º

(Contratação de Seguro)

1. Os desenvolvedores e fornecedores de IA devem contratar produtos de seguro adequados para produtos e serviços de IA, nomeadamente os seguros de segurança cibernética e seguros de responsabilidade civil de terceiros.
2. O Estado incentiva as seguradoras a explorar e desenvolver produtos de seguro adequados para produtos e serviços de IA.

CAPÍTULO III

PROTECÇÃO DOS DIREITOS E INTERESSES DOS USUÁRIOS

ARTIGO 23.º

(Direitos Iguais)

Os desenvolvedores e fornecedores de IA devem adoptar medidas razoáveis para assegurar a igualdade entre os usuários, garantir a universalidade e a equidade dos produtos e serviços, e evitar preconceitos e discriminação com base em género, crença, região, idade, etnia e capacidade económica.

ARTIGO 24.º

(Direito à Informação)

1. No fornecimento de produtos e serviços, os fornecedores de IA devem garantir o direito à informação dos usuários e fornecer as seguintes informações de forma apropriada:
 - a) Nome, outras informações importantes e forma de obtenção de informações relevantes do fornecedor de produtos e serviços de IA;
 - b) Funções, propósitos e intenção, e principais mecanismos de operação dos produtos e serviços de IA;

- c) Limitações funcionais, riscos potenciais e possíveis impactos sobre os direitos e interesses dos usuários dos produtos e serviços de IA;
 - d) Informações de licenciamento ou registo dos produtos e serviços de IA;
 - e) Direitos e canais de reclamação e recursos disponíveis para os usuários;
 - f) Outras informações previstas na legislação aplicável.
2. Os desenvolvedores de IA devem cooperar com os fornecedores de IA no cumprimento das obrigações previstas no número anterior.

ARTIGO 25.º

(Protecção da Privacidade e das Informações Pessoais)

1. Os desenvolvedores e fornecedores de IA devem proteger a privacidade e as informações pessoais, nos termos da legislação aplicável.
2. Os desenvolvedores e fornecedores de IA devem aceitar e tratar prontamente os pedidos de consulta, cópia, correcção, aperfeiçoamento e exclusão das informações pessoais dos indivíduos, nos termos da legislação aplicável.
3. Os desenvolvedores e fornecedores de IA não devem utilizar a IA para analisar ou avaliar os hábitos comportamentais, interesses ou informações sobre a situação económica, de saúde ou de crédito de uma pessoa sem o seu consentimento, salvo se for para assegurar o cumprimento da lei nos termos prescritos na legislação aplicável.
4. Os desenvolvedores e fornecedores de IA devem informar claramente os usuários, com a devida antecedência, caso os seus produtos e serviços apresentem riscos à protecção ou à privacidade, ou possam violar os direitos e interesses relacionados às informações pessoais dos usuários.
5. Os desenvolvedores e fornecedores de IA não devem colectar informações pessoais não essenciais, reter ilegalmente informações

inseridas e registos de uso que possam identificar os usuários, nem fornecer ilegalmente essas informações e registos a terceiros.

ARTIGO 26.º

(Direito a Esclarecimento e a Recusa de Decisões Baseadas em IA)

1. As pessoas cujos direitos e interesses legítimos possam ser afectados por produtos e serviços de IA têm o direito de:
 - a) Solicitar os devidos esclarecimentos ao fornecedor de IA;
 - b) Rejeitar as decisões tomadas exclusivamente por produtos e serviços de IA;
 - c) Solicitar que o fornecedor de IA repita a tomada de decisão com a participação de seres humanos.
2. Os fornecedores de IA devem garantir aos usuários o direito de se retirarem ou recusarem o uso de IA, salvo se tal for parte das funções básicas de produtos e serviços.

ARTIGO 27.º

(Direitos de Propriedade Intelectual de Conteúdo Gerado por IA)

1. O conteúdo gerado por IA que preencham os requisitos da legislação sobre a propriedade intelectual para o seu reconhecimento como obra, invenção ou criação, é protegido nos termos dessa legislação, desde que o respectivo titular ou proprietário seja uma pessoa singular ou colectiva, com personalidade jurídica e capacidade jurídica.
2. O usuário deve divulgar como tal, o conteúdo gerado por IA, quando for tratado como obra, invenção ou criação, nos termos da legislação aplicável.
3. O fornecedor de IA e o usuário devem celebrar acordo sobre a titularidade do conteúdo gerado por IA, e, na ausência de acordo ou se o acordo for ambíguo, os direitos relevantes serão conferidos ao usuário.

ARTIGO 28.º

(Direitos e Interesses dos Trabalhadores)

1. O empregador não deve utilizar IA de forma indevida para violar os direitos e interesses legítimos dos trabalhadores.
2. Os empregadores devem informar claramente aos trabalhadores sobre o escopo de uso, as funções básicas e a base legal da IA ao celebrar contratos de trabalho.
3. É proibido ao empregador a tomada de decisões punitivas com base exclusiva em IA, bem como de usar IA para estender ilegalmente as jornadas de trabalho ou violar os direitos dos trabalhadores ao descanso e férias.
4. É igualmente proibido ao empregador o uso da IA para realizar actividades de gestão interna que violem a privacidade e os direitos relacionados a protecção de dados pessoais.

ARTIGO 29.º

(Direitos e Interesses de Grupos Digitalmente Desfavorecidos)

Os desenvolvedores e fornecedores de IA devem considerar plenamente as necessidades diferenciadas de menores, idosos, mulheres, pessoas com deficiência e outros grupos com menor acesso e habilidades digitais, fornecendo-lhes produtos e serviços de IA inclusivos, estáveis e acessíveis.

ARTIGO 30.º

(Direito de Obter Ajuda e Treinamento)

1. Os desenvolvedores e fornecedores de IA devem fornecer meios adequados de interacção homem-máquina para facilitar o uso pelos usuários.
2. Os fornecedores de produtos e serviços de IA que envolvam direitos e interesses legítimos de pessoas devem fornecer assistência e treinamento em habilidades.

ARTIGO 31.º

(Direito de Reclamação e de Acção Judicial)

1. Os fornecedores de IA devem estabelecer um mecanismo célere para apreciar e decidir sobre as reclamações formuladas pelas pessoas no exercício dos seus direitos.
2. As decisões desfavoráveis de reclamações devem ser fundamentadas e notificadas por escrito dentro de um prazo razoável.
3. É assistido às pessoas o direito de acção judicial nos termos da lei, nos casos em que o fornecedor de IA decida desfavoravelmente a reclamação formulada ou não a proceda a sua apreciação de forma oportuna e tempestiva.

CAPÍTULO IV

OBRIGAÇÕES E REQUISITOS A OBSERVAR PELOS DESENVOLVEDORES E FORNECEDORES DE IA

SECÇÃO I

DISPOSIÇÕES GERAIS

ARTIGO 32.º

(Obrigações de Segurança)

1. Os desenvolvedores e fornecedores de IA devem adoptar medidas organizacionais e técnicas para garantir que o desenvolvimento e fornecimento de produtos e serviços de IA sejam realizados de acordo com as disposições desta Lei e demais legislação, prevenindo a ocorrência de incidentes de segurança em IA.
2. Os desenvolvedores e fornecedores de IA devem realizar inspecções e monitoramento regulares de vulnerabilidades e riscos de segurança em *frameworks* de código aberto, *softwares* e *hardwares* básicos, e ambientes de implantação, além de monitorar em tempo real possíveis ataques.

3. Devem também salvar informações de *log* das actividades de desenvolvimento e fornecimento de IA, conforme exigido por legislação aplicável.
4. As contramedidas para riscos de segurança em IA devem ser proporcionais à magnitude dos riscos, à probabilidade de ocorrência, ao nível de desenvolvimento tecnológico e ao custo de implementação.

ARTIGO 33.º

(Avaliação de Riscos de Segurança)

1. Os desenvolvedores e fornecedores de IA devem realizar uma avaliação de riscos de segurança antes de fornecer produtos e serviços, devendo registar as circunstâncias do tratamento.
2. A avaliação de riscos de segurança em IA deve incluir:
 - a) Potenciais vieses ou discriminações;
 - b) Impacto sobre o interesse público, os direitos e interesses individuais e riscos de segurança;
 - c) Se a revisão de ética científica e tecnológica foi conduzida conforme a lei;
 - d) Se as medidas de protecção são legais, eficazes e apropriadas ao nível de risco.
3. Em caso de mudanças significativas nos produtos e serviços de IA, a avaliação de riscos de segurança deve ser refeita.
4. Os desenvolvedores e fornecedores de IA podem realizar avaliações de riscos de segurança por eles próprios ou por intermédio de terceiros.

5. O relatório de avaliação de riscos de segurança e os registos das circunstâncias de tratamento devem ser mantidos por um período não inferior a três anos.

ARTIGO 34.º

(Comunicação de Incidentes de Segurança e Protecção Significativos)

1. Os desenvolvedores e fornecedores de IA devem tomar medidas imediatas para lidar com incidentes de segurança e protecção em IA.
2. No caso de um incidente significativo, deve-se comunicar imediatamente autoridade competente da IA, nos termos a estabelecer em regulamento próprio.
3. Os métodos para a comunicação de incidentes significativos de segurança em IA são estabelecidos pela autoridade competente da IA.

ARTIGO 35.º

(Manutenção da Segurança dos Segurados)

1. Após a contratação de seguros, os desenvolvedores e fornecedores de IA devem garantir a segurança dos segurados conforme a lei.
2. A seguradora pode, de acordo com o contrato, inspeccionar o estado de segurança do segurado e fazer recomendações por escrito para melhorar a segurança ou conformidade dos produtos e serviços de IA, eliminando riscos técnicos potenciais.
3. Se o desenvolvedor ou fornecedor de IA não cumprir sua responsabilidade de manter a segurança dos segurados, a seguradora tem o direito de solicitar um aumento no prémio ou rescindir o contrato.
4. A seguradora pode, com o consentimento do segurado, adoptar medidas de precaução para garantir a segurança dos segurados.

ARTIGO 36.º

(Qualidade dos Dados)

1. Os desenvolvedores de IA devem adoptar medidas eficazes para melhorar a qualidade dos dados de treinamento, aprimorando a veracidade, precisão, objectividade e diversidade dos conjuntos de dados.
2. Os desenvolvedores de IA devem tomar as medidas necessárias caso sejam encontrados dados proibidos por leis e regulamentos.

ARTIGO 37.º

(Directrizes de Conformidade)

1. Os fornecedores de IA devem garantir que os produtos e serviços fornecidos estejam em conformidade com as disposições desta Lei e demais legislação relevantes, assegurando que suas funções sejam seguras, transparentes, estáveis e sustentáveis.
2. Os fornecedores de IA devem esclarecer de forma apropriada o público-alvo, ocasiões e usos aplicáveis de seus produtos e serviços, orientando os usuários a entendê-los e utilizá-los de forma segura, científica e racional.
3. Caso verifiquem que os usuários estão utilizando os produtos e serviços de IA para actividades ilícitas, os fornecedores de IA devem adoptar medidas como advertências, restrições de funções e suspensão ou interrupção dos serviços, mantendo os registos relevantes e reportando o facto a autoridade competente para a fiscalização e supervisão da IA.

ARTIGO 38.º

(Segurança e Protecção de Conteúdo)

1. Os fornecedores que oferecem serviços de informações em rede devem cumprir as obrigações de segurança da informação em rede, nos termos estabelecidos na lei.
2. Os fornecedores devem adoptar medidas para prevenir a geração de informações falsas, prejudiciais ou de outros conteúdos proibidos por lei e regulamento.

3. Caso descubram conteúdo ilegal, devem tomar medidas imediatas, como interromper a geração e transmissão, eliminá-lo e relatá-lo ao principal departamento de fiscalização de IA.

ARTIGO 39.º

(Obrigações de Identificação)

1. Os desenvolvedores e fornecedores de IA devem colocar identificadores invisíveis em locais e áreas razoáveis do conteúdo dos produtos e serviços, e estabelecer um mecanismo de rastreabilidade da informação para garantir a legibilidade e segurança desses identificadores invisíveis.
2. Quando os produtos e serviços de IA possam causar confusão ou identificação incorrecta pelo público, o fornecedor deve adoptar medidas técnicas para adicionar, em locais e áreas razoáveis do conteúdo, identificadores visíveis que não prejudiquem o uso pelos usuários, informando o público de forma clara sobre as características dos produtos e serviços de IA.
3. Nenhuma pessoa ou qualquer outra organização pode usar meios técnicos para apagar, alterar ou ocultar os identificadores adicionados aos produtos e serviços de IA em conformidade com a lei.

ARTIGO 40.º

(Requisitos de Acesso)

1. Os desenvolvedores e fornecedores de IA devem obter as autorizações necessárias nos termos da lei, se da legislação aplicável resultar a obrigação de licenciamento do desenvolvimento e fornecimento de produtos e serviços de IA.
2. O investimento em produtos e serviços de IA também deve cumprir as disposições da legislação sobre investimento privado.

SECÇÃO II

IA CRÍTICA

ARTIGO 41.º

(Abrangência da IA Crítica)

A IA crítica inclui os seguintes tipos:

- a) IA aplicada a infra-estruturas críticas de informação;
- b) IA que impacte significativamente direitos pessoais como a vida, liberdade e a dignidade;
- c) Modelos fundacionais que alcancem determinados níveis em aspectos como capacidade computacional, parâmetros ou escala de uso;
- d) Outros casos prescritos por leis e regulamentos.

ARTIGO 42.º

(Medidas de Protecção para a IA Crítica)

1. Os desenvolvedores e fornecedores de IA crítica devem estabelecer medidas de protecção de segurança e sincronizar o planeamento, construção e uso dessa IA.
2. Desenvolvedores, fornecedores e usuários de IA crítica devem dar prioridade à aquisição de equipamentos físicos e serviços de informação seguros e confiáveis.
3. Os desenvolvedores de IA crítica que realizarem actividades de rotulagem de dados devem formular regras de rotulagem de dados em conformidade com leis e regulamentos e os requisitos prescritos pela autoridade competente da IA, estabelecendo um mecanismo de auditoria de rotulagem de dados para melhorar a equidade, precisão e veracidade da rotulagem.

ARTIGO 43.º

(Estrutura Organizacional para IA Crítica)

1. Os desenvolvedores e fornecedores de IA crítica devem criar uma estrutura especializada na gestão de segurança responsável pela gestão de segurança da IA crítica.
2. Os desenvolvedores e fornecedores de IA crítica devem igualmente designar uma pessoa responsável pela protecção da IA, encarregada da supervisão e gestão das actividades de desenvolvimento e fornecimento da IA, bem como das medidas de protecção adoptadas.
3. As informações de contacto da pessoa responsável devem ser públicas, devendo o seu nome e informações de contacto ser reportados à autoridade competente da IA.

ARTIGO 44.º

(Registo da IA Crítica)

1. Os fornecedores de IA crítica devem, no prazo de 7 dias úteis a partir da data de notificação de determinação como fornecedores de IA crítica, registar-se na plataforma nacional de fiscalização de IA e realizar os procedimentos de arquivamento.
2. A autoridade competente da IA deve, no prazo de 30 dias úteis, realizar o arquivamento ou solicitar materiais adicionais.
3. Outros produtos e serviços de IA que, por lei, exijam registo, devem seguir os procedimentos prescritos por lei e regulamento.

ARTIGO 45.º

(Avaliação de Riscos de Segurança da IA Crítica)

1. Os desenvolvedores e fornecedores de IA crítica devem realizar, por eles próprios ou por intermédio de terceiros, pelo menos uma avaliação de riscos de segurança da IA crítica por ano.

2. Os problemas de segurança identificados durante a avaliação referida no número anterior, devem ser imediatamente corrigidos e reportados à autoridade competente da IA.

ARTIGO 46.º

(Divulgação de Riscos de Segurança da IA Crítica)

1. Os desenvolvedores e fornecedores de IA crítica devem estabelecer um mecanismo de divulgação de riscos de segurança, fortalecendo o monitoramento em todos os aspectos da IA.
2. Sempre que se identificarem riscos de segurança, os desenvolvedores e fornecedores de IA crítica devem cumprir as obrigações de notificação e informação dos usuários de forma imediata.
3. Os desenvolvedores e fornecedores de IA crítica devem também fornecer meios apropriados de interação humano-computador para facilitar a supervisão manual efectiva durante o uso dos produtos e serviços.

ARTIGO 47.º

(Resposta a Emergências de Segurança para IA Crítica)

1. Os desenvolvedores e fornecedores de IA crítica devem estabelecer um plano de resposta a emergências de segurança.
2. Em caso de incidente de segurança, devem activar imediatamente o plano, resumir as informações de risco, adoptar medidas correctivas apropriadas e reportar à autoridade competente da IA.
3. Os desenvolvedores e fornecedores de IA crítica podem ainda adoptar medidas emergenciais, incluindo a interrupção de operações quando necessário, e retomar as operações assim que os riscos de segurança forem eliminados.

ARTIGO 48.º

(Obrigação de Reportar Alterações nas Entidades de IA Crítica)

Quaisquer alterações que ocorram na estrutura societária dos desenvolvedores e fornecedores de IA crítica, sejam elas fusões, cisões ou dissoluções, devem imediatamente ser comunicadas à autoridade competente da IA e ao mesmo tempo que de assegurar uma gestão da IA crítica em conformidade com os requisitos estabelecidos por essa autoridade.

CAPÍTULO V

REGIMES ESPECIAIS DE APLICAÇÃO DA IA

ARTIGO 49.º

(Uso de IA por Órgãos do Estado e pela Administração Pública)

Os órgãos e serviços do Estado e da administração pública que utilizem IA devem respeitar os princípios da constitucionalidade, juridicidade, legalidade, justiça, boa-fé, transparência e proporcionalidade, devendo apenas recorrer a decisões baseadas em IA apenas como referência.

ARTIGO 50.º

(IA Jurisdicional)

Os órgãos jurisdicionais apenas devem usar a IA para auxiliar nas suas decisões, devendo observar princípios da constitucionalidade, juridicidade, segurança, legalidade e transparência.

ARTIGO 51.º

(IA para Notícias)

O uso de IA em serviços de notícias deve assegurar a veracidade das informações, utilizando identificadores visíveis para conteúdo gerado por IA.

ARTIGO 52.º

(IA Médica)

Os serviços médicos baseados em IA devem possuir as licenças adequadas, e as decisões baseadas em IA devem servir apenas como referência médica.

ARTIGO 53.º

(*Bots* Sociais)

Os fornecedores de *bots* sociais devem controlar a qualidade das informações e impedir abusos que manipulem a opinião pública.

ARTIGO 54.º

(Reconhecimento Biométrico)

O uso de IA em dados biométricos deve ter um propósito específico e adoptar medidas rigorosas de protecção.

ARTIGO 55.º

(Condução Autónoma)

Os veículos autónomos devem cumprir regulamentos específicos e assegurar a segurança no trânsito.

ARTIGO 56.º

(Requisitos Especiais para IA de Propósito Geral)

Os desenvolvedores de IA de propósito geral devem garantir segurança e confiabilidade, realizando avaliações regulares e relatando os resultados à autoridade competente da IA.

CAPÍTULO VI

MODELO DE GOVERNAÇÃO DA IA

ARTIGO 57.º

(Governança Diversificada e Colaborativa)

O Estado estabelece e aperfeiçoa o sistema de governação da IA, caracterizado pela liderança da administração pública, coordenação com a sociedade e participação pública, e constrói um modelo de governação colaborativa e diversificada no campo da IA.

ARTIGO 58.º

(Mecanismo de Coordenação Geral)

1. O Estado estabelece um mecanismo de planeamento e coordenação geral para a IA, com o objectivo de orientar, coordenar e planear de forma abrangente o desenvolvimento e a gestão da IA em Angola.
2. O mecanismo de coordenação geral para IA cabe à autoridade competente da IA e deve promover o seguinte:
 - a) Pesquisas sobre a IA;
 - b) Formulação e implementação de estratégias e planos sobre a IA;
 - c) Estabelecimento e implementação de mecanismos para supervisão e gestão de riscos da IA;
 - d) Formulação de regras e padrões específicos para a revisão ética, rotulagem de dados, segurança da IA crítica, categorização e registo de licenças;
 - e) Construção de um sistema de serviços orientado à sociedade para avaliação de IA, e apoiar instituições relevantes na educação e formação em IA;
 - f) Outras funções estabelecidas em diploma próprio.

ARTIGO 59.º

(Coordenação Diversificada)

O Estado incentiva a criação de organizações da indústria de IA, promovendo a colaboração com instituições educacionais e científicas para prevenir e gerir riscos de IA.

ARTIGO 60.º

(Comissão de Especialistas)

A autoridade competente da IA e demais órgãos e serviços da administração pública relevantes organizam uma comissão de especialistas para a prestação de suporte técnico e consultivo em tecnologia, ética e legislação.

CAPÍTULO VII

REGULAÇÃO, SUPERVISÃO E FISCALIZAÇÃO

ARTIGO 61.º

(Autoridade Competente da IA)

1. Para efeitos da presente Lei, deve ser estabelecida, por regulamento próprio, uma autoridade competente responsável pela Inteligência Artificial.
2. Sem prejuízo dos demais órgãos e serviços administrativos relevantes, à autoridade competente da IA cabe exercer as funções de regulação, supervisão e fiscalização da IA em Angola.

ARTIGO 62.º

(Funções de Regulatórias e de Fiscalização)

A autoridade competente da IA, em colaboração com as demais autoridades nas indústrias ou áreas relevantes, têm as seguintes funções:

- a) Formular normas técnicas de implementação para fiscalização e gestão da IA;
- b) Realizar campanhas educativas sobre conformidade e orientar desenvolvedores, fornecedores e usuários de IA no cumprimento das suas obrigações legais;
- c) Organizar avaliações de risco de produtos e serviços de IA;
- d) Investigar e lidar com actividades ilegais relacionadas ao desenvolvimento, fornecimento e uso de IA;
- e) Apreçar e decidir sobre queixas e denúncias relativas a produtos e serviços de IA;
- f) Outras funções prescritas em diploma próprio.

ARTIGO 63.º

(Categorização e Classificação)

1. O Estado estabelece um sistema de categorização e classificação da IA com base na sua importância para o desenvolvimento económico e social e no grau de risco que pode causar à segurança nacional, ao interesse público ou aos direitos e interesses legítimos das pessoas.
2. A autoridade competente da IA estabelece mecanismos de avaliação, ajustando padrões de classificação conforme o desenvolvimento tecnológico e cenários de aplicação.

ARTIGO 64.º

(Fiscalização Especial da IA Crítica)

O Estado implementa um sistema de supervisão especial para IA crítica, incluindo:

- a) Identificação e divulgação de IA crítica;
- b) Emissão de catálogos de produtos para aquisição de IA crítica;
- c) Avaliações regulares ou certificações de segurança realizadas por terceiros;

- d) Inspeções e auditorias de segurança de produtos de IA crítica;
- e) Exercícios regulares de resposta a emergências de segurança.

ARTIGO 65.º

(Monitoramento de Riscos e Resposta a Emergências)

A autoridade competente da IA coordena a formulação de sistemas de monitoramento e de alerta de segurança em IA, colecta e análise de informações de segurança, bem como a notificação pública de informações relevantes.

ARTIGO 66.º

(Avaliação e Certificação)

O Estado promove a avaliação e certificação de segurança em IA, apoiando organizações profissionais que realizem essas actividades.

ARTIGO 67.º

(Supervisão, Inspeção e Cooperação)

A autoridade competente da IA pode realizar inspeções, copiar documentos relevantes e, quando necessário, apreender equipamentos utilizados ilegalmente.

CAPÍTULO VIII

REGIME DE RESPONSABILIDADE DA IA

SECÇÃO I

RESPONSABILIDADE CONTRA-ORDENACIONAL

ARTIGO 68.º

(Contra-ordenação)

1. Quem desenvolva, implemente ou comercialize sistemas de IA comete contra-ordenação por violação às disposições desta lei.

2. As contra-ordenações podem ser simples ou graves, nos termos dos artigos seguintes.

ARTIGO 69.º

(Contra-ordenações Simples)

Constituem contra-ordenações simples, as seguintes:

- a) Não elaboração ou apresentação de planos de desenvolvimento de IA;
- b) Construção de infra-estruturas computacionais com tecnologias não seguras ou sem conformidade com padrões de segurança;
- c) Falta de realização de inspecções regulares de segurança;
- d) Uso inadequado ou não licenciado de plataformas públicas de recursos computacionais;
- e) Não disponibilizar ou partilhar dados públicos conforme estipulado.

ARTIGO 70.º

(Contra-ordenações Graves)

Constituem contra-ordenações graves, as seguintes:

- a) Falta de registo de IA crítica dentro do prazo legal;
- b) Não comunicação de incidentes de segurança significativos às autoridades competentes;
- c) Falta de avaliação de riscos de segurança em IA crítica;
- d) Negação ao direito de esclarecimento ou recusa de decisões baseadas exclusivamente em IA;
- e) Colecta de informações pessoais sem consentimento ou uso indevido de IA para avaliações privadas;
- f) Violação de direitos de propriedade intelectual;
- g) Violação da privacidade, segurança ou direitos fundamentais dos utilizadores;
- h) Construção de redes de informação que comprometam a cibersegurança;
- i) Não disponibilizar ou partilhar dados públicos conforme estipulado;

- j) Não cumprimento de padrões éticos em pesquisas financiadas com recursos públicos;
- k) Desenvolvimento de modelos algorítmicos sem respeito às normas de segurança ou à circulação legal de dado;
- l) Não contratação de seguros obrigatórios para produtos e serviços de IA.

ARTIGO 71.º

(Responsabilidade Contra-ordenacional Objectiva)

É punido por contra-ordenação, independentemente da comprovação de dolo ou negligência, sempre que se constate a utilização inadequada de sistemas de IA que:

- a) Comprometa a privacidade, segurança ou direitos fundamentais dos utilizadores;
- b) Infrinja normas técnicas ou éticas previstas na lei ou regulamento.

ARTIGO 72.º

(Coimas)

1. As contra-ordenações simples são puníveis com as seguintes coimas:
 - a) Tratando-se de pessoa singular, o montante mínimo da coima é de 1 salário mínimo nacional e o máximo de 1 000 salários;
 - b) Tratando de pessoa colectiva, o montante mínimo da coima é de 10 salários mínimos nacionais e o máximo de 7 500 salários.
2. As contra-ordenações graves são puníveis com as seguintes coimas:
 - c) Tratando-se de pessoa singular, o montante mínimo da coima é de 10 salários mínimos nacionais e o máximo de 7 500 salários;
 - d) Tratando de pessoa colectiva, o montante mínimo da coima é de 50 salários mínimos nacionais e o máximo de 15 000 salários.

ARTIGO 73.º

(Sanções Acessórias)

As contra-ordenações graves podem ser simultaneamente punidas com coima e com as seguintes sanções acessórias:

- a) Perda dos equipamentos ou sistemas e demais objectos utilizados na prática da contra-ordenação;
- b) Encerramento do estabelecimento ou instalações utilizadas para a prática da contra-ordenação por período de dois anos;
- c) Privação do direito a subsídio ou benefício outorgado por entidade ou serviço público por período de dois anos;
- d) Suspensão de registos, licenças ou quaisquer autorizações dadas nos termos da presente lei e demais legislação complementar, por período de dois anos.

ARTIGO 74.º

(Aplicação das Coimas e Sanções Acessórias)

1. As coimas e sanções acessórias previstas na presente lei, são aplicadas pela autoridade competente da IA.
2. Na aplicação de coimas e acessórias previstas na presente lei, são observados os seguintes critérios de graduação:
 - a) Grau de culpabilidade do agente;
 - b) Gravidade da contra-ordenação, considerando o risco ou dano causado aos direitos fundamentais e ao interesse público;
 - c) Capacidade económica do agente, garantindo proporcionalidade e eficácia da sanção;
 - d) Benefícios económicos obtidos com a prática da contra-ordenação;
 - e) Circunstâncias atenuantes e agravantes;
 - f) Medidas de correcção espontâneas adoptadas pelo agente após a identificação da contra-ordenação;

- g) Grau de colaboração com as autoridades administrativas durante o processo de fiscalização.

ARTIGO 75.º

(Regime Supletivo)

A Lei sobre o Regime Geral das Contra-Ordenações é supletivamente aplicáveis a tudo que não esteja previsto na presente secção.

SECÇÃO II

RESPONSABILIDADE PENAL

ARTIGO 76.º

(Crimes no Âmbito da IA)

1. Comete crime punível com pena de prisão de 1 a 12 anos, salvo se outra pena mais gravosa não resultar da legislação penal, quem proceder a implantação ou utilização dolosa de sistemas de inteligência artificial, com a finalidade de:
 - a) Violar a privacidade e os direitos fundamentais das pessoas;
 - b) Promover discriminação ou incitar ao ódio através de algoritmos;
 - c) Criar danos graves à segurança nacional, à ordem pública ou ao processo democrático;
 - d) Facilitar a prática de crimes contra o Estado, incluindo espionagem; terrorismo ou outros actos que atentem contra a segurança nacional;
 - e) Comprometer de forma irreparável a integridade de instituições ou a segurança nacional.
2. Tratando-se de pessoa colectiva ou entidades equiparadas, aos crimes previstos no número anterior são aplicadas as penas de multa entre 200 e 360 dias ou dissolução, sem prejuízo das penas acessórias estabelecidas na lei penal para as pessoas colectivas e entidades equiparadas.
3. A aplicação das penas previstas no número anterior, não exclui a responsabilidade criminal do agente que actuou em nome da pessoa colectiva

ou entidade equiparada, ainda que seja em conformidade com as instruções desta.

ARTIGO 77.º

(Circunstâncias Agravantes Penais)

As penas previstas na presente lei, são agravadas até um terço quando:

- a) Houver reincidência nos termos da legislação penal e processual penal;
- b) O crime for cometido com uso de tecnologias avançadas, como *deepfakes* ou *bots* automatizados para manipular a opinião pública;
- c) O crime ocorrer em contextos de estado de excepção constitucional, situação de calamidade pública ou períodos eleitorais.

ARTIGO 78.º

(Suspensão Condicional da Pena)

Sem prejuízo da legislação penal, a execução da pena pode ser suspensa, se o agente cumprir com as seguintes condições:

- a) Reparação dos danos causados às vítimas;
- b) Participação em programas de sensibilização ou capacitação sobre o uso ético da IA;
- c) Reu primário e assumir o compromisso de não reincidência.

ARTIGO 79.º

(Concurso de Crime e Contra-ordenação)

Em caso de concurso de entre um crime e uma contra-ordenação, o tribunal que julgar o crime pode também aplicar a coima e as medidas acessórias estabelecidas na presente lei, salvo se a autoridade competente da IA as tiver já aplicado ou existir um processo de contra-ordenação pendente.

SECÇÃO III

RESPONSABILIDADE CIVIL

ARTIGO 80.º

(Responsabilidade Objectiva)

1. Constitui-se na obrigação de reparar os danos ou de indemnizar os lesados, aquele que, independentemente da culpa, desenvolva ou comercialize sistemas de inteligência artificial que tenha causado danos a terceiros ou interesses públicos ou nacionais.
2. Responsabilidade civil dos desenvolvedores e fornecedores de IA é solidária, nos termos da lei geral.

ARTIGO 81.º

(Responsabilidade Civil Conexa com a Penal)

1. A responsabilidade civil é independente da responsabilidade penal.
2. Constituindo-se o facto gerador de responsabilidade civil um crime, o pedido civil de indemnização pode ser deduzido no âmbito do processo-crime e corre por apenso a este nos termos da lei processual penal.

CAPÍTULO IX

DISPOSIÇÕES FINAIS

ARTIGO 82.º

(Publicidade das Sanções)

As decisões sancionatórias definitivas são publicadas e divulgadas com o objectivo de dissuadir os crimes e contra-ordenações, bem como promover a transparência, respeitando os direitos de privacidade do agente.

ARTIGO 83.º

(Receitas das Sanções)

Os valores arrecadados com multas e coimas serão destinados à autoridade competente da IA e aplicados no fortalecimento da fiscalização, educação pública e inovação tecnológica.

ARTIGO 84.º

(Mecanismo Piloto de Supervisão)

O Estado estabelece mecanismos piloto de supervisão, oferecendo incentivos e facilidades para desenvolvedores e fornecedores que participem de projectos-piloto.

ARTIGO 85.º

(Dúvidas e omissões)

As dúvidas e omissões resultantes da interpretação e aplicação da presente lei são resolvidas pela Assembleia Nacional.

ARTIGO 86.º

(Entrada em vigor)

A presente lei entra em vigor na data da sua publicação.

Vista e aprovada pela Assembleia Nacional, em Luanda, aos _____ de _____ de 2025.

A Presidente da Assembleia Nacional, **Carolina Cerqueira**.

Promulgada em _____ de _____ de 2025

Publique-se.

O Presidente da República, **João Manuel Gonçalves Lourenço**