REGULAMENTO INTELIGÊNCIA ARTIFICIAL

—

PONTOS-CHAVE

MARÇO 2024

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

Passados quase três anos da proposta apresentada pela Comissão Europeia, o Regulamento do Parlamento Europeu e do Conselho que Estabelece Regras Harmonizadas em Matéria de Inteligência Artificial (Regulamento Inteligência Artificial ou Regulamento) ganha os seus contornos finais. A votação nos comités do Parlamento Europeu ocorreu no passado dia 13 de fevereiro e falta apenas a aprovação do texto final pelo plenário, que, tendo estado anteriormente antevista para meados de abril, está agora agendada para 13 de março.

Tendo em conta que o texto aprovado recentemente pelos comités relevantes está já muito perto da versão final, a Morais Leitão – Digital Cluster Inteligência Artificial apresenta agora um breve guia sobre os pontos-chave do Regulamento Inteligência Artificial.

I. CONSIDERAÇÕES GERAIS: ENQUADRAMENTO, ÂMBITO E DEFINIÇÕES

O Regulamento Inteligência Artificial surge para proteger o mercado interno e visa estabelecer um quadro jurídico uniforme para os sistemas de inteligência artificial, em conformidade com os valores da União Europeia. Este Regulamento traz novas definições relevantes e aplica-se a múltiplos operadores de sistemas de inteligência artificial.

DE ONDE SURGE O REGULAMENTO INTELIGÊNCIA ARTIFICIAL?

Desde que a Comissão Europeia apresentou a proposta do Regulamento Inteligência Artificial a 21 de abril de 2021 que as instituições europeias e os Estados-Membros têm vindo a debater a forma de tratar a temática da inteligência artificial (IA) num enquadramento europeu que garanta a livre circulação de bens e serviços baseados na IA e a proteção dos direitos fundamentais.

Para evitar a existência de diferentes regras e restrições a nível nacional, que conduziriam à fragmentação do mercado interno e, por conseguinte, diminuiriam a segurança jurídica dos operadores, o Regulamento consagra um nível de proteção coerente e elevado em toda a União Europeia (UE), de modo a garantir que os sistemas de IA são confiáveis.

O Regulamento tem vários objetivos: *(i)* melhorar o funcionamento do mercado interno, estabelecendo um quadro jurídico uniforme para os sistemas de IA, em conformidade com os valores da UE; *(ii)* promover a adoção de uma IA centrada no ser humano e fiável, assegurando simultaneamente um elevado nível de proteção da saúde, da segurança, dos direitos fundamentais (incluindo a democracia e o Estado de Direito) e da proteção do ambiente; e *(iii)* apoiar a inovação.

A QUEM SE APLICA O REGULAMENTO?

O Regulamento aplica-se a múltiplos operadores de sistemas de IA:

- Fornecedores que coloquem sistemas de IA no mercado ou os coloquem em serviço no território da União, independentemente de estarem localizados na UE ou num país terceiro;
- Utilizadores localizados na UE;
- Fornecedores e utilizadores localizados fora da UE, quando o resultado do seu sistema for utilizado na União;
- Importadores e distribuidores;
- Fabricantes de produtos;
- Representantes autorizados de fornecedores fora da UE; e
- Pessoas afetadas que estejam localizadas na UE.

No entanto, as questões de segurança nacional e os modelos com o único objetivo de investigação e desenvolvimento científico estão explicitamente excluídos do Regulamento.

QUAIS AS PRINCIPAIS DEFINIÇÕES?

A presente definição de um sistema de IA, nos termos consagrados no Regulamento, – «sistema baseado em máquinas concebido para funcionar com níveis variáveis de autonomia e que pode apresentar adaptabilidade após a implantação e que, para objetivos explícitos ou implícitos, infere, a partir dos dados que recebe, como gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais»[1] –, foi atualizada para estar mais estreitamente alinhada com o trabalho em curso das organizações internacionais que trabalham em matéria de IA (por exemplo, a OCDE). Além disso, esta definição não se destina a abranger os sistemas de *software* tradicionais mais simples ou as abordagens de programação, que se baseiam em regras definidas exclusivamente por pessoas singulares para executar operações automaticamente.

Outras definições relevantes incluem a distinção entre "fornecedor" (quem desenvolve um sistema de IA e o coloca no mercado ou o coloca em serviço), "utilizador" (quem utiliza o sistema de IA), "importador" (quem coloca no mercado interno um sistema de IA desenvolvido por alguém fora da UE) e "distribuidor" (quem disponibiliza um sistema de IA na UE e não é um fornecedor ou importador).

1. Tradução livre de «machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments».

II. PRÁTICAS DE INTELIGÊNCIA ARTIFICIAL PROIBIDAS

Várias práticas de IA são proibidas pelo Regulamento Inteligência Artificial, ainda que com a possibilidade de exceções, em que são previstas medidas de mitigação dos riscos possíveis. A proibição de certas práticas visa garantir um nível mínimo de proteção dos direitos fundamentais.

QUAIS SÃO OS MECANISMOS DE IA PROIBIDOS?

De acordo com o artigo 5.º, são proibidas a colocação no mercado, a entrada em serviço ou a mera utilização de sistemas de IA que, com o objetivo de distorcer ou modificar comportamentos, de uma forma que cause ou seja suscetível de causar danos significativos a uma pessoa ou a um grupo:

- Usem técnicas propositadamente manipuladoras ou enganosas; ou
- Que explorem vulnerabilidades pessoais[2], bem como a utilização de sistemas de categorização biométrica que categorizem pessoas com base nos seus dados biométricos para deduzir as suas demais características.

Proíbem-se sistemas que levem à avaliação ou à classificação de pessoas, com base no seu comportamento, inferindo dele características pessoais, conduzindo a tratamentos desfavoráveis relativos a contextos diversos daqueles para os quais se recolheram os dados ou meramente injustificados ou desproporcionais.

No domínio penal, e no que respeita aos dados biométricos, são proibidos os sistemas que permitam a identificação remota "em tempo real" e em locais públicos, salvo na medida em que o seu uso seja estritamente necessário para:

- A procura de vítimas de crimes como rapto, tráfico de seres humanos e exploração sexual, bem como para a busca de pessoas desaparecidas;
- A prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança das pessoas, ou uma genuína e presente (ou previsível) ameaça de ataque terrorista; e
- A localização ou a identificação de uma pessoa suspeita da prática de crime para efeitos de investigação criminal ou execução de pena, quando o referido crime seja punido com uma moldura cujo máximo seja superior a quatro anos de prisão.

Além disso, são ainda proibidos os mecanismos de policiamento preditivo, quando estes tenham por base a previsão do risco do cometimento de um crime, com base na definição de um perfil de um indivíduo. Não são proibidos, no entanto, sistemas que avaliem o envolvimento de uma pessoa numa atividade criminosa, quando tenham por base factos objetivos e verificáveis.

São, por fim, proibidos os sistemas que criem ou expandam bases de dados de reconhecimento facial através da recolha de imagens faciais na internet ou CCTV e os que infiram emoções nos locais de trabalho e estabelecimentos de ensino, salvo quando estejam em causa razões de saúde ou segurança.

QUAIS AS CIRCUNSTÂNCIAS EM QUE SE APLICAM EXCEÇÕES À PROIBIÇÃO?

As exceções à proibição do recurso a sistemas de identificação biométrica à distância "em tempo real" em locais acessíveis ao público não são de aplicação imediata, estando as condições para a sua aplicação claramente definidas. Deve, em cada caso, ser feito um juízo norteado pelo interesse público, um balanço entre os potenciais prejuízos a evitar (nomeadamente, danos para a vida e para a integridade física de pessoas) e os riscos envolvidos.

Ainda que admissíveis, **tais exceções não são absolutas**, devendo ser circunscritas no tempo, no espaço e nas pessoas a que se aplicam, bem como submetidas a uma prévia avaliação de impacto nos direitos fundamentais, à semelhança dos sistemas de IA de risco elevado, por forma a identificar riscos específicos para indivíduos ou grupos de indivíduos.

A sua utilização permitida está sujeita a uma prévia autorização, que será vinculativa, por parte de uma autoridade judicial ou por uma autoridade administrativa independente, especialmente no que concerne às situações da alínea d) do n.º 1 e do n.º 2 deste artigo (relativo a sistemas de identificação biométrica à distância "em tempo real"). Para tal, é necessário submeter um pedido fundamentado, em sintonia com as normas do direito nacional expressas no n.º 4 deste artigo, fazendo-se acompanhar de provas claras e objetivas de que a utilização do sistema nestes modos é necessária e proporcional à

[2] Desta proibição excetua-se a rotulagem ou a filtragem de conjuntos de dados biométricos legalmente adquiridos, tais como imagens, com base em dados biométricos, nem a categorização de dados biométricos no domínio penal.

prossecução de um dos objetivos especificados na alínea d) do n.º 1, limitando-se ao absolutamente imprescindível (em matérias de tempo e de abrangência geográfica e pessoal). As autoridades devem assegurar-se que nenhuma decisão é vinculativa quando seja apenas tomada com base nos resultados do sistema de identificação biométrica à distância.

Para estas autorizações, impõe-se, que, para o efeito, os Estados-Membros respeitem, no mínimo (porque lhes é permitido estabelecerem um regime mais restritivo), as condições enumeradas na alínea d) do n.º 1 e nos n.ºs 2 e 3 do artigo 5.º, bem como que, de forma pormenorizada, prevejam, na sua legislação nacional, os objetivos passíveis de justificar o uso desses sistemas e as regras associadas quer ao procedimento de pedido, emissão e exercício dessa autorização, quer ao controlo destes e apresentação do associado relatório.

Sendo notificados dessas utilizações, as autoridades nacionais dos Estados-Membros têm de submeter à Comissão um relatório anual, que seguirá o modelo fornecido pela mesma. Estes relatórios serão anualmente publicados pela Comissão, excluindo os dados sensíveis relativos à atividade das autoridades policiais.

É POSSÍVEL APLICAR ESTAS EXCEÇÕES COM CARÁTER URGENTE, SEM A SUBMISSÃO DE UMA AVALIAÇÃO DE IMPACTO NOS DIREITOS FUNDAMENTAIS?

Em situações em que a urgência justificada determine a impossibilidade desse controlo, a utilização do sistema poderá ser iniciada sem a prévia autorização. No entanto, esta tem de ser prontamente justificada, num máximo de 24 horas, e a avaliação de impacto nos direitos fundamentais deverá ser submetida, quando possível.

No caso de esta autorização ser rejeitada, cessa de imediato a utilização do sistema em causa, levando à eliminação dos dados e de todos os resultados e produtos obtidos a partir dessa utilização.

OS ESTADOS-MEMBROS PODEM LEGISLAR SOBRE ESTAS EXCEÇÕES?

A proposta de Regulamento permite aos Estados a imposição de regimes mais restritivos e impõe-lhes ainda que, de forma pormenorizada, prevejam, na sua legislação nacional, os objetivos passíveis de justificar o uso desses sistemas e as regras associadas quer ao procedimento de pedido, emissão e exercício dessa autorização, quer ao controlo destes e apresentação do associado relatório.

QUAIS AS CONSEQUÊNCIAS DA COLOCAÇÃO NO MERCADO, DA ENTRADA EM SERVIÇO OU DA MERA UTILIZAÇÃO DE SISTEMAS DE IA PROIBIDOS POR PESSOAS SINGULARES OU COLETIVAS?

O Regulamento fixou as coimas pelo incumprimento em valores até 35 milhões de euros para pessoas singulares, ou até 7% do volume de negócios anual, para pessoas coletivas.

III. SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO

Entre os sistemas de IA permitidos e os sistemas de IA proibidos, encontramos os sistemas de IA de risco elevado. Estes sistemas, listados no Anexo III do Regulamento Inteligência Artificial, embora não proibidos, estão sujeitos a diversas limitações específicas para mitigar os riscos envolvidos.

QUAIS OS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL QUALIFICADOS COMO DE RISCO ELEVADO?

Os sistemas de IA de risco elevado representam a categoria mais ampla do Regulamento e, neste sentido, encontram-se adstritos a requisitos regulatórios rigorosos alinhados com a Carta dos Direitos Fundamentais da União Europeia.

Neste sentido, os critérios de classificação como sistemas de risco elevado são baseados no seu potencial impacto negativo na saúde, na segurança ou nos direitos fundamentais. Tal qualificação considera a probabilidade de tais riscos como o contexto do seu uso.

Um sistema de IA é, assim, qualificado como de risco elevado mediante o preenchimento cumulativo das seguintes condições:

- O sistema de IA é tido como uma componente de segurança de um produto, ou o próprio é um produto, que se enquadra na legislação da UE elencada no Anexo II; e
- O produto para o qual o sistema de IA é tido como componente de segurança, ou o sistema de IA como produto, encontra-se sujeito a uma avaliação de conformidade realizada por terceiros para colocação no mercado ou prestação de serviço.

A adicionar ao preenchimento de tais requisitos, e caso se enquadrem na lista do Anexo III, serão tidos como de risco elevado, quanto à sua aplicação:

- As infraestruturas críticas (*e.g.*, transportes públicos) que coloquem em causa a segurança;
- As ferramentas de formação educacional ou vocacional que possam influenciar as oportunidades de educação e de carreira profissional;
- As componentes de segurança de produtos, como será o caso de cirurgias realizadas por *robots*;
- As ferramentas de gestão de emprego, incluindo *software* usado em processos de contratação;
- Os serviços privados e públicos essenciais, como sistemas de pontuação de crédito que podem negar aos indivíduos o acesso a empréstimos;
- As ferramentas de aplicação da lei que podem afetar os direitos fundamentais;
- As ferramentas de gestão de migração, asilo e controle de fronteiras;
- Os sistemas usados na administração da justiça e processos democráticos.

O Regulamento estabelece que as disposições para sistemas de IA de risco elevado entrarão em vigor 36 meses após a publicação.

QUAIS SÃO AS REGRAS APLICÁVEIS AOS FORNECEDORES?

Nos termos do Regulamento, os fornecedores de IA têm um conjunto de obrigações em relação aos sistemas de IA de risco elevado.

Sistema de gestão de qualidade: os fornecedores de sistemas de IA de risco elevado devem implementar um sistema de gestão da qualidade documentado, de forma a garantir a conformidade com o Regulamento. Tal sistema deve abranger vários aspetos, incluindo: *(i)* estratégias de conformidade regulamentar; *(ii)* procedimentos de conceção e desenvolvimento; *(iii)* gestão de riscos; *(iv)* monitorização pós-comercialização; *(v)* comunicação de incidentes; *(vi)* gestão de dados; *(vii)* protocolos de comunicação; *(viii)* manutenção de registos; *(ix)* gestão de recursos; e *(x)* responsabilidade do pessoal.

A aplicação de tais requisitos deve ser **proporcional à dimensão da organização do fornecedor**, assegurando simultaneamente o nível necessário de rigor e de proteção. Quanto aos fornecedores sujeitos a legislação setorial específica da União, tais requisitos podem ser integrados nos sistemas existentes. As instituições financeiras sujeitas à legislação da UE, cumprem as obrigações de gestão da qualidade através da adesão a regras de governação interna, tendo em conta as normas harmonizadas pertinentes.

Neste sentido os fornecedores devem atentar às seguintes obrigações:

Conservação de documentos: devem conservar os documentos durante um período de 10 anos após o sistema de IA ter sido colocado no mercado ou ter entrado em serviço. Tal documentação inclui a documentação técnica, do sistema de gestão da qualidade, os registos das alterações aprovadas pelos organismos notificados, os documentos emitidos pelos organismos notificados e a declaração de conformidade europeia. Cada Estado-Membro estabelecerá as condições para conservar esta documentação em caso de insolvência ou cessação de atividade do prestador;

Registos automáticos: devem conservar os registos gerados automaticamente a partir dos seus sistemas, enquanto estes estiverem sob o seu controlo, durante um período mínimo de seis meses, salvo disposição em contrário da legislação da União ou nacional aplicável, nomeadamente em matéria de proteção de dados pessoais;

Ações corretivas: devem tomar medidas corretivas de forma imediata (*e.g.*, correção, remoção, desativação ou recolha) se acreditarem ou tiverem motivos para acreditar que um sistema que lançaram no mercado ou colocaram em uso não cumpre os requisitos do Regulamento;

Dever de informação: devem notificar os distribuidores do sistema e, se necessário, os utilizadores, o representante autorizado e os importadores caso um sistema de IA de risco elevado representar um risco e o fornecedor tiver conhecimento desse facto. Adicionalmente, o fornecedor deve investigar imediatamente as causas, em cooperação com a entidade implantadora, se for caso disso, e informar as autoridades de nacionais competentes nos Estados-Membros nos quais o sistema foi disponibilizado;

Cooperação com as autoridades competentes: os fornecedores devem *(i)* a pedido de uma autoridade competente, fornecer todas as informações e documentação necessárias para demonstrar a conformidade com os requisitos, numa língua compreendida pela autoridade ou numa língua oficial da União determinada pelo Estado-Membro em causa, *(ii)* conceder acesso aos registos do sistema a pedido de uma autoridade nacional competente e, por último, *(iii)* tais informações obtidas pela autoridade nacional competente devem ser tratadas de forma confidencial.

Adicionalmente, é estabelecido que fornecedores de sistemas de Inteligência Artificial de risco elevado estabelecidos fora da EU devem nomear um representante autorizado na UE. Tal representante deve desempenhar as tarefas especificadas no mandato recebido do fornecedor. O representante autorizado deve rescindir o mandato se considerar que o fornecedor atua de forma contrária às suas obrigações previstas no Regulamento Inteligência Artificial, informando as autoridades competentes em conformidade.

Além disso, os fornecedores e terceiros que fornecem componentes ou serviços para sistemas de IA de alto risco devem elaborar acordos de prestação de informação e assistência. O *AI Office* pode recomendar modelos de cláusulas contratuais para estes acordos. Finalmente, estas disposições devem respeitar os direitos de propriedade intelectual e as informações comerciais confidenciais.

COMO É REALIZADA A QUALIFICAÇÃO SUPERVENIENTE COMO FORNECEDOR?

Qualquer pessoa singular ou coletiva deve ser considerada "fornecedor de um sistema de IA de elevado risco", sujeitando-se às respetivas obrigações consagradas no Regulamento, quando: *(i)* coloque o seu próprio nome ou a sua marca num sistema de IA de elevado risco previamente colocado no mercado ou em serviço; *(ii)* altere substancialmente um sistema de IA de elevado risco previamente colocado no mercado ou em serviço; ou *(iii)* altere a finalidade de um sistema de IA (incluindo sistemas de IA de finalidade geral) previamente colocado no mercado ou em serviço de modo a que esse sistema passe a ser classificado como sendo de elevado risco, para efeitos do Regulamento.

Nestes casos, o fornecedor que inicialmente colocou o sistema de IA no mercado ou em serviço deixa de ser considerado como fornecedor, muito embora deva cooperar e disponibilizar a informação necessária para o cumprimento das obrigações que decorrem para o fornecedor, quando não tenha proibido a alteração do seu sistema para um sistema de elevado risco.

QUAIS SÃO AS REGRAS APLICÁVEIS AOS DISTRIBUIDORES?

Os distribuidores devem verificar se os sistemas de IA de alto risco *(i)* exibem a marcação de conformidade CE exigida, *(ii)* incluem a documentação e as instruções de utilização necessárias e se *(iii)* o fornecedor e o importador cumpriram as obrigações que recaem

sobre si, quando aplicável. Os distribuidores devem também assegurar que *(iv)* as condições de armazenamento e/ou de transporte não prejudicam a conformidade do sistema de IA.

Caso existam motivos para se considerar que um sistema de IA de risco elevado não se encontra em conformidade com o Regulamento, não estará autorizado a disponibilizar esse sistema no mercado até ser reposta a sua conformidade.

Por sua vez, se um sistema de IA de risco elevado já disponibilizado no mercado não cumprir as exigências previstas no Regulamento, o distribuidor deverá adotar todas as medidas corretivas que se afigurem necessárias, incluindo a de retirada ou de recolha desse sistema do mercado. O distribuidor deverá também assegurar que o fornecedor, o importador ou qualquer operador envolvido tomam as ações corretivas adequadas.

Na eventualidade de um sistema de IA de risco elevado representar um risco para a saúde, para a segurança ou para a proteção de direitos fundamentais, o distribuidor está obrigado a informar as autoridades nacionais competentes dos Estados-Membros em que disponibilizou esse sistema, bem como o fornecedor ou o importador do mesmo, conforme aplicável.

Finalmente, o Regulamento prevê ainda deveres de informação e de cooperação dos distribuidores com as autoridades nacionais competentes, mediante pedidos fundamentados destas.

QUAIS SÃO AS REGRAS APLICÁVEIS AOS IMPORTADORES?

Os importadores, antes de colocarem um sistema de IA de risco elevado no mercado, devem assegurarse de que o referido sistema: *(i)* se encontra em conformidade com as regras previstas; *(ii)* possui toda a documentação técnica necessária; *(iii)* é portador do certificado de conformidade europeu; e *(iv)* tem um representante nomeado. As condições de admissibilidade no mercado devem ser asseguradas pelos importadores quando o sistema se encontra à sua responsabilidade, o que inclui armazenamento e transporte.

Os importadores devem ainda impedir a disponibilização ao mercado de sistema IA que acreditem não estar em conformidade com o presente regulamento, o que devem fazer até o mesmo verificar todas as condições legais. Os importadores devem ainda notificar o fornecedor sempre que o sistema de IA apresente riscos para a saúde, segurança ou direitos fundamentais.

Quando comercializado, o sistema de IA deve ainda assegurar um conjunto de indicações, tais como: *(i)* o nome do importador; *(ii)* o nome comercial registado ou a marca; e *(iii)* o respetivo endereço de contacto, informações estas que devem constar, ora da embalagem, ora da documentação que o acompanha.

Os importadores devem guardar, **por um período de 10 anos** após a entrada no Mercado ou a entrada em serviço, **cópia do certificado** emitido por entidade competente, **instruções de uso** e **declaração de conformidade da UE**, sempre que aplicável.

Os importadores têm ainda de cooperar, sempre que solicitado, com as autoridades competentes, o que, entre outros aspetos, se traduz na disponibilização de documentação na língua da autoridade notificante.

QUAIS SÃO AS REGRAS APLICÁVEIS AOS UTILIZADORES?

Enquanto participantes da cadeia de valor dos sistemas de IA de risco elevado, sobre os utilizadores desses sistemas, impendem um conjunto de obrigações cujo regime assenta numa bipartição.

A bipartição traduz-se na previsão de:

1. Obrigações universais que vinculam todos os utilizadores dos sistemas de IA de risco elevado; e

2. Obrigações adicionais ou específicas que abrangem apenas alguns utilizadores ou alguns contextos ou usos dos sistemas de IA de risco elevado.

[3] Ou a sua recondução ao cumprimento de outros deveres de governação decorrentes de legislação regulatória setorial específica, como sucede, no caso dos utilizadores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/EU - *Diretiva relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento* - relativamente aos quais os deveres de monitorização dos sistemas de IA de risco elevado e de conservação de logs consideram-se satisfeitos mediante o cumprimento (ou devem integrar-se nesse cumprimento) das regras relativas aos sistemas (dispositivos), processos e mecanismos de *governance* internos decorrentes da legislação regulatória de transposição daquela Diretiva.

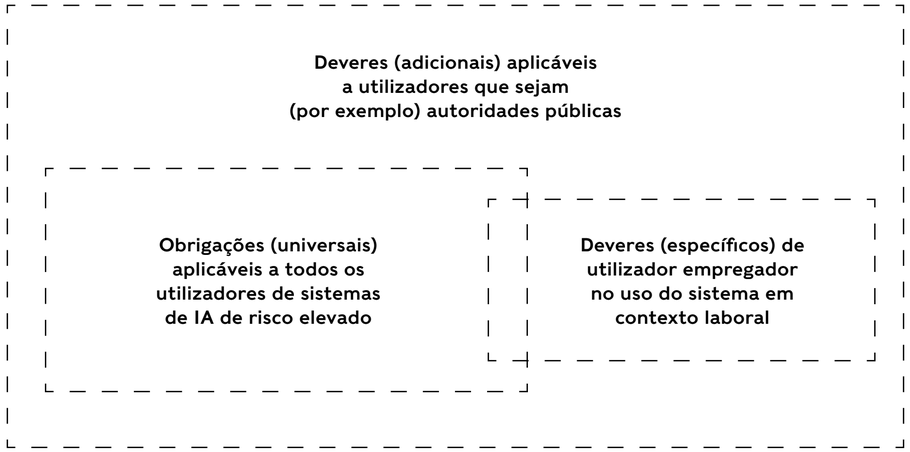
As especialidades que justificam a previsão de deveres adicionais ou específicos[3] e que apenas vinculam esses utilizadores ou que só se aplicam em determinadas circunstâncias, contextos ou fins da utilização dos sistemas de IA de elevado risco podem decorrer de diferentes elementos, tais como:

2.1. A natureza do utilizador (por exemplo, entre outros, utilizadores que sejam autoridades públicas ou entidades sujeitas ao direito público ou que prestem serviço público);

2.2. A qualidade em que o utilizador atua e do contexto em que utiliza o sistema (por exemplo, utilizadores, enquanto empregadores, no uso que façam de sistemas de IA de alto risco em contexto laboral);

2.3. Os fins a que o utilizador destine o uso dos sistemas de IA de risco elevado (por exemplo, utilizadores que recorram a sistemas de IA de risco elevado na tomada de decisões respeitantes a pessoas singulares); e ainda

2.4. O controlo concreto que possam ou não ter sobre diferentes aspetos do sistema (por exemplo, um utilizador que exerça controlo sobre os dados de entrada dos sistemas de IA de risco elevado que utilize).



Uma exemplificação, gráfica, do que é dito acima pode ser ilustrada do modo seguinte:

É de notar que:

- Sobre os utilizadores sujeitos aos deveres adicionais recaem não apenas estes, como também as obrigações universais aplicáveis a todos os utilizadores de sistemas de IA de risco elevado; e

- Sobre um mesmo utilizador podem incidir vários tipos de deveres adicionais ou específicos (por exemplo, num mesmo sujeito jurídico, para além dos gerais podem cumular-se os deveres adicionais decorrentes da sua natureza pública e os especiais associados à utilização de sistemas de IA de risco elevado, enquanto empregador e em contexto laboral).

Obrigações (universais) aplicáveis, em todos os casos, aos utilizadores de sistemas de IA de risco elevado:

- Dever de adoção de medidas técnicas e organizativas adequadas para garantir uma utilização do sistema de IA de risco elevado conforme com as instruções de uso, designadamente, no que respeita à aplicação de medidas de supervisão humana indicadas pelo fornecedor;

- Dever de controlo (monitorização) do funcionamento do sistema de IA de risco elevado com base nas instruções de uso e dever de fornecimento de dados relevantes para o sistema de acompanhamento pós-comercialização do fornecedor;

- Deveres de comunicação ao fornecedor do sistema de IA de risco elevado (ou a outros participantes da cadeia de valor) e à autoridade de fiscalização do mercado de riscos da utilização do sistema de acordo com as instruções, para a saúde e segurança ou para a proteção dos direitos fundamentais das pessoas, identificados pelo utilizador no âmbito do dever de monitorização, ou em caso de identificação da ocorrência de incidente grave decorrente dessa utilização;

- Dever de suspensão de utilização do sistema em casos de identificação daqueles riscos ou ocorrência de incidente grave;

- Dever de consideração (utilização) da informação contida nas instruções de utilização que devem acompanhar o sistema de risco elevado para a realização, pelo utilizador, de avaliação de impacto sobre a proteção de dados (DPIA) quando a sua realização, pelo utilizador, seja exigida nos termos do RGPD;

- Deveres gerais de cooperação com as autoridades nacionais competentes.

DEPENDENDO DO CONTROLO SOBRE DIFERENTES ASPETOS DO SISTEMA UTILIZADO, ESTÃO AINDA PREVISTAS AS SEGUINTES OBRIGAÇÕES:

- Garantir que as pessoas singulares designadas para assegurar a supervisão humana dos sistemas de IA de risco elevado dispõem de competência, formação, poderes e apoio (de meios) necessários para o efeito;

- Assegurar que os dados de entrada dos sistemas de IA de risco elevado são pertinentes e suficientemente representativos em função da finalidade prevista do sistema de IA de risco elevado, na medida em que o utilizador exerça controlo sobre esses dados;

- Conservar os *logs* (registos) gerados automaticamente pelo sistema de IA de risco elevado pelo prazo mínimo de 6 meses desde que esses *logs* estejam sob o controlo do utilizador.

Dependendo da utilização dada aos sistemas (em conjugação ou não com determinada qualidade do utilizador) podem ainda mencionar-se os seguintes deveres:

- Dever de prestar informação às pessoas singulares relativamente às quais utilize sistemas de IA de risco elevado na tomada de decisões do recurso a esses sistemas para esse fim;

- Dever do utilizador que seja empregador de prestar informação aos trabalhadores afetados e às suas estruturas representativas, de que os trabalhadores irão ficar abrangidos pelo uso do sistema de IA de risco elevado em contexto laboral, antes de iniciar essa utilização;

- Dever de realizar uma avaliação prévia de impacto nos direitos fundamentais e de notificar a autoridade de fiscalização do mercado dos resultados da avaliação, previamente à utilização do sistema de IA de risco elevado sempre que o utilizador (com algumas exceções):

  - seja um organismo de direito público;

  - seja um operador privado que preste serviços públicos;

  - use um sistema de IA de risco elevado para, relativamente a uma pessoa singular, fazer avaliação de crédito, determinar o *scoring* de crédito (exceto para deteção de fraude de crédito) ou fazer avaliação de risco e tarifação nos ramos de seguros de vida e saúde, quando esteja em causa o acesso ou uso de serviços privados essenciais ou serviços e benefícios públicos essenciais.

Prevê-se que o Serviço Europeu para a Inteligência Artificial desenvolva um modelo de questionário, através de uma ferramenta automatizada, para ajudar os utilizadores a implementar o dever de avaliação prévia de uma forma simplificada.

Obrigações adicionalmente aplicáveis aos utilizadores de sistemas de IA de risco elevado atendendo (exclusivamente) à respetiva natureza:

- **Autoridades públicas ou instituições, órgãos, organismos e agências da União Europeia**

- Registar-se, selecionar o sistema de IA de risco elevado que tencionam utilizar e registar a sua utilização na base de dados da UE relativa a sistemas de inteligência artificial de risco elevado[4];

- Abster-se de utilizar o sistema caso não se encontre registado na mencionada base de dados da UE e, neste caso, informar disso o fornecedor ou o distribuidor.

Estão ainda previstos deveres específicos que conferem salvaguardas adicionais no que se refere à **utilização de sistemas de IA** (que estão qualificados como de risco elevado) para uso de **identificação biométrica** à distância (posterior), particularmente, por **autoridades públicas policiais**.

4. Cfr. artigos 51.º e 60.º do Regulamento.

IV. MODELOS DE IA DE FINALIDADE GERAL

Após várias discussões ocorridas desde a publicação da primeira versão da proposta do Regulamento Inteligência Artificial pela Comissão Europeia, as instituições chegaram a um acordo sobre a regulamentação relativamente aos modelos de IA de finalidade geral, como o ChatGPT.

Em que consistem os modelos GPAI?

Os modelos de *General Purpose Artificial Intelligence* (GPAI) são definidos como um modelo de IA cujo processo de treino é realizado de forma autossuficiente com recurso a grande conjunto de dados. Estes modelos têm capacidade de dar resposta a um leque alargado de pedidos e de executar um amplo conjunto de tarefas, independentemente da forma como o modelo é colocado no mercado europeu. Estes modelos têm como vantagem a possibilidade de serem integrados em vários sistemas ou aplicações *downstream*. Um dos exemplos mais populares é o ChatGPT.

Quais são as principais obrigações aplicáveis aos modelos GPAI?

Transparência é a palavra-chave: quando os sistemas de IA são destinados a interagir diretamente com pessoas, devem ser projetados e desenvolvidos de tal forma que que as mesmas sejam informadas de maneira clara e explícita ou se encontrem claramente conscientes de que se encontram a interagir com um sistema de IA, pelo menos no momento da primeira interação.

Dentro da mesma lógica, os fornecedores de sistemas de IA que geram dados sintéticos (áudio, imagem ou texto) devem garantir que esses dados são marcados num formato legível por um outro sistema e identificáveis como conteúdo gerado artificialmente ou manipulado – a menos que tal prejudique o lado criativo da obra, *i.e.*, gerar uma piada sobre a interação de sistemas de IA com pessoas.

Quanto à tensão entre a **proteção dos direitos de autor e *mining* de texto e dados**, é estabelecido que «qualquer uso de conteúdo protegido por direitos de autor requer a autorização do titular dos direitos envolvidos, a menos que se apliquem exceções e limitações de direitos de autor relevantes». Assim, quando os direitos foram expressamente reservados por meio de um "*opt out*" adequado, os fornecedores de modelos GPAI necessitam de obter uma autorização dos titulares dos direitos, caso queiram realizar operações de *mining* sobre aquele texto e dados, em consonância com a de Mercado Único Digital.

Adicionalmente, os fornecedores devem:

- Elaborar e manter atualizada a documentação técnica do modelo GPAI;
- Elaborar, manter atualizada e disponibilizar documentação a fornecedores de sistemas de IA que pretendam integrar o GPAI no seu sistema de IA;
- Implementar uma política relativa ao respeito pela legislação europeia dos Direitos de Autor;
- Elaborar e tornar disponível publicamente um sumário suficientemente detalhado sobre os dados usados para efeitos de treino do modelo GPAI.

Todos os GPAI têm um risco baixo ou limitado?

Os modelos GPAI apresentam, geralmente, risco limitado. Contudo, **os modelos GPAI podem apresentar riscos sistémicos**, nomeadamente quando produzem: *(i)* efeitos negativos, reais ou razoavelmente previsíveis quanto a incidentes de grande dimensão; *(ii)* interrupções de setores críticos e impactos graves na saúde pública e segurança; *(iii)* quaisquer efeitos negativos reais ou razoavelmente previsíveis quanto processos democráticos, segurança pública e económica; ou *(iv)* a disseminação de conteúdo ilegal, falso ou discriminatório.

Portanto, um modelo GPAI deve ser classificado com **risco sistémico** se preencher um dos seguintes critérios:

a. O sistema tem capacidades de grande impacto avaliadas com base em ferramentas e metodologias técnicas apropriadas, incluindo indicadores e *benchmarks* – a presunção de capacidade de grande impacto decorre da quantidade computacional cumulativa para o treino, medida em operações de vírgula flutuante por segundo (FLOP[5]) for maior que 10^25;

5. Trata-se de uma medida de desempenho computacional.

b. É baseado numa decisão da Comissão.

Além dos requisitos estabelecidos *supra*, os modelos GPAI com risco sistémico devem:

- Identificar, avaliar e mitigar riscos sistémicos;
- Manter registo, documentar e relatar incidentes graves ao Serviço Europeu para a Inteligência Artificial;
- Garantir um nível adequado de proteção de cibersegurança.

O Regulamento incentiva o cumprimento das obrigações acima referidas através da adoção e **implementação de um código de conduta**.

É de notar que os modelos GPAI, caso sejam classificados como sistemas de alto risco ou tidos como componentes de sistemas de IA de alto risco, podem ser obrigados a cumprir as obrigações *supra* em relação aos sistemas de alto risco.

Estas obrigações são aplicáveis a todos os modelos de GPAI?

Para promover a inovação e o crescimento do ecossistema da UE, **algumas destas obrigações não se aplicam**, caso o modelo GPAI seja disponibilizado sob uma **licença livre e de código aberto**[6], exceto se apresentar riscos sistémicos.

6. A licença será considerada livre quando os utilizadores puderem aceder, usar, modificar e redistribuir livremente esses modelos ou versões modificadas dos mesmos.

V. MEDIDAS DE SUPORTE À INOVAÇÃO

Está prevista a criação a nível nacional de sandboxes regulatórias e a possibilidade de testagem em condições reais, oferecendo, assim, às empresas, e em particular, às PMEs e start-ups oportunidades para o desenvolvimento e treino de sistemas de IA inovadores antes da sua colocação no mercado.

COMO FUNCIONAM AS *SANDBOXES*?

De acordo com o Regulamento Inteligência Artificial, as autoridades nacionais competentes (sozinhas ou em cooperação com as autoridades de outros Estados-Membros) deverão criar pelo menos um ambiente de teste regulamentar, isto é, uma *sandbox* física, digital ou híbrida. Está em causa um "ambiente" experimental concreto e controlado, onde (potenciais) fornecedores de sistemas de IA poderão desenvolver, treinar, validar e testar um sistema de IA, durante um período de tempo limitado, e de acordo com um plano que descreve os objetivos, as condições, o calendário, a metodologia e os requisitos para as atividades realizadas no âmbito da *sandbox*.

As *sandboxes* visam promover a inovação e acelerar o acesso ao mercado, aumentar a segurança jurídica, facilitar a aprendizagem regulamentar baseada em provas e apoiar a cooperação e a partilha de melhores práticas em benefício das empresas e das autoridades. Em alternativa à criação de uma nova *sandbox*, poderão também ser utilizadas *sandboxes* já existentes, contanto que a participação proporcione um nível equivalente de cobertura nacional. Em ambos os casos, a autoridade competente deve, a pedido do prestador, fornecer prova escrita das atividades concluídas com êxito, e um relatório de saída que descreva pormenorizadamente tanto as atividades desenvolvidas, como os respetivos resultados, inclusive de aprendizagem. Estes documentos podem e devem ser utilizados pelas autoridades de fiscalização de mercado e pelos organismos notificados, para acelerar os procedimentos de avaliação da conformidade.

COMO FUNCIONA A TESTAGEM EM AMBIENTE REAL?

No contexto das *sandbox* de IA, que oferecem um ambiente controlado para o desenvolvimento, treino, teste e validação de sistemas de IA, **será também possível a realização de testes em ambiente real, mediante autorização das autoridades competentes nacionais.** Tal autorização inclui os termos e condições específicos da testagem, abrangendo as salvaguardas necessárias para a proteção dos direitos fundamentais, saúde e segurança.

Além disso, é possível que fornecedores ou potenciais fornecedores ("fornecedores") de sistemas de IA de risco elevado, em conformidade com o Anexo III, realizem testes em condições reais fora das *sandbox*. Tais testes devem estar em conformidade com um plano de testes em ambiente real, cujos elementos serão detalhados em atos de implementação da Comissão.

A testagem em ambiente real poderá ocorrer **em qualquer fase da vida do sistema**, antes da colocação no mercado ou da respetiva implementação, e de forma independente ou em colaboração.

Para realizar testes em condições reais, os fornecedores deverão cumprir cumulativamente várias condições, incluindo, mas não se limitando a:

1. Elaborar um plano de testes em ambiente real e submetê-lo à autoridade nacional competente (ANC) do mercado onde o teste será realizado;

2. Obter aprovação e autorização para o plano de testes por parte da ANC;

3. Registar o teste em ambiente real na secção não pública da base de dados da UE, com um número de identificação único em toda a União (com certas exceções para sistemas de IA de risco elevado, no âmbito de aplicação da lei, migração, asilo e gestão de controlo de fronteiras);

4. Garantir que o fornecedor se encontre estabelecido na UE ou tenha nomeado um representante legal dentro da UE;

5. Implementar salvaguardas apropriadas para dados recolhidos e tratados para finalidades de testes;

6. Garantir que indivíduos de grupos vulneráveis se encontrem adequadamente protegidos.

Tais condições não apenas possibilitam que as ANC monitorizem tais testes, mas também que os fornecedores consigam identificar os incidentes e eventuais medidas de mitigação de maneira adequada. Além disso, o consentimento informado dos participantes do teste é obrigatório, o que significa que os fornecedores devem comunicar claramente a natureza, a finalidade, e as condições do teste, assim como o direito dos participantes de retirar o consentimento a qualquer momento.

EXISTEM REGRAS ESPECIAIS PARA PME?

As pequenas e médias empresas beneficiarão de um conjunto de medidas que incluem, entre outras, o **acesso prioritário** aos ambientes de testagem, canais de comunicação dedicados e **redução de taxas** que venham a ser devidas no seguimento das avaliações de conformidade.

VI. GOVERNANÇA E QUADRO SANCIONATÓRIO

O Regulamento Inteligência Artificial estabelece um quadro de governação complexo, com a intervenção coordenada de novas autoridades responsáveis pela respetiva aplicação, quer ao nível da UE, quer a nível nacional. As infrações ao disposto no Regulamento poderão resultar em sanções com coimas de valor elevado.

QUEM FARÁ CUMPRIR O REGULAMENTO NA UNIÃO EUROPEIA?

No âmbito da Comissão Europeia, é estabelecido o Serviço Europeu para a Inteligência Artificial com o objetivo de desenvolver as competências e as capacidades da UE no domínio da IA e contribuir para a aplicação da legislação da União nesta matéria.

O Serviço Europeu para a IA também tem como missão acompanhar a implantação de sistemas de IA e as obrigações dos fornecedores (especialmente para sistemas de risco elevado e *general-purpose* AI com risco sistémico).

Para além do Serviço Europeu para a IA, o Regulamento também cria o Comité Europeu para a Inteligência Artificial – composto por representantes dos Estados-Membros, um painel científico de peritos independentes e um órgão consultivo – para aconselhar e assistir a Comissão e os EstadosMembros a fim de facilitar a aplicação coerente e eficaz do Regulamento. Este Comité é responsável por um conjunto de tarefas consultivas, incluindo a emissão de pareceres, recomendações, aconselhamento ou contribuição para orientações sobre questões relacionadas com a aplicação do Regulamento (nomeadamente questões de execução, especificações técnicas ou normas relativas a requisitos) e o aconselhamento da Comissão e dos Estados-Membros e das suas autoridades nacionais competentes sobre questões específicas relacionadas com a IA.

E NOS ESTADOS-MEMBROS?

Os Estados-Membros têm de estabelecer pelo menos duas autoridades nacionais competentes, para assegurarem a aplicação e a execução do Regulamento: uma autoridade de controlo e uma autoridade de fiscalização do mercado.

Estas autoridades nacionais exercem as suas competências de maneira independente, imparcial e objetiva para garantir a aplicação e a execução do Regulamento em cada Estado-Membro.

Em particular, o Regulamento exige que as autoridades nacionais disponham permanentemente de recursos humanos suficientes, cujas competências e conhecimentos especializados deverão incluir uma compreensão profunda das tecnologias de IA, dos dados e da computação de dados, da proteção dos dados pessoais, de cibersegurança, dos direitos fundamentais e dos riscos para a saúde e a segurança, bem como o conhecimento das normas e dos requisitos legais em vigor.

Além disso, os Estados-Membros não devem criar obstáculos injustificados à colocação no mercado ou à disponibilização de sistemas de IA de risco elevado que cumpram os requisitos estabelecidos no Regulamento.

No caso de investigações criminais, é necessária a autorização prévia das autoridades judiciais ou administrativas para a utilização de sistemas de IA para a identificação biométrica à distância.

A MINHA EMPRESA NÃO TEM SEDE NA UE, TENHO DE CUMPRIR O REGULAMENTO?

Sim, quer esteja estabelecida na União ou num país terceiro, a empresa que implementar ou colocar no mercado europeu um sistema de IA, terá de cumprir o Regulamento. Mesmo que treine um sistema de IA numa jurisdição com requisitos menos exigentes relativamente a direitos de autor, deverá ser assegurado um nível de proteção semelhante ao previsto no Regulamento.

O QUE ACONTECE SE HOUVER UMA INFRAÇÃO?

A violação das obrigações previstas no Regulamento poderá resultar em sanções (coimas) que podem ir **até 35 milhões de euros ou até 7% do volume de negócios anual**, a nível mundial, de uma empresa no exercício financeiro anterior, consoante o valor que for mais elevado.

No entanto, haverá um **período de carência** para os fornecedores de GPAI, aos quais não poderão ser aplicadas coimas durante o primeiro ano após a entrada em vigor do Regulamento.

VII. PRÓXIMAS ETAPAS DO REGULAMENTO INTELIGÊNCIA ARTIFICIAL

Quais as próximas etapas do Regulamento Inteligência Artificial?

- **Publicação: haverá ainda trabalho técnico a completar para a fixação do texto e, uma vez formalmente adotado pelo Parlamento Europeu e pelo Conselho, o Regulamento será publicado no Jornal Oficial da União Europeia;**

- **Entrada em vigor: o Regulamento entrará em vigor 20 dias após a sua publicação;**

- **Período de transição: após a sua publicação, o Regulamento entrará então no seu período de transição, sendo a maior parte das suas regras aplicáveis no prazo de 24 meses contados a partir da data de entrada em vigor, com outros marcos temporais para a aplicação de certas matérias, destacando-se, em especial o caso das regras relativamente a práticas de inteligência artificial proibidas que serão aplicáveis no prazo de 6 meses.**

CONTACTE-NOS

ARTIFICIAL INTELLIGENCE
ML Digital Cluster

A equipa ML Digital Cluster Inteligência Artificial continuará a acompanhar atentamente todos os desenvolvimentos do Regulamento Inteligência Artificial, mantendo-se ao dispor para qualquer esclarecimento adicional.

DIGITAL TOGETHER,
FIRM FOR TOMORROW.

HEAD OFFICE
LISBOA
Rua Castilho, 165
1070-050 Lisboa
T +351 213 817 400
F +351 213 817 499
mlgtslisboa@mlgts.pt

PORTUGAL
ANGOLA
MOÇAMBIQUE
CABO VERDE
SINGAPURA

LexMundi
Member

mlgts.pt

MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA & ASSOCIADOS