COMISSÃO
EUROPEIA

Bruxelas, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

QUE ESTABELECE REGRAS HARMONIZADAS EM MATÉRIA DE INTELIGÊNCIA ARTIFICIAL (REGULAMENTO INTELIGÊNCIA ARTIFICIAL) E ALTERA DETERMINADOS ATOS LEGISLATIVOS DA UNIÃO

{SEC(2021) 167 final} - {SWD(2021) 84 final} - {SWD(2021) 85 final}

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

1.1. Razões e objetivos da proposta

A presente exposição de motivos acompanha a proposta de regulamento que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial). A inteligência artificial (IA) é uma família de tecnologias em rápida evolução capaz de oferecer um vasto conjunto de benefícios económicos e sociais a todo o leque de indústrias e atividades sociais. Ao melhorar as previsões, otimizar as operações e a afetação de recursos e personalizar o fornecimento dos serviços, a utilização da inteligência artificial pode contribuir para resultados benéficos para a sociedade e o ambiente e conceder vantagens competitivas às empresas e à economia europeia. Essa ação torna-se especialmente necessária em setores de elevado impacto, incluindo os domínios das alterações climáticas, do ambiente e da saúde, do setor público, das finanças, da mobilidade, dos assuntos internos e da agricultura. Contudo, os mesmos elementos e técnicas que produzem os benefícios socioeconómicos da IA também podem trazer novos riscos ou consequências negativas para os cidadãos e a sociedade. À luz da velocidade da evolução tecnológica e dos possíveis desafios, a UE está empenhada em alcançar uma abordagem equilibrada. É do interesse da União preservar a liderança tecnológica da UE e assegurar que novas tecnologias, desenvolvidas e exploradas respeitando os valores, os direitos fundamentais e os princípios da União, estejam ao serviço dos cidadãos europeus.

A presente proposta honra o compromisso político assumido pela presidente Ursula von der Leyen, que anunciou nas suas orientações políticas para 2019-2024, intituladas «Uma União mais ambiciosa»[1], que a Comissão apresentaria uma proposta legislativa relativa a uma abordagem europeia coordenada às implicações humanas e éticas da inteligência artificial. Na sequência desse anúncio, a Comissão publicou, em 19 de fevereiro de 2020, o Livro Branco sobre a inteligência artificial — Uma abordagem europeia virada para a excelência e a confiança[2]. O Livro Branco define as opções políticas sobre a forma de alcançar o duplo objetivo de promover a adoção da IA e de abordar os riscos associados a determinadas utilizações desta tecnologia. A presente proposta visa dar execução ao segundo objetivo, desenvolvendo um ecossistema de confiança mediante a proposta de um quadro jurídico para uma IA de confiança. A proposta tem como base os valores e os direitos fundamentais da UE e pretende dar às pessoas e a outros utilizadores a confiança necessária para adotarem soluções baseadas em IA, ao mesmo tempo que incentiva as empresas para que as desenvolvam. A inteligência artificial deve ser uma ferramenta ao serviço das pessoas e uma força positiva para a sociedade com o objetivo final de aumentar o bem-estar dos seres humanos. As regras aplicáveis às tecnologias de inteligência artificial disponibilizadas no mercado da União ou que afetam as pessoas da União devem, por isso, centrar-se no ser humano, de modo que as pessoas possam confiar que a tecnologia é utilizada de uma forma segura e em cumprimento da lei, incluindo em matéria de respeito dos direitos fundamentais. Na sequência da publicação do Livro Branco, a Comissão lançou uma consulta abrangente das partes interessadas, a qual revelou um grande interesse por parte de um vasto número de partes que apoiaram amplamente a intervenção regulamentar com vista a resolver os desafios e as preocupações relacionadas com a crescente utilização da IA.

---

[1] https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_pt.pdf.

[2] Comissão Europeia: Livro Branco sobre a inteligência artificial — Uma abordagem europeia virada para a excelência e a confiança [COM(2020) 65 final].

A proposta também dá resposta a pedidos explícitos do Parlamento Europeu e do Conselho Europeu, que têm apelado, repetidamente, para a ação legislativa, com vista a assegurar o bom funcionamento do mercado interno de sistemas de inteligência artificial («sistemas de IA»), no qual os benefícios e os riscos da IA sejam abordados de forma adequada a nível da União. A proposta apoia o objetivo da União de estar na vanguarda mundial do desenvolvimento de uma inteligência artificial que seja segura, ética e de confiança, conforme mencionado pelo Conselho Europeu[3], e garanta a proteção de princípios éticos, conforme pedido especificamente pelo Parlamento Europeu[4].

Em 2017, o Conselho Europeu apelou para que fosse tomada a «consciência da urgência em fazer face às tendências emergentes, entre as quais se contam a inteligência artificial [...], com a garantia simultânea de um elevado nível de proteção dos dados, direitos digitais e normas éticas»[5]. Nas suas Conclusões sobre o plano coordenado para o desenvolvimento e utilização da inteligência artificial «Made in Europe», de 2019[6], o Conselho continuou a destacar a importância de assegurar o pleno respeito dos direitos dos cidadãos europeus e apelou para uma reapreciação da legislação pertinente em vigor, para torná-la adequada à sua finalidade no que respeita às novas oportunidades que a inteligência artificial oferece e aos desafios que coloca. O Conselho Europeu também convidou a Comissão a definir claramente as aplicações de inteligência artificial que devem ser consideradas de risco elevado[7].

As Conclusões, mais recentes, de 21 de outubro de 2020 reforçaram a importância de dar resposta a desafios como a opacidade, a complexidade, os preconceitos [ou enviesamentos], um certo grau de imprevisibilidade e comportamentos parcialmente autónomos de determinados sistemas de IA, a fim de garantir a compatibilidade destes sistemas com os direitos fundamentais e facilitar a aplicação das normas jurídicas[8].

O Parlamento Europeu também realizou um trabalho considerável no domínio da IA. Em outubro de 2020, adotou um conjunto de resoluções no domínio da IA, nomeadamente em matéria de ética[9], responsabilidade[10] e direitos de autor[11]. Em 2021, seguiram-se resoluções no domínio da IA em matéria penal[12] e nos domínios da educação, da cultura e do setor audiovisual[13]. A Resolução do Parlamento Europeu sobre o regime relativo aos aspetos éticos

---

3 Conselho Europeu, Reunião extraordinária do Conselho Europeu (1 e 2 de outubro de 2020) — Conclusões [EUCO 13/20, 2020, p. 6].

4 Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas [2020/2012(INL)].

5 Conselho Europeu, *Reunião do Conselho Europeu (19 de outubro de 2017) — Conclusões* [EUCO 14/17, 2017, p. 8].

6 Conselho da União Europeia, *Inteligência artificial: b) Conclusões sobre o plano coordenado para a inteligência artificial — Adoção* [6177/19, 2019].

7 Conselho Europeu, *Reunião extraordinária do Conselho Europeu (1 e 2 de outubro de 2020) — Conclusões* [EUCO 13/20, 2020].

8 Conselho da União Europeia, *Conclusões da Presidência — A Carta dos Direitos Fundamentais no contexto da inteligência artificial e da transformação digital* [11481/20, 2020].

9 Resolução do Parlamento Europeu, de 20 de outubro de 2020, sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas [2020/2012(INL)].

10 Resolução do Parlamento Europeu, de 20 de outubro de 2020, sobre o regime de responsabilidade civil aplicável à inteligência artificial [2020/2014(INL)].

11 Resolução do Parlamento Europeu, de 20 de outubro de 2020, sobre os direitos de propriedade intelectual para o desenvolvimento de tecnologias ligadas à inteligência artificial [2020/2015(INI)].

12 Projeto de relatório do Parlamento Europeu sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais [2020/2016(INI)].

13 Projeto de relatório do Parlamento Europeu sobre a inteligência artificial na educação, na cultura e no setor audiovisual [2020/2017(INI)]. A Comissão adotou, neste contexto, o «Plano de Ação para a

da inteligência artificial, da robótica e das tecnologias conexas recomenda especificamente à Comissão que proponha uma ação legislativa para tirar partido dos benefícios e das oportunidades da IA, mas também para garantir a proteção de princípios éticos. A resolução inclui uma parte da proposta legislativa de um regulamento relativo aos princípios éticos para o desenvolvimento, implantação e utilização da inteligência artificial, da robótica e das tecnologias conexas. Em conformidade com o compromisso político assumido pela presidente Ursula von der Leyen nas suas orientações políticas relativamente às resoluções adotadas pelo Parlamento Europeu nos termos do artigo 225.º do TFUE, a presente proposta tem em conta a resolução acima mencionada do Parlamento Europeu, no pleno respeito dos princípios da proporcionalidade, da subsidiariedade e da iniciativa Legislar Melhor.

Tendo em conta este contexto político, a Comissão apresenta uma proposta de quadro regulamentar em matéria de inteligência artificial com os seguintes **objetivos específicos**:

- garantir que os sistemas de IA colocados no mercado da União e utilizados sejam seguros e respeitem a legislação em vigor em matéria de direitos fundamentais e valores da União,
- garantir a segurança jurídica para facilitar os investimentos e a inovação no domínio da IA,
- melhorar a governação e a aplicação efetiva da legislação em vigor em matéria de direitos fundamentais e dos requisitos de segurança aplicáveis aos sistemas de IA,
- facilitar o desenvolvimento de um mercado único para as aplicações de IA legítimas, seguras e de confiança e evitar a fragmentação do mercado.

Para alcançar esses objetivos, a presente proposta apresenta uma abordagem regulamentar horizontal equilibrada e proporcionada ao domínio da inteligência artificial, que se limita aos requisitos mínimos necessários para dar resposta aos riscos e aos problemas associados à IA, sem restringir ou prejudicar indevidamente a evolução tecnológica ou aumentar desproporcionalmente o custo de colocação no mercado das soluções de IA. A proposta estabelece um quadro jurídico sólido e flexível. Por um lado, as suas escolhas regulamentares fundamentais, incluindo os requisitos baseados em princípios que os sistemas de IA devem respeitar, são abrangentes e estão preparadas para o futuro. Por outro lado, cria um sistema regulamentar proporcionado, centrado numa abordagem regulamentar baseada no risco bem definida que não cria restrições desnecessárias ao comércio e na qual a intervenção jurídica é adaptada às situações concretas em que existe um motivo de preocupação justificado ou em que tal preocupação pode ser razoavelmente antecipada num futuro próximo. Ao mesmo tempo, o quadro jurídico inclui mecanismos flexíveis que permitem a sua adaptação dinâmica à medida que a tecnologia evolui e surgem novas situações preocupantes.

A proposta estabelece regras harmonizadas para o desenvolvimento, a colocação no mercado e a utilização de sistemas de IA na União na sequência de uma abordagem proporcionada baseada no risco. Propõe-se uma definição inequívoca e preparada para o futuro de «inteligência artificial». Algumas práticas de IA particularmente prejudiciais são proibidas, uma vez que violam os valores da União, e são propostas restrições e salvaguardas específicas relativamente a determinadas utilizações de sistemas de identificação biométrica à distância para efeitos de manutenção da ordem pública. A proposta estabelece uma metodologia de análise de riscos sólida para definir sistemas de IA de «risco elevado» que criam riscos

---

Educação Digital 2021-2027 — Reconfigurar a educação e a formação para a era digital» [COM(2020) 624 final], que prevê o desenvolvimento de orientações éticas em matéria de inteligência artificial e utilização de dados no ensino.

significativos para a saúde e a segurança ou para os direitos fundamentais das pessoas. Esses sistemas de IA terão de cumprir um conjunto de requisitos obrigatórios horizontais para uma IA de confiança e seguir procedimentos de avaliação da conformidade antes de poderem ser colocados no mercado da União. Os fornecedores e os utilizadores desses sistemas também estão sujeitos a obrigações previsíveis, proporcionadas e claras para garantir a segurança e o respeito da legislação em vigor que protege os direitos fundamentais ao longo de todo o ciclo de vida dos sistemas de IA. No caso de alguns sistemas de IA específicos, apenas são propostas obrigações de transparência mínimas, em particular quando são utilizados sistemas de conversação automática ou «falsificações profundas».

As regras propostas serão executadas por intermédio de um sistema de governação a nível dos Estados-Membros, aproveitando estruturas já existentes, e de um mecanismo de cooperação a nível da União, ou seja, o novo Comité Europeu para a Inteligência Artificial. Também são propostas medidas adicionais para apoiar a inovação, em particular por via de ambientes de testagem da regulamentação da IA e de outras medidas que visam reduzir os encargos regulamentares e apoiar as pequenas e médias empresas (PME) e as empresas em fase de arranque.

1.2. Coerência com as disposições existentes da mesma política setorial

A natureza horizontal da proposta exige a plena coerência com a legislação da União em vigor aplicável aos setores em que os sistemas de IA de risco elevado já são utilizados ou serão provavelmente utilizados num futuro próximo.

É igualmente garantida coerência com a Carta dos Direitos Fundamentais da UE e a legislação derivada da União em vigor em matéria de proteção de dados, defesa dos consumidores, não discriminação e igualdade de género. A proposta não prejudica e completa o Regulamento Geral sobre a Proteção de Dados [Regulamento (UE) 2016/679] e a Diretiva sobre a Proteção de Dados na Aplicação da Lei [Diretiva (UE) 2016/680] com um conjunto de regras harmonizadas aplicáveis à conceção, ao desenvolvimento e à utilização de determinados sistemas de IA de risco elevado e restrições a determinadas utilizações de sistemas de identificação biométrica à distância. Além disso, a proposta completa o direito da União em vigor em matéria de não discriminação com requisitos específicos que visam minimizar o risco de discriminação algorítmica, em particular no que diz respeito à conceção e à qualidade dos conjuntos de dados utilizados no desenvolvimento de sistemas de IA, complementados com obrigações de testagem, gestão de riscos, documentação e supervisão humana ao longo do ciclo de vida dos sistemas de IA. A proposta não prejudica a aplicação do direito da concorrência da União.

No que diz respeito aos sistemas de IA de risco elevado que são componentes de segurança de produtos, a presente proposta será integrada na legislação de segurança setorial em vigor para assegurar a coerência, evitar as duplicações e minimizar os encargos adicionais. Em particular, no que diz respeito aos sistemas de IA de risco elevado relacionados com produtos abrangidos pela legislação do novo quadro legislativo (NQL) (por exemplo, máquinas, dispositivos médicos, brinquedos), os requisitos aplicáveis aos sistemas de IA estabelecidos na presente proposta serão verificados no âmbito dos procedimentos de avaliação da conformidade previstos na correspondente legislação do NQL. No que diz respeito à interligação dos requisitos, embora os riscos de segurança específicos dos sistemas de IA devam ser abrangidos pelos requisitos da presente proposta, a legislação do NQL visa assegurar a segurança global do produto final e, como tal, pode incluir requisitos específicos relativos à integração segura de um sistema de IA no produto final. A proposta de regulamento relativo às máquinas, que é adotada no mesmo dia que a presente proposta, reflete plenamente esta abordagem. A presente proposta não é diretamente aplicável aos

sistemas de IA de risco elevado relacionados com produtos abrangidos pela legislação da «antiga abordagem» (por exemplo, aviação, automóveis). Contudo, os requisitos essenciais *ex ante* aplicáveis aos sistemas de IA de risco elevado estabelecidos na presente proposta terão de ser tidos em conta aquando da adoção de atos de execução ou delegados ao abrigo dessa legislação.

No que diz respeito aos sistemas de IA fornecidos ou utilizados por instituições de crédito regulamentadas, as autoridades responsáveis pela supervisão da legislação da União em matéria de serviços financeiros devem ser designadas autoridades competentes para a supervisão dos requisitos estabelecidos na presente proposta, para assegurar uma execução coerente das obrigações previstas na presente proposta e da legislação da União em matéria de serviços financeiros nos casos em que os sistemas de IA sejam, até certo ponto, implicitamente regulamentados relativamente ao sistema de governação interno das instituições de crédito. A fim de aumentar a coerência, o procedimento de avaliação da conformidade e algumas das obrigações processuais dos fornecedores impostas nos termos da presente proposta são integradas nos procedimentos previstos na Diretiva 2013/36/UE relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial[14].

A presente proposta é coerente com o direito da União aplicável em matéria de serviços, incluindo os serviços intermediários regulamentados pela Diretiva 2000/31/CE (Diretiva sobre o comércio eletrónico)[15] e pela proposta de Regulamento Serviços Digitais (RSD)[16] recentemente apresentada pela Comissão.

Relativamente aos sistemas de IA que são componentes de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça geridos pela Agência da União Europeia para a Gestão Operacional de Sistemas Informáticos de Grande Escala no Espaço de Liberdade, Segurança e Justiça (eu-LISA), a proposta não se aplica aos sistemas de IA que sejam colocados no mercado ou colocados em serviço antes de ter decorrido um ano desde a data de aplicação do presente regulamento, salvo se a substituição ou alteração desses atos jurídicos implicar uma alteração significativa da conceção ou da finalidade prevista do sistema ou dos sistemas de IA em causa.

1.3. Coerência com as outras políticas da União

A proposta faz parte de um pacote abrangente de medidas que visa resolver os problemas decorrentes do desenvolvimento e da utilização da IA, examinados no Livro Branco sobre a inteligência artificial. Como tal, é garantida a coerência e a complementaridade com outras iniciativas em curso ou planeadas da Comissão que também visam responder a esses problemas, incluindo a revisão da legislação setorial em matéria de produtos (por exemplo, a Diretiva Máquinas e a Diretiva Segurança Geral dos Produtos) e as iniciativas que abordam questões de responsabilidade associadas às novas tecnologias, incluindo os sistemas de IA. Essas iniciativas desenvolvem e completam a presente proposta, a fim de conferir certeza

---

[14] Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176 de 27.6.2013, p. 338).

[15] Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade de informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO L 178 de 17.7.2000, p. 1).

[16] Ver a proposta de regulamento do Parlamento Europeu e do Conselho relativo a um mercado único de serviços digitais (Regulamento Serviços Digitais) e que altera a Diretiva 2000/31/CE [COM(2020) 825 final].

jurídica e promover o desenvolvimento de um ecossistema de confiança em matéria de IA na Europa.

A proposta é ainda coerente com a estratégia digital global da Comissão no contributo que presta para promover o conceito de «tecnologia ao serviço das pessoas», um dos três principais pilares da orientação política e dos objetivos anunciados na Comunicação «Construir o futuro digital da Europa»[17]. Estabelece um quadro coerente, eficaz e proporcionado para assegurar que a IA seja desenvolvida de modo que respeite os direitos das pessoas e conquiste a sua confiança, preparando a Europa para a era digital e transformando os próximos dez anos na **Década Digital**[18].

Além disso, a promoção da inovação baseada na IA está estreitamente associada ao **Regulamento Governação de Dados**[19]**,** à **Diretiva Dados Abertos**[20] e a outras iniciativas estabelecidas na **Estratégia europeia para os dados**[21], que criarão mecanismos e serviços de confiança para a reutilização, a partilha e o agrupamento de dados, elementos essenciais para o desenvolvimento de modelos de IA baseados em dados de elevada qualidade.

A proposta também reforça de forma significativa o papel da União na definição de regras e padrões mundiais e promove uma IA de confiança que é coerente com os valores e os interesses da União. Constitui uma base importante para a União continuar a colaborar com os parceiros externos, incluindo os países terceiros, e em fóruns internacionais em questões relacionadas com a IA.

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

2.1. Base jurídica

A base jurídica da proposta é, em primeiro lugar, o artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), que prevê a adoção de medidas para assegurar o estabelecimento e o funcionamento do mercado interno.

A presente proposta constitui uma parte fundamental da estratégia para o mercado único digital da UE. O principal objetivo da presente proposta é assegurar o correto funcionamento do mercado interno mediante a criação de regras harmonizadas para o desenvolvimento, a colocação no mercado da União e a utilização de produtos e serviços que integram tecnologias de IA ou que são fornecidos como sistemas de IA autónomos. Alguns Estados-Membros já estão a ponderar regras nacionais para assegurar que a inteligência artificial seja segura e seja desenvolvida e utilizada em conformidade com as obrigações de proteção dos direitos fundamentais. Esta situação é suscetível de gerar dois grandes problemas: i) uma fragmentação do mercado interno no que diz respeito aos elementos essenciais relativos aos requisitos aplicáveis aos produtos e serviços baseados na inteligência artificial, à respetiva comercialização, utilização, responsabilidade e supervisão pelas autoridades públicas; ii) a redução substancial da segurança jurídica para os fornecedores e os utilizadores de sistemas de IA no que se refere à forma como as regras em vigor e as novas

[17] Comunicação da Comissão: Construir o futuro digital da Europa [COM(2020) 67 final].

[18] Orientações para a Digitalização até 2030: a via europeia para a Década Digital.

[19] Proposta de regulamento relativo à governação de dados (Regulamento Governação de Dados) [COM(2020) 767].

[20] Diretiva (UE) 2019/1024 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativa aos dados abertos e à reutilização de informações do setor público [PE/28/2019/REV/1] (JO L 172 de 26.6.2019, p. 56).

[21] Comunicação da Comissão: Uma estratégia europeia para os dados [COM(2020) 66 final].

regras serão aplicadas a esses sistemas na União. Dada a vasta circulação de produtos e serviços entre fronteiras, a melhor solução para estes dois problemas passa por recorrer à legislação de harmonização da UE.

Efetivamente, a proposta define requisitos obrigatórios comuns aplicáveis à conceção e ao desenvolvimento de determinados sistemas de IA antes de estes serem colocados no mercado, os quais serão subsequentemente operacionalizados por via de normas técnicas harmonizadas. A proposta também aborda a situação após a colocação no mercado de sistemas de IA, por meio da harmonização do método de realização dos controlos *ex post*.

Além disso, tendo em conta que a presente proposta contém determinadas regras específicas aplicáveis à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, nomeadamente restrições à utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, é adequado basear o presente regulamento no artigo 16.º do TFUE, no respeitante a essas regras específicas.

2.2. Subsidiariedade (no caso de competência não exclusiva)

A natureza da inteligência artificial, que muitas vezes depende de conjuntos de dados amplos e variados e pode ser integrada em qualquer produto ou serviço que circule livremente no mercado interno, implica que os objetivos da presente proposta não podem ser alcançados com eficácia apenas pela ação dos Estados-Membros. Além disso, a emergência de um mosaico de regras nacionais potencialmente divergentes prejudicaria a circulação homogénea de produtos e serviços associados a sistemas de IA em toda a UE e seria ineficaz para garantir a segurança e a proteção dos direitos fundamentais e dos valores da União nos diferentes Estados-Membros. A adoção de abordagens nacionais para a resolução dos problemas apenas criaria mais insegurança jurídica e obstáculos e abrandaria a aceitação da inteligência artificial pelo mercado.

Os objetivos da presente proposta podem ser mais bem alcançados a nível da União, evitando assim uma maior fragmentação do mercado único em quadros nacionais potencialmente contraditórios que impeçam a livre circulação dos produtos e dos serviços que integram inteligência artificial. Um quadro regulamentar europeu sólido para uma inteligência artificial de confiança também assegurará condições de concorrência equitativas e protegerá todos os cidadãos, reforçando ao mesmo tempo a competitividade e a base industrial da Europa neste domínio. Só uma ação comum a nível da União pode proteger também a soberania digital da União e tirar partido dos seus instrumentos e poderes regulamentares para moldar as regras e as normas mundiais.

2.3. Proporcionalidade

A proposta tem por base os atuais quadros jurídicos e é proporcionada e necessária para alcançar os objetivos a que se propõe, uma vez que segue uma abordagem baseada no risco e impõe encargos regulamentares apenas quando é provável que um sistema de IA represente riscos elevados para os direitos fundamentais e a segurança. Por outro lado, no caso dos sistemas de IA que não são de risco elevado, apenas são impostas obrigações de transparência bastante limitadas, por exemplo, no que diz respeito à prestação de informações para sinalizar a utilização de um sistema de IA quando este interage com seres humanos. No caso dos sistemas de IA de risco elevado, os requisitos relativos à elevada qualidade dos dados, à documentação e à rastreabilidade, à transparência, à supervisão humana, à exatidão e à solidez são estritamente necessários para atenuar os riscos para os direitos fundamentais e a segurança colocados pela inteligência artificial e que não abrangidos por outros quadros jurídicos existentes. As normas harmonizadas e as orientações de apoio, bem como as ferramentas de

conformidade, auxiliarão os fornecedores e os utilizadores no cumprimento dos requisitos estabelecidos pela proposta e na minimização dos seus custos. Os custos incorridos pelos operadores são proporcionados aos objetivos alcançados e aos benefícios económicos e reputacionais que os operadores podem esperar desta proposta.

2.4. Escolha do instrumento

A escolha de um regulamento como instrumento jurídico justifica-se pela necessidade de aplicar uniformemente as novas regras, como a definição de inteligência artificial, a proibição de determinadas práticas prejudiciais possibilitadas pela IA e a classificação de determinados sistemas de IA. A aplicabilidade direta de um regulamento, em conformidade com o artigo 288.º do TFUE, reduzirá a fragmentação jurídica e facilitará o desenvolvimento de um mercado único para sistemas de IA legítimos, seguros e de confiança. Para isso, introduzirá um conjunto harmonizado de requisitos básicos no que diz respeito aos sistemas de IA classificados como de risco elevado, bem como obrigações aplicáveis aos fornecedores e aos utilizadores desses sistemas, melhorará a proteção dos direitos fundamentais e proporcionará segurança jurídica para os operadores e os consumidores.

Ao mesmo tempo, as disposições do regulamento não são excessivamente prescritivas e deixam margem a diferentes níveis de ação por parte dos Estados-Membros em termos de elementos que não comprometem os objetivos da iniciativa, em particular a organização interna do sistema de fiscalização do mercado e a adoção de medidas que visam promover a inovação.

3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

3.1. Consulta das partes interessadas

A presente proposta é resultado de uma consulta extensiva das principais partes interessadas, na qual a Comissão aplicou os princípios gerais e as normas mínimas de consulta das partes interessadas.

Em 19 de fevereiro de 2020, foi lançada, juntamente com a publicação do Livro Branco sobre a inteligência, artificial uma **consulta pública em linha**, que decorreu até 14 de junho de 2020. O objetivo dessa consulta era recolher pontos de vista e opiniões sobre o Livro Branco. A consulta visou todas as partes interessadas dos setores público e privado, incluindo administrações públicas, autoridades locais, organizações comerciais e não comerciais, parceiros sociais, peritos, académicos e cidadãos. Uma vez analisadas as respostas recebidas, a Comissão publicou uma síntese dos resultados e as respostas individuais no seu sítio Web[22].

No total, foram recebidos 1 215 contributos, dos quais 352 de empresas ou organizações/associações comerciais, 406 de cidadãos (92 % eram cidadãos da UE), 152 em nome de instituições académicas/de investigação e 73 de autoridades públicas. As opiniões da sociedade civil foram representadas por 160 respondentes (9 dos quais eram organizações de consumidores, 129 eram organizações não governamentais e 22 eram sindicatos), sendo que 72 respondentes contribuíram identificando-se como «Outros». Das 352 empresas e representantes da indústria, 222 eram empresas e representantes comerciais, sendo que 41,5 % eram micro, pequenas e médias empresas. As restantes eram associação empresariais. De um modo geral, 84 % das respostas das empresas e da indústria eram provenientes da UE-27. Dependendo da pergunta, entre 81 e 598 dos respondentes utilizaram a opção de texto livre

[22] Consultar todos os resultados da consulta aqui.

para inserir observações. Foram apresentadas mais de 450 posições escritas através do portal EU Survey, quer como complemento das respostas aos inquéritos (mais de 400), quer como contributos autónomos (mais de 50).

De uma forma geral, existe consenso entre as partes interessadas quanto à necessidade de agir. Uma grande maioria das partes interessadas concorda que existem lacunas legislativas ou que é necessária nova legislação. Contudo, várias partes interessadas alertaram a Comissão para a necessidade de evitar duplicação, obrigações contraditórias e excesso de regulamentação. Houve vários comentários a sublinhar a importância de um quadro regulamentar tecnologicamente neutro e proporcionado.

De uma forma geral, as partes interessadas solicitaram uma definição estreita, clara e precisa de «inteligência artificial». As partes interessadas também sublinharam que, além da clarificação do termo «inteligência artificial», é importante definir os termos «risco», «risco elevado», «risco baixo», «identificação biométrica à distância» e «prejuízo/dano».

A maioria dos respondentes manifestou-se explicitamente a favor da abordagem baseada no risco. A utilização de um quadro baseado no risco foi considerada uma opção melhor do que aplicar uma regulamentação generalizada a todos os sistemas de IA. Os tipos de riscos e ameaças devem ser baseados numa abordagem setorial e casuística. Os riscos também devem ser calculados tendo em conta o impacto nos direitos e na segurança.

Os ambientes de testagem da regulamentação podem ser bastante úteis para a promoção da IA e são acolhidos com agrado por determinadas partes interessadas, especialmente as associações empresariais.

Entre as partes interessadas que manifestaram a sua opinião sobre os modelos de execução, mais de 50 %, sobretudo entre as associações comerciais, mostraram-se a favor da combinação de uma autoavaliação de riscos *ex ante* e de uma execução *ex post* aplicável aos sistemas de IA de risco elevado.

3.2. Obtenção e utilização de competências especializadas

A proposta tem como base dois anos de análise e estreita cooperação das partes interessadas, incluindo académicos, empresas, parceiros sociais, organizações não governamentais, Estados-Membros e cidadãos. O trabalho preparatório foi iniciado em 2018 com a criação de um **grupo de peritos de alto nível (GPAN) sobre a IA** com uma composição inclusiva e ampla de 52 peritos bem conhecidos incumbidos de prestar aconselhamento à Comissão sobre a aplicação da estratégia da Comissão para a inteligência artificial. Em abril de 2019, a Comissão manifestou o seu apoio[23] aos requisitos essenciais estabelecidos nas «Orientações éticas para uma IA de confiança» do GPAN[24], que tinham sido revistos para ter em conta mais de 500 observações das partes interessadas. Os requisitos essenciais refletem uma abordagem generalizada e comum segundo a qual o desenvolvimento e a utilização da IA se devem pautar por determinados princípios essenciais orientados por valores, conforme comprovado por um conjunto de códigos e princípios éticos desenvolvidos por várias organizações privadas e públicas de dentro e fora da Europa. A lista de avaliação para uma inteligência artificial de confiança[25] tornou esses requisitos operacionais num processo piloto que incluiu mais de 350 organizações.

---

[23] Comissão Europeia: *Aumentar a confiança numa inteligência artificial centrada no ser humano* [COM(2019) 168].

[24] GPAN, *Orientações éticas para uma IA de confiança*, 2019.

[25] GPAN, *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*, 2020 [não traduzida para português].

Além disso, foi criada a **Aliança da IA**[26], uma plataforma onde aproximadamente 4 000 partes interessadas podem debater as implicações tecnológicas e sociais da IA, culminando numa assembleia de IA anual.

O **Livro Branco** sobre a inteligência artificial desenvolveu esta abordagem inclusiva, incitando as observações de mais de 1 250 partes interessadas, incluindo mais de 450 posições escritas. Consequentemente, a Comissão publicou uma avaliação de impacto inicial que, por sua vez, deu origem a mais de 130 observações[27]. Também foram organizadas **outras sessões de trabalho e eventos para as partes interessadas** cujos resultados apoiam a análise da avaliação de impacto e as escolhas políticas efetuadas na presente proposta[28]. Foi ainda encomendado um **estudo externo** para contribuir para a avaliação de impacto.

3.3. Avaliação de impacto

Em consonância com a sua política «Legislar melhor», a Comissão realizou uma avaliação de impacto para a presente proposta, que foi analisada pelo Comité de Controlo da Regulamentação da Comissão. Foi realizada uma reunião com o Comité de Controlo da Regulamentação, em 16 de dezembro de 2020, à qual se seguiu um parecer negativo. Após uma revisão substancial da avaliação de impacto para ter em conta as observações e uma nova apresentação da avaliação de impacto, o Comité de Controlo da Regulamentação emitiu um parecer positivo em 21 de março de 2021. O anexo 1 da avaliação de impacto inclui os pareceres do Comité de Controlo da Regulamentação, as recomendações deste e uma explicação sobre como foram tidas em conta.

A Comissão estudou diversas opções políticas para alcançar o objetivo geral da proposta, que consiste em **assegurar o correto funcionamento do mercado único**, criando condições para o desenvolvimento e a utilização de uma inteligência artificial de confiança na União.

Foram avaliadas quatro opções políticas com diferentes graus de intervenção regulamentar:

- **Opção 1**: um instrumento legislativo da UE que criasse um regime de rotulagem voluntária;
- **Opção 2**: uma abordagem *ad hoc* a nível setorial;
- **Opção 3**: um instrumento legislativo horizontal da UE que seguisse uma abordagem baseada no risco proporcionada;
- **Opção 3+**: um instrumento legislativo horizontal da UE que seguisse uma abordagem baseada no risco proporcionada, completada por códigos de conduta para os sistemas de IA que não são de risco elevado;
- **Opção 4**: um instrumento legislativo horizontal da UE que estabelecesse requisitos obrigatórios para todos os sistemas de IA, independentemente do risco que representam.

De acordo com a metodologia estabelecida da Comissão, cada opção política foi avaliada tendo em conta os impactos económicos e sociais, com particular ênfase nos impactos nos

---

[26] A Aliança da IA é um fórum multilateral lançado em junho de 2018, https://ec.europa.eu/digital-single-market/en/european-ai-alliance.

[27] Comissão Europeia: *Inception Impact Assessment For a Proposal for a legal act of the European Parliament and the Council laying down requirements for Artificial Intelligence* [não traduzida para português].

[28] Para obter mais informações sobre todas as consultas realizadas, consultar o anexo 2 da avaliação de impacto.

direitos fundamentais. É dada preferência à opção 3+, um quadro regulamentar apenas aplicável aos sistemas de IA de risco elevado, com a possibilidade de todos os fornecedores de sistemas de IA que não são de risco elevado seguirem um código de conduta. Os requisitos dirão respeito aos dados, à documentação e à rastreabilidade, à prestação de informações e à transparência, à supervisão humana, à exatidão e à solidez e seriam obrigatórios para os sistemas de IA de risco elevado. As empresas que introduzam códigos de conduta para outros sistemas de IA fá-lo-ão de modo voluntário.

A opção preferida foi considerada adequada para alcançar mais eficazmente os objetivos da presente proposta. Ao exigir um conjunto de ações, restrito mas eficaz, por parte dos fornecedores e utilizadores de inteligência artificial, a opção preferida limita os riscos de violação dos direitos fundamentais e da segurança dos cidadãos e promove a supervisão e a execução eficazes, ao associar os requisitos apenas aos sistemas em que existe um risco elevado de ocorrência dessas violações. Consequentemente, essa opção mantém os custos de conformidade num valor mínimo, evitando assim um abrandamento desnecessário da adoção da tecnologia devido a preços e custos de conformidade mais elevados. De modo a excluir as possíveis desvantagens para as PME, esta opção inclui inúmeras disposições para apoiar a conformidade e reduzir os respetivos custos, incluindo a criação de ambientes de testagem da regulamentação e a obrigação de ter em conta os interesses das PME aquando da fixação de taxas a pagar pela avaliação da conformidade.

A opção preferida aumentará a confiança dos cidadãos na inteligência artificial, as empresas beneficiarão de maior segurança jurídica e os Estados-Membros não terão qualquer motivo para tomarem uma ação unilateral que possa fragmentar o mercado único. Em resultado de uma maior procura motivada por uma maior confiança, do aumento da disponibilidade das ofertas devido à segurança jurídica e da ausência de obstáculos ao movimento transfronteiras de sistemas de IA, o mercado único da inteligência artificial irá provavelmente florescer. A União Europeia continuará a desenvolver um ecossistema de inteligência artificial em rápido crescimento, com serviços e produtos inovadores que integram a tecnologia de IA ou sistemas de IA autónomos, o que conduz a um aumento da autonomia digital.

As empresas ou autoridades públicas que desenvolvam ou utilizem aplicações de IA que representam um risco elevado para a segurança ou para os direitos fundamentais dos cidadãos terão de cumprir requisitos e obrigações específicos. O cumprimento destes requisitos implicaria, para o fornecimento de um sistema de IA de risco elevado de gama média com um preço aproximado de 170 000 EUR, custos de aproximadamente 6 000 EUR a 7 000 EUR até 2025. No caso dos utilizadores de inteligência artificial, haveria ainda o custo anual pelo tempo despendido a garantir a supervisão humana, sempre que adequado, dependendo do caso de utilização. Esses custos foram estimados em aproximadamente 5 000 EUR a 8 000 EUR por ano. Os custos de verificação podem corresponder a mais 3 000 EUR a 7 500 EUR no caso dos fornecedores de IA de risco elevado. As empresas ou autoridades públicas que desenvolvam ou utilizem aplicações de IA que não sejam consideradas de risco elevado apenas terão obrigações mínimas de informação. Contudo, estas empresas ou autoridades podem escolher juntar-se a outros e, em conjunto, adotar um código de conduta para seguir requisitos adequados e garantir que os seus sistemas de IA sejam de confiança. Nesse caso, os custos seriam, no máximo, tão elevados quanto os custos impostos aos sistemas de IA de risco elevado, mas provavelmente inferiores.

Os impactos das opções políticas nas diferentes categorias de partes interessadas (operadores económicos/empresas; organismos de avaliação da conformidade, organismos de normalização e outros organismos públicos; indivíduos/cidadãos; investigadores) são descritos pormenorizadamente no anexo 3 da avaliação de impacto que fundamenta a presente proposta.

3.4. Adequação e simplificação da regulamentação

A presente proposta estabelece obrigações que serão aplicáveis aos fornecedores e aos utilizadores de sistemas de IA de risco elevado. No caso dos fornecedores que desenvolvem e colocam esses sistemas no mercado da União, a proposta criará segurança jurídica e assegurará a ausência de obstáculos ao fornecimento transfronteiras de produtos e serviços baseados na IA. No caso das empresas que utilizam a IA, promoverá a confiança entre os seus clientes. No caso das administrações públicas nacionais, esta opção promoverá a confiança pública na utilização da IA e reforçará os mecanismos de execução (mediante a introdução de um mecanismo de coordenação europeu, do fornecimento das capacidades adequadas e da facilitação das auditorias dos sistemas de IA com a aplicação de novos requisitos relacionados com a documentação, a rastreabilidade e a transparência). Além disso, o quadro estipulará medidas específicas para apoiar a inovação, incluindo ambientes de testagem da regulamentação e medidas específicas para ajudar os utilizadores e os fornecedores de pequena dimensão de sistemas de IA de risco elevado a cumprirem as novas regras.

A proposta também visa especificamente o reforço da competitividade e da base industrial da Europa no domínio da inteligência artificial. É assegurada uma coerência completa com a legislação setorial da União aplicável aos sistemas de IA (por exemplo, em matéria de produtos e serviços) que trará maior clareza e simplificará a execução das novas regras.

3.5. Direitos fundamentais

Dadas as suas características específicas (por exemplo, a opacidade, a complexidade, a dependência dos dados, o comportamento autónomo), a utilização da inteligência artificial pode afetar negativamente um conjunto de direitos fundamentais consagrados na Carta dos Direitos Fundamentais da UE (a seguir designada por «Carta»). A presente proposta procura assegurar um nível elevado de proteção desses direitos fundamentais e visa fazer face aos vários riscos mediante uma abordagem baseada no risco claramente definida. Graças a um conjunto de requisitos relativos a uma IA de confiança e obrigações proporcionadas para todos os participantes da cadeia de valor, a proposta melhorará e promoverá a proteção dos direitos consagrados na Carta: o direito à dignidade do ser humano (artigo 1.º), o respeito pela vida privada e familiar e a proteção de dados pessoais (artigos 7.º e 8.º), a não discriminação (artigo 21.º) e a igualdade entre homens e mulheres (artigo 23.º). A proposta pretende evitar um efeito inibidor nos direitos à liberdade de expressão (artigo 11.º) e à liberdade de reunião (artigo 12.º), garantir a proteção do direito à ação e a um tribunal imparcial e dos direitos de presunção de inocência e de defesa (artigos 47.º e 48.º), bem como do direito a uma boa administração. Além disso, conforme aplicável em determinados domínios, a proposta afetará de forma positiva os direitos de um conjunto de grupos especiais, como os direitos dos trabalhadores a condições de trabalho justas e equitativas (artigo 31.º), o direito a um elevado nível de defesa dos consumidores (artigo 28.º), os direitos das crianças (artigo 24.º) e o direito de integração das pessoas com deficiência (artigo 26.º). O direito a um elevado nível de proteção do ambiente e melhoria da sua qualidade (artigo 37.º) também é relevante, incluindo em relação à saúde e à segurança dos cidadãos. As obrigações relativas à testagem *ex ante*, à gestão de riscos e à supervisão humana também facilitarão o respeito de outros direitos fundamentais, graças à minimização do risco de decisões assistidas por IA erradas ou enviesadas em domínios críticos como a educação e a formação, o emprego, serviços essenciais, a manutenção da ordem pública e o sistema judicial. Caso continuem a ocorrer violações dos direitos fundamentais, as pessoas afetadas têm acesso a vias eficazes de recurso graças à garantia da transparência e da rastreabilidade dos sistemas de IA, associadas a fortes controlos *ex post*.

A presente proposta impõe algumas restrições à liberdade de empresa (artigo 16.º) e à liberdade das artes e das ciências (artigo 13.º), a fim de assegurar o cumprimento de razões imperativas de reconhecido interesse público, como a saúde, a segurança, a defesa dos consumidores e a proteção de outros direitos fundamentais («inovação responsável») em caso de desenvolvimento e utilização de tecnologia de IA de risco elevado. Essas restrições são proporcionadas e limitadas ao mínimo necessário para prevenir e atenuar riscos de segurança graves e possíveis violações dos direitos fundamentais.

O aumento das obrigações de transparência também não afetará desproporcionadamente o direito à proteção da propriedade intelectual (artigo 17.º, n.º 2), uma vez que estarão limitadas às informações mínimas necessárias para as pessoas singulares exercerem o seu direito à ação e à transparência necessária perante as autoridades de supervisão e execução, em conformidade com os mandatos destas. Qualquer divulgação de informações será realizada de acordo com a legislação aplicável, incluindo a Diretiva (UE) 2016/943 relativa à proteção de *know-how* e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais. Quando precisam de obter acesso a informações confidenciais ou a código-fonte para analisarem o cumprimento das obrigações substanciais, as autoridades públicas e os organismos notificados ficam sujeitos a obrigações de confidencialidade vinculativas.

4. INCIDÊNCIA ORÇAMENTAL

Os Estados-Membros serão obrigados a designar autoridades de controlo responsáveis pela aplicação dos requisitos legislativos. A sua função de controlo pode ter como base mecanismos existentes, por exemplo, relativos aos organismos de avaliação da conformidade ou à fiscalização do mercado, mas exigirá conhecimentos tecnológicos e recursos humanos e financeiros suficientes. Em função da estrutura preexistente em cada Estado-Membro, este valor pode variar entre 1 e 25 equivalentes a tempo completo por Estado-Membro.

É disponibilizada uma panorâmica pormenorizada dos custos na «ficha financeira» anexa à presente proposta.

5. OUTROS ELEMENTOS

5.1. Planos de execução e acompanhamento, avaliação e prestação de informações

A criação de um mecanismo de acompanhamento e avaliação sólido é crucial para garantir que a proposta seja eficaz para alcançar os seus objetivos específicos. A Comissão ficará responsável por acompanhar os efeitos da proposta e criará um sistema para registar aplicações de IA de risco elevado autónomas numa base de dados pública à escala europeia. Este registo também permitirá que as autoridades competentes, os utilizadores e outras pessoas interessadas verifiquem se o sistema de IA de risco elevado cumpre os requisitos estabelecidos na proposta e exerçam uma maior supervisão dos sistemas de IA que representam riscos elevados para os direitos fundamentais. Para alimentar esta base de dados, os fornecedores de IA serão obrigados a prestar informações importantes sobre os seus sistemas e a apresentar a avaliação da conformidade desses sistemas.

Além disso, os fornecedores de IA serão obrigados a informar as autoridades nacionais competentes sobre incidentes graves ou anomalias que constituam infrações às obrigações em matéria de direitos fundamentais assim que tomarem conhecimento das mesmas, bem como sobre eventuais recolhas ou retiradas de sistemas de IA do mercado. As autoridades nacionais competentes investigarão, subsequentemente, os incidentes/anomalias, recolherão todas as informações necessárias e transmitirão regularmente essas informações à Comissão, incluindo

metadados adequados. A Comissão completará estas informações sobre os incidentes por meio de uma análise abrangente do mercado global da inteligência artificial.

A Comissão publicará um relatório de avaliação e reexame do quadro para a inteligência artificial proposto no prazo de cinco anos a contar da data da sua aplicação.

5.2. Explicação pormenorizada das disposições específicas da proposta

5.2.1. ÂMBITO E DEFINIÇÕES (TÍTULO I)

O **título I** define o objeto do regulamento e o âmbito das novas regras que abrangem a colocação no mercado, a colocação em serviço e a utilização de sistemas de IA. Também estabelece as definições utilizadas no instrumento. A definição de «sistema de IA» constante do quadro jurídico pretende ser o mais tecnologicamente neutra e preparada para o futuro possível, tendo em conta a rápida evolução tecnológica e de mercado no domínio da inteligência artificial. De modo a garantir a segurança jurídica necessária, o título I é completado pelo anexo I, que inclui uma lista pormenorizada de abordagens e técnicas de desenvolvimento de inteligência artificial, que a Comissão adaptará em conformidade com as novas evoluções tecnológicas. São também claramente definidos os participantes essenciais da cadeia de valor no domínio da IA, como os fornecedores e os utilizadores de sistemas de IA, abrangendo os operadores públicos e privados, de modo que assegure condições de concorrência equitativas.

5.2.2. PRÁTICAS DE INTELIGÊNCIA ARTIFICIAL PROIBIDAS (TÍTULO II)

O **título II** estabelece uma lista de práticas de IA proibidas. O regulamento segue uma abordagem baseada no risco e diferencia entre as utilizações de IA que criam: i) um risco inaceitável, ii) um risco elevado, iii) um risco baixo ou mínimo. A lista de práticas proibidas do título II inclui todos os sistemas de IA cuja utilização seja considerada inaceitável por violar os valores da União, por exemplo, por violar os direitos fundamentais. As proibições abrangem práticas com potencial significativo para manipular as pessoas por meio de técnicas subliminares que lhes passam despercebidas ou explorar as vulnerabilidades de grupos específicos, como as crianças ou as pessoas com deficiência, para distorcer substancialmente o seu comportamento de uma forma que seja suscetível de causar danos psicológicos ou físicos a essa ou a outra pessoa. Outras práticas manipuladoras ou exploratórias que são possibilitadas pelos sistemas de IA e que afetam os adultos podem ser abrangidas pela legislação em matéria de proteção de dados, de defesa dos consumidores e de serviços digitais, que garante que as pessoas singulares sejam devidamente informadas e tenham a liberdade de decidir não se sujeitar a uma definição de perfis ou a outras práticas que possam afetar o seu comportamento. A proposta também proíbe a classificação social assente na IA para uso geral por parte das autoridades públicas. Por último, é igualmente proibida a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, a não ser que se apliquem determinadas exceções limitadas.

5.2.3. SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO (TÍTULO III)

O **título III** inclui regras específicas relativas aos sistemas de IA que criam um risco elevado para a saúde e a segurança ou para os direitos fundamentais de pessoas singulares. Em conformidade com uma abordagem baseada no risco, esses sistemas de IA de risco elevado são autorizados no mercado europeu, mas estão sujeitos ao cumprimento de determinados requisitos obrigatórios e a uma avaliação da conformidade *ex ante*. A classificação de um sistema de IA como de risco elevado tem como base a finalidade prevista desse sistema, em conformidade com a atual legislação relativa à segurança dos produtos. Como tal, classificar

um sistema como de risco elevado não depende só da função do sistema de IA, mas também da finalidade específica e das modalidades para as quais aquele sistema é utilizado.

O título III, capítulo 1, estabelece as regras de classificação e identifica duas categorias principais de sistemas de IA de risco elevado:

- sistemas de IA concebidos para serem utilizados como componentes de segurança de produtos que estão sujeitos a uma avaliação da conformidade *ex ante* por terceiros,
- outros sistemas de IA autónomos com implicações em matéria de direitos fundamentais que são explicitamente mencionados no anexo III.

A lista de sistemas de IA de risco elevado constante do anexo III inclui um número limitado de sistemas de IA cujos riscos já se materializaram ou são suscetíveis de se materializar num futuro próximo. A fim de garantir que o regulamento possa ser ajustado a novas utilizações e aplicações de IA, a Comissão pode alargar a lista de sistemas de IA de risco elevado utilizados em determinados domínios predefinidos, mediante a aplicação de um conjunto de critérios e de uma metodologia de avaliação de riscos.

O capítulo 2 estabelece os requisitos legais aplicáveis aos sistemas de IA de risco elevado relativamente aos dados e à governação de dados, à documentação e à manutenção de registos, à transparência e à prestação de informações aos utilizadores, à supervisão humana, à solidez, à exatidão e à segurança. Os requisitos mínimos propostos já são habituais para muitos operadores diligentes e resultam de um trabalho preparatório de dois anos, decorrente das Orientações Éticas do GPAN[29], aplicado numa fase-piloto por mais de 350 organizações[30]. Também são amplamente coerentes com outras recomendações e princípios internacionais, o que assegura que o quadro para inteligência artificial proposto seja compatível com os adotados pelos parceiros comerciais internacionais da UE. As soluções técnicas específicas para garantir o cumprimento desses requisitos podem, mediante o critério do fornecedor do sistema de IA, derivar de normas ou de outras especificações técnicas ou ser desenvolvidas de acordo com conhecimentos gerais de engenharia ou científicos. Esta flexibilidade é particularmente importante, porque permite que os fornecedores de sistemas de IA escolham o método de cumprimento dos requisitos, tendo em conta os progressos científicos e tecnológicos de ponta neste domínio.

O capítulo 3 indica um conjunto evidente de obrigações horizontais impostas aos fornecedores de sistemas de IA de risco elevado. Também são impostas obrigações proporcionadas aos utilizadores e a outros participantes de toda a cadeia de valor da IA (por exemplo, importadores, distribuidores, mandatários).

O capítulo 4 estabelece o quadro aplicável aos organismos notificados que participam como terceiros independentes nos procedimentos de avaliação da conformidade, ao passo que o capítulo 5 explica pormenorizadamente os procedimentos de avaliação da conformidade que devem ser seguidos para cada tipo de sistema de IA de risco elevado. A abordagem da avaliação da conformidade visa minimizar os encargos impostos aos operadores económicos e aos organismos notificados, cujas capacidades devem ser progressivamente reforçadas ao longo do tempo. Os sistemas de IA concebidos para serem utilizados como componentes de segurança de produtos que são regulamentados por atos do novo quadro legislativo (por

[29] Grupo de Peritos de Alto Nível em Inteligência Artificial, *Orientações éticas para uma IA de confiança*, 2019.

[30] Também foram apoiados na Comunicação da Comissão «Aumentar a confiança numa inteligência artificial centrada no ser humano», de 2019.

exemplo, máquinas, brinquedos, dispositivos médicos, etc.) serão sujeitos aos mesmos mecanismos de conformidade e execução *ex ante* e *ex post* aplicáveis aos produtos dos quais são um componente. A principal diferença é que os mecanismos de *ex ante* e *ex post* assegurarão o cumprimento não só dos requisitos estabelecidos pela legislação setorial, mas também dos requisitos estabelecidos pelo presente regulamento.

No que diz respeito aos sistemas de IA de risco elevado autónomos que são mencionados no anexo III, será criado um novo sistema de conformidade e execução. É seguido o modelo do novo quadro legislativo, em que a avaliação é efetuada por meio de controlos internos realizados pelos fornecedores, à exceção dos sistemas de identificação biométrica à distância, que serão sujeitos a uma avaliação da conformidade por terceiros. Uma avaliação da conformidade *ex ante* abrangente por meio de controlos internos, aliada a uma forte execução *ex post*, poderá constituir uma solução eficaz e razoável para esses sistemas, dada a fase inicial da intervenção regulamentar e o facto de o setor da inteligência artificial ser bastante inovador e de só agora estarem a ser reunidos conhecimentos especializados para as auditorias. Uma avaliação dos sistemas de IA de risco elevado autónomos por meio de controlos internos exigirá o cumprimento *ex ante* completo, eficaz e devidamente documentado de todos os requisitos do regulamento e a conformidade com sistemas sólidos de gestão de riscos e da qualidade e de acompanhamento pós-comercialização. Depois de ter efetuado a avaliação da conformidade necessária, o fornecedor deve registar esses sistemas de IA de risco elevado autónomos numa base de dados da UE que será gerida pela Comissão, a fim de aumentar a transparência e a supervisão públicas e de reforçar a supervisão *ex post* por parte das autoridades competentes. Por outro lado, por motivos de coerência com a atual legislação relativa à segurança dos produtos, as avaliações da conformidade dos sistemas de IA que são componentes de segurança de produtos seguirão um sistema baseado em procedimentos de avaliação da conformidade por terceiros já estabelecidos nessa legislação setorial relativa à segurança dos produtos. Serão necessárias novas avaliações da conformidade *ex ante* em caso de modificações substanciais dos sistemas de IA (nomeadamente alterações que excedam o que foi predeterminado pelo fornecedor na documentação técnica e verificado no momento da avaliação da conformidade *ex ante* inicial).

5.2.4. OBRIGAÇÕES DE TRANSPARÊNCIA APLICÁVEIS A DETERMINADOS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL (TÍTULO IV)

O **título IV** abrange determinados sistemas de IA para ter em conta os riscos específicos que a manipulação dos mesmos representa. Aplicar-se-ão obrigações de transparência aos sistemas que: i) interagem com seres humanos, ii) são utilizados para detetar emoções ou determinar a associação com categorias (sociais) com base ems dados biométricos, iii) geram ou manipulam conteúdos («falsificações profundas»). As pessoas devem ser informadas quando interagem com um sistema de IA ou as suas emoções ou características são reconhecidas por meios automatizados. Se um sistema de IA for utilizado para gerar ou manipular conteúdos de imagem, áudio ou vídeo consideravelmente semelhantes a conteúdos autênticos, deve ser obrigatório divulgar que os conteúdos são gerados por meios automatizados, sob reserva de exceções para fins legítimos (manutenção da ordem pública, liberdade de expressão). Deste modo, as pessoas podem tomar decisões informadas ou distanciar-se de determinadas situações.

5.2.5. MEDIDAS DE APOIO À INOVAÇÃO (TÍTULO V)

O **título V** contribui para o objetivo de criar um quadro jurídico inovador, preparado para o futuro e resistente a perturbações. Para tal, as autoridades nacionais competentes são incentivadas a criar ambientes de testagem da regulamentação. Além disso, é criado um quadro básico no que diz respeito à governação, à supervisão e à responsabilidade. Os

ambientes de testagem da regulamentação da IA criam um ambiente controlado para testar tecnologias inovadoras durante um período limitado com base num plano de testagem acordado com as autoridades competentes. O título V também inclui medidas para reduzir os encargos regulamentares impostos às PME e às empresas em fase de arranque.

5.2.6. GOVERNAÇÃO E EXECUÇÃO (TÍTULOS VI, VII E VII)

O **título VI** cria os sistemas de governação a nível da União e nacional. A nível da União, a proposta cria um Comité Europeu para a Inteligência Artificial (a seguir designado por «Comité»), composto por representantes dos Estados-Membros e da Comissão. O Comité facilitará uma aplicação simples, eficaz e harmonizada do presente regulamento, contribuindo para a cooperação eficaz entre as autoridades nacionais de controlo e a Comissão e prestando aconselhamento e conhecimentos especializados à Comissão. O Comité irá ainda recolher e partilhar informações sobre boas práticas entre os Estados-Membros.

A nível nacional, os Estados-Membros terão de designar uma ou mais autoridades nacionais competentes e, entre elas, a autoridade nacional de controlo, para efeitos de supervisão da aplicação e da execução do regulamento. A Autoridade Europeia para a Proteção de Dados atuará como autoridade competente para a supervisão das instituições, órgãos e organismos da União abrangidas pelo âmbito do presente regulamento.

O **título VII** visa facilitar as atividades de controlo da Comissão e das autoridades nacionais mediante a criação de uma base de dados à escala da UE para os sistemas de IA de risco elevado autónomos com implicações em matéria de direitos fundamentais. A base de dados será gerida pela Comissão e receberá dados dos fornecedores de sistemas de IA, que serão obrigados a registar os seus sistemas antes de os colocar no mercado ou em serviço.

O **título VIII** estabelece as obrigações de controlo e de comunicação aplicáveis aos fornecedores de sistemas de IA no que diz respeito ao acompanhamento pós-comercialização e à comunicação e investigação de incidentes e anomalias relacionados com a IA. As autoridades de fiscalização do mercado também controlarão o mercado e investigarão o cumprimento das obrigações e dos requisitos aplicáveis a todos os sistemas de IA de risco elevado já colocados no mercado. As autoridades de fiscalização do mercado terão todas as competências previstas no Regulamento (UE) 2019/1020 relativo à fiscalização do mercado. A execução *ex post* deve assegurar que, após a colocação do sistema de IA no mercado, as autoridades públicas dispõem dos poderes e dos recursos para intervir caso os sistemas de IA criem riscos inesperados que exijam uma ação rápida. As autoridades controlarão ainda o cumprimento das obrigações aplicáveis aos operadores por força do regulamento. A proposta não prevê a criação automática de mais organismos ou autoridades a nível dos Estados-Membros. Como tal, os Estados-Membros podem nomear (e tirar partido dos conhecimentos especializados de) autoridades setoriais existentes, a quem seriam confiados os poderes de controlo e execução das disposições do regulamento.

O acima disposto não prejudica o sistema existente e a repartição de poderes ou a execução *ex post* das obrigações em matéria de direitos fundamentais nos Estados-Membros. Quando tal se afigure necessário para cumprirem o seu mandato, as atuais autoridades de supervisão e execução também terão o poder de solicitar e aceder à documentação mantida por força deste regulamento e, caso seja necessário, de solicitar às autoridades de fiscalização do mercado que organizem testes ao sistema de IA de risco elevado por recurso a meios técnicos.

5.2.7. CÓDIGOS DE CONDUTA (TÍTULO IX)

O **título IX** estabelece um quadro para a criação de códigos de conduta, que visa incentivar os fornecedores de sistemas de IA que não são de risco elevado a aplicar voluntariamente os requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado (conforme indicado no

título III). Os fornecedores de sistemas de IA que não são de risco elevado podem criar e aplicar autonomamente os códigos de conduta. Esses códigos também podem incluir compromissos voluntários relacionados, por exemplo, com a sustentabilidade ambiental, a acessibilidade das pessoas com deficiência, a participação das partes interessadas na conceção e no desenvolvimento de sistemas de IA e a diversidade das equipas de desenvolvimento.

5.2.8. DISPOSIÇÕES FINAIS (TÍTULOS X, XI E XII)

O **título X** salienta a obrigação de todas as partes respeitarem a confidencialidade das informações e dos dados e estabelece regras para o intercâmbio das informações obtidas durante a aplicação do regulamento. O título X também inclui medidas para assegurar a execução eficaz do regulamento por via de sanções efetivas, proporcionadas e dissuasivas aplicáveis a infrações às disposições.

O **título XI** estabelece as regras para o exercício dos poderes delegados e de execução. A proposta habilita a Comissão a adotar, se for caso disso, atos de execução para garantir a aplicação uniforme do regulamento ou atos delegados para atualizar ou completar as listas constantes dos anexos I a VII.

O **título XII** incumbe a Comissão de avaliar regularmente a necessidade de atualizar o anexo III e preparar relatórios regulares sobre a avaliação e o reexame do regulamento. Também estabelece disposições finais, incluindo um período de transição diferenciado para a data inicial da aplicação do regulamento, de maneira que facilite uma aplicação simples por todas as partes em causa.

2021/0106 (COD)

Proposta de

REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

QUE ESTABELECE REGRAS HARMONIZADAS EM MATÉRIA DE INTELIGÊNCIA ARTIFICIAL (REGULAMENTO INTELIGÊNCIA ARTIFICIAL) E ALTERA DETERMINADOS ATOS LEGISLATIVOS DA UNIÃO

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente os artigos 16.º e 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu[31],

Tendo em conta o parecer do Comité das Regiões[32],

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) A finalidade do presente regulamento é melhorar o funcionamento do mercado interno mediante o estabelecimento de um quadro jurídico uniforme para o desenvolvimento, a comercialização e a utilização da inteligência artificial em conformidade com os valores da União. O presente regulamento observa um conjunto de razões imperativas de reconhecido interesse público, como o elevado nível de proteção da saúde, da segurança e dos direitos fundamentais, e assegura a livre circulação transfronteiras de produtos e serviços baseados em inteligência artificial, evitando assim que os Estados-Membros imponham restrições ao desenvolvimento, à comercialização e à utilização dos sistemas de inteligência artificial, salvo se explicitamente autorizado pelo presente regulamento.

(2) Os sistemas de inteligência artificial (sistemas de IA) podem ser implantados facilmente em vários setores da economia e da sociedade, incluindo além fronteiras, e circular por toda a União. Certos Estados-Membros já ponderaram a adoção de regras nacionais para assegurar que a inteligência artificial seja segura e seja desenvolvida e utilizada em conformidade com as obrigações de proteção dos direitos fundamentais. As diferenças entre regras nacionais podem conduzir à fragmentação do mercado interno e reduzir a segurança jurídica para os operadores que desenvolvem ou utilizam sistemas de IA. Como tal, é necessário assegurar um nível de proteção elevado e coerente em toda a União e evitar divergências que prejudiquem a livre circulação dos sistemas de IA e dos produtos e serviços conexos no mercado interno, mediante o estabelecimento de obrigações uniformes para os operadores e a garantia da proteção uniforme das razões imperativas de reconhecido interesse público e dos direitos das

[31] JO C […] de […], p. […].
[32] JO C […] de […], p. […].

pessoas em todo o mercado interno, com base no artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE). Visto que o presente regulamento contém regras específicas aplicáveis à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, nomeadamente restrições à utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, é apropriado basear este regulamento no artigo 16.º do TFUE, no respeitante a essas regras específicas. Face a essas regras específicas e ao recurso ao artigo 16.º do TFUE, é apropriado consultar o Comité Europeu para a Proteção de Dados.

(3) A inteligência artificial é uma família de tecnologias em rápida evolução, capaz de oferecer um vasto conjunto de benefícios económicos e sociais a todo o leque de indústrias e atividades sociais. Ao melhorar as previsões, otimizar as operações e a repartição de recursos e personalizar as soluções digitais disponibilizadas às pessoas e às organizações, a utilização da inteligência artificial pode conferir importantes vantagens competitivas às empresas e contribuir para progressos sociais e ambientais, por exemplo, nos cuidados de saúde, na agricultura, na educação e na formação, na gestão das infraestruturas, na energia, nos transportes e logística, nos serviços públicos, na segurança, na justiça, na eficiência energética e dos recursos e na atenuação das alterações climáticas e adaptação às mesmas.

(4) Ao mesmo tempo, em função das circunstâncias relativas à sua aplicação e utilização específicas, a inteligência artificial pode criar riscos e prejudicar interesses públicos e direitos protegidos pela legislação da União. Esses prejuízos podem ser materiais ou imateriais.

(5) Como tal, é necessário adotar um quadro jurídico da União que estabeleça regras harmonizadas em matéria de inteligência artificial para promover o desenvolvimento, a utilização e a adoção da inteligência artificial no mercado interno e que, ao mesmo tempo, proporcione um nível elevado de proteção de interesses públicos, como a saúde e a segurança e a proteção dos direitos fundamentais, conforme reconhecido e protegido pelo direito da União. Para alcançar esse objetivo, torna-se necessário estabelecer regras aplicáveis à colocação no mercado e à colocação em serviço de determinados sistemas de IA, garantindo assim o correto funcionamento do mercado interno e permitindo que esses sistemas beneficiem do princípio de livre circulação dos produtos e dos serviços. Ao estabelecer essas regras, o presente regulamento apoia o objetivo da União de estar na vanguarda mundial do desenvolvimento de uma inteligência artificial que seja segura, ética e de confiança, conforme mencionado pelo Conselho Europeu[33] e garante a proteção de princípios éticos, conforme solicitado especificamente pelo Parlamento Europeu[34].

(6) A definição de «sistema de IA» deve ser inequívoca, para assegurar a segurança jurídica, concedendo em simultâneo a flexibilidade suficiente para se adaptar a futuras evoluções tecnológicas. A definição deve basear-se nas principais características funcionais do *software*, em particular a capacidade, tendo em vista um determinado conjunto de objetivos definidos pelos seres humanos, de criar resultados, tais como conteúdos, previsões, recomendações ou decisões que influenciam o ambiente com o

[33] Conselho Europeu, Reunião extraordinária do Conselho Europeu (1 e 2 de outubro de 2020) — Conclusões [EUCO 13/20, 2020, p. 6].

[34] Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime relativo aos aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas [2020/2012(INL)].

qual o sistema interage, quer numa dimensão física, quer digital. Os sistemas de IA podem ser concebidos para operar com diferentes níveis de autonomia e ser utilizados autonomamente ou como componente de um produto, independentemente de o sistema estar fisicamente incorporado no produto (integrado) ou servir a funcionalidade do produto sem estar incorporado nele (não integrado). A definição de «sistema de IA» deve ser completada por uma lista de técnicas e abordagens específicas utilizadas para o seu desenvolvimento, que deve ser atualizada face à evolução do mercado e da tecnologia, mediante a adoção de atos delegados da Comissão que alterem essa lista.

(7) A definição de «dados biométricos» utilizada no presente regulamento está em consonância e deve ser interpretada de forma coerente com a definição de «dados biométricos» constante do artigo 4.º, ponto 14, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[35], do artigo 3.º, ponto 18, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho[36] e do artigo 3.º, ponto 13, da Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho[37].

(8) O conceito de «sistema de identificação biométrica à distância» utilizado no presente regulamento deve ser definido, de modo funcional, como um sistema de IA que se destina à identificação de pessoas singulares à distância por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência, sem que se saiba, antecipadamente, se a pessoa visada estará presente e pode ser identificada, independentemente da tecnologia, dos processos ou dos tipos de dados biométricos utilizados. Tendo em conta as diferentes características e formas como são utilizados, bem como os diferentes riscos inerentes, deve ser efetuada uma distinção entre sistemas de identificação biométrica à distância «em tempo real» e «em diferido». No caso dos sistemas «em tempo real», a recolha dos dados biométricos, a comparação e a identificação ocorrem de imediato, quase de imediato ou, em todo o caso, sem um atraso significativo. Não pode haver, a este respeito, margem para contornar as regras do presente regulamento sobre a utilização «em tempo real» dos sistemas de IA em causa por via da introdução de ligeiros retardamentos no sistema. Os sistemas «em tempo real» implicam a utilização «ao vivo» ou «quase ao vivo» de materiais, como vídeos, criados por uma câmara ou outro dispositivo com uma funcionalidade semelhante. Por outro lado, no caso dos sistemas «em diferido», os dados biométricos já foram recolhidos e a comparação e a identificação ocorrem apenas após um atraso significativo. Estes sistemas utilizam materiais, tais como imagens ou vídeos, criados por câmaras de televisão em circuito fechado ou dispositivos privados antes de o sistema ser utilizado relativamente às pessoas singulares em causa.

---

35 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

36 Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

37 Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (Diretiva sobre a Proteção de Dados na Aplicação da Lei) (JO L 119 de 4.5.2016, p. 89).

(9) Para efeitos do presente regulamento, deve entender-se por «espaço acessível ao público» qualquer espaço físico que seja acessível ao público, independentemente de o espaço em questão ser detido por uma entidade privada ou pública. Como tal, a definição não abrange locais de natureza privada ou que não são de acesso livre a terceiros, incluindo as autoridades policiais, a não ser que essas partes tenham sido especificamente convidadas ou autorizadas, tais como residências, clubes privados, escritórios, armazéns e fábricas. Os espaços em linha também não são abrangidos, uma vez que não são espaços físicos. Contudo, a mera possibilidade de aplicar determinadas condições para o acesso a um espaço particular, como bilhetes de admissão ou restrições de idade, não significa que o espaço não é acessível ao público na aceção do presente regulamento. Consequentemente, além dos espaços públicos, como as ruas, as partes relevantes dos edifícios governamentais e a maioria das infraestruturas de transporte, espaços como cinemas, teatros, lojas e centros comerciais também são, por norma, acessíveis ao público. Para determinar se um espaço é acessível ao público deve recorrer-se a uma análise casuística, tendo em conta as especificidades da situação em apreço.

(10) Para assegurar condições de concorrência equitativas e uma proteção eficaz dos direitos e das liberdades das pessoas singulares em toda a União, as regras estabelecidas no presente regulamento devem aplicar-se aos fornecedores de sistemas de IA de uma forma não discriminatória, independentemente de estarem estabelecidos na União ou num país terceiro, e aos utilizadores de sistemas de IA estabelecidos na União.

(11) Face à natureza digital dos sistemas de IA, determinados sistemas devem ser abrangidos pelo âmbito do presente regulamento, mesmo quando não são colocados no mercado ou em serviço, nem são utilizados na União. Esta situação verifica-se, por exemplo, quando um operador estabelecido na União contrata determinados serviços a um operador estabelecido fora da União relativamente a uma atividade a realizar por um sistema de IA que seria considerado «de risco elevado» e cujos efeitos afetam pessoas singulares localizadas na União. Nessas circunstâncias, o operador fora da União poderia utilizar o seu sistema de IA para tratar dados recolhidos e transferidos licitamente da União e fornecer ao operador contratante na União o resultado desse sistema de IA decorrente desse tratamento, sem que o sistema de IA em causa fosse colocado no mercado ou em serviço ou utilizado na União. Para evitar que o presente regulamento seja contornado e para assegurar uma proteção eficaz das pessoas singulares localizadas na União, o presente regulamento deve ser igualmente aplicável a fornecedores e utilizadores de sistemas de IA estabelecidos num país terceiro nos casos em que o resultado desses sistemas seja utilizado na União. No entanto, para ter em conta os mecanismos existentes e as necessidades especiais de cooperação com os parceiros estrangeiros com quem são trocadas informações e dados, o presente regulamento não deve ser aplicável às autoridades públicas de um país terceiro e às organizações internacionais quando estas atuam no âmbito de acordos internacionais celebrados a nível nacional ou europeu para efeitos de cooperação policial e judiciária com a União ou com os seus Estados-Membros. Tais acordos têm sido celebrados bilateralmente entre Estados-Membros e países terceiros ou entre a União Europeia, a Europol e outras agências da UE e países terceiros e organizações internacionais.

(12) O presente regulamento deverá ser também aplicável a instituições, órgãos e organismos da União quando atuam como fornecedor ou utilizador de um sistema de IA. Os sistemas de IA desenvolvidos ou utilizados exclusivamente para efeitos militares devem ser excluídos do âmbito do presente regulamento, caso essa utilização

seja abrangida pela competência exclusiva da política externa e de segurança comum regulamentada nos termos do título V do Tratado da União Europeia (TUE). O presente regulamento não prejudica a responsabilidade dos prestadores intermediários de serviços estabelecida na Diretiva 2000/31/CE do Parlamento Europeu e do Conselho [na redação que lhe foi dada pelo Regulamento Serviços Digitais].

(13) A fim de assegurar um nível elevado e coerente de proteção dos interesses públicos nos domínios da saúde, da segurança e dos direitos fundamentais, devem ser criadas normas comuns aplicáveis a todos os sistemas de IA de risco elevado. Essas normas devem ser coerentes com a Carta dos Direitos Fundamentais da União Europeia (a seguir designada por «Carta») e não discriminatórias, bem como estar em consonância com os compromissos comerciais internacionais da União.

(14) Para que o conjunto de normas vinculativas aplicáveis aos sistemas de IA seja proporcionado e eficaz, deve seguir-se uma abordagem baseada no risco claramente definida. Essa abordagem deve adaptar o tipo e o conteúdo dessas normas à intensidade e ao âmbito dos riscos criados pelos sistemas de IA. Como tal, é necessário proibir determinadas práticas de inteligência artificial, estabelecer requisitos aplicáveis aos sistemas de IA de risco elevado e obrigações para os operadores pertinentes, bem como estabelecer obrigações de transparência para determinados sistemas de IA.

(15) Além das inúmeras utilizações benéficas da inteligência artificial, essa tecnologia pode ser utilizada indevidamente e conceder instrumentos novos e poderosos para práticas manipuladoras, exploratórias e de controlo social. Essas práticas são particularmente prejudiciais e devem ser proibidas, pois desrespeitam valores da União, como a dignidade do ser humano, a liberdade, a igualdade, a democracia e o Estado de direito, bem como direitos fundamentais da União, incluindo o direito à não discriminação, à proteção de dados pessoais e à privacidade, e os direitos das crianças.

(16) Deve ser proibida a colocação no mercado, a colocação em serviço ou a utilização de determinados sistemas de IA concebidos para distorcer o comportamento humano, os quais são passíveis de provocar danos físicos ou psicológicos. Esses sistemas de IA utilizam componentes subliminares que não são detetáveis pelos seres humanos ou exploram vulnerabilidades de crianças e adultos associadas à sua idade e às suas incapacidades físicas ou mentais. A intenção destes sistemas é distorcer substancialmente o comportamento de uma pessoa de uma forma que cause ou seja suscetível de causar danos a essa ou a outra pessoa. A intenção pode não ser detetada caso a distorção do comportamento humano resulte de fatores externos ao sistema de IA que escapam ao controlo do fornecedor ou do utilizador. A proibição não pode impedir a investigação desses sistemas de IA para efeitos legítimos, desde que essa investigação não implique uma utilização do sistema de IA em relações homem-máquina que exponha pessoas singulares a danos e seja efetuada de acordo com normas éticas reconhecidas para fins de investigação científica.

(17) Os sistemas de IA que possibilitam a classificação social de pessoas singulares para uso geral das autoridades públicas ou em nome destas podem criar resultados discriminatórios e levar à exclusão de determinados grupos. Estes sistemas podem ainda violar o direito à dignidade e à não discriminação e os valores da igualdade e da justiça. Esses sistemas de IA avaliam ou classificam a credibilidade de pessoas singulares com base no seu comportamento social em diversos contextos ou em características de personalidade ou pessoais, conhecidas ou previsíveis. A classificação social obtida por meio desses sistemas de IA pode levar ao tratamento prejudicial ou

desfavorável de pessoas singulares ou grupos inteiros das mesmas em contextos sociais não relacionados com o contexto nos quais os dados foram originalmente gerados ou recolhidos ou a um tratamento prejudicial que é injustificado ou desproporcionado face à gravidade do seu comportamento social. Como tal, esses sistemas de IA devem ser proibidos.

(18) A utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» de pessoas singulares em espaços acessíveis ao público para efeitos de manutenção da ordem pública é considerada particularmente intrusiva para os direitos e as liberdades das pessoas em causa, visto que pode afetar a vida privada de uma grande parte da população, dar origem a uma sensação de vigilância constante e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais. Além disso, dado o impacto imediato e as oportunidades limitadas para a realização de controlos adicionais ou correções da utilização desses sistemas que funcionam «em tempo real», estes dão origem a riscos acrescidos para os direitos e as liberdades das pessoas visadas pelas autoridades policiais.

(19) Como tal, deve ser proibida a utilização desses sistemas para efeitos de manutenção da ordem pública, salvo em três situações enunciadas exaustivamente e definidas de modo restrito, em que a utilização é estritamente necessária por motivos de interesse público importante e cuja importância prevalece sobre os riscos. Essas situações implicam a procura de potenciais vítimas de crimes, incluindo crianças desaparecidas, certas ameaças à vida ou à segurança física de pessoas singulares ou ameaças de ataque terrorista, e a deteção, localização, identificação ou instauração de ações penais relativamente a infratores ou suspeitos de infrações penais a que se refere a Decisão-Quadro 2002/584/JAI do Conselho[38], desde que puníveis no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro. Esse limiar para a pena ou medida de segurança privativa de liberdade prevista no direito nacional contribui para assegurar que a infração seja suficientemente grave para justificar potencialmente a utilização de sistemas de identificação biométrica à distância «em tempo real». Além disso, das 32 infrações penais enumeradas na Decisão-Quadro 2002/584/JAI do Conselho, algumas são provavelmente mais pertinentes do que outras, já que o recurso à identificação biométrica à distância «em tempo real» será previsivelmente necessário e proporcionado em graus extremamente variáveis no respeitante à deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito das diferentes infrações penais enumeradas e tendo em conta as prováveis diferenças em termos de gravidade, probabilidade e magnitude dos prejuízos ou das possíveis consequências negativas.

(20) A fim de assegurar que esses sistemas sejam utilizados de uma forma responsável e proporcionada, também importa estabelecer que, em cada uma dessas três situações enunciadas exaustivamente e definidas de modo restrito, é necessário ter em conta determinados elementos, em especial no que se refere à natureza da situação que dá origem ao pedido e às consequências da utilização para os direitos e as liberdades de todas as pessoas em causa e ainda às salvaguardas e condições previstas para a utilização. Além disso, a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública deve estar sujeita a limites espaciais e temporais adequados, tendo em

[38] Decisão-Quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros (JO L 190 de 18.7.2002, p. 1).

conta, especialmente, os dados ou indícios relativos às ameaças, às vítimas ou ao infrator. A base de dados de pessoas utilizada como referência deve ser adequada a cada utilização em cada uma das três situações acima indicadas.

(21) Cada utilização de um sistema de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública deve estar sujeita a uma autorização expressa e específica de uma autoridade judiciária ou de uma autoridade administrativa independente de um Estado-Membro. Em princípio, essa autorização deve ser obtida antes da sua utilização, salvo em situações de urgência devidamente justificadas, ou seja, quando a necessidade de utilizar os sistemas em causa torna efetiva e objetivamente impossível obter uma autorização antes de iniciar essa utilização. Nessas situações de urgência, a utilização deve limitar-se ao mínimo absolutamente necessário e estar sujeita a salvaguardas e condições adequadas, conforme determinado pelo direito nacional e especificado no contexto de cada caso de utilização urgente pela própria autoridade policial. Ademais, nessas situações, a autoridade policial deve procurar obter quanto antes uma autorização, apresentando as razões para não ter efetuado o pedido mais cedo.

(22) Além disso, no âmbito do quadro exaustivo estabelecido pelo presente regulamento, importa salientar que essa utilização no território de um Estado-Membro apenas deve ser possível uma vez que o Estado-Membro em causa tenha decidido possibilitar expressamente a autorização dessa utilização de acordo com o presente regulamento nas regras de execução previstas no direito nacional. Consequentemente, ao abrigo do presente regulamento, os Estados-Membros continuam a ser livres de não possibilitar essa utilização ou de apenas possibilitar essa utilização relativamente a alguns dos objetivos passíveis de justificar uma utilização autorizada identificados no presente regulamento.

(23) A utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» de pessoas singulares em espaços acessíveis ao público para efeitos de manutenção da ordem pública implica necessariamente o tratamento de dados biométricos. As regras do presente regulamento que proíbem essa utilização, salvo em certas exceções, e que têm por base o artigo 16.º do TFUE, devem aplicar-se como *lex specialis* relativamente às regras em matéria de tratamento de dados biométricos previstas no artigo 10.º da Diretiva (UE) 2016/680, regulando assim essa utilização e o tratamento de dados biométricos conexo de uma forma exaustiva. Como tal, essa utilização e esse tratamento apenas devem ser possíveis se forem compatíveis com o quadro estabelecido pelo presente regulamento, sem que exista margem, fora desse quadro, para as autoridades competentes utilizarem esses sistemas e efetuarem o tratamento desses dados pelos motivos enunciados no artigo 10.º da Diretiva (UE) 2016/680, caso atuem para efeitos de manutenção da ordem pública. Neste contexto, o presente regulamento não pretende constituir o fundamento jurídico do tratamento de dados pessoais, nos termos do artigo 8.º da Diretiva (UE) 2016/680. Contudo, a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para outros fins que não os policiais, incluindo por parte das autoridades competentes, não deve ser abrangida pelo quadro específico relativo a essa utilização para efeitos de manutenção da ordem pública estabelecido pelo presente regulamento. Assim, uma utilização para outros fins que não a manutenção da ordem pública não deve estar sujeita ao requisito de autorização previsto no presente regulamento nem às eventuais regras de execução previstas no direito nacional.

(24) Qualquer tratamento de dados biométricos e de outros dados pessoais envolvidos na utilização de sistemas de IA para fins de identificação biométrica, desde que não estejam associados à utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, conforme regida pelo presente regulamento, incluindo quando esses sistemas são utilizados pelas autoridades competentes em espaços acessíveis ao público para outros fins que não os policiais, deve continuar a cumprir todos os requisitos decorrentes do artigo 9.º, n.º 1, do Regulamento (UE) 2016/679, do artigo 10.º, n.º 1, do Regulamento (UE) 2018/1725 e do artigo 10.º da Diretiva (UE) 2016/680, conforme aplicável.

(25) Nos termos do artigo 6.º-A do Protocolo (n.º 21) relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao TUE e ao TFUE, a Irlanda não fica vinculada pelas regras estabelecidas no artigo 5.º, n.º 1, alínea d), e n.os 2 e 3, do presente regulamento e adotadas com base no artigo 16.º do TFUE que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades que se enquadram no âmbito da parte III, título V, capítulos 4 ou 5, do TFUE, caso não esteja vinculada por regras que rejam formas de cooperação judiciária em matéria penal ou de cooperação policial no âmbito das quais devam ser observadas as disposições definidas com base no artigo 16.º do TFUE.

(26) Nos termos dos artigos 2.º e 2.º-A do Protocolo (n.º 22) relativo à posição da Dinamarca, anexo ao TUE e ao TFUE, a Dinamarca não fica vinculada pelas regras estabelecidas no artigo 5.º, n.º 1, alínea d), e n.os 2 e 3, do presente regulamento e adotadas com base no artigo 16.º do TFUE que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades que se enquadram no âmbito de aplicação da parte III, título V, capítulos 4 ou 5, do TFUE, nem fica sujeita à aplicação das mesmas.

(27) Os sistemas de IA de risco elevado só podem ser colocados no mercado da União ou colocados em serviço se cumprirem determinados requisitos obrigatórios. Esses requisitos devem assegurar que os sistemas de IA de risco elevado disponíveis na União ou cujos resultados sejam utilizados na União não representam riscos inaceitáveis para interesses públicos importantes da União, conforme reconhecidos e protegidos pelo direito da União. A classificação de «risco elevado» aplicada a sistemas de IA deve limitar-se aos sistemas que têm um impacto prejudicial substancial na saúde, na segurança e nos direitos fundamentais das pessoas no território da União e essa limitação deve minimizar quaisquer potenciais restrições ao comércio internacional, se for caso disso.

(28) Os sistemas de IA podem produzir resultados adversos para a saúde e a segurança das pessoas, em particular quando esses sistemas funcionam como componentes de produtos. Em conformidade com os objetivos da legislação de harmonização da União, designadamente facilitar a livre circulação de produtos no mercado interno e assegurar que apenas os produtos seguros e conformes entram no mercado, é importante prevenir e atenuar devidamente os riscos de segurança que possam ser criados por um produto devido aos seus componentes digitais, incluindo sistemas de IA. A título de exemplo, os robôs, que se têm tornado cada vez mais autónomos, devem operar com segurança e realizar as suas funções em ambientes complexos, seja num contexto industrial ou de assistência e cuidados pessoais. De igual forma, no setor da saúde, em que os riscos para a vida e a saúde são particularmente elevados, os cada vez mais sofisticados sistemas de diagnóstico e sistemas que apoiam decisões humanas devem produzir resultados exatos e de confiança. A dimensão dos impactos

adversos causados pelo sistema de IA nos direitos fundamentais protegidos pela Carta é particularmente importante quando se classifica um sistema de IA como sendo de risco elevado. Esses direitos incluem o direito à dignidade do ser humano, o respeito da vida privada e familiar, a proteção de dados pessoais, a liberdade de expressão e de informação, a liberdade de reunião e de associação, a não discriminação, a defesa dos consumidores, os direitos dos trabalhadores, os direitos das pessoas com deficiência, o direito à ação e a um tribunal imparcial, a presunção de inocência e o direito de defesa e o direito a uma boa administração. Além desses direitos, é importante salientar que as crianças têm direitos específicos, consagrados no artigo 24.º da Carta da UE e na Convenção das Nações Unidas sobre os Direitos da Criança (descritos em mais pormenor no Comentário geral n.º 25 da Convenção das Nações Unidas sobre os Direitos da Criança no respeitante ao ambiente digital), que exigem que as vulnerabilidades das crianças sejam tidas em conta e que estas recebam a proteção e os cuidados necessários ao seu bem-estar. O direito fundamental a um nível elevado de proteção do ambiente consagrado na Carta e aplicado nas políticas da União também deve ser tido em conta ao avaliar a gravidade dos danos que um sistema de IA pode causar, incluindo em relação à saúde e à segurança das pessoas.

(29) Relativamente aos sistemas de IA de risco elevado que são componentes de segurança de produtos ou sistemas ou que são, eles próprios, produtos ou sistemas abrangidos pelo âmbito do Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho[39], do Regulamento (UE) n.º 167/2013 do Parlamento Europeu e do Conselho[40], do Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho[41], da Diretiva 2014/90/UE do Parlamento Europeu e do Conselho[42], da Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho[43], do Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho[44], do Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho[45] e do

39 Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008, relativo ao estabelecimento de regras comuns no domínio da segurança da aviação civil e que revoga o Regulamento (CE) n.º 2320/2002 (JO L 97 de 9.4.2008, p. 72).

40 Regulamento (UE) n.º 167/2013 do Parlamento Europeu e do Conselho, de 5 de fevereiro de 2013, relativo à homologação e fiscalização do mercado de tratores agrícolas e florestais (JO L 60 de 2.3.2013, p. 1).

41 Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho, de 15 de janeiro de 2013, relativo à homologação e fiscalização do mercado dos veículos de duas ou três rodas e dos quadriciclos (JO L 60 de 2.3.2013, p. 52).

42 Diretiva 2014/90/UE do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativa aos equipamentos marítimos e que revoga a Diretiva 96/98/CE do Conselho (JO L 257 de 28.8.2014, p. 146).

43 Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, relativa à interoperabilidade do sistema ferroviário na União Europeia (JO L 138 de 26.5.2016, p. 44).

44 Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, relativo à homologação e à fiscalização do mercado dos veículos a motor e seus reboques, e dos sistemas, componentes e unidades técnicas destinados a esses veículos, que altera os Regulamentos (CE) n.º 715/2007 e (CE) n.º 595/2009 e revoga a Diretiva 2007/46/CE (JO L 151 de 14.6.2018, p. 1).

45 Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho, de 4 de julho de 2018, relativo a regras comuns no domínio da aviação civil que cria a Agência da União Europeia para a Segurança da Aviação, altera os Regulamentos (CE) n.º 2111/2005, (CE) n.º 1008/2008, (UE) n.º 996/2010 e (UE) n.º 376/2014 e as Diretivas 2014/30/UE e 2014/53/UE do Parlamento Europeu e do Conselho, e revoga os Regulamentos (CE) n.º 552/2004 e (CE) n.º 216/2008 do Parlamento Europeu e do Conselho e o Regulamento (CEE) n.º 3922/91 do Conselho (JO L 212 de 22.8.2018, p. 1).

Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho[46], é adequado alterar esses atos para assegurar que a Comissão tenha em conta, aquando da adoção de futuros atos delegados ou de execução baseados nesses atos, os requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado estabelecidos no presente regulamento, atendendo às especificidades técnicas e regulamentares de cada setor e sem interferir com os mecanismos de governação, de avaliação da conformidade e de execução existentes nem com as autoridades estabelecidas nestes regulamentos.

(30) Relativamente aos sistemas de IA que são componentes de segurança de produtos ou que são, eles próprios, produtos abrangidos pelo âmbito de determinada legislação de harmonização da União, é apropriado classificá-los como de risco elevado ao abrigo do presente regulamento nos casos em que forem objeto de um procedimento de avaliação da conformidade realizado por um organismo terceiro de avaliação da conformidade nos termos dessa legislação de harmonização da União aplicável. Em particular, tais produtos são máquinas, brinquedos, ascensores, aparelhos e sistemas de proteção destinados a ser utilizados em atmosferas potencialmente explosivas, equipamentos de rádio, equipamentos sob pressão, equipamentos de embarcações de recreio, instalações por cabo, aparelhos a gás, dispositivos médicos e dispositivos médicos para diagnóstico *in vitro*.

(31) Classificar um sistema de IA como de risco elevado nos termos do presente regulamento não implica necessariamente que o produto cujo componente de segurança é o sistema de IA ou que o próprio sistema de IA enquanto produto seja considerado «de risco elevado», segundo os critérios estabelecidos na legislação de harmonização da União aplicável ao produto. Tal verifica-se no respeitante ao Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho[47] e ao Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho[48], que preveem a avaliação por terceiros da conformidade de produtos de risco médio e elevado.

(32) Relativamente aos sistemas de IA autónomos, ou seja, sistemas de IA de risco elevado que não são componentes de segurança de produtos nem são, eles próprios, produtos, é apropriado classificá-los como de risco elevado se, em função da finalidade prevista, representarem um risco elevado de danos para a saúde e a segurança ou de prejuízo para os direitos fundamentais das pessoas, tendo em conta a gravidade dos possíveis danos e a probabilidade dessa ocorrência, e se forem utilizados num conjunto de domínios especificamente predefinidos no regulamento. A identificação desses

---

46 Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, relativo aos requisitos de homologação de veículos a motor e seus reboques e dos sistemas, componentes e unidades técnicas destinados a esses veículos, no que se refere à sua segurança geral e à proteção dos ocupantes dos veículos e dos utentes da estrada vulneráveis, que altera o Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho e revoga os Regulamentos (CE) n.º 78/2009, (CE) n.º 79/2009 e (CE) n.º 661/2009 do Parlamento Europeu e do Conselho e os Regulamentos (CE) n.º 631/2009, (UE) n.º 406/2010, (UE) n.º 672/2010, (UE) n.º 1003/2010, (UE) n.º 1005/2010, (UE) n.º 1008/2010, (UE) n.º 1009/2010, (UE) n.º 19/2011, (UE) n.º 109/2011, (UE) n.º 458/2011, (UE) n.º 65/2012, (UE) n.º 130/2012, (UE) n.º 347/2012, (UE) n.º 351/2012, (UE) n.º 1230/2012, e (UE) 2015/166 da Comissão (JO L 325 de 16.12.2019, p. 1).

47 Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.º 178/2002 e o Regulamento (CE) n.º 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho (JO L 117 de 5.5.2017, p. 1).

48 Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos para diagnóstico *in vitro* e que revoga a Diretiva 98/79/CE e a Decisão 2010/227/UE da Comissão (JO L 117 de 5.5.2017, p. 176).

sistemas baseia-se na mesma metodologia e nos mesmos critérios previstos para futuras alterações da lista de sistemas de IA de risco elevado.

(33) As imprecisões técnicas dos sistemas de IA concebidos para a identificação biométrica à distância de pessoas singulares podem conduzir a resultados enviesados e ter efeitos discriminatórios. Esta questão é particularmente importante no que diz respeito à idade, à etnia, ao sexo ou a deficiências das pessoas. Como tal, os sistemas de identificação biométrica à distância «em tempo real» e «em diferido» devem ser classificados como de risco elevado. Face aos riscos que estes dois tipos de sistemas de identificação biométrica à distância representam, ambos devem estar sujeitos a requisitos específicos relativos às capacidades de registo e à supervisão humana.

(34) No tocante à gestão e ao funcionamento de infraestruturas críticas, é apropriado classificar como de risco elevado os sistemas de IA concebidos para serem utilizados como componentes de segurança na gestão e no controlo do tráfego rodoviário e das redes de abastecimento de água, gás, aquecimento e eletricidade, uma vez que a falha ou anomalia destes sistemas pode pôr em risco a vida e a saúde das pessoas em larga escala e provocar perturbações substanciais das atividades sociais e económicas normais.

(35) Os sistemas de IA utilizados no domínio da educação ou formação profissional, designadamente para determinar o acesso ou a afetação de pessoas a instituições de ensino e de formação profissional ou para avaliar testes que as pessoas realizam no âmbito da sua educação ou como pré-condição para a mesma, devem ser considerados de risco elevado, uma vez que determinam o percurso académico e profissional das pessoas e, como tal, afetam a capacidade destas para garantir a subsistência. Se indevidamente concebidos e utilizados, estes sistemas podem violar o direito à educação e à formação, bem como o direito a não ser alvo de discriminação e de perpetuação de padrões históricos de discriminação.

(36) Os sistemas de IA utilizados nos domínios do emprego, da gestão de trabalhadores e do acesso ao emprego por conta própria, nomeadamente para efeitos de recrutamento e seleção, de tomada de decisões sobre promoções e despedimentos, de repartição de tarefas e de controlo ou avaliação de pessoas no âmbito de relações contratuais de trabalho também devem ser classificados como de risco elevado, uma vez que podem ter um impacto significativo nas perspetivas de carreira e na subsistência dessas pessoas. O conceito de «relações contratuais relacionadas com o trabalho» deve abranger os funcionários e as pessoas que prestam serviços por intermédio de plataformas, conforme mencionado no programa de trabalho da Comissão para 2021. Em princípio, essas pessoas não devem ser consideradas «utilizadores» na aceção do presente regulamento. Ao longo do processo de recrutamento e na avaliação, promoção ou retenção de pessoas em relações contratuais relacionadas com o trabalho, esses sistemas podem perpetuar padrões históricos de discriminação, por exemplo, contra as mulheres, certos grupos etários, pessoas com deficiência ou pessoas de uma determinada origem racial ou étnica ou orientação sexual. Os sistemas de IA utilizados para controlar o desempenho e o comportamento destas pessoas podem ter ainda um impacto nos seus direitos à proteção de dados pessoais e à privacidade.

(37) Outro domínio no qual a utilização de sistemas de IA merece especial atenção é o acesso a determinados serviços e prestações essenciais, de cariz privado e público, e o usufruto dos mesmos, os quais são necessários para que as pessoas participem plenamente na sociedade ou melhorem o seu nível de vida. Em particular, os sistemas de IA utilizados para avaliar a classificação de crédito ou a capacidade de

endividamento de pessoas singulares devem ser classificados como sistemas de IA de risco elevado, uma vez que determinam o acesso dessas pessoas a recursos financeiros ou a serviços essenciais, como o alojamento, a eletricidade e os serviços de telecomunicações. Os sistemas de IA utilizados para essa finalidade podem conduzir à discriminação de pessoas ou grupos e perpetuar padrões históricos de discriminação, por exemplo, em razão da origem étnica ou racial, deficiência, idade ou orientação sexual, ou criar novas formas de impactos discriminatórios. Tendo em conta a dimensão bastante limitada do impacto e as alternativas disponíveis no mercado, é apropriado isentar os sistemas de IA utilizados para efeitos de avaliação da capacidade de endividamento e de classificação de crédito que sejam colocados em serviço por fornecedores de pequena dimensão para utilização própria. Normalmente, as pessoas singulares que se candidatam ou que recebem prestações e serviços de assistência pública de autoridades públicas dependem dos mesmos e estão numa posição vulnerável face às autoridades competentes. Caso sejam utilizados para determinar a recusa, redução, revogação ou recuperação dessas prestações e serviços pelas autoridades, os sistemas de IA podem ter um impacto significativo na subsistência das pessoas e podem infringir os seus direitos fundamentais, como o direito à proteção social, à não discriminação, à dignidade do ser humano ou à ação. Como tal, esses sistemas devem ser classificados como de risco elevado. No entanto, o presente regulamento não pode constituir um obstáculo ao desenvolvimento e à utilização de abordagens inovadoras na administração pública, que tirariam partido de uma maior utilização de sistemas de IA conformes e seguros, desde que esses sistemas não representem um risco elevado para as pessoas coletivas e singulares. Por último, os sistemas de IA utilizados para enviar ou estabelecer prioridades no envio de serviços de resposta a emergências devem ser classificados como de risco elevado, uma vez que tomam decisões em situações bastante críticas que afetam a vida, a saúde e os bens das pessoas.

(38) As ações das autoridades policiais que implicam certas utilizações dos sistemas de IA são caracterizadas por um grau substancial de desequilíbrio de poder e podem conduzir à vigilância, detenção ou privação da liberdade de uma pessoa singular, bem como ter outros impactos adversos nos direitos fundamentais garantidos pela Carta. Em particular, se não for treinado com dados de alta qualidade, não cumprir os requisitos adequados em termos de exatidão ou solidez ou não tiver sido devidamente concebido e testado antes de ser colocado no mercado ou em serviço, o sistema de IA pode destacar pessoas de uma forma discriminatória ou incorreta e injusta. Além disso, o exercício de importantes direitos fundamentais processuais, como o direito à ação e a um tribunal imparcial, a presunção de inocência e o direito de defesa, pode ser prejudicado, em particular, se esses sistemas de IA não forem suficientemente transparentes, explicáveis e documentados. Como tal, é apropriado classificar como de risco elevado um conjunto de sistemas de IA concebidos para serem utilizados no contexto da manutenção da ordem pública, no qual a exatidão, a fiabilidade e a transparência são particularmente importantes para evitar impactos adversos, reter a confiança do público e assegurar a responsabilidade e vias de recurso eficazes. Tendo em conta a natureza das atividades em causa e os riscos associados às mesmas, esses sistemas de IA de risco elevado devem incluir, em particular, sistemas de IA concebidos para serem utilizados pelas autoridades policiais em avaliações individuais de riscos, em polígrafos e em instrumentos semelhantes ou para detetar o estado emocional de uma pessoa singular, para detetar «falsificações profundas», para avaliar a fiabilidade dos elementos de prova em processos penais, para prever a ocorrência ou a recorrência de uma infração penal real ou potencial com base na definição de perfis

de pessoas singulares ou para avaliar os traços de personalidade e as características ou o comportamento criminal passado de pessoas singulares ou grupos, para a definição de perfis no decurso da deteção, investigação ou repressão de infrações penais, bem como para o estudo analítico de crimes relativos a pessoas singulares. Os sistemas de IA especificamente concebidos para serem utilizados em processos administrativos por autoridades fiscais e aduaneiras não devem ser considerados sistemas de IA de risco elevado utilizados por autoridades policiais para efeitos de prevenção, deteção, investigação e repressão de infrações penais.

(39) Os sistemas de IA utilizados na gestão da migração, do asilo e do controlo das fronteiras afetam pessoas que, muitas vezes, se encontram numa posição particularmente vulnerável e que dependem do resultado das ações das autoridades públicas competentes. Como tal, a exatidão, a natureza não discriminatória e a transparência dos sistemas de IA utilizados nesses contextos são particularmente importantes para garantir o respeito dos direitos fundamentais das pessoas em causa, nomeadamente os seus direitos à livre circulação, à não discriminação, à proteção da vida privada e dos dados pessoais, à proteção internacional e a uma boa administração. Deste modo, é apropriado classificar como de risco elevado os sistemas de IA concebidos para serem utilizados por autoridades públicas competentes incumbidas de funções no domínio da gestão da migração, do asilo e do controlo das fronteiras, como polígrafos e instrumentos semelhantes, ou para detetar o estado emocional de uma pessoa singular; para avaliar determinados riscos colocados pelas pessoas singulares que entram no território de um Estado-Membro ou pedem um visto ou asilo; para verificar a autenticidade dos documentos apresentados pelas pessoas singulares; para auxiliar as autoridades públicas competentes na análise dos pedidos de asilo, de visto e de autorização de residência e das queixas relacionadas, com o objetivo de estabelecer a elegibilidade das pessoas singulares que requerem determinado estatuto. Os sistemas de IA no domínio da gestão da migração, do asilo e do controlo das fronteiras abrangidos pelo presente regulamento devem cumprir os requisitos processuais estabelecidos na Diretiva 2013/32/UE do Parlamento Europeu e do Conselho[49], no Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho[50] e noutra legislação aplicável.

(40) Determinados sistemas de IA concebidos para a administração da justiça e os processos democráticos devem ser classificados como de risco elevado, tendo em conta o seu impacto potencialmente significativo na democracia, no Estado de direito e nas liberdades individuais, bem como no direito à ação e a um tribunal imparcial. Em particular, para fazer face aos riscos de potenciais enviesamentos, erros e opacidade, é apropriado classificar como de risco elevado os sistemas de IA concebidos para auxiliar as autoridades judiciárias na investigação e na interpretação de factos e do direito e na aplicação da lei a um conjunto específico de factos. Contudo, essa classificação não deve ser alargada aos sistemas de IA concebidos para atividades administrativas puramente auxiliares que não afetam a administração efetiva da justiça em casos individuais, como a anonimização ou a pseudonimização de decisões

[49] Diretiva 2013/32/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa a procedimentos comuns de concessão e retirada do estatuto de proteção internacional (JO L 180 de 29.6.2013, p. 60).

[50] Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho, de 13 de julho de 2009, que estabelece o Código Comunitário de Vistos (Código de Vistos) (JO L 243 de 15.9.2009, p. 1).

judiciais, documentos ou dados, comunicações entre pessoal, tarefas administrativas ou afetação de recursos.

(41) A classificação de um sistema de IA como de risco elevado por força do presente regulamento não deve ser interpretada como uma indicação de que a utilização do sistema é necessariamente lícita ao abrigo de outros atos do direito da União ou ao abrigo do direito nacional compatível com o direito da União, por exemplo, em matéria de proteção de dados pessoais ou de utilização de polígrafos e de instrumentos semelhantes ou de outros sistemas para detetar o estado emocional de pessoas singulares. Essa utilização deve continuar sujeita ao cumprimento dos requisitos aplicáveis resultantes da Carta e dos atos do direito derivado da União e do direito nacional em vigor. O presente regulamento não pode ser entendido como um fundamento jurídico para o tratamento de dados pessoais, incluindo de categorias especiais de dados pessoais, se for caso disso.

(42) Para atenuar os riscos dos sistemas de IA de risco elevado colocados no mercado ou colocados em serviço no mercado da União para os utilizadores e as pessoas afetadas, devem aplicar-se determinados requisitos obrigatórios, tendo em conta a finalidade de utilização prevista do sistema e de acordo com o sistema de gestão de riscos a estabelecer pelo fornecedor.

(43) Os sistemas de IA de risco elevado devem estar sujeitos ao cumprimento de requisitos relativos à qualidade dos conjuntos de dados utilizados, à documentação técnica e à manutenção de registos, à transparência e à prestação de informações aos utilizadores, à supervisão humana, à solidez, à exatidão e à cibersegurança. Esses requisitos são necessários para atenuar eficazmente os riscos para a saúde, a segurança e os direitos fundamentais, em função da finalidade prevista do sistema e quando não existam outras medidas menos restritivas do comércio, evitando, assim, restrições injustificadas do comércio.

(44) A disponibilidade de dados de elevada qualidade é um fator essencial para o desempenho de vários sistemas de IA, sobretudo quando são utilizadas técnicas que envolvem o treino de modelos, com vista a assegurar que o sistema de IA de risco elevado funcione como pretendido e de modo seguro e não se torne a fonte de uma discriminação proibida pelo direito da União. Para garantir conjuntos de dados de treino, validação e teste de elevada qualidade é necessário aplicar práticas adequadas de governação e gestão de dados. Os conjuntos de dados de treino, validação e teste devem ser suficientemente relevantes, representativos, livres de erros e completos, tendo em vista a finalidade prevista do sistema. Também devem ter as propriedades estatísticas adequadas, nomeadamente no que respeita às pessoas ou aos grupos de pessoas nos quais o sistema de IA de risco elevado será utilizado. Em particular, os conjuntos de dados de treino, validação e teste devem ter em conta, na medida do exigido face à sua finalidade prevista, as características, as funcionalidades ou os elementos que são específicos do ambiente ou do contexto geográfico, comportamental ou funcional no qual o sistema de IA será utilizado. A fim de proteger os direitos de outras pessoas da discriminação que possa resultar do enviesamento dos sistemas de IA, os fornecedores devem poder efetuar também o tratamento de categorias especiais de dados pessoais por motivos de interesse público importante, para assegurar o controlo, a deteção e a correção de enviesamentos em sistemas de IA de risco elevado.

(45) No contexto do desenvolvimento de sistemas de IA de risco elevado, determinados intervenientes, como fornecedores, organismos notificados e outras entidades

interessadas, como polos de inovação digital, instalações de teste e experimentação e investigadores, devem poder aceder e utilizar conjuntos de dados de elevada qualidade dentro das respetivas áreas de intervenção relacionadas com o presente regulamento. Os espaços comuns europeus de dados criados pela Comissão e a facilitação da partilha de dados entre empresas e com as administrações públicas por motivos de interesse público serão cruciais para conceder um acesso fiável, responsável e não discriminatório a dados de elevada qualidade para o treino, a validação e o teste de sistemas de IA. Por exemplo, no domínio da saúde, o espaço europeu de dados de saúde facilitará o acesso não discriminatório a dados de saúde e o treino de algoritmos de inteligência artificial com base nesses conjuntos de dados, de forma segura, oportuna, transparente, fidedigna e protetora da privacidade e sob a alçada de uma governação institucional adequada. As autoridades competentes, incluindo as autoridades setoriais, que concedem ou apoiam o acesso aos dados também podem apoiar o fornecimento de dados de elevada qualidade para fins de treino, validação e teste de sistemas de IA.

(46) Para verificar o cumprimento dos requisitos estabelecidos no presente regulamento, é essencial dispor de informações sobre o desenvolvimento dos sistemas de IA de risco elevado e sobre o seu desempenho ao longo do respetivo ciclo de vida. Tal exige a manutenção de registos e a disponibilização de documentação técnica que contenham as informações necessárias para avaliar o cumprimento, por parte do sistema de IA, dos requisitos aplicáveis. Essas informações devem incluir as características gerais, as capacidades e as limitações do sistema, os algoritmos, os dados e os processos de treino, teste e validação utilizados, bem como documentação sobre o sistema de gestão de riscos aplicado. A documentação técnica deve estar sempre atualizada.

(47) Para fazer face à opacidade que pode tornar determinados sistemas de IA incompreensíveis ou demasiado complexos para as pessoas singulares, os sistemas de IA de risco elevado devem observar um certo grau de transparência. Os utilizadores devem ser capazes de interpretar o resultado do sistema e utilizá-lo de forma adequada. Como tal, os sistemas de IA de risco elevado devem ser acompanhados de documentação pertinente e instruções de utilização e incluir informações concisas e claras, nomeadamente informações relativas a possíveis riscos para os direitos fundamentais e de discriminação, se for caso disso.

(48) Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que permita a sua supervisão por pessoas singulares. Para o efeito, o fornecedor do sistema deve identificar medidas de supervisão humana adequadas antes da colocação no mercado ou da colocação em serviço do sistema. Em particular, se for caso disso, essas medidas devem garantir que o sistema integre restrições operacionais que não possam ser neutralizadas pelo próprio sistema e que respondam ao operador humano e que as pessoas singulares a quem foi atribuída a supervisão humana tenham as competências, a formação e a autoridade necessárias para desempenhar essa função.

(49) Os sistemas de IA de risco elevado devem ter um desempenho coerente ao longo de todo o ciclo de vida e apresentar um nível adequado de exatidão, solidez e cibersegurança, de acordo com o estado da técnica geralmente reconhecido. O nível e as métricas de exatidão devem ser comunicadas aos utilizadores.

(50) A solidez técnica é um requisito essencial dos sistemas de IA de risco elevado. Estes sistemas devem ser resistentes aos riscos associados às suas limitações (por exemplo, erros, falhas, incoerências, situações inesperadas), bem como a ações maliciosas suscetíveis de pôr em causa a segurança do sistema de IA e dar origem a

comportamentos prejudiciais ou indesejáveis. A falta de proteção contra estes riscos pode causar problemas de segurança ou afetar negativamente os direitos fundamentais, por exemplo, devido a decisões erradas ou a resultados errados ou enviesados gerados pelo sistema de IA.

(51) A cibersegurança desempenha um papel fundamental para garantir que os sistemas de IA sejam resistentes às ações de terceiros mal-intencionados que tentam explorar as vulnerabilidades dos sistemas com o objetivo de lhes alterar a utilização, o comportamento e o desempenho ou por em causa as propriedades de segurança. Os ciberataques contra sistemas de IA podem tirar partido de ativos específicos de inteligência artificial, como os conjuntos de dados de treino (por exemplo, contaminação de dados) ou os modelos treinados (por exemplo, ataques antagónicos), ou explorar vulnerabilidades dos ativos digitais do sistema de IA ou da infraestrutura de tecnologias da informação e comunicação (TIC) subjacente. A fim de assegurar um nível de cibersegurança adequado aos riscos, os fornecedores de sistemas de IA de risco elevado devem tomar medidas adequadas, tendo ainda em devida conta a infraestrutura de TIC subjacente.

(52) No âmbito da legislação de harmonização da União, devem ser estabelecidas regras aplicáveis à colocação no mercado, à colocação em serviço e à utilização de sistemas de IA de risco elevado coerentes com o Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho[51], que estabelece os requisitos de acreditação e fiscalização de produtos, a Decisão n.º 768/2008/CE do Parlamento Europeu e do Conselho[52], relativa a um quadro comum para a comercialização de produtos, e o Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho[53], relativo à fiscalização do mercado e à conformidade dos produtos (a seguir designados conjuntamente por «novo quadro legislativo [para a comercialização de produtos]»).

(53) É apropriado que uma pessoa singular ou coletiva específica, identificada como «fornecedor», assuma a responsabilidade pela colocação no mercado ou pela colocação em serviço de um sistema de IA de risco elevado, independentemente de ser ou não a pessoa que concebeu ou desenvolveu o sistema.

(54) O fornecedor deve introduzir um sistema de gestão da qualidade sólido, garantir a realização do procedimento de avaliação da conformidade exigido, elaborar a documentação pertinente e estabelecer um sistema de acompanhamento pós-comercialização capaz. As autoridades públicas que colocam em serviço sistemas de IA de risco elevado para sua própria utilização podem adotar e aplicar as regras relativas ao sistema de gestão da qualidade no âmbito do sistema de gestão da qualidade adotado a nível nacional ou regional, consoante o caso, tendo em conta as especificidades do setor e as competências e a organização da autoridade pública em causa.

---

51 Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos, e que revoga o Regulamento (CEE) n.º 339/93 (JO L 218 de 13.8.2008, p. 30).

52 Decisão n.º 768/2008/CE do Parlamento Europeu e do Conselho, de 9 de julho de 2008, relativa a um quadro comum para a comercialização de produtos, e que revoga a Decisão 93/465/CEE (JO L 218 de 13.8.2008, p. 82).

53 Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativo à fiscalização do mercado e à conformidade dos produtos e que altera a Diretiva 2004/42/CE e os Regulamentos (CE) n.º 765/2008 e (UE) n.º 305/2011 (Texto relevante para efeitos do EEE) (JO L 169 de 25.6.2019, p. 1).

(55) Caso um sistema de IA de risco elevado que é um componente de segurança de um produto abrangido por legislação setorial do novo quadro legislativo não seja colocado no mercado ou em serviço de forma independente desse produto, o fabricante do produto final, conforme definido no correspondente ato do novo quadro legislativo, deve cumprir as obrigações dos fornecedores estabelecidas no presente regulamento e assegurar que o sistema de IA integrado no produto final cumpre os requisitos do presente regulamento.

(56) Para permitir a execução do presente regulamento e criar condições de concorrência equitativas para os operadores, tendo ainda em conta as diferentes formas de disponibilização de produtos digitais, é importante assegurar que, em qualquer circunstância, uma pessoa estabelecida na União possa fornecer às autoridades todas as informações necessárias sobre a conformidade de um sistema de IA. Como tal, antes de disponibilizarem os seus sistemas de IA na União, caso não seja possível identificar um importador, os fornecedores estabelecidos fora da União devem, através de mandato escrito, designar um mandatário estabelecido na União.

(57) Em consonância com os princípios do novo quadro legislativo, devem ser estabelecidas obrigações específicas aplicáveis a determinados operadores económicos, como os importadores e os distribuidores, de modo que garanta a segurança jurídica e facilite a conformidade regulamentar desses operadores.

(58) Dada a natureza dos sistemas de IA e os riscos para a segurança e os direitos fundamentais possivelmente associados à sua utilização, nomeadamente no que respeita à necessidade de assegurar um controlo adequado do desempenho de um sistema de IA num cenário real, é apropriado determinar responsabilidades específicas para os utilizadores. Em particular, os utilizadores devem utilizar os sistemas de IA de risco elevado de acordo com as instruções de utilização e devem ser equacionadas outras obrigações relativas ao controlo do funcionamento dos sistemas de IA e à manutenção de registos, se for caso disso.

(59) É apropriado definir que o utilizador do sistema de IA é a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo sob cuja autoridade o sistema de IA é operado, salvo se o sistema for utilizado no âmbito de uma atividade pessoal de caráter não profissional.

(60) Face à complexidade da cadeia de valor da inteligência artificial, determinados terceiros, nomeadamente os envolvidos na venda e no fornecimento de *software*, ferramentas e componentes de *software*, modelos pré-treinados e dados, ou os fornecedores de serviços de rede, devem cooperar, consoante o caso, com os fornecedores e os utilizadores, para permitir que estes cumpram as obrigações estabelecidas no presente regulamento, e com as autoridades competentes estabelecidas no presente regulamento.

(61) A normalização deve desempenhar um papel fundamental, disponibilizando aos fornecedores soluções técnicas que assegurem o cumprimento do presente regulamento. O cumprimento de normas harmonizadas, conforme definido no Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho[54], deve

[54] Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativo à normalização europeia, que altera as Diretivas 89/686/CEE e 93/15/CEE do Conselho e as Diretivas 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE e 2009/105/CE do Parlamento Europeu e do Conselho e revoga a Decisão 87/95/CEE do Conselho e a Decisão n.º 1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12).

constituir um meio de os fornecedores demonstrarem a conformidade com os requisitos do presente regulamento. Contudo, a Comissão pode adotar especificações técnicas comuns em domínios onde não existem normas harmonizadas ou onde estas são insuficientes.

(62) A fim de assegurar um nível elevado de fiabilidade dos sistemas de IA de risco elevado, estes devem ser sujeitos a uma avaliação da conformidade antes de serem colocados no mercado ou em serviço.

(63) Para minimizar os encargos impostos aos operadores e evitar possíveis duplicações, é apropriado que, no caso dos sistemas de IA de risco elevado relacionados com produtos abrangidos por legislação de harmonização da União na sequência da abordagem do novo quadro legislativo, o cumprimento dos requisitos do presente regulamento por parte desses sistemas de IA seja aferido no âmbito da avaliação da conformidade já prevista nessa legislação. Como tal, a aplicabilidade dos requisitos do presente regulamento não deve afetar a lógica, a metodologia ou a estrutura geral específicas da avaliação da conformidade realizada nos termos do correspondente ato do novo quadro legislativo. Esta abordagem encontra-se refletida na íntegra na interligação entre o presente regulamento e o [Regulamento Máquinas]. Embora os riscos de segurança dos sistemas de IA que garantem funções de segurança nas máquinas sejam tratados nos requisitos do presente regulamento, determinados requisitos específicos do [Regulamento Máquinas] assegurarão a integração segura de sistemas de IA nas máquinas em geral, de modo que não ponha em causa a segurança das máquinas no seu todo. O [Regulamento Máquinas] aplica a mesma definição de sistema de IA do presente regulamento.

(64) Dada a experiência mais vasta dos certificadores de pré-comercialização profissionais no domínio da segurança dos produtos e a diferente natureza dos riscos inerentes, é apropriado limitar, pelo menos numa fase inicial da aplicação do presente regulamento, o âmbito da avaliação da conformidade por terceiros aos sistemas de IA de risco elevado que não estejam relacionados com produtos. Como tal, a avaliação da conformidade desses sistemas deve ser realizada, regra geral, pelo fornecedor sob a sua própria responsabilidade, com a exceção única dos sistemas de IA concebidos para serem utilizados para a identificação biométrica à distância de pessoas, cuja avaliação da conformidade, contanto que os sistemas em causa não sejam proibidos, deve contar com a participação de um organismo notificado.

(65) Para efeitos de avaliação da conformidade por terceiros de sistemas de IA concebidos para serem utilizados para a identificação biométrica à distância de pessoas, o presente regulamento prevê que as autoridades nacionais competentes designem organismos notificados, os quais devem cumprir uma série de requisitos, nomeadamente em termos de independência, competência e ausência de conflitos de interesse.

(66) Em consonância com a noção comummente estabelecida de modificação substancial de produtos regulamentados pela legislação de harmonização da União, é apropriado que um sistema de IA seja objeto de uma nova avaliação da conformidade sempre que seja alterado de maneira que possa afetar o cumprimento do presente regulamento ou que a finalidade prevista do sistema se altere. Além disso, no que respeita aos sistemas de IA que continuam a «aprender» depois de terem sido colocados no mercado ou em serviço (ou seja, que adaptam automaticamente o modo de funcionamento), é necessário criar regras que determinem que as alterações do algoritmo e do desempenho predeterminados pelo fornecedor e examinados aquando da avaliação da conformidade não constituem uma modificação substancial.

(67) Para que possam circular livremente dentro do mercado interno, os sistemas de IA de risco elevado devem apresentar a marcação CE para indicar o cumprimento do presente regulamento. Os Estados-Membros não podem criar obstáculos injustificados à colocação no mercado ou à colocação em serviço de sistemas de IA de risco elevado que cumpram os requisitos previstos no presente regulamento e apresentem a marcação CE.

(68) Em certas condições, uma disponibilização rápida de tecnologias inovadoras pode ser crucial para a saúde e a segurança das pessoas e da sociedade em geral. Como tal, é apropriado que, por razões excecionais de segurança pública ou proteção da vida e da saúde das pessoas singulares e de proteção da propriedade industrial e comercial, os Estados-Membros possam autorizar a colocação no mercado ou a colocação em serviço de sistemas de IA que não foram objeto de uma avaliação da conformidade.

(69) Para facilitar o trabalho da Comissão e dos Estados-Membros no domínio da inteligência artificial, bem como aumentar a transparência para o público, os fornecedores de sistemas de IA de risco elevado que não os relacionados com produtos abrangidos pelo âmbito da atual legislação de harmonização da União devem ser obrigados a registar esses sistemas de IA de risco elevado numa base de dados da UE que será criada e gerida pela Comissão. A Comissão deve ser o responsável pelo tratamento dessa base de dados, nos termos do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho[55]. Para assegurar que a base de dados esteja plenamente operacional à data de implantação, o procedimento para a criação da base de dados deve incluir a elaboração de especificações funcionais pela Comissão e um relatório de auditoria independente.

(70) Determinados sistemas de IA concebidos para interagir com pessoas singulares ou para criar conteúdos podem representar riscos específicos de usurpação de identidade ou fraude, independentemente de serem considerados de risco elevado ou não. Como tal, em certas circunstâncias, a utilização destes sistemas deve ser sujeita a obrigações de transparência específicas sem prejudicar os requisitos e as obrigações aplicáveis aos sistemas de IA de risco elevado. Em particular, as pessoas singulares devem ser notificadas de que estão a interagir com um sistema de IA, a não ser que tal seja óbvio tendo em conta as circunstâncias e o contexto de utilização. Além disso, as pessoas singulares devem ser notificadas quando são expostas a um sistema de reconhecimento de emoções ou a um sistema de categorização biométrica. Essas informações e notificações devem ser fornecidas em formatos acessíveis a pessoas com deficiência. Além disso, os utilizadores que recorrem a um sistema de IA para gerar ou manipular conteúdos de imagem, áudio ou vídeo que sejam consideravelmente semelhantes a pessoas, locais ou acontecimentos reais e que, falsamente, pareçam ser autênticos a outrem devem divulgar que os conteúdos foram criados de forma artificial ou manipulados, identificando como tal o resultado da inteligência artificial e divulgando a sua origem artificial.

(71) A inteligência artificial é uma família de tecnologias em rápida evolução que exige novas formas de supervisão regulamentar e um espaço seguro para a experimentação, garantindo ao mesmo tempo uma inovação responsável e a integração de salvaguardas

[55] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

e medidas de atenuação dos riscos adequadas. Para assegurar um quadro jurídico propício à inovação, preparado para o futuro e resistente a perturbações, as autoridades nacionais competentes de um ou vários Estados-Membros devem ser incentivadas a criar ambientes de testagem da regulamentação da inteligência artificial que facilitem o desenvolvimento e o teste de sistemas de IA inovadores sob uma supervisão regulamentar rigorosa, antes que estes sistemas sejam colocados no mercado ou em serviço.

(72) Os objetivos dos ambientes de testagem da regulamentação devem passar por: fomentar a inovação no domínio da IA, mediante a criação de um ambiente controlado de experimentação e teste na fase de desenvolvimento e pré-comercialização, com vista a assegurar que os sistemas de IA inovadores cumprem o presente regulamento e outra legislação aplicável dos Estados-Membros e da União; reforçar a segurança jurídica para os inovadores; melhorar a supervisão e a compreensão, por parte das autoridades competentes, das oportunidades, dos riscos emergentes e dos impactos da utilização da inteligência artificial; e acelerar o acesso aos mercados, nomeadamente por via da eliminação dos entraves para as pequenas e médias empresas (PME) e as empresas em fase de arranque. Para assegurar uma aplicação uniforme em toda a União e economias de escala, é apropriado criar regras comuns para a implantação dos ambientes de testagem da regulamentação e um quadro para a cooperação entre as autoridades competentes envolvidas na supervisão desses ambientes. O presente regulamento deve estabelecer o fundamento jurídico para a utilização de dados pessoais recolhidos para outras finalidades com vista ao desenvolvimento de determinados sistemas de IA por motivos de interesse público no âmbito do ambiente de testagem da regulamentação da IA, em conformidade com o artigo 6.º, n.º 4, do Regulamento (UE) 2016/679 e do artigo 6.º do Regulamento (UE) 2018/1725 e sem prejuízo do artigo 4.º, n.º 2, da Diretiva (UE) 2016/680. Os participantes no ambiente de testagem devem assegurar salvaguardas adequadas e cooperar com as autoridades competentes, nomeadamente seguindo as suas orientações e atuando de forma célere e de boa-fé para atenuar eventuais riscos elevados para a segurança e os direitos fundamentais que possam revelar-se durante o desenvolvimento e a experimentação no ambiente de testagem. A conduta dos participantes no ambiente de testagem deve ser tida em conta quando as autoridades competentes decidirem sobre a aplicação de uma coima, nos termos do artigo 83.º, n.º 2, do Regulamento (UE) 2016/679 e do artigo 57.º da Diretiva (UE) 2016/680.

(73) A fim de promover e proteger a inovação, é importante ter em especial atenção os interesses dos fornecedores e utilizadores de sistemas de IA de pequena dimensão. Para esse efeito, os Estados-Membros devem desenvolver iniciativas dirigidas a esses operadores, incluindo ações de sensibilização e comunicação de informações. Além disso, os interesses e as necessidades específicas dos fornecedores de pequena dimensão devem ser tidas em conta quando os organismos notificados fixam as taxas a pagar pela avaliação da conformidade. Os custos de tradução associados à documentação obrigatória e à comunicação com as autoridades podem constituir um custo substancial para os fornecedores e outros operadores, nomeadamente para os fornecedores de menor dimensão. Os Estados-Membros podem eventualmente assegurar que uma das línguas por si determinadas e aceites para a elaboração de documentação pelos fornecedores e a comunicação com os operadores seja uma língua amplamente compreendida pelo maior número possível de utilizadores transfronteiras.

(74) Para minimizar os riscos para a aplicação resultantes da falta de conhecimentos e competências especializadas no mercado, bem como facilitar o cumprimento, por parte

dos fornecedores e dos organismos notificados, das obrigações que lhes são impostas pelo presente regulamento, a «plataforma IA a pedido», os polos europeus de inovação digital e as instalações de ensaio e experimentação criadas pela Comissão e pelos Estados-Membros a nível nacional ou europeu podem eventualmente contribuir para a aplicação do presente regulamento. No âmbito da respetiva missão e domínios de competência, estas entidades podem prestar apoio técnico e científico aos fornecedores e aos organismos notificados.

(75) É apropriado que a Comissão facilite, tanto quanto possível, o acesso a instalações de teste e experimentação aos organismos, grupos ou laboratórios criados ou acreditados nos termos da legislação de harmonização da União pertinente e que desempenham funções no contexto da avaliação da conformidade dos produtos ou dispositivos abrangidos por essa legislação de harmonização da União. Tal é, nomeadamente, o caso dos painéis de peritos, dos laboratórios especializados e dos laboratórios de referência no domínio dos dispositivos médicos, referidos nos Regulamentos (UE) 2017/745 e (UE) 2017/746.

(76) A fim de facilitar uma aplicação simples, eficaz e harmoniosa do presente regulamento, deve ser criado um Comité Europeu para a Inteligência Artificial. O Comité deve ser responsável por uma série de funções consultivas, nomeadamente a emissão de pareceres, recomendações, conselhos ou orientações em questões relacionadas com a aplicação do presente regulamento, incluindo no tocante a especificações técnicas ou normas existentes relativas aos requisitos indicados no presente regulamento, e a prestação de aconselhamento e assistência à Comissão sobre questões específicas relacionadas com a inteligência artificial.

(77) Os Estados-Membros desempenham um papel fundamental na aplicação e execução do presente regulamento. Nesse sentido, cada Estado-Membro deve designar uma ou várias autoridades nacionais competentes para efeitos de supervisão da aplicação e execução do presente regulamento. A fim de aumentar a eficácia organizativa dos Estados-Membros e de criar um ponto de contacto oficial para o público e outras contrapartes a nível dos Estados-Membros e da União, cada Estado-Membro deve designar uma autoridade nacional como autoridade nacional de controlo.

(78) Para assegurar que os fornecedores de sistemas de IA de risco elevado possam aproveitar a experiência adquirida na utilização de sistemas de IA de risco elevado para melhorarem os seus sistemas e o processo de conceção e desenvolvimento ou possam adotar possíveis medidas corretivas em tempo útil, todos os fornecedores devem dispor de um sistema de acompanhamento pós-comercialização. Este sistema também é fundamental para assegurar uma resolução mais eficaz e atempada dos eventuais riscos decorrentes dos sistemas de IA que continuam a «aprender» depois de terem sido colocados no mercado ou em serviço. Neste contexto, os fornecedores devem ainda ser obrigados a introduzir um sistema para comunicar às autoridades competentes quaisquer incidentes graves ou violações do direito nacional e da União que protege os direitos fundamentais resultantes da utilização dos sistemas de IA que fornecem.

(79) Para assegurar uma execução adequada e eficaz dos requisitos e das obrigações estabelecidas no presente regulamento, que faz parte da legislação de harmonização da União, o sistema de fiscalização do mercado e de conformidade dos produtos estabelecido no Regulamento (UE) 2019/1020 deve ser aplicado na íntegra. Quando tal for necessário ao cumprimento do seu mandato, as autoridades públicas ou os organismos nacionais que supervisionam a aplicação do direito da União que protege

direitos fundamentais, incluindo os organismos de promoção da igualdade, também devem ter acesso à documentação elaborada por força do presente regulamento.

(80) A legislação da União em matéria de serviços financeiros inclui regras e requisitos relativos à governação interna e à gestão dos riscos aplicáveis às instituições financeiras regulamentadas durante a prestação desses serviços, incluindo quando estas utilizam sistemas de IA. Para assegurar a coerência na aplicação e na execução das obrigações previstas no presente regulamento e das regras e requisitos da legislação da União aplicáveis aos serviços financeiros, as autoridades responsáveis pela supervisão e execução da legislação no domínio dos serviços financeiros, incluindo, se for caso disso, o Banco Central Europeu, devem ser designadas autoridades competentes para efeitos de supervisão da aplicação do presente regulamento, incluindo o exercício de funções de fiscalização do mercado, no que diz respeito aos sistemas de IA fornecidos ou utilizados por instituições financeiras regulamentadas e supervisionadas. A fim de reforçar a coerência entre o presente regulamento e as regras aplicáveis às instituições de crédito regulamentadas pela Diretiva 2013/36/UE do Parlamento Europeu e do Conselho[56], também é apropriado integrar o procedimento de avaliação da conformidade e algumas das obrigações processuais dos fornecedores relativas à gestão de riscos, ao acompanhamento pós-comercialização e à documentação nas obrigações e procedimentos em vigor por força da mesma diretiva. No intuito de evitar sobreposições, também devem ser previstas derrogações limitadas no respeitante ao sistema de gestão da qualidade dos fornecedores e à obrigação de controlo imposta aos utilizadores de sistemas de IA de risco elevado, contanto que tal se aplique a instituições de crédito regulamentadas pela Diretiva 2013/36/UE.

(81) O desenvolvimento de outros sistemas de IA, que não sejam sistemas de IA de risco elevado, de acordo com os requisitos do presente regulamento pode conduzir a uma maior utilização de inteligência artificial fiável na União. Os fornecedores de sistemas de IA que não são de risco elevado devem ser incentivados a criar códigos de conduta que visem promover a aplicação voluntária dos requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado. Os fornecedores devem ainda ser incentivados a aplicar voluntariamente requisitos adicionais relacionados, por exemplo, com a sustentabilidade ambiental, a acessibilidade das pessoas com deficiência, a participação das partes interessadas na conceção e no desenvolvimento de sistemas de IA e a diversidade das equipas de desenvolvimento. A Comissão pode desenvolver iniciativas, incluindo de natureza setorial, para facilitar a redução de obstáculos técnicos que impeçam o intercâmbio transfronteiras de dados para o desenvolvimento da inteligência artificial, incluindo em matéria de infraestruturas de acesso aos dados e de interoperabilidade semântica e técnica de diferentes tipos de dados.

(82) Não obstante, é importante que os sistemas de IA relacionados com produtos que não são de risco elevado, nos termos do presente regulamento, e que, como tal, não são obrigados a cumprir os requisitos do mesmo, sejam seguros quando são colocados no mercado ou em serviço. A fim de contribuir para alcançar esse objetivo, a

[56] Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito e empresas de investimento, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176 de 27.6.2013, p. 338).

Diretiva 2001/95/CE do Parlamento Europeu e do Conselho[57] será aplicada como uma rede de segurança.

(83) Para assegurar uma cooperação de confiança e construtiva entre as autoridades competentes a nível da União e nacional, todas as partes envolvidas na aplicação do presente regulamento devem respeitar a confidencialidade das informações e dos dados obtidos no exercício das suas funções.

(84) Os Estados-Membros devem tomar todas as medidas necessárias para assegurar a aplicação das disposições do presente regulamento, inclusive estabelecendo sanções efetivas, proporcionadas e dissuasivas aplicáveis à sua violação. No caso de determinadas violações específicas, os Estados-Membros devem ter em conta as margens e os critérios estabelecidos no presente regulamento. A Autoridade Europeia para a Proteção de Dados deve ter competências para impor coimas às instituições, órgãos e organismos da União que se enquadram no âmbito do presente regulamento.

(85) Para assegurar que é possível adaptar o quadro regulamentar quando necessário, o poder de adotar atos nos termos do artigo 290.º do TFUE deve ser delegado na Comissão no que diz respeito à alteração das técnicas e abordagens que definem sistemas de IA mencionadas no anexo I, da legislação de harmonização da União enumerada no anexo II, da lista de sistemas de IA de risco elevado constante do anexo III, das disposições relativas à documentação técnica que constam do anexo IV, do conteúdo da declaração de conformidade UE estabelecido no anexo V, das disposições relativas aos procedimentos de avaliação da conformidade que constam dos anexos VI e VII e das disposições que definem os sistemas de IA de risco elevado aos quais se deve aplicar o procedimento de avaliação da conformidade com base na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica. É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor[58]. Em particular, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados.

(86) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão. Essas competências deverão ser exercidas nos termos do Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho[59].

(87) Atendendo a que o objetivo do presente regulamento não pode ser suficientemente alcançado pelos Estados-Membros e pode, devido à dimensão ou aos efeitos da ação, ser mais bem alcançado ao nível da União, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do TUE.

---

57 Diretiva 2001/95/CE do Parlamento Europeu e do Conselho, de 3 de dezembro de 2001, relativa à segurança geral dos produtos (JO L 11 de 15.1.2002, p. 4).

58 JO L 123 de 12.5.2016, p. 1.

59 Regulamento (UE) n.º 182/2011 do Parlamento Europeu e do Conselho, de 16 de fevereiro de 2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controlo pelos Estados-Membros do exercício das competências de execução pela Comissão (JO L 55 de 28.2.2011, p. 13).

Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para atingir aquele objetivo.

(88) O presente regulamento deve aplicar-se a partir de … [*Serviço das Publicações: inserir a data estabelecida no artigo 85.º*]. Contudo, as estruturas relacionadas com a governação e o sistema de avaliação da conformidade devem estar operacionais antes dessa data, pelo que as disposições relativas aos organismos notificados e à estrutura de governação devem aplicar-se a partir de … [*Serviço das Publicações: inserir a data correspondente a três meses a contar da data de entrada em vigor do presente regulamento*]. Além disso, os Estados-Membros devem estabelecer as regras em matéria de sanções, incluindo coimas, e notificá-las à Comissão, bem como assegurar que sejam aplicadas de forma efetiva e adequada à data de aplicação do presente regulamento. Como tal, as disposições relativas às sanções devem aplicar-se a partir de … [*Serviço das Publicações: inserir a data correspondente a doze meses a contar da data de entrada em vigor do presente regulamento*].

(89) A Autoridade Europeia para a Proteção de Dados e o Comité Europeu para a Proteção de Dados foram consultados nos termos do artigo 42.º, n.º 2, do Regulamento (UE) 2018/1725, e emitiram parecer em […],

ADOTARAM O PRESENTE REGULAMENTO:

TÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º
Objeto

O presente regulamento estabelece:

a) Regras harmonizadas para a colocação no mercado, a colocação em serviço e a utilização de sistemas de inteligência artificial («sistemas de IA») na União;

b) Proibições de certas práticas de inteligência artificial;

c) Requisitos específicos para sistemas de IA de risco elevado e obrigações para os operadores desses sistemas;

d) Regras de transparência harmonizadas para sistemas de IA concebidos para interagir com pessoas singulares, sistemas de reconhecimento de emoções e sistemas de categorização biométrica, bem como para sistemas de IA usados para gerar ou manipular conteúdos de imagem, áudio ou vídeo;

e) Regras relativas à fiscalização e vigilância do mercado.

Artigo 2.º
Âmbito

1. O presente regulamento é aplicável a:

a) Fornecedores que coloquem no mercado ou coloquem em serviço sistemas de IA no território da União, independentemente de estarem estabelecidos na União ou num país terceiro;

b) Utilizadores de sistemas de IA localizados na União;

c) Fornecedores e utilizadores de sistemas de IA localizados num país terceiro, se o resultado produzido pelo sistema for utilizado na União.

2. Aos sistemas de IA de risco elevado que são componentes de segurança de produtos ou sistemas ou que são, eles próprios, produtos ou sistemas abrangidos pelo âmbito dos atos a seguir enumerados, apenas é aplicável o artigo 84.º do presente regulamento:

a) Regulamento (CE) n.º 300/2008;

b) Regulamento (UE) n.º 167/2013;

c) Regulamento (UE) n.º 168/2013;

d) Diretiva 2014/90/UE;

e) Diretiva (UE) 2016/797;

f) Regulamento (UE) 2018/858;

g) Regulamento (UE) 2018/1139;

h) Regulamento (UE) 2019/2144.

3. O presente regulamento não se aplica aos sistemas de IA desenvolvidos ou usados exclusivamente para fins militares.

4. O presente regulamento não se aplica a autoridades públicas de países terceiros, nem a organizações internacionais abrangidas pelo âmbito do presente regulamento nos termos do n.º 1, quando essas autoridades ou organizações usem sistemas de IA no âmbito de acordos internacionais para efeitos de cooperação policial e judiciária com a União ou com um ou vários Estados-Membros.

5. O presente regulamento não afeta a aplicação das disposições relativas à responsabilidade dos prestadores intermediários de serviços estabelecidas no capítulo II, secção IV, da Diretiva 2000/31/CE do Parlamento Europeu e do Conselho[60] [*a substituir pelas disposições correspondentes do Regulamento Serviços Digitais*].

Artigo 3.º
Definições

Para efeitos do presente regulamento, entende-se por:

1) «Sistema de inteligência artificial» (sistema de IA), um programa informático desenvolvido com uma ou várias das técnicas e abordagens enumeradas no anexo I, capaz de, tendo em vista um determinado conjunto de objetivos definidos por seres humanos, criar resultados, tais como conteúdos, previsões, recomendações ou decisões, que influenciam os ambientes com os quais interage;

2) «Fornecedor», uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que desenvolva um sistema de IA ou que tenha um sistema de IA desenvolvido com vista à sua colocação no mercado ou colocação em serviço sob o seu próprio nome ou marca, a título oneroso ou gratuito;

[60] Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, relativa a certos aspetos legais dos serviços da sociedade da informação, em especial do comércio eletrónico, no mercado interno («Diretiva sobre o comércio eletrónico») (JO L 178 de 17.7.2000, p. 1).

3) «Fornecedor de pequena dimensão», um fornecedor que seja uma micro ou pequena empresa na aceção da Recomendação 2003/361/CE da Comissão[61];

4) «Utilizador», uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que utilize, sob a sua autoridade, um sistema de IA, salvo se o sistema de IA for utilizado no âmbito de uma atividade pessoal de caráter não profissional;

5) «Mandatário», uma pessoa singular ou coletiva estabelecida na União que tenha recebido um mandato escrito de um fornecedor de um sistema de IA para, respetivamente, executar e cumprir em seu nome as obrigações e os procedimentos previstos no presente regulamento;

6) «Importador», uma pessoa singular ou coletiva estabelecida na União que coloca no mercado ou coloca em serviço um sistema de IA que ostenta o nome ou a marca de uma pessoa singular ou coletiva estabelecida fora da União;

7) «Distribuidor», uma pessoa singular ou coletiva inserida na cadeia de abastecimento, distinta do fornecedor e do importador, que disponibiliza um sistema de IA no mercado da União sem alterar as suas propriedades;

8) «Operador», um fornecedor, utilizador, mandatário, importador ou distribuidor;

9) «Colocação no mercado», a primeira disponibilização de um sistema de IA no mercado da União;

10) «Disponibilização no mercado», o fornecimento de um sistema de IA para distribuição ou utilização no mercado da União no âmbito de uma atividade comercial, a título oneroso ou gratuito;

11) «Colocação em serviço», o fornecimento de um sistema de IA para a primeira utilização no mercado da União, diretamente ao utilizador ou para utilização própria, para a finalidade prevista;

12) «Finalidade prevista», a utilização à qual o fornecedor destina o sistema de IA, incluindo o contexto específico e as condições de utilização, conforme especificado nas informações facultadas pelo fornecedor nas instruções de utilização, nos materiais e declarações promocionais ou de venda, bem como na documentação técnica;

13) «Utilização indevida razoavelmente previsível», a utilização de um sistema de IA de uma forma não conforme com a sua finalidade prevista, mas que pode resultar de comportamentos humanos ou de interações com outros sistemas razoavelmente previsíveis;

14) «Componente de segurança de um produto ou sistema», um componente de um produto ou sistema que cumpre uma função de segurança nesse produto ou sistema ou cuja falha ou anomalia põe em risco a segurança e a saúde de pessoas ou bens;

15) «Instruções de utilização», as informações facultadas pelo fornecedor para esclarecer o utilizador, em especial, sobre a finalidade prevista e a utilização correta de um sistema de IA, incluindo o enquadramento geográfico, comportamental ou funcional específico no qual o sistema de IA de risco elevado se destina a ser utilizado;

---

61 Recomendação da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).

16) «Recolha de um sistema de IA», qualquer medida que vise obter a devolução ao fornecedor de um sistema de IA disponibilizado a utilizadores;

17) «Retirada de um sistema de IA», qualquer medida que vise impedir a distribuição, apresentação ou oferta de um sistema de IA;

18) «Desempenho de um sistema de IA», a capacidade de um sistema de IA para alcançar a sua finalidade prevista;

19) «Autoridade notificadora», a autoridade nacional responsável por estabelecer e executar os procedimentos necessários para a avaliação, designação e notificação de organismos de avaliação da conformidade e pela fiscalização destes;

20) «Avaliação da conformidade», o processo de verificar se estão preenchidos os requisitos estabelecidos no título III, capítulo 2, do presente regulamento relacionados com um sistema de IA;

21) «Organismo de avaliação da conformidade», um organismo que realiza atividades de avaliação da conformidade por terceiros, nomeadamente testagem, certificação e inspeção;

22) «Organismo notificado», um organismo de avaliação da conformidade designado nos termos do presente regulamento ou de outra legislação de harmonização da União aplicável;

23) «Modificação substancial», uma alteração do sistema de IA após a sua colocação no mercado ou colocação em serviço que afeta a conformidade do sistema de IA com os requisitos estabelecidos no título III, capítulo 2, do presente regulamento ou conduz a uma modificação da finalidade prevista relativamente à qual o sistema de IA foi avaliado;

24) «Marcação de conformidade CE» (marcação CE), a marcação pela qual um fornecedor atesta que um sistema de IA está em conformidade com os requisitos estabelecidos no título III, capítulo 2, do presente regulamento e na restante legislação da União aplicável que harmoniza as condições de comercialização de produtos («legislação de harmonização da União») em que seja prevista a respetiva aposição;

25) «Acompanhamento pós-comercialização», todas as atividades que os fornecedores de sistemas de IA empreendem para recolher e analisar proativamente dados sobre a experiência adquirida com a utilização de sistemas de IA que colocaram no mercado ou em serviço, com vista a identificar a eventual necessidade de aplicar imediatamente quaisquer medidas corretivas ou preventivas necessárias;

26) «Autoridade de fiscalização do mercado», a autoridade nacional que realiza as atividades e toma medidas nos previstas no Regulamento (UE) 2019/1020;

27) «Norma harmonizada», uma norma europeia, na aceção do artigo 2.º, n.º 1, alínea c), do Regulamento (UE) n.º 1025/2012;

28) «Especificações comuns», um documento, que não uma norma, que contém soluções técnicas que proporcionam um meio para cumprir certos requisitos e obrigações estabelecidas no presente regulamento;

29) «Dados de treino», os dados usados para treinar um sistema de IA mediante o ajustamento dos seus parâmetros passíveis de serem aprendidos, incluindo os pesos de uma rede neuronal;

30) «Dados de validação», os dados utilizados para realizar uma avaliação do sistema de IA treinado e para ajustar os seus parâmetros não passíveis de serem aprendidos e o seu processo de aprendizagem, a fim de, entre outros objetivos, evitar um sobreajustamento; sendo que o conjunto de dados de validação pode ser um conjunto de dados separado ou parte de um conjunto de dados de treino, quer como divisão fixa ou variável;

31) «Dados de teste», os dados utilizados para realizar uma avaliação independente do sistema de IA treinado e validado, a fim de confirmar o desempenho esperado desse sistema antes de ser colocado no mercado ou em serviço;

32) «Dados de entrada», os dados fornecidos a um sistema de IA, ou por ele obtidos diretamente, com base nos quais o sistema produz um resultado;

33) «Dados biométricos», dados pessoais resultantes de um tratamento técnico específico das características físicas, fisiológicas ou comportamentais de uma pessoa singular, os quais permitem obter ou confirmar a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;

34) «Sistema de reconhecimento de emoções», um sistema de IA concebido para identificar ou inferir emoções ou intenções de pessoas singulares com base nos seus dados biométricos;

35) «Sistema de categorização biométrica», um sistema de IA concebido para classificar pessoas singulares em categorias específicas, tais como sexo, idade, cor do cabelo, cor dos olhos, tatuagens, origem étnica ou orientação sexual ou política, com base nos seus dados biométricos;

36) «Sistema de identificação biométrica à distância», um sistema de IA concebido para identificar pessoas singulares à distância por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência, sem que o utilizador do sistema de IA saiba antecipadamente se a pessoa em causa estará presente e pode ser identificada;

37) «Sistema de identificação biométrica à distância "em tempo real"», um sistema de identificação biométrica à distância em que a recolha de dados biométricos, a comparação e a identificação ocorrem sem atraso significativo. Para evitar que as regras sejam contornadas, tal inclui não apenas a identificação instantânea, mas também a identificação com ligeiro atraso;

38) «Sistema de identificação biométrica à distância "em diferido"», um sistema de identificação biométrica à distância que não seja um sistema de identificação biométrica à distância em «tempo real»;

39) «Espaço acessível ao público», qualquer espaço físico aberto ao público, independentemente da eventual aplicação de condições de acesso específicas;

40) «Autoridade policial»:

a) Uma autoridade pública competente para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas; ou

b) Qualquer outro organismo ou entidade designados pelo direito de um Estado-Membro para exercer autoridade pública e poderes públicos para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou

execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas;

41) «Manutenção da ordem pública», as atividades realizadas por autoridades policiais para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas;

42) «Autoridade nacional de controlo», a autoridade à qual um Estado-Membro atribui a responsabilidade pela execução e aplicação do presente regulamento, pela coordenação das atividades confiadas a esse Estado-Membro, por atuar como ponto de contacto único para a Comissão e por representar o Estado-Membro no Comité Europeu para a Inteligência Artificial;

43) «Autoridade nacional competente», a autoridade de controlo, a autoridade notificadora ou a autoridade de fiscalização do mercado designadas a nível nacional;

44) «Incidente grave», qualquer incidente que, direta ou indiretamente, tenha, poderia ter tido ou possa vir a ter alguma das seguintes consequências:

a) A morte de uma pessoa ou danos graves para a saúde de uma pessoa, bens, ou o ambiente,

b) Uma perturbação grave e irreversível da gestão e do funcionamento de uma infraestrutura crítica.

Artigo 4.º
Alterações do anexo I

A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para alterar a lista de técnicas e abordagens enumeradas no anexo I, a fim de a atualizar face à evolução do mercado e da tecnologia com base em características similares às técnicas e abordagens constantes da lista.

TÍTULO II

PRÁTICAS DE INTELIGÊNCIA ARTIFICIAL PROIBIDAS

Artigo 5.º

1. Estão proibidas as seguintes práticas de inteligência artificial:

a) A colocação no mercado, a colocação em serviço ou a utilização de um sistema de IA que empregue técnicas subliminares que contornem a consciência de uma pessoa para distorcer substancialmente o seu comportamento de uma forma que cause ou seja suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa;

b) A colocação no mercado, a colocação em serviço ou a utilização de um sistema de IA que explore quaisquer vulnerabilidades de um grupo específico de pessoas associadas à sua idade ou deficiência física ou mental, a fim de distorcer substancialmente o comportamento de uma pessoa pertencente a esse grupo de uma forma que cause ou seja suscetível de causar danos físicos ou psicológicos a essa ou a outra pessoa;

c) A colocação no mercado, a colocação em serviço ou a utilização de sistemas de IA por autoridades públicas ou em seu nome para efeitos de avaliação ou classificação da credibilidade de pessoas singulares durante um certo período com base no seu comportamento social ou em características de personalidade ou pessoais, conhecidas ou previsíveis, em que a classificação social conduz a uma das seguintes situações ou a ambas:

i) tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas em contextos sociais não relacionados com os contextos nos quais os dados foram originalmente gerados ou recolhidos,

ii) tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos inteiros das mesmas que é injustificado e desproporcionado face ao seu comportamento social ou à gravidade do mesmo;

d) A utilização de sistemas de identificação biométrica à distância em «tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública, salvo se essa utilização for estritamente necessária para alcançar um dos seguintes objetivos:

i) a investigação seletiva de potenciais vítimas específicas de crimes, nomeadamente crianças desaparecidas,

ii) a prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de um ataque terrorista,

iii) a deteção, localização, identificação ou instauração de ação penal relativamente a um infrator ou suspeito de uma infração penal referida no artigo 2.º, n.º 2, da Decisão-Quadro 2002/584/JAI do Conselho[62] e punível no Estado-Membro em causa com pena ou medida de segurança privativas de liberdade de duração máxima não inferior a três anos e tal como definidas pela legislação desse Estado-Membro.

2. A utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d), deve ter em conta os seguintes elementos:

a) A natureza da situação que origina a possível utilização, em especial a gravidade, a probabilidade e a magnitude dos prejuízos causados na ausência da utilização do sistema;

b) As consequências da utilização do sistema para os direitos e as liberdades de todas as pessoas afetadas, em especial a gravidade, a probabilidade e a magnitude dessas consequências.

Além disso, a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública que vise alcançar um dos objetivos referidos no n.º 1, alínea d), deve observar salvaguardas e condições necessárias e proporcionadas em relação a tal

[62] Decisão-quadro 2002/584/JAI do Conselho, de 13 de junho de 2002, relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros (JO L 190 de 18.7.2002, p. 1).

utilização, nomeadamente no respeitante a limitações temporais, geográficas e das pessoas visadas.

3. No tocante ao n.º 1, alínea d), e ao n.º 2, cada utilização específica de um sistema de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública está sujeita a autorização prévia concedida por uma autoridade judiciária ou por uma autoridade administrativa independente do Estado-Membro no qual a utilização terá lugar após apresentação de um pedido fundamentado em conformidade com as regras de execução previstas no direito nacional a que se refere o n.º 4. Contudo, numa situação de urgência devidamente justificada, a utilização do sistema pode ser iniciada sem uma autorização e esta pode ser solicitada apenas durante ou após a utilização.

   A autoridade judiciária ou administrativa competente apenas deve conceder a autorização se considerar, com base em dados objetivos ou indícios claros que lhe tenham sido apresentados, que a utilização do sistema de identificação biométrica à distância «em tempo real» em apreço é necessária e proporcionada para alcançar um dos objetivos especificados no n.º 1, alínea d), conforme identificado no pedido. Ao decidir sobre o pedido, a autoridade judiciária ou administrativa competente tem em conta os elementos referidos no n.º 2.

4. Um Estado-Membro pode decidir prever a possibilidade de autorizar total ou parcialmente a utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública dentro dos limites e sob as condições enumeradas no n.º 1, alínea d), e nos n.os 2 e 3. Esse Estado-Membro estabelece na sua legislação nacional as regras pormenorizadas aplicáveis ao pedido, à emissão e ao exercício das autorizações a que se refere o n.º 3, bem como à supervisão das mesmas. Essas regras especificam igualmente em relação a que objetivos enumerados no n.º 1, alínea d), incluindo quais das infrações penais referidas na subalínea iii) da mesma, as autoridades competentes podem ser autorizadas a usar esses sistemas para efeitos de manutenção da ordem pública.

TÍTULO III

SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO

CAPÍTULO 1

CLASSIFICAÇÃO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL COMO SENDO DE RISCO ELEVADO

Artigo 6.º

Regras para a classificação de sistemas de inteligência artificial de risco elevado

1. Independentemente de a colocação no mercado ou a colocação em serviço de um sistema de IA ser feita separadamente dos produtos a que se referem as alíneas a) e b), esse sistema de IA é considerado de risco elevado quando estejam satisfeitas ambas as condições que se seguem:

a) O sistema de IA destina-se a ser utilizado como um componente de segurança de um produto ou é, ele próprio, um produto abrangido pela legislação de harmonização da União enumerada no anexo II;

b) Nos termos da legislação de harmonização da União enumerada no anexo II, o produto cujo componente de segurança é o sistema de IA, ou o próprio sistema de IA enquanto produto deve ser sujeito a uma avaliação da conformidade por terceiros com vista à colocação no mercado ou à colocação em serviço.

2. Além dos sistemas de IA de risco elevado referidos no n.º 1, os sistemas de IA referidos no anexo III são também considerados de risco elevado.

Artigo 7.º
Alterações do anexo III

1. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para atualizar a lista do anexo III, aditando sistemas de IA de risco elevado que preencham ambas as condições que se seguem:

a) Os sistemas de IA destinam-se a ser utilizados em qualquer um dos domínios enumerados no anexo III, pontos 1 a 8;

b) Os sistemas de IA representam um risco de danos para a saúde e a segurança ou um risco de impacto adverso nos direitos fundamentais que, em termos de gravidade e probabilidade de ocorrência, é equivalente ou superior ao risco de danos ou impacto adverso representado pelos sistemas de IA de risco elevado já referidos no anexo III.

2. Ao avaliar, para efeitos do disposto no n.º 1, se um sistema de IA representa um risco de danos para a saúde e a segurança ou um risco de impacto adverso nos direitos fundamentais equivalente ou superior ao risco de danos representado pelos sistemas de IA de risco elevado já referidos no anexo III, a Comissão tem em consideração os seguintes critérios:

a) A finalidade prevista do sistema de IA;

b) O grau de utilização efetiva ou a probabilidade de utilização de um sistema de IA;

c) Em que medida a utilização de um sistema de IA já causou danos para a saúde e a segurança ou um impacto adverso nos direitos fundamentais ou suscitou preocupações significativas quanto à concretização desses danos ou desse impacto adverso, conforme demonstrado por relatórios ou alegações documentadas apresentadas às autoridades nacionais competentes;

d) O potencial grau desses danos ou desse impacto adverso, nomeadamente em termos de intensidade e de capacidade para afetar um grande número de pessoas;

e) O grau de dependência das pessoas potencialmente lesadas ou adversamente afetadas em relação ao resultado produzido por um sistema de IA, em especial se, por razões práticas ou jurídicas, aquelas não puderem razoavelmente autoexcluir-se desse resultado;

f) A posição de vulnerabilidade das pessoas potencialmente prejudicadas ou adversamente afetadas em relação ao utilizador de um sistema de IA,

nomeadamente devido a um desequilíbrio de poder ou de conhecimento, a circunstâncias económicas ou sociais, ou à idade;

g) A facilidade de reversão do resultado produzido com um sistema de IA, tendo em conta que os resultados com impacto na saúde ou na segurança das pessoas não podem ser considerados como facilmente reversíveis;

h) Em que medida a legislação da União em vigor prevê:

i) medidas de reparação eficazes em relação aos riscos representados por um sistema de IA, com exclusão de pedidos de indemnização,

ii) medidas eficazes para prevenir ou minimizar substancialmente esses riscos.

CAPÍTULO 2

REQUISITOS APLICÁVEIS A SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO

Artigo 8.º
Cumprimento dos requisitos

1. Os sistemas de IA de risco elevado devem cumprir os requisitos estabelecidos neste capítulo.

2. A finalidade prevista do sistema de IA de risco elevado e o sistema de gestão de riscos a que se refere o artigo 9.º devem ser tidos em conta para efeitos do cumprimento desses requisitos.

Artigo 9.º
Sistema de gestão de riscos

1. Deve ser criado, implantado, documentado e mantido um sistema de gestão de riscos em relação a sistemas de IA de risco elevado.

2. O sistema de gestão de riscos deve consistir num processo iterativo contínuo, executado ao longo de todo o ciclo de vida de um sistema de IA de risco elevado, o que requer atualizações regulares sistemáticas. Deve compreender as seguintes etapas:

a) Identificação e análise dos riscos conhecidos e previsíveis associados a cada sistema de IA de risco elevado;

b) Estimativa e avaliação de riscos que podem surgir quando o sistema de IA de risco elevado é usado em conformidade com a sua finalidade prevista e em condições de utilização indevida razoavelmente previsíveis;

c) Avaliação de outros riscos que possam surgir, baseada na análise dos dados recolhidos a partir do sistema de acompanhamento pós-comercialização a que se refere o artigo 61.º;

d) Adoção de medidas de gestão de riscos adequadas em conformidade com o disposto nos números que se seguem.

3. As medidas de gestão de riscos a que se refere o n.º 2, alínea d), devem ter em devida consideração os efeitos e eventuais interações resultantes da aplicação combinada

dos requisitos estabelecidos no presente capítulo. Devem também ter em conta o estado da técnica geralmente reconhecido, incluindo o que se encontrar refletido em normas harmonizadas ou especificações comuns pertinentes.

4. As medidas de gestão de riscos a que se refere o n.º 2, alínea d), devem levar a que o eventual risco residual associado a cada perigo, bem como o risco residual global dos sistemas de IA de risco elevado, sejam considerados aceitáveis, contanto que o sistema de IA de risco elevado seja usado em conformidade com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsíveis. Os riscos residuais devem ser comunicados ao utilizador.

   Ao identificar as medidas de gestão de riscos mais apropriadas, deve assegurar-se o seguinte:

   a) Eliminação ou redução de riscos tanto quanto possível, graças a processos de conceção e desenvolvimento adequados;

   b) Se for caso disso, adoção de medidas de atenuação e controlo adequadas em relação a riscos que não possam ser eliminados;

   c) Prestação de informações adequadas nos termos do artigo 13.º, em especial no atinente aos riscos a que se refere o n.º 2, alínea b), do presente artigo e, se for caso disso, formação dos utilizadores.

   Na eliminação ou redução de riscos relacionados com a utilização do sistema de IA de risco elevado, há que ter em consideração o conhecimento técnico, a experiência, a educação e a formação que se pode esperar que o utilizador possua e o ambiente em que está previsto utilizar o sistema.

5. Os sistemas de IA de risco elevado devem ser sujeitos a testes para que se identifiquem as medidas de gestão de riscos mais apropriadas. Os testes asseguram que os sistemas de IA de risco elevado tenham um desempenho coerente com a finalidade prevista e que cumpram os requisitos estabelecidos no presente capítulo.

6. Os procedimentos de teste são adequados para alcançar a finalidade prevista do sistema de IA e não precisam de ir além do necessário para alcançar essa finalidade.

7. Os testes dos sistemas de IA de risco elevado devem ser realizados, consoante apropriado, em qualquer momento durante o processo de desenvolvimento e, em qualquer caso, antes da colocação no mercado ou da colocação em serviço. Os testes devem ser realizados relativamente a métricas previamente definidas e a limiares probabilísticos que são apropriados para a finalidade prevista do sistema de IA de risco elevado.

8. Ao implantar o sistema de gestão de riscos descrito nos n.os 1 a 7, deve tomar-se especificamente em conta se o sistema de IA de risco elevado é suscetível de ser acedido por crianças ou de ter impacto nas mesmas.

9. Em relação às instituições de crédito regulamentadas pela Diretiva 2013/36/UE, os aspetos descritos nos n.os 1 a 8 fazem parte dos procedimentos de gestão de riscos estabelecidos por essas instituições nos termos do artigo 74.º da referida diretiva.

Artigo 10.º
Dados e governação de dados

1. Os sistemas de IA de risco elevado que utilizem técnicas que envolvam o treino de modelos com dados devem ser desenvolvidos com base em conjuntos de dados de

treino, validação e teste que cumpram os critérios de qualidade referidos nos n.os 2 a 5.

2. Os conjuntos de dados de treino, validação e teste devem estar sujeitos a práticas adequadas de governação e gestão de dados. Essas práticas dizem nomeadamente respeito:

   a) Às escolhas de conceção tomadas;

   b) À recolha de dados;

   c) Às operações de preparação e tratamento de dados necessárias, tais como anotação, rotulagem, limpeza, enriquecimento e agregação;

   d) À formulação dos pressupostos aplicáveis, nomeadamente no que diz respeito às informações que os dados devem medir e representar;

   e) À avaliação prévia da disponibilidade, quantidade e adequação dos conjuntos de dados que são necessários;

   f) Ao exame para detetar eventuais enviesamentos;

   g) À identificação de eventuais lacunas ou deficiências de dados e de possíveis soluções para as mesmas.

3. Os conjuntos de dados de treino, validação e teste devem ser pertinentes, representativos, isentos de erros e completos. Devem ter as propriedades estatísticas adequadas, nomeadamente, quando aplicável, no tocante às pessoas ou grupos de pessoas em que o sistema de IA de risco elevado se destina a ser utilizado. Estas características dos conjuntos de dados podem ser satisfeitas a nível de conjuntos de dados individuais ou de uma combinação dos mesmos.

4. Os conjuntos de dados de treino, validação e teste devem ter em conta, na medida do necessário para a finalidade prevista, as características ou os elementos que são idiossincráticos do enquadramento geográfico, comportamental ou funcional específico no qual o sistema de IA de risco elevado se destina a ser utilizado.

5. Na medida do estritamente necessário para assegurar o controlo, a deteção e a correção de enviesamentos em relação a sistemas de IA de risco elevado, os fornecedores desses sistemas podem tratar categorias especiais de dados pessoais a que se refere o artigo 9.º, n.º 1, do Regulamento (UE) 2016/679, o artigo 10.º da Diretiva (UE) 2016/680 e o artigo 10.º, n.º 1, do Regulamento (UE) 2018/1725, assegurando salvaguardas adequadas dos direitos fundamentais e liberdades das pessoas singulares, incluindo impor limitações técnicas à reutilização e utilizar medidas de segurança e preservação da privacidade de última geração, tais como a pseudonimização ou a cifragem nos casos em que a anonimização possa afetar significativamente a finalidade preconizada.

6. Devem ser aplicadas práticas adequadas de governação e gestão de dados ao desenvolvimento de sistemas de IA de risco elevado que não utilizam técnicas que envolvem o treino de modelos, para assegurar que esses sistemas de IA de risco elevado cumprem o disposto no n.º 2.

Artigo 11.º
Documentação técnica

1. A documentação técnica de um sistema de IA de risco elevado deve ser elaborada antes da colocação no mercado ou colocação em serviço desse sistema e mantida atualizada.

   A documentação técnica deve ser elaborada de maneira que demonstre que o sistema de IA de risco elevado cumpre os requisitos estabelecidos no presente capítulo e deve facultar às autoridades nacionais competentes e aos organismos notificados todas as informações necessárias para aferir a conformidade do sistema de IA com esses requisitos. A documentação técnica deve conter, no mínimo, os elementos previstos no anexo IV.

2. Caso um sistema de IA de risco elevado relacionado com um produto, ao qual sejam aplicáveis os atos jurídicos enumerados no anexo II, secção A, seja colocado no mercado ou colocado em serviço, deve ser elaborada uma única documentação técnica que contenha todas as informações enumeradas no anexo IV e as informações exigidas nos termos desses atos jurídicos.

3. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para alterar o anexo IV, se for caso disso, com vista a assegurar que, tendo em conta a evolução técnica, a documentação técnica forneça todas as informações necessárias para aferir a conformidade do sistema com os requisitos estabelecidos no presente capítulo.

Artigo 12.º
Manutenção de registos

1. Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos com capacidades que permitam o registo automático de eventos («registos») enquanto o sistema de IA de risco elevado estiver em funcionamento. Essas capacidades de registo devem estar em conformidade com normas reconhecidas ou especificações comuns.

2. As capacidades de registo devem assegurar um nível de rastreabilidade do funcionamento do sistema de IA ao longo do seu ciclo de vida que seja adequado à finalidade prevista do sistema.

3. Em especial, as capacidades de registo devem permitir o controlo do funcionamento do sistema de IA de risco elevado no que diz respeito à ocorrência de situações que possam dar azo a que o sistema de IA apresente um risco na aceção do artigo 65.º, n.º 1, ou dar origem a uma modificação substancial, e facilitar o acompanhamento pós-comercialização a que se refere o artigo 61.º.

4. Em relação aos sistemas de IA de risco elevado a que se refere o anexo III, ponto 1, alínea a), as capacidades de registo devem proporcionar, no mínimo:

   a) O registo do período de cada utilização do sistema (data e hora de início e data e hora de fim de cada utilização);

   b) A base de dados de referência relativamente à qual os dados de entrada foram verificados pelo sistema;

   c) Os dados de entrada cuja pesquisa conduziu a uma correspondência;

d) A identificação das pessoas singulares envolvidas na verificação dos resultados, conforme referido no artigo 14.º, n.º 5.

Artigo 13.º
Transparência e prestação de informações aos utilizadores

1. Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que assegure que o seu funcionamento seja suficientemente transparente para permitir aos utilizadores interpretar o resultado do sistema e utilizá-lo corretamente. Deve ser garantido um tipo e um grau adequado de transparência, que permita cumprir as obrigações que incumbem ao utilizador e ao fornecedor por força do capítulo 3 do presente título.

2. Os sistemas de IA de risco elevado devem ser acompanhados de instruções de utilização, num formato digital ou outro adequado, que incluam informações concisas, completas, corretas e claras que sejam pertinentes, acessíveis e compreensíveis para os utilizadores.

3. As informações a que se refere o n.º 2 devem especificar:

   a) A identidade e os dados de contacto do fornecedor e, se for caso disso, do seu mandatário;

   b) As características, capacidades e limitações de desempenho do sistema de IA de risco elevado, incluindo:

      i) a finalidade prevista do sistema,

      ii) o nível de exatidão, solidez e cibersegurança a que se refere o artigo 15.º relativamente ao qual o sistema de IA de risco elevado foi testado e validado e que pode ser esperado, bem como quaisquer circunstâncias conhecidas e previsíveis que possam ter um impacto nesse nível esperado de exatidão, solidez e cibersegurança,

      iii) qualquer circunstância conhecida ou previsível, relacionada com a utilização do sistema de IA de risco elevado de acordo com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsíveis, que possa causar riscos para a saúde e a segurança ou os direitos fundamentais,

      iv) o desempenho do sistema no tocante às pessoas ou grupos de pessoas em que o sistema se destina a ser utilizado,

      v) quando oportuno, especificações para os dados de entrada, ou quaisquer outras informações importantes em termos dos conjuntos de dados de treino, validação e teste usados, tendo em conta a finalidade prevista do sistema de IA;

   c) As alterações do sistema de IA de risco elevado e do seu desempenho que foram predeterminadas pelo fornecedor aquando da avaliação da conformidade inicial, se for caso disso;

   d) As medidas de supervisão humana a que se refere o artigo 14.º, incluindo as soluções técnicas adotadas para facilitar a interpretação dos resultados dos sistemas de IA pelos utilizadores;

e) A vida útil esperada do sistema de IA de risco elevado e quaisquer medidas de manutenção e assistência necessárias para assegurar o correto funcionamento desse sistema de IA, incluindo no tocante a atualizações do *software*.

Artigo 14.º
Supervisão humana

1. Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de tal modo, incluindo com ferramentas de interface homem-máquina apropriadas, que possam ser eficazmente supervisionados por pessoas singulares durante o período de utilização do sistema de IA.

2. A supervisão humana deve procurar prevenir ou minimizar os riscos para a saúde, a segurança ou os direitos fundamentais que possam surgir quando um sistema de IA de risco elevado é usado em conformidade com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsíveis, em especial quando esses riscos persistem apesar da aplicação de outros requisitos estabelecidos neste capítulo.

3. A supervisão humana deve ser assegurada por meio de um ou de todos os seguintes tipos de medidas:

   a) Medidas identificadas e integradas, quando tecnicamente viável, pelo fornecedor no sistema de IA de risco elevado antes de este ser colocado no mercado ou colocado em serviço;

   b) Medidas identificadas pelo fornecedor antes de o sistema de IA de risco elevado ser colocado no mercado ou colocado em serviço e que sejam adequadas para implantação por parte do utilizador.

4. As medidas a que se refere o n.º 3 devem permitir que as pessoas responsáveis pela supervisão humana façam o seguinte, em função das circunstâncias:

   a) Compreendam completamente as capacidades e limitações do sistema de IA de risco elevado e sejam capazes de controlar devidamente o seu funcionamento, de modo que os sinais de anomalias, disfuncionalidades e desempenho inesperado possam ser detetados e resolvidos o mais rapidamente possível;

   b) Estejam conscientes da possível tendência para confiar automaticamente ou confiar excessivamente no resultado produzido pelo sistema de IA de risco elevado («enviesamento da automatização»), em especial relativamente aos sistemas de IA de risco elevado usados para fornecer informações ou recomendações com vista à tomada de decisões por pessoas singulares;

   c) Sejam capazes de interpretar corretamente o resultado do sistema de IA de risco elevado, tendo em conta, nomeadamente, as características do sistema e as ferramentas e os métodos de interpretação disponíveis;

   d) Sejam capazes de decidir, em qualquer situação específica, não usar o sistema de IA de risco elevado ou ignorar, anular ou reverter o resultado do sistema de IA de risco elevado;

   e) Serem capazes de intervir no funcionamento do sistema de IA de risco elevado ou interromper o sistema por meio de um botão de «paragem» ou procedimento similar.

5. Em relação aos sistemas de IA de risco elevado a que se refere o anexo III, ponto 1, alínea a), as medidas referidas no n.º 3 devem, além disso, permitir assegurar que nenhuma ação ou decisão seja tomada pelo utilizador com base na identificação resultante do sistema, salvo se a mesma tiver sido verificada e confirmada por, pelo menos, duas pessoas singulares.

Artigo 15.º
Exatidão, solidez e cibersegurança

1. Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira que alcancem, tendo em conta a finalidade prevista, um nível apropriado de exatidão, solidez e cibersegurança e apresentem um desempenho coerente em relação a tais aspetos durante o ciclo de vida.

2. As instruções de utilização que acompanham os sistemas de IA de risco elevado devem declarar os níveis de exatidão e a métrica de exatidão aplicável.

3. Os sistemas de IA de risco elevado devem ser resistentes a erros, falhas ou incoerências que possam ocorrer no sistema ou no ambiente em que aquele opera, em especial devido à interação com pessoas singulares ou outros sistemas.

   A solidez dos sistemas de IA de risco elevado pode ser alcançada por via de soluções de redundância técnica, que podem incluir planos de reserva ou de segurança à prova de falhas.

   Os sistemas de IA de risco elevado que continuam a aprender após a colocação no mercado ou a colocação em serviço devem ser desenvolvidos de maneira que assegure que os resultados possivelmente enviesados devido a resultados usados como dados de entrada para futuras operações («circuitos de realimentação») sejam devidamente abordados por via de medidas de atenuação adequadas.

4. Os sistemas de IA de risco elevado devem ser resistentes a tentativas de terceiros não autorizados de alterar a sua utilização ou desempenho explorando as vulnerabilidades do sistema.

   As soluções técnicas destinadas a assegurar a cibersegurança dos sistemas de IA de risco elevado devem ser adequadas às circunstâncias e aos riscos de cada caso.

   As soluções técnicas para resolver vulnerabilidades específicas da inteligência artificial devem incluir, se for caso disso, medidas para prevenir e controlar ataques que visem manipular o conjunto de dados de treino («contaminação de dados»), dados de entrada preparados para fazer com que o modelo cometa um erro («exemplos antagónicos»), ou falhas do modelo.

CAPÍTULO 3

OBRIGAÇÕES DOS FORNECEDORES E UTILIZADORES DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO E DE OUTRAS PARTES

Artigo 16.º
Obrigações dos fornecedores de sistemas de inteligência artificial de risco elevado

Os fornecedores de sistemas de IA de risco elevado devem:

a) Assegurar que os seus sistemas de IA de risco elevado cumprem os requisitos estabelecidos no capítulo 2 do presente título;

b) Dispor de um sistema de gestão da qualidade que cumpra o disposto no artigo 17.º;

c) Elaborar a documentação técnica do sistema de IA de risco elevado;

d) Quando tal esteja sob o seu controlo, manter os registos gerados automaticamente pelos sistemas de IA de risco elevado que fornecem;

e) Assegurar que o sistema de IA de risco elevado seja sujeito ao procedimento de avaliação da conformidade aplicável, antes da colocação no mercado ou da colocação em serviço;

f) Respeitar as obrigações de registo a que se refere o artigo 51.º;

g) Adotar as medidas corretivas necessárias, se o sistema de IA de risco elevado não estiver em conformidade com os requisitos estabelecidos no capítulo 2 do presente título;

h) Informar as autoridades nacionais competentes dos Estados-Membros nos quais disponibilizaram o sistema de IA ou o colocaram em serviço e, se for caso disso, o organismo notificado sobre a não conformidade e quaisquer medidas corretivas tomadas;

i) Apor a marcação CE nos sistemas de IA de risco elevado para indicar a conformidade com o presente regulamento de acordo com o artigo 49.º;

j) Mediante pedido de uma autoridade nacional competente, demonstrar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título.

Artigo 17.º
Sistema de gestão da qualidade

1. Os fornecedores de sistemas de IA de risco elevado devem criar um sistema de gestão da qualidade que assegure a conformidade com o presente regulamento. Esse sistema deve estar documentado de uma forma sistemática e ordenada, sob a forma de políticas, procedimentos e instruções escritas, e deve incluir, no mínimo, os seguintes aspetos:

   a) Uma estratégia para o cumprimento da regulamentação, incluindo a observância de procedimentos de avaliação da conformidade e de procedimentos de gestão de modificações do sistema de IA de risco elevado;

   b) Técnicas, procedimentos e ações sistemáticas a utilizar para a conceção, controlo da conceção e verificação da conceção do sistema de IA de risco elevado;

   c) Técnicas, procedimentos e ações sistemáticas a utilizar para o desenvolvimento, controlo da qualidade e garantia da qualidade do sistema de IA de risco elevado;

   d) Procedimentos de exame, teste e validação a realizar antes, durante e após o desenvolvimento do sistema de IA de risco elevado e a frequência com a qual têm de ser realizados;

   e) Especificações técnicas, incluindo normas, a aplicar e, se as normas harmonizadas em causa não forem aplicadas na íntegra, os meios a usar para

assegurar que o sistema de IA de risco elevado cumpra os requisitos estabelecidos no capítulo 2 do presente título;

f) Sistemas e procedimentos de gestão de dados, incluindo recolha de dados, análise de dados, rotulagem de dados, armazenamento de dados, filtragem de dados, prospeção de dados, agregação de dados, conservação de dados e qualquer outra operação relativa aos dados que seja realizada antes e para efeitos da colocação no mercado ou colocação em serviço de sistemas de IA de risco elevado;

g) O sistema de gestão de riscos a que se refere o artigo 9.º;

h) O estabelecimento, aplicação e manutenção de um sistema de acompanhamento pós-comercialização, nos termos do artigo 61.º;

i) Procedimentos de comunicação de incidentes graves e de anomalias em conformidade com o artigo 62.º;

j) A gestão da comunicação com autoridades nacionais competentes, autoridades competentes, incluindo as setoriais, disponibilizando ou apoiando o acesso a dados, organismos notificados, outros operadores, clientes ou outras partes interessadas;

k) Sistemas e procedimentos de manutenção de registos de toda a documentação e informação importante;

l) Gestão de recursos, incluindo medidas relacionadas com a segurança do aprovisionamento;

m) Um quadro que defina as responsabilidades do pessoal com funções de gestão e do restante pessoal no atinente a todos os aspetos elencados no presente número.

2. A aplicação dos aspetos referidos no n.º 1 deve ser proporcionada à dimensão da organização do fornecedor.

3. Em relação aos fornecedores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE, considera-se que a obrigação de criar um sistema de gestão da qualidade é satisfeita mediante o cumprimento das regras relativas a sistemas, processos e mecanismos de governação interna previstas no artigo 74.º da referida diretiva. Neste contexto, devem ser tidas em conta quaisquer normas harmonizadas referidas no artigo 40.º do presente regulamento.

Artigo 18.º
Obrigação de elaborar documentação técnica

1. Os fornecedores de sistemas de IA de risco elevado devem elaborar a documentação técnica a que se refere o artigo 11.º de acordo com o anexo IV.

2. Os fornecedores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE devem manter a documentação técnica como parte da documentação relativa a sistemas, processos e mecanismos de governação interna elaborada nos termos do artigo 74.º da referida diretiva.

Artigo 19.º
Avaliação da conformidade

1. Os fornecedores de sistemas de IA de risco elevado devem assegurar que os sistemas que fornecem são sujeitos a um procedimento de avaliação da conformidade de acordo com o artigo 43.º, antes de serem colocados no mercado ou colocados em serviço. Assim que a conformidade dos sistemas de IA com os requisitos estabelecidos no capítulo 2 do presente título tiver sido demonstrada na sequência de uma avaliação da conformidade, os fornecedores devem elaborar uma declaração de conformidade UE de acordo com o artigo 48.º e apor a marcação de conformidade CE de acordo com o artigo 49.º.

2. Em relação aos sistemas de IA de risco elevado referidos no anexo III, ponto 5, alínea b), colocados no mercado ou colocados em serviço por fornecedores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE, a avaliação da conformidade deve ser realizada no âmbito do procedimento a que se referem os artigos 97.º a 101.º da mesma diretiva.

Artigo 20.º
Registos gerados automaticamente

1. Os fornecedores de sistemas de IA de risco elevado devem manter os registos gerados automaticamente pelos respetivos sistemas de IA de risco elevado, desde que esses registos estejam sob o seu controlo por força de uma disposição contratual com o utilizador ou de uma disposição legal. Os registos devem ser mantidos por um período adequado em função da finalidade prevista do sistema de IA de risco elevado e das obrigações legais aplicáveis nos termos da legislação da União ou nacional.

2. Os fornecedores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE devem manter os registos gerados automaticamente pelos respetivos sistemas de IA de risco elevado como parte da documentação prevista no artigo 74.º da referida diretiva.

Artigo 21.º
Medidas corretivas

Os fornecedores de sistemas de IA de risco elevado que considerem ou tenham motivos para crer que um sistema de IA de risco elevado que colocaram no mercado ou colocaram em serviço não está em conformidade com o presente regulamento devem tomar imediatamente as medidas corretivas necessárias para repor a conformidade do sistema em questão ou proceder à retirada ou recolha do mesmo, consoante o caso. Devem igualmente informar do facto os distribuidores do sistema de IA de risco elevado em questão e, se for caso disso, o mandatário e os importadores.

Artigo 22.º
Dever de informação

Se o sistema de IA de risco elevado apresentar um risco na aceção do artigo 65.º, n.º 1, e esse risco for do conhecimento do fornecedor do sistema, este último deve informar imediatamente as autoridades nacionais competentes dos Estados-Membros nos quais disponibilizou o sistema e, se for caso disso, o organismo notificado que emitiu um certificado para o sistema de IA de risco elevado, em especial sobre a não conformidade e quaisquer as medidas corretivas tomadas.

Artigo 23.º
Cooperação com as autoridades competentes

Os fornecedores de sistemas de IA de risco elevado devem, mediante pedido de uma autoridade nacional competente, prestar a essa autoridade todas as informações e documentação necessárias para demonstrar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, numa língua oficial da União determinada pelo Estado-Membro em questão. Mediante pedido fundamentado de uma autoridade nacional competente, os fornecedores devem igualmente conceder a essa autoridade o acesso aos registos gerados automaticamente pelo sistema de IA de risco elevado, desde que esses registos estejam sob o seu controlo por força de uma disposição contratual com o utilizador ou de uma disposição legal.

Artigo 24.º
Obrigações dos fabricantes de produtos

Se um sistema de IA de risco elevado relacionado com produtos aos quais são aplicáveis os atos jurídicos enumerados no anexo II, secção A, for colocado no mercado ou colocado em serviço juntamente com o produto fabricado em conformidade com esses atos jurídicos e sob o nome do fabricante do produto, este último fica incumbido de garantir a conformidade do sistema de IA com o presente regulamento e, no que diz respeito ao sistema de IA, tem as mesmas obrigações impostas ao fornecedor pelo presente regulamento.

Artigo 25.º
Mandatários

1. Antes de disponibilizarem os seus sistemas no mercado da União, caso não seja possível identificar um importador, os fornecedores estabelecidos fora da União devem, através de mandato escrito, designar um mandatário estabelecido na União.

2. O mandatário deve praticar os atos definidos no mandato conferido pelo fornecedor. O mandato deve habilitar o mandatário a exercer as seguintes funções:

   a) Manter uma cópia da declaração de conformidade UE e da documentação técnica à disposição das autoridades nacionais competentes e das autoridades nacionais a que se refere o artigo 63.º, n.º 7;

   b) Prestar a uma autoridade nacional competente, mediante pedido fundamentado, todas as informações e documentação necessárias para demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, incluindo o acesso aos registos gerados automaticamente pelo sistema de IA de risco elevado, desde que esses registos se encontrem sob o controlo do fornecedor por força de uma disposição contratual com o utilizador ou de uma disposição legal;

   c) Cooperar com as autoridades nacionais competentes, mediante pedido fundamentado, em qualquer ação que estas empreendam em relação ao sistema de IA de risco elevado.

Artigo 26.º
Obrigações dos importadores

1. Antes de colocarem um sistema de IA de risco elevado no mercado, os importadores desse sistema devem assegurar-se de que:

a) O fornecedor desse sistema de IA realizou o procedimento de avaliação da conformidade adequado;

b) O fornecedor elaborou a documentação técnica em conformidade com o anexo IV;

c) O sistema ostenta a marcação de conformidade exigida e está acompanhado da documentação e das instruções de utilização necessárias.

2. Se um importador considerar ou tiver motivos para crer que um sistema de IA de risco elevado não está em conformidade com o presente regulamento, não pode colocar esse sistema de IA no mercado enquanto o mesmo não for tornado conforme. Se o sistema de IA de risco elevado apresentar um risco na aceção do artigo 65.º, n.º 1, o importador deve informar desse facto o fornecedor do sistema de IA e as autoridades de fiscalização do mercado.

3. Os importadores devem indicar o seu nome, nome comercial registado ou marca registada e endereço de contacto no sistema de IA de risco elevado, ou, se tal não for possível, na respetiva embalagem ou na documentação que o acompanha, conforme aplicável.

4. Enquanto um sistema de IA de risco elevado estiver sob a responsabilidade dos importadores, estes devem assegurar, se for caso disso, que as condições de armazenamento ou de transporte não prejudicam a conformidade do sistema com os requisitos enunciados no capítulo 2 do presente título.

5. Os importadores devem prestar às autoridades nacionais competentes, mediante pedido fundamentado, todas as informações e documentação necessárias para demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, numa língua que possa ser facilmente compreendida pela autoridade nacional competente em causa, incluindo o acesso aos registos gerados automaticamente pelo sistema de IA de risco elevado, desde que esses registos se encontrem sob o controlo do fornecedor por força de uma disposição contratual com o utilizador ou de uma disposição legal. Devem igualmente cooperar com essas autoridades nacionais competentes em qualquer ação que estas empreendam em relação a esse sistema.

Artigo 27.º
Obrigações dos distribuidores

1. Antes de disponibilizarem um sistema de IA de risco elevado no mercado, os distribuidores devem verificar se o sistema de IA de risco elevado ostenta a marcação de conformidade CE exigida, se está acompanhado da documentação e das instruções de utilização necessárias e se o fornecedor e o importador do sistema, consoante o caso, cumpriram as obrigações estabelecidas no presente regulamento.

2. Se um distribuidor considerar ou tiver motivos para crer que um sistema de IA de risco elevado não está em conformidade com os requisitos estabelecidos no capítulo 2 do presente título, não pode disponibilizar esse sistema de IA de risco elevado no mercado enquanto o mesmo não for tornado conforme com os referidos requisitos. Além disso, se o sistema apresentar um risco na aceção do artigo 65.º, n.º 1, o distribuidor deve informar desse facto o fornecedor ou o importador do sistema, conforme o caso.

3. Enquanto um sistema de IA de risco elevado estiver sob a responsabilidade dos distribuidores, estes devem assegurar, se for caso disso, que as condições de armazenamento ou de transporte não prejudicam a conformidade do sistema com os requisitos enunciados no capítulo 2 do presente título.

4. Um distribuidor que considere ou tenha motivos para crer que um sistema de IA de risco elevado que disponibilizou no mercado não em conformidade com os requisitos estabelecidos no capítulo 2 do presente título deve tomar as medidas corretivas necessárias para repor a conformidade desse sistema com os referidos requisitos, proceder à retirada ou recolha do mesmo ou assegurar que o fornecedor, o importador ou qualquer operador envolvido, consoante o caso, toma essas medidas corretivas. Se um sistema de IA de risco elevado apresentar um risco na aceção do artigo 65.º, n.º 1, o distribuidor deve informar imediatamente desse facto as autoridades nacionais competentes dos Estados-Membros em que disponibilizou o produto, apresentando dados, sobretudo no que se refere à não conformidade e às medidas corretivas tomadas.

5. Mediante pedido fundamentado de uma autoridade nacional competente, os distribuidores de sistemas de IA de risco elevado devem prestar a essa autoridade todas as informações e documentação necessárias para demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título. Os distribuidores devem igualmente cooperar com essa autoridade nacional competente em qualquer ação que esta empreenda.

Artigo 28.º

Obrigações dos distribuidores, importadores, utilizadores e outros terceiros

1. Qualquer distribuidor, importador, utilizador ou outro terceiro será considerado um fornecedor para efeitos do presente regulamento e ficará sujeito às obrigações do fornecedor estabelecidas no artigo 16.º em qualquer uma das seguintes circunstâncias:

   a) Se coloca no mercado ou colocar em serviço um sistema de IA de risco elevado sob o seu nome ou marca;

   b) Se modificar a finalidade prevista de um sistema de IA de risco elevado já colocado no mercado ou colocado em serviço;

   c) Se introduzir uma modificação substancial no sistema de IA de risco elevado.

2. Sempre que se verificarem as circunstâncias a que se refere o n.º 1, alíneas b) ou c), o fornecedor que inicialmente colocou no mercado ou colocou em serviço o sistema de IA de risco elevado deixará de ser considerado um fornecedor para efeitos do presente regulamento.

Artigo 29.º

Obrigações dos utilizadores de sistemas de inteligência artificial de risco elevado

1. Os utilizadores de sistemas de IA de risco elevado devem utilizá-los de acordo com as instruções de utilização que acompanham os sistemas, nos termos dos n.os 2 e 5.

2. As obrigações previstas no n.º 1 não excluem outras obrigações do utilizador previstas na legislação da União ou nacional nem prejudicam o poder discricionário do utilizador para organizar os seus próprios recursos e atividades para efeitos de aplicação das medidas de supervisão humana indicadas pelo fornecedor.

3. Sem prejuízo do disposto no n.º 1, desde que o utilizador exerça controlo sobre os dados de entrada, esse utilizador deve assegurar que os dados de entrada sejam adequados à finalidade prevista do sistema de IA de risco elevado.

4. Os utilizadores devem controlar o funcionamento do sistema de IA de risco elevado com base nas instruções de utilização. Se tiverem motivos para considerar que a utilização de acordo com as instruções de utilização pode fazer com que o sistema de IA apresente um risco na aceção do artigo 65.º, n.º 1, devem informar o fornecedor ou distribuidor e suspender a utilização do sistema. Devem também informar o fornecedor ou distribuidor e interromper a utilização do sistema de IA caso identifiquem qualquer incidente grave ou anomalia na aceção do artigo 62.º. Se o utilizador não conseguir entrar em contacto com o fornecedor, aplica-se, por analogia, o artigo 62.º.

   Em relação aos utilizadores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE, considera-se que a obrigação de controlo estabelecida no primeiro parágrafo é satisfeita mediante o cumprimento das regras relativas a sistemas, processos e mecanismos de governação interna previstas no artigo 74.º da referida diretiva.

5. Os utilizadores de sistemas de IA de risco elevado devem manter os registos gerados automaticamente por esse sistema de IA de risco elevado, desde que esses registos estejam sob o seu controlo. Os registos devem ser mantidos por um período adequado em função da finalidade prevista do sistema de IA de risco elevado e das obrigações legais aplicáveis nos termos da legislação da União ou nacional.

   Os utilizadores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE devem manter os registos como parte da documentação relativa a sistemas, processos e mecanismos de governação interna prevista no artigo 74.º da referida diretiva.

6. Os utilizadores de sistemas de IA de risco elevado devem usar as informações recebidas nos termos do artigo 13.º para cumprirem a sua obrigação de realizar uma avaliação de impacto sobre a proteção de dados nos termos do artigo 35.º do Regulamento (UE) 2016/679 ou do artigo 27.º da Diretiva (UE) 2016/680, conforme aplicável.

CAPÍTULO 4

AUTORIDADES NOTIFICADORAS E ORGANISMOS NOTIFICADOS

Artigo 30.º
Autoridades notificadoras

1. Cada Estado-Membro deve designar ou criar uma autoridade notificadora responsável por estabelecer e executar os procedimentos necessários para a avaliação, a designação e a notificação de organismos de avaliação da conformidade e pela fiscalização destes.

2. Os Estados-Membros podem designar um organismo nacional de acreditação a que se refere o Regulamento (CE) n.º 765/2008 como autoridade notificadora.

3. As autoridades notificadoras devem ser criadas, organizadas e geridas de maneira que garanta a ausência de conflitos de interesses com os organismos de avaliação da conformidade e a objetividade e imparcialidade das suas atividades.

4. As autoridades notificadoras devem estar organizadas de maneira que as decisões relativas à notificação dos organismos de avaliação da conformidade sejam tomadas por pessoas competentes diferentes daquelas que realizaram a avaliação desses organismos.

5. As autoridades notificadoras não podem propor nem desempenhar qualquer atividade que seja da competência dos organismos de avaliação da conformidade, nem prestar quaisquer serviços de consultoria com caráter comercial ou em regime de concorrência.

6. As autoridades notificadoras devem proteger a confidencialidade das informações obtidas.

7. As autoridades notificadoras devem dispor de recursos humanos com competência técnica em número suficiente para o correto exercício das suas funções.

8. As autoridades notificadoras devem certificar-se de que as avaliações da conformidade são realizadas de modo proporcionado, evitando encargos desnecessários para os fornecedores, e de que os organismos notificados executam as suas atividades tendo devidamente em conta a dimensão da empresa, o setor no qual opera, a sua estrutura e o grau de complexidade do sistema de IA em apreço.

Artigo 31.º

Apresentação de pedido de notificação por um organismo de avaliação da conformidade

1. Os organismos de avaliação da conformidade devem apresentar um pedido de notificação à autoridade notificadora do Estado-Membro onde se encontram estabelecidos.

2. O pedido de notificação deve ser acompanhado de uma descrição das atividades de avaliação da conformidade, do módulo ou dos módulos de avaliação da conformidade e das tecnologias de inteligência artificial em relação às quais o organismo se considera competente, bem como de um certificado de acreditação, se existir, emitido por um organismo nacional de acreditação, que ateste que o organismo de avaliação da conformidade cumpre os requisitos estabelecidos no artigo 33.º Deve ser igualmente anexado qualquer documento válido relacionado com designações vigentes do organismo notificado requerente ao abrigo de qualquer outra legislação de harmonização da União.

3. Se não lhe for possível apresentar o certificado de acreditação, o organismo de avaliação da conformidade deve fornecer à autoridade notificadora as provas documentais necessárias à verificação, ao reconhecimento e à fiscalização regular da sua conformidade com os requisitos estabelecidos no artigo 33.º. Em relação aos organismos notificados designados ao abrigo de qualquer outra legislação de harmonização da União, todos os documentos e certificados associados a essas designações podem ser usados para fundamentar o seu processo de designação nos termos do presente regulamento, consoante adequado.

Artigo 32.º

Procedimento de notificação

1. As autoridades notificadoras só podem notificar organismos de avaliação da conformidade que cumpram os requisitos previstos no artigo 33.º.

2. As autoridades notificadoras devem notificar a Comissão e os restantes Estados-Membros utilizando um instrumento de notificação eletrónica criado e gerido pela Comissão.

3. A notificação deve incluir dados completos das atividades de avaliação da conformidade, do módulo ou módulos de avaliação da conformidade e das tecnologias de inteligência artificial em questão.

4. O organismo de avaliação da conformidade em causa apenas pode exercer as atividades de organismo notificado se nem a Comissão nem os restantes Estados-Membros tiverem levantado objeções no mês seguinte à notificação.

5. As autoridades notificadoras devem comunicar à Comissão e aos restantes Estados-Membros todas as alterações importantes subsequentemente introduzidas na notificação.

Artigo 33.º
Organismos notificados

1. Os organismos notificados devem verificar a conformidade de um sistema de IA de risco elevado de acordo com os procedimentos de avaliação da conformidade a que se refere o artigo 43.º.

2. Os organismos notificados devem satisfazer os requisitos em termos de organização, gestão da qualidade, recursos e processos que sejam necessários para o exercício das suas tarefas.

3. A estrutura organizacional, a atribuição de responsabilidades, a cadeia hierárquica e o funcionamento dos organismos notificados devem ser de molde a assegurar a confiança no desempenho e nos resultados das atividades de avaliação da conformidade que os organismos notificados realizam.

4. Os organismos notificados devem ser independentes do fornecedor de um sistema de IA de risco elevado relativamente ao qual realizam atividades de avaliação da conformidade. Os organismos notificados devem também ser independentes de qualquer outro operador que tenha um interesse económico no sistema de IA de risco elevado que é avaliado, bem como de quaisquer concorrentes do fornecedor.

5. Os organismos notificados devem estar organizados e funcionar de maneira que garanta a independência, a objetividade e a imparcialidade das suas atividades. Os organismos notificados devem documentar e estabelecer uma estrutura e procedimentos capazes de salvaguardar essa imparcialidade e de promover e aplicar os princípios da imparcialidade em toda a sua organização, pessoal e atividades de avaliação.

6. Os organismos notificados devem dispor de procedimentos documentados que garantam que o seu pessoal, comités, filiais, subcontratantes e qualquer outro organismo associado ou pessoal de organismos externos respeitam a confidencialidade das informações de que tenham conhecimento durante a realização das atividades de avaliação da conformidade, salvo se a divulgação daquelas for exigida por lei. O pessoal dos organismos notificados deve estar sujeito ao sigilo profissional no que se refere a todas as informações que obtiver no exercício das suas funções no âmbito do presente regulamento, exceto em relação às autoridades notificadoras do Estado-Membro em que exerce as suas atividades.

7. Os organismos notificados devem dispor de procedimentos relativos ao exercício de atividades que tenham em devida conta a dimensão de uma empresa, o setor em que opera, a sua estrutura e o grau de complexidade do sistema de IA em questão.

8. Os organismos notificados devem subscrever um seguro de responsabilidade civil adequado para as suas atividades de avaliação da conformidade, a menos que essa responsabilidade seja assumida pelo Estado-Membro em causa nos termos da legislação nacional ou que esse Estado-Membro seja diretamente responsável pela avaliação da conformidade.

9. Os organismos notificados devem ser capazes de executar todas as tarefas que lhes forem atribuídas pelo presente regulamento com a maior integridade profissional e a competência exigida no domínio específico, quer essas tarefas sejam executadas por eles próprios, quer em seu nome e sob a sua responsabilidade.

10. Os organismos notificados devem dispor de competências internas suficientes para poderem avaliar eficazmente as tarefas realizadas em seu nome por partes externas. Para o efeito, em todas as circunstâncias e para cada procedimento de avaliação da conformidade e cada tipo de sistema de IA de risco elevado para os quais tenham sido designados, os organismos notificados devem dispor permanentemente de suficiente pessoal administrativo, técnico e científico com experiência e conhecimentos relativos às tecnologias de inteligência artificial em apreço, aos dados e à computação de dados e aos requisitos estabelecidos no capítulo 2 do presente título.

11. Os organismos notificados devem participar em atividades de coordenação conforme referido no artigo 38.º. Além disso, devem participar, diretamente ou por meio de representantes, em organizações europeias de normalização, ou assegurar que têm conhecimentos e se mantêm atualizados acerca das normas aplicáveis.

12. Os organismos notificados devem disponibilizar e, mediante pedido, apresentar toda a documentação importante, incluindo a documentação elaborada pelos fornecedores, à autoridade notificadora a que se refere o artigo 30.º para que esta possa exercer as suas atividades de avaliação, designação, notificação, controlo e fiscalização e ainda para facilitar a avaliação descrita no presente capítulo.

Artigo 34.º
Filiais e subcontratantes dos organismos notificados

1. Sempre que um organismo notificado subcontratar tarefas específicas relacionadas com a avaliação da conformidade ou recorrer a uma filial, deve assegurar que o subcontratante ou a filial cumprem os requisitos previstos no artigo 33.º e informar a autoridade notificadora desse facto.

2. Os organismos notificados devem assumir plena responsabilidade pelas tarefas executadas por subcontratantes ou filiais, independentemente do local em que estes se encontram estabelecidos.

3. As atividades só podem ser exercidas por um subcontratante ou por uma filial mediante acordo do fornecedor.

4. Os organismos notificados devem manter à disposição da autoridade notificadora os documentos necessários respeitantes à avaliação das qualificações do subcontratante ou da filial e ao trabalho efetuado por estes nos termos do presente regulamento.

Artigo 35.º

Números de identificação e listas de organismos notificados designados nos termos do presente regulamento

1. A Comissão atribui um número de identificação aos organismos notificados. O número atribuído é único, mesmo que o organismo esteja notificado ao abrigo de vários atos da União.

2. A Comissão publica a lista de organismos notificados ao abrigo do presente regulamento, incluindo os números de identificação que lhes foram atribuídos e as atividades em relação às quais foram notificados. A Comissão assegura a atualização dessa lista.

Artigo 36.º

Alterações das notificações

1. Caso uma autoridade notificadora suspeite ou seja informada de que um organismo notificado deixou de cumprir os requisitos estabelecidos no artigo 33.º, ou de que não cumpre as suas obrigações, deve imediatamente investigar a matéria com a máxima diligência. Neste contexto, deve informar o organismo notificado em causa sobre as objeções levantadas e dar-lhe a possibilidade de expressar as suas observações. Caso a autoridade notificadora conclua que o organismo notificado deixou de cumprir os requisitos estabelecidos no artigo 33.º, ou que não cumpre as suas obrigações, deve restringir, suspender ou retirar a notificação, consoante o caso, em função da gravidade do incumprimento. Deve ainda informar imediatamente a Comissão e os restantes Estados-Membros deste facto.

2. Em caso de restrição, suspensão ou retirada da notificação, ou caso o organismo notificado tenha cessado atividade, a autoridade notificadora deve tomar as medidas necessárias para assegurar que os processos desse organismo notificado são assumidos por outro organismo notificado ou mantidos à disposição das autoridades notificadoras competentes, se estas o solicitarem.

Artigo 37.º

Contestação da competência dos organismos notificados

1. A Comissão investiga, sempre que necessário, todos os casos em que haja motivos para duvidar do cumprimento dos requisitos estabelecidos no artigo 33.º por parte de um organismo notificado.

2. A autoridade notificadora deve facultar à Comissão, mediante pedido, todas as informações importantes relacionadas com a notificação do organismo notificado em causa.

3. A Comissão garante que todas as informações confidenciais obtidas no decurso das suas investigações nos termos do presente artigo são tratadas de forma confidencial.

4. Caso verifique que um organismo notificado não cumpre ou deixou de cumprir os requisitos estabelecidos no artigo 33.º, a Comissão adota uma decisão fundamentada solicitando ao Estado-Membro notificador que tome as medidas corretivas necessárias, incluindo, se for caso disso, a retirada da notificação. O referido ato de execução é adotado de acordo com o procedimento de exame a que se refere o artigo 74.º, n.º 2.

Artigo 38.º
Coordenação dos organismos notificados

1. A Comissão assegura que, no respeitante aos domínios abrangidos pelo presente regulamento, são instituídas modalidades de coordenação e cooperação adequadas entre organismos notificados ativos nos procedimentos de avaliação da conformidade de sistemas de IA nos termos do presente regulamento e que as mesmas decorrem devidamente sob a forma de um grupo setorial de organismos notificados.

2. Os Estados-Membros devem assegurar que os organismos por si notificados participam, diretamente ou por meio de representantes designados, nos trabalhos desse grupo.

Artigo 39.º
Organismos de avaliação da conformidade de países terceiros

Os organismos de avaliação da conformidade criados ao abrigo da legislação de um país terceiro com o qual a União tenha celebrado um acordo podem ser autorizados a executar as atividades de organismos notificados nos termos do presente regulamento.

CAPÍTULO 5

NORMAS, AVALIAÇÃO DA CONFORMIDADE, CERTIFICADOS, REGISTO

Artigo 40.º
Normas harmonizadas

Presume-se que os sistemas de IA de risco elevado que estão em conformidade com normas harmonizadas, ou com partes destas, cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia*, são conformes com os requisitos estabelecidos no capítulo 2 do presente título, desde que tais normas abranjam esses requisitos.

Artigo 41.º
Especificações comuns

1. Na ausência das normas harmonizadas a que se refere o artigo 40.º ou caso a Comissão considere que as normas harmonizadas existentes são insuficientes ou que é necessário abordar preocupações específicas em termos de segurança ou direitos fundamentais, a Comissão pode, por meio de atos de execução, adotar especificações comuns relativas aos requisitos estabelecidos no capítulo 2 do presente título. Os referidos atos de execução são adotados de acordo com o procedimento de exame a que se refere o artigo 74.º, n.º 2.

2. Ao preparar as especificações comuns a que se refere o n.º 1, a Comissão recolhe as opiniões dos organismos ou grupos de peritos pertinentes criados nos termos do direito setorial da União aplicável.

3. Presume-se que os sistemas de IA de risco elevado que estão em conformidade com as especificações comuns a que se refere o n.º 1 são conformes com os requisitos estabelecidos no capítulo 2 do presente título, desde que tais especificações comuns abranjam esses requisitos.

4. Os fornecedores que não cumprirem as especificações comuns a que se refere o n.º 1 devem justificar devidamente que adotaram soluções técnicas, no mínimo, equivalentes.

Artigo 42.º
Presunção de conformidade com determinados requisitos

1. Tendo em conta a sua finalidade prevista, presume-se que os sistemas de IA de risco elevado que foram treinados e testados com recurso a dados relativos ao enquadramento geográfico, comportamental e funcional específico no qual se destinam a ser utilizados são conformes com o requisito estabelecido no artigo 10.º, n.º 4.

2. Presume-se que os sistemas de IA de risco elevado que foram certificados ou relativamente aos quais foi emitida uma declaração de conformidade no âmbito de um sistema de certificação da cibersegurança estabelecido nos termos do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[63] e cujas referências foram publicadas no *Jornal Oficial da União Europeia* são conformes com os requisitos de cibersegurança estabelecidos no artigo 15.º do presente regulamento, contanto que o certificado de cibersegurança ou a declaração de conformidade ou partes dos mesmos abranjam esses requisitos.

Artigo 43.º
Avaliação da conformidade

1. No respeitante aos sistemas de IA de risco elevado enumerados no anexo III, ponto 1, quando, ao demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, o fornecedor tiver aplicado normas harmonizadas a que se refere o artigo 40.º, ou, se for caso disso, especificações comuns a que se refere o artigo 41.º, o fornecedor deve seguir um dos seguintes procedimentos:

   a) O procedimento de avaliação da conformidade baseado no controlo interno a que se refere o anexo VI;

   b) O procedimento de avaliação da conformidade baseado na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica, com a participação de um organismo notificado, a que se refere o anexo VII.

   Quando, ao demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, o fornecedor não tiver aplicado ou tiver aplicado apenas parcialmente normas harmonizadas a que se refere o artigo 40.º, ou se tais normas harmonizadas não existirem e as especificações comuns a que se refere o artigo 41.º não estiverem disponíveis, o fornecedor deve seguir o procedimento de avaliação da conformidade preconizado no anexo VII.

   Para efeitos do procedimento de avaliação da conformidade a que se refere o anexo VII, o fornecedor pode escolher qualquer um dos organismos notificados. Contudo, se o sistema se destinar a ser colocado em serviço por autoridades competentes em

[63] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 1).

matéria de manutenção da ordem pública, imigração ou asilo, bem como por instituições, órgãos e organismos da UE, a autoridade de fiscalização do mercado a que se refere o artigo 63.º, n.os 5 ou 6, consoante o caso, deve atuar como um organismo notificado.

2. Em relação aos sistemas de IA de risco elevado enumerados no anexo III, pontos 2 a 8, os fornecedores devem seguir o procedimento de avaliação da conformidade baseado no controlo interno a que se refere o anexo VI, que não prevê a participação de um organismo notificado. Em relação aos sistemas de IA de risco elevado referidos no anexo III, ponto 5, alínea b), que são colocados no mercado ou colocados em serviço por instituições de crédito regulamentadas pela Diretiva 2013/36/UE, a avaliação da conformidade deve ser realizada no âmbito do procedimento a que se referem os artigos 97.º a 101.º da mesma diretiva.

3. Em relação aos sistemas de IA de risco elevado aos quais são aplicáveis atos jurídicos enumerados no anexo II, secção A, o fornecedor deve seguir o procedimento de avaliação da conformidade aplicável nos termos desses atos jurídicos. Os requisitos estabelecidos no capítulo 2 do presente título aplicam-se a esses sistemas de IA de risco elevado e devem fazer parte dessa avaliação. É igualmente aplicável o disposto no anexo VII, pontos 4.3, 4.4, 4.5, e ponto 4.6, quinto parágrafo.

   Para efeitos dessa avaliação, os organismos notificados que tenham sido notificados ao abrigo dos referidos atos jurídicos ficam habilitados a verificar a conformidade dos sistemas de IA de risco elevado com os requisitos estabelecidos no capítulo 2 do presente título, contanto que a conformidade desses organismos notificados com os requisitos estabelecidos no artigo 33.º, n.os 4, 9 e 10, tenha sido avaliada no contexto do procedimento de notificação previsto nesses atos jurídicos.

   Sempre que os atos jurídicos enumerados no anexo II, secção A, permitam ao fabricante do produto renunciar a uma avaliação da conformidade por terceiros, desde que tenha aplicado todas as normas harmonizadas que abrangem os requisitos previstos nesses atos, esse fabricante apenas pode fazer uso de tal opção se tiver também aplicado normas harmonizadas ou, se for caso disso, especificações comuns a que se refere o artigo 41.º que abranjam os requisitos estabelecidos no capítulo 2 do presente título.

4. Os sistemas de IA de risco elevado devem ser sujeitos a um novo procedimento de avaliação da conformidade sempre que forem substancialmente modificados, independentemente de o sistema modificado se destinar a distribuição ulterior ou continuar a ser usado pelo utilizador atual.

   No respeitante aos sistemas de IA de risco elevado que continuam a aprender após a colocação no mercado ou a colocação em serviço, as alterações introduzidas no sistema de IA de risco elevado e no seu desempenho que tenham sido predeterminadas pelo fornecedor aquando da avaliação da conformidade inicial e façam parte das informações contidas na documentação técnica a que se refere o anexo VI, ponto 2, alínea f), não constituem uma modificação substancial.

5. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para atualizar os anexos VI e VII, a fim de introduzir elementos dos procedimentos de avaliação da conformidade que se tornem necessários à luz da evolução técnica.

6. A Comissão fica habilitada a adotar atos delegados para alterar os n.os 1 e 2, a fim de sujeitar os sistemas de IA de risco elevado referidos no anexo III, pontos 2 a 8, ao

procedimento de avaliação da conformidade referido no anexo VII ou a partes daquele. A Comissão adota esses atos delegados tendo em conta a eficácia do procedimento de avaliação da conformidade baseado no controlo interno a que se refere o anexo VI na prevenção ou minimização dos riscos para a saúde e a segurança e a proteção dos direitos fundamentais representados por esses sistemas, bem como a disponibilidade de capacidades e recursos adequados entre os organismos notificados.

Artigo 44.º
Certificados

1. Os certificados emitidos por organismos notificados nos termos do anexo VII devem ser redigidos numa língua oficial da União determinada pelo Estado-Membro em que estiver estabelecido o organismo notificado ou numa outra língua oficial da União aceite pelo organismo notificado.

2. Os certificados são válidos pelo período neles indicado, que não pode exceder cinco anos. A pedido do fornecedor, a validade de um certificado pode ser prorrogada por novos períodos não superiores a cinco anos, com base numa reavaliação segundo os procedimentos de avaliação da conformidade aplicáveis.

3. Se verificar que um sistema de IA deixou de cumprir os requisitos estabelecidos no capítulo 2 do presente título, o organismo notificado deve suspender, retirar ou restringir o certificado emitido, tendo em conta o princípio da proporcionalidade, a não ser que o fornecedor do sistema garanta o cumprimento desses requisitos tomando as medidas corretivas necessárias num prazo adequado estabelecido pelo organismo notificado. O organismo notificado deve fundamentar a sua decisão.

Artigo 45.º
Recurso das decisões dos organismos notificados

Os Estados-Membros devem assegurar a disponibilidade de um procedimento de recurso das decisões às partes com um interesse legítimo nessa decisão.

Artigo 46.º
Obrigações de informação dos organismos notificados

1. Os organismos notificados devem comunicar à autoridade notificadora as seguintes informações:

   a) Certificados da União de avaliação da documentação técnica, todos os suplementos desses certificados, bem como aprovações do sistema de gestão da qualidade emitidos de acordo com os requisitos do anexo VII;

   b) Recusas, restrições, suspensões ou retiradas de certificados da União de avaliação da documentação técnica ou de aprovações de sistemas de gestão da qualidade emitidos em conformidade com os requisitos constantes do anexo VII;

   c) As circunstâncias que afetem o âmbito ou as condições de notificação;

   d) Pedidos de informação que tenham recebido das autoridades de fiscalização do mercado sobre as atividades de avaliação da conformidade;

e) Se lhes for solicitado, as atividades de avaliação da conformidade realizadas no âmbito da respetiva notificação e quaisquer outras atividades exercidas, nomeadamente atividades transfronteiras e de subcontratação.

2. Cada organismo notificado deve informar os outros organismos notificados sobre:

a) As aprovações de sistemas de gestão da qualidade que tenha recusado, suspendido ou retirado e, se lhe for pedido, as aprovações que tenha concedido a sistemas de qualidade;

b) Os certificados UE de avaliação da documentação técnica ou quaisquer suplementos dos mesmos que tenha recusado, retirado, suspendido ou restringido de outro modo e, se lhe for pedido, os certificados e/ou suplementos dos mesmos que tenha emitido.

3. Cada organismo notificado deve disponibilizar aos outros organismos notificados que realizam atividades de avaliação da conformidade semelhantes, abrangendo as mesmas tecnologias de inteligência artificial, informações importantes sobre questões relativas aos resultados negativos e, se lhe for pedido, aos resultados positivos de procedimentos de avaliação da conformidade.

Artigo 47.º
Derrogação do procedimento de avaliação da conformidade

1. Em derrogação do artigo 43.º, qualquer autoridade de fiscalização do mercado pode autorizar a colocação no mercado ou a colocação em serviço de determinados sistemas de IA de risco elevado no território do Estado-Membro em causa, por motivos excecionais de segurança pública ou de proteção da vida e da saúde das pessoas, de proteção do ambiente e de proteção de ativos industriais e infraestruturas essenciais. Essa autorização deve ser concedida por um período limitado, enquanto os procedimentos de avaliação da conformidade necessários estiverem a ser executados, e cessa assim que esses procedimentos tiverem sido concluídos. A conclusão desses procedimentos deve ser realizada sem demora injustificada.

2. A autorização a que se refere o n.º 1 apenas deve ser concedida se a autoridade de fiscalização do mercado concluir que o sistema de IA de risco elevado cumpre os requisitos do capítulo 2 do presente título. A autoridade de fiscalização do mercado deve informar a Comissão e os outros Estados-Membros sobre qualquer autorização concedida nos termos do n.º 1.

3. Se, no prazo de 15 dias a contar da receção da informação a que se refere o n.º 2, nem os Estados-Membros nem a Comissão tiverem levantado objeções a uma autorização concedida por uma autoridade de fiscalização do mercado de um Estado-Membro em conformidade com o n.º 1, considera-se que a mesma é justificada.

4. Se, nos 15 dias subsequentes à receção da notificação a que se refere o n.º 2, um Estado-Membro levantar objeções a uma autorização concedida por uma autoridade de fiscalização do mercado de outro Estado-Membro, ou se a Comissão considerar que a autorização é contrária ao direito da União ou que a conclusão dos Estados-Membros relativa à conformidade do sistema a que se refere o n.º 2 é infundada, a Comissão procede sem demora a consultas com o Estado-Membro em causa. Os operadores em questão devem ser consultados e ter a possibilidade de apresentar as suas observações. Tendo em conta essas observações, a Comissão decide se a autorização se justifica ou não. A Comissão designa o Estado-Membro e o operador ou operadores em causa como destinatários da decisão.

5. Se a autorização for considerada injustificada, a autoridade de fiscalização do mercado do Estado-Membro em causa deve retirá-la.

6. Em derrogação dos n.os 1 a 5, no respeitante a sistemas de IA de risco elevado concebidos para serem usados como componentes de segurança de dispositivos ou que sejam, eles próprios, dispositivos abrangidos pelos Regulamentos (UE) 2017/745 e (UE) 2017/746, o artigo 59.º do Regulamento (UE) 2017/745 e o artigo 54.º do Regulamento (UE) 2017/746 também são aplicáveis no atinente à derrogação da avaliação da conformidade do cumprimento dos requisitos estabelecidos no capítulo 2 do presente título.

Artigo 48.º
Declaração de conformidade UE

1. O fornecedor deve elaborar uma declaração de conformidade UE escrita para cada sistema de IA e mantê-la à disposição das autoridades nacionais competentes por um período de dez anos a contar da data de colocação no mercado ou colocação em serviço do sistema de IA. A declaração de conformidade UE deve especificar o sistema de IA para o qual foi elaborada. Deve ser fornecida uma cópia da declaração de conformidade UE às autoridades nacionais competentes, mediante pedido.

2. A declaração de conformidade UE deve mencionar que o sistema de IA de risco elevado em questão cumpre os requisitos estabelecidos no capítulo 2 do presente título. A declaração de conformidade UE deve conter as informações indicadas no anexo V e ser traduzida para uma ou várias línguas oficiais da União exigidas pelos Estados-Membros em que o sistema de IA de risco elevado é disponibilizado.

3. Se os sistemas de IA de risco elevado estiverem sujeitos a outra legislação de harmonização da União que também exija uma declaração de conformidade UE, deve ser elaborada uma única declaração de conformidade UE respeitante a todos os atos jurídicos da UE aplicáveis ao sistema de IA de risco elevado. A declaração deve incluir todas as informações necessárias para identificar a legislação de harmonização da União a que diz respeito.

4. Ao elaborar a declaração de conformidade UE, o fornecedor deve assumir a responsabilidade pelo cumprimento dos requisitos estabelecidos no capítulo 2 do presente título. O fornecedor deve manter a declaração de conformidade UE atualizada, consoante necessário.

5. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 73.º para atualizar o conteúdo da declaração de conformidade UE preconizado no anexo V, a fim de introduzir elementos que se tornem necessários à luz da evolução técnica.

Artigo 49.º
Marcação de conformidade CE

1. A marcação CE deve ser aposta de modo visível, legível e indelével em sistemas de IA de risco elevado. Caso a natureza do sistema de IA de risco elevado não permita ou não garanta essas características da marcação, esta deve ser aposta na embalagem ou na documentação que acompanha o sistema, conforme mais adequado.

2. A marcação CE a que se refere o n.º 1 está sujeita aos princípios gerais estabelecidos no artigo 30.º do Regulamento (CE) n.º 765/2008.

3. Quando aplicável, a marcação CE deve ser seguida pelo número de identificação do organismo notificado responsável pelos procedimentos de avaliação da conformidade estabelecidos no artigo 43.º. O número de identificação deve ser igualmente indicado em qualquer material promocional que mencione que o sistema de IA de risco elevado cumpre os requisitos aplicáveis à marcação CE.

Artigo 50.º
Conservação de documentos

O fornecedor deve manter à disposição das autoridades nacionais competentes, durante os dez anos subsequentes à data de colocação no mercado ou de colocação em serviço do sistema de IA:

a) A documentação técnica a que se refere o artigo 11.º;

b) A documentação relativa ao sistema de gestão da qualidade a que se refere o artigo 17.º;

c) A documentação relativa às alterações aprovadas pelos organismos notificados, se for caso disso;

d) As decisões e outros documentos emitidos pelos organismos notificados, se for caso disso;

e) A declaração de conformidade UE a que se refere o artigo 48.º.

Artigo 51.º
Registo

Antes da colocação no mercado ou da colocação em serviço de um sistema de IA de risco elevado referido no artigo 6.º, n.º 2, o fornecedor ou, se for caso disso, o mandatário deve registar esse sistema na base de dados da UE a que se refere o artigo 60.º.

TÍTULO IV

OBRIGAÇÕES DE TRANSPARÊNCIA APLICÁVEIS A DETERMINADOS SISTEMAS DE INTELIGÊNCIA ARTIFICIAL

Artigo 52.º
Obrigações de transparência aplicáveis a determinados sistemas de inteligência artificial

1. Os fornecedores devem assegurar que os sistemas de IA destinados a interagir com pessoas singulares sejam concebidos e desenvolvidos de maneira que as pessoas singulares sejam informadas de que estão a interagir com um sistema de IA, salvo se tal se revelar óbvio dadas as circunstâncias e o contexto de utilização. Esta obrigação não se aplica a sistemas de IA legalmente autorizados para detetar, prevenir, investigar e reprimir infrações penais, salvo se esses sistemas estiverem disponíveis ao público para denunciar uma infração penal.

2. Os utilizadores de um sistema de reconhecimento de emoções ou de um sistema de categorização biométrica devem informar sobre o funcionamento do sistema as pessoas a ele expostas. Esta obrigação não se aplica a sistemas de IA usados para categorização biométrica que sejam legalmente autorizados para detetar, prevenir e investigar infrações penais.

3. Os utilizadores de um sistema de IA que gera ou manipula conteúdos de imagem, áudio ou vídeo que sejam consideravelmente semelhantes a pessoas, objetos, locais ou outras entidades ou acontecimentos reais e que, falsamente, pareçam ser autênticos e verdadeiros a uma pessoa («falsificação profunda») devem divulgar que o conteúdo foi gerado ou manipulado artificialmente.

   Contudo, o primeiro parágrafo não se aplica se a utilização for legalmente autorizada para detetar, prevenir, investigar e reprimir infrações penais ou for necessária para exercer o direito à liberdade de expressão e o direito à liberdade das artes e das ciências consagrados na Carta dos Direitos Fundamentais da UE, desde que salvaguarde adequadamente os direitos e as liberdades de terceiros.

4. Os n.os 1, 2 e 3 não afetam os requisitos e as obrigações estabelecidos no título III do presente regulamento.

TÍTULO V

MEDIDAS DE APOIO À INOVAÇÃO

Artigo 53.º
Ambientes de testagem da regulamentação da inteligência artificial

1. Os ambientes de testagem da regulamentação da IA estabelecidos pelas autoridades competentes de um ou vários Estados-Membros ou pela Autoridade Europeia para a Proteção de Dados devem proporcionar um ambiente controlado que facilite o desenvolvimento, a testagem e a validação de sistemas de IA inovadores por um período limitado antes da sua colocação no mercado ou colocação em serviço de acordo com um plano específico. Tal deve ocorrer sob a supervisão e orientação diretas das autoridades competentes com vista a garantir a conformidade com os requisitos do presente regulamento e, quando pertinente, de outra legislação da União e dos Estados-Membros supervisionada no ambiente de testagem.

2. Os Estados-Membros devem assegurar que, no caso de os sistemas de IA inovadores envolverem o tratamento de dados pessoais ou de outro modo se enquadrarem na competência de supervisão de outras autoridades nacionais ou autoridades competentes que disponibilizam ou apoiam o acesso a dados, as autoridades nacionais de proteção de dados e essas outras autoridades nacionais são associadas ao funcionamento do ambiente de testagem da regulamentação da IA.

3. Os ambientes de testagem da regulamentação da IA não afetam os poderes de supervisão e de correção das autoridades competentes. A identificação de quaisquer riscos significativos para a saúde e a segurança e os direitos fundamentais durante o desenvolvimento e a testagem desses sistemas deve conduzir à adoção imediata de medidas de atenuação e, na sua falta, à suspensão do processo de desenvolvimento e testagem até que se verifique essa atenuação.

4. Os participantes no ambiente de testagem da regulamentação da IA continuam a ser responsáveis, nos termos da legislação aplicável da União e dos Estados-Membros em matéria de responsabilidade, por quaisquer danos infligidos a terceiros em resultado da experimentação que ocorre no ambiente de testagem.

5. As autoridades competentes dos Estados-Membros que criaram ambientes de testagem da regulamentação da IA devem coordenar as suas atividades e cooperar no quadro do Comité Europeu para a Inteligência Artificial. Essas autoridades devem

apresentar relatórios anuais ao Comité e à Comissão sobre os resultados da aplicação desse sistema, incluindo boas práticas, ensinamentos retirados e recomendações sobre a sua configuração e, se for caso disso, sobre a aplicação do presente regulamento e de outra legislação da União supervisionada no ambiente de testagem.

6. As modalidades e condições de funcionamento dos ambientes de testagem da regulamentação da IA, incluindo os critérios de elegibilidade e o procedimento de candidatura, seleção, participação e saída do ambiente de testagem, bem como os direitos e as obrigações dos participantes, devem ser estabelecidas em atos de execução. Os referidos atos de execução são adotados de acordo com o procedimento de exame a que se refere o artigo 74.º, n.º 2.

Artigo 54.º

Tratamento adicional de dados pessoais para efeitos de desenvolvimento de certos sistemas de inteligência artificial de interesse público no ambiente de testagem da regulamentação da inteligência artificial

1. No ambiente de testagem da regulamentação da IA, os dados pessoais legalmente recolhidos para outras finalidades podem ser tratados com vista a desenvolver e testar certos sistemas de IA inovadores no ambiente de testagem nas seguintes condições:

   a) Os sistemas de IA inovadores devem ser desenvolvidos para salvaguarda de um interesse público substancial num ou mais dos seguintes domínios:

      i) prevenção, investigação, deteção ou repressão de infrações penais, ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas, sob o controlo e a responsabilidade das autoridades competentes. O tratamento obedece ao disposto na legislação do Estado-Membro ou da União,

      ii) segurança pública e saúde pública, nomeadamente a prevenção, o controlo e o tratamento de doenças,

      iii) elevado nível de proteção e melhoria da qualidade do ambiente;

   b) Os dados tratados são necessários para cumprir um ou vários dos requisitos referidos no título III, capítulo 2, caso esses requisitos não possam ser eficazmente cumpridos mediante tratamento de dados anonimizados, sintéticos ou outros dados não pessoais;

   c) Existem mecanismos de controlo eficazes para identificar quaisquer riscos elevados para os direitos fundamentais dos titulares dos dados que possam surgir durante a experimentação no ambiente de testagem, bem como um mecanismo de resposta para atenuar prontamente esses riscos e, se necessário, interromper o tratamento;

   d) Todos os dados pessoais a tratar no contexto do ambiente de testagem se encontram num ambiente de tratamento de dados funcionalmente separado, isolado e protegido sob o controlo dos participantes, sendo apenas acessíveis a pessoas autorizadas;

   e) Nenhuns dados pessoais tratados são transmitidos, transferidos ou acedidos, de outro modo, por terceiros;

f) Nenhum tratamento de dados pessoais no contexto do ambiente de testagem dá origem a medidas ou decisões que afetem os titulares dos dados;

g) Todos os dados pessoais tratados no contexto do ambiente de testagem são apagados assim que a participação no ambiente de testagem terminar ou que os dados pessoais atingirem o fim do respetivo período de conservação;

h) Os registos do tratamento de dados pessoais no contexto do ambiente de testagem são mantidos durante a participação no ambiente de testagem e pelo período de um ano após o respetivo termo, apenas enquanto forem necessários para efeitos exclusivos de cumprimento de obrigações em matéria de responsabilidade e documentação previstas no presente artigo ou em outra legislação da União ou dos Estados-Membros aplicável;

i) É mantida, juntamente com os resultados dos testes, uma descrição completa e pormenorizada do processo e da lógica subjacentes ao treino, ao teste e à validação do sistema de IA como parte da documentação técnica prevista no anexo IV;

j) Uma breve síntese do projeto de IA desenvolvido no ambiente de testagem, incluindo os seus objetivos e resultados esperados, é publicada no sítio Web das autoridades competentes.

2. O n.º 1 não prejudica a legislação da União ou dos Estados-Membros que exclui o tratamento para outras finalidades que não as explicitamente mencionadas nessa legislação.

Artigo 55.º

Medidas para fornecedores e utilizadores de pequena dimensão

1. Os Estados-Membros devem empreender as seguintes ações:

a) Proporcionar aos fornecedores de pequena dimensão e às empresas em fase de arranque acesso prioritário aos ambientes de testagem da regulamentação da IA, desde que cumpram as condições de elegibilidade;

b) Organizar atividades de sensibilização específicas sobre a aplicação do presente regulamento adaptadas às necessidades dos fornecedores e utilizadores de pequena dimensão;

c) Se for caso disso, criar um canal específico para comunicação com fornecedores e utilizadores de pequena dimensão e outros inovadores, com o intuito de fornecer orientações e responder a consultas sobre a aplicação do presente regulamento.

2. Os interesses e as necessidades específicas dos fornecedores de pequena dimensão devem ser tidas em conta aquando da fixação das taxas a pagar pela avaliação da conformidade nos termos do artigo 43.º, reduzindo essas taxas proporcionalmente à sua dimensão e à dimensão do mercado.

TÍTULO VI

GOVERNAÇÃO

CAPÍTULO 1

COMITÉ EUROPEU PARA A INTELIGÊNCIA ARTIFICIAL

Artigo 56.º
Criação do Comité Europeu para a Inteligência Artificial

1. É criado um Comité Europeu para a Inteligência Artificial (adiante designado por «Comité»).

2. O Comité presta aconselhamento e assistência à Comissão com vista a:

   a) Contribuir para a cooperação eficaz entre as autoridades nacionais de controlo e a Comissão no tocante às matérias abrangidas pelo presente regulamento;

   b) Coordenar e contribuir para a elaboração de orientações e análises por parte da Comissão e das autoridades nacionais de controlo, bem como de outras autoridades competentes, sobre questões emergentes no mercado interno no tocante às matérias abrangidas pelo presente regulamento;

   c) Auxiliar as autoridades nacionais de controlo e a Comissão a garantirem a aplicação coerente do presente regulamento.

Artigo 57.º
Estrutura do Comité

1. O Comité é composto pelas autoridades nacionais de controlo, que são representadas pelo seu presidente ou funcionário de alto nível equivalente, e pela Autoridade Europeia para a Proteção de Dados. Podem ser convidadas para as reuniões outras autoridades nacionais, sempre que as questões debatidas sejam pertinentes para as mesmas.

2. O Comité adota o seu regulamento interno por maioria simples dos membros que o compõem, após a autorização da Comissão. O regulamento interno deve conter igualmente os aspetos operacionais relacionados com o exercício das funções do Comité elencadas no artigo 58.º. O Comité pode constituir subgrupos consoante adequado para efeitos da análise de questões específicas.

3. O Comité é presidido pela Comissão. A Comissão convoca as reuniões e prepara a ordem de trabalhos de acordo com as funções do Comité nos termos do presente regulamento e com o seu regulamento interno. A Comissão presta apoio administrativo e analítico às atividades do Comité nos termos com o presente regulamento.

4. O Comité pode convidar peritos e observadores externos para participarem nas suas reuniões e pode realizar intercâmbios com terceiros interessados, a fim de fundamentar as suas atividades, na medida adequada. Para o efeito, a Comissão pode facilitar intercâmbios entre o Comité e outras instituições, órgãos, organismos e grupos consultivos da União.

Artigo 58.º
Funções do Comité

Ao prestar aconselhamento e assistência à Comissão nos termos do artigo 56.º, n.º 2, o Comité deve em particular:

a) Recolher e partilhar conhecimentos técnicos e boas práticas entre Estados-Membros;

b) Contribuir para uniformizar práticas administrativas nos Estados-Membros, nomeadamente no respeitante ao funcionamento dos ambientes de testagem da regulamentação a que se refere o artigo 53.º;

c) Emitir pareceres, recomendações ou contribuições escritas sobre matérias relacionadas com a aplicação do presente regulamento, em especial:

   i) sobre especificações técnicas ou normas existentes relativas aos requisitos estabelecidos no título III, capítulo 2,

   ii) sobre a utilização de normas harmonizadas ou especificações comuns a que se referem os artigos 40.º e 41.º,

   iii) sobre a preparação de documentos de orientação, nomeadamente as orientações relativas à fixação de coimas a que se refere o artigo 71.º.

CAPÍTULO 2

AUTORIDADES NACIONAIS COMPETENTES

Artigo 59.º
Designação das autoridades nacionais competentes

1. Cada Estado-Membro deve criar ou designar autoridades nacionais competentes a fim de assegurar a aplicação e execução do presente regulamento. As autoridades nacionais competentes devem estar organizadas de modo que garanta a objetividade e a imparcialidade das suas atividades e funções.

2. Cada Estado-Membro deve designar uma autoridade nacional de controlo entre as autoridades nacionais competentes. A autoridade nacional de controlo deve atuar enquanto autoridade notificadora e autoridade de fiscalização do mercado, salvo se, por razões organizacionais e administrativas, o Estado-Membro tiver de designar mais do que uma autoridade.

3. Os Estados-Membros devem informar a Comissão da designação ou designações e, se for caso disso, dos motivos que os levaram a designar mais do que uma autoridade.

4. Os Estados-Membros devem assegurar que as autoridades nacionais competentes disponham dos recursos financeiros e humanos adequados para exercerem as funções que lhes incumbem nos termos do presente regulamento. Em especial, as autoridades nacionais competentes devem dispor permanentemente de suficiente pessoal cujas competências e conhecimentos especializados incluam uma compreensão profunda das tecnologias de inteligência artificial, dos dados e da computação de dados, dos direitos fundamentais e dos riscos para a saúde e a segurança, bem como conhecimento das normas e dos requisitos legais em vigor.

5. Os Estados-Membros devem apresentar anualmente relatórios à Comissão sobre a situação dos recursos financeiros e humanos ao dispor das autoridades nacionais competentes, incluindo uma avaliação da sua adequação. A Comissão transmite essas informações ao Comité para apreciação e eventuais recomendações.

6. A Comissão facilita o intercâmbio de experiências entre as autoridades nacionais competentes.

7. As autoridades nacionais competentes podem fornecer orientações e prestar aconselhamento sobre a execução do presente regulamento, nomeadamente aos fornecedores de pequena dimensão. Sempre que as autoridades nacionais competentes pretendam fornecer orientações e prestar aconselhamento em relação a um sistema de IA em domínios abrangidos por outra legislação da União, as autoridades nacionais competentes ao abrigo dessa legislação da União devem ser consultadas, conforme adequado. Os Estados-Membros também podem criar um ponto de contacto central para a comunicação com os operadores.

8. Sempre que as instituições, órgãos e organismos da União se insiram no âmbito do presente regulamento, a Autoridade Europeia para a Proteção de Dados deve atuar como a autoridade competente para o controlo dos mesmos.

TÍTULO VII

BASE DE DADOS DA UE RELATIVA A SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO AUTÓNOMOS

Artigo 60.º

Base de dados da UE relativa a sistemas de inteligência artificial de risco elevado autónomos

1. A Comissão, em colaboração com os Estados-Membros, cria e mantém uma base de dados da UE que contenha as informações referidas no n.º 2 relativas aos sistemas de IA de risco elevado a que se refere o artigo 6.º, n.º 2, que sejam registados em conformidade com o artigo 51.º.

2. Cabe aos fornecedores introduzir os dados enumerados no anexo VIII na base de dados da UE. A Comissão faculta-lhes apoio técnico e administrativo.

3. As informações que constam da base de dados da UE devem estar acessíveis ao público.

4. A base de dados da UE só pode conter dados pessoais se estes forem necessários para recolher e tratar informações em conformidade com o presente regulamento. Essas informações incluem os nomes e os contactos das pessoas singulares responsáveis pelos registos no sistema e com autoridade jurídica para representar o fornecedor.

5. A Comissão é considerada responsável pelo tratamento de dados da base de dados da UE. Além disso, assegura aos fornecedores o apoio técnico e administrativo adequado.

TÍTULO VIII

ACOMPANHAMENTO PÓS-COMERCIALIZAÇÃO, PARTILHA DE INFORMAÇÕES, FISCALIZAÇÃO DO MERCADO

CAPÍTULO 1

ACOMPANHAMENTO PÓS-COMERCIALIZAÇÃO

Artigo 61.º
Acompanhamento pós-comercialização pelos fornecedores e plano de acompanhamento pós-comercialização aplicável a sistemas de inteligência artificial de risco elevado

1. Os fornecedores devem criar e documentar um sistema de acompanhamento pós-comercialização que seja proporcionado à natureza das tecnologias de inteligência artificial e aos riscos do sistema de IA de risco elevado.

2. O sistema de acompanhamento pós-comercialização deve recolher, documentar e analisar de forma ativa e sistemática dados pertinentes fornecidos pelos utilizadores ou recolhidos por meio de outras fontes sobre o desempenho dos sistemas de IA de risco elevado ao longo da sua vida útil, bem como permitir ao fornecedor avaliar a contínua conformidade dos sistemas de IA com os requisitos estabelecidos no título III, capítulo 2.

3. O sistema de monitorização pós-comercialização deve basear-se num plano de acompanhamento pós-comercialização. O plano de acompanhamento pós-comercialização deve fazer parte da documentação técnica referida no anexo IV. A Comissão adota um ato de execução com disposições pormenorizadas que estabeleçam um modelo para o plano de acompanhamento pós-comercialização e a lista de elementos a incluir no plano.

4. No respeitante aos sistemas de IA de risco elevado abrangidos pelos atos jurídicos referidos no anexo II, relativamente aos quais já se encontram estabelecidos um sistema e um plano de acompanhamento pós-comercialização ao abrigo dessa legislação, os elementos descritos nos n.os 1, 2 e 3 devem ser integrados nesse sistema e nesse plano, consoante adequado.

   O primeiro parágrafo também é aplicável aos sistemas de IA de risco elevado referidos no anexo III, ponto 5, alínea b), colocados no mercado ou colocados em serviço por instituições de crédito regulamentadas pela Diretiva 2013/36/UE.

CAPÍTULO 2

PARTILHA DE INFORMAÇÕES SOBRE INCIDENTES E ANOMALIAS

Artigo 62.º
Comunicação de incidentes graves e anomalias

1. Os fornecedores de sistemas de IA de risco elevado colocados no mercado da União devem comunicar quaisquer incidentes graves ou anomalias desses sistemas que constituam um incumprimento de obrigações impostas pela legislação da União

destinada a proteger os direitos fundamentais às autoridades de fiscalização do mercado dos Estados-Membros onde esse incidente ou incumprimento ocorrer.

Essa notificação deve ser efetuada imediatamente após o fornecedor ter determinado uma relação causal entre o sistema de IA e o incidente ou anomalia ou a probabilidade razoável dessa relação e, em qualquer caso, o mais tardar 15 dias após o fornecedor ter conhecimento do incidente grave ou da anomalia.

2. Após receção de uma notificação relacionada com um incumprimento de obrigações impostas por legislação da União destinada a proteger os direitos fundamentais, a autoridade de fiscalização do mercado deve informar as autoridades ou os organismos públicos nacionais referidos no artigo 64.º, n.º 3. A Comissão elabora orientações específicas para facilitar o cumprimento das obrigações previstas no n.º 1. As referidas orientações devem ser publicadas, o mais tardar, 12 meses após a entrada em vigor do presente regulamento.

3. Relativamente aos sistemas de IA de risco elevado referidos no anexo III, ponto 5, alínea b), colocados no mercado ou colocados em serviço por fornecedores que sejam instituições de crédito regulamentadas pela Diretiva 2013/36/UE e relativamente aos sistemas de IA de risco elevado que sejam componentes de segurança de dispositivos ou sejam, eles próprios, dispositivos abrangidos pelos Regulamentos (UE) 2017/745 e (UE) 2017/746, a notificação de incidentes graves ou anomalias limita-se aos casos que constituam um incumprimento de obrigações impostas por legislação da União destinada a proteger os direitos fundamentais.

CAPÍTULO 3

EXECUÇÃO

Artigo 63.º

Fiscalização do mercado e controlo dos sistemas de inteligência artificial presentes no mercado da União

1. O Regulamento (UE) 2019/1020 é aplicável aos sistemas de IA abrangidos pelo presente regulamento. Contudo, para efeitos da execução efetiva do presente regulamento:

   a) Qualquer referência a um operador económico nos termos do Regulamento (UE) 2019/1020 deve ser entendida como incluindo todos os operadores identificados no título III, capítulo 3, do presente regulamento;

   b) Qualquer referência a um produto nos termos do Regulamento (UE) 2019/1020 deve ser entendida como incluindo todos os sistemas de IA que se enquadrem no âmbito do presente regulamento.

2. A autoridade nacional de controlo deve comunicar regularmente à Comissão os resultados das atividades de fiscalização do mercado pertinentes. A autoridade nacional de controlo deve comunicar, sem demora, à Comissão e às autoridades nacionais da concorrência adequadas quaisquer informações reveladas no decurso de atividades de fiscalização do mercado que possam ter interesse para efeitos de aplicação do direito da União relativo às regras de concorrência.

3. No caso dos sistemas de IA de risco elevado relacionados com produtos aos quais se apliquem atos jurídicos enunciados no anexo II, secção A, a autoridade de

fiscalização do mercado para efeitos do presente regulamento deve ser a autoridade responsável pelas atividades de fiscalização do mercado designada nos termos desses atos jurídicos.

4. No caso dos sistemas de IA colocados no mercado, colocados em serviço ou utilizados por instituições financeiras regulamentadas pela legislação da União em matéria de serviços financeiros, a autoridade de fiscalização do mercado para efeitos do presente regulamento deve ser a autoridade responsável pela supervisão financeira dessas instituições ao abrigo da referida legislação.

5. No respeitante aos sistemas de IA enumerados no anexo III, ponto 1, alínea a), contanto que sejam utilizados para efeitos de manutenção da ordem pública, e pontos 6 e 7, os Estados-Membros devem designar como autoridades de fiscalização do mercado para efeitos do presente regulamento as autoridades de controlo no domínio da proteção de dados, designadas nos termos da Diretiva (UE) 2016/680 ou do Regulamento (UE) 2016/679, ou as autoridades nacionais competentes que fiscalizam as atividades das autoridades competentes em matéria de manutenção da ordem pública, imigração ou asilo que colocam em serviço ou utilizam esses sistemas.

6. Sempre que as instituições, órgãos e organismos da União se insiram no âmbito do presente regulamento, a Autoridade Europeia para a Proteção de Dados deve atuar como a autoridade de fiscalização do mercado dos mesmos.

7. Os Estados-Membros devem facilitar a coordenação entre as autoridades de fiscalização do mercado designadas nos termos do presente regulamento e outras autoridades ou organismos nacionais competentes que supervisionam a aplicação da legislação de harmonização da União enunciada no anexo III ou de outra legislação da União que possa ser aplicável aos sistemas de IA de risco elevado referidos no anexo III.

Artigo 64.º
Acesso a dados e a documentação

1. No que toca ao acesso a dados e a documentação no contexto das suas atividades, as autoridades de fiscalização do mercado devem dispor de total acesso aos conjuntos de dados de treino, validação e teste utilizados pelo fornecedor, incluindo através de interfaces de programação de aplicações ou outros meios e ferramentas técnicas adequadas que possibilitem o acesso remoto.

2. Sempre que necessário para avaliar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no título III, capítulo 2, e mediante pedido fundamentado, deve ser concedido às autoridades de fiscalização do mercado o acesso ao código-fonte do sistema de IA.

3. As autoridades ou organismos públicos nacionais que supervisionam ou asseguram, no atinente à utilização de sistemas de IA de risco elevado referidos no anexo III, o respeito das obrigações previstas na legislação da União que protege os direitos fundamentais devem ter poderes para solicitar e aceder a toda a documentação elaborada ou mantida nos termos do presente regulamento, nos casos em que o acesso a essa documentação for necessário para o exercício das competências incluídas nos seus mandatos e dentro dos limites das respetivas jurisdições. A autoridade ou o organismo público competente deve informar a autoridade de

fiscalização do mercado do Estado-Membro em causa de qualquer pedido dessa natureza.

4. No prazo de três meses a contar da entrada em vigor do presente regulamento, cada Estado-Membro deve identificar as autoridades ou os organismos públicos referidos no n.º 3 e elaborar uma lista que esteja acessível ao público no sítio Web da autoridade nacional de controlo. Os Estados-Membros devem notificar a lista à Comissão e a todos os outros Estados-Membros e mantê-la atualizada.

5. Se a documentação referida no n.º 3 for insuficiente para determinar se ocorreu um incumprimento de obrigações impostas por legislação da União destinada a proteger os direitos fundamentais, a autoridade ou o organismo público referido no n.º 3 pode apresentar um pedido fundamentado à autoridade de fiscalização do mercado para organizar a testagem do sistema de IA de risco elevado por recurso a meios técnicos. A autoridade de fiscalização do mercado deve organizar a testagem com a participação ativa da autoridade ou do organismo público requerente num prazo razoável após o pedido.

6. Todas as informações e documentação que as autoridades ou organismos públicos nacionais referidos no n.º 3 obtenham nos termos das disposições do presente artigo devem ser tratadas em conformidade com as obrigações de confidencialidade estabelecidas no artigo 70.º.

Artigo 65.º
Procedimento aplicável aos sistemas de inteligência artificial que apresentam riscos a nível nacional

1. Entende-se por «sistema de IA que apresenta um risco» um «produto que apresenta um risco», na aceção do artigo 3.º, ponto 19, do Regulamento (UE) 2019/1020, contanto que estejam em causa riscos para a saúde e a segurança ou para a proteção dos direitos fundamentais das pessoas.

2. Se a autoridade de fiscalização do mercado de um Estado-Membro tiver motivos suficientes para considerar que um sistema de IA apresenta um risco, tal como descrito no n.º 1, deve avaliar o sistema de IA em causa no que diz respeito à conformidade do mesmo com todos os requisitos e obrigações previstos no presente regulamento. Se estiverem presentes riscos para a proteção dos direitos fundamentais, a autoridade de fiscalização do mercado também deve informar as autoridades ou os organismos públicos nacionais competentes referidos no artigo 64.º, n.º 3. Os operadores envolvidos devem cooperar na medida do necessário com as autoridades de fiscalização do mercado e as outras autoridades ou organismos públicos nacionais referidos no artigo 64.º, n.º 3.

   Se, no decurso dessa avaliação, a autoridade de fiscalização do mercado verificar que o sistema de IA não cumpre os requisitos e as obrigações previstas no presente regulamento, deve exigir imediatamente ao operador correspondente que tome todas as medidas corretivas adequadas para assegurar a conformidade do sistema de IA, para o retirar do mercado ou para o recolher num prazo fixado pela autoridade que seja razoável e proporcionado à natureza do risco.

   A autoridade de fiscalização do mercado deve informar desse facto o organismo notificado pertinente. O artigo 18.º do Regulamento (UE) 2019/1020 é aplicável às medidas referidas no segundo parágrafo.

3. Se a autoridade de fiscalização do mercado considerar que a não conformidade não se limita ao respetivo território nacional, deve comunicar à Comissão e aos outros Estados-Membros os resultados da avaliação e as medidas que exigiu que o operador tomasse.

4. O operador deve garantir a aplicação de todas as medidas corretivas adequadas relativamente aos sistemas de IA em causa por si disponibilizados no mercado da União.

5. Se o operador de um sistema de IA não adotar as medidas corretivas adequadas no prazo referido no n.º 2, a autoridade de fiscalização do mercado deve tomar todas as medidas provisórias adequadas para proibir ou restringir a disponibilização do sistema de IA no respetivo mercado nacional, para o retirar do mercado ou para o recolher. A referida autoridade deve informar sem demora a Comissão e os outros Estados-Membros da adoção de tais medidas.

6. A notificação referida no n.º 5 deve conter todas as informações disponíveis, em especial os dados necessários à identificação do sistema de IA não conforme, a origem do sistema de IA, a natureza da alegada não conformidade e o risco conexo, a natureza e a duração das medidas nacionais adotadas, bem como as observações do operador em causa. As autoridades de fiscalização do mercado devem, nomeadamente, indicar se a não conformidade se deve a uma ou várias das seguintes razões:

   a) O incumprimento, por parte do sistema de IA, dos requisitos estabelecidos no título III, capítulo 2;

   b) Deficiências das normas harmonizadas ou das especificações comuns que, nos termos dos artigos 40.º e 41.º, conferem uma presunção de conformidade.

7. As autoridades de fiscalização do mercado dos Estados-Membros, com exceção da autoridade de fiscalização do mercado do Estado-Membro que desencadeou o procedimento, devem informar sem demora a Comissão e os outros Estados-Membros das medidas tomadas e das informações adicionais de que disponham relativamente à não conformidade do sistema de IA em causa e, em caso de desacordo com a medida nacional notificada, das suas objeções.

8. Se, no prazo de três meses a contar da receção das informações referidas no n.º 5, nem os Estados-Membros nem a Comissão tiverem levantado objeções à medida provisória tomada por um Estado-Membro, considera-se que a mesma é justificada. Esta disposição aplica-se sem prejuízo dos direitos processuais do operador em causa previstos no artigo 18.º do Regulamento (UE) 2019/1020.

9. As autoridades de fiscalização do mercado de todos os Estados-Membros devem garantir que as medidas restritivas adequadas relativas ao produto em causa, como a retirada deste do respetivo mercado, sejam tomadas sem demora.

Artigo 66.º
Procedimento de salvaguarda da União

1. Se, nos três meses subsequentes à receção da notificação a que se refere o artigo 65.º, n.º 5, um Estado-Membro levantar objeções a uma medida tomada por outro Estado-Membro, ou a Comissão considerar que a medida é contrária ao direito da União, a Comissão procede sem demora a consultas com o Estado-Membro e o operador ou operadores em causa e avalia a medida nacional. Em função dos

resultados dessa avaliação, a Comissão decide se a medida nacional é ou não justificada no prazo de nove meses a contar da notificação referida no artigo 65.º, n.º 5, e notifica essa decisão ao Estado-Membro em causa.

2. Se a medida nacional for considerada justificada, todos os Estados-Membros devem tomar as medidas necessárias para garantir que o sistema de IA não conforme seja retirado dos respetivos mercados, informando a Comissão das mesmas. Se a medida nacional for considerada injustificada, o Estado-Membro em causa deve revogá-la.

3. Se a medida nacional for considerada justificada e a não conformidade do sistema de IA for atribuída a deficiências das normas harmonizadas ou das especificações comuns referidas nos artigos 40.º e 41.º do presente regulamento, a Comissão aplica o procedimento previsto no artigo 11.º do Regulamento (UE) n.º 1025/2012.

Artigo 67.º
Sistemas de inteligência artificial conformes que apresentam um risco

1. Se, uma vez realizada a avaliação prevista no artigo 65.º, a autoridade de fiscalização do mercado de um Estado-Membro verificar que, embora conforme com o presente regulamento, um sistema de IA apresenta um risco para a saúde ou a segurança das pessoas, para o cumprimento de obrigações impostas por legislação da União ou nacional destinada a proteger os direitos fundamentais ou para outras vertentes de proteção do interesse público, deve exigir ao operador correspondente que tome todas as medidas adequadas para garantir que quando o sistema de IA em causa for colocado no mercado ou colocado em serviço já não apresente esse risco, para o retirar do mercado ou para o recolher num prazo fixado pela autoridade que seja razoável e proporcionado à natureza do risco.

2. O fornecedor ou outros operadores envolvidos devem assegurar que a medida corretiva seja tomada no tocante a todos os sistemas de IA em causa que tenham disponibilizado no mercado da União no prazo fixado pela autoridade de fiscalização do mercado do Estado-Membro referido no n.º 1.

3. O Estado-Membro deve informar imediatamente a Comissão e os restantes Estados-Membros deste facto. Essa notificação deve incluir todas as informações disponíveis, em particular os dados necessários à identificação do sistema de IA em causa, a origem e a cadeia de abastecimento do sistema de IA, a natureza do risco conexo e a natureza e duração das medidas nacionais adotadas.

4. A Comissão procede sem demora a consultas com os Estados-Membros e com o operador em causa e avalia as medidas nacionais adotadas. Em função dos resultados dessa avaliação, a Comissão decide se a medida é ou não justificada e, se necessário, propõe medidas adequadas.

5. A Comissão designa os Estados-Membros como destinatários da decisão.

Artigo 68.º
Não conformidade formal

1. Se a autoridade de fiscalização do mercado de um Estado-Membro constatar um dos factos a seguir enunciados, deve exigir ao fornecedor em causa que ponha termo à não conformidade verificada:

   a) A marcação de conformidade foi aposta em violação do disposto no artigo 49.º;

   b) A marcação de conformidade não foi aposta;

c) A declaração de conformidade UE não foi elaborada;

d) A declaração de conformidade UE não foi elaborada corretamente;

e) O número de identificação do organismo notificado envolvido, se for caso disso, no procedimento de avaliação da conformidade não foi aposto.

2. Se a não conformidade referida no n.º 1 persistir, o Estado-Membro em causa deve tomar as medidas adequadas para restringir ou proibir a disponibilização no mercado do sistema de IA de risco elevado ou para garantir que o mesmo seja recolhido ou retirado do mercado.

TÍTULO IX

CÓDIGOS DE CONDUTA

Artigo 69.º
Códigos de conduta

1. A Comissão e os Estados-Membros devem incentivar e facilitar a elaboração de códigos de conduta destinados a fomentar a aplicação voluntária dos requisitos estabelecidos no título III, capítulo 2, a sistemas de IA que não sejam sistemas de IA de risco elevado, com base em especificações técnicas e soluções que configurem meios adequados de assegurar a conformidade com os referidos requisitos atendendo à finalidade prevista dos sistemas.

2. A Comissão e o Comité devem incentivar e facilitar a elaboração de códigos de conduta destinados a fomentar a aplicação voluntária a sistemas de IA de requisitos relacionados, por exemplo, com a sustentabilidade ambiental, a acessibilidade das pessoas com deficiência, a participação das partes interessadas na conceção e no desenvolvimento de sistemas de IA e a diversidade das equipas de desenvolvimento, com base em objetivos claros e indicadores-chave de desempenho que permitam medir a consecução desses objetivos.

3. Os códigos de conduta podem ser elaborados por fornecedores de sistemas de IA a título individual ou por organizações que os representem, ou ambos, nomeadamente com a participação de utilizadores e de quaisquer partes interessadas e das respetivas organizações representativas. Os códigos de conduta podem abranger um ou mais sistemas de IA, tendo em conta a semelhança da finalidade prevista desses sistemas.

4. A Comissão e o Comité devem ter em conta as necessidades e os interesses específicos dos fornecedores de pequena dimensão e das empresas em fase de arranque quando incentivam e facilitam a elaboração de códigos de conduta.

TÍTULO X

CONFIDENCIALIDADE E SANÇÕES

Artigo 70.º
Confidencialidade

1. As autoridades nacionais competentes e os organismos notificados envolvidos na aplicação do presente regulamento devem respeitar a confidencialidade das

informações e dos dados obtidos no exercício das suas funções e atividades de modo que protejam, em especial:

a) Os direitos de propriedade intelectual e as informações comerciais confidenciais ou segredos comerciais de uma pessoa singular ou coletiva, incluindo o código-fonte, exceto nos casos a que se refere o artigo 5.º da Diretiva 2016/943 relativa à proteção de *know-how* e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais;

b) A execução efetiva do presente regulamento, em especial no que diz respeito à realização de inspeções, investigações ou auditorias; c) Interesses públicos e nacionais em matéria de segurança;

c) A integridade de processos penais ou administrativos.

2. Sem prejuízo do n.º 1, no caso de sistemas de IA de risco elevado referidos no anexo III, pontos 1, 6 e 7, utilizados por autoridades competentes em matéria de manutenção da ordem pública, de imigração ou de asilo, as informações trocadas numa base confidencial entre as autoridades nacionais competentes e entre as autoridades nacionais competentes e a Comissão não podem ser divulgadas sem consultar previamente a autoridade nacional competente de origem e o utilizador, quando tal divulgação prejudicar interesses públicos e nacionais em matéria de segurança.

   Se as autoridades competentes em matéria de manutenção da ordem pública, de imigração ou de asilo forem os fornecedores de sistemas de IA de risco elevado referidos no anexo III, pontos 1, 6 e 7, a documentação técnica referida no anexo IV deve permanecer nas instalações dessas autoridades. As referidas autoridades devem assegurar que as autoridades de fiscalização do mercado referidas no artigo 63.º, n.os 5 e 6, consoante o caso, possam, mediante pedido, aceder imediatamente à documentação ou obter uma cópia da mesma. O acesso à referida documentação ou a qualquer cópia da mesma só pode ser concedido ao pessoal da autoridade de fiscalização do mercado que detenha o nível apropriado de credenciação de segurança.

3. O disposto nos n.os 1 e 2 não afeta os direitos e obrigações da Comissão, dos Estados-Membros e dos organismos notificados no que se refere ao intercâmbio de informações e à divulgação de avisos, nem o dever de informação que incumbe às partes em causa no âmbito do direito penal dos Estados-Membros.

4. A Comissão e os Estados-Membros podem, quando necessário, trocar informações confidenciais com autoridades reguladoras de países terceiros com as quais tenham celebrado acordos de confidencialidade bilaterais ou multilaterais desde que garantam um nível adequado de confidencialidade.

Artigo 71.º
Sanções

1. Em conformidade com os termos e as condições previstas no presente regulamento, os Estados-Membros devem estabelecer o regime de sanções, incluindo coimas, aplicáveis em caso de infração ao presente regulamento e devem tomar todas as medidas necessárias para garantir que o mesmo é aplicado correta e eficazmente. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas. Devem ter

especialmente em conta os interesses dos fornecedores de pequena dimensão e das empresas em fase de arranque e a respetiva viabilidade económica.

2. Os Estados-Membros devem notificar a Comissão dessas regras e dessas medidas e também, sem demora, de qualquer alteração ulterior das mesmas.

3. Ficam sujeitas a coimas até 30 000 000 EUR ou, se o infrator for uma empresa, até 6 % do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado, as seguintes infrações:

   a) Incumprimento da proibição das práticas de inteligência artificial referidas no artigo 5.º;

   b) Não conformidade do sistema de IA com os requisitos estabelecidos no artigo 10.º.

4. A não conformidade do sistema de IA com quaisquer requisitos ou obrigações por força do presente regulamento, que não os estabelecidos nos artigos 5.º e 10.º, fica sujeita a coimas até 20 000 000 EUR ou, se o infrator for uma empresa, até 4 % do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado.

5. O fornecimento de informações incorretas, incompletas ou enganadoras aos organismos notificados e às autoridades nacionais competentes em resposta a um pedido fica sujeito a coimas até 10 000 000 EUR ou, se o infrator for uma empresa, até 2 % do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado.

6. A decisão relativa ao montante da coima a aplicar em cada caso deve ter em conta todas as circunstâncias pertinentes da situação específica, bem como os seguintes elementos:

   a) A natureza, a gravidade e a duração da infração e das suas consequências;

   b) Se outras autoridades de fiscalização do mercado já aplicaram coimas ao mesmo operador pela mesma infração;

   c) A dimensão e quota-parte de mercado do operador que cometeu a infração.

7. Cada Estado-Membro deve definir regras que permitam determinar se e em que medida podem ser aplicadas coimas às autoridades e organismos públicos estabelecidos nesse Estado-Membro.

8. Dependendo do ordenamento jurídico dos Estados-Membros, as regras relativas às coimas podem ser aplicadas de maneira que as coimas sejam impostas por tribunais nacionais ou por outros organismos competentes, tal como previsto nesses Estados-Membros. A aplicação dessas regras nesses Estados-Membros deve ter um efeito equivalente.

Artigo 72.º
Coimas aplicáveis às instituições, órgãos e organismos da União

1. A Autoridade Europeia para a Proteção de Dados pode impor coimas às instituições, órgãos e organismos da União que se enquadrem no âmbito do presente regulamento. Ao decidir sobre a imposição de uma coima e o montante da mesma, devem ser tidas em conta, em cada caso, todas as circunstâncias pertinentes da situação específica, bem como os seguintes elementos:

a) A natureza, a gravidade e a duração da infração e das suas consequências;

b) A cooperação com a Autoridade Europeia para a Proteção de Dados no sentido de corrigir a infração e atenuar os possíveis efeitos adversos da mesma, nomeadamente o cumprimento de eventuais medidas previamente impostas pela Autoridade Europeia para a Proteção de Dados contra a instituição, órgão ou organismo da União em causa relativamente à mesma matéria;

c) Quaisquer infrações similares anteriormente cometidas pela instituição, órgão ou organismo da União.

2. Ficam sujeitas a coimas até 500 000 EUR as seguintes infrações:

a) Incumprimento da proibição das práticas de inteligência artificial referidas no artigo 5.º;

b) Não conformidade do sistema de IA com os requisitos estabelecidos no artigo 10.º.

3. A não conformidade do sistema de IA com quaisquer requisitos ou obrigações por força do presente regulamento, que não os estabelecidos nos artigos 5.º e 10.º, fica sujeita a coimas até 250 000 EUR.

4. Antes de tomar decisões nos termos do presente artigo, a Autoridade Europeia para a Proteção de Dados deve conceder à instituição, órgão ou organismo da União objeto do procedimento por si aplicado a oportunidade de se pronunciar sobre a matéria que constitui possível infração. A Autoridade Europeia para a Proteção de Dados deve basear as suas decisões unicamente nos elementos e nas circunstâncias relativamente às quais as partes em causa puderam apresentar as observações. Os queixosos, caso existam, devem ser estreitamente associados ao procedimento.

5. Os direitos de defesa das partes em causa devem ser plenamente respeitados no desenrolar do processo. As partes interessadas devem ter o direito de aceder ao processo da Autoridade Europeia para a Proteção de Dados, sob reserva do interesse legítimo dos indivíduos ou das empresas relativamente à proteção dos respetivos dados pessoais ou segredos comerciais.

6. Os fundos recolhidos em resultado da imposição das coimas previstas no presente artigo constituem receitas do orçamento geral da União.

TÍTULO XI

DELEGAÇÃO DE PODERES E PROCEDIMENTO DE COMITÉ

Artigo 73.º
Exercício da delegação

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2. O poder de adotar atos delegados referido no artigo 4.º, no artigo 7.º, n.º 1, no artigo 11.º, n.º 3, no artigo 43.º, n.ºs 5 e 6, e no artigo 48.º, n.º 5, é conferido à Comissão por tempo indeterminado contar de [*data de entrada em vigor do presente regulamento*].

3. A delegação de poderes referida no artigo 4.º, no artigo 7.º, n.º 1, no artigo 11.º, n.º 3, no artigo 43.º, n.ºs 5 e 6, e no artigo 48.º, n.º 5, pode ser revogada em qualquer

momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou numa data posterior nela especificada. A decisão de revogação não afeta os atos delegados já em vigor.

4. Assim que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

5. Os atos delegados adotados nos termos do artigo 4.º, do artigo 7.º, n.º 1, do artigo 11.º, n.º 3, do artigo 43.º, n.ºs 5 e 6, e do artigo 48.º, n.º 5, só entram em vigor se nem o Parlamento Europeu nem o Conselho formularem objeções no prazo de três meses a contar da notificação desses atos a estas duas instituições ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho informarem a Comissão de que não formularão objeções. O referido prazo é prorrogável por três meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 74.º
Procedimento de comité

1. A Comissão é assistida por um comité. Este comité é um comité na aceção do Regulamento (UE) n.º 182/2011.

2. Caso se remeta para o presente número, aplica-se o artigo 5.º do Regulamento (UE) n.º 182/2011.

TÍTULO XII

DISPOSIÇÕES FINAIS

Artigo 75.º
Alteração do Regulamento (CE) n.º 300/2008

Ao artigo 4.º, n.º 3, do Regulamento (CE) n.º 300/2008, é aditado o seguinte parágrafo:

«Aquando da adoção de medidas de execução relacionadas com especificações técnicas e procedimentos para a aprovação e utilização de equipamentos de segurança respeitantes a sistemas de inteligência artificial na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 76.º
Alteração do Regulamento (UE) n.º 167/2013

Ao artigo 17.º, n.º 5, do Regulamento (UE) n.º 167/2013, é aditado o seguinte parágrafo:

«Aquando da adoção de atos delegados nos termos do primeiro parágrafo relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 77.º
Alteração do Regulamento (UE) n.º 168/2013

Ao artigo 22.º, n.º 5, do Regulamento (UE) n.º 168/2013, é aditado o seguinte parágrafo:

«Aquando da adoção de atos delegados nos termos do primeiro parágrafo relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 78.º
Alteração da Diretiva 2014/90/UE

Ao artigo 8.º da Diretiva 2014/90/UE, é aditado o seguinte número:

«4. Aquando da realização das atividades previstas no n.º 1 e da adoção de especificações técnicas e normas de ensaio em conformidade com os n.os 2 e 3 respeitantes a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, Comissão tem em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 79.º
Alteração da Diretiva (UE) 2016/797

Ao artigo 5.º da Diretiva (UE) 2016/797, é aditado o seguinte número:

«12. «Aquando da adoção de atos delegados nos termos do n.º 1 e de atos de execução nos termos do n.º 11 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 80.º
Alteração do Regulamento (UE) 2018/858

Ao artigo 5.º do Regulamento (UE) 2018/858, é aditado o seguinte número:

«4. Aquando da adoção de atos delegados nos termos do n.º 3 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do

Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 81.º
Alteração do Regulamento (UE) 2018/1139

O Regulamento (UE) 2018/1139 é alterado do seguinte modo:

1) Ao artigo 17.º, é aditado o seguinte número:

«3. Sem prejuízo do disposto no n.º 2, aquando da adoção de atos de execução nos termos do n.º 1 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»;

2) Ao artigo 19.º, é aditado o seguinte número:

«4. Aquando da adoção de atos delegados nos termos dos n.os 1 e 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.»;

3) Ao artigo 43.º, é aditado o seguinte número:

«4. Aquando da adoção de atos de execução nos termos do n.º 1 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.»;

4) Ao artigo 47.º, é aditado o seguinte número:

«3. Aquando da adoção de atos delegados nos termos dos n.os 1 e 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.»;

5) Ao artigo 57.º, é aditado o seguinte parágrafo:

Aquando da adoção desses atos de execução relativamente a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.»;

6) Ao artigo 58.º, é aditado o seguinte número:

«3. Aquando da adoção de atos delegados nos termos dos n.os 1 e 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX [relativo à inteligência artificial], devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.»

Artigo 82.º
Alteração do Regulamento (UE) 2019/2144

Ao artigo 11.º do Regulamento (UE) 2019/2144, é aditado o seguinte número:

«3. Aquando da adoção de atos de execução nos termos do n.º 2 relativos a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) YYYY/XX do Parlamento Europeu e do Conselho [relativo à inteligência artificial]*, devem ser tidos em conta os requisitos estabelecidos no título III, capítulo 2, desse regulamento.

_____

* Regulamento (UE) YYYY/XX [relativo à inteligência artificial] (JO …).»

Artigo 83.º
Sistemas de inteligência artificial já colocados no mercado ou em serviço

1. O presente regulamento não se aplica aos sistemas de IA que sejam componentes dos sistemas informáticos de grande escala criados pelos atos jurídicos enumerados no anexo IX que tenham sido colocados no mercado ou colocados em serviço antes de *[12 meses após a data de aplicação do presente regulamento referida no artigo 85.º, n.º 2]*, salvo se a substituição ou alteração desses atos jurídicos implicar uma alteração significativa da conceção ou da finalidade prevista do sistema ou dos sistemas de IA em causa.

   Os requisitos estabelecidos no presente regulamento devem ser tidos em conta, se for caso disso, na avaliação de cada um dos sistemas informáticos de grande escala criados pelos atos jurídicos enumerados no anexo IX, a realizar como previsto nos respetivos atos.

2. O presente regulamento só se aplica aos sistemas de IA de risco elevado, que não os referidos no n.º 1, que tenham sido colocados no mercado ou colocados em serviço antes de *[data de aplicação do presente regulamento referida no artigo 85.º, n.º 2]*, se, após esta data, os referidos sistemas forem sido sujeitos a alterações significativas em termos de conceção ou finalidade prevista.

Artigo 84.º
Avaliação e reexame

1. A Comissão avalia a necessidade de alterar a lista que consta do anexo III uma vez por ano após a entrada em vigor do presente regulamento.

2. Até [*três anos após a data de aplicação do presente regulamento referida no artigo 85.º, n.º 2*] e subsequentemente de quatro em quatro anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e reexame do presente regulamento. Os relatórios devem ser divulgados ao público.

3. Os relatórios referidos no n.º 2 devem dar especial atenção ao seguinte:

   a) A situação das autoridades nacionais competentes em termos dos recursos financeiros e humanos necessários para exercer eficazmente as funções que lhes foram atribuídas nos termos do presente regulamento;

   b) O estado das sanções, designadamente das coimas referidas no artigo 71.º, n.º 1, aplicadas pelos Estados-Membros em consequência de infrações às disposições do presente regulamento.

4. No prazo de [*três anos a contar da data de aplicação do presente regulamento referida no artigo 85.º, n.º 2*] e subsequentemente de quatro em quatro anos, a Comissão avalia o impacto e a eficácia dos códigos de conduta com vista a fomentar a aplicação dos requisitos estabelecidos no título III, capítulo 2, e, eventualmente, de outros requisitos adicionais a sistemas de IA que não sejam sistemas de IA de risco elevado.

5. Para efeitos do disposto nos n.os 1 a 4, o Comité, os Estados-Membros e as autoridades nacionais competentes devem facultar à Comissão as informações que esta solicitar.

6. Ao efetuar as avaliações e os reexames a que se referem os n.os 1 a 4, a Comissão tem em consideração as posições e as conclusões do Comité, do Parlamento Europeu, do Conselho e de outros organismos ou fontes pertinentes.

7. Se necessário, a Comissão apresenta propostas adequadas com vista a alterar o presente regulamento, atendendo, em especial, à evolução das tecnologias e aos progressos da sociedade da informação.

Artigo 85.º
Entrada em vigor e aplicação

1. O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

2. O presente regulamento é aplicável a partir de [*vinte e quatro meses após a sua entrada em vigor*].

3. Em derrogação do disposto no n.º 2:

   a) O título III, capítulo 4, e o título VI são aplicáveis a partir de [*três meses após a entrada em vigor do presente regulamento*];

   b) O artigo 71.º é aplicável a partir de [doze meses após a entrada em vigor do presente regulamento].

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

1.2. Domínio(s) de intervenção abrangido(s)

1.3. A proposta/iniciativa refere-se a:

1.4. Objetivo(s)

1.4.1. Objetivo(s) geral(ais)

1.4.2. Objetivo(s) específico(s)

1.4.3. Resultado(s) e impacto esperados

1.4.4. Indicadores de resultados

1.5. Justificação da proposta/iniciativa

1.5.1. Necessidade(s) a satisfazer a curto ou a longo prazo, incluindo um calendário pormenorizado de aplicação da iniciativa

1.5.2. Valor acrescentado da participação da União (que pode resultar de diferentes fatores, como, por exemplo, ganhos de coordenação, segurança jurídica, maior eficácia ou complementaridades). Para efeitos do presente ponto, entende-se por «valor acrescentado da intervenção da União» o valor resultante da intervenção da União que se acrescenta ao valor que teria sido criado pelos Estados-Membros de forma isolada

1.5.3. Ensinamentos retirados de experiências anteriores semelhantes

1.5.4. Compatibilidade com o quadro financeiro plurianual e eventuais sinergias com outros instrumentos adequados

1.5.5. Avaliação das diferentes opções de financiamento disponíveis, incluindo possibilidades de reafetação

1.6. Duração e impacto financeiro da proposta/iniciativa

1.7. Modalidade(s) de gestão prevista(s)

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

2.2. Sistema de gestão e de controlo

2.2.1. Justificação da(s) modalidade(s) de gestão, do(s) mecanismo(s) de execução do financiamento, das modalidades de pagamento e da estratégia de controlo propostos

2.2.2. Informações sobre os riscos identificados e o(s) sistema(s) de controlo interno criado(s) para os atenuar

2.2.3. Estimativa e justificação da relação custo-eficácia dos controlos (rácio «custos de controlo/valor dos respetivos fundos geridos») e avaliação dos níveis previstos de risco de erro (no pagamento e no encerramento)

2.3. Medidas de prevenção de fraudes e irregularidades

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(ais) de despesas envolvida(s)

3.2. Impacto financeiro estimado da proposta nas dotações

3.2.1. Síntese do impacto estimado nas dotações operacionais

3.2.2. Estimativa das realizações financiadas com dotações operacionais

3.2.3. Síntese do impacto estimado nas dotações de natureza administrativa

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

3.2.5. Participação de terceiros no financiamento

3.3. Impacto estimado nas receitas

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União

1.2. Domínio(s) de intervenção abrangido(s)

Redes de Comunicação, Conteúdos e Tecnologias;

Mercado interno, Indústria, Empreendedorismo e PME;

O impacto orçamental diz respeito às novas atribuições confiadas à Comissão, incluindo o apoio ao Comité Europeu para a Inteligência Artificial;

Atividade: construir o futuro digital da Europa.

1.3. A proposta/iniciativa refere-se a:

X **uma nova ação**

☐ **uma nova ação na sequência de um projeto-piloto/ação preparatória**[64]

☐ **uma prorrogação de uma ação existente**

☐ **uma ação redirecionada para uma nova ação**

1.4. Objetivo(s)

1.4.1. Objetivo(s) geral(ais)

O objetivo geral da intervenção consiste em assegurar o correto funcionamento do mercado único, criando condições para o desenvolvimento e a utilização de uma inteligência artificial de confiança na União.

1.4.2. Objetivo(s) específico(s)

Objetivo específico n.º 1

Definir requisitos específicos aplicáveis aos sistemas de IA e estabelecer obrigações para todos os participantes da cadeia de valor com vista a assegurar que os sistemas de IA colocados no mercado e utilizados sejam seguros e respeitem a legislação em vigor em matéria de direitos fundamentais e valores da União;

Objetivo específico n.º 2

Garantir a segurança jurídica para facilitar os investimentos e a inovação no domínio da IA, clarificando quais requisitos essenciais, obrigações e procedimentos relativos à conformidade e ao cumprimento devem ser seguidos para colocar ou utilizar um sistema de IA no mercado da União;

Objetivo específico n.º 3

Reforçar a governação e a aplicação efetiva da legislação em vigor em matéria de direitos fundamentais e dos requisitos de segurança aplicáveis aos sistemas de IA,

[64] A que se refere o artigo 54.º, n.º 2, alíneas a) ou b), do Regulamento Financeiro.

conferindo novos poderes às autoridades competentes, atribuindo-lhes recursos e definindo novas regras relativas aos procedimentos de avaliação da conformidade e de acompanhamento *ex post*, bem como à divisão das funções de governação e supervisão entre os níveis nacional e da UE;

Objetivo específico n.º 4

Facilitar o desenvolvimento de um mercado único para aplicações de IA legítimas, seguras e de confiança e evitar a fragmentação do mercado, atuando a nível da UE para definir requisitos mínimos aplicáveis aos sistemas de IA que serão colocados e utilizados no mercado da União em conformidade com a legislação em vigor em matéria de direitos fundamentais e segurança.

1.4.3. Resultado(s) e impacto esperados

Especificar os efeitos que a proposta/iniciativa poderá ter nos beneficiários/na população visada.

Os fornecedores de IA devem beneficiar de um conjunto de requisitos mínimos, mas claros, que criem segurança jurídica e garantam o acesso a todo o mercado único.

Os utilizadores de IA devem beneficiar da segurança jurídica de que os sistemas de IA de risco elevado que compram cumprem a legislação e os valores europeus.

Os consumidores devem beneficiar da redução do risco de violações da sua segurança e dos seus direitos fundamentais.

1.4.4. Indicadores de resultados

Especificar os indicadores que permitem acompanhar a execução da proposta/iniciativa.

Indicador 1

Número de incidentes graves ou desempenhos de inteligência artificial que constituem um incidente grave ou uma infração às obrigações em matéria de direitos fundamentais (semestral) por áreas de aplicações e calculado: a) em termos absolutos, b) como percentagem das aplicações implantadas; c) como percentagem dos cidadãos envolvidos.

Indicador 2

a) Investimento total em IA na UE (anual)

b) Investimento total em IA por Estado-Membro (anual)

c) Percentagem de empresas que utilizam IA (anual)

d) Percentagem de PME que utilizam IA (anual)

As alíneas a) e b) serão calculadas com base em fontes oficiais, usando como valores de referência estimativas privadas

c) Os dados referentes às alíneas c) e d) serão recolhidos por meio de inquéritos regulares junto das empresas

1.5. Justificação da proposta/iniciativa

1.5.1. Necessidade(s) a satisfazer a curto ou a longo prazo, incluindo um calendário pormenorizado de aplicação da iniciativa

O regulamento deve ser plenamente aplicável um ano e meio após a sua adoção. Contudo, antes dessa data devem já estar em funcionamento elementos da estrutura de governação. Em especial, os Estados-Membros devem ter previamente designado autoridades existentes e/ou criado novas autoridades para a execução das funções definidas na legislação, sendo que o Comité Europeu para a Inteligência Artificial deve estar criado e em funcionamento. A base de dados europeia de sistemas de IA deve estar a funcionar em pleno à data de aplicação do regulamento. Assim, paralelamente ao processo de adoção, torna-se necessário criar a base de dados, para que o seu desenvolvimento esteja concluído quando o regulamento entrar em vigor.

1.5.2. Valor acrescentado da participação da União (que pode resultar de diferentes fatores, como, por exemplo, ganhos de coordenação, segurança jurídica, maior eficácia ou complementaridades). Para efeitos do presente ponto, entende-se por «valor acrescentado da intervenção da União» o valor resultante da intervenção da União que se acrescenta ao valor que teria sido criado pelos Estados-Membros de forma isolada.

A emergência de um mosaico de regras nacionais potencialmente divergentes prejudicará o fornecimento homogéneo de sistemas de IA em toda a UE e será ineficaz para garantir a segurança e a proteção dos direitos fundamentais e dos valores da União nos diferentes Estados-Membros. Uma ação legislativa comum no domínio da IA a nível da UE pode estimular o mercado interno e revela grande potencial para proporcionar à indústria europeia uma vantagem competitiva a nível global e economias de escala que não podem ser conseguidas pelos Estados-Membros de forma isolada.

1.5.3. Ensinamentos retirados de experiências anteriores semelhantes

A Diretiva Comércio Eletrónico (Diretiva 2000/31/CE) estabelece o quadro central para o funcionamento do mercado único e a supervisão dos serviços digitais e define uma estrutura de base para um mecanismo de cooperação geral entre os Estados-Membros, abrangendo, em princípio, todos os requisitos aplicáveis aos serviços digitais. A avaliação da diretiva evidenciou insuficiências em vários aspetos deste mecanismo de cooperação, incluindo aspetos processuais importantes, como a ausência de prazos claros para as respostas dos Estados-Membros, juntamente com uma ausência geral de respostas aos pedidos dirigidos pelas suas contrapartes. Tal conduziu, ao longo dos anos, a uma falta de confiança entre os Estados-Membros na resposta a preocupações sobre os fornecedores que oferecem serviços digitais transfronteiras. A avaliação da diretiva mostrou a necessidade de definir um conjunto de regras e requisitos diferenciados a nível europeu. Por este motivo, a aplicação das obrigações específicas estabelecidas no presente regulamento exigirá um mecanismo de cooperação específico a nível da UE, com uma estrutura de governação que assegure a coordenação de organismos responsáveis específicos a nível da UE.

1.5.4. Compatibilidade com o quadro financeiro plurianual e eventuais sinergias com outros instrumentos adequados

O regulamento que estabelece regras harmonizadas em matéria de inteligência artificial e altera determinados atos legislativos da União define um novo quadro

comum de requisitos aplicáveis aos sistemas de IA, que vai além do enquadramento previsto na legislação existente. Por este motivo, esta proposta obriga ao estabelecimento de uma nova função reguladora e coordenadora a nível nacional e europeu.

No que diz respeito a possíveis sinergias com outros instrumentos adequados, o papel das autoridades notificadoras a nível nacional pode ser desempenhado pelas autoridades nacionais responsáveis pelo exercício de funções semelhantes nos termos de outros regulamentos da UE.

Além disso, o aumento da confiança na IA e o subsequente incentivo ao investimento no desenvolvimento e na adoção de soluções de IA contribuirão para os objetivos do Programa Europa Digital (PED), que define a difusão da IA como uma das suas cinco prioridades.

1.5.5. Avaliação das diferentes opções de financiamento disponíveis, incluindo possibilidades de reafetação

Haverá lugar à reafetação de pessoal. Os restantes custos serão suportados pela dotação do PED, atendendo a que o objetivo do presente regulamento — garantir uma IA de confiança — contribui diretamente para um dos principais objetivos do programa — acelerar o desenvolvimento e a implantação da IA na Europa.

1.6. Duração e impacto financeiro da proposta/iniciativa

☐ **duração limitada**

– ☐ em vigor entre [DD/MM]AAAA e [DD/MM]AAAA

– ☐ Impacto financeiro no período compreendido entre AAAA e AAAA para as dotações de autorização e entre AAAA a AAAA para as dotações de pagamento.

X **duração ilimitada**

– Aplicação com um período de arranque progressivo entre um/dois anos (a determinar),

– seguido de um período de aplicação a um ritmo de cruzeiro.

1.7. Modalidade(s) de gestão prevista(s)[65]

X **Gestão direta** por parte da Comissão

– ☐ pelos seus serviços, incluindo o pessoal nas delegações da União;

– ☐ pelas agências de execução

☐ **Gestão partilhada** com os Estados-Membros

☐ **Gestão indireta** confiando tarefas de execução orçamental:

– ☐ a países terceiros ou organismos por estes designados;

– ☐ a organizações internacionais e respetivas agências (a especificar);

– ☐ ao BEI e ao Fundo Europeu de Investimento;

– ☐ aos organismos referidos nos artigos 70.º e 71.º do Regulamento Financeiro;

– ☐ a organismos de direito público;

– ☐ aos organismos regidos pelo direito privado com uma missão de serviço público na medida em que prestem garantias financeiras adequadas;

– ☐ a organismos regidos pelo direito privado de um Estado-Membro com a responsabilidade pela execução de uma parceria público-privada e que prestem garantias financeiras adequadas;

– ☐ a pessoas encarregadas da execução de ações específicas no quadro da PESC por força do título V do Tratado da União Europeia, identificadas no ato de base pertinente.

– *Se for indicada mais de uma modalidade de gestão, queira especificar na secção «Observações».*

Observações

[65] As explicações sobre as modalidades de gestão e as referências ao Regulamento Financeiro estão disponíveis no sítio BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html.

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e prestação de informações

Especificar a periodicidade e as condições.

O regulamento será reexaminado e avaliado no prazo de cinco anos a contar da data de entrada em vigor. A Comissão apresentará um relatório sobre as conclusões da avaliação ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu.

2.2. Sistema(s) de gestão e de controlo

2.2.1. Justificação da(s) modalidade(s) de gestão, do(s) mecanismo(s) de execução do financiamento, das modalidades de pagamento e da estratégia de controlo propostos

O regulamento estabelece uma nova política no que respeita a regras harmonizadas para o fornecimento de sistemas de inteligência artificial no mercado interno, assegurando simultaneamente o respeito da segurança e dos direitos fundamentais. Estas novas regras exigem um mecanismo de controlo da coerência na aplicação transfronteiras das obrigações do presente regulamento, sob a forma de um novo grupo consultivo que coordene as atividades das autoridades nacionais.

Para desempenhar estas novas funções, é necessário dotar os serviços da Comissão dos recursos adequados. Estima-se que a aplicação do novo regulamento exija 10 ETC (5 ETC para apoiar as atividades do Comité e 5 ETC para a Autoridade Europeia para a Proteção de Dados na qualidade de organismo notificador para os sistemas de IA implantados por um organismo da União Europeia).

2.2.2. Informações sobre os riscos identificados e o(s) sistema(s) de controlo interno criado(s) para os atenuar

Para garantir que os membros do Comité tenham a possibilidade de fazer uma análise informada com base em provas factuais, prevê-se que o Comité seja apoiado pela estrutura administrativa da Comissão e que seja criado um grupo de peritos para prestar informações especializadas adicionais, se for caso disso.

2.2.3. Estimativa e justificação da relação custo-eficácia dos controlos (rácio «custos de controlo/valor dos respetivos fundos geridos») e avaliação dos níveis previstos de risco de erro (no pagamento e no encerramento)

Em relação às despesas de reunião, atendendo ao baixo valor por transação (por exemplo, reembolso das despesas de viagem por reunião), os procedimentos de controlo habituais afiguram-se suficientes. Relativamente ao desenvolvimento da base de dados, a atribuição de contratos é abrangida pelo forte sistema de controlo interno existente na DG CNECT, baseado em atividades de contratação centralizadas.

2.3. Medidas de prevenção de fraudes e irregularidades

Especificar as medidas de prevenção e de proteção existentes ou previstas, como, por exemplo, da estratégia antifraude.

As atuais medidas de prevenção da fraude aplicáveis à Comissão cobrirão as dotações adicionais necessárias para efeitos do presente regulamento.

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(ais) de despesas envolvida(s)

- Atuais rubricas orçamentais

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

Rubrica do quadro financeiro plurianual	Rubrica orçamental	Tipo de despesa	Participação			
	Número	DD/DND[66]	dos países EFTA[67]	dos países candidatos[68]	de países terceiros	na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro
7	20 02 06 Despesas administrativas	DND	NÃO	NÃO	NÃO	NÃO
1	02 04 03 PED — Inteligência Artificial	DD	SIM	NÃO	NÃO	NÃO
1	02 01 30 01 Despesas de apoio ao Programa Europa Digital	DND	SIM	NÃO	NÃO	NÃO

3.2. Impacto financeiro estimado da proposta nas dotações

3.2.1. Síntese do impacto estimado na despesa nas dotações operacionais

– ☐ A proposta/iniciativa não acarreta a utilização de dotações operacionais

– X A proposta/iniciativa acarreta a utilização de dotações operacionais, tal como explicitado seguidamente:

Em milhões de EUR (três casas decimais)

[66] DD = dotações diferenciadas/DND = dotações não diferenciadas.

[67] EFTA: Associação Europeia de Comércio Livre.

[68] Países candidatos e, se for caso disso, países candidatos potenciais dos Balcãs Ocidentais.

Rubrica do quadro financeiro plurianual	1	

DG: CNECT				Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**[69]	**TOTAL**	
• Dotações operacionais											
Rubrica orçamental[70] 02 04 03		Autorizações	(1a)		1,000						**1,000**
		Pagamentos	(2 a)		0,600	0,100	0,100	0,100	0,100		**1,000**
Rubrica orçamental		Autorizações	(1b)								
		Pagamentos	(2b)								
Dotações de natureza administrativa financiadas a partir da dotação de programas específicos[71]											
Rubrica orçamental 02 01 30 01			(3)		0,240	0,240	0,240	0,240	0,240		**1,200**
TOTAL das dotações para a DG CNECT		Autorizações	=1a+1b +3		**1,240**		**0,240**	**0,240**	**0,240**		**2,200**
		Pagamentos	=2a+2b +3		**0,840**	**0,340**	**0,340**	**0,340**	**0,340**		**2,200**

69 Indicativo e dependente da disponibilidade orçamental.

70 De acordo com a nomenclatura orçamental oficial.

71 Assistência técnica e/ou administrativa e despesas de apoio à execução de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.

• TOTAL das dotações operacionais	Autorizações	(4)		1,000						**1,000**
	Pagamentos	(5)		0,600	0,100	0,100	0,100	0,100		**1,000**
• TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos		(6)		**0,240**	**0,240**	**0,240**	**0,240**	**0,240**		**1,200**
TOTAL das dotações para a RUBRICA 1 do quadro financeiro plurianual	Autorizações	=4+ 6		1,240	0,240	0,240	0,240	0,240		**2,200**
	Pagamentos	=5+ 6		0,840	0,340	0,340	0,340	0,340		**2,200**

Se o impacto da proposta/iniciativa incidir sobre mais de uma rubrica, repetir a secção acima:

• TOTAL das dotações operacionais (todas as rubricas operacionais)	Autorizações	(4)								
	Pagamentos	(5)								
• TOTAL das dotações de natureza administrativa financiadas a partir da dotação de programas específicos (todas as rubricas operacionais)		(6)								
TOTAL das dotações para as RUBRICAS 1 a 6 do quadro financeiro plurianual (Montante de referência)	Autorizações	=4+ 6								
	Pagamentos	=5+ 6								

Rubrica do quadro financeiro plurianual	**7**	«Despesas administrativas»

Esta secção deve ser preenchida com «dados orçamentais de natureza administrativa» a inserir em primeiro lugar no anexo da ficha financeira legislativa (anexo V das regras internas), que é carregada no DECIDE para efeitos das consultas interserviços.

Em milhões de EUR (três casas decimais)

		Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**Após 2027**[72]	**TOTAL**
DG: CNECT								
• Recursos humanos		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Outras despesas administrativas		**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,010**	**0,050**
TOTAL DG CNECT	**Dotações**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,850**
Autoridade Europeia para a Proteção de Dados								
• Recursos humanos		0,760	0,760	0,760	0,760	0,760	0,760	**3,800**
• Outras despesas administrativas								
TOTAL AEPD	**Dotações**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**0,760**	**3,800**
TOTAL das dotações para a RUBRICA 7 do quadro financeiro plurianual	(Total das autorizações = total dos pagamentos)	1,530	1,530	1,530	1,530	1,530	1,530	**7,650**

Em milhões de EUR (três casas decimais)

		Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**		**TOTAL**
TOTAL das dotações	Autorizações		2,770	1,770	1,770	1,770	1,770		**9,850**

[72] Todos os montantes inscritos nesta coluna são indicativos e estão sujeitos ao prosseguimento dos programas e à disponibilidade das dotações.

para as RUBRICAS 1 a 7 do quadro financeiro plurianual	Pagamentos		2,370	1,870	1,870	1,870	1,870	**9,850**

3.2.2. Estimativa das realizações financiadas com dotações operacionais

Dotações de autorização em milhões de EUR (três casas decimais)

Indicar os objetivos e as realizações ⇩			Ano **2022**		Ano **2023**		Ano **2024**		Ano **2025**		Ano **2026**		Ano **2027**		Após **2027**[73]		**TOTAL**	
	REALIZAÇÕES																	
	Tipo	Custo médio	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º Total	Custo total
OBJETIVO ESPECÍFICO n.º 1[74]…																		
Base de dados					1	1,000	1		1		1		1		1	0,100	1	1,000
Reuniões -					10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	10	0,200	50	1,000
Atividades de comunicação					2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	2	0,040	10	0,040
Subtotal objetivo específico n.º 1																		
OBJETIVO ESPECÍFICO N.º 2…																		
- Realização																		
Subtotal objetivo específico n.º 2																		
TOTAIS					13	0,240	13	0,240	13	0,240	13	0,240	13	0,240	13	0,100	65	2,200

[73] Todos os montantes inscritos nesta coluna são indicativos e estão sujeitos ao prosseguimento dos programas e à disponibilidade das dotações.

[74] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)…».

3.2.3. Síntese do impacto estimado nas dotações de natureza administrativa

– ☐ A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa

– X A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (três casas decimais)

	Ano **2022**	Ano **2023**	Ano **2024**	Ano **2025**	Ano **2026**	Ano **2027**	**Anualmente após 2027**[75]	**TOTAL**
RUBRICA 7 do quadro financeiro plurianual								
Recursos humanos		1,520	1,520	1,520	1,520	1,520	**1,520**	**7,600**
Outras despesas administrativas		0,010	0,010	0,010	0,010	0,010	**0,010**	**0,050**
Subtotal RUBRICA 7 do quadro financeiro plurianual		1,530	1,530	1,530	1,530	1,530	**1,530**	**7,650**
Com exclusão da RUBRICA 7[76] **do quadro financeiro plurianual**								
Recursos humanos								
Outras despesas de natureza administrativa		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
Subtotal Com exclusão da RUBRICA 7 do quadro financeiro plurianual		0,240	0,240	0,240	0,240	0,240	**0,240**	**1,20**
TOTAL		**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**1,770**	**8,850**

As dotações relativas aos recursos humanos e outras despesas administrativas necessárias serão cobertas pelas dotações da DG já afetadas à gestão da ação e/ou reafetadas na DG e, se necessário, pelas eventuais dotações adicionais que sejam concedidas à DG gestora no âmbito do processo de afetação anual e atendendo às restrições orçamentais.

75 Todos os montantes inscritos nesta coluna são indicativos e estão sujeitos ao prosseguimento dos programas e à disponibilidade das dotações.

76 Assistência técnica e/ou administrativa e despesas de apoio à execução de programas e/ou ações da UE (antigas rubricas «BA»), bem como investigação direta e indireta.

3.2.3.1. Necessidades estimadas de recursos humanos

– ☐ A proposta/iniciativa não acarreta a utilização de recursos humanos.

– X A proposta/iniciativa acarreta a utilização de recursos humanos, tal como explicitado seguidamente:

As estimativas devem ser expressas em termos de equivalente a tempo completo

.		Ano **2023**	Ano **2024**	Ano **2025**	**2026**	**2027**	**Após 2027**[77]	
• Lugares do quadro do pessoal (funcionários e agentes temporários)								
20 01 02 01 (na sede e nas representações da Comissão)		10	10	10	10	10	10	
20 01 02 03 (nas delegações)								
01 01 01 01 (investigação indireta)								
01 01 01 11 (investigação direta)								
Outras rubricas orçamentais (especificar)								
• Pessoal externo (em equivalente a tempo completo: ETC)[78]								
20 02 01 (AC, PND e TT da dotação global)								
20 02 03 (AC, AL, PND, TT e JPD nas delegações)								
XX 01 xx **yy zz**[79]	- na sede							
	- nas delegações							
01 01 01 02 (AC, PND e TT - Investigação indireta)								
01 01 01 12 (AC, PND e TT - Investigação direta)								
Outras rubricas orçamentais (especificar)								
TOTAL		**10**	**10**	**10**	**10**	**10**	**10**	

XX constitui o domínio de intervenção ou o título orçamental em causa.

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente a nível da DG, complementados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

Espera-se que a AEPD forneça metade dos recursos necessários.

Descrição das tarefas a executar:

Funcionários e agentes temporários	Serão necessários 4 AD ETC e 1 AST ETC incumbidos de preparar um total de 13-16 reuniões, elaborar relatórios, dar seguimento ao trabalho político (por exemplo, relativamente a futuras alterações da lista de aplicações de IA de risco elevado) e manter relações com as autoridades dos Estados-Membros. No caso dos sistemas de IA desenvolvidos pelas instituições da UE, a Autoridade Europeia para a Proteção de Dados é responsável. Com base na experiência acumulada, estima-se que sejam necessários 5 AD ETC para cumprir as responsabilidades da AEPD previstas na proposta legislativa.
Pessoal externo	

[77] Todos os montantes inscritos nesta coluna são indicativos e estão sujeitos ao prosseguimento dos programas e à disponibilidade das dotações.

[78] AC = agente contratual; AL = agente local; PND = perito nacional destacado; TT = trabalhador temporário; JPD = jovem perito nas delegações.

[79] Sublimite para o pessoal externo coberto pelas dotações operacionais (antigas rubricas «BA»).

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

A proposta/iniciativa:

– X pode ser integralmente financiada por meio da reafetação de fundos no quadro da rubrica pertinente do quadro financeiro plurianual (QFP).

Não é necessário qualquer tipo de reprogramação.

– ☐ requer o recurso à margem não afetada na rubrica em causa do QFP e/ou o recurso aos instrumentos especiais definidos no Regulamento QFP.

Explicitar as necessidades, especificando as rubricas orçamentais em causa e as quantias correspondentes, bem como os instrumentos cuja utilização é proposta.

– ☐ implica uma revisão do QFP.

Explicitar as necessidades, especificando as rubricas orçamentais em causa e as quantias correspondentes.

3.2.5. Participação de terceiros no financiamento

A proposta/iniciativa:

– X não prevê o cofinanciamento por terceiros

– ☐ prevê o seguinte cofinanciamento por terceiros, a seguir estimado:

Dotações em milhões de EUR (três casas decimais)

	Ano **N**[80]	Ano **N+1**	Ano **N+2**	Ano **N+3**	Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)			Total
Especificar o organismo de cofinanciamento								
TOTAL das dotações cofinanciadas								

[80] O ano N é o do início da aplicação da proposta/iniciativa. Substituir «N» pelo primeiro ano de execução previsto (por exemplo: 2021). Proceder do mesmo modo relativamente aos anos seguintes.

3.3. Impacto estimado nas receitas

– ☐ A proposta/iniciativa tem o impacto financeiro a seguir descrito:

– ☐ A proposta/iniciativa tem o impacto financeiro a seguir descrito:

– ☐ noutras receitas

– ☐ noutras receitas

– indicar se as receitas são afetadas a rubricas de despesas ☐

Em milhões de EUR (três casas decimais)

Rubrica orçamental das receitas:	Dotações disponíveis para o atual exercício	Impacto da proposta/iniciativa[81]						
		Ano **N**	Ano **N+1**	Ano **N+2**	Ano **N+3**	Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)		
Artigo …….								

Relativamente às receitas afetadas, especificar a(s) rubrica(s) orçamental(ais) de despesas envolvida(s).

Outras observações (p. ex., método/fórmula utilizado/a para o cálculo do impacto sobre as receitas ou qualquer outra informação).

[81] No que diz respeito aos recursos próprios tradicionais (direitos aduaneiros e quotizações sobre o açúcar), as quantias indicadas devem ser apresentadas em termos líquidos, isto é, quantias brutas após dedução de 20 % a título de despesas de cobrança.