Pérez-Llorca

TECHLAW

Inteligência artificial

JUNHO 2024

Um desafio para as empresas e para os reguladores

Andy Ramos

Sócio de Direito Digital

aramos@perezllorca.com
+34 91 423 20 72

Raúl Rubio

Sócio de Direito Digital

rrubio@perezllorca.com
+34 91 353 45 59

Adolfo Mesquita Nunes

Sócio de Direito Digital

adolfomesquitanunes@perezllorca.com
+351 912 585 103

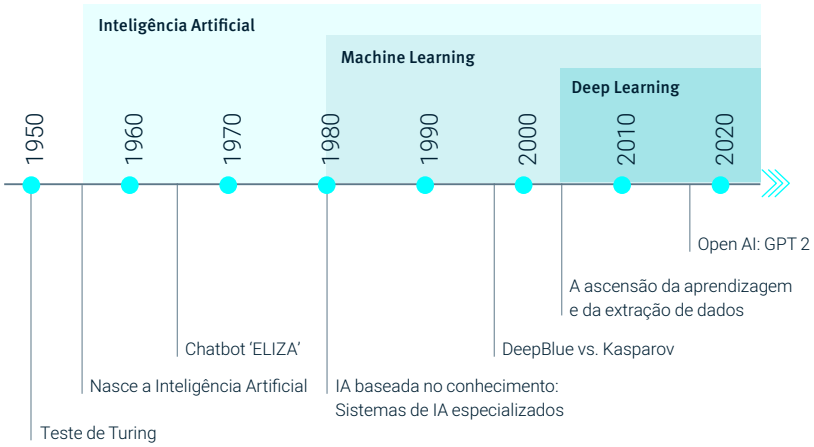
_ ANDY RAMOS, RAÚL RUBIO, ADOLFO MESQUITA NUNES, FRANCISCO RIBEIRO FERREIRA E ISABEL IGLESIAS

A primeira regulamentação da Inteligência Artificial está aqui. Aspetos fundamentais.

1. Introdução

Na era digital, a Inteligência Artificial ("**IA**") tornou-se um elemento central da inovação e do desenvolvimento tecnológico, provocando transformações significativas em todos os sectores da economia e da sociedade. O enorme potencial da IA tem, porém, gerado alguma inquietação e preocupação relativamente aos riscos que acarreta para os direitos e liberdades dos cidadãos, suscitando debates sobre o desenvolvimento e a utilização responsável e ética desta tecnologia e sendo proposta a regulação de potenciais conflitos mesmo antes de estes ocorrerem.

Para mais informações sobre os aspetos gerais da IA, recomenda-se a consulta da primeira publicação desta série, disponível aqui.



Evolução da inteligência artificial

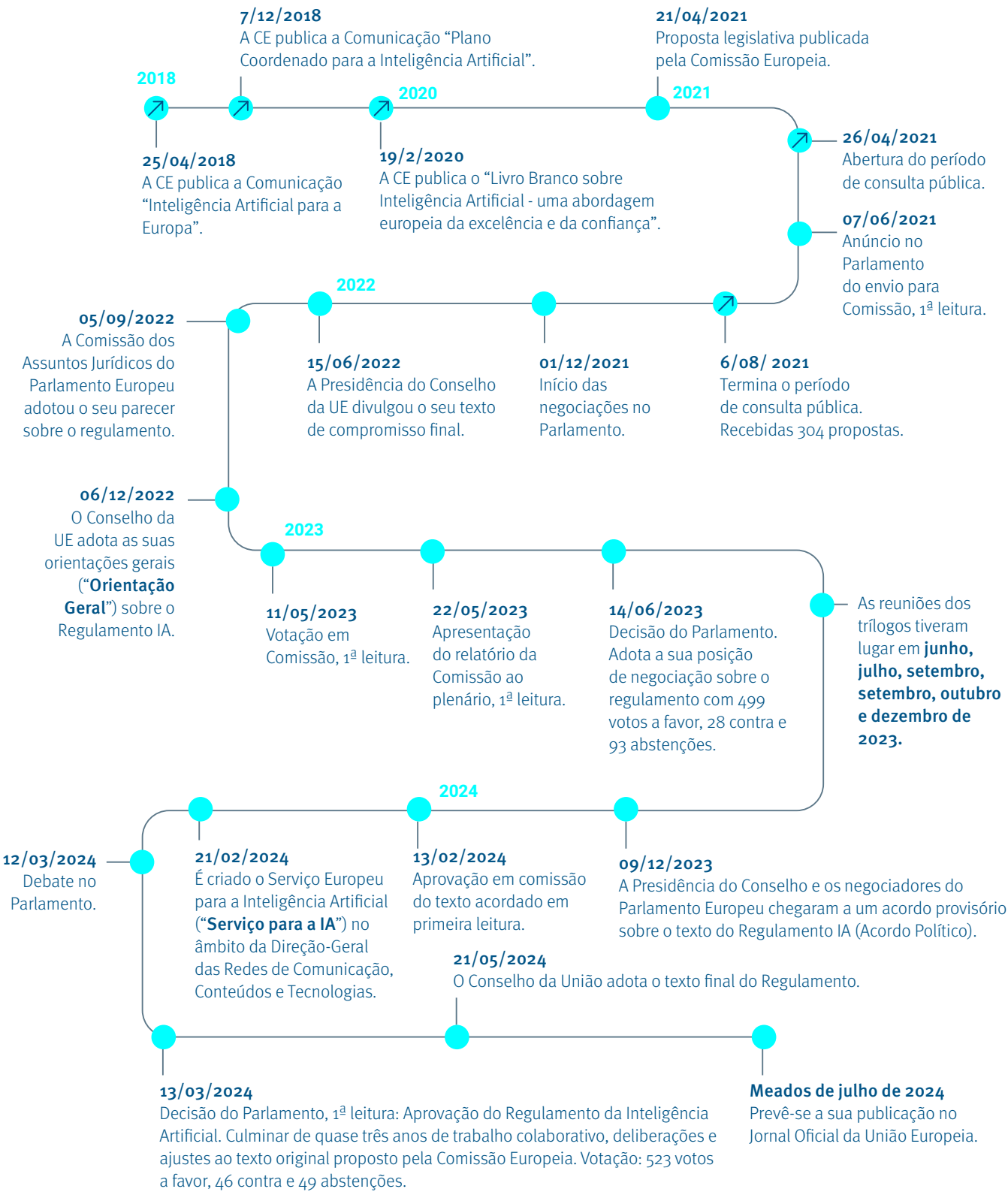
O Parlamento Europeu adotou, a 13 de março de 2024, o Regulamento da Inteligência Artificial (o "**Regulamento IA**"), um quadro legislativo destinado a estabelecer regras harmonizadas em matéria de IA nos Estados-Membros. O legislador europeu pretende que o Regulamento seja parte de um ecossistema de IA seguro, fiável e alinhado com os valores e princípios europeus. Ao fazê-lo, a UE procura posicionar-se como líder na implementação de um enquadramento jurídico completo para a IA, que não só aborda os riscos associados à sua utilização, mas também promove o seu desenvolvimento ético e humano.

Este regulamento, resultado de um longo processo legislativo, defende formalmente uma abordagem equilibrada que procura promover a inovação e o desenvolvimento tecnológico, ao mesmo tempo que garante a proteção da saúde, da segurança e dos direitos fundamentais dos cidadãos europeus. No entanto, como veremos adiante, as medidas de controlo previstas no regulamento superam largamente as medidas de promoção, sendo estas últimas muito mais vagas e pouco desenvolvidas em relação ao nível de especificidade das primeiras, o que é incoerente com os próprios considerandos do regulamento e com o atual estado incipiente da IA.

A presente nota jurídica tem por objetivo apresentar uma análise dos aspetos mais relevantes do texto adotado, as implicações jurídicas e empresariais e algumas recomendações práticas sobre a forma de adaptar a atividade económica de qualquer empresa afetada pelo regulamento.

2. Cronologia do Regulamento

O processo de elaboração e aprovação do Regulamento IA foi complexo e meticuloso, dado o carácter inovador da norma e da própria tecnologia, bem como a importância e o potencial impacto da IA na sociedade. A cronologia dos principais acontecimentos que conduziram à recente adoção do regulamento é a seguinte:



3. Objetivo do regulamento

O objetivo declarado do Regulamento IA é melhorar o funcionamento do mercado interno, estabelecendo um quadro jurídico uniforme para o desenvolvimento, a colocação no mercado, a colocação em serviço e a utilização de sistemas de IA na UE.

O regulamento procura promover a adoção de uma IA centrada no ser humano e de confiança, assegurando simultaneamente um elevado nível de proteção da saúde, da segurança e dos direitos fundamentais, e apoiar a inovação. Além disso, estabelece regras harmonizadas para a introdução no mercado de sistemas de IA, proibições de certas práticas de IA, requisitos específicos para sistemas de IA de risco elevado, regras de transparência e medidas de apoio à inovação.

> ***"o regulamento procura equilibrar a promoção da inovação e do desenvolvimento tecnológico com a necessidade de garantir que a IA seja desenvolvida e utilizada de uma forma que respeite os direitos e valores fundamentais da União Europeia".***

Além disso, o Considerando 27 do Regulamento IA destaca a importância de uma abordagem baseada no risco para estabelecer regras eficazes e proporcionadas, sublinhando também as Orientações Éticas para uma IA de Confiança de 2019, que foram elaboradas pelo Grupo Independente de Peritos de Alto Nível sobre a Inteligência Artificial criado pela Comissão. O grupo propôs sete requisitos essenciais não vinculativos para promover uma IA de confiança. Estes requisitos incluem: ação humana e supervisão; solidez técnica e segurança; privacidade e governação de dados; transparência; diversidade, não discriminação e equidade; bem-estar social e ambiental; e responsabilização. Estas diretrizes, embora não sejam juridicamente vinculativas, complementam os requisitos do regulamento.

REQUISITOS ÉTICOS ESSENCIAIS:

Ação humana e supervisão

Transparência, diversidade, não discriminação e equidade

Solidez técnica e segurança

Bem-estar social e ambiental

Privacidade e gestão de dados

Responsabilidade

4. O regulamento ia em números

Recitais

113 itens

+107.000 palavras

13 títulos

13 anexos

20 actos delegados e de execução

5. Âmbito de aplicação do regulamento

O regulamento é aplicável a:	Não se aplica a:
– Prestadores que introduzam no mercado ou coloquem em serviço sistemas de IA ou modelos de IA de finalidade geral na União, independentemente da sua localização.	– Domínios não abrangidos pelo âmbito de aplicação da legislação da UE.
– Responsáveis pela implantação de sistemas de IA estabelecidos ou localizados na União.	– Competências dos Estados-Membros no domínio da segurança nacional.

El Reglamento será aplicable a:	No será aplicable a:
– Prestadores e responsáveis pela implantação de sistemas de IA localizados em países terceiros quando a informação de saída é utilizada na União.	– Sistemas de IA utilizados exclusivamente para fins militares, de defesa ou de segurança nacional, independentemente do tipo de entidade que realiza essas atividades.
– Importadores e distribuidores de sistemas de IA.	– Autoridades públicas de países terceiros e organizações internacionais quando utilizam sistemas de AI no âmbito de acordos internacionais ou de cooperação para efeitos de aplicação da lei e de cooperação judiciária com a União ou com um ou mais Estados-Membros, desde que ofereçam garantias suficientes no que respeita à proteção dos direitos e liberdades fundamentais das pessoas.
– Fabricantes de produtos que introduzam ou colocam em funcionamento um sistema de IA no mercado juntamente com o seu produto.	– Domínios abrangidos pelas disposições relativas à responsabilidade dos prestadores de serviços intermediários estabelecidas no capítulo II do Regulamento (UE) 2022/2065 (Regulamento dos Serviços Digitais).
– Mandatários autorizados de prestadores não estabelecidos na União.	– Sistemas ou modelos de IA desenvolvidos e encomendados especificamente com o objetivo de investigação e desenvolvimento científico.
– Pessoas afetadas localizadas na União.	– A qualquer atividade de investigação, ensaio ou desenvolvimento relacionada com sistemas ou modelos de IA antes da sua introdução no mercado ou colocação em serviço.
– Quanto a certos sistemas de IA de risco elevado sujeita a regulação harmonizada da EU no setor dos transportes (Secção B do Anexo I), apenas se aplicam os artigos 102.º a 109.º, o artigo 112.º e, se essa legislação harmonizada o previr, o artigo 57.º	– Responsáveis pela implantação que sejam pessoas singulares que utilizem sistemas de IA no exercício de uma atividade puramente pessoal de natureza não profissional.
– Aplica-se a sistemas de IA, ainda que divulgados ao abrigo de licenças gratuitas e de código aberto, sempre que sejam colocados no mercado ou colocados em serviço e se enquadrem como sistemas de IA proibidos, de risco elevado ou sujeitos a obrigações de transparência.	– Sistemas de IA de fonte aberta ou divulgados ao abrigo de licenças gratuitas, salvo as exceções mencionadas.

6. Definição de sistema de inteligência artificial

Nos termos do n.º 1 do artigo 3.º do regulamento, um sistema de IA é um sistema baseado em máquinas e concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais.

Com esta formulação, o legislador europeu pretende que o seu conceito de IA seja sustentável ao longo do tempo, o que exige que englobe uma gama excecionalmente ampla de técnicas de análise de dados, sendo aplicável a uma grande variedade de tecnologias atualmente utilizadas no sector empresarial e na administração pública.

7. Classificação dos sistemas de ia

A categorização dos sistemas de IA ao abrigo do regulamento centra-se no conceito de risco[1], classificando esses sistemas de acordo com o nível de risco que representam para a sociedade, a segurança, os direitos fundamentais e o bem-estar humano. Assim, **o regulamento regula principalmente os sistemas de IA de risco elevado**, estabelecendo

1 Nos termos do n.º 2 do artigo 3.º do Regulamento IA, "risco" é a combinação da probabilidade de ocorrência de danos com a gravidade desses danos..

requisitos pormenorizados para o seu desenvolvimento, implantação e utilização. Podemos distinguir os seguintes tipos de sistemas de IA:

- **Sistemas de IA proibidos:** Algumas aplicações de IA são proibidas devido aos riscos em relação aos direitos e liberdades fundamentais que, na perspetiva do legislador, são inaceitáveis. Entre elas incluem-se os sistemas de vigilância em massa; os sistemas que manipulam o comportamento humano para contornar a autonomia das pessoas ou exploram as vulnerabilidades de um grupo específico de pessoas devido à sua idade ou deficiência; sistemas que realizem inferências emocionais em contextos laborais ou educativos; ou a instituição de mecanismos de crédito social por autoridades públicas, entre outras.

- **Sistemas de IA de risco elevado:** os sistemas de IA são considerados de risco elevado quando são suscetíveis de afetar de forma significativa os direitos fundamentais ou a segurança das pessoas. Estes sistemas estão sujeitos a requisitos regulatórios rigorosos, incluindo sistemas de gestão de riscos, avaliações de conformidade, padrões elevados de transparência, documentação técnica antes da introdução no mercado, obrigações de manutenção de registos, medidas de supervisão humana e fortes salvaguardas em matéria de proteção de dados e de cibersegurança.

- **Sistemas de IA com risco limitado ou obrigações especiais de transparência:** o regulamento inclui disposições relacionadas com a transparência e a prestação de informações adequadas aos utilizadores. Isto inclui requisitos para que os prestadores de sistemas de IA informem claramente os utilizadores quando estão a interagir com um sistema de IA, assegurando que as pessoas estão cientes da natureza automatizada da interação.

8. Práticas de ia proibidas

O regulamento prevê uma série de práticas proibidas em relação aos sistemas de IA, como a colocação no mercado, a colocação em serviço ou a utilização de:

- **Técnicas subliminares e manipulativas**: sistemas de IA que utilizem técnicas subliminares ou manipulativas com o objetivo de alterar significativamente o comportamento das pessoas singulares de forma a prejudicar a sua capacidade de tomar decisões informadas.

- **Exploração de vulnerabilidades**: sistemas de IA que explorem vulnerabilidades de indivíduos ou grupos específicos, com base na sua idade, deficiência ou estatuto socioeconómico, a fim de alterar substancialmente o seu comportamento de uma forma que lhes possa causar prejuízos significativos.

- **Sistemas de crédito social**: sistemas de IA para avaliar ou classificar indivíduos ou grupos ao longo do tempo com base no seu comportamento social ou características pessoais ou de personalidade, podendo resultar num tratamento prejudicial ou desfavorável em contextos não relacionados com os dados recolhidos.

- **Vigilância preditiva individual**: sistemas de IA especificamente destinados a avaliar o risco de uma pessoa cometer uma infração penal, com base unicamente na definição do seu perfil ou na avaliação das suas características de personalidade. Os sistemas de IA que apoiem a avaliação do envolvimento de uma pessoa em certa atividade criminosa não estão abrangidos, desde que essa avaliação já se baseie previamente em factos objetivos e verificáveis.

- **Reconhecimento facial e bases de dados**: a criação ou expansão de bases de dados de reconhecimento facial através da extração não seletiva (*scraping*) de imagens faciais da Internet ou através de sistemas de videovigilância. Esta prática é proibida devido às implicações para a privacidade e ao potencial de vigilância em massa.

- **Sistemas de inferência emocional no trabalho e na educação**: é proibida a utilização de sistemas de IA concebidos para detetar emoções ou intenções de indivíduos no local de trabalho ou na educação, exceto quando utilizados por razões médicas ou de segurança.

- **Sistemas de identificação biométrica em espaços públicos**: com certas exceções, sistemas de identificação biométrica à distância em tempo real em espaços acessíveis ao público para efeitos de aplicação da lei.

9. Sistemas de risco elevado

Os sistemas de IA de risco elevado são aqueles que representam um potencial significativo de danos para a segurança, a saúde ou os direitos fundamentais das pessoas. Por esta razão, estes sistemas estão sujeitos a um controlo particularmente intenso ao abrigo do Regulamento IA, a fim de garantir que são implementados de forma segura e fiável.

9.1. Classificação dos sistemas de risco elevado

Biometria	» Sistemas de identificação biométrica à distância. Exceção: Quando o seu único objetivo é confirmar a identidade da pessoa. » Sistemas de IA para categorização biométrica com base em atributos ou características sensíveis ou protegidos. » Sistemas de IA para o reconhecimento de emoções.
Infraestructuras críticas	» Sistemas de IA como componentes de segurança na gestão e operação de infraestruturas digitais críticas, tráfego, abastecimento de água, gás, aquecimento ou eletricidade.
Acceso a serviços privados essenciais e a serviços e prestações públicas essenciais	» Sistemas de IA utilizados pelas autoridades públicas para avaliar a elegibilidade para serviços e prestações de assistência pública essenciais, incluindo cuidados de saúde. » Sistemas de IA para avaliar a capacidade de solvabilidade, a classificação de crédito, o risco de seguro e a fixação de preços, bem como para avaliar e classificar chamadas de emergência
Gestão da migração, do asilo e do controlo das fronteiras	» Sistemas de IA das autoridades competentes para avaliação dos riscos (segurança, saúde, migração irregular), análise de pedidos de asilo, vistos, autorizações de residência e deteção, reconhecimento ou identificação de pessoas
IA em produtos regulados	» São ainda qualificados como sistemas de IA de risco elevado os que: » Se destinam a ser utilizados como componentes de segurança de produtos abrangidos pela legislação de harmonização da União enumerada no anexo I do Regulamento IA, ou em que o próprio sistema de IA é um produto desse tipo (Regulamento relativo às máquinas, Diretiva relativa à segurança dos brinquedos, etc.); e » Um sistema de IA não é considerado de risco elevado se não representar um risco significativo para a saúde, a segurança ou os direitos fundamentais das pessoas singulares, nomeadamente por não influenciar substancialmente o resultado da tomada de decisões. É este o caso quando a sua utilização se limita a: i) desempenhar uma tarefa processual restrita; ii) melhorar o resultado de uma atividade humana previamente concluída; iii) detetar padrões de tomada de decisão sem influenciar as decisões sem uma revisão humana adequada; iv) executar uma tarefa preparatória no âmbito de um dos domínios enumerados no Anexo III.
Educação e formação profissional	» Sistemas de IA para determinar o acesso/admissão ou afetação de pessoas singulares a instituições de ensino e formação profissional de todos os níveis. » Sistemas de IA para avaliar os resultados da aprendizagem ou o nível de escolaridade adequado. » Sistemas de IA para monitorização e deteção de comportamentos proibidos durante os exames.

Emprego, gestão dos trabalhadores e acesso ao emprego por conta própria	» Sistemas de IA para recrutamento, seleção, análise e filtragem de candidaturas a emprego, avaliação de candidatos. » Sistemas de IA para serem utilizados em decisões que afetam as condições de trabalho, a promoção, a cessação das relações de trabalho, a atribuição de tarefas, a supervisão e a avaliação do desempenho no âmbito das relações laborais.
Aplicação da lei	» Sistemas de IA para avaliar o risco de uma pessoa vir a ser vítima de infrações penais, a fiabilidade das provas, a probabilidade de uma pessoa cometer um crime ou reincidir e a definição de perfis durante a deteção, investigação ou repressão de infrações penais. » Sistemas de IA para ser usados como polígrafos ou instrumentos semelhantes.
Administração da justiça e processos democráticos	» Sistemas de IA para assistir autoridades judiciais na investigação e interpretação de factos e de direito, para aplicação da lei ou utilização na resolução alternativa de litígios. » Sistemas de IA para influenciar eleições ou comportamentos eleitorais. Exceção: sistemas a que as pessoas visadas não estejam expostas, como ferramentas para organizar campanhas políticas. » Quando os produtos dos quais o sistema de IA é um componente de segurança, ou o próprio sistema de IA enquanto produto, devam ser, de acordo com a referida legislação de harmonização, submetidos a uma avaliação de conformidade por terceiros com vista à sua colocação no mercado ou colocação em serviço.
No entanto, um sistema de AI será sempre considerado de risco elevado quando efectua a definição de perfis de pessoas singulares.	

9.2. Obrigações dos sistemas de IA de risco elevado

Para poderem funcionar no mercado da UE, estes sistemas devem cumprir os seguintes requisitos:

- **Avaliação da conformidade**: antes de serem colocados no mercado ou em serviço, estes sistemas devem ser submetidos a uma avaliação da conformidade para verificar se cumprem todos os requisitos de segurança e desempenho do regulamento. Isto inclui ensaios exaustivos para validar a exatidão, a robustez e a segurança do sistema.
- **Transparência e relatórios**: Os prestadores devem garantir que a documentação dos sistemas de IA de risco elevado seja detalhada e acessível. Isto inclui informações sobre a metodologia, os algoritmos, as decisões de conceção e as capacidades e limitações do sistema, permitindo uma transparência total sobre a forma como o sistema funciona e os dados que utiliza. Os prestadores de sistemas de IA de alto risco devem também fornecer aos responsáveis pela implantação desses sistemas informações claras e adequadas sobre as capacidades e limitações do sistema.
    - **Gestão dos riscos**: devem estabelecer e documentar um sistema de gestão dos riscos, de forma sistemática e contínua ao longo do ciclo de vida do sistema de AI de risco elevado. Esse sistema deve incluir a identificação, análise, estimativa e avaliação dos riscos conhecidos e previsíveis, bem como a adoção de medidas adequadas de gestão dos riscos para os enfrentar.
    - **Documentação técnica**: devem manter documentação técnica que demonstre a conformidade do sistema de IA com os requisitos exigidos.
    - **Registo de atividades**: devem manter um registo das operações do sistema de IA para garantir a rastreabilidade dos seus resultados. Além disso, os sistemas de IA de risco elevado devem tecnicamente permitir o registo automático de eventos (*logs*) ao longo do seu ciclo de vida.
- **Identificação do prestador**: os prestadores de sistemas de IA de risco elevado devem indicar no sistema, na sua embalagem e na documentação que o acompanha o seu nome, o nome comercial registado ou a marca registada e o seu endereço de contacto.

- **Qualidade e governança de dados**: deve ser garantido que os conjuntos de dados utilizados para treino, testagem e validação do sistema de IA são relevantes para o seu objetivo, representativos e isentos de erros e vieses, através de políticas adequadas de governança de dados.

- **Supervisão humana**: deve existir supervisão humana do sistema para minimizar os riscos e permitir a intervenção em caso de mau funcionamento do sistema, a fim de atenuar os riscos de decisões autónomas erradas ou prejudiciais. Os operadores devem ser formados e ter a autoridade necessária para monitorizar e, se necessário, intervir ou desativar o sistema de IA.

- **Cooperação com as autoridades**: os prestadores de sistemas de IA de risco elevado devem cooperar com as autoridades reguladoras e fornecer todas as informações necessárias para demonstrar a conformidade do sistema com os requisitos legais. Isto inclui também o fornecimento de acesso aos registos e à documentação do sistema quando solicitado pelas autoridades competentes.

- **Robustez e exatidão**: devem garantir que o sistema de IA é robusto, exato e capaz de tratar erros ou incoerências durante o funcionamento.

- **Cibersegurança**: devem ser aplicadas medidas adequadas para garantir a cibersegurança e a integridade do sistema. Em particular, podem ser aplicadas medidas para prevenir e responder a ataques destinados a manipular os dados de treino (*data poisoning*) ou de componentes pré-treinados utilizados no treino (*model poisoning*), entradas concebidas para levar o modelo de IA a cometer um erro, ataques de confidencialidade, etc.

- **Notificação e registo**: o sistema de IA de risco elevado deve ser registado numa base de dados da UE antes de este ser colocado no mercado (ver ponto 9.3).

  Certas obrigações aplicam-se apenas a determinados operadores:

- **Avaliação da conformidade**: Os distribuidores e outros operadores ao longo da cadeia de valor (como os importadores e os implantadores) têm obrigações específicas, como verificar a conformidade do sistema antes de o colocar no mercado, assegurar condições adequadas de armazenamento e transporte e tomar medidas caso detetem não conformidades ou riscos.

- **Avaliação de impacto nos direitos fundamentais**: os responsáveis pela implantação que sejam entidades reguladas pelo direito público ou entidades privadas prestadoras de serviços públicos devem realizar verificações de impacto destinadas a garantir que a utilização do sistema de IA não conduz à discriminação e que respeita os direitos fundamentais.

- **Mandatário autorizado**: antes de colocar um sistema de IA de risco elevado no mercado da UE, os prestadores estabelecidos em países terceiros devem nomear, através de um mandato escrito, um mandatário autorizado que esteja estabelecido na UE.

  Em suma, os sistemas de IA de risco elevado estão sujeitos a um quadro regulamentar pormenorizado que exige conformidade a vários níveis, desde a validação da sua tecnologia até à governação dos dados que processam. Estas medidas visam proteger os indivíduos e a sociedade dos potenciais danos que estes sistemas podem causar se não forem adequadamente geridos.

9.3. Base de dados da UE para sistemas de risco elevado

A base de dados da UE relativa a sistemas de IA de risco elevado é uma iniciativa fundamental no âmbito do regulamento, que visa centralizar e facilitar o acesso a informação pormenorizada sobre estes sistemas, aumentando assim a transparência e fortalecendo a atividade de supervisão. Esta base de dados será criada e mantida pela Comissão Europeia em cooperação com os Estados-Membros e conterá dados pormenorizados sobre os sistemas de IA de risco elevado enquadrados numa das utilizações listadas no Anexo III (ver ponto 9.1) e registados ao abrigo do presente regulamento.

A obrigação de se registarem a si próprios e ao sistema de IA de risco elevado incumbe:

- No setor privado, ao prestador ou, se for caso disso, ao seu mandatário autorizado, sempre antes da colocação no mercado ou da colocação em serviço.

- No setor público, às autoridades públicas, instituições, agências ou organismos públicos responsáveis pela implantação ou às pessoas que atuem em seu nome, sempre antes da colocação em serviço ou da utilização do sistema.

Nos casos em que a IA é utilizada no âmbito da gestão da migração, asilo e gestão do controlo das fronteiras, o registo será feito numa secção segura e não pública da base de dados da EU, à qual apenas a Comissão e as autoridades nacionais de supervisão têm acesso.

O registo dos sistemas de IA de risco elevado abrangidos pelo ponto 2 do anexo III (sistemas de IA em infraestruturas críticas) será efetuado a nível nacional.

9.3.1. Funções e características desta base de dados: deve incluir dados específicos introduzidos tanto pelos prestadores de sistemas como pelos responsáveis pela implantação, se forem autoridades públicas. Estes dados vão desde os pormenores de identificação do sistema e dos seus prestadores até às informações técnicas e de conformidade. A Comissão Europeia ficou incumbida de aprovar as especificações funcionais da base de dados e da sua atualização, com a assistência de um comité de peritos.

9.3.2. Acessibilidade e privacidade: as informações registadas serão facilmente acessíveis ao público, garantindo-se uma navegação e compreensão facilitadas da base de dados. No entanto, haverá restrições específicas para as informações sensíveis, as quais só serão acessíveis pelas autoridades de fiscalização do mercado e pela Comissão, a menos que haja um consentimento expresso para alargar esse acesso.

9.3.3. Proteção de dados: a base de dados só conterá dados pessoais na medida do necessário para cumprir as suas funções reguladas, mantendo a conformidade com os regulamentos da UE em matéria de proteção de dados. A gestão da base de dados será efetuada com um elevado nível de segurança, incluindo medidas de cibersegurança para proteger as informações armazenadas.

Esta base de dados representa um passo fundamental para uma maior transparência na utilização da IA, permitindo um controlo público e regulamentar mais eficaz dos sistemas de IA que possam ter um impacto significativo na segurança e nos direitos fundamentais dos cidadãos.

10. Obrigações de transparência dos prestadores e responsáveis pela implantação de determinados sistemas de ia

O legislador considerou como essencial para cumprir os objetivos do regulamento a transparência relativamente a certos aspetos dos sistemas de IA. Assim, o Regulamento IA estabelece requisitos claros que devem ser seguidos para promover a transparência e a confiança do público, tanto nos sistemas classificados como de risco elevado, como em determinados sistemas que apresentem características particulares.

Os prestadores de serviços devem assegurar que **qualquer sistema de IA destinado a interagir diretamente com seres humanos seja claramente identificado como tal**, exceto se tal for óbvio do ponto de vista de uma pessoa singular razoavelmente informada, atenta e advertida. Esta obrigação destina-se a garantir que os utilizadores tenham consciência de que estão a interagir com um sistema de IA e não com um ser humano. Esta obrigação é extensiva aos s**istemas que geram conteúdos sintéticos**, como áudio, imagem, vídeo ou texto, cujos conteúdos de saída devem ser claramente marcados para serem reconhecidos como gerados ou manipulados por IA.

Além disso, os responsáveis pela implantação de sistemas específicos, como os sistemas de **reconhecimento de emoções ou de categorização biométrica**, devem informar as pessoas expostas a esses sistemas sobre o seu funcionamento e o tratamento dos seus dados pessoais.

Por último, **os sistemas de IA que manipulam conteúdos de imagem, áudio ou vídeo que constituam falsificações profundas (*deep fakes*)** devem indicar claramente que esses conteúdos foram gerados ou manipulados artificialmente.

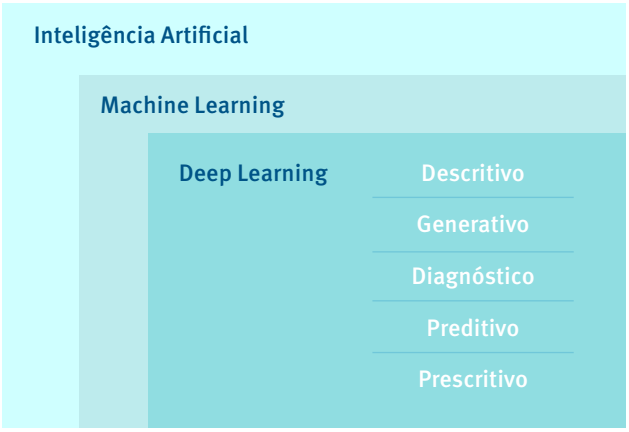
11. Utilização da ia pela administração pública

Embora se trate de um regulamento horizontal, o Regulamento IA presta especial atenção à utilização de sistemas de IA por autoridades públicas. Em primeiro lugar, porque muitas das utilizações dos sistemas de IA classificados como de risco elevado estão associadas a funções tipicamente administrativas (sistemas de IA na administração da justiça e dos processos democráticos, gestão da migração, asilo e controlo de fronteiras, serviços e benefícios públicos essenciais, etc.). Assim, as entidades públicas estarão sujeitas às obrigações associadas aos sistemas de risco elevado, quer enquanto prestadores (quando desenvolvam um sistema de IA para sua utilização) como enquanto responsáveis pela implantação, quando contratam o seu serviço a um prestador externo.

O regulamento especifica que as autoridades públicas responsáveis pela implantação de sistemas de IA de risco elevado são obrigados a efetuar uma avaliação de impacto que a utilização desse sistema possa ter nos direitos fundamentais. Esta avaliação deverá ser feita antes da primeira utilização do sistema e deverá ser atualizada sempre que o responsável pela implantação considerar que algum dos elementos essenciais se alterou ou deixou de estar atualizado, e deve ser notificada às autoridades de supervisão competentes.

12. Sobre modelos de ia de finalidade geral

Uma das novidades mais relevantes das últimas alterações ao Regulamento é a instituição de um quadro regulamentar específico para os modelos de IA de finalidade geral, como o ChatGPT, o Google Gemini ou o Meta Llama, que são concebidos para abordar uma vasta gama de tarefas e são normalmente treinados em grandes volumes de dados utilizando métodos avançados como a aprendizagem autossupervisionada, não supervisionada ou por reforço. Estes modelos podem ser comercializados de várias formas, incluindo como módulos, bibliotecas, descarregamentos diretos ou cópias em papel, embora os métodos mais comuns sejam através de API ou como um serviço Web. Estes modelos de base requerem componentes adicionais, como interfaces de utilizador, para funcionarem como sistemas de IA funcionais.



A IA generativa (GenAI) é uma abordagem à investigação em IA. Centra-se no desenvolvimento de modelos capazes de gerar conteúdos novos e criativos, como imagens, texto ou mesmo música. Ao contrário dos sistemas de IA tradicionais que se baseiam em regras predefinidas ou padrões aprendidos, os modelos generativos são concebidos para produzir dados originais através da compreensão profunda das estruturas e características subjacentes aos conjuntos de dados de treino. Estes modelos inserem-se na categoria de *machine learning* e utilizam técnicas de *deep learning* para gerar conteúdos semelhantes aos criados por seres humanos. Baseiam-se em *large language models* (LLM) para interagir com os utilizadores.

12.1. Classificação dos modelos de la finalidade geral

O regulamento distingue entre os simples modelos de finalidade geral e os modelos de finalidade geral com riscos sistémicos.

Um modelo de IA de finalidade geral será considerado como um modelo com risco sistémico se satisfizer qualquer um dos seguintes critérios:

- Dispor de capacidades de elevado impacto, determinadas com base em ferramentas técnicas e metodologias adequadas, incluindo indicadores e parâmetros de referência.
- Ter capacidades de impacto equivalentes aos descritos no ponto anterior, de acordo com uma decisão da Comissão tomada de iniciativa própria ou em resposta a um alerta qualificado do grupo de peritos científicos, tendo por base os critérios especificados no Anexo XIII[2].
- Considera-se que um modelo de IA de finalidade geral tem capacidades de grande impacto, conforme descrito no primeiro ponto, se a quantidade acumulada de cálculo utilizada para o seu treino, medido em FLOPs[3], for superior a 10^25.

Além disso, a Comissão está habilitada a emitir atos delegados para ajustar os limiares acima referidos, bem como para atualizar os valores de referência e os indicadores em função das evoluções tecnológicas, tais como melhorias nos algoritmos ou na eficiência do *hardware*.

Estes modelos devem cumprir obrigações específicas quando são introduzidos no mercado, incluindo a realização de avaliações de impacto e de testes de resistência para detetar e atenuar os riscos potenciais.

2 Para o efeito, o Anexo XIII estabelece seguintes critérios: (i) O número de parâmetros que compõem o modelo, o que influencia diretamente a sua complexidade e capacidade de processamento; (ii) A qualidade e dimensão do conjunto de dados utilizado para treinar o modelo, que pode ser medido de por métodos como a utilização de *tokens*, (iii) O volume computacional total utilizado para treinar o modelo, expresso em operações de vírgula flutuante (FLOP) ou através da combinação de outras variáveis, como o custo estimado do treino, o tempo necessário e o consumo energético associado; (iv) As características dos *inputs e outputs* do modelo, incluindo aspetos como a conversão texto-texto em modelos linguísticos de grande escala, a conversão texto-imagem, a multimodalidade e os limiares de ponta para avaliar o impacto significativo de cada modalidade, bem como o tipo específico de *inputs e outputs*, por exemplo, sequências biológicas (v) Parâmetros de referência e avaliações de desempenho do modelo, tendo em conta aspetos como o número de tarefas que pode realizar sem treino adicional, a sua capacidade de se adaptar e aprender novas tarefas, o seu grau de autonomia, a escalabilidade e as ferramentas a que pode aceder; (vi) Se tem elevado impacto no mercado interno, o que se presume quando tiver sido disponibilizado a, pelo menos, 10.000 utilizadores empresariais registados na UE; (vii) O número de utilizadores finais registados que interagem com o modelo.

3 FLOP ou Operação de Ponto Flutuante: qualquer operação ou tarefa matemática que envolva números de ponto flutuante, que são um subconjunto dos números reais normalmente representados nos computadores por um número inteiro de precisão fixa elevado pelo expoente inteiro de uma base fixa.

Os prestadores destes modelos devem assegurar elevados níveis de transparência e cooperação com as autoridades, incluindo a disponibilização de documentação pormenorizada sobre a conceção, as capacidades e as limitações do modelo. Esta informação deve ser acessível não só às autoridades, mas também a outros prestadores que integrem estes modelos em sistemas de AI mais alargados.

12.2. Obrigações

12.2.1. Modelos de IA de finalidade geral

O regulamento impõe uma série de obrigações comuns aos prestadores de modelos de IA de finalidade geral para garantir que esses modelos sejam implementados de forma responsável e segura. Uma das principais obrigações é o desenvolvimento e a atualização contínua da **documentação técnica detalhada do modelo**. Esta documentação deve incluir informações sobre o processo de treino, os testes efetuados e os resultados das avaliações destes modelos. Os elementos específicos a abranger são descritos em pormenor no Anexo XI do regulamento e devem ser disponibilizados ao **Serviço para a IA**[4] e às autoridades nacionais competentes, mediante pedido destas.

Além disso, os prestadores devem tornar esta documentação acessível a outros prestadores de sistemas de IA que planeiem integrar o modelo de finalidade geral nos seus próprios sistemas de IA. Esta documentação deve permitir que esses terceiros compreendam plenamente as capacidades e limitações do modelo e cumpram as suas próprias obrigações regulamentares. Esta obrigação não prejudica dos direitos de propriedade intelectual e das informações comerciais confidenciais ou segredos comerciais dos respetivos titulares.

Outra obrigação importante é a de os prestadores destes modelos estabelecerem uma política para garantir o cumprimento da legislação da União em matéria de direitos de propriedade intelectual, e, em particular, para identificar e respeitar, incluindo através de tecnologias de ponta, a reserva expressa dos titulares de direitos de autor contra a extração dos seus textos e dados, um direito previsto na Diretiva (UE) 2019/790.

Os prestadores devem também desenvolver e publicar um resumo pormenorizado dos conteúdos utilizados para a formação de modelos de IA de finalidade geral, de acordo com os formatos fornecidos pelo Serviço para a AI.

Além disso, espera-se que os prestadores dessas tecnologias colaborem com a Comissão e as autoridades competentes em qualquer ação regulatória relacionada com os seus modelos e sigam as melhores práticas e normas harmonizadas para demonstrar o cumprimento de todas estas obrigações.

12.2.2. Modelos de IA de finalidade geral com risco sistémico

Os prestadores de modelos de IA de finalidade geral com risco sistémico devem cumprir as seguintes obrigações adicionais: (i) realizar a avaliação dos modelos utilizando protocolos e ferramentas normalizados que reflitam o atual estado da arte, incluindo a realização e documentação de testagens antagónicas para identificar e minimizar os riscos sistémicos; (ii) Avaliar e mitigar potenciais riscos sistémicos ao nível da União que possam surgir da utilização do sistema, incluindo as suas fontes; (iii) monitorizar, documentar e comunicar sem demora injustificada quaisquer incidentes graves, juntamente com potenciais medidas corretivas, ao Serviço para a IA e, se necessário, às autoridades nacionais competentes; (iv) assegurar um nível adequado de proteção da cibersegurança tanto para o modelo de AI como para a sua infraestrutura física, incluindo medidas de proteção contra a utilização maliciosa ou ataques que comprometam a integridade e o funcionamento seguro do modelo; Até à publicação de uma norma harmonizada, os prestadores podem aderir a códigos de boas práticas para demonstrar o cumprimento destas obrigações (ver secção 12.3).

12.3. Códigos de boas práticas

O artigo 56.º do regulamento prevê a criação e a promoção de códigos de boas práticas a nível da UE, que serão fundamentais para garantir que os prestadores de modelos de IA cumprem adequadamente as obrigações impostas pelo Regulamento IA e alinhar as suas práticas com as normas éticas e jurídicas exigidas. O Serviço para a AI desempenhará um papel fundamental no incentivo e facilitação do desenvolvimento destes códigos, garantindo que abrangem as obrigações especificadas nos artigos anteriores, tais como a documentação adequada dos modelos e a gestão do risco sistémico.

4 Em 29 de maio de 2024, a Comissão anunciou a criação do Serviço para a IA, estabelecido no âmbito da Comissão Europeia. O Serviço para a IA visa permitir o futuro desenvolvimento, implementação e utilização da IA de uma forma que promova os benefícios sociais e económicos e a inovação, atenuando simultaneamente os riscos, e desempenhará um papel fundamental na aplicação do Regulamento IA, especialmente em relação aos modelos de IA de finalidade geral. O comunicado de imprensa pode ser consultado no seguinte endereço: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2982

Os códigos devem incluir procedimentos e estratégias para manter a informação atualizada em relação aos desenvolvimentos tecnológicos e de mercado, assegurar um nível adequado de pormenor sobre o conteúdo utilizado no treino de modelos e definir medidas para avaliar e gerir os riscos sistémicos. Além disso, devem estabelecer os métodos para documentar esses riscos e a sua atenuação, tendo em conta a gravidade, a probabilidade e as dificuldades específicas em lidar com eles.

Assim que um código de prática for aprovado pela Comissão através de um ato de execução, adquirirá validade geral na UE, ou seja, presumir-se-á que os prestadores que aderirem a um código de boas práticas aprovado estão em conformidade com as obrigações do regulamento. Na ausência de um código de boas práticas ou se um código de boas práticas não for considerado adequado, os prestadores terão de demonstrar a conformidade através de outros meios adequados, que devem ser aprovados pela Comissão.

Os códigos de boas práticas devem incluir orientações sobre:

1. Realização de avaliações de impacto social

2. Implementação de sistemas de gestão de riscos

3. Adoção de medidas de redução e mitigação dos riscos

4. Documentação e registo de modelos de IA

5. Cooperação com as autoridades nacionais competentes

Os códigos de boas práticas não são vinculativos por si só, mas servem como guias que os fornecedores de sistemas de IA podem seguir para demonstrar conformidade com as obrigações estabelecidas no Regulamento IA. A adesão a estes códigos é voluntária, mas a partir do momento em que um fornecedor decide seguir um código de boas práticas aprovado pela CE, presume-se que cumpre com as obrigações especificadas no Regulamento IA.

13. Medidas de apoio à inovação

Tal como foi referido na introdução da presente nota, a UE pretende que o Regulamento IA sirva de impulso à inovação no domínio da IA. Para este efeito, o regulamento estabelece uma série de medidas de apoio à inovação, incluindo as seguintes:

***Sandboxes* regulatórios**	A criação de ambientes de testagem controlados para permitir que os prestadores de modelos de IA testem as suas inovações num ambiente controlado, em condições específicas e sob a supervisão das autoridades.
Aconselhamento e apoio técnico	Orientação e apoio das autoridades competentes aos prestadores e criadores de IA na identificação de riscos para os direitos fundamentais, a segurança e a saúde dos utilizadores, o cumprimento dos requisitos regulamentares e as expectativas em matéria de inovação responsável.
Cooperação e trabalho coordenado	Promoção da cooperação entre as autoridades nacionais competentes, os prestadores de modelos de IA e outras partes interessadas para partilhar conhecimentos e experiências.
Financiamento	Facilitar o acesso ao financiamento e aos programas de apoio à investigação e ao desenvolvimento de modelos de IA.
Normalização	Promover a normalização e a certificação dos modelos de IA para garantir a segurança e a conformidade regulamentar.
PME	Apoia a inovação através da inclusão de medidas específicas que prestam especial atenção às pequenas e médias empresas (PME), incluindo *startups*.

13.1. Sobre as *sandboxes* regulatórias

Os ambientes de testagem da regulamentação da IA (*sandboxes* regulatórias) são espaços seguros e regulados nos quais as empresas, os investigadores e os *developers* podem experimentar novos produtos, serviços ou sistemas de IA sem o cumprimento estrito da regulamentação aplicável, mas ao abrigo de um quadro de supervisão específico, por um período de tempo limitado e assegurando a existência de salvaguardas adequadas. Os Estados-Membros devem assegurar a criação de, pelo menos, uma sandbox regulatória de IA a nível nacional, que deverá estar operacional até dois anos após a entrada em vigor do regulamento.

Estes espaços de testagem são supervisionados pelas autoridades nacionais competentes e têm por objetivo:

- **Incentivar a inovação**: proporcionar um ambiente onde a inovação possa ter lugar com menos riscos e mais liberdade, o que é especialmente útil para as pequenas e médias empresas ("**PMEs**") que podem não ter recursos para suportar os custos associados ao cumprimento das obrigações complexas, facilitando assim o desenvolvimento e a implementação de modelos inovadores de IA.

- **Identificar e atenuar os riscos**: permitir identificar e resolver potenciais problemas éticos, de segurança ou privacidade antes de os produtos ou serviços serem lançados no mercado. Assim, a *sandbox* permite aos prestadores demonstrar a segurança e a conformidade dos seus sistemas de IA, bem como facilitar a identificação e a resolução de potenciais riscos e problemas antes da introdução total no mercado.

- **Ajudar as entidades reguladoras a compreender melhor as novas tecnologias e as suas implicações**: este facto pode influenciar a criação de políticas e regulamentos mais eficazes e adaptados à era digital.

13.2. Medidas dirigidas a PMEs

O artigo 62.º do Regulamento IA estabelece medidas de apoio às PME, incluindo as *startups*, centradas no acesso a *sandboxes* regulatórias, a atividades de formação e sensibilização, na comunicação e apoio sobre o Regulamento IA e na sua participação no desenvolvimento de normalização. As medidas previstas pelo legislador incluem:

- o acesso prioritário a *sandboxes* regulatórias às PME com sede ou sucursal num país da UE que satisfaçam determinadas condições e critérios de seleção.

- realização de atividades de sensibilização e formação sobre a aplicação do Regulamento IA tendo em conta as necessidades reais das PME e das *startups*.

- utilização de canais de comunicação para aconselhamento e resposta a questões sobre a aplicação do Regulamento IA, incluindo uma plataforma de informação centralizada a ser criada e mantida pelo Serviço para a IA.

- incentivo à participação das PME no processo de desenvolvimento da normalização.

- disposições particulares sobre as taxas a pagar pela avaliação de conformidade, em função da dimensão e do mercado das PME.

- promoção da convergência nos contratos públicos de sistemas de IA.

- aplicação de coimas de menor montante no caso de incumprimento de certas disposições, tendo em conta a sua capacidade económica[5].

13.3. Derrogações para operadores específicos (microempresas)

Em resposta às críticas sobre o facto de o Regulamento IA impor excessiva regulamentação às startups, o legislador europeu aliviou a carga burocrática para as microempresas[6], que podem simplificar certos elementos do sistema de gestão da qualidade exigido pelo artigo 17.º do Regulamento IA[7]) siempre y cuando no tengan entidades asociadas o vinculadas según dicha

5 Ver nº 6 do artigo 99º do Regulamento IA.

6 De acordo com a definição fornecida na Recomendação da Comissão de 6 de maio de 2003 relativa à definição de micro, pequenas e médias empresas, disponível na seguinte ligação: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32003H0361.

7 Os prestadores de sistemas de IA de risco elevado estão obrigados pelo Regulamento IA a estabelecer um sistema de gestão da qualidade. Este sistema deve documentar as políticas e os procedimentos, incluindo as estratégias de *compliance*, a conceção, o desenvolvimento, os ensaios, as especificações técnicas, a gestão dos dados e dos riscos, a vigilância pós-comercialização, a comunicação de incidentes e a comunicação com as autoridades e as partes interessadas, adaptados à dimensão da organização.

Recomendación. Por su parte, la Comisión desarrollará directrices para simplificar estos elementos sin comprometer el nivel de protección o los requisitos exigidos para sistemas de IA de alto riesgo. Tal simplificación no eximirá a las microempresas de cumplir con otros requisitos y obligaciones del Reglamento, incluidos los especificados en los artículos 9 al 15, 72 y 73.

14. Sanções

O regulamento estabelece um sistema de coimas em consonância com outros regulamentos europeus recentes, como o Regulamento Geral sobre a Proteção de Dados ("**RGPD**"), o Regulamento Mercados Digitais ("**DMA**") ou o Regulamento Serviços Digitais ("**DSA**"). em particular:

Até 35 milhões de euros ou até 7% do volume de negócios mundial total do exercício financeiro anterior (consoante o mais elevado)	em caso de incumprimento das práticas proibidas de IA previstas no artigo 5.º.
Até 15 milhões de euros ou até 3% do volume de negócios total a nível mundial do exercício financeiro anterior (consoante o montante mais elevado)	em caso de incumprimento de certas obrigações[8] relativas aos prestadores, importadores e outros operadores dos sistemas de IA e aos organismos notificados, para além das referidas no artigo 5.º.
Até 7,5 milhões de euros ou até 1% do volume de negócios total a nível mundial do exercício financeiro anterior (consoante o montante mais elevado)	pela apresentação de informações inexatas, incompletas ou deturpadas aos organismos notificados ou às autoridades nacionais competentes.
Até 1,5 milhões de euros	para as instituições, órgãos e organismos da União: em caso de incumprimento da proibição das práticas de IA referidas no artigo 5.
Até 750 000 euros	para as instituições, órgãos e organismos da União: em caso de incumprimento dos requisitos ou obrigações previstas no regulamento, com exceção das previstas no artigo 5.
Até 3% do volume de negócios mundial total do exercício financeiro anterior ou 15 milhões de euros (consoante o montante mais elevado)	para os prestadores de modelos de IA de finalidade geral por infrações intencionais ou por negligência das obrigações previstas no Regulamento IA aplicáveis a estes sistemas.

15. Entrada em vigor e próximas etapas

Extraoficialmente, soube-se que o Regulamento será publicado no Jornal Oficial da União Europeia a meio de julho. Entrará em vigor 20 dias depois e será plenamente aplicável 24 meses após essa data, com as seguintes exceções:

- Os capítulos I e II (disposições gerais e práticas proibidas) são aplicáveis **6 meses** após a data de entrada em vigor do regulamento.
- Os códigos de boas práticas devem estar concluídos **9 meses** após a data de entrada em vigor do regulamento.
- A Secção 4 do Capítulo III, o Capítulo V, o Capítulo VII e o Capítulo XII (obrigações para a governação da IA de finalidade geral) serão aplicáveis **12 meses** após a data de entrada em vigor do regulamento, com exceção do artigo 101.º (coimas no âmbito das obrigações aplicáveis aos sistemas de IA de finalidade geral).
- O nº 1 do artigo 6º e as restantes obrigações relativas aos sistemas de risco elevado serão aplicáveis **36 meses** após a data de entrada em vigor do regulamento.

8. Essas obrigações são: (i) as obrigações previstas no artigo 16.º para os prestadores de sistemas de IA de risco elevado; (ii) as obrigações dos mandatários autorizados previstas no artigo 22.º; (iii) as obrigações dos importadores previstas no artigo 23.º; (iv) as obrigações dos distribuidores previstas no artigo 24.º; (v) as obrigações dos responsáveis pela implantação previstas no artigo 26.º; vi) os requisitos e obrigações dos organismos notificados nos termos dos artigos 31º, 33º, nº 1, 33º, nº 3 e 33º, nº 4 ou 34º; vii) as obrigações de transparência dos prestadores e responsáveis pela implantação nos termos do artigo 50º.

Datas relevantes

Entrada em vigor: 20 dias após a sua publicação oficial no Jornal Oficial da União Europeia.

- Após 3 meses: Comunicação das autoridades nacionais e desenvolvimento nacional do regime de sanções.

- Aos 6 meses: Proibição de IA de risco inaceitável.

- **Até 9 meses**: Devem estar em vigor códigos de boas práticas.

- **Aos 12 meses**: Aplicabilidade à IA de objetivo geral.

- **Após 18 meses**: Publicação de orientações práticas de implementação do Regulamento pela Comissão.

- **Ao fim de 2 anos**:

    - Aplicação geral do Regulamento IA;

    - A Comissão deve avaliar e apresentar um relatório sobre a necessidade de alterar a lista de áreas de utilização de risco elevado e, posteriormente, de quatro em quatro anos.

- **Após 5 anos**: revisão do regulamento

16. Principais desafios que o regulamento coloca às empresas

A regulamentação da IA apresenta desafios importantes que estão no centro dos debates contemporâneos sobre tecnologia e política regulatória. Com o Regulamento IA, os legisladores europeus optaram por uma regulamentação precoce, tentando antecipar possíveis utilizações abusivas da IA ou tipos de inovação que entendem ser prejudiciais para a sociedade. No entanto, o próprio regulamento pode ser um desafio à inovação pelas empresas inovadoras, devido aos limites e restrições que lhes impõe, a nível teórico, para equilibrar a promoção do desenvolvimento tecnológico com a sua utilização responsável e ética. Alguns dos desafios que as empresas enfrentarão nos próximos anos serão os seguintes:

- **Adaptação das empresas**: o novo regulamento é extenso e pode ter uma vasta margem de interpretação. As empresas que desenvolvem e utilizam sistemas de IA terão de se adaptar a ele, muitas vezes sem saber exatamente como interpretar e aplicar as obrigações previstas. Compreender a interação entre o regulamento e as regras existentes aplicáveis à IA, nomeadamente em matéria de proteção de dados, propriedade intelectual e governação de dados, será também uma questão fundamental para as organizações. A incapacidade de gerir adequadamente estas interações pode ser uma fonte de risco significativo. Por conseguinte, não se trata apenas de uma questão de *compliance* jurídica, pois o novo Regulamento IA afetará a forma como as organizações investem na inovação, o que terá um impacto direto nos negócios.

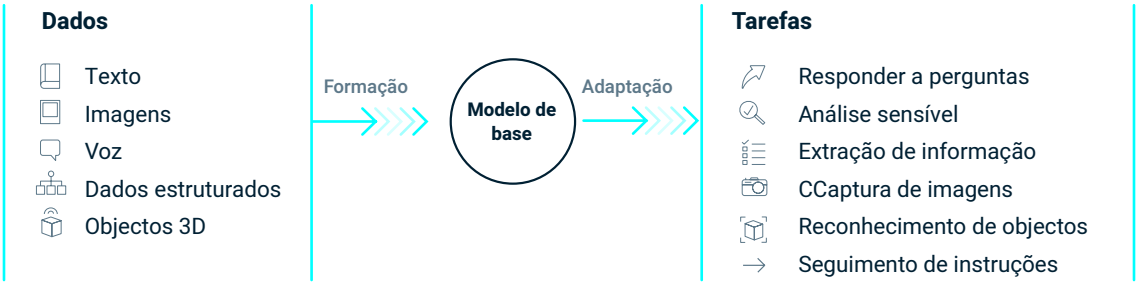
- **Efeito Bruxelas**: o legislador europeu procurou repetir no Regulamento IA o chamado *Brussels Effect* do RGPD. O objetivo é obrigar todos os operadores a cumprir as obrigações e os princípios do regulamento, independentemente do seu país de origem, quando os seus produtos ou serviços estejam presentes na UE.

- **Evolução tecnológica**: a rápida evolução da IA coloca o desafio de manter o regulamento atualizada para fazer face aos novos desenvolvimentos tecnológicos, com um risco claro de obsolescência das suas normas.

- **Aplicação e execução**: A aplicação do regulamento também coloca desafios às autoridades em termos de supervisão e execução, exigindo recursos e instrumentos de controlo adequados, como formação e ferramentas tecnológicas.

17. O que é que as empresas devem fazer a partir de agora?

Os sistemas de IA mais recentes, em particular a IA generativa, que permitem o desenvolvimento de texto, vídeo ou imagens sintéticas, baseiam-se na arquitetura transformer, que assenta em modelos fundacionais, designados pelo regulamento como "modelos de IA de finalidade geral". Estes modelos diferem dos sistemas de IA propriamente ditos pela sua autonomia e capacidade de influenciar estes últimos em ambientes físicos ou virtuais. Estes modelos têm um grau considerável de generalidade e são capazes de executar com competência uma grande variedade de tarefas distintas, independentemente da forma como o modelo seja introduzido no mercado, e podem ser integrados numa variedade de sistemas ou aplicações a jusante.



Tendo em conta o grande potencial dos "modelos de IA de finalidade geral", o legislador europeu considerou necessário dedicar-lhes inteiramente um capítulo (artigos 51.º a 56.º), com obrigações específicas para os seus prestadores (analisadas na secção 12.2 infra), incluindo, entre outras, as seguintes:

1) Nomear um mandatário autorizado que esteja estabelecido na UE, caso o prestador esteja localizado num país terceiro;

2) Desenvolver e manter atualizada a documentação técnica do modelo, incluindo o seu processo de formação e ensaio e os resultados da avaliação, que deve ser disponibilizada, a pedido, ao Serviço para a AI e às autoridades nacionais competentes;

3) Desenvolver e manter atualizada a informação e a documentação a disponibilizar a quem pretenda integrar o modelo de IA de finalidade geral nos seus sistemas de IA. Embora o regulamento não especifique quais as informações que estes prestadores devem fornecer, afirma que estas devem ser suficientes para que os prestadores de sistemas de IA compreendam as capacidades e limitações do modelo de IA de objetivo geral.

4) Preparar um protocolo para assegurar a aplicação da legislação em matéria de direitos de propriedade intelectual, em especial no que diz respeito ao mecanismo de exclusão previsto no artigo 4.º, n.º 3, da Diretiva (UE) 2019/790.

5) Fornecer publicamente informações sobre o conteúdo utilizado para formar o modelo de AI de finalidade geral, seguindo o formato fornecido pelo Serviço para a AI.

6) No caso de um modelo de IA de finalidade geral com risco sistémico, devido ao seu elevado impacto, devem ser cumpridos os seguintes requisitos adicionais:

   a) notificar sem demora a Comissão Europeia logo que se saiba que este requisito será cumprido;

   b) avaliar o modelo, incluindo a realização e documentação de testes de simulação contraditórios para detetar e reduzir o risco sistémico;

   c) acompanhar e, se for caso disso, comunicar os incidentes graves e as eventuais medidas corretivas; e

   d) estabelecer um nível adequado de proteção da cibersegurança.

Estas obrigações terão de ser respeitadas apenas pelos modelos de IA de finalidade geral. Esta abordagem seletiva sublinha a importância da recente aprovação do regulamento, que constitui um marco na regulamentação desta tecnologia emergente, que afetará, de uma forma ou de outra, qualquer empresa que utilize um sistema de IA. Este novo contexto jurídico impõe desafios significativos, mas também oportunidades, que, para serem aproveitadas, requerem um conhecimento profundo do novo regulamento e da forma como este pode afetar as organizações e os indivíduos

De seguida, apresentamos uma série de recomendações práticas para navegar com sucesso este novo enquadramento regulatório, garantindo que a implementação e utilização da IA é conduzida de forma ética, segura e em conformidade com a lei.

Na perspetiva dos responsáveis pela implantação ou utilizadores profissionais, propomos a adoção das seguintes medidas:

- **Avaliar o impacto do novo regulamento**: acreditamos que é essencial avaliar o impacto do Regulamento IA o mais rapidamente possível para compreender de que forma este afetará a organização e as suas operações. É muito provável que o ciclo de vida das tecnologias de IA a implementar ou desenvolver após a entrada em vigor do regulamento seja mais longo do que os próximos dois anos (data efetiva de implementação na maioria dos casos); esperar até lá pode colocar os investimentos em risco e prejudicar a reputação da organização.

- **Identificar as áreas afetadas da organização e conceber um modelo de governança**: será necessário determinar quais as áreas internas que serão afetadas pela implementação de sistemas de IA e como. Isto permitir-nos-á conceber um modelo de governança que ajude a atuação coordenada e coerente no âmbito da IA, equilibrando os aspetos de *compliance* com a abordagem estratégica e empresarial.

- **Desenvolver um plano de formação**: O enfoque na formação e na sensibilização nas fases iniciais ajudará a interpretar melhor o impacto do novo regulamento nas diferentes áreas e a obter os melhores resultados possíveis do novo contexto. A formação deve centrar-se não só nos aspetos puramente formais de *compliance*, mas também na perspetiva ética e de reputação, bem como na própria utilização responsável e eficiente desta tecnologia, ajudando assim a minimizar os riscos em sentido lato. É necessário um plano de choque inicial, mas é também imperativo conceber e implementar um plano de formação contínua que permita à organização manter-se atualizada em relação às mudanças comerciais, tecnológicas e legislativas previsíveis, mantendo os padrões necessários de conhecimento e sensibilização ao longo do tempo.

- **Integrar o quadro jurídico nos processos de inovação (*legal by design*)**: será necessário integrar o novo quadro jurídico nos processos de inovação desde o início para garantir a *compliance by design* dos sistemas de IA. Por outro lado, o novo regulamento é uma das muitas regras que têm impacto no domínio digital. A conceção de um modelo de dados suficientemente adaptável às alterações regulamentares e que permita a implementação de diferentes níveis de conformidade contribuirá para melhorar a eficiência dos processos e sistemas da organização.

- **Inventariar soluções baseadas em IA**: Inventariar todas as soluções baseadas em IA utilizadas pela organização e classificar o seu nível de risco não é apenas um requisito de conformidade legal, mas uma ferramenta estratégica que permitirá às organizações gerir o risco, otimizar recursos e permanecer ágeis e responsáveis num cenário tecnológico complexo e em constante evolução.

- **Preparação de políticas específicas de IA**: estas políticas devem abranger vários aspetos do ciclo de vida e da utilização da IA, assegurando que todas as atividades relacionadas são conduzidas de forma ética, segura e em conformidade com a lei (utilização, desenvolvimento, aquisição, proteção de dados, auditoria e conformidade).

- **Mapeamento dos riscos e avaliação dos limiares aceitáveis**: Este processo envolve a identificação, análise e hierarquização dos riscos associados à utilização e ao desenvolvimento da IA, bem como a definição de limites claros sobre o que é considerado um nível de risco aceitável. Esta abordagem proactiva da gestão dos riscos será essencial para criar confiança e garantir o êxito a longo prazo da utilização das tecnologias de IA.

- **Adaptar os processos de contratação com prestadores de IA**: será necessário adaptar os modelos contratuais para garantir que os prestadores de IA cumprem o novo regulamento, atualizar os processos de aprovação e desenvolver mecanismos de gestão de riscos de terceiros neste domínio. Algumas das principais ações nesta área serão: a definição de requisitos específicos, procedimentos de avaliação, critérios de negociação, gestão de direitos intangíveis, ou a formação dos departamentos de compras e negociadores de contratos.

- **Rever e atualizar as apólices de seguro em relação à utilização e desenvolvimento de sistemas de IA**: será importante, em primeiro lugar, realizar uma avaliação detalhada dos riscos associados à utilização e desenvolvimento de sistemas de IA que inclua riscos técnicos, como falhas de *software* ou violações de segurança, e riscos jurídicos ou éticos, como violações da privacidade ou responsabilidade por decisões automatizadas. Com base nessa avaliação de risco, a cobertura dos seguros existentes deve ser revista para identificar potenciais lacunas ou exclusões que possam deixar a organização exposta a riscos relacionados com a IA. A partir daí, deve ser feito um trabalho com as seguradoras para desenvolver ou ajustar políticas que abordem especificamente os riscos associados à IA, o que pode incluir cobertura para erros e omissões no desenvolvimento de *software*, responsabilidade pelo produto, violações de dados e outros riscos específicos da tecnologia.

- **Avaliar o impacto nos direitos fundamentais**: a IA tem potencial para afetar de forma significativa vários direitos fundamentais dos cidadãos, incluindo a privacidade, a não discriminação, a liberdade de expressão e o direito a um processo de tomada de decisões justo e equitativo. Tal como o RGPD exige, em certos casos, a elaboração de uma avaliação de impacto sobre a proteção de dados (DPA), as organizações deverão desenvolver os seus modelos de avaliação de impacto sobre os direitos humanos (HRIA) para garantir o correto cumprimento do Regulamento IA.

- **Adaptar a organização ao conjunto de requisitos do Regulamento IA**: tendo em conta os prazos de aplicabilidade das diversas obrigações fixados pelo regulamento, será necessário desenvolver e aplicar um plano completo de adaptação. Algumas ações dependem de atos de execução que serão levados a cabo pelas administrações públicas nos próximos dois anos, pelo que não poderão ser executadas desde o início. No entanto, é essencial conceber uma estratégia a este respeito e coordenar o calendário de conformidade com o conjunto de decisões tecnológicas e empresariais que a organização planeia desenvolver neste domínio.

Pérez-Llorca

TECHLAW

Inteligência artificial

JUNHO 2024

Um desafio para as empresas e para os reguladores

Barcelona
-
Brussels
-
Lisbon
-
London
-
Madrid
-
New York
-
Singapore

perezllorca.com

- **Analisar os dados utilizados para treinar modelos de IA de finalidade geral**: dadas as obrigações de transparência estabelecidas no regulamento sobre os *datasets* utilizados para treinar um modelo linguístico de grande escala ou um modelo fundacionais, as empresas que utilizam sistemas de IA, especialmente a IA generativa, devem garantir que estes foram treinados sem infringir os direitos de terceiros relativamente aos dados utilizados e são suficientes para cumprir as obrigações no que diz respeito aos direitos fundamentais dos cidadãos. Essa análise deve ser devidamente documentada para ser mostrada ao Serviço para a IA, mediante pedido deste.

- **Desenvolvimento de mecanismos para a proteção de ativos incorpóreos**: este aspeto é particularmente relevante, tanto no desenvolvimento interno de sistemas de IA, como na aquisição de sistemas de IA de terceiros, incluindo cenários híbridos e os que envolvem *software* de fonte aberta ou ao abrigo de licenças gratuitas. Em muitos casos, a proteção de ativos incorpóreos só pode ser alcançada com base na legislação de proteção dos segredos comerciais. Esta legislação é particularmente rigorosa quando se trata de avaliar os mecanismos de proteção implementados desde as primeiras fases de concetualização da solução a proteger. É também fundamental avaliar que medidas serão tomadas para evitar a violação de direitos de terceiros em processos como o treino de ferramentas de IA ou o chamado "*fine tuning*", entre outros.

- **Acompanhar os desenvolvimentos legislativos e regulamentares**: manter-se atualizado sobre os desenvolvimentos legislativos e regulamentares para se adaptar a quaisquer alterações na legislação sobre IA.

- **Participar no desenvolvimento de boas práticas**: recomendamos a participação setorial na conceção de boas práticas, a fim de partilhar conhecimentos e experiências com outras organizações. O Regulamento IA é uma legislação transversal e cheia de conceitos indeterminados, suscetíveis de diferentes interpretações. A verticalização por sectores de atividade, *use cases* ou tecnologias através da definição de normas técnico-jurídicas e de boas práticas pode contribuir para aumentar o nível de segurança jurídica neste domínio, facilitando o investimento e o apoio à inovação, mantendo o necessário equilíbrio com as garantias exigidas pelo Regulamento IA.

- **Desenvolvimento de um modelo e de um plano de auditoria adaptados**: esta abordagem permitirá uma avaliação efetiva da conformidade dos sistemas de AI com a regulamentação aplicável, as normas éticas e os requisitos de segurança. Ao adotar uma abordagem sistemática e baseada em evidências, as organizações poderão demonstrar o seu empenho na responsabilização e na excelência na aplicação da IA.

Estas são apenas algumas das ações que as empresas que utilizam sistemas de IA podem tomar hoje para fazer uma transição suave para a conformidade com o Regulamento IA, com uma perceção positiva e capacitadora desta nova tecnologia, que não temos dúvidas de que trará mudanças significativas na sociedade e nos negócios.