UNIÃO EUROPEIA

PARLAMENTO EUROPEU **CONSELHO**

Bruxelas, 14 de maio de 2024
(OR. en)

2021/0106(COD) **PE-CONS 24/24**

TELECOM 54
JAI 238
COPEN 69
CYBER 37
DATAPROTECT 76
EJUSTICE 11
COSI 16
IXIM 49
ENFOPOL 63
RELEX 180
MI 151
COMPET 154
CODEC 412

ATOS LEGISLATIVOS E OUTROS INSTRUMENTOS

Assunto:	REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial)

REGULAMENTO (UE) 2024/...
DO PARLAMENTO EUROPEU E DO CONSELHO

de ...

que cria regras harmonizadas em matéria de inteligência artificial
e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013,
(UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144
e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828
(Regulamento da Inteligência Artificial)

(Texto relevante para efeitos do EEE)

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[1],

Tendo em conta o parecer do Banco Central Europeu[2],

Tendo em conta o parecer do Comité das Regiões[3],

Deliberando de acordo com o processo legislativo ordinário[4],

---

1 JO C 517 de 22.12.2021, p. 56.
2 JO C 115 de 11.3.2022, p. 5.
3 JO C 97 de 28.2.2022, p. 60.
4 Posição do Parlamento Europeu de 13 de março de 2024 (ainda não publicada no Jornal Oficial) e decisão do Conselho de ....

Considerando o seguinte:

(1) O presente regulamento tem por objetivo a melhoria do funcionamento do mercado interno mediante a previsão de um regime jurídico uniforme, em particular para o desenvolvimento, a colocação no mercado, a colocação em serviço e a utilização de sistemas de inteligência artificial (sistemas de IA) na União, em conformidade com os valores da União, a fim de promover a adoção de uma inteligência artificial (IA) centrada no ser humano e de confiança, assegurando simultaneamente um elevado nível de proteção da saúde, da segurança, dos direitos fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia («Carta»), nomeadamente a democracia, o Estado de direito e a proteção do ambiente, a proteção contra os efeitos nocivos dos sistemas de IA na União, e de apoiar a inovação. O presente regulamento assegura a livre circulação transfronteiriça de produtos e serviços baseados em IA, evitando assim que os Estados-Membros imponham restrições ao desenvolvimento, à comercialização e à utilização dos sistemas de IA, salvo se explicitamente autorizado pelo presente regulamento.

(2) O presente regulamento deverá ser aplicado em conformidade com os valores da União consagrados na Carta, facilitando a proteção das pessoas singulares, das empresas, da democracia, do Estado de direito e proteção ambiental, promovendo simultaneamente a inovação e o emprego e colocando a União na liderança em matéria de adoção de uma IA de confiança.

(3) Os sistemas de IA podem ser facilmente implantados numa grande variedade de setores da economia e em muitos quadrantes da sociedade, inclusive além fronteiras, e podem circular facilmente por toda a União. Certos Estados-Membros já ponderaram a adoção de regras nacionais para assegurar que a IA seja de confiança e segura e seja desenvolvida e utilizada em conformidade com as obrigações em matéria de direitos fundamentais. As diferenças entre regras nacionais podem conduzir à fragmentação do mercado interno e reduzir a segurança jurídica para os operadores que desenvolvem, importam ou utilizam sistemas de IA. Como tal, é necessário assegurar um nível de proteção elevado e coerente em toda a União, com vista a alcançar uma IA de confiança, e evitar divergências que prejudiquem a livre circulação, a inovação, a implantação e a adoção 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 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 para efeitos de aplicação da lei, à utilização de sistemas de IA para a avaliação de risco em relação a pessoas singulares para efeitos de aplicação da lei e à utilização de sistemas de IA para categorização biométrica para efeitos de aplicação da lei, 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.

(4) A IA é uma família de tecnologias em rápida evolução que contribui para um vasto conjunto de benefícios económicos, ambientais e sociais em 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 IA pode conferir importantes vantagens competitivas às empresas e contribuir para progressos sociais e ambientais, por exemplo, nos cuidados de saúde, na agricultura, na segurança alimentar, na educação e na formação, nos meios de comunicação social, no desporto, na cultura, na gestão das infraestruturas, na energia, nos transportes e na logística, nos serviços públicos, na segurança, na justiça, na eficiência energética e dos recursos, na monitorização ambiental, na preservação e recuperação da biodiversidade e dos ecossistemas e na atenuação das alterações climáticas e adaptação às mesmas.

(5) Ao mesmo tempo, em função das circunstâncias relativas à sua aplicação, utilização e nível de evolução tecnológica específicos, a IA pode criar riscos e prejudicar interesses públicos e direitos fundamentais protegidos pela legislação da União. Esses prejuízos podem ser materiais ou imateriais, incluindo danos físicos, psicológicos, sociais ou económicos.

(6) Tendo em conta o grande impacto que a IA pode ter na sociedade e a necessidade de criar confiança, é fundamental que a IA e o respetivo regime regulamentar sejam desenvolvidos em conformidade com os valores da União consagrados no artigo 2.º do Tratado da União Europeia (TUE), com os direitos e liberdades fundamentais consagrados nos Tratados e, nos termos do artigo 6.º do TUE, com a Carta. Como condição prévia, a IA deverá ser uma tecnologia centrada no ser humano. Deverá servir de instrumento para as pessoas, com o objetivo último de aumentar o bem-estar humano.

(7) A fim de assegurar um nível elevado e coerente de proteção dos interesses públicos nos domínios da saúde, da segurança e dos direitos fundamentais, deverão ser estabelecidas regras comuns aplicáveis a todos os sistemas de IA de risco elevado. Essas normas deverão ser coerentes com a Carta, não discriminatórias e estar em consonância com os compromissos comerciais internacionais da União. Deverão também ter em conta a Declaração Europeia sobre os Direitos e Princípios Digitais para a Década Digital e as Orientações Éticas para uma IA de Confiança do Grupo de Peritos de Alto Nível em IA (AI HLEG, do inglês High-Level Expert Group on Artificial Intelligence).

(8) Como tal, é necessário adotar um regime jurídico da União que estabeleça regras harmonizadas em matéria de IA para promover o desenvolvimento, a utilização e a adoção da IA 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 defesa dos direitos fundamentais, incluindo a democracia, o Estado de direito e a proteção do ambiente, conforme reconhecido e protegido pelo direito da União. Para alcançar esse objetivo, torna-se necessário estabelecer regras que regulem a colocação no mercado, a colocação em serviço e a utilização 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. Tais regras deverão ser claras e sólidas na defesa dos direitos fundamentais, apoiando novas soluções inovadoras e permitindo um ecossistema europeu de intervenientes públicos e privados que criem sistemas de IA em consonância com os valores da União e que explorem o potencial da transformação digital em todas as regiões da União. Ao estabelecer essas regras, bem como as medidas de apoio à inovação, com especial destaque para as pequenas e médias empresas (PME), incluindo as empresas em fase de arranque, o presente regulamento apoia o objetivo de promover a abordagem europeia da IA centrada no ser humano, assim como o de estar na vanguarda mundial do desenvolvimento de uma IA segura, ética e de confiança, conforme declarado pelo Conselho Europeu[5], e garante a proteção de princípios éticos, conforme solicitado especificamente pelo Parlamento Europeu[6].

---

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

6 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)].

(9) Deverão ser previstas regras harmonizadas 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[7], a Decisão n.º 768/2008/CE do Parlamento Europeu e do Conselho[8] e o Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho[9] (novo regime jurídico). As regras harmonizadas estabelecidas no presente regulamento deverão aplicar-se em todos os setores e, em consonância com a abordagem do novo regime jurídico, não deverão prejudicar a legislação da União em vigor, nomeadamente em matéria de proteção de dados, defesa dos consumidores, direitos fundamentais, emprego, proteção dos trabalhadores e segurança dos produtos, que o presente regulamento vem complementar. Consequentemente, permanecem inalterados e plenamente aplicáveis todos os direitos e vias de recurso concedidos nessa legislação da União aos consumidores e a outras pessoas em relação às quais os sistemas de IA possam ter um impacto negativo, nomeadamente no que diz respeito à indemnização por eventuais danos nos termos da Diretiva 85/374/CEE do Conselho[10].

---

7 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 que revoga o Regulamento (CEE) n.º 339/93 (JO L 218 de 13.8.2008, p. 30).

8 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).

9 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 (JO L 169 de 25.6.2019, p. 1).

10 Diretiva 85/374/CEE do Conselho, de 25 de julho de 1985, relativa à aproximação das disposições legislativas, regulamentares e administrativas dos Estados-Membros em matéria de responsabilidade decorrente dos produtos defeituosos (JO L 210 de 7.8.1985, p. 29).

Além disso, no contexto do emprego e da proteção dos trabalhadores, o presente regulamento não deverá, por conseguinte, afetar o direito da União em matéria de política social nem a legislação laboral nacional, que seja conforme com o direito da União, no que diz respeito ao emprego e às condições de trabalho, incluindo a saúde e a segurança no trabalho e a relação entre empregadores e trabalhadores. O presente regulamento também não deverá prejudicar o exercício dos direitos fundamentais reconhecidos pelos Estados-Membros e a nível da União, incluindo o direito ou a liberdade de fazer greve ou a liberdade de realizar outras ações abrangidas pelos sistemas específicos de relações laborais dos Estados-Membros, os direitos de negociação, de celebração e execução de convenções coletivas, ou de realização de ações coletivas de acordo com o direito nacional. O presente regulamento não deverá afetar as disposições destinadas a melhorar as condições de trabalho nas plataformas digitais estabelecidas numa Diretiva do Parlamento Europeu e do Conselho relativa à melhoria das condições de trabalho nas plataformas digitais. Além disso, presente regulamento visa ainda reforçar a eficácia desses direitos e vias de recurso existentes, estabelecendo requisitos e obrigações específicos, nomeadamente no que diz respeito à transparência, à documentação técnica e à manutenção de registos dos sistemas de IA. Além disso, as obrigações impostas aos vários operadores envolvidos na cadeia de valor da IA nos termos do presente regulamento deverão aplicar-se sem prejuízo da legislação nacional, que seja conforme com o direito da União, com o efeito de limitar a utilização de determinados sistemas de IA sempre que essa legislação não seja abrangida pelo âmbito de aplicação do presente regulamento ou prossiga objetivos legítimos de interesse público que não os prosseguidos pelo presente regulamento. Por exemplo, a legislação laboral nacional e a legislação em matéria de proteção de menores, nomeadamente pessoas com menos de 18 anos, tendo em conta o Comentário Geral n.º 25 (2021) das Nações Unidas sobre os direitos das crianças em ambiente digital, na medida em que não sejam específicos dos sistemas de IA e prossigam outros objetivos legítimos de interesse público, não deverão ser afetados pelo presente regulamento.

(10) O direito fundamental à proteção de dados pessoais está salvaguardado em especial pelos Regulamentos (UE) 2016/679[11] e (UE) 2018/1725[12] do Parlamento Europeu e do Conselho e pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho[13]. Além disso, a Diretiva 2002/58/CE do Parlamento Europeu e do Conselho[14] protege a vida privada e a confidencialidade das comunicações, nomeadamente através de condições colocadas ao armazenamento de dados pessoais e não pessoais em equipamentos terminais e a qualquer acesso a partir dos mesmos. Esses atos jurídicos da União constituem a base para um tratamento de dados sustentável e responsável, nomeadamente quando os conjuntos de dados incluem uma combinação de dados pessoais e não pessoais. O presente regulamento não visa afetar a aplicação do direito da União já em vigor que rege o tratamento de dados pessoais, incluindo as funções e as competências das autoridades de supervisão independentes responsáveis pelo controlo do cumprimento desses instrumentos.

---

11 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).

12 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).

13 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).

14 Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

Da mesma forma, não afeta as obrigações dos prestadores nem dos responsáveis pela implantação de sistemas de IA, enquanto responsáveis pelo tratamento de dados ou subcontratantes, decorrentes do direito da União ou do direito nacional em matéria de proteção de dados pessoais, na medida em que a conceção, o desenvolvimento ou a utilização de sistemas de IA envolva o tratamento de dados pessoais. É igualmente conveniente clarificar que os titulares de dados continuam a usufruir de todos os direitos e garantias que lhes são conferidos por esse direito da União, incluindo os direitos relacionados com as decisões individuais exclusivamente automatizadas, nomeadamente a definição de perfis. As regras harmonizadas para a colocação no mercado, a colocação em serviço e a utilização de sistemas de IA estabelecidas no presente regulamento deverão facilitar a aplicação efetiva e permitir o exercício dos direitos dos titulares de dados e de outras vias de recurso garantidas pelo direito da União em matéria de proteção de dados pessoais e de outros direitos fundamentais.

(11) O presente regulamento não prejudica as disposições em matéria de responsabilidade dos prestadores de serviços intermediários conforme prevista no Regulamento (UE) 2022/0265 do Parlamento Europeu e do Conselho[15].

[15] Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho, de 19 de outubro de 2022, relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais) (JO L 277 de 27.10.2022, p. 1).

(12) O conceito de «sistema de IA» constante do presente regulamento deverá ser definido de forma inequívoca e estar estreitamente alinhado com o trabalho das organizações internacionais ativas no domínio da IA, a fim de assegurar a segurança jurídica, facilitar a convergência internacional e a ampla aceitação, concedendo em simultâneo a flexibilidade suficiente para se adaptar a rápidas evoluções tecnológicas neste domínio. Além disso, a definição deverá basear-se nas principais características dos sistemas de IA que o distinguem de sistemas de software ou abordagens de programação tradicionais mais simples e não deverá abranger sistemas baseados nas regras definidas exclusivamente por pessoas singulares para executarem operações automaticamente. Uma característica principal dos sistemas de IA é a sua capacidade de fazer inferências. Esta capacidade de fazer inferências refere-se ao processo de obtenção dos resultados, tais como previsões, conteúdos, recomendações ou decisões, que possam influenciar ambientes físicos e virtuais, e à capacidade dos sistemas de IA para obter modelos ou algoritmos, ou ambos, a partir de entradas ou dados. As técnicas que permitem fazer inferências durante a construção de um sistema de IA incluem abordagens de aprendizagem automática que aprendem com os dados a forma de alcançarem determinados objetivos, e abordagens baseadas na lógica e no conhecimento que fazem inferências a partir do conhecimento codificado ou da representação simbólica da tarefa a resolver. A capacidade de um sistema de IA fazer inferências vai além do tratamento básico de dados, permitindo a aprendizagem, o raciocínio ou a modelização. O termo «baseado em máquinas» refere-se ao facto de os sistemas de IA funcionarem em máquinas.

A referência a objetivos explícitos ou implícitos visa sublinhar que os sistemas de IA podem funcionar de acordo com objetivos explícitos definidos ou com objetivos implícitos. Os objetivos do sistema de IA podem ser diferentes da finalidade prevista para o sistema de IA num contexto específico. Para efeitos do presente regulamento, deverá entender-se por «ambientes» os contextos em que os sistemas de IA operam, ao passo que os resultados gerados pelo sistema de IA refletem diferentes funções desempenhadas pelos sistemas de IA e incluem previsões, conteúdos, recomendações ou decisões. Os sistemas de IA são concebidos para operar com diferentes níveis de autonomia, o que significa que têm um certo grau de independência das ações efetuadas por intervenção humana e de capacidade para funcionarem sem intervenção humana. A capacidade de adaptação que um sistema de IA poderá apresentar após a implantação refere-se a capacidades de autoaprendizagem, permitindo que o sistema mude enquanto estiver a ser utilizado. Os sistemas de IA podem ser utilizados autonomamente ou como componentes 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).

(13) O conceito de «responsável pela implantação» a que se refere o presente regulamento deverá ser interpretado como qualquer pessoa singular ou coletiva, incluindo uma autoridade pública, agência ou outro organismo, que utilize um sistema de IA sob a sua autoridade, salvo se o sistema de IA for utilizado no âmbito da sua atividade pessoal não profissional. Dependendo do tipo de sistema de IA, a utilização do sistema pode afetar outras pessoas além do responsável pela implantação.

(14) O conceito de «dados biométricos» utilizado no presente regulamento deverá ser interpretado à luz do conceito de dados biométricos na aceção do artigo 4.º, ponto 14, do Regulamento (UE) 2016/679, do artigo 3.º, ponto 18, do Regulamento (UE) 2018/1725 e do artigo 3.º, ponto 13, da Diretiva (UE) 2016/680. Os dados biométricos podem permitir a autenticação, identificação ou categorização de pessoas singulares e o reconhecimento de emoções de pessoas singulares.

(15) O conceito de «identificação biométrica» a que se refere o presente regulamento deverá ser definido como o reconhecimento automatizado de características humanas físicas, fisiológicas e comportamentais, tais como o rosto, o movimento dos olhos, a forma do corpo, a voz, a pronúncia, a marcha, a postura, a frequência cardíaca, a pressão arterial, o odor, as características da digitação, com o objetivo de verificar a identidade de uma pessoa comparando os dados biométricos dessa pessoa com dados biométricos de pessoas armazenados numa base de dados de referência, independentemente de a pessoa ter ou não dado consentimento prévio. Estão excluídos os sistemas de IA concebidos para serem utilizados na verificação biométrica, que inclui a autenticação, cujo único objetivo seja confirmar que uma pessoa singular específica é quem afirma ser, e confirmar a identidade de uma pessoa singular com o único objetivo de ter acesso a um serviço, desbloquear um dispositivo ou ter acesso de segurança a um local.

(16) O conceito de «sistema de categorização biométrica» a que se refere o presente regulamento deverá ser definido como a atribuição de pessoas singulares a categorias específicas com base nos seus dados biométricos. Essas categorias específicas podem dizer respeito a aspetos como sexo, idade, cor do cabelo, cor dos olhos, tatuagens, traços comportamentais ou de personalidade, língua, religião, pertença a uma minoria nacional, orientação sexual ou política. Tal não inclui os sistemas de categorização biométrica que sejam um elemento meramente acessório intrinsecamente ligado a outro serviço comercial, o que significa que o elemento não pode, por razões técnicas objetivas, ser utilizado sem o serviço principal e a integração desse elemento ou funcionalidade não constitui um meio para contornar a aplicabilidade das regras do presente regulamento. Por exemplo, os filtros que categorizam as características faciais ou corporais utilizadas nos mercados em linha poderão constituir um desses elementos acessórios, uma vez que só podem ser utilizados associados ao serviço principal que consiste em vender um produto, ao darem ao consumidor a possibilidade de se pré-visualizar a usar o produto e ajudando-o a tomar uma decisão de compra. Os filtros utilizados nos serviços de redes sociais em linha que categorizam características faciais ou corporais para permitir que os utilizadores acrescentem ou alterem imagens ou vídeos também poderão ser considerados elementos acessórios, uma vez que esses filtros não podem ser utilizados sem o serviço principal dos serviços da rede social, que consiste na partilha de conteúdos em linha.

(17) O conceito de «sistema de identificação biométrica à distância» a que se refere o presente regulamento deverá ser definido, de modo funcional, como um sistema de IA que se destina à identificação de pessoas singulares sem a sua participação ativa, normalmente à distância, por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência, independentemente da tecnologia, dos processos ou dos tipos de dados biométricos específicos utilizados. Tais sistemas de identificação biométrica à distância são geralmente utilizados para detetar várias pessoas ou o seu comportamento em simultâneo, a fim de facilitar significativamente a identificação de pessoas singulares sem a sua participação ativa. Estão excluídos os sistemas de IA concebidos para serem utilizados na verificação biométrica, que inclui a autenticação, cujo único objetivo seja confirmar que uma pessoa singular específica é quem afirma ser e confirmar a identidade de uma pessoa singular com o único objetivo de lhe conceder acesso a um serviço, desbloquear um dispositivo ou ter acesso de segurança a um local. Essa exclusão justifica-se pelo facto de esses sistemas serem suscetíveis de ter um impacto ligeiro nos direitos fundamentais das pessoas singulares em comparação com os sistemas de identificação biométrica à distância que podem ser utilizados para o tratamento de dados biométricos de um grande número de pessoas sem a sua participação ativa. No caso dos sistemas «em tempo real», a recolha dos dados biométricos, a comparação e a identificação ocorrem de forma instantânea, quase instantânea ou, em todo o caso, sem um desfasamento significativo. Não deverá haver, a este respeito, margem para contornar as regras do presente regulamento sobre a utilização «em tempo real» dos sistemas de IA em causa prevendo ligeiros desfasamentos no sistema. Os sistemas «em tempo real» implicam a utilização «ao vivo» ou «quase ao vivo» de materiais, como imagens vídeo, gerados por uma câmara ou outro dispositivo com uma funcionalidade semelhante. No caso dos sistemas «em diferido», ao invés, os dados biométricos já foram recolhidos e a comparação e a identificação ocorrem com um desfasamento significativo. Estes sistemas utilizam materiais, tais como imagens ou vídeos, gerados por câmaras de televisão em circuito fechado ou dispositivos privados antes de o sistema ser utilizado relativamente às pessoas singulares em causa.

(18) O conceito de «sistema de reconhecimento de emoções» a que se refere o presente regulamento deverá ser definido como um sistema de IA concebido para identificar ou inferir emoções ou intenções de pessoas singulares com base nos seus dados biométricos. O conceito refere-se a emoções ou intenções como a felicidade, a tristeza, a raiva, a surpresa, a repugnância, o embaraço, o entusiasmo, a vergonha, o desprezo, a satisfação e o divertimento. Não inclui estados físicos, como dor ou fadiga, incluindo, por exemplo, sistemas utilizados para detetar o estado de fadiga dos pilotos ou motoristas profissionais para efeitos de prevenção de acidentes. Também não inclui a mera deteção de expressões, gestos ou movimentos rapidamente visíveis, a menos que sejam utilizados para identificar ou inferir emoções. Essas expressões podem ser expressões faciais básicas, tais como franzir a testa ou sorrir, ou gestos como o movimento das mãos, dos braços ou da cabeça, ou características da voz de uma pessoa, como levantar a voz ou sussurrar.

(19) Para efeitos do presente regulamento, deverá entender-se por «espaço acessível ao público» qualquer espaço físico que seja acessível a um número indeterminado de pessoas singulares e independentemente de o espaço em questão ser detido por uma entidade privada ou pública, independentemente da atividade para a qual o espaço possa ser utilizado – por exemplo, para o comércio (por exemplo, lojas, restaurantes, cafés), para a prestação de serviços (por exemplo, bancos, atividades profissionais, hotelaria), para o desporto (por exemplo, piscinas, ginásios, estádios), para os transportes (designadamente estações de autocarros, metropolitanos e ferroviárias, aeroportos, meios de transporte), para o entretenimento (por exemplo, cinemas, teatros, museus, salas de concertos e salas de conferências), ou para o lazer ou outros (por exemplo, estradas, praças, parques, florestas ou parques infantis públicos). Um espaço também deverá ser classificado como acessível ao público se, independentemente das eventuais restrições de capacidade ou de segurança, o acesso estiver sujeito a certas condições predeterminadas, que podem ser preenchidas por um número indeterminado de pessoas, tais como a compra de um bilhete ou título de transporte, a inscrição prévia ou uma determinada idade. Em contrapartida, um espaço não deverá ser considerado acessível ao público se o acesso for limitado a pessoas singulares específicas e definidas, seja nos termos do direito da União ou do direito nacional diretamente relacionado com a segurança pública ou por manifestação clara da vontade da pessoa que exerça a autoridade pertinente no espaço. A possibilidade factual de acesso por si só, (como uma porta destrancada ou um portão aberto numa vedação) não implica que o espaço seja acessível ao público na presença de indicações ou circunstâncias que sugiram o contrário, como sinais que proíbam ou restrinjam o acesso. As instalações de empresas e fábricas, bem como os escritórios e os locais de trabalho a que se pretende que apenas os trabalhadores e prestadores de serviços pertinentes tenham acesso, são espaços que não são acessíveis ao público. Os espaços acessíveis ao público não deverão incluir prisões nem zonas de controlo fronteiriço. Alguns outros espaços são compostos tanto por espaços não acessíveis ao público como e por espaços acessíveis ao público, tais como um corredor de um edifício residencial privado necessário para aceder a um gabinete médico ou a um aeroporto. Os espaços em linha também não são abrangidos, uma vez que não são espaços físicos. Para determinar se um espaço é acessível ao público deverá recorrer-se a uma análise casuística, tendo em conta as especificidades da situação em apreço.

(20) A fim de obter os maiores benefícios dos sistemas de IA, protegendo simultaneamente os direitos fundamentais, a saúde e a segurança e permitir o controlo democrático, a literacia no domínio da IA deverá dotar os prestadores, os responsáveis pela implantação e as pessoas afetadas das noções necessárias para tomarem decisões informadas sobre os sistemas de IA. Essas noções podem variar em função do contexto pertinente e podem incluir a compreensão da correta aplicação dos elementos técnicos durante a fase de desenvolvimento do sistema de IA, as medidas a aplicar durante a sua utilização, as formas adequadas de interpretar o resultado do sistema de IA e, no caso das pessoas afetadas, os conhecimentos necessários para compreender de que forma as decisões tomadas com a assistência da IA as afetarão. No contexto da aplicação do presente regulamento, a literacia no domínio da IA deverá proporcionar a todos os intervenientes pertinentes da cadeia de valor da IA os conhecimentos necessários para assegurar o cumprimento adequado e a sua correta execução. Além disso, a ampla aplicação de medidas de literacia no domínio da IA e a introdução de medidas de acompanhamento adequadas poderão contribuir para melhorar as condições de trabalho e, em última análise, apoiar a consolidação e a trajetória da inovação de uma IA de confiança na União. O Comité Europeu para a Inteligência Artificial («Comité») deverá apoiar a Comissão na promoção de ferramentas de literacia no domínio da IA, da sensibilização do público e da compreensão das vantagens, riscos, garantias, direitos e obrigações relacionados com a utilização de sistemas de IA. Em cooperação com as partes interessadas pertinentes, a Comissão e os Estados-Membros deverão facilitar a elaboração de códigos de conduta voluntários para promover a literacia no domínio da IA entre as pessoas que lidam com o desenvolvimento, o funcionamento e a utilização da IA.

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

(22) Atendendo à sua natureza digital, determinados sistemas de IA deverão ser abrangidos pelo âmbito do presente regulamento, mesmo não sendo colocados no mercado, colocados em serviço nem utilizados na União. Tal aplica-se, por exemplo, quando um operador estabelecido na União contrata determinados serviços a um operador estabelecido num país terceiro relativamente a uma atividade a realizar por um sistema de IA que seja considerado de risco elevado. Nessas circunstâncias, o sistema de IA utilizado num país terceiro pelo operador poderá tratar dados recolhidos e transferidos licitamente da União e facultar ao operador contratante na União os resultados desse sistema de IA decorrentes do tratamento desses dados, sem que o sistema de IA em causa seja colocado no mercado, colocado 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 deverá ser igualmente aplicável a prestadores e a responsáveis pela implantação de sistemas de IA que estejam estabelecidos num país terceiro, na medida em que esteja prevista a utilização na União dos resultados produzidos por esses sistemas.

No entanto, para ter em conta os mecanismos existentes e as necessidades especiais da cooperação futura com os parceiros estrangeiros com quem são trocadas informações e dados, o presente regulamento não deverá ser aplicável às autoridades públicas de um país terceiro nem às organizações internacionais quando estas atuam no âmbito da cooperação ou de acordos internacionais celebrados a nível da União ou ao nível nacional para efeitos de cooperação policial e judiciária com a União ou os Estados-Membros, desde que o país terceiro ou organização internacional em causa apresente garantias adequadas em matéria de proteção dos direitos e liberdades fundamentais das pessoas. Se for caso disso, tal pode abranger as atividades das entidades às quais os países terceiros confiam a funções específicas de apoio a essa cooperação policial e judiciária. Tais regimes de cooperação ou acordos têm sido estabelecidos bilateralmente entre Estados-Membros e países terceiros, ou entre a União Europeia, a Europol e outras agências da União e países terceiros e organizações internacionais. As autoridades competentes para a supervisão das autoridades responsáveis pela aplicação da lei e judiciárias ao abrigo do presente regulamento deverão avaliar se esses regimes de cooperação ou acordos internacionais preveem garantias adequadas no que diz respeito à proteção dos direitos e liberdades fundamentais das pessoas. As autoridades nacionais destinatárias e as instituições, órgãos e organismos destinatários da União que utilizam esses resultados na União continuam a ser responsáveis por assegurar que a sua utilização é conforme com o direito da União. Se esses acordos internacionais forem revistos ou se forem celebrados novos acordos no futuro, as partes contratantes deverão envidar todos os esforços para alinhar esses acordos com os requisitos do presente regulamento.

(23) O presente regulamento deverá ser também aplicável a instituições, órgãos e organismos da União quando atuam como prestador ou responsável pela implantação de um sistema de IA.

(24) Se, e na medida em que, os sistemas de IA forem colocados no mercado, colocados em serviço ou utilizados com ou sem modificação desses sistemas para fins militares, de defesa ou de segurança nacional, tais sistemas deverão ser excluídos do âmbito de aplicação do presente regulamento, independentemente do tipo de entidade que realiza essas atividades, seja ela designadamente uma entidade pública ou privada. No que diz respeito aos fins militares e de defesa, essa exclusão é justificada tanto pelo artigo 4.º, n.º 2, do TUE como pelas especificidades da política de defesa dos Estados—Membros e da União abrangidas pelo título V, capítulo 2, do TUE, que estão sujeitas ao direito internacional público, que é, por conseguinte, o regime jurídico mais adequado para a regulamentação dos sistemas de IA no contexto da utilização da força letal e de outros sistemas de IA no contexto de atividades militares e de defesa. No que diz respeito aos fins de segurança nacional, a exclusão justifica-se tanto pelo facto de a segurança nacional continuar a ser da exclusiva responsabilidade dos Estados—Membros, em conformidade com o artigo 4.º, n.º 2, do TUE, como pela natureza específica e pelas necessidades operacionais específicas das atividades de segurança nacional e pelas regras nacionais específicas aplicáveis a essas atividades. No entanto, se um sistema de IA desenvolvido, colocado no mercado, colocado em serviço ou utilizado para fins militares, de defesa ou de segurança nacional for utilizado, temporária ou permanentemente, para outros fins, como por exemplo, para fins civis ou humanitários, de aplicação da lei ou de segurança pública, será abrangido pelo âmbito de aplicação do presente regulamento. Nesse caso, as entidades que utilizarem o sistema de IA para fins que não sejam fins militares, de defesa ou de segurança nacional deverão assegurar a conformidade do sistema com o presente regulamento, a menos que o sistema de IA já esteja em conformidade com o presente regulamento. Os sistemas de IA colocados no mercado ou colocados em serviço para um fim excluído, nomeadamente um fim militar, de defesa ou de segurança nacional, e um ou mais fins não excluídos, como fins civis ou de aplicação da lei, são abrangidos pelo âmbito de aplicação do presente regulamento e os prestadores desses sistemas deverão assegurar a conformidade com o presente regulamento. Nesses casos, o facto de um sistema de IA poder ser abrangido pelo âmbito de aplicação do presente regulamento não deverá afetar a possibilidade de as entidades que realizam atividades de segurança nacional, de defesa e militares, independentemente do tipo de entidade que realiza essas atividades, utilizarem para fins de segurança nacional, de defesa e militares sistemas de IA cuja utilização esteja excluída do âmbito de aplicação do presente regulamento. Um sistema de IA colocado no mercado para fins civis ou de aplicação da lei que seja utilizado com ou sem modificações para fins militares, de defesa ou de segurança nacional não deverá ser abrangido pelo âmbito de aplicação do presente regulamento, independentemente do tipo de entidade que realiza essas atividades.

(25) O presente regulamento deverá apoiar a inovação, deverá respeitar a liberdade da ciência e não deverá prejudicar as atividades de investigação e desenvolvimento. Por conseguinte, é necessário excluir do seu âmbito de aplicação os sistemas e modelos de IA especificamente desenvolvidos e colocados em serviço exclusivamente para fins de investigação e desenvolvimento científicos. Além disso, é necessário assegurar que o presente regulamento não afete de outra forma as atividades científicas de investigação e desenvolvimento em matéria de sistemas ou modelos de IA antes de ser colocado no mercado ou colocado em serviço. No que diz respeito às atividades de investigação, testagem e desenvolvimento orientadas para os produtos relativas a sistemas ou modelos de IA, as disposições do presente regulamento também não deverão ser aplicáveis antes de esses sistemas e modelos serem colocados em serviço ou colocados no mercado. Essa exclusão não prejudica a obrigação de cumprir o presente regulamento sempre que um sistema de IA abrangido pelo âmbito de aplicação do presente regulamento for colocado no mercado ou colocado em serviço em resultado dessas atividades de investigação e desenvolvimento, nem a aplicação das disposições relativas aos ambientes de testagem da regulamentação da IA e à testagem em condições reais. Além disso, sem prejuízo da exclusão de sistemas de IA especificamente desenvolvidos e colocados em serviço para fins exclusivos de investigação e desenvolvimento científicos, qualquer outro sistema de IA que possa ser utilizado para a realização de atividades de investigação e desenvolvimento deverá continuar sujeito às disposições do presente regulamento. Em todo o caso, todas as atividades de investigação e desenvolvimento deverão ser realizadas em conformidade com normas éticas e profissionais reconhecidas em matéria de investigação científica e deverão ser conduzidas em conformidade com o direito da União aplicável.

(26) Para que o conjunto de normas vinculativas aplicáveis aos sistemas de IA seja proporcionado e eficaz, deverá seguir-se uma abordagem baseada no risco claramente definida. Essa abordagem deverá adaptar o tipo e o conteúdo dessas normas à intensidade e ao âmbito dos riscos que podem ser criados pelos sistemas de IA. Como tal, é necessário proibir determinadas práticas inaceitáveis de IA, 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.

(27) Embora a abordagem baseada no risco constitua a base para um conjunto proporcionado e eficaz de regras vinculativas, é importante recordar as Orientações Éticas para uma IA de Confiança, elaboradas em 2019 pelo IA HLEG independente nomeado pela Comissão. Nessas orientações, o IA HLEG desenvolveu sete princípios éticos não vinculativos para a IA, que se destinam a ajudar a garantir que a IA é de confiança e eticamente correta. Os sete princípios incluem: iniciativa e supervisão por humanos; solidez técnica e segurança; privacidade e governação dos dados; transparência; diversidade, não discriminação e equidade; bem-estar social e ambiental e responsabilização. Sem prejuízo dos requisitos juridicamente vinculativos do presente regulamento e de qualquer outras disposições aplicáveis do direito da União, essas orientações contribuem para a conceção de uma IA coerente, de confiança e centrada no ser humano, em consonância com a Carta e com os valores em que se funda a União. De acordo com as orientações do IA HLEG, «iniciativa e supervisão por humanos» significa que todos os sistemas de IA são desenvolvidos e utilizados como uma ferramenta ao serviço das pessoas, que respeita a dignidade humana e a autonomia pessoal e que funciona de uma forma que possa ser adequadamente controlada e supervisionada por seres humanos.

Solidez técnica e segurança significa que os sistemas de IA são desenvolvidos e utilizados de forma a permitir a solidez em caso de problemas e a resiliência contra tentativas de alteração da sua utilização ou desempenho que permitam a utilização ilícita por terceiros, e a minimizar os danos não intencionais. Por privacidade e governação dos dados entende-se que os sistemas de IA são desenvolvidos e utilizados em conformidade com as regras existentes em matéria de privacidade e de proteção de dados, ao mesmo tempo que o tratamento de dados satisfaz normas elevadas em termos de qualidade e de integridade. A transparência significa que os sistemas de IA são desenvolvidos e utilizados de forma a permitir uma rastreabilidade e explicabilidade adequadas, sensibilizando ao mesmo tempo os seres humanos para o facto de estarem a comunicar ou a interagir com um sistema de IA, informando devidamente os responsáveis pela implantação das capacidades e limitações desse sistema de IA e informando as pessoas afetadas dos direitos que lhes assistem. Diversidade, não discriminação e equidade indica que os sistemas de IA são desenvolvidos e utilizados de forma a incluir diferentes intervenientes e a promover a igualdade de acesso, a igualdade de género e a diversidade cultural, evitando simultaneamente efeitos discriminatórios e enviesamentos injustos que sejam proibidos pelo direito da União ou pelo direito nacional. Por bem-estar social e ambiental entende-se que os sistemas de IA são desenvolvidos e utilizados de forma sustentável e respeitadora do ambiente, bem como de forma a beneficiar todos os seres humanos, controlando e avaliando ao mesmo tempo os impactos de longo prazo nas pessoas, na sociedade e na democracia. A aplicação desses princípios deverá traduzir-se, sempre que possível, na conceção e na utilização de modelos de IA. Em qualquer caso, deverão servir de base para a elaboração de códigos de conduta ao abrigo do presente regulamento. Todas as partes interessadas, incluindo a indústria, o meio académico, a sociedade civil e as organizações de normalização, são incentivadas a ter em conta, consoante o caso, os princípios éticos para o desenvolvimento de boas práticas e normas voluntárias.

(28) Além das suas inúmeras utilizações benéficas, a IA, pode também ser utilizada indevidamente e conceder instrumentos novos e poderosos para práticas manipuladoras, exploratórias e de controlo social. Essas práticas são particularmente prejudiciais e abusivas e deverão ser proibidas por desrespeitarem valores da União, como a dignidade do ser humano, a liberdade, a igualdade, a democracia e o Estado de direito, bem como os direitos fundamentais consagrados na Carta, nomeadamente o direito à não discriminação, à proteção de dados pessoais e à privacidade, e os direitos das crianças.

(29) As técnicas de manipulação propiciadas pela IA podem ser utilizadas para persuadir as pessoas a adotarem comportamentos indesejados, ou para as enganar incentivando-as a tomar decisões de uma forma que subverta e prejudique a sua autonomia, a sua tomada de decisões e a sua liberdade de escolha. A colocação no mercado, a colocação em serviço ou a utilização de determinados sistemas de IA com o objetivo ou o efeito de distorcer substancialmente o comportamento humano, sendo passível a ocorrência de danos significativos, em especial com repercussões negativas suficientemente importantes na saúde física, psicológica ou nos interesses financeiros, são particularmente perigosas e deverão, por isso, ser proibidas. Esses sistemas de IA utilizam quer componentes subliminares, como estímulos de áudio, de imagem e de vídeo dos quais as pessoas não se conseguem aperceber por serem estímulos que ultrapassam a perceção humana, quer outras técnicas manipuladoras ou enganadoras que subvertem ou prejudicam a autonomia, a tomada de decisões ou a liberdade de escolha das pessoas de uma maneira de que estas não têm consciência dessas técnicas ou que, mesmo que tenham consciência das mesmas, ainda possam ser enganadas ou não as possam impedir de controlar ou não lhes possam resistir. Tal poderá ser facilitado, por exemplo, por interfaces máquina-cérebro ou por realidade virtual, que permitem um maior nível de controlo do tipo de estímulos apresentados às pessoas, na medida em que podem distorcer substancialmente o seu comportamento de uma forma significativamente nociva. Além disso, os sistemas de IA podem também explorar vulnerabilidades de uma pessoa ou de um grupo específico de pessoas devido à sua idade, à sua deficiência na aceção da Diretiva (UE) 2019/882 do Parlamento Europeu e do Conselho[16], ou a uma situação social ou económica específica suscetível de tornar essas pessoas mais vulneráveis à exploração, como as pessoas que vivem em situação de pobreza extrema ou as minorias étnicas ou religiosas.

---

[16] Diretiva (UE) 2019/882 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos requisitos de acessibilidade dos produtos e serviços (JO L 151 de 7.6.2019, p. 70).

Esses sistemas de IA podem ser colocados no mercado, colocados em serviço ou utilizados com o objetivo ou o efeito de distorcer substancialmente o comportamento de uma pessoa e de uma forma que cause ou seja razoavelmente suscetível de causar danos significativos a essa ou a outra pessoa ou grupos de pessoas, incluindo danos que possam ser acumulados ao longo do tempo, razão pela qual deverão ser proibidos. Pode não ser possível presumir que existe intenção de distorcer o comportamento se a distorção resultar de fatores externos ao sistema de IA que estejam fora do controlo do prestador ou do responsável pela implantação, nomeadamente fatores que podem não ser razoavelmente previsíveis e que, por conseguinte, o prestador ou responsável pela implantação do sistema de IA não possam atenuar. De qualquer modo, não é necessário que o prestador ou o responsável pela implantação tenha a intenção de causar danos significativos, basta que tal dano resulte das práticas manipuladoras ou exploratórias baseadas na IA. As proibições de tais práticas de IA complementam as disposições da Diretiva 2005/29/CE do Parlamento Europeu e do Conselho[17], nomeadamente as que proíbem as práticas comerciais desleais que causam danos económicos ou financeiros aos consumidores, em quaisquer circunstâncias, independentemente de serem aplicadas através de sistemas de IA ou de outra forma. As proibições de práticas manipuladoras e exploratórias previstas no presente regulamento não deverão afetar as práticas lícitas no contexto de tratamentos médicos, como o tratamento psicológico de uma doença mental ou a reabilitação física, sempre que tais práticas sejam realizadas em conformidade com a lei e as normas médicas aplicáveis, como, por exemplo, o consentimento explícito das pessoas ou dos seus representantes legais. Além disso, as práticas comerciais comuns e legítimas, como por exemplo no domínio da publicidade, que cumpram a lei aplicável não deverão, por si só, ser consideradas práticas manipuladoras prejudiciais tornadas possíveis pela IA.

---

[17] Diretiva 2005/29/CE do Parlamento Europeu e do Conselho, de 11 de maio de 2005, relativa às práticas comerciais desleais das empresas face aos consumidores no mercado interno e que altera a Diretiva 84/450/CEE do Conselho, as Diretivas 97/7/CE, 98/27/CE e 2002/65/CE do Parlamento Europeu e do Conselho e o Regulamento (CE) n.º 2006/2004 do Parlamento Europeu e do Conselho («Diretiva relativa às práticas comerciais desleais») (JO L 149 de 11.6.2005, p. 22).

(30) Deverão ser proibidos os sistemas de categorização biométrica baseados em dados biométricos de pessoas singulares, como o rosto ou as impressões digitais, para deduzir ou inferir as suas opiniões políticas, a filiação sindical, as convicções religiosas ou filosóficas, a raça, a vida sexual ou a orientação sexual de uma pessoa. Essa proibição não deverá abranger a rotulagem legal, a filtragem ou a categorização de conjuntos de dados biométricos adquiridos em conformidade com o direito da União ou o direito nacional em função dos dados biométricos, como a triagem de imagens em função da cor do cabelo ou da cor dos olhos, que podem, por exemplo, ser utilizadas no domínio da aplicação da lei.

(31) Os sistemas de IA que possibilitam a classificação social de pessoas singulares por intervenientes públicos ou privados 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 pessoas singulares ou grupos de pessoas singulares com base em múltiplos pontos de dados relacionados com o seu comportamento social em diversos contextos ou em características pessoais ou de personalidade conhecidas, inferidas ou previsíveis ao longo de determinados períodos. A classificação social obtida por meio desses sistemas de IA pode levar ao tratamento prejudicial ou desfavorável de pessoas singulares ou grupos inteiros de pessoas singulares em contextos sociais não relacionados com o contexto em que os dados foram originalmente gerados ou recolhidos, ou a um tratamento prejudicial desproporcionado ou injustificado face à gravidade do seu comportamento social. Como tal, deverão ser proibidos sistemas de IA que impliquem tais práticas de classificação inaceitáveis e conducentes a esses resultados prejudiciais ou desfavoráveis. Essa proibição não deverá afetar as práticas de avaliação lícitas de pessoas singulares efetuadas para um fim específico, em conformidade com o direito da União e o direito nacional.

(32) 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 aplicação da lei é 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. 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. Estes possíveis resultados enviesados e efeitos discriminatórios são particularmente relevantes no que diz respeito à idade, etnia, raça, sexo ou deficiência. Além disso, o impacto imediato e as oportunidades limitadas para a realização de controlos adicionais ou correções no que respeita à utilização desses sistemas que funcionam em tempo real acarretam riscos acrescidos para os direitos e as liberdades das pessoas em causa no contexto, ou afetadas, pelas autoridades responsáveis pela aplicação da lei.

(33) Como tal, deverá ser proibida a utilização desses sistemas para efeitos de aplicação da lei, salvo em situações enunciadas exaustivamente e definidas de modo restrito, em que essa utilização é estritamente necessária por motivos de interesse público importante e cuja importância prevalece sobre os riscos. Nessas situações incluem-se a busca de determinadas vítimas de crimes, nomeadamente pessoas desaparecidas; certas ameaças à vida ou à segurança física de pessoas singulares ou ameaças de ataque terrorista; e a localização ou identificação de infratores ou suspeitos de infrações penais a que se refere um anexo do presente regulamento, desde que essas infrações penais sejam puníveis no Estado-Membro em causa com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a quatro 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, a lista de infrações penais prevista no anexo do presente regulamento baseia-se nas 32 infrações penais enumeradas na Decisão-Quadro 2002/584/JAI do Conselho[18], tendo em conta que algumas delas são na prática provavelmente mais pertinentes do que outras, já que o recurso à identificação biométrica à distância «em tempo real» poderá previsivelmente ser necessário e proporcionado em graus extremamente variáveis no respeitante à localização ou identificação de um infrator ou suspeito das diferentes infrações penais enumeradas e tendo em conta as prováveis diferenças em termos de gravidade, probabilidade e magnitude dos danos ou das possíveis consequências negativas.

---

[18] 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).

Uma ameaça iminente à vida ou à segurança física de pessoas singulares também poderá resultar de uma perturbação grave causada a uma infraestrutura crítica, na aceção do artigo 2.º, ponto 4, da Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho[19], sempre que a perturbação ou a destruição dessa infraestrutura crítica resulte numa ameaça iminente à vida ou à segurança física de uma pessoa, inclusive ao prejudicar gravemente o fornecimento de bens essenciais à população ou o exercício das funções essenciais do Estado. Além disso, o presente regulamento deverá preservar a capacidade das autoridades competentes em matéria de aplicação da lei, controlo das fronteiras, imigração ou asilo para realizarem controlos de identidade na presença da pessoa em causa, em conformidade com as condições estabelecidas no direito da União e no direito nacional para esses controlos. Em especial, as autoridades competentes em matéria de aplicação da lei, controlo das fronteiras, imigração ou asilo deverão poder utilizar sistemas de informação, em conformidade com o direito da União ou o direito nacional, para identificar pessoas que, durante um controlo de identidade, se recusem a ser identificadas ou não sejam capazes de declarar ou provar a sua identidade, sem serem obrigadas a obter uma autorização prévia por força do presente regulamento. Pode tratar-se, por exemplo, de uma pessoa envolvida num crime que não queira, ou não possa devido a um acidente ou doença, revelar a sua identidade às autoridades responsáveis pela aplicação da lei.

---

[19] Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho (JO L 333 de 27.12.2022, p. 164).

(34) A fim de assegurar que esses sistemas sejam utilizados de uma forma responsável e proporcionada, também importa estabelecer que, em cada uma dessas 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 aplicação da lei só deverá ocorrer para efeitos de confirmação da identidade de uma pessoa especificamente visada e deverá ser limitada ao estritamente necessário no que respeita ao período, bem como ao âmbito geográfico e pessoal, tendo em conta, especialmente, os dados ou indícios relativos às ameaças, às vítimas ou ao infrator. A utilização do sistema de identificação biométrica à distância em tempo real em espaços acessíveis ao público só deverá ser autorizada se a competente autoridade responsável pela aplicação da lei tiver concluído uma avaliação de impacto sobre os direitos fundamentais e, salvo disposição em contrário no presente regulamento, tiver registado o sistema na base de dados prevista no presente regulamento. A base de dados de pessoas utilizada como referência deverá ser adequada a cada utilização em cada uma das situações acima indicadas.

(35) Cada utilização de um sistema de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de aplicação da lei deverá estar sujeita a uma autorização expressa e específica de uma autoridade judiciária ou de uma autoridade administrativa independente de um Estado-Membro cuja decisão seja vinculativa. Em princípio, essa autorização deverá ser obtida antes da utilização do sistema de IA com vista a identificar uma ou várias pessoas. Deverão ser permitidas exceções a essa regra em situações devidamente justificadas por motivos de urgência, nomeadamente em situações em que a necessidade de utilizar os sistemas em causa seja tal que torne efetiva e objetivamente impossível obter uma autorização antes de iniciar a utilização do sistema de IA. Nessas situações de urgência, a utilização do sistema de IA deverá 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 responsável pela aplicação da lei. Além disso, em tais situações, a autoridade responsável pela aplicação da lei deverá solicitar essa autorização, apresentando simultaneamente as razões para não ter podido solicitá-la mais cedo, sem demora injustificada e, o mais tardar, no prazo de 24 horas. Se essa autorização for recusada, a utilização de sistemas de identificação biométrica em tempo real associados a essa autorização deverá cessar com efeitos imediatos e todos os dados relacionados com essa utilização deverão ser suprimidos e apagados. Tais dados incluem dados de entrada adquiridos diretamente por um sistema de IA durante a utilização desse sistema, bem como os resultados da utilização associada a essa autorização. Não deverá incluir os dados de entrada licitamente adquiridos em conformidade com outras disposições pertinentes do direito da União ou do direito nacional. Em qualquer caso, nenhuma decisão que produza efeitos jurídicos adversos sobre uma pessoa deverá ser tomada exclusivamente com base nos resultados saídos do sistema de identificação biométrica à distância.

(36) A fim de desempenharem as suas funções em conformidade com os requisitos estabelecidos no presente regulamento e nas regras nacionais, as autoridades de fiscalização do mercado competentes e a autoridade nacional de proteção de dados deverão ser notificadas de cada utilização do sistema de identificação biométrica em tempo real. As autoridades de fiscalização do mercado e as autoridades nacionais de proteção de dados que tenham sido notificadas deverão apresentar à Comissão um relatório anual sobre a utilização de sistemas de identificação biométrica em tempo real.

(37) Além disso, no âmbito do regime exaustivo estabelecido pelo presente regulamento, importa salientar que essa utilização no território de um Estado-Membro em conformidade com o presente regulamento apenas deverá ser possível uma vez que o Estado-Membro em causa tenha decidido possibilitar expressamente a autorização dessa utilização 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. Essas regras nacionais deverão ser comunicadas à Comissão no prazo de 30 dias a contar da sua adoção.

(38) 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 aplicação da lei 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, deverão 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 deverão ser possíveis se forem compatíveis com o regime estabelecido pelo presente regulamento, sem que exista margem, fora desse regime, 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 aplicação da lei. Nesse 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 de aplicação da lei, inclusive por parte das autoridades competentes, não deverá ser abrangida pelo regime específico relativo a essa utilização para efeitos de aplicação da lei estabelecido pelo presente regulamento. Assim, uma utilização para outros fins que não a aplicação da lei não deverá estar sujeita ao requisito de autorização previsto no presente regulamento nem às regras de execução aplicáveis do direito nacional que possam dar prevalência a essa autorização.

(39) 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 aplicação da lei conforme regida pelo presente regulamento deverá continuar a cumprir todos os requisitos decorrentes do artigo10.º da Diretiva (UE) 2016/680. Para outros fins que não a aplicação da lei, o artigo 9.º, n.º 1, do Regulamento (UE) 2016/679 e o artigo 10.º, n.º 1, do Regulamento (UE) 2018/1725 proíbem o tratamento de dados biométricos, salvo nos casos abrangidos pelas exceções limitadas previstas nesses artigos. Em aplicação do artigo 9.º, n.º 1, do Regulamento (UE) 2016/679, a utilização da identificação biométrica à distância para outros fins que não a aplicação da lei já foi objeto de decisões de proibição por parte das autoridades nacionais de proteção de dados.

(40) 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, primeiro parágrafo, alínea g), na medida em que se aplica à utilização de sistemas de categorização biométrica para atividades no domínio da cooperação policial e da cooperação judicial em matéria penal, no artigo 5.º, n.º1, primeiro parágrafo, alínea d), na medida em que se aplica à utilização de sistemas de IA abrangidos por essa disposição, no artigo 5.º, n.º 1, primeiro parágrafo, alínea h), no artigo 5.º, n.os 3 a 6, e no artigo 26.º, n.º 10, do presente regulamento, 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 a Irlanda 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.

(41) 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, primeiro parágrafo, alínea g), na medida em que se aplica à utilização de sistemas de categorização biométrica para atividades no domínio da cooperação policial e da cooperação judicial em matéria penal, no artigo 5.º, n.º1, primeiro parágrafo, alínea d), na medida em que se aplica à utilização de sistemas de IA abrangidos por essa disposição, e no artigo 5.º, n.º 1, primeiro parágrafo, alínea h), n.os 2 a 6, e no artigo 26.º, n. 10, do presente regulamento, 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.

(42) Em conformidade com a presunção de inocência, as pessoas singulares na União deverão ser sempre avaliadas em função do seu comportamento real. As pessoas singulares nunca poderão ser julgadas com base no comportamento previsto pela IA com base exclusivamente na definição do seu perfil, nos traços ou características da sua personalidade, como a nacionalidade, o local de nascimento, o local de residência, o número de filhos, o nível de endividamento ou o tipo de automóvel que têm, sem que exista uma suspeita razoável do seu envolvimento numa atividade criminosa com base em factos objetivos verificáveis, e sem uma avaliação humana dos mesmos. Por conseguinte, deverá ser proibido efetuar avaliações de risco de pessoas singulares que visem avaliar a probabilidade de cometerem infrações ou prever a ocorrência de uma infração penal real ou potencial exclusivamente com base na definição do seu perfil ou na avaliação dos traços e características da sua personalidade. Em todo o caso, essa proibição não se refere nem diz respeito a análises de risco que não se baseiem na definição de perfis de pessoas ou nos traços e características da personalidade de pessoas, tais como sistemas de IA que utilizam análises de risco para avaliar a probabilidade de fraude financeira por parte de empresas com base em transações suspeitas, ou ferramentas de análise de risco para prever a probabilidade de localização de estupefacientes ou mercadorias ilícitas pelas autoridades aduaneiras, por exemplo, com base em rotas de tráfico conhecidas.

(43) A colocação no mercado, a colocação em serviço para esse fim específico ou a utilização de sistemas de IA que criam ou expandem bases de dados de reconhecimento facial através da recolha aleatória de imagens faciais da Internet ou de imagens de CCTV deverão ser proibidas por essa prática aumentar o sentimento de vigilância em larga escala e poder conduzir a violações grosseiras dos direitos fundamentais, incluindo o direito à privacidade.

(44) Existem sérias preocupações quanto à base científica dos sistemas de IA que visam identificar ou inferir emoções, especialmente porque a expressão de emoções varia consideravelmente entre culturas e situações, e até num mesmo indivíduo. Entre as principais deficiências desses sistemas contam-se a fiabilidade limitada, a falta de especificidade e a possibilidade limitada de generalização. Assim sendo, os sistemas de IA que identificam ou fazem inferências de emoções ou intenções de pessoas singulares com base nos seus dados biométricos podem conduzir a resultados discriminatórios e ser intrusivos nos direitos e liberdades das pessoas em causa. Tendo em conta o desequilíbrio de poder no contexto do trabalho ou da educação, combinado com a natureza intrusiva destes sistemas, tais sistemas podem conduzir a um tratamento prejudicial ou desfavorável de certas pessoas singulares ou de grupos inteiros de pessoas singulares. Por conseguinte, deverá ser proibida a colocação no mercado, a colocação em serviço ou a utilização de sistemas de IA concebidos para serem utilizados na deteção do estado emocional das pessoas em situações relacionadas com o local de trabalho e a educação. Essa proibição não deverá abranger os sistemas de IA colocados no mercado exclusivamente por razões médicas ou de segurança, como os sistemas destinados a utilização terapêutica.

(45) As práticas proibidas pelo direito da União, nomeadamente a legislação sobre proteção de dados, não discriminação, defesa do consumidor e direito da concorrência, não poderão ser afetadas pelo presente regulamento.

(46) Os sistemas de IA de risco elevado só deverão ser colocados no mercado da União, colocados em serviço ou utilizados se cumprirem determinados requisitos obrigatórios. Esses requisitos deverão assegurar que os sistemas de IA de risco elevado disponíveis na União ou cujos resultados sejam utilizados na União não representem riscos inaceitáveis para interesses públicos importantes da União, conforme reconhecidos e protegidos pelo direito da União. Com base no novo regime jurídico, tal como clarificado na comunicação da Comissão intitulada «Guia Azul de 2022 sobre a aplicação das regras da UE em matéria de produtos»[20], a regra geral é a de que mais do que um ato jurídico da legislação de harmonização da União, como os Regulamentos (UE) 2017/745[21] e (UE) 2017/746[22] do Parlamento Europeu e do Conselho ou a Diretiva 2006/42/CE do Parlamento Europeu e do Conselho[23], pode ser aplicável a um produto, uma vez que a disponibilização ou a colocação em serviço só pode ter lugar quando o produto cumprir toda a legislação de harmonização da União aplicável. A fim de assegurar a coerência e evitar encargos administrativos ou custos desnecessários, os prestadores de um produto que contenha um ou mais sistemas de IA de risco elevado, aos quais se aplicam os requisitos do presente regulamento e os requisitos dos atos enumerados na lista da legislação de harmonização da União constante de um anexo do presente regulamento, deverão ser flexíveis no que diz respeito às decisões operacionais sobre a forma otimizada de assegurar a conformidade de um produto que contenha um ou mais sistemas de IA com todos os requisitos aplicáveis da legislação harmonizada da União. A classificação de risco elevado aplicada a sistemas de IA deverá limitar-se aos sistemas que têm um impacto prejudicial substancial na saúde, na segurança e nos direitos fundamentais das pessoas na União, e tal limitação deverá minimizar quaisquer potenciais restrições ao comércio internacional.

---

20 JO C 247 de 29.6.2022, p. 1.

21 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).

22 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).

23 Diretiva 2006/42/CE do Parlamento Europeu e do Conselho, de 17 de maio de 2006, relativa às máquinas e que altera a Diretiva 95/16/CE (JO L 157 de 9.6.2006, p. 24).

(47) Os sistemas de IA poderão ter repercussões negativas na saúde e na segurança das pessoas, em particular quando esses sistemas funcionam como componentes de segurança 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, cada vez mais autónomos, deverão poder operar com segurança e desempenhar as suas funções em ambientes complexos, seja num contexto industrial ou de assistência e cuidados pessoais. De igual forma, no setor da saúde – um setor no qual os riscos para a vida e a saúde são particularmente elevados –, os sistemas de diagnóstico e os sistemas que apoiam decisões humanas, que estão cada vez mais sofisticados, deverão produzir resultados exatos e de confiança.

(48) A dimensão das repercussões negativas causadas 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, o direito à não discriminação, o direito à educação, a defesa dos consumidores, os direitos dos trabalhadores, os direitos das pessoas com deficiência, a igualdade de género, os direitos de propriedade intelectual, o direito à ação e a um tribunal imparcial, o direito à defesa e a presunção de inocência, e o direito a uma boa administração. Além desses direitos, é importante salientar o facto de que as crianças têm direitos específicos, consagrados no artigo 24.º da Carta e na Convenção das Nações Unidas sobre os Direitos da Criança, desenvolvidos com 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 deverá ser tido em conta ao avaliar a gravidade dos danos que um sistema de IA pode causar, nomeadamente em relação à saúde e à segurança das pessoas.

(49) 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 de aplicação do Regulamento (CE) n.º 300/2008 do Parlamento Europeu e do Conselho[24], do Regulamento (UE) n.º 167/2013 do Parlamento Europeu e do Conselho[25], do Regulamento (UE) n.º 168/2013 do Parlamento Europeu e do Conselho[26], da Diretiva 2014/90/UE do Parlamento Europeu e do Conselho[27], da Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho[28],

---

24 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).

25 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).

26 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).

27 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).

28 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).

do Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho[29], do Regulamento (UE) 2018/1139 do Parlamento Europeu e do Conselho[30] e do Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho[31], é adequado alterar esses atos para assegurar que a Comissão tenha em conta os requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado estabelecidos no presente regulamento aquando da adoção de quaisquer atos delegados ou de execução pertinentes com base nesses atos, atendendo às especificidades técnicas e regulamentares de cada setor e sem interferir nos mecanismos existentes de governação, de avaliação da conformidade e de execução nem com as autoridades estabelecidas nesses atos.

---

[29] 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).

[30] 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).

[31] 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).

(50) 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 enumerada num anexo do presente regulamento, é apropriado classificá-los como sendo de risco elevado nos termos do presente regulamento se o produto em causa for 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, esses 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, dispositivos médicos para diagnóstico in vitro, automóveis e aviação

(51) A classificação de um sistema de IA como sendo de risco elevado nos termos do presente regulamento não deverá implicar necessariamente que se considere o produto cujo componente de segurança é o sistema de IA, ou o próprio sistema de IA enquanto produto, como sendo de «risco elevado» segundo os critérios estabelecidos na legislação de harmonização da União aplicável ao produto. É o caso, nomeadamente dos Regulamentos (UE) 2017/745 e (UE) 2017/746, em que é prevista uma avaliação da conformidade por terceiros para produtos de risco médio e elevado.

(52) Relativamente aos sistemas de IA autónomos, nomeadamente os sistemas de IA de risco elevado que não são componentes de segurança de produtos, ou que não são, eles próprios, produtos, é apropriado classificá-los como sendo de risco elevado se, à luz da sua 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 da ocorrência desses danos, e se forem utilizados num conjunto de domínios especificamente predefinidos no presente regulamento. A identificação desses sistemas baseia-se na mesma metodologia e nos mesmos critérios previstos também para futuras alterações da lista de sistemas de IA de risco elevado que a Comissão deverá ficar habilitada a adotar, através de atos delegados, a fim de ter em conta o rápido ritmo da evolução tecnológica, bem como as potenciais alterações na utilização de sistemas de IA.

(53) É igualmente importante esclarecer que podem existir casos específicos em que os sistemas de IA referidos em domínios predefinidos especificados no presente regulamento não conduzam a um risco significativo de prejuízo para os interesses jurídicos protegidos nesses domínios por não influenciarem significativamente a tomada de decisões ou não prejudicarem substancialmente esses interesses. Para efeitos do presente regulamento, um sistema de IA que não influencie significativamente o resultado da tomada de decisões deverá ser entendido como um sistema de IA que não tem impacto na substância nem, por conseguinte, no resultado da tomada de decisões, seja ele humano ou automatizado. Um sistema de IA que não influencie significativamente o resultado da tomada de decisões poderá incluir situações em que uma ou mais das seguintes condições estejam preenchidas. A primeira condição deverá ser a de que o sistema de IA se destina a desempenhar uma tarefa processual restrita, como um sistema de IA que transforma dados não estruturados em dados estruturados, um sistema de IA que classifica os documentos recebidos em categorias ou um sistema de IA que é utilizado para detetar duplicações entre um grande número de aplicações. Essas tarefas são de natureza tão restrita e limitada que representam apenas riscos limitados que não aumentam pela utilização num contexto que seja enumerado num anexo do presente regulamento como sendo uma utilização de um sistema de IA de risco elevado. A segunda condição deverá ser a de que a tarefa desempenhada pelo sistema de IA se destina a melhorar o resultado de uma atividade humana previamente concluída que possa ser relevante para efeitos dos usos de risco elevado enumerados num anexo do presente regulamento. Tendo em conta essas características, o sistema de IA proporciona apenas uma camada adicional a uma atividade humana, consequentemente com um risco reduzido. Essa condição será, por exemplo, aplicável aos sistemas de IA destinados a melhorar a linguagem utilizada em documentos redigidos anteriormente, por exemplo em relação ao tom profissional, ao estilo académico ou ao alinhamento do texto com uma determinada mensagem de marca. A terceira condição deverá ser a de que o sistema de IA se destina a detetar padrões de tomada de decisão ou desvios em relação aos padrões de tomada de decisão anteriores.

O risco será reduzido porque a utilização do sistema de IA segue-se a uma avaliação humana previamente concluída, que não se destina a substituir nem a influenciar, sem uma revisão humana adequada. Esses sistemas de IA incluem, por exemplo, os que, tendo em conta um determinado padrão de atribuição de notas de um professor, podem ser utilizados para verificar *ex post* se o professor se pode ter desviado do padrão de atribuição de notas, de modo a assinalar potenciais incoerências ou anomalias. A quarta condição deverá ser a de que o sistema de IA se destina a executar uma tarefa que é apenas preparatória para uma avaliação pertinente para efeitos dos sistemas de IA enumerados num anexo do presente regulamento, tornando assim o possível impacto do resultado do sistema muito reduzido em termos de risco para a avaliação a realizar. Essa condição abrange, entre outras coisas, soluções inteligentes para o tratamento de ficheiros que incluem várias funções, como a indexação, a pesquisa, o processamento de texto e de voz ou a ligação de dados a outras fontes de dados, ou sistemas de IA utilizados para a tradução de documentos iniciais. Em qualquer caso, deverá considerar-se que os sistemas de IA utilizados em casos concretos de utilização de risco elevado, enumerados num anexo do presente regulamento, apresentam riscos significativos de danos para a saúde, a segurança ou os direitos fundamentais se o sistema de IA implicar a definição de perfis na aceção do artigo 4.º, ponto 4, do Regulamento (UE) 2016/679, do artigo 3.º, ponto 4, da Diretiva (UE) 2016/680 ou do artigo 3.º, ponto 5, do Regulamento (UE) 2018/1725. A fim de assegurar a rastreabilidade e a transparência, um prestador que considere que um sistema de IA não é de risco elevado com base nas condições referidas **supra** deverá elaborar a documentação da avaliação antes de esse sistema ser colocado no mercado ou colocado em serviço e deverá apresentar essa documentação às autoridades nacionais competentes mediante pedido. Tal prestador deverá ser obrigado a registar o sistema de IA na base de dados da UE criada ao abrigo do presente regulamento. Com vista a disponibilizar orientações adicionais para a aplicação prática das condições ao abrigo das quais os sistemas de IA referidos num anexo ao presente regulamento não são, a título excecional, de risco elevado, a Comissão deverá, após consulta do Comité, disponibilizar orientações que especifiquem essa aplicação prática, completadas por uma lista exaustiva de exemplos práticos de casos de utilização de sistemas de IA que sejam de risco elevado e de casos de utilização risco não elevado.

(54) Uma vez que os dados biométricos constituem uma categoria especial de dados pessoais, é adequado classificar como sendo de risco elevado vários casos de utilização críticos de sistemas biométricos, na medida em que a sua utilização seja permitida pelo direito da União e o direito nacional aplicáveis. As inexatidões técnicas dos sistemas de IA concebidos para a identificação biométrica à distância de pessoas singulares podem conduzir a resultados enviesados e ter efeitos discriminatórios. O risco desses resultados enviesados e efeitos discriminatórios é particularmente relevante no que diz respeito à idade, etnia, raça, sexo ou deficiência. Os sistemas de identificação biométrica à distância deverão ser, por conseguinte, classificados como de risco elevado, tendo em conta os riscos que representam. Dessa classificação estão excluídos os sistemas de IA concebidos para serem utilizados na verificação biométrica, incluindo a autenticação, cujo único objetivo é confirmar que uma pessoa singular específica é quem afirma ser e confirmar a identidade de uma pessoa singular com o único objetivo de ter acesso a um serviço, desbloquear um dispositivo ou ter acesso seguro a uma instalação. Além disso, os sistemas de IA concebidos para serem utilizados para categorização biométrica de acordo com atributos ou características sensíveis protegidos nos termos do artigo 9.º, n.º 1, do Regulamento (UE) 2016/679 com base em dados biométricos, na medida em que não sejam proibidos nos termos do presente regulamento, e os sistemas de reconhecimento de emoções não proibidos nos termos do presente regulamento deverão ser classificados como sendo de risco elevado. Os sistemas biométricos destinados a serem utilizados exclusivamente para permitir medidas de cibersegurança e de proteção de dados pessoais não deverão ser considerados sistemas de IA de risco elevado.

(55) No tocante à gestão e ao funcionamento de infraestruturas críticas, é apropriado classificar como sendo de risco elevado os sistemas de IA que se destinam a ser utilizados como componentes de segurança na gestão e no funcionamento das infraestruturas digitais críticas conforme enumeradas no ponto 8 do anexo I da Diretiva (UE) 2022/2557, do trânsito rodoviário e das redes de abastecimento de água, gás, aquecimento e eletricidade, uma vez que a falha ou anomalia desses 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. Os componentes de segurança das infraestruturas críticas, incluindo as infraestruturas digitais críticas, são sistemas utilizados para proteger diretamente a integridade física das infraestruturas críticas ou a saúde e a segurança das pessoas e dos bens, mas que não são necessários para o funcionamento do sistema. A falha ou a anomalia desses componentes pode conduzir diretamente a riscos para a integridade física das infraestruturas críticas e, por conseguinte, a riscos para a saúde e a segurança das pessoas e dos bens. Os componentes destinados a serem utilizados exclusivamente para fins de cibersegurança não deverão ser considerados componentes de segurança. Os exemplos de componentes de segurança dessas infraestruturas críticas podem incluir sistemas de monitorização da pressão da água ou sistemas de controlo de alarmes de incêndio em centros de computação em nuvem.

(56) A implantação de sistemas de IA no domínio da educação é importante para promover a educação e a formação digitais de elevada qualidade e permitir que todos os aprendentes e professores adquiram e partilhem as aptidões e competências digitais necessárias, incluindo a literacia mediática e o pensamento crítico, a fim de participarem ativamente na economia, na sociedade e nos processos democráticos. Contudo, os sistemas de IA utilizados no domínio da educação ou da formação profissional, nomeadamente para determinar o acesso ou a admissão, para afetar pessoas a instituições ou a programas de ensino e de formação profissional em todos os níveis, para avaliar os resultados de aprendizagem das pessoas, para aferir o grau de ensino adequado para uma pessoa e influenciar de forma substancial o nível de ensino e formação que as pessoas receberão, ou a que serão capazes de aceder, ou para monitorizar e detetar comportamentos proibidos de estudantes durante os testes, deverão ser considerados sistemas de IA de risco elevado, uma vez que podem determinar o percurso educativo e profissional de uma pessoa e, como tal, pode afetar a capacidade dessa pessoa assegurar a subsistência. Se indevidamente concebidos e utilizados, estes sistemas podem ser particularmente intrusivos e violar o direito à educação e à formação, bem como o direito a não ser alvo de discriminação nem de perpetuação de padrões históricos de discriminação, por exemplo contra as mulheres, determinados grupos etários, pessoas com deficiência ou pessoas de uma determinada origem racial ou étnica ou orientação sexual.

(57) 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 pessoal, de tomada de decisões que afetem os termos da relação de trabalho, de promoção e cessação das relações contratuais de trabalho, de atribuição de tarefas com base em comportamentos individuais, traços ou características pessoais, e de controlo ou avaliação de pessoas no âmbito de relações contratuais de trabalho também deverão ser classificados como sendo de risco elevado, uma vez que podem ter um impacto significativo nas perspetivas de carreira, na subsistência dessas pessoas e nos direitos dos trabalhadores. O conceito de «relações contratuais de trabalho» deverá abranger de forma significativa os funcionários e as pessoas que prestam serviços por intermédio de plataformas a que se refere o programa de trabalho da Comissão para 2021. Ao longo do processo de recrutamento e na avaliação, promoção ou retenção de pessoal em relações contratuais de trabalho, esses sistemas podem perpetuar padrões históricos de discriminação, por exemplo, contra as mulheres, contra certos grupos etários, contra as pessoas com deficiência ou contra pessoas de uma determinada origem racial ou étnica ou orientação sexual. Os sistemas de IA utilizados para controlar o desempenho e o comportamento dessas pessoas podem ainda comprometer os seus direitos fundamentais à proteção de dados pessoais e à privacidade.

(58) 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 especial, as pessoas singulares que se candidatam a receber ou que recebem prestações e serviços de assistência pública essenciais de autoridades públicas, nomeadamente serviços de cuidados de saúde, prestações de segurança social, serviços sociais que prestam proteção em casos como maternidade, doença, acidentes de trabalho, dependência ou velhice e perda de emprego e assistência social e de habitação, dependem normalmente dessas prestações e serviços e estão numa posição vulnerável face às autoridades responsáveis. Caso sejam utilizados para determinar a concessão, recusa, redução, revogação ou recuperação dessas prestações e serviços pelas autoridades, nomeadamente para determinar se os beneficiários têm legítimo direito a essas prestações ou serviços, os sistemas de IA podem ter um impacto significativo na subsistência das pessoas e podem violar os seus direitos fundamentais, como o direito à proteção social, à não discriminação, à dignidade do ser humano ou à ação, pelo que deverão ser classificados como sendo de risco elevado. No entanto, o presente regulamento não deverá 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 acarretem um risco elevado para as pessoas coletivas e singulares.

Além disso, os sistemas de IA utilizados para avaliar a classificação de crédito ou a solvabilidade de pessoas singulares deverão 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 essas finalidades podem conduzir à discriminação entre pessoas ou grupos e podem perpetuar padrões históricos de discriminação, como em razão da origem étnica ou racial, do género, da deficiência, da idade ou da orientação sexual, ou podem criar novas formas de impacto discriminatório. No entanto, os sistemas de IA previstos pelo direito da União para efeitos de deteção de fraudes na oferta de serviços financeiros e para fins prudenciais com vista a calcular os requisitos de capital das instituições de crédito e das seguradoras não deverão ser considerados de risco elevado nos termos do presente regulamento. Além disso, os sistemas de IA concebidos com vista a serem utilizados para avaliação dos riscos e fixação de preços em relação a pessoas singulares para seguros de saúde e de vida também podem ter um impacto significativo na subsistência das pessoas e, se não forem devidamente concebidos, desenvolvidos e utilizados, podem infringir os seus direitos fundamentais e ter consequências graves para a vida e a saúde das pessoas, incluindo a exclusão financeira e a discriminação. Por último, os sistemas de IA utilizados para avaliar e classificar chamadas de emergência efetuadas por pessoas singulares ou para enviar ou estabelecer prioridades no envio de serviços de primeira resposta a emergências, nomeadamente pela polícia, bombeiros e assistência médica, bem como por sistemas de triagem de doentes para cuidados de saúde de emergência, também deverão ser classificados como sendo de risco elevado, uma vez que tomam decisões em situações bastante críticas que afetam a vida, a saúde e os bens das pessoas.

(59) Tendo em conta o papel e a responsabilidade das autoridades responsáveis pela aplicação da lei, as suas ações 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 outras repercussões negativas 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 desempenho, 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 selecionar pessoas de uma forma discriminatória, incorreta ou injusta. Além disso, o exercício de importantes direitos fundamentais processuais, como o direito à ação e a um tribunal imparcial, o direito à defesa e a presunção de inocência, pode ser prejudicado, em particular, se esses sistemas de IA não forem suficientemente transparentes, explicáveis e documentados. Como tal, é apropriado classificar como sendo de risco elevado, na medida em que a sua utilização seja permitida nos termos do direito da União e o direito nacional aplicáveis, vários sistemas de IA que se destinam a ser utilizados no contexto da aplicação da lei, no qual a exatidão, a fiabilidade e a transparência são particularmente importantes para evitar repercussões negativas, manter a confiança do público e assegurar a responsabilidade e vias de recurso eficazes.

Tendo em conta a natureza das atividades e os riscos associados às mesmas, esses sistemas de IA de risco elevado deverão incluir, em particular, sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei ou por instituições, órgãos ou organismos da União, ou em seu nome, em apoio das autoridades responsáveis pela aplicação da lei para avaliar o risco de uma pessoa singular vir a ser vítima de infrações penais, como polígrafos e instrumentos semelhantes, para avaliar a fiabilidade dos elementos de prova no decurso da investigação ou da repressão de infrações penais, e, na medida em que tal não seja proibido nos termos do presente regulamento, para avaliar o risco de uma pessoa singular cometer uma infração ou reincidência não apenas com base na definição de perfis de pessoas singulares ou na avaliação os traços e características da personalidade ou do comportamento criminal passado de pessoas singulares ou grupos, para a definição de perfis no decurso da deteção, investigação ou repressão de infrações penais. Os sistemas de IA especificamente concebidos para serem utilizados em processos administrativos por autoridades fiscais e aduaneiras, bem como por unidades de informação financeira que desempenhem funções administrativas de análise de informações nos termos do direito da União em matéria de combate ao branqueamento de capitais, não deverão ser classificados como sistemas de IA de risco elevado utilizados por autoridades responsáveis pela aplicação da lei para efeitos de prevenção, deteção, investigação e repressão de infrações penais. A utilização de ferramentas de IA pelas autoridades responsáveis pela aplicação da lei e por outras autoridades pertinentes não deverá tornar-se um fator de desigualdade nem de exclusão. Não se deverá descurar o impacto da utilização de ferramentas de IA nos direitos de defesa dos suspeitos, nomeadamente a dificuldade de obter informações significativas sobre o funcionamento desses sistemas e a dificuldade daí resultante de contestar os seus resultados em tribunal, em particular quando se trate de pessoas singulares sob investigação.

(60) 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, na medida em que a sua utilização seja permitida ao abrigo do direito da União e o direito nacional aplicáveis, é apropriado classificar como sendo de risco elevado os sistemas de IA concebidos para serem utilizados por autoridades públicas competentes, ou em seu nome, ou por instituições, órgãos ou organismos da União incumbidos de funções no domínio da gestão da migração, do asilo e do controlo das fronteiras, como polígrafos e instrumentos semelhantes, para avaliar determinados riscos colocados por pessoas singulares que entram no território de um Estado-Membro ou apresentam um pedido de visto ou asilo, para ajudar as autoridades públicas competentes na análise, incluindo a avaliação conexa da fiabilidade dos elementos de prova, dos pedidos de asilo, de visto e de autorização de residência e das queixas relacionadas, no que toca ao objetivo de estabelecer a elegibilidade das pessoas singulares que requerem determinado estatuto, para efeitos de deteção, reconhecimento ou identificação de pessoas singulares no contexto da gestão da migração, do asilo e do controlo das fronteiras, com exceção da verificação de documentos de viagem.

Os sistemas de IA no domínio da gestão da migração, do asilo e do controlo das fronteiras abrangidos pelo presente regulamento deverão cumprir os requisitos processuais pertinentes estabelecidos no Regulamento (CE) n.º 810/2009 do Parlamento Europeu e do Conselho[32], na Diretiva 2013/32/UE do Parlamento Europeu e do Conselho[33] e em outras disposições pertinentes do direito da União. A utilização de sistemas de IA na gestão da migração, do asilo e do controlo das fronteiras não deverá, em caso algum, ser utilizada pelos Estados-Membros nem pelas instituições, órgãos ou organismos da União como meio de contornar as suas obrigações internacionais nos termos da Convenção das Nações Unidas relativa ao Estatuto dos Refugiados, celebrada em Genebra em 28 de julho de 1951, com a redação que lhe foi dada pelo Protocolo de 31 de janeiro de 1967. Também não deverão, de modo algum, ser utilizados para violar o princípio da não repulsão nem para recusar vias legais seguras e eficazes de entrada no território da União, incluindo o direito à proteção internacional.

---

32 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).

33 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).

(61) Determinados sistemas de IA concebidos para a administração da justiça e os processos democráticos deverão ser classificados como sendo 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 sendo de risco elevado os sistemas de IA concebidos para serem utilizados por uma autoridade judiciária ou para, em seu nome, auxiliar autoridades judiciárias na investigação e interpretação de factos e do direito e na aplicação da lei a um conjunto específico de factos. Os sistemas de IA concebidos para serem utilizados por entidades de resolução alternativa de litígios para esses fins também deverão ser considerados de risco elevado quando os resultados dos procedimentos de resolução alternativa de litígios produzam efeitos jurídicos para as partes. A utilização de ferramentas de IA pode auxiliar o poder de tomada de decisão dos magistrados ou da independência judicial, mas não o deverá substituir, a decisão final tem de continuar a ser uma atividade humana. Contudo, a classificação de sistemas de IA como sendo de risco elevado não deverá 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 judiciais, documentos ou dados, comunicações entre pessoal ou tarefas administrativas.

(62) Sem prejuízo das regras previstas no Regulamento (UE) 2024/… do Parlamento Europeu e do Conselho[34+], e a fim de fazer face aos riscos quer de interferência externa indevida no direito de voto consagrado no artigo 39.º da Carta, quer de efeitos adversos na democracia e no Estado de direito, os sistemas de IA concebidos para serem utilizados para influenciar o resultado de uma eleição ou referendo, ou o comportamento eleitoral de pessoas singulares no exercício do seu direito de voto em eleições ou referendos, deverão ser classificados como sendo sistemas de IA de risco elevado, com exceção dos sistemas de IA a cujos resultados as pessoas singulares não estejam diretamente expostas, como os instrumentos utilizados para organizar, otimizar e estruturar campanhas políticas de um ponto de vista administrativo e logístico.

(63) A classificação de um sistema de IA como sendo de risco elevado por força do presente regulamento não deverá ser interpretada como uma indicação de que a utilização do sistema é 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 deverá 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 deverá ser entendido como um fundamento jurídico para o tratamento de dados pessoais, inclusive de categorias especiais de dados pessoais, se for caso disso, salvo disposição específica em contrário no presente regulamento.

---

34 Regulamento (UE) 2024/… do Parlamento Europeu e do Conselho de … sobre a transparência e o direcionamento da propaganda política (JO L…, ELI: …).

\+ JO: Inserir no texto o número do regulamento que consta do documento PE-CONS 90/23 (2021/0381(COD)) e completar a nota de rodapé correspondente.

(64) Para atenuar os riscos dos sistemas de IA de risco elevado colocados no mercado ou colocados em serviço e para assegurar um elevado nível de fiabilidade, deverão aplicar-se determinados requisitos obrigatórios aos sistemas de IA de risco elevado, tendo em conta a finalidade prevista e o contexto de utilização do sistema de IA e de acordo com o sistema de gestão de riscos a estabelecer pelo prestador. As medidas adotadas pelos prestadores para cumprirem os requisitos obrigatórios do presente regulamento deverão ter em conta o estado da arte geralmente reconhecido em matéria de IA e ser proporcionadas e eficazes para cumprir os objetivos do presente regulamento. Com base no novo regime jurídico, tal como clarificado na comunicação da Comissão intitulada «"Guia Azul" de 2022 sobre a aplicação das regras da UE em matéria de produtos», a regra geral é a de que mais do que um ato jurídico da legislação de harmonização da União pode ser aplicável a um produto, uma vez que a sua disponibilização ou colocação em serviço só podem ter lugar quando o produto cumprir toda a legislação de harmonização da União aplicável. Os perigos dos sistemas de IA abrangidos pelos requisitos do presente regulamento dizem respeito a aspetos diferentes da legislação de harmonização da União em vigor, pelo que os requisitos do presente regulamento complementarão o atual corpo de legislação de harmonização da União. Por exemplo, as máquinas ou os dispositivos médicos que incorporam um sistema de IA podem apresentar riscos não abrangidos pelos requisitos essenciais de saúde e segurança estabelecidos nas disposições pertinentes do direito harmonizado da União, uma vez que tal legislação setorial não aborda os riscos específicos dos sistemas de IA.

Tal implica a aplicação simultânea e complementar dos vários atos legislativos. A fim de assegurar a coerência e evitar encargos administrativos e custos desnecessários, os prestadores de um produto que contenha um ou mais sistemas de IA de risco elevado, aos quais se aplicam os requisitos do presente regulamento e da legislação de harmonização da União com base no novo regime jurídico e enumerados num anexo do presente regulamento, deverão ser flexíveis no que diz respeito às decisões operacionais sobre a forma otimizada de assegurar a conformidade de um produto que contenha um ou mais sistemas de IA com todos os requisitos aplicáveis dessa legislação harmonizada da União. Tal flexibilidade poderá significar, por exemplo, a decisão do prestador de integrar uma parte dos processos necessários de testagem e comunicação de informações e de informação e documentação exigidos pelo presente regulamento na documentação e nos procedimentos já existentes exigidos nos termos da legislação de harmonização da União, com base no novo regime jurídico e enumerado num anexo do presente regulamento. Tal não deverá de modo algum prejudicar a obrigação do prestador de cumprir todos os requisitos aplicáveis.

(65) O sistema de gestão de riscos deverá consistir num processo iterativo contínuo, que seja planeado e executado ao longo de todo o ciclo de vida de um sistema de IA de risco elevado. Esse processo deverá ter por objetivo identificar e atenuar os riscos pertinentes dos sistemas de IA para a saúde, a segurança e os direitos fundamentais. O sistema de gestão de riscos deverá ser revisto e atualizado regularmente, a fim de assegurar a sua eficácia contínua, bem como a justificação e documentação de quaisquer decisões e medidas significativas tomadas ao abrigo do presente regulamento. Este processo deverá assegurar que o prestador identifique riscos ou repercussões negativas e aplique medidas de atenuação dos riscos conhecidos e razoavelmente previsíveis dos sistemas de IA para a saúde, a segurança e os direitos fundamentais à luz das suas finalidades previstas e da sua utilização indevida razoavelmente previsível, incluindo os possíveis riscos decorrentes da interação entre o sistema de IA e o ambiente em que opera. O sistema de gestão de riscos deverá adotar as medidas de gestão dos riscos mais adequadas à luz do estado da arte no domínio da IA. Ao identificar as medidas de gestão dos riscos mais adequadas, o prestador deverá documentar e explicar as escolhas feitas e, se for caso disso, envolver peritos e partes interessadas externas. Ao identificar a utilização indevida razoavelmente previsível de sistemas de IA de risco elevado, o prestador deverá abranger as utilizações dos sistemas de IA que, embora não diretamente abrangidas pela finalidade prevista e indicadas nas instruções de utilização, possa, no entanto, razoavelmente esperar-se que resultem de um comportamento humano facilmente previsível no contexto das características específicas e da utilização de um sistema de IA. Quaisquer circunstâncias conhecidas ou previsíveis, relacionadas com a utilização do sistema de IA de risco elevado em conformidade com a sua finalidade prevista ou em condições de utilização indevida razoavelmente previsível, que possam causar riscos para a saúde e a segurança ou os direitos fundamentais deverão ser incluídas nas instruções de utilização que são disponibilizadas pelo prestador. O objetivo é assegurar que o responsável pela implantação esteja ciente delas e as tenha em conta ao utilizar o sistema de IA de risco elevado. A identificação e a aplicação de medidas de atenuação dos riscos em caso de utilização indevida previsível por força do presente regulamento não deverão exigir medidas de treino adicionais específicas para o sistema de IA de risco elevado por parte do prestador, a fim de as combater. No entanto, os prestadores são incentivados a considerar essas medidas de treino adicionais a fim de atenuarem as utilizações indevidas razoavelmente previsíveis, conforme necessário e adequado.

(66) Os sistemas de IA de risco elevado deverão estar sujeitos ao cumprimento de requisitos relativos à gestão de riscos, à qualidade e à pertinência dos conjuntos de dados utilizados, à documentação técnica e à manutenção de registos, à transparência e à prestação de informações aos responsáveis pela implantação, 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. Uma vez que não estão razoavelmente disponíveis outras medidas menos restritivas ao comércio, esses requisitos não constituem restrições injustificadas ao comércio.

(67) Os dados de elevada qualidade e o acesso a dados de elevada qualidade desempenham um papel essencial ao proporcionarem estrutura e garantirem 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 uma fonte de uma discriminação proibida pelo direito da União. Para garantir conjuntos de dados de treino, validação e testagem de elevada qualidade é necessário aplicar práticas adequadas de governação e gestão de dados. Os conjuntos de dados de treino, validação e testagem, incluindo os rótulos, deverão ser pertinentes, suficientemente representativos e, tanto quanto possível, isentos de erros e completos, tendo em conta a finalidade prevista do sistema. A fim de facilitar o cumprimento da legislação da União em matéria de proteção de dados, como o Regulamento (UE) 2016/679, as práticas de governação e de gestão de dados deverão incluir, no caso dos dados pessoais, a transparência sobre a finalidade inicial da recolha de dados. Os conjuntos de dados deverão também ter as propriedades estatísticas adequadas, nomeadamente no que respeita às pessoas ou grupos de pessoas nos quais o sistema de IA de risco elevado se destina a ser utilizado, com especial atenção para a atenuação de eventuais enviesamentos nos conjuntos de dados que sejam suscetíveis de afetar a saúde e a segurança das pessoas, afetar negativamente os direitos fundamentais ou conduzir a discriminações proibidas pelo direito da União, especialmente quando os resultados dos dados influenciam entradas para operações futuras («circuitos de realimentação»). Os enviesamentos podem, por exemplo, ser inerentes a conjuntos de dados de base, especialmente quando são usados ou gerados dados históricos ao serem aplicados os sistemas a situações reais.

Os resultados apresentados pelos sistemas de IA poderão ser influenciados por enviesamentos inerentes que tendem a aumentar gradualmente, e, desse modo, a perpetuar e a ampliar a discriminação existente, em particular de pessoas pertencentes a grupos vulneráveis, nomeadamente de grupos raciais ou étnicos. O requisito de os conjuntos de dados serem o mais completos possível e isentos de erros não deverá afetar a utilização de técnicas de preservação da privacidade no contexto do desenvolvimento e testagem de sistemas de IA. Em especial, os conjuntos de dados deverão ter em conta, na medida do exigido face à sua finalidade prevista, as funcionalidades, as características ou os elementos que são específicos do cenário geográfico, contextual, comportamental ou funcional no qual o sistema de IA se destina a ser utilizado. Os requisitos relacionados com a governação dos dados podem ser cumpridos recorrendo a terceiros que ofereçam serviços de conformidade certificados, incluindo a verificação da governação dos dados, da integridade dos conjuntos de dados e das práticas de treino, validação e testagem de dados, desde que seja assegurado o cumprimento dos requisitos em matéria de dados do presente regulamento.

(68) No contexto do desenvolvimento e avaliação de sistemas de IA de risco elevado, determinados intervenientes, como prestadores, organismos notificados e outras entidades pertinentes, como polos de inovação digital, instalações de testagem e experimentação e investigadores, deverão ter a possibilidade de aceder a conjuntos de dados de elevada qualidade dentro das áreas de intervenção desses intervenientes 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 a testagem 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 IA com base nesses conjuntos de dados, de forma respeitadora da privacidade, segura, atempada, transparente e digna de confiança, 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 a disponibilização de dados de elevada qualidade para fins de treino, validação e testagem de sistemas de IA.

(69) O direito à privacidade e à proteção de dados pessoais tem de ser garantido ao longo de todo o ciclo de vida do sistema de IA. A este respeito, os princípios da minimização dos dados e da proteção de dados desde a conceção e por norma, tal como estabelecidos na legislação da União em matéria de proteção de dados, são aplicáveis quando se realiza o tratamento de dados. As medidas tomadas pelos prestadores para assegurar o cumprimento desses princípios podem incluir não só a anonimização e a cifragem, mas também a utilização de tecnologias que permitam a introdução de algoritmos nos dados e o treino dos sistemas de IA sem a transmissão entre as partes ou a cópia dos próprios dados em bruto ou estruturados, sem prejuízo dos requisitos em matéria de governação de dados previstos no presente regulamento.

(70) A fim de proteger o direito de terceiros da discriminação que possa resultar do enviesamento nos sistemas de IA, os prestadores deverão, a título excecional, na medida do estritamente necessário para assegurar a deteção e a correção de enviesamentos em relação aos sistemas de IA de risco elevado, sob reserva de salvaguardas adequadas dos direitos e liberdades fundamentais das pessoas singulares e na sequência da aplicação de todas as condições aplicáveis estabelecidas no presente regulamento, para além das condições estabelecidas nos Regulamentos (UE) 2016/679 e (UE) 2018/1725 e na Diretiva (UE) 2016/680, ser capazes de tratar também categorias especiais de dados pessoais, por razões de interesse público substancial, na aceção do artigo 9.º, n.º 2, alínea g), do Regulamento (UE) 2016/679 e do artigo 10.º, n.º 2, alínea g), do Regulamento (UE) 2018/1725.

(71) Dispor de informações compreensíveis sobre a forma como os sistemas de IA de risco elevado foram desenvolvidos e sobre o seu desempenho ao longo da sua vida útil é essencial para permitir a rastreabilidade desses sistemas, verificar o cumprimento dos requisitos previstos no presente regulamento, bem como o acompanhamento das suas operações e o acompanhamento pós-comercialização. Para tal, é necessário manter registos e disponibilizar documentação técnica com as informações necessárias para avaliar se o sistema de IA cumpre os requisitos aplicáveis e facilita o acompanhamento pós-comercialização. Essas informações deverão incluir as características gerais, as capacidades e as limitações do sistema, os algoritmos, os dados e os processos de treino, testagem e validação utilizados, bem como a documentação relativa ao sistema de gestão de riscos aplicado, e ser redigidas de forma clara e compreensiva. A documentação técnica deverá ser mantida devidamente atualizada ao longo de toda a vida útil do sistema de IA. Além disso, os sistemas de IA de risco elevado deverão permitir tecnicamente o registo automático de eventos, por meio de registos, durante a vida útil do sistema.

(72) A fim de dar resposta às preocupações relacionadas com a opacidade e a complexidade de determinados sistemas de IA e ajudar os responsáveis pela implantação a cumprir as obrigações que lhes incumbem por força do presente regulamento, deverá ser exigida transparência aos sistemas de IA de risco elevado antes de serem colocados no mercado ou colocados em serviço. Os sistemas de IA de risco elevado deverão ser concebidos de forma a permitir aos responsáveis pela implantação compreender a forma como funciona o sistema de IA, avaliar a sua funcionalidade e compreender os seus pontos fortes e limitações. Os sistemas de IA de risco elevado deverão ser acompanhados de informações adequadas sob a forma de instruções de utilização. Tais informações deverão incluir as características, capacidades e limitações do desempenho do sistema de IA. Esses elementos abrangerão informações sobre eventuais circunstâncias conhecidas e previsíveis relacionadas com a utilização do sistema de IA de risco elevado, incluindo ações do responsável pela implantação que possam influenciar o comportamento e o desempenho do sistema, ao abrigo das quais o sistema de IA pode conduzir a riscos para a saúde, a segurança e os direitos fundamentais, sobre as alterações que foram predeterminadas e avaliadas para efeitos de conformidade pelo prestador e sobre as medidas de supervisão humana pertinentes, incluindo as medidas destinadas a facilitar a interpretação dos resultados do sistema de IA pelos responsáveis pela implantação. A transparência, incluindo as instruções de utilização que as acompanham, deverá ajudar os responsáveis pela implantação na utilização do sistema e apoiar a sua tomada de decisões informadas. Entre outros, os responsáveis pela implantação deverão estar em melhor posição para fazer a escolha correta do sistema que tencionam utilizar à luz das obrigações que lhes são aplicáveis, ser instruídos sobre as utilizações previstas e proibidas e utilizar o sistema de IA de forma correta e conforme adequado. A fim de melhorar a legibilidade e a acessibilidade das informações incluídas nas instruções de utilização, deverão ser incluídos, se for caso disso, exemplos ilustrativos, por exemplo, sobre as limitações e as utilizações previstas e proibidas do sistema de IA. Os prestadores deverão assegurar que toda a documentação, incluindo as instruções de utilização, contém informações significativas, abrangentes, acessíveis e compreensíveis, tendo em conta as necessidades e os conhecimentos previsíveis dos responsáveis pela implantação visados. As instruções de utilização deverão ser disponibilizadas numa língua que possa ser facilmente compreendida pelos responsáveis pela implantação visados, conforme determinado pelo Estado-Membro em causa.

(73) Os sistemas de IA de risco elevado deverão ser concebidos e desenvolvidos de maneira que pessoas singulares possam supervisionar o seu funcionamento, assegurar que são utilizados como previsto e que os seus impactos são abordados ao longo do ciclo de vida do sistema. Para o efeito, o prestador do sistema deverá 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 deverão garantir que o sistema esteja sujeito a restrições operacionais integradas impossíveis de serem anuladas pelo próprio sistema e responda ao operador humano, bem como que as pessoas singulares a quem seja atribuída a supervisão humana tenham as competências, a formação e a autoridade necessárias para desempenhar essa função. É igualmente essencial, conforme adequado, assegurar que os sistemas de IA de risco elevado incluam mecanismos para orientar e informar uma pessoa singular incumbida da supervisão humana de forma a que tome decisões informadas sobre se, quando e como intervir, a fim de evitar consequências negativas ou riscos, ou a que pare o sistema se não funcionar como previsto. Tendo em conta as consequências significativas para as pessoas em caso de uma correspondência incorreta por determinados sistemas de identificação biométrica, é conveniente prever um requisito reforçado de supervisão humana para esses sistemas, de modo a que o responsável pela implantação não possa tomar qualquer medida ou decisão com base na identificação resultante do sistema, a menos que tal tenha sido verificado e confirmado separadamente por, pelo menos, duas pessoas singulares. Essas pessoas podem pertencer a uma ou mais entidades e incluir a pessoa que opera ou utiliza o sistema. Este requisito não deverá implicar encargos ou atrasos desnecessários e pode ser suficiente que as verificações separadas efetuadas pelas diferentes pessoas sejam automaticamente gravadas nos registos gerados pelo sistema. Tendo em conta as especificidades dos domínios da aplicação da lei, da migração, do controlo das fronteiras e do asilo, este requisito não deverá aplicar-se nos casos em que o direito da União ou o direito nacional considere que a aplicação desse requisito é desproporcionada.

(74) Os sistemas de IA de risco elevado deverão ter um desempenho coerente ao longo de todo o seu ciclo de vida e apresentar um nível adequado de exatidão, solidez e cibersegurança, à luz da finalidade prevista e de acordo com o estado da arte geralmente reconhecido. A Comissão e as organizações e partes interessadas pertinentes são incentivadas a ter em devida consideração a atenuação dos riscos e os impactos negativos do sistema de IA. O nível esperado dos parâmetros de desempenho deverá vir declarado nas instruções de utilização que o acompanham. Os prestadores são instados a comunicar essas informações aos responsáveis pela implantação de uma forma clara e facilmente compreensível, sem mal-entendidos nem declarações enganosas. O direito da União em matéria de metrologia legal, incluindo as Diretivas 2014/31/UE[35] e 2014/32/UE[36] do Parlamento Europeu e do Conselho, visa garantir a exatidão das medições e contribuir para a transparência e a lealdade das transações comerciais. Nesse contexto, em cooperação com as partes interessadas e a organização pertinentes, como as autoridades responsáveis pela metrologia e pela avaliação comparativa, a Comissão deverá incentivar, se for caso disso, o desenvolvimento de parâmetros de referência e metodologias de medição para os sistemas de IA. Ao fazê-lo, a Comissão deverá tomar nota e colaborar com os parceiros internacionais que trabalham em metrologia e em indicadores de medição pertinentes relacionados com a IA.

---

35 Diretiva 2014/31/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos sob pressão no mercado (JO L 96 de 29.3.2014, p. 107).

36 Diretiva 2014/32/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização no mercado de equipamentos de medição (JO L 096 de 29.3.2014, p. 149).

(75) A solidez técnica é um requisito essencial dos sistemas de IA de risco elevado. Esses sistemas deverão ser resistentes a comportamentos prejudiciais ou indesejáveis que possam resultar de limitações dentro dos sistemas ou do ambiente em que os sistemas operam (por exemplo, erros, falhas, incoerências, situações inesperadas). Por conseguinte, deverão ser tomadas medidas técnicas e organizativas para assegurar a solidez dos sistemas de IA de risco elevado, por exemplo através da conceção e do desenvolvimento de soluções técnicas adequadas para prevenir ou minimizar comportamentos nocivos ou indesejáveis. Essa solução técnica pode incluir, por exemplo, mecanismos que permitam ao sistema interromper o seu funcionamento de forma segura (planos de segurança à prova de falhas) caso se verifiquem determinadas anomalias ou caso o funcionamento ocorra fora de certos limites predeterminados. 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.

(76) 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 de por em causa as suas propriedades de segurança. Os ciberataques contra sistemas de IA podem tirar partido de ativos específicos de IA, como os conjuntos de dados de treino (p. ex., contaminação de dados) ou os modelos treinados (p. ex., ataques antagónicos ou inferência de membros), 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 prestadores de sistemas de IA de risco elevado deverão tomar medidas adequadas, como os controlos de segurança, tendo ainda em devida conta a infraestrutura de TIC subjacente.

(77) Sem prejuízo dos requisitos relacionados com a solidez e a exatidão estabelecidos no presente regulamento, os sistema de IA de risco elevado abrangidos pelo âmbito de aplicação de um regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais, nos termos desse regulamento, podem demonstrar a conformidade com o requisito de cibersegurança do presente regulamento ao cumprirem os requisitos essenciais de cibersegurança estabelecidos nesse regulamento. Quando os sistemas de IA de risco elevado cumprem os requisitos essenciais de um regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais, deverão ser considerados conformes com os requisitos de cibersegurança estabelecidos no presente regulamento, desde que o cumprimento desses requisitos seja demonstrado na declaração UE de conformidade ou em partes da mesma emitida nos termos desse regulamento. Para o efeito, a avaliação dos riscos de cibersegurança associados a um produto com elementos digitais classificado como sistema de IA de risco elevado nos termos do presente regulamento, realizada ao abrigo de um regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais, deverá ter em conta os riscos para a ciberresiliência de um sistema de IA no que diz respeito às tentativas de terceiros não autorizados de alterar a sua utilização, comportamento ou desempenho, incluindo vulnerabilidades específicas da IA, como a contaminação de dados ou ataques antagónicos, bem como os riscos pertinentes para os direitos fundamentais, tal como exigido pelo presente regulamento.

(78) O procedimento de avaliação da conformidade previsto no presente regulamento deverá aplicar-se aos requisitos essenciais de cibersegurança de um produto com elementos digitais abrangido por um Regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e classificado como sistema de IA de risco elevado nos termos do presente regulamento. No entanto, esta regra não deverá resultar na redução do nível de garantia necessário para os produtos críticos com elementos digitais abrangidos por um regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais. Por conseguinte, em derrogação desta regra, os sistemas de IA de risco elevado abrangidos pelo âmbito de aplicação do presente regulamento e que também são qualificados como produtos importantes e críticos com elementos digitais nos termos de um regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais, e aos quais se aplica o procedimento de avaliação da conformidade baseado no controlo interno referido num anexo do presente regulamento, são sujeitos às disposições em matéria de avaliação da conformidade de um regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais, no que diz respeito aos requisitos essenciais em matéria de cibersegurança desse regulamento. Neste caso, em relação a todos os outros aspetos abrangidos pelo presente regulamento, deverão aplicar-se as respetivas disposições em matéria de avaliação da conformidade com base no controlo interno estabelecidas num anexo do presente regulamento. Com base nos conhecimentos e competências especializados da ENISA sobre a política de cibersegurança e as funções atribuídas à ENISA nos termos do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[37], a Comissão Europeia deverá cooperar com a ENISA em questões relacionadas com a cibersegurança dos sistemas de IA.

---

[37] 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. 15).

(79) É apropriado que uma pessoa singular ou coletiva específica, identificada como «prestador», 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.

(80) Enquanto signatários da Convenção das Nações Unidas sobre os Direitos das Pessoas com Deficiência, a União e os seus Estados-Membros estão legalmente obrigados a proteger as pessoas com deficiência contra a discriminação e a promover a sua igualdade, a assegurar que as pessoas com deficiência gozem da mesma igualdade de acesso que outros às tecnologias e sistemas de informação e comunicação e a assegurar o respeito pela privacidade das pessoas com deficiência. Tendo em conta a crescente importância e utilização de sistemas de IA, a aplicação dos princípios de conceção universal a todas as novas tecnologias e serviços deverá garantir o acesso pleno e equitativo de todas as pessoas potencialmente afetadas pelas tecnologias de IA ou que utilizem essas tecnologias, incluindo as pessoas com deficiência, de uma forma que tenha plenamente em conta a sua inerente dignidade e diversidade. Por conseguinte, é essencial que os prestadores assegurem a plena conformidade com os requisitos de acessibilidade, incluindo a Diretiva (UE) 2016/2102 do Parlamento Europeu e do Conselho[38] e a Diretiva (UE) 2019/882. Os prestadores deverão assegurar o cumprimento destes requisitos desde a conceção. Por conseguinte, as medidas necessárias deverão ser integradas, tanto quanto possível, na conceção do sistema de IA de risco elevado.

---

[38] Diretiva (UE) 2016/2102 do Parlamento Europeu e do Conselho, de 26 de outubro de 2016, relativa à acessibilidade dos sítios web e das aplicações móveis de organismos do setor público (JO L 327 de 2.12.2016, p. 1).

(81) O prestador deverá 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 sólido de acompanhamento pós-comercialização. Os prestadores de sistemas de IA de risco elevado sujeitos a obrigações relativas aos sistemas de gestão da qualidade nos termos do direito setorial aplicável da União deverão ter a possibilidade de incluir os elementos do sistema de gestão da qualidade previstos no presente regulamento como parte do sistema de gestão da qualidade existente previsto nesse outro direito setorial da União. A complementaridade entre o presente regulamento e o direito setorial da União em vigor deverá também ser tida em conta nas futuras atividades de normalização ou orientações adotadas pela Comissão. 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.

(82) 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 prestar 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, os prestadores estabelecidos em países terceiros deverão, através de mandato escrito, designar um mandatário estabelecido na União. O mandatário desempenha um papel central ao garantir a conformidade dos sistemas de IA de risco elevado colocados no mercado ou colocados em serviço na União por esses prestadores que não estão estabelecidos na União e ao atuar como pessoa de contacto desses prestadores estabelecida na União.

(83) Tendo em conta a natureza e a complexidade da cadeia de valor dos sistemas de IA e em consonância com o novo regime jurídico, é essencial garantir a segurança jurídica e facilitar o cumprimento do presente regulamento. Por conseguinte, é necessário clarificar o papel e as obrigações específicas dos operadores pertinentes ao longo dessa cadeia de valor, como os importadores e os distribuidores, que podem contribuir para o desenvolvimento de sistemas de IA. Em determinadas situações, esses operadores poderão desempenhar mais do que uma função ao mesmo tempo, pelo que deverão cumprir cumulativamente todas as obrigações relevantes associadas a essas funções. Por exemplo, um operador pode atuar simultaneamente como distribuidor e importador.

(84) A fim de garantir a segurança jurídica, é necessário tornar claro que, em determinadas condições específicas, qualquer distribuidor, importador, responsável pela implantação ou outro terceiro deverá ser considerado prestador de um sistema de IA de risco elevado e, por conseguinte, deverá assumir todas as obrigações pertinentes. Tal será o caso se essa entidade puser o seu nome ou marca num sistema de IA de risco elevado já colocado no mercado ou colocado em serviço, sem prejuízo de disposições contratuais que estabeleçam que as obrigações são atribuídas de outro modo. Tal seria também o caso se essa entidade efetuar uma modificação substancial de um sistema de IA de risco elevado que já tenha sido colocado no mercado ou já tenha sido colocado em serviço de forma a que continue a ser um sistema de IA de risco elevado nos termos do presente regulamento, ou se alterar a finalidade prevista de um sistema de IA, incluindo um sistema de IA de finalidade geral, que não tenha sido classificado como sendo de risco elevado e já tenha sido colocado no mercado ou colocado em serviço, de forma a que o sistema de IA se torne um sistema de IA de risco elevado nos termos do presente regulamento. Essas disposições deverão aplicar-se sem prejuízo das disposições mais específicas estabelecidas em determinada legislação de harmonização da União com base no novo regime jurídico, conjuntamente com o presente regulamento. Por exemplo, o artigo 16.º, n.º 2, do Regulamento (UE) 2017/745, que estabelece que determinadas alterações não deverão ser consideradas alterações de um dispositivo suscetíveis de afetar a sua conformidade com os requisitos aplicáveis, deverá continuar a aplicar-se aos sistemas de IA de risco elevado que sejam dispositivos médicos na aceção do referido regulamento.

(85) Sistemas de IA de finalidade geral podem ser utilizados por si próprios como sistemas de IA de risco elevado ou ser componentes de outros sistemas de IA de risco elevado. Por conseguinte, devido à sua natureza específica e a fim de assegurar uma partilha equitativa de responsabilidades ao longo da cadeia de valor da IA, os prestadores desses sistemas deverão, independentemente de poderem ser utilizados como sistemas de IA de risco elevado enquanto tal por outros prestadores ou como componentes de sistemas de IA de risco elevado, e salvo disposição em contrário no presente regulamento, deverão colaborar estreitamente com os prestadores dos sistemas de IA de risco elevado relevantes, a fim de permitir a sua conformidade com as obrigações pertinentes previstas no presente regulamento e com as autoridades competentes criadas nos termos do presente regulamento.

(86) Se, nas condições estabelecidas no presente regulamento, o prestador que colocou inicialmente o sistema de IA no mercado ou o colocou em serviço deixar de ser considerado prestador para efeitos do presente regulamento, e se não tiver excluído expressamente a mudança do sistema de IA para um sistema de IA de risco elevado, o primeiro prestador deverá, no entanto, cooperar estreitamente e disponibilizar as informações necessárias e prestar o acesso técnico razoavelmente esperado e outra assistência necessária para o cumprimento das obrigações estabelecidas no presente regulamento, em especial no que diz respeito ao cumprimento da avaliação da conformidade dos sistemas de IA de risco elevado.

(87) Além disso, caso um sistema de IA de risco elevado que seja um componente de segurança de um produto abrangido pelo âmbito de aplicação da legislação de harmonização da União com base no novo regime jurídico não seja colocado no mercado ou colocado em serviço independentemente desse produto, o fabricante do produto, conforme definido na referida legislação deverá cumprir as obrigações dos prestadores previstas no presente regulamento e deverá, nomeadamente, assegurar que o sistema de IA integrado no produto final cumpre os requisitos do presente regulamento.

(88) Na cadeia de valor da IA, várias entidades disponibilizam frequentemente sistemas de IA, ferramentas e serviços, mas também componentes ou processos que são incorporados pelo prestador no sistema de IA com vários objetivos, nomeadamente o treino de modelos, a reciclagem do treino de modelos, a testagem e a avaliação de modelos, a integração em software ou outros aspetos do desenvolvimento de modelos. Essas entidades desempenham um papel importante na cadeia de valor para com o prestador do sistema de IA de risco elevado no qual os seus sistemas de IA, ferramentas, serviços, componentes ou processos estão integrados, e deverão facultar a esse prestador, mediante acordo escrito, as informações, capacidades, acesso técnico e demais assistência necessários com base no estado da arte geralmente reconhecido, a fim de permitir que o prestador cumpra plenamente as obrigações estabelecidas no presente regulamento, sem comprometer os seus próprios direitos de propriedade intelectual ou segredos comerciais.

(89) Os terceiros que tornam acessíveis ao público ferramentas, serviços, processos ou componentes de IA que não sejam modelos de IA de finalidade geral não deverão ser obrigados a cumprir requisitos que visem as responsabilidades ao longo da cadeia de valor da IA, em especial para com o prestador que os utilizou ou os integrou, quando essas ferramentas, serviços, processos ou componentes de IA são disponibilizados ao abrigo de uma licença gratuita e aberta. Os criadores de ferramentas, serviços, processos ou componentes de IA gratuitos e de fonte aberta que não sejam modelos de IA de finalidade geral deverão ser incentivados a aplicar práticas de documentação amplamente adotadas, como modelos de cartões e folhas de dados, como forma de acelerar a partilha de informações ao longo da cadeia de valor da IA, permitindo a promoção de sistemas de IA de confiança na União.

(90) A Comissão poderá desenvolver e recomendar modelos voluntários de cláusulas contratuais entre prestadores de sistemas de IA de risco elevado e terceiros que disponibilizem ferramentas, serviços, componentes ou processos utilizados ou integrados em sistemas de IA de risco elevado, a fim de facilitar a cooperação ao longo da cadeia de valor. Ao elaborar modelos de cláusulas contratuais voluntárias, a Comissão deverá também ter em conta eventuais requisitos contratuais aplicáveis em setores ou casos comerciais específicos.

(91) 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 responsáveis pela implantação. Em particular, os responsáveis pela implantação deverão tomar medidas técnicas e organizacionais adequadas para assegurar que utilizam os sistemas de IA de risco elevado de acordo com as instruções de utilização e deverão ser equacionadas outras obrigações relativas ao controlo do funcionamento dos sistemas de IA e à manutenção de registos, se for caso disso. Além disso, os responsáveis pela implantação deverão assegurar que as pessoas encarregadas de aplicar as instruções de utilização e de supervisão humana, tal como estabelecido no presente regulamento, têm as competências necessárias, em especial um nível adequado de literacia, formação e autoridade no domínio da IA para desempenhar adequadamente essas funções. Essas obrigações não deverão prejudicar outras obrigações do responsável pela implantação em relação a sistemas de IA de risco elevado nos termos do direito da União ou do direito nacional.

(92) O presente regulamento não prejudica a obrigação de os empregadores informarem ou de informarem e consultarem os trabalhadores ou os seus representantes, nos termos do direito e das práticas da União ou nacionais, incluindo a Diretiva 2002/14/CE do Parlamento Europeu e do Conselho[39], sobre as decisões de colocação em serviço ou de utilização de sistemas de IA. Continua a ser necessário garantir a informação dos trabalhadores e dos seus representantes sobre a implantação prevista de sistemas de IA de risco elevado no local de trabalho quando não estiverem cumpridas as condições para essas obrigações de informação ou de informação e consulta previstas noutros instrumentos jurídicos. Além disso, esse direito de informação é acessório e necessário ao objetivo de proteção dos direitos fundamentais subjacente ao presente regulamento. Por conseguinte, o presente regulamento deverá estabelecer um requisito de informação para esse efeito, sem afetar os direitos existentes dos trabalhadores.

---

[39] Diretiva 2002/14/CE do Parlamento Europeu e do Conselho, de 11 de março de 2002, que estabelece um quadro geral relativo à informação e à consulta dos trabalhadores na Comunidade Europeia (JO L 80 de 23.3.2002, p. 29).

(93) Ainda que os riscos relacionados com os sistemas de IA possam resultar da forma como esses sistemas são concebidos, tais riscos também podem decorrer da forma como os sistemas de IA são utilizados. Os responsáveis pela implantação de sistemas de IA de risco elevado desempenham, por conseguinte, um papel fundamental na garantia da proteção dos direitos fundamentais, complementando as obrigações do prestador aquando do desenvolvimento do sistema de IA. Os responsáveis pela implantação estão em melhor posição para entender de que forma o sistema de IA de risco elevado será utilizado em concreto, pelo que, graças a um conhecimento mais preciso do contexto de utilização, das pessoas ou grupos de pessoas suscetíveis de serem afetados, incluindo os grupos vulneráveis, conseguem identificar potenciais riscos significativos que não foram previstos na fase de desenvolvimento. Os responsáveis pela implantação de sistemas de IA de risco elevado enumerados num anexo do presente regulamento também desempenham um papel crítico na informação de pessoas singulares e deverão, quando tomam decisões ou ajudam a tomar decisões relacionadas com pessoas singulares, conforme o caso, informar as pessoas singulares de que estão sujeitas à utilização do sistema de IA de risco elevado. Essas informações deverão incluir a finalidade prevista e o tipo de decisões que toma. O responsável pela implantação deverá também informar as pessoas singulares do seu direito à explicação a que se refere o presente regulamento. No que diz respeito aos sistemas de IA de risco elevado utilizados para fins de aplicação da lei, essa obrigação deverá ser aplicada em conformidade com o artigo 13.º da Diretiva (UE) 2016/680.

(94) Qualquer tratamento de dados biométricos envolvido na utilização de sistemas de IA destinados à identificação biométrica para efeitos de aplicação da lei tem de cumprir o disposto no artigo 10.º da Diretiva (UE) 2016/680, segundo o qual tal tratamento só é autorizado se for estritamente necessário, se estiver sujeito a garantias adequadas dos direitos e liberdades do titular dos dados e se for autorizado pelo direito da União ou de um Estado-Membro. Essa utilização, quando autorizada, também tem de respeitar os princípios estabelecidos no artigo 4.º, n.º 1, da Diretiva (UE) 2016/680, nomeadamente a licitude, a lealdade e a transparência, a limitação da finalidade, a exatidão e a limitação da conservação.

(95) Sem prejuízo do direito da União aplicável, nomeadamente do Regulamento (UE) 2016/679 e da Diretiva (UE) 2016/680, tendo em conta a natureza intrusiva dos sistemas de identificação biométrica à distância em diferido, a utilização de sistemas de identificação biométrica à distância em diferido deverá estar sujeita a salvaguardas. Os sistemas de identificação biométrica à distância em diferido deverão ser sempre utilizados de uma forma proporcionada, legítima e estritamente necessária e, por conseguinte, orientada, em termos das pessoas a identificar, da localização, do âmbito temporal e com base num conjunto de dados fechados de imagens vídeo captadas licitamente. Em qualquer caso, os sistemas de identificação biométrica à distância em diferido não deverão ser utilizados no âmbito da aplicação da lei para conduzir a uma vigilância indiscriminada. As condições para a identificação biométrica à distância em diferido não deverão, em caso algum, constituir uma base para contornar as condições da proibição e as exceções rigorosas aplicáveis à identificação biométrica à distância em tempo real.

(96) A fim de assegurar de forma eficiente a proteção dos direitos fundamentais, os responsáveis pela implantação de sistemas de IA de risco elevado que sejam organismos de direito público, ou as entidades privadas que prestam serviços públicos e os responsáveis pela implantação de determinados sistemas de IA de risco elevado enumerados num anexo do presente regulamento, como as entidades bancárias ou seguradoras, deverão realizar uma avaliação do seu impacto nos direitos fundamentais antes da sua colocação em serviço. Os serviços de natureza pública importantes para as pessoas também podem ser prestados por entidades privadas. As entidades privadas que prestam esses serviços públicos estão ligados a funções de interesse público, designadamente nos domínios da educação, dos cuidados de saúde, dos serviços sociais, da habitação e da administração da justiça. O objetivo da avaliação do impacto nos direitos fundamentais é que o responsável pela implantação identifique os riscos específicos para os direitos das pessoas ou grupos de pessoas suscetíveis de serem afetados e identifique as medidas a tomar em caso de concretização desses riscos. A avaliação de impacto deverá ser efetuada antes da implantação do sistema de IA de risco elevado e deverá ser atualizada quando o responsável pela implantação considerar que qualquer um dos fatores pertinentes se alterou. A avaliação de impacto deverá identificar os processos pertinentes do responsável pela implantação em que o sistema de IA de risco elevado será utilizado em conformidade com a sua finalidade prevista e deverá incluir uma descrição do período e da frequência em que o sistema se destina a ser utilizado, bem como de categorias específicas de pessoas singulares e grupos suscetíveis de serem afetados no contexto específico de utilização.

A avaliação deverá também incluir a identificação de riscos específicos de danos suscetíveis de ter impacto nos direitos fundamentais dessas pessoas ou grupos. Ao realizar esta avaliação, o responsável pela implantação deverá ter em conta as informações pertinentes para uma avaliação adequada do impacto, incluindo, mas não exclusivamente, as informações facultadas pelo prestador do sistema de IA de risco elevado nas instruções de utilização. À luz dos riscos identificados, os responsáveis pela implantação deverão determinar as medidas a tomar em caso de concretização desses riscos, incluindo, por exemplo, mecanismos de governação nesse contexto específico de utilização, tais como mecanismos de supervisão humana de acordo com as instruções de utilização ou procedimentos de tratamento de queixas e de reparação, uma vez que poderão ser fundamentais para atenuar os riscos para os direitos fundamentais em casos concretos de utilização. Após a realização dessa avaliação de impacto, o responsável pela implantação deverá notificar a autoridade de fiscalização do mercado competente. Se for caso disso, para recolher as informações pertinentes necessárias para realizar a avaliação de impacto, os responsáveis pela implantação de sistemas de IA de risco elevado, em especial quando os sistemas de IA são utilizados no setor público, poderão implicar as partes interessadas pertinentes, incluindo os representantes de grupos de pessoas suscetíveis de serem afetadas pelo sistema de IA, peritos independentes e organizações da sociedade civil, na realização dessas avaliações de impacto e na conceção de medidas a tomar em caso de concretização dos riscos. O Serviço Europeu para a Inteligência Artificial («Serviço para a IA») deverá desenvolver um modelo de questionário, a fim de facilitar a conformidade e reduzir os encargos administrativos para os responsáveis pela implantação.

(97) O conceito de modelos de IA de finalidade geral deverá ser claramente definido e distinguido do conceito de sistemas de IA, a fim de proporcionar segurança jurídica. A definição deverá basear-se nas principais características funcionais de um modelo de IA de finalidade geral, em especial na generalidade e na capacidade de desempenhar com competência uma vasta gama de funções distintas. Estes modelos são normalmente treinados com grandes quantidades de dados, através de vários métodos, como a aprendizagem autossupervisionada, não supervisionada ou por reforço. Os modelos de IA de finalidade geral podem ser colocados no mercado de várias formas, nomeadamente através de bibliotecas, interfaces de programação de aplicações, para descarregamento direto ou como cópia física. Estes modelos podem ser alterados ou aperfeiçoados em novos modelos. Embora os modelos de IA sejam componentes essenciais dos sistemas de IA, não constituem, por si só, sistemas de IA. Os modelos de IA exigem a adição de outros componentes, como, por exemplo, uma interface de utilizador, para se tornarem sistemas de IA. Os modelos de IA são tipicamente integrados e fazem parte integrante dos sistemas de IA. O presente regulamento estabelece regras específicas para os modelos de IA de finalidade geral e para os modelos de IA de finalidade geral que apresentam riscos sistémicos, as quais se deverão aplicar também quando estes modelos são integrados ou fazem parte integrante de um sistema de IA. Deverá entender-se que as obrigações dos prestadores de modelos de IA de finalidade geral deverão aplicar-se assim que os modelos de IA de finalidade geral sejam colocados no mercado.

Quando o prestador de um modelo de IA de finalidade geral integra um modelo próprio no seu próprio sistema de IA que é disponibilizado no mercado ou colocado em serviço, esse modelo deverá ser considerado colocado no mercado e, por conseguinte, as obrigações previstas no presente regulamento para os modelos deverão continuar a aplicar-se para além das obrigações aplicáveis aos sistemas de IA. As obrigações estabelecidas para os modelos não deverão, em caso algum, aplicar-se quando um modelo próprio for utilizado para processos puramente internos não essenciais para disponibilizar um produto ou um serviço a terceiros e os direitos das pessoas singulares não forem afetados. Tendo em conta os seus potenciais efeitos significativamente negativos, os modelos de IA de finalidade geral com risco sistémico deverão estar sempre sujeitos às obrigações pertinentes nos termos do presente regulamento. A definição não deverá abranger os modelos de IA utilizados antes da sua colocação no mercado exclusivamente para fins de atividades de investigação, desenvolvimento e prototipagem. Tal não prejudica a obrigação de cumprir o presente regulamento quando, na sequência dessas atividades, um modelo for colocado no mercado.

(98) Embora a generalidade de um modelo possa, entre outros critérios, ser também determinada por vários parâmetros, deverá considerar-se os modelos com, pelo menos, mil milhões de parâmetros e treinados com uma grande quantidade de dados utilizando a autossupervisão em escala para apresentar uma generalidade significativa e executar com competência uma vasta gama de tarefas distintas.

(99) Os grandes modelos generativos de IA são um exemplo típico de um modelo de IA de finalidade geral, uma vez que permitem a geração flexível de conteúdos, por exemplo, sob a forma de texto, áudio, imagens ou vídeo, que podem facilmente adaptar-se a uma vasta gama de tarefas distintas.

(100) Quando um modelo de IA de finalidade geral é integrado num sistema de IA ou dele faz parte integrante, este sistema deverá ser considerado um sistema de IA de finalidade geral se, graças a esta integração, tiver a capacidade de servir uma variedade de finalidades. Um sistema de IA de finalidade geral pode ser utilizado diretamente ou ser integrado em outros sistemas de IA.

(101) Os prestadores de modelos de IA de finalidade geral têm um papel e uma responsabilidade específicos na cadeia de valor da IA, uma vez que os modelos que facultam podem constituir a base de uma série de sistemas a jusante, muitas vezes disponibilizados por prestadores a jusante que precisam de ter uma boa compreensão dos modelos e das suas capacidades, tanto para permitir a integração desses modelos nos seus produtos como para cumprir as suas obrigações nos termos deste ou de outros regulamentos. Por conseguinte, deverão ser previstas medidas de transparência proporcionadas, incluindo a elaboração e a atualização da documentação e a prestação de informações sobre o modelo de IA de finalidade geral para a sua utilização pelos prestadores a jusante. A documentação técnica deverá ser elaborada e mantida atualizada pelo prestador do modelo de IA de finalidade geral para efeitos da sua disponibilização, mediante pedido, ao Serviço para a IA e às autoridades nacionais competentes. O conjunto mínimo de elementos a incluir nessa documentação deverá ser estabelecido em anexos específicos do presente regulamento. A Comissão deverá estar habilitada a alterar esses anexos por meio de atos delegados à luz da evolução tecnológica.

(102) O software e os dados, incluindo os modelos, lançados ao abrigo de uma licença gratuita e de fonte aberta que lhes permita serem partilhados abertamente e que permita aos utilizadores aceder-lhes livremente, utilizá-los, modificá-los e redistribuí-los, ou a versões modificadas dos mesmos, podem contribuir para a investigação e a inovação no mercado e podem proporcionar oportunidades de crescimento significativas para a economia da União. Deverá considerar-se que os modelos de IA de finalidade geral lançados ao abrigo de licenças gratuitas e de fonte aberta asseguram elevados níveis de transparência e abertura se os seus parâmetros, incluindo as ponderações, as informações sobre a arquitetura do modelo e as informações sobre a utilização do modelo, forem disponibilizados ao público. A licença deverá também ser considerada gratuita e de fonte aberta quando permite aos utilizadores executar, copiar, distribuir, estudar, alterar e melhorar o software e os dados, incluindo os modelos, na condição de serem atribuídos os créditos ao prestador original do modelo e de serem respeitadas as condições de distribuição idênticas ou comparáveis.

(103) Componentes de IA gratuitos e de fonte aberta abrangem o software e os dados, incluindo modelos e modelos de IA de finalidade geral, ferramentas, serviços ou processos de um sistema de IA. Os componentes de IA gratuitos e de fonte aberta podem ser disponibilizados através de diferentes canais, nomeadamente o seu desenvolvimento em repositórios abertos. Para efeitos do presente regulamento, os componentes de IA disponibilizados por um preço ou convertidos em dinheiro de outra forma, nomeadamente no âmbito da prestação de apoio técnico ou de outros serviços (inclusive através de uma plataforma de software) relacionados com o componente de IA, ou a utilização de dados pessoais por motivos que não sejam exclusivamente para melhorar a segurança, a compatibilidade ou a interoperabilidade do software, com exceção das transações entre microempresas, não deverão beneficiar das exceções previstas para os componentes de IA gratuitos e de fonte aberta. O facto de disponibilizar componentes de IA através de repositórios abertos não deverá, por si só, constituir uma conversão em dinheiro.

(104) Os prestadores de modelos de IA de finalidade geral lançados ao abrigo de uma licença gratuita e de fonte aberta e cujos parâmetros, incluindo as ponderações, as informações sobre a arquitetura do modelo e as informações sobre a utilização de modelos, são disponibilizados ao público deverão ser objeto de exceções no que diz respeito aos requisitos relacionados com a transparência impostos aos modelos de IA de finalidade geral, a menos que se possa considerar que apresentam um risco sistémico, caso em que a circunstância de o modelo ser transparente e acompanhado de uma licença de fonte aberta não deverá ser considerada um motivo suficiente para excluir o cumprimento das obrigações previstas no presente regulamento. Em todo o caso, uma vez que o lançamento de modelos de IA de finalidade geral ao abrigo de licenças gratuitas e de fonte aberta não revela necessariamente informações substanciais sobre o conjunto de dados utilizado para o treino ou aperfeiçoamento do modelo nem sobre a forma como foi assegurada a conformidade da legislação em matéria de direitos de autor, a exceção prevista para os modelos de IA de finalidade geral ao cumprimento dos requisitos relacionados com a transparência não deverá dizer respeito à obrigação de elaborar um resumo sobre os conteúdos utilizados para o treino de modelos nem à obrigação de aplicar uma política de cumprimento da legislação da União em matéria de direitos de autor, em especial para identificar e cumprir a reserva de direitos prevista no artigo 4.º, n.º 3, da Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho[40].

[40] Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE (JO L 130 de 17.5.2019, p. 92).

(105) Os modelos de IA de finalidade geral, em especial os grandes modelos generativos de IA, capazes de gerar texto, imagens e outros conteúdos, apresentam oportunidades de inovação únicas, mas também desafios para artistas, autores e outros criadores e para a forma como os seus conteúdos criativos são criados, distribuídos, utilizados e consumidos. O desenvolvimento e o treino de tais modelos exigem o acesso a grandes quantidades de texto, imagens, vídeos e outros dados. As técnicas de prospeção de textos e dados podem ser amplamente utilizadas neste contexto para recuperar e analisar esses conteúdos, que podem ser protegidos por direitos de autor e direitos conexos. Qualquer utilização de conteúdos protegidos por direitos de autor exige a autorização dos titulares dos direitos em causa, a menos que se apliquem exceções e limitações pertinentes em matéria de direitos de autor. A Diretiva (UE) 2019/790 introduziu exceções e limitações que permitem reproduções e extrações de obras ou outro material para efeitos de prospeção de textos e dados, sob determinadas condições. Ao abrigo destas regras, os titulares de direitos podem optar por reservar os seus direitos sobre as suas obras ou outro material para impedir a prospeção de textos e dados, a menos que tal seja feito para fins de investigação científica. Sempre que os direitos de exclusão tenham sido expressamente reservados de forma adequada, os prestadores de modelos de IA de finalidade geral têm de obter uma autorização dos titulares de direitos caso pretendam realizar uma prospeção de textos e dados nessas obras.

(106) Os prestadores que colocam modelos de IA de finalidade geral no mercado da União deverão assegurar o cumprimento das obrigações pertinentes previstas no presente regulamento. Para o efeito, os prestadores de modelos de IA de finalidade geral deverão pôr em prática uma política que cumpra o direito da União em matéria de direitos de autor e direitos conexos, em especial para identificar e cumprir a reserva de direitos expressa pelos titulares de direitos nos termos do artigo 4.º, n.º 3, da Diretiva (UE) 2019/790. Qualquer prestador que coloque um modelo de IA de finalidade geral no mercado da União deverá cumprir esta obrigação, independentemente da jurisdição em que têm lugar os atos relevantes em matéria de direitos de autor subjacentes ao treino desses modelos de IA de finalidade geral. Tal é necessário para assegurar condições de concorrência equitativas entre os prestadores de modelos de IA de finalidade geral em que nenhum prestador possa obter uma vantagem competitiva no mercado da União aplicando normas de direitos de autor menos rigorosas do que as previstas na União.

(107) A fim de aumentar a transparência dos dados utilizados no treino prévio e no treino de modelos de IA de finalidade geral, incluindo textos e dados protegidos pela legislação em matéria de direitos de autor, é adequado que os prestadores desses modelos elaborem e disponibilizem ao público um resumo suficientemente pormenorizado dos conteúdos utilizados para o treino do modelo de IA de finalidade geral. Embora tendo devidamente em conta a necessidade de proteger os segredos comerciais e as informações comerciais de caráter confidencial, esse resumo deverá, de um modo geral, ser abrangente no seu âmbito de aplicação, em vez de ser tecnicamente pormenorizado, a fim de facilitar às partes com interesses legítimos, incluindo os titulares de direitos de autor, o exercício e a aplicação dos seus direitos ao abrigo do direito da União, por exemplo, enumerando as principais coleções ou conjuntos de dados que entraram no treino do modelo, como grandes bases de dados públicas ou privadas ou arquivos de dados, e oferecendo uma explicação narrativa sobre outras fontes de dados utilizadas. É conveniente que o Serviço para a IA disponibilize um modelo para o resumo, que deverá ser simples e eficaz, e permita ao prestador facultar o resumo exigido sob a forma narrativa.

(108) No que diz respeito às obrigações impostas aos prestadores de modelos de IA de finalidade geral para que ponham em prática uma política de cumprimento da legislação da União em matéria de direitos de autor e disponibilizem ao público um resumo dos conteúdos utilizados para o treino, o Serviço para a IA deverá controlar se o prestador cumpriu essas obrigações sem verificar ou proceder a uma avaliação obra a obra dos dados de treino no que respeita aos direitos de autor. O presente regulamento não afeta a aplicação das regras em matéria de direitos de autor previstas no direito da União.

(109) O cumprimento das obrigações aplicáveis aos prestadores de modelos de IA de finalidade geral deverá ser consentâneo e proporcionado ao tipo de prestador do modelo, excluindo a necessidade de conformidade para as pessoas que desenvolvem ou utilizam modelos para fins de investigação não profissional ou científica, que deverão, no entanto, ser incentivadas a cumprir voluntariamente esses requisitos. Sem prejuízo do direito da União em matéria de direitos de autor, o cumprimento dessas obrigações deverá ter devidamente em conta a dimensão do prestador e permitir formas simplificadas de conformidade para as PME, incluindo as empresas em fase de arranque, que não deverão representar um custo excessivo nem desencorajar a utilização de tais modelos. Em caso de alteração ou aperfeiçoamento de um modelo, as obrigações dos prestadores de modelos de IA de finalidade geral deverão limitar-se a essa alteração ou aperfeiçoamento, por exemplo, complementando a documentação técnica já existente com informações sobre as alterações, nomeadamente novas fontes de dados de treino, como forma de cumprir as obrigações da cadeia de valor previstas no presente regulamento.

(110) Os modelos de IA de finalidade geral poderão representar riscos sistémicos que incluem, entre outros, quaisquer efeitos negativos reais ou razoavelmente previsíveis em relação a acidentes graves, perturbações de setores críticos e consequências graves para a saúde e a segurança públicas; quaisquer efeitos negativos, reais ou razoavelmente previsíveis, em processos democráticos e na segurança pública e económica; a divulgação de conteúdos ilegais, falsos ou discriminatórios. Os riscos sistémicos deverão ser entendidos como aumentando as capacidades e o alcance do modelo, podendo surgir ao longo de todo o ciclo de vida do modelo e ser influenciados por condições de utilização indevida, fiabilidade do modelo, equidade e segurança do modelo, pelo nível de autonomia do modelo, pelo seu acesso a ferramentas, modalidades novas ou combinadas, estratégias de lançamento e distribuição, pelo potencial de remoção de barreiras de segurança e outros fatores. Em especial, as abordagens internacionais identificaram, até à data, a necessidade de prestar atenção aos riscos decorrentes de uma potencial utilização indevida intencional ou de problemas não intencionais de controlo relacionados com o alinhamento com a intenção humana; os riscos químicos, biológicos, radiológicos e nucleares, tais como as formas como as barreiras à entrada podem ser baixadas, inclusive para o desenvolvimento, a conceção, a aquisição ou a utilização de armas; as capacidades cibernéticas ofensivas, tais como as formas em que a descoberta, exploração ou utilização operacional de vulnerabilidades pode ser permitida; os efeitos da interação e da utilização de ferramentas, incluindo, por exemplo, a capacidade de controlar os sistemas físicos e de interferir com as infraestruturas críticas; os riscos decorrentes de os modelos fazerem cópias de si próprios ou de «autorreplicação», ou de treinarem outros modelos; a forma como os modelos podem dar origem a enviesamentos prejudiciais e a discriminação, com riscos para os indivíduos, as comunidades ou as sociedades; a facilitação da desinformação ou o prejuízo para a privacidade, com ameaças para os valores democráticos e os direitos humanos; o risco de que um acontecimento específico conduza a uma reação em cadeia com efeitos negativos consideráveis que possam afetar até uma cidade inteira, uma atividade num domínio inteiro ou uma comunidade inteira.

(111) É conveniente estabelecer uma metodologia para a classificação de modelos de IA de finalidade geral como modelos de IA de finalidade geral com riscos sistémicos. Uma vez que os riscos sistémicos resultam de capacidades particularmente elevadas, deverá considerar-se que um modelo de IA de finalidade geral apresenta riscos sistémicos se tiver capacidades de elevado impacto, avaliadas com base em ferramentas e metodologias técnicas adequadas ou um impacto significativo no mercado interno devido ao seu alcance. Entende-se por capacidades de elevado impacto em modelos de IA de finalidade geral as capacidades que correspondam ou excedam as capacidades registadas nos modelos de IA de finalidade geral mais avançados. O conjunto completo de capacidades num modelo poderá ser mais bem compreendido após a sua colocação no mercado ou quando os responsáveis pela implantação interagirem com o modelo. De acordo com o estado da arte no momento da entrada em vigor do presente regulamento, a quantidade acumulada de cálculo utilizado para o treino do modelo de IA de finalidade geral medido em operações de vírgula flutuante é uma das aproximações pertinentes para as capacidades do modelo. A quantidade acumulada de cálculo utilizado para o treino inclui o cálculo utilizado nas atividades e métodos destinados a reforçar as capacidades do modelo antes da implantação, como o treino prévio, a geração de dados sintéticos e o aperfeiçoamento. Por conseguinte, deverá ser estabelecido um limiar inicial de operação de vírgula flutuante que, se for cumprido por um modelo de IA de finalidade geral, conduz à presunção de que o modelo é um modelo de IA de finalidade geral com riscos sistémicos. Este limiar deverá ser ajustado ao longo do tempo para refletir as mudanças tecnológicas e industriais, tais como as melhorias algorítmicas ou uma maior eficiência do hardware, e deverá ser complementado com parâmetros de referência e indicadores da capacidade dos modelos.

Para o fundamentar, o Serviço para a IA deverá colaborar com a comunidade científica, a indústria, a sociedade civil e outros peritos. Os limiares, bem como as ferramentas e os parâmetros de referência para a avaliação das capacidades de elevado impacto, deverão ser indicadores fortes da generalidade, das suas capacidades e do risco sistémico associado dos modelos de IA de finalidade geral, e poderão ter em conta a forma como o modelo será colocado no mercado ou o número de utilizadores que pode afetar. Para complementar este sistema, a Comissão deverá ter a possibilidade de tomar decisões individuais que designem um modelo de IA de finalidade geral como sendo um modelo de IA de finalidade geral com risco sistémico, caso se verifique que esse modelo tem capacidades ou impacto equivalentes aos captados pelo limiar estabelecido. Essa decisão deverá ser tomada com base numa avaliação global dos critérios de designação do modelo de IA de finalidade geral com risco sistémico estabelecidos num anexo do presente regulamento, tais como a qualidade ou a dimensão do conjunto de dados de treino, o número de utilizadores profissionais e finais, as suas modalidades de entrada e saída, o seu nível de autonomia e escalabilidade ou as ferramentas a que tem acesso. Mediante pedido fundamentado de um prestador cujo modelo tenha sido designado um modelo de IA de finalidade geral com risco sistémico, a Comissão deverá ter em conta o pedido e pode decidir reavaliar se ainda é possível considerar que o modelo de IA de finalidade geral apresenta riscos sistémicos.

(112) É igualmente necessário tornar claro um procedimento para a classificação de um modelo de IA de finalidade geral com riscos sistémicos. Deverá presumir-se que um modelo de IA de finalidade geral que cumpra o limiar aplicável às capacidades de elevado impacto é um modelo de IA de finalidade geral com risco sistémico. O mais tardar duas semanas após o cumprimento dos requisitos ou após ter conhecimento de que um modelo de IA de finalidade geral cumprirá os requisitos que conduzem à presunção, o prestador deverá notificar o Serviço para a IA. Este aspeto é especialmente pertinente em relação ao limiar de operações de vírgula flutuante, uma vez que o treino de modelos de IA de finalidade geral exige um planeamento considerável, que inclui a afetação inicial de recursos de cálculo e, por conseguinte, os prestadores de modelos de IA de finalidade geral conseguem saber se o seu modelo cumprirá o limiar antes da conclusão do treino. No contexto dessa notificação, o prestador deverá poder demonstrar que um modelo de IA de finalidade geral, devido às suas características específicas, excecionalmente não apresenta riscos sistémicos e que, por conseguinte, não deverá ser classificado como sendo um modelo de IA de finalidade geral com riscos sistémicos. Essas informações são úteis para o Serviço para a IA antecipar a colocação no mercado de modelos de IA de finalidade geral com riscos sistémicos e os prestadores poderem começar a dialogar com o Serviço para a IA numa fase precoce. Essas informações são especialmente importantes no que diz respeito aos modelos de IA de finalidade geral que se prevê sejam lançados como fonte aberta, uma vez que, após o lançamento de modelos de fonte aberta, as medidas necessárias para assegurar o cumprimento das obrigações decorrentes do presente regulamento podem ser mais difíceis de aplicar.

(113) Se a Comissão tomar conhecimento de que um modelo de IA de finalidade geral cumpre os requisitos para se classificar como modelo de IA de finalidade geral com risco sistémico, facto que anteriormente não era conhecido ou sobre o qual o prestador em causa não notificou a Comissão, a Comissão deverá ficar habilitada a designá-lo como tal. Um sistema de alertas qualificados deverá assegurar que o Serviço para a IA é informado pelo painel científico sobre modelos de IA de finalidade geral que possivelmente deverão ser classificados como modelos de IA de finalidade geral com risco sistémico, a par das atividades de acompanhamento do Serviço para a IA.

(114) Os prestadores de modelos de IA de finalidade geral que apresentem riscos sistémicos deverão estar sujeitos, para além das obrigações previstas para os prestadores de modelos de IA de finalidade geral, a obrigações que visem identificar e atenuar esses riscos e assegurar um nível adequado de proteção da cibersegurança, independentemente de serem disponibilizados como modelos autónomos ou incorporados num sistema de IA ou num produto. Para alcançar esses objetivos, o presente regulamento deverá exigir que os prestadores realizem as avaliações necessárias dos modelos, em especial antes da sua primeira colocação no mercado, incluindo a realização de testagens antagónicas dos modelos e a respetiva documentação, se for caso disso também por meio de testagens internas ou externas independentes. Além disso, os prestadores de modelos de IA de finalidade geral com riscos sistémicos deverão avaliar e atenuar continuamente os riscos sistémicos, nomeadamente pondo em prática políticas de gestão de riscos, como processos de responsabilização e governação, executando o acompanhamento pós-comercialização, adotando medidas adequadas ao longo de todo o ciclo de vida do modelo e cooperando com os intervenientes pertinentes ao longo de toda a cadeia de valor da IA.

(115) Os prestadores de modelos de IA de finalidade geral com riscos sistémicos deverão avaliar e atenuar eventuais riscos sistémicos. Se, apesar dos esforços para identificar e prevenir riscos relacionados com um modelo de IA de finalidade geral que possa apresentar riscos sistémicos, o desenvolvimento ou a utilização do modelo causar um incidente grave, o prestador do modelo de IA de finalidade geral deverá, sem demora injustificada, acompanhar o incidente e comunicar quaisquer informações pertinentes e eventuais medidas corretivas à Comissão e às autoridades nacionais competentes. Além disso, os prestadores deverão assegurar um nível adequado de proteção do modelo e das suas infraestruturas físicas em termos de cibersegurança, se for caso disso ao longo de todo o ciclo de vida do modelo. A proteção em termos de cibersegurança relacionada com os riscos sistémicos associados à utilização maliciosa ou a ataques deverá ter devidamente em conta as fugas acidentais de modelos, os lançamentos não autorizados, o contornamento de medidas de segurança e a defesa contra ciberataques, o acesso não autorizado ou o roubo de modelos. Essa proteção poderá ser facilitada garantindo as ponderações dos modelos, algoritmos, servidores e conjuntos de dados, nomeadamente por intermédio de medidas de segurança operacional para a segurança da informação, de políticas específicas em matéria de cibersegurança, de soluções técnicas e estabelecidas adequadas e de controlos informáticos e físicos do acesso, adequados às circunstâncias pertinentes e aos riscos envolvidos.

(116) O Serviço para a IA deverá incentivar e facilitar a elaboração, a revisão e a adaptação de códigos de práticas, tendo em conta as abordagens internacionais. Todos os prestadores de modelos de IA de finalidade geral poderão ser convidados a participar. A fim de assegurar que os códigos de práticas refletem o estado da arte e têm devidamente em conta um conjunto diversificado de perspetivas, o Serviço para a IA deverá colaborar com as autoridades nacionais competentes pertinentes e poderá, se for caso disso, consultar organizações da sociedade civil e outras partes interessadas e peritos pertinentes, incluindo o painel científico, para a elaboração desses códigos. Os códigos de práticas deverão abranger as obrigações dos prestadores de modelos de IA de finalidade geral e de modelos de IA de finalidade geral que apresentem riscos sistémicos. Além disso, no que diz respeito aos riscos sistémicos, os códigos de práticas deverão ajudar a estabelecer uma taxonomia do tipo e da natureza dos riscos sistémicos a nível da União, incluindo das suas fontes. Os códigos de práticas deverão também centrar-se na avaliação específica dos riscos e em medidas de atenuação.

(117) Os códigos de práticas deverão representar um instrumento central para o cumprimento adequado das obrigações previstas no presente regulamento para os prestadores de modelos de IA de finalidade geral. Os prestadores deverão poder recorrer a códigos de práticas para demonstrar o cumprimento das obrigações. Por meio de atos de execução, a Comissão pode decidir aprovar um código de práticas e conferir-lhe uma validade geral na União ou, em alternativa, estabelecer regras comuns para a execução das obrigações pertinentes, se, no momento em que o presente regulamento se tornar aplicável, não for possível finalizar um código de práticas ou este não for considerado adequado pelo Serviço para a IA. Uma vez publicada uma norma harmonizada e considerada adequada para abranger as obrigações pertinentes do Serviço para a IA, a conformidade com uma norma europeia harmonizada deverá conferir aos prestadores a presunção de conformidade. Os prestadores de modelos de IA de finalidade geral deverão, além disso, ser capazes de demonstrar a conformidade utilizando meios alternativos adequados, se não estiverem disponíveis códigos de práticas nem normas harmonizadas, ou se os prestadores optarem por não se basear neles.

(118) O presente regulamento regula os sistemas de IA e modelos de IA, impondo determinados requisitos e obrigações aos intervenientes pertinentes no mercado que os colocam no mercado, colocam em serviço ou em utilização na União, complementando assim as obrigações dos prestadores de serviços intermediários que incorporam esses sistemas ou modelos nos seus serviços regulados pelo Regulamento (UE) 2022/2065. Na medida em que esses sistemas ou modelos estejam incorporados naquelas que são designadas por plataformas em linha de muito grande dimensão ou motores de pesquisa em linha de muito grande dimensão, estão sujeitos ao regime de gestão de riscos previsto no Regulamento (UE) 2022/2065. Por conseguinte, deverá presumir-se que as obrigações correspondentes do presente Regulamento foram cumpridas, a menos que surjam e sejam identificados nesses modelos riscos sistémicos significativos não abrangidos pelo Regulamento (UE) 2022/2065. Neste contexto, os prestadores de plataformas em linha de muito grande dimensão e de motores de pesquisa em linha de muito grande dimensão são obrigados a avaliar os potenciais riscos sistémicos decorrentes da conceção, do funcionamento e da utilização dos seus serviços, incluindo a forma como a conceção dos sistemas algorítmicos utilizados no serviço pode contribuir para esses riscos, bem como os riscos sistémicos decorrentes de potenciais utilizações indevidas. Esses prestadores são igualmente obrigados a tomar medidas de atenuação adequadas no respeito dos direitos fundamentais.

(119) Tendo em conta o ritmo rápido da inovação e a evolução tecnológica dos serviços digitais no âmbito dos diferentes instrumentos do direito da União, em especial tendo em conta a utilização e a perceção dos seus destinatários, os sistemas de IA abrangidos pelo presente regulamento podem ser prestados como serviços intermediários ou partes dos mesmos, na aceção do Regulamento (UE) 2022/2065, que deverão ser interpretados de forma tecnologicamente neutra. Por exemplo, os sistemas de IA podem ser utilizados para a disponibilização de motores de pesquisa em linha, em especial na medida em que um sistema de IA, como um robô de conversação em linha, efetua em princípio pesquisas em todos os sítios Web, depois incorpora os resultados nos conhecimentos que já tem e utiliza os conhecimentos atualizados para gerar um resultado único que combina diferentes fontes de informação.

(120) Além disso, a fim de facilitar a aplicação efetiva do Regulamento (UE) 2022/2065, as obrigações impostas por força do presente regulamento aos prestadores e responsáveis pela implantação de determinados sistemas de IA são particularmente relevantes para permitir detetar e divulgar se os resultados desses sistemas são artificialmente gerados ou manipulados. Tal aplica-se, em especial, às obrigações dos prestadores de plataformas em linha de muito grande dimensão ou de motores de pesquisa em linha de muito grande dimensão que consistem em identificar e atenuar os riscos sistémicos que possam resultar da divulgação de conteúdos artificialmente gerados ou manipulados, em especial o risco de efeitos negativos reais ou previsíveis nos processos democráticos, no debate público e nos processos eleitorais, nomeadamente através da desinformação.

(121) A normalização deverá desempenhar um papel fundamental, disponibilizando aos prestadores soluções técnicas que assegurem a conformidade com o presente regulamento, em consonância com o estado da arte, a fim de promover a inovação, a competitividade e o crescimento no mercado único. O cumprimento de normas harmonizadas conforme definido no artigo 2.º, ponto 1, alínea c), do Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho[41], das quais normalmente se espera que reflitam o estado da arte, deverá constituir um meio de os prestadores demonstrarem a conformidade com os requisitos do presente regulamento. Por conseguinte, deverá ser incentivada uma representação equilibrada de interesses que implique todas as partes interessadas na elaboração de normas, em especial as PME, as organizações de consumidores e as partes interessadas ambientalistas e da sociedade civil, em conformidade com os artigos 5.º e 6.º do Regulamento (UE) n.º 1025/2012. A fim de facilitar a conformidade, os pedidos de normalização deverão ser emitidos pela Comissão sem demora injustificada. Quando preparar o pedido de normalização, a Comissão deverá consultar o fórum consultivo e o Comité, a fim de recolher conhecimentos especializados pertinentes. No entanto, na ausência de referências pertinentes a normas harmonizadas, a Comissão deverá poder estabelecer, através de atos de execução e após consulta do fórum consultivo, especificações comuns para determinados requisitos ao abrigo do presente regulamento.

---

41 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).

A especificação comum deverá ser uma solução excecional de recurso para facilitar a obrigação do prestador de cumprir os requisitos do presente regulamento caso o pedido de normalização não tenha sido aceite por nenhuma das organizações europeias de normalização, caso as normas harmonizadas pertinentes não respondam de forma suficiente às preocupações em matéria de direitos fundamentais, caso as normas harmonizadas não satisfaçam o pedido ou caso haja atrasos na adoção de uma norma harmonizada adequada. Se esse atraso na adoção de uma norma harmonizada se dever à complexidade técnica dessa norma, a Comissão deverá tomar esse facto em consideração antes de ponderar o estabelecimento de especificações comuns. Ao elaborar especificações comuns, a Comissão é incentivada a cooperar com os parceiros internacionais e os organismos internacionais de normalização.

(122) Sem prejuízo da utilização de normas harmonizadas e especificações comuns, é conveniente presumir que os prestadores de um sistema de IA de risco elevado que tenha sido treinado e testado em dados que reflitam o cenário geográfico, comportamental, contextual ou funcional específico no qual o sistema de IA se destina a ser utilizado cumprem a medida pertinente prevista no requisito de governação de dados estabelecido no presente regulamento. Sem prejuízo dos requisitos relacionados com a solidez e a exatidão estabelecidos no presente regulamento, em conformidade com o artigo 54.º, n.º 3, do Regulamento (UE) 2019/881, deverá presumir-se que os sistemas de IA de risco elevado que tenham sido certificados ou relativamente aos quais tenha sido emitida uma declaração de conformidade no âmbito de um sistema de certificação da cibersegurança estabelecido nos termos desse regulamento, e cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia*, cumprem os requisitos de cibersegurança do presente regulamento, contanto que o certificado de cibersegurança ou a declaração de conformidade ou partes dos mesmos abranjam os requisitos de cibersegurança do presente regulamento. Tal não prejudica a natureza voluntária desse sistema de certificação da cibersegurança.

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

(124) Para minimizar os encargos impostos aos operadores e evitar possíveis duplicações, é conveniente que, no caso dos sistemas de IA de risco elevado relacionados com produtos abrangidos por legislação de harmonização da União com base no novo regime jurídico, o cumprimento dos requisitos do presente regulamento por parte desses sistemas de IA seja aferido no âmbito da avaliação da conformidade já prevista nessa lei. Como tal, a aplicabilidade dos requisitos do presente regulamento não deverá afetar a lógica, a metodologia ou a estrutura geral específicas da avaliação da conformidade nos termos da legislação de harmonização da União pertinente.

(125) Dada a complexidade dos sistemas de IA de risco elevado e os riscos que lhes estão associados, é importante desenvolver um procedimento de avaliação da conformidade adequado para sistemas de IA de risco elevado que envolvam organismos notificados, a chamada avaliação da conformidade por terceiros. Contudo, dada a atual experiência 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. Por conseguinte, a avaliação da conformidade desses sistemas deverá ser realizada, regra geral, pelo prestador sob a sua própria responsabilidade, com a única exceção dos sistemas de IA concebidos para utilização em biometria.

(126) Sempre que seja necessário realizar avaliações da conformidade por terceiros, os organismos notificados deverão ser notificados por força do presente regulamento pelas autoridades nacionais competentes, desde que cumpram uma série de requisitos, nomeadamente em termos de independência, competência, ausência de conflitos de interesse e requisitos de cibersegurança adequados. A notificação desses organismos deverá ser enviada pelas autoridades nacionais competentes à Comissão e aos outros Estados-Membros por meio do instrumento de notificação eletrónica desenvolvido e gerido pela Comissão nos termos do artigo R23 do anexo I da Decisão n.º 768/2008/CE.

(127) Em conformidade com os compromissos assumidos pela União no âmbito do Acordo sobre os Obstáculos Técnicos ao Comércio da Organização Mundial do Comércio, é adequado facilitar o reconhecimento mútuo dos resultados da avaliação da conformidade produzidos pelos organismos de avaliação da conformidade competentes, independentes do território em que se encontram estabelecidos, desde que esses organismos de avaliação da conformidade estabelecidos ao abrigo da legislação de um país terceiro cumpram os requisitos aplicáveis do presente regulamento e que a União tenha celebrado um acordo nessa medida. Neste contexto, a Comissão deverá explorar ativamente possíveis instrumentos internacionais para esse efeito e, em especial, celebrar acordos de reconhecimento mútuo com países terceiros.

(128) Em consonância com a noção comummente estabelecida de modificação substancial de produtos regulamentados pela legislação de harmonização da União, sempre que ocorra uma alteração que possa afetar a conformidade de um sistema de IA de risco elevado com o presente Regulamento (p. ex., alteração do sistema operativo ou da arquitetura do software), ou sempre que a finalidade prevista do sistema se altere, é apropriado que esse sistema de IA seja considerado um novo sistema de IA que deverá ser submetido a uma nova avaliação da conformidade. No entanto, as alterações que ocorrem no algoritmo e no desempenho dos sistemas de IA que continuam a «aprender» depois de terem sido colocados no mercado ou colocados em serviço, nomeadamente que adaptam automaticamente o modo de funcionamento, não deverão constituir uma modificação substancial, desde que tenham sido predeterminadas pelo prestador e examinadas aquando da avaliação da conformidade.

(129) Para que possam circular livremente dentro do mercado interno, os sistemas de IA de risco elevado deverão apresentar a marcação CE para indicar a sua conformidade com o presente regulamento. No caso dos sistemas de IA de risco elevado integrados num produto, deverá ser aposta uma marcação CE física, que pode ser complementada por uma marcação CE digital. No caso dos sistemas de IA de risco elevado disponibilizados apenas digitalmente, deverá ser utilizada uma marcação CE digital. Os Estados-Membros não poderão criar obstáculos injustificados à colocação no mercado nem à colocação em serviço de sistemas de IA de risco elevado que cumpram os requisitos previstos no presente regulamento e apresentem a marcação CE.

(130) Em certas condições, uma disponibilização rápida de tecnologias inovadoras pode ser crucial para a saúde e a segurança das pessoas, para a proteção do ambiente e as alterações climáticas e para a sociedade em geral. Como tal, é apropriado que, por razões excecionais de segurança pública ou proteção da vida e da saúde das pessoas singulares, da proteção do ambiente e da proteção dos ativos industriais e infraestruturais essenciais, as autoridades de fiscalização do mercado possam autorizar a colocação no mercado ou a colocação em serviço de sistemas de IA que não tenham sido objeto de uma avaliação da conformidade. Em situações devidamente justificadas, tal como previsto no presente regulamento, as autoridade responsáveis pela aplicação da lei ou as autoridades de proteção civil podem colocar em serviço um sistema de IA de risco elevado específico sem autorização da autoridade de fiscalização do mercado, desde que essa autorização seja solicitada durante ou após a utilização sem demora injustificada.

(131) Para facilitar o trabalho da Comissão e dos Estados-Membros no domínio da IA, bem como aumentar a transparência para o público, os prestadores de sistemas de IA de risco elevado que não os relacionados com produtos abrangidos pelo âmbito da legislação de harmonização da União em vigor aplicável, bem como os prestadores que consideram que um sistema de IA de risco elevado enumerado nos casos concretos de risco elevado num anexo do presente regulamento não é de risco elevado com base numa derrogação, deverão ser obrigados a registarem-se a si mesmos e a registar as informações sobre o seu sistema de IA de risco elevado numa base de dados da UE, a criar e gerir pela Comissão. Antes de um sistema de IA enumerado nos casos concretos de risco elevado de risco elevado num anexo do presente regulamento, os responsáveis pela implantação de sistemas de IA de risco elevado que sejam autoridades, agências ou organismos públicos, deverão registar-se nessa base de dados e selecionar o sistema que tencionam utilizar.

Os outros responsáveis pela implantação deverão ter o direito de o fazer voluntariamente. Esta secção da base de dados da UE deverá ser acessível ao público, gratuitamente, e as informações deverão ser facilmente navegáveis, compreensíveis e legíveis por máquina. A base de dados da UE deverá também ser de fácil utilização, por exemplo oferecendo funcionalidades de pesquisa, nomeadamente através de palavras-chave, que permitam ao público em geral encontrar informações pertinentes a apresentar aquando do registo dos sistemas de IA de risco elevado e nos tipos de sistemas de IA de risco elevado, estabelecidas num anexo do presente regulamento a que os sistemas de IA de risco elevado correspondem. Qualquer modificação substancial de sistemas de IA de risco elevado também deverá ser registada na base de dados da UE. No caso dos sistemas de IA de risco elevado no domínio da aplicação da lei, da migração, do asilo e da gestão do controlo das fronteiras, as obrigações de registo deverão ser cumpridas numa secção não pública protegida da base de dados da UE. O acesso à secção segura não pública deverá ser estritamente limitado à Comissão e às autoridades de fiscalização do mercado no que diz respeito à respetiva secção nacional dessa base de dados. Os sistemas de IA de risco elevado no domínio das infraestruturas críticas só deverão ser registados a nível nacional. A Comissão deverá ser a responsável pelo tratamento da base de dados da UE, em conformidade com o Regulamento (UE) 2018/1725. Para assegurar que a base de dados esteja plenamente operacional à data de implantação, o procedimento para a criação da base de dados da UE deverá incluir o desenvolvimento de especificações funcionais pela Comissão e um relatório de auditoria independente. A Comissão deverá ter em conta os riscos para a cibersegurança e os riscos no exercício das suas funções de responsável pelo tratamento de dados na base de dados da UE. A fim de maximizar a disponibilidade e a utilização da base de dados pelo público, a base de dados da UE, incluindo as informações disponibilizadas através da mesma, deverá cumprir os requisitos estabelecidos na Diretiva (UE) 2019/882.

(132) Determinados sistemas de IA concebidos para interagir com pessoas singulares ou para criar conteúdos podem representar riscos específicos de usurpação de identidade ou dissimulação, independentemente de serem considerados de risco elevado ou não. Como tal, em certas circunstâncias, a utilização desses sistemas deverá ser sujeita a obrigações de transparência específicas, sem prejuízo dos requisitos e obrigações aplicáveis aos sistemas de IA de risco elevado, e a exceções específicas, a fim de ter em conta a necessidade especial da aplicação da lei. Em particular, as pessoas singulares deverão ser informadas de que estão a interagir com um sistema de IA, salvo se tal for óbvio do ponto de vista de uma pessoa singular razoavelmente informada, atenta e advertida, tendo em conta as circunstâncias e o contexto de utilização. Ao aplicar essa obrigação, as características das pessoas singulares pertencentes a grupos vulneráveis devido à sua idade ou deficiência deverão ser tidas em conta na medida em que o sistema de IA também se destine a interagir com esses grupos. Além disso, as pessoas singulares deverão ser notificadas quando forem expostas a sistemas de IA que, através do tratamento dos seus dados biométricos, possam identificar ou inferir as emoções ou intenções dessas pessoas ou atribuí-las a categorias específicas. Essas categorias específicas podem dizer respeito a aspetos como sexo, idade, cor do cabelo, cor dos olhos, tatuagens, traços de personalidade, origem étnica, preferências e interesses pessoais. Essas informações e notificações deverão ser apresentadas em formatos acessíveis a pessoas com deficiência.

(133) Um número de sistemas de IA consegue gerar grandes quantidades de conteúdos sintéticos que se tornam cada vez mais difíceis para os seres humanos de distinguir dos conteúdos gerados por seres humanos e autênticos. A ampla disponibilidade e o aumento das capacidades desses sistemas têm um impacto significativo na integridade e na confiança no ecossistema da informação, suscitando novos riscos de desinformação e manipulação em grande escala, fraude, usurpação de identidade e dissimulação dos consumidores. À luz desses impactos, do rápido ritmo tecnológico e da necessidade de novos métodos e técnicas para rastrear a origem das informações, é adequado exigir que os prestadores desses sistemas incorporem soluções técnicas que permitam a marcação num formato legível por máquina e a deteção de que o resultado foi gerado ou manipulado por um sistema de IA e não por um ser humano. Essas técnicas e métodos deverão ser suficientemente fiáveis, interoperáveis, eficazes e robustos, na medida em que tal seja tecnicamente viável, tendo em conta as técnicas disponíveis ou uma combinação de técnicas, tais como marcas de água, identificações de metadados, métodos criptográficos para comprovar a proveniência e autenticidade do conteúdo, métodos de registo, impressões digitais ou outras técnicas, conforme seja adequado. Ao aplicar essa obrigação, os prestadores deverão ter igualmente em conta as especificidades e as limitações dos diferentes tipos de conteúdos e a evolução tecnológica e do mercado no terreno, tal como refletido no estado da arte geralmente reconhecido. Essas técnicas e métodos podem ser aplicados ao nível do sistema de IA ou ao nível do modelo de IA, incluindo modelos de IA de finalidade geral que geram conteúdos, facilitando assim o cumprimento desta obrigação pelo prestador a jusante do sistema de IA. É adequado prever que, para que se mantenha proporcionada, esta obrigação de marcação não deva abranger os sistemas de IA que desempenhem principalmente uma função de apoio à edição normalizada ou aos sistemas de IA que não alterem substancialmente os dados de entrada apresentados pelo responsável pela implantação nem a semântica dos mesmos.

(134) Além das soluções técnicas utilizadas pelos prestadores do sistema de IA, os responsáveis pela implantação que recorrem a um sistema de IA para gerar ou manipular conteúdos de imagem, áudio ou vídeo cuja semelhança considerável com pessoas, objetos, locais, entidades ou eventos reais possa levar uma pessoa a crer, erroneamente, que são autênticos ou verdadeiros («falsificações profundas»), deverão também revelar de forma clara e percetível que os conteúdos foram artificialmente criados ou manipulados, identificando os resultados da IA como tal e divulgando a sua origem artificial. O cumprimento desta obrigação de transparência não deverá ser interpretado como indicando que a utilização do sistema de IA ou dos seus resultados entrava o direito à liberdade de expressão e o direito à liberdade das artes e das ciências consagrados na Carta, em especial se os conteúdos fizerem parte de uma obra ou programa de natureza manifestamente criativa, satírica, artística, ficcional ou análoga, sob reserva de garantias adequadas dos direitos e liberdades de terceiros. Nesses casos, a obrigação de transparência para as falsificações profundas estabelecida no presente regulamento limita-se à divulgação da existência de tais conteúdos gerados ou manipulados, de uma forma adequada que não prejudique a exibição ou a fruição da obra, incluindo a sua exploração e utilização normais, mantendo simultaneamente a sua utilidade e qualidade. Além disso, é igualmente adequado prever uma obrigação semelhante de divulgação em relação ao texto gerado ou manipulado por IA, na medida em que seja publicado com o objetivo de informar o público sobre questões de interesse público, a menos que o conteúdo gerado por IA tenha sido submetido a um processo de análise ou controlo editorial humano e uma pessoa singular ou coletiva detenha a responsabilidade editorial pela publicação do conteúdo.

(135) Sem prejuízo da natureza obrigatória e da plena aplicabilidade das obrigações de transparência, a Comissão pode também incentivar e facilitar a elaboração de códigos de práticas a nível da União, a fim de facilitar a aplicação efetiva das obrigações em matéria de deteção e identificação de conteúdos artificialmente gerados ou manipulados, incluindo o apoio a disposições práticas para tornar acessíveis, se for caso disso, os mecanismos de deteção e facilitar a cooperação com outros intervenientes ao longo da cadeia de valor, a divulgação de conteúdos ou o controlo da sua autenticidade e proveniência, com vista a permitir que o público distinga eficazmente os conteúdos gerados por IA.

(136) A fim de facilitar a aplicação efetiva do Regulamento (UE) 2022/2065, as obrigações impostas por força do presente regulamento aos prestadores e responsáveis pela implantação de determinados sistemas de IA são particularmente pertinentes para permitir detetar e divulgar se os resultados desses sistemas são artificialmente gerados ou manipulados. Tal aplica-se, em especial, às obrigações dos prestadores de plataformas em linha de muito grande dimensão ou de motores de pesquisa em linha de muito grande dimensão que consistem em identificar e atenuar os riscos sistémicos que possam resultar da divulgação de conteúdos artificialmente gerados ou manipulados, em especial o risco de efeitos negativos reais ou previsíveis nos processos democráticos, no debate público e nos processos eleitorais, nomeadamente através da desinformação. O requisito de identificar conteúdos gerados por sistemas de IA nos termos do presente regulamento não prejudica a obrigação prevista no artigo 16.º, n.º 6, do Regulamento (UE) 2022/2065 de os prestadores de serviços de alojamento virtual procederem ao tratamento de notificações sobre conteúdos ilegais recebidas nos termos do artigo 16.º, n.º 1 desse regulamento, e não deverá influenciar a avaliação e a decisão sobre a ilegalidade dos conteúdos específicos. Essa avaliação deverá ser efetuada unicamente à luz das regras que regem a legalidade do conteúdo.

(137) O cumprimento das obrigações de transparência aplicáveis aos sistemas de IA abrangidas pelo presente regulamento não deverá ser interpretado como indicando que a utilização do sistema de IA ou dos seus resultados é lícita ao abrigo do presente regulamento ou de outra legislação da União e dos Estados-Membros e não deverá prejudicar outras obrigações de transparência dos responsáveis pela implantação de sistemas de IA estabelecidas no direito da União ou do direito nacional.

(138) A IA é uma família de tecnologias em rápida evolução que exige supervisão regulamentar e um espaço seguro e controlado para a experimentação, garantindo ao mesmo tempo uma inovação responsável e a integração de salvaguardas e medidas de atenuação dos riscos adequadas. Para assegurar um regime jurídico que promova a inovação, preparado para o futuro e resistente a perturbações, os Estados-Membros deverão assegurar que as respetivas autoridades nacionais competentes criem pelo menos um ambiente de testagem da regulamentação da IA a nível nacional que facilite o desenvolvimento e a testagem de sistemas de IA inovadores sob uma supervisão regulamentar rigorosa, antes de estes sistemas serem colocados no mercado ou colocados em serviço. Os Estados-Membros poderão também cumprir esta obrigação participando em ambientes de testagem da regulamentação já existentes ou criando conjuntamente um ambiente de testagem com uma ou mais autoridades competentes dos Estados-Membros, na medida em que essa participação proporcione um nível equivalente de cobertura nacional para os Estados-Membros participantes. Os ambientes de testagem da regulamentação da IA poderão ser criados sob forma física, digital ou híbrida e podem acolher produtos físicos e digitais. As autoridades responsáveis pela criação deverão também assegurar que os ambientes de testagem da regulamentação da IA dispõem dos recursos adequados para o seu funcionamento, nomeadamente recursos financeiros e humanos.

(139) Os ambientes de testagem da regulamentação da IA deverão ter os seguintes objetivos: fomentar a inovação no domínio da IA, mediante a criação de um ambiente controlado de experimentação e testagem na fase de desenvolvimento e pré-comercialização, com vista a assegurar que os sistemas de IA inovadores são conformes com o presente regulamento e com outras disposições pertinentes do direito da União e do direito nacional. Além disso, os ambientes de testagem da regulamentação da IA deverão visar melhorar a segurança jurídica para os inovadores, bem como a supervisão e compreensão, por parte das autoridades competentes, das oportunidades, dos riscos emergentes e dos impactos da utilização da IA, facilitar a aprendizagem da regulamentação para as autoridades e as empresas, nomeadamente com vista a futuras adaptações do regime jurídico, apoiar a cooperação e a partilha de boas práticas com as autoridades envolvidas no ambiente de testagem da regulamentação da IA, e acelerar o acesso aos mercados, nomeadamente eliminando os entraves para as PME, incluindo as empresas em fase de arranque. Os ambientes de testagem da regulamentação da IA deverão estar amplamente disponíveis em toda a União, devendo ser prestada especial atenção à sua acessibilidade para as PME, incluindo as empresas em fase de arranque. A participação nos ambientes de testagem da regulamentação da IA deverá centrar-se em problemas que criam incerteza jurídica para os prestadores e potenciais prestadores ao inovarem, fazerem experiências com a IA na União e contribuírem para uma aprendizagem regulamentar baseada em dados concretos. A supervisão dos sistemas de IA nos ambientes de testagem da regulamentação da IA deverá, por conseguinte, abranger o seu desenvolvimento, treino, testagem e validação antes de os sistemas serem colocados no mercado ou colocados em serviço, bem como a noção e a ocorrência de modificações substanciais que possam exigir um novo procedimento de avaliação da conformidade. A identificação de quaisquer riscos significativos durante o desenvolvimento e a testagem desses sistemas de IA deverá resultar na atenuação adequada dos riscos e, na sua falta, na suspensão do processo de desenvolvimento e testagem.

Se for caso disso, as autoridades nacionais competentes que criam ambientes de testagem da regulamentação da IA deverão cooperar com outras autoridades pertinentes, incluindo as que supervisionam a proteção dos direitos fundamentais, e poderão permitir a participação de outros intervenientes no ecossistema da IA, tais como organizações de normalização, organismos notificados, instalações de ensaio e experimentação, laboratórios de investigação e experimentação, polos europeus de inovação digital e organizações pertinentes das partes interessadas e da sociedade civil, quer nacionais quer europeus. Para garantir uma aplicação uniforme em toda a União e assegurar economias de escala, é apropriado criar regras comuns para a implantação dos ambientes de testagem da regulamentação da IA e um regime para a cooperação entre as autoridades competentes envolvidas na supervisão desses ambientes. Os ambientes de testagem da regulamentação da IA criados ao abrigo do presente regulamento não deverão prejudicar outras disposições pertinentes do direito que preveja a criação de outros ambientes de testagem destinados a assegurar o cumprimento do direito que não o presente regulamento. Se for caso disso, as autoridades competentes responsáveis por esses outros ambientes de testagem da regulamentação deverão ter em conta os benefícios da utilização desses ambientes de testagem também com o objetivo de assegurar a conformidade dos sistemas de IA com o presente regulamento. Mediante acordo entre as autoridades nacionais competentes e os participantes no ambiente de testagem da regulamentação da IA, a testagem em condições reais também pode ser efetuada e supervisionada no âmbito do ambiente de testagem da regulamentação da IA.

(140) O presente regulamento deverá estabelecer o fundamento jurídico para a utilização, pelos prestadores e potenciais prestadores no ambiente de testagem da regulamentação da IA, 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, apenas em condições específicas, em conformidade com o artigo 6.º, n.º 4, e artigo 9.º, n.º 2, alínea g), do Regulamento (UE) 2016/679 e com os artigos 5.º, 6.º e 10.º do Regulamento (UE) 2018/1725, e sem prejuízo do artigo 4.º, n.º 2, e do artigo 10.º da Diretiva (UE) 2016/680. Todas as outras obrigações dos responsáveis pelo tratamento de dados e todos os outros direitos dos titulares dos dados ao abrigo dos Regulamentos (UE) 2016/679 e (UE) 2018/1725 e da Diretiva (UE) 2016/680 continuam a ser aplicáveis. Em especial, o presente regulamento não deverá constituir uma base jurídica na aceção do artigo 22.º, n.º 2, alínea b), do Regulamento (UE) 2016/679 e do artigo 24.º, n.º 2, alínea b), do Regulamento (UE) 2018/1725. Os prestadores e potenciais prestadores no ambiente de testagem da regulamentação da IA deverão 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 adequadamente eventuais riscos significativos identificados para a segurança, a saúde e os direitos fundamentais que possam revelar-se durante o desenvolvimento, a testagem e a experimentação nesse ambiente de testagem.

(141) A fim de acelerar o processo de desenvolvimento e colocação no mercado dos sistemas de IA de risco elevado enumerados num anexo do presente regulamento, é importante que os prestadores ou potenciais prestadores desses sistemas também possam beneficiar de um regime específico para testar esses sistemas em condições reais, sem participarem num ambiente de testagem da regulamentação da IA. Contudo, nesses casos, tendo em conta as possíveis consequências dessas testagens para as pessoas singulares, deverá ser assegurado que o presente regulamento introduz garantias e condições adequadas e suficientes para os prestadores ou potenciais prestadores. Essas garantias deverão incluir, nomeadamente, o pedido de consentimento informado às pessoas singulares para participarem na testagem em condições reais, salvo no que respeita à aplicação da lei em que a tentativa de obtenção do consentimento informado impediria o sistema de IA de ser testado. O consentimento das pessoas singulares para participar nessa testagem ao abrigo do presente regulamento é distinto e sem prejuízo do consentimento dos titulares dos dados para o tratamento dos seus dados pessoais ao abrigo da legislação aplicável em matéria de proteção de dados.

É igualmente importante minimizar os riscos e permitir a supervisão pelas autoridades competentes e, por conseguinte, exigir que os potenciais prestadores tenham um plano de testagem em condições reais apresentado à autoridade de fiscalização do mercado competente, registar a testagem em secções específicas da base de dados da UE, sob reserva de algumas exceções limitadas, estabelecer limitações ao período durante o qual as testagens podem ser realizadas e exigir garantias adicionais para pessoas pertencentes a certos grupos vulneráveis, bem como um acordo escrito que defina as funções e responsabilidades dos potenciais prestadores e responsáveis pela implantação e uma supervisão eficaz por parte do pessoal competente envolvido na testagem em condições reais. Além disso, é conveniente prever salvaguardas adicionais para assegurar que as previsões, recomendações ou decisões do sistema de IA possam ser efetivamente revertidas e ignoradas e que os dados pessoais sejam protegidos e apagados quando os titulares tiverem retirado o seu consentimento para participar na testagem, sem prejuízo dos seus direitos enquanto titulares de dados ao abrigo da legislação da União em matéria de proteção de dados. No que diz respeito à transferência de dados, é igualmente conveniente prever que os dados recolhidos e tratados para efeitos de testagem em condições reais só sejam transferidos para países terceiros quando forem estabelecidas garantias adequadas e aplicáveis ao abrigo do direito da União, nomeadamente em conformidade com as bases para a transferência de dados pessoais nos termos do direito da União em matéria de proteção de dados, ao passo que, para os dados não pessoais, sejam estabelecidas garantias adequadas em conformidade com o direito da União, como os Regulamentos (UE) 2022/868[42] e (UE) 2023/2854[43]do Parlamento Europeu e do Conselho.

---

[42] Regulamento (UE) 2022/868 do Parlamento Europeu e do Conselho, de 30 de maio de 2022, relativo à governação europeia de dados e que altera o Regulamento (UE) 2018/1724 (Regulamento Governação de Dados) (JO L 152 de 3.6.2022, p. 1).

[43] Regulamento (UE) 2023/2854 do Parlamento Europeu e do Conselho, de 13 de dezembro de 2023, relativo a regras harmonizadas sobre o acesso equitativo aos dados e a sua utilização e que altera o Regulamento (UE) 2017/2394 e a Diretiva (UE) 2020/1828 (Regulamento dos Dados) (JO L, 2023/2854 de 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

(142) A fim de garantir que a IA conduza a resultados benéficos do ponto de vista social e ambiental, os Estados-Membros são incentivados a apoiar e promover a investigação e o desenvolvimento de soluções de IA em prol de resultados social e ambientalmente benéficos, tais como soluções baseadas na IA para aumentar a acessibilidade para as pessoas com deficiência, combater as desigualdades socioeconómicas ou cumprir as metas ambientais, através da afetação de recursos suficientes, incluindo financiamento público e da União e, se for caso disso e desde que os critérios de elegibilidade e seleção sejam cumpridos, tendo em conta, em especial, projetos que prossigam esses objetivos. Esses projetos deverão ser baseados no princípio da cooperação interdisciplinar entre criadores de IA, especialistas em matéria de desigualdade, não discriminação, acessibilidade e direitos do consumidor, ambientais e digitais, bem como do meio académico.

(143) A fim de promover e proteger a inovação, é importante ter em especial atenção os interesses das PME, incluindo as empresas em fase de arranque, que sejam prestadores e responsáveis pela implantação de sistemas de IA. Para esse efeito, os Estados-Membros deverão desenvolver iniciativas dirigidas a esses operadores, incluindo ações de sensibilização e comunicação de informações. Os Estados-Membros deverão proporcionar às PME, incluindo às empresas em fase de arranque, com sede social ou sucursal na União acesso prioritário aos ambientes de testagem da regulamentação da IA, desde que aquelas cumpram as condições de elegibilidade e os critérios de seleção e sem impedir que outros prestadores e potenciais prestadores tenham acesso aos ambientes de testagem, contanto que estejam preenchidas as mesmas condições e critérios. Os Estados-Membros deverão utilizar os canais existentes e, se for caso disso, criar novos canais específicos para comunicar com as PME, incluindo as empresas em fase de arranque, os responsáveis pela implantação, outros inovadores e, conforme adequado, as autoridades públicas locais, a fim de apoiar as PME ao longo da sua trajetória de desenvolvimento, facultando orientações e respondendo a perguntas sobre a aplicação do presente regulamento. Sempre que adequado, esses canais deverão trabalhar em conjunto para criar sinergias e assegurar a homogeneidade da sua orientação às PME, inclusive às empresas em fase de arranque, e aos responsáveis pela implantação. Paralelamente, os Estados-Membros deverão facilitar a participação das PME e de outras partes interessadas pertinentes nos processos de desenvolvimento de normalização. Além disso, os interesses e as necessidades específicos dos prestadores que são PME, incluindo empresas em fase de arranque, deverão ser tidos em conta quando os organismos notificados fixam as taxas a pagar pela avaliação da conformidade. A Comissão deverá avaliar periodicamente os custos de certificação e de conformidade para as PME, incluindo as empresas em fase de arranque, através de consultas transparentes, e deverá trabalhar com os Estados-Membros para baixar esses custos.

Por exemplo, os custos de tradução associados à documentação obrigatória e à comunicação com as autoridades podem constituir um encargo substancial para os prestadores e outros operadores, nomeadamente para os prestadores de menor dimensão. Os Estados-Membros deverão eventualmente assegurar que uma das línguas por si determinadas e aceites para a documentação pertinente dos prestadores e para a comunicação com os operadores seja uma língua amplamente compreendida pelo maior número possível de responsáveis pela implantação transfronteiriça. A fim de dar resposta às necessidades específicas das PME, incluindo as empresas em fase de arranque, a Comissão deverá disponibilizar modelos normalizados para os domínios abrangidos pelo presente regulamento, a pedido do Comité para a IA. Além disso, a Comissão deverá complementar os esforços dos Estados-Membros, disponibilizando uma plataforma única de informação com informações de fácil utilização sobre o presente regulamento para todos os prestadores e responsáveis pela implantação, organizando campanhas de comunicação adequadas para sensibilizar para as obrigações decorrentes do presente regulamento e avaliando e promovendo a convergência das melhores práticas em procedimentos de contratação pública relacionados com sistemas de IA. As empresas de média dimensão que eram até recentemente consideradas como de pequena dimensão, na aceção do anexo da Recomendação 2003/361/CE[44] da Comissão, deverão ter acesso a essas medidas de apoio, uma vez que essas novas empresas de média dimensão podem, por vezes, não dispor dos recursos jurídicos e da formação necessários para assegurar a compreensão e o cumprimento adequados do presente regulamento.

[44] 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).

(144) A fim de promover e proteger a inovação, a plataforma IA a pedido, todos os programas e projetos de financiamento pertinentes da União – como o Programa Europa Digital e o Horizonte Europa – executados pela Comissão e pelos Estados-Membros a nível da União ou a nível nacional deverão, conforme o caso, contribuir para a consecução dos objetivos do presente regulamento.

(145) A fim de minimizar os riscos para a aplicação resultantes da falta de conhecimentos e competências especializadas no mercado, bem como para facilitar o cumprimento, por parte dos prestadores, nomeadamente das PME, incluindo as empresas em fase de arranque, 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 da União ou a nível nacional poderão eventualmente contribuir para a aplicação do presente regulamento. No âmbito da respetiva missão e domínios de competência, a plataforma de IA a pedido, os polos europeus de inovação digital e as instalações de ensaio e experimentação podem prestar, em particular, apoio técnico e científico aos prestadores e aos organismos notificados.

(146) Além disso, tendo em conta a dimensão muito reduzida de alguns operadores e a fim de assegurar a proporcionalidade no que diz respeito aos custos da inovação, é conveniente permitir que as microempresas satisfaçam uma das obrigações mais onerosas, designadamente o estabelecimento de um sistema de gestão da qualidade, de uma forma simplificada que reduza os seus encargos administrativos e custos, sem afetar o nível de proteção nem a necessidade de cumprir os requisitos aplicáveis aos sistemas de IA de risco elevado. A Comissão deverá elaborar orientações para especificar os elementos do sistema de gestão da qualidade a cumprir desta forma simplificada pelas microempresas.

(147) É apropriado que a Comissão facilite, tanto quanto possível, o acesso a instalações de ensaio 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. É este o caso, nomeadamente, dos painéis de peritos, dos laboratórios especializados e dos laboratórios de referência no domínio dos dispositivos médicos, nos termos dos Regulamentos (UE) 2017/745 e (UE) 2017/746.

(148) O presente regulamento deverá estatuir um modelo de governação que permita coordenar e apoiar a aplicação do presente regulamento a nível nacional, bem como criar capacidades a nível da União e integrar as partes interessadas no domínio da IA. A aplicação e execução efetivas do presente regulamento exigem um modelo de governação que permita coordenar e desenvolver conhecimentos especializados centrais a nível da União. O Serviço para a IA foi criado por decisão da Comissão[45] e tem como missão desenvolver os conhecimentos especializados e as capacidades da União no domínio da IA e contribuir para a aplicação da legislação da União em matéria de IA. Os Estados-Membros deverão facilitar o desempenho das funções do Serviço para a IA com vista a apoiar o desenvolvimento dos conhecimentos especializados e das capacidades da União a nível da União e a reforçar o funcionamento do mercado único digital. Além disso, deverá ser criado um Comité composto por representantes dos Estados-Membros, um painel científico que integre a comunidade científica e um fórum consultivo que permita às partes interessadas darem o seu contributo para a aplicação do presente regulamento, tanto a nível da União como nacional. O desenvolvimento dos conhecimentos especializados e das capacidades da União deverão também incluir a utilização dos recursos e conhecimentos especializados existentes, nomeadamente através de sinergias com estruturas criadas no contexto da aplicação a nível da União de outra lei e de sinergias com iniciativas conexas a nível da União, como a Empresa Comum para a Computação Europeia de Alto Desempenho e as instalações de ensaio e experimentação no domínio da IA no âmbito do Programa Europa Digital.

[45] Decisão da Comissão, de 24.1.2024, que cria o Serviço Europeu para a Inteligência Artificial, C (2024) 390.

(149) A fim de facilitar uma aplicação simples, eficaz e harmoniosa do presente regulamento, deverá ser criado um Comité. O Comité deverá refletir os vários interesses do ecossistema de IA e ser composto por representantes dos Estados-Membros. O Comité deverá ser responsável por uma série de funções consultivas, nomeadamente a emissão de pareceres, recomendações e conselhos, ou o contributo para orientações em questões relacionadas com a aplicação do presente regulamento, inclusive no tocante a questões de execução, especificações técnicas ou normas existentes relativas aos requisitos estabelecidos no presente regulamento, e a prestação de aconselhamento à Comissão a aos Estados--Membros e respetivas autoridades nacionais competentes sobre questões específicas relacionadas com a IA. A fim de dar alguma flexibilidade aos Estados-Membros na designação dos seus representantes no Comité, esses representantes podem ser quaisquer pessoas pertencentes a entidades públicas que deverão ter as competências e os poderes pertinentes para facilitar a coordenação a nível nacional e contribuir para o desempenho das funções do Comité. O Comité deverá criar dois subgrupos permanentes a fim de proporcionar uma plataforma de cooperação e intercâmbio entre as autoridades de fiscalização do mercado e as autoridades notificadoras sobre questões relacionadas, respetivamente, com a fiscalização do mercado e os organismos notificados. O subgrupo permanente para a fiscalização do mercado deverá atuar como grupo de cooperação administrativa (ADCO) para efeitos do presente regulamento, na aceção do artigo 30.º do Regulamento (UE) 2019/1020. Em consonância com o artigo 33.º do referido Regulamento, a Comissão deverá apoiar as atividades do subgrupo permanente para a fiscalização do mercado, realizando avaliações ou estudos de mercado, nomeadamente com vista a identificar aspetos do presente regulamento que exijam uma coordenação específica e urgente entre as autoridades de fiscalização do mercado. O Comité pode constituir outros subgrupos permanentes ou temporários consoante adequado para efeitos da análise de questões específicas. O Comité deverá também cooperar, se for caso disso, com os organismos, grupos de peritos e redes pertinentes da União ativos no contexto de outras disposições pertinentes do direito da União, incluindo, em especial, os que operam ao abrigo do direito pertinente da União em matéria de dados, produtos e serviços digitais.

(150) A fim de assegurar a participação das partes interessadas na execução e aplicação do presente regulamento, deverá ser criado um fórum consultivo para aconselhar e disponibilizar conhecimentos técnicos especializados ao Comité e à Comissão. A fim de assegurar uma representação variada e equilibrada das partes interessadas entre interesses comerciais e não comerciais e, dentro da categoria de interesses comerciais, no que diz respeito às PME e a outras empresas, o fórum consultivo deverá englobar, nomeadamente, a indústria, as empresas em fase de arranque, as PME, o meio académico, a sociedade civil, incluindo os parceiros sociais, bem como a Agência dos Direitos Fundamentais, a ENISA, o Comité Europeu de Normalização (CEN), o Comité Europeu de Normalização Eletrotécnica (CENELEC) e o Instituto Europeu de Normalização das Telecomunicações (ETSI).

(151) A fim de apoiar a aplicação e a execução do presente regulamento, em especial as atividades de acompanhamento do Serviço para a IA no que diz respeito aos modelos de IA de finalidade geral, deverá ser criado um painel científico de peritos independentes. Os peritos independentes que constituem o painel científico deverão ser selecionados com base em conhecimentos científicos ou técnicos atualizados no domínio da IA e deverão desempenhar as suas funções com imparcialidade e objetividade e assegurar a confidencialidade das informações e dos dados obtidos no desempenho das suas funções e atividades. A fim de permitir o reforço das capacidades nacionais necessárias para a execução efetiva do presente regulamento, os Estados-Membros deverão poder solicitar o apoio do grupo de peritos que constituem o painel científico para as suas atividades de execução.

(152) A fim de apoiar a execução adequada dos sistemas de IA e reforçar as capacidades dos Estados-Membros, deverão ser criadas e disponibilizadas aos Estados-Membros estruturas da União de apoio à testagem de IA.

(153) Os Estados-Membros desempenham um papel fundamental na aplicação e execução do presente regulamento. Nesse sentido, cada Estado-Membro deverá designar pelo menos uma autoridade notificadora e pelo menos uma autoridade de fiscalização do mercado como autoridades nacionais competentes do mercado para efeitos de supervisão da aplicação e execução do presente regulamento. Os Estados-Membros podem decidir nomear qualquer tipo de entidade pública para desempenhar as funções das autoridades nacionais competentes na aceção do presente regulamento, de acordo com as suas características e necessidades específicas em matéria de organização nacional. A fim de aumentar a eficácia organizativa dos Estados-Membros e de criar um ponto de contacto oficial único para o público e as outras contrapartes a nível dos Estados-Membros e da União, cada Estado-Membro deverá designar uma autoridade de fiscalização do mercado que atue como um ponto de contacto único.

(154) As autoridades nacionais competentes deverão exercer os seus poderes de forma independente, imparcial e sem enviesamentos, a fim de salvaguardar os princípios da objetividade das suas atividades e funções e de assegurar a aplicação e execução do presente regulamento. Os membros dessas autoridades deverão abster-se de qualquer ato incompatível com as suas funções e estar sujeitos às regras de confidencialidade previstas no presente regulamento.

(155) Para assegurar que os prestadores 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 eventuais medidas corretivas em tempo útil, todos os prestadores deverão dispor de um sistema de acompanhamento pós-comercialização. Se for caso disso, o acompanhamento pós-comercialização deverá incluir uma análise da interação com outros sistemas de IA, incluindo outros dispositivos e software. O acompanhamento pós-comercialização não deverá abranger os dados operacionais sensíveis dos responsáveis pela implantação que sejam autoridades responsáveis pela aplicação da lei. 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 colocados em serviço. Neste contexto, os prestadores também deverão ser obrigados a dispor de um sistema para comunicar às autoridades competentes quaisquer incidentes graves resultantes da utilização dos seus sistemas de IA, ou seja, incidentes ou anomalias que conduzam à morte ou a danos graves para a saúde, perturbações graves e irreversíveis da gestão e do funcionamento de infraestruturas críticas, violações das obrigações decorrentes do direito da União destinadas a proteger os direitos fundamentais ou danos graves à propriedade ou ao ambiente.

(156) Para assegurar uma execução adequada e eficaz dos requisitos e obrigações estabelecidos 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 deverá ser aplicado na íntegra. As autoridades de fiscalização do mercado designadas nos termos do presente regulamento deverão dispor de todos os poderes de execução estabelecidos no presente regulamento e no Regulamento (UE) 2019/1020 e deverão exercer os seus poderes e desempenhar as suas funções de forma independente, imparcial e objetiva. Embora a maioria dos sistemas de IA não esteja sujeita a requisitos e obrigações específicos nos termos do presente regulamento, as autoridades de fiscalização do mercado podem tomar medidas em relação a todos os sistemas de IA que apresentem um risco em conformidade com o presente regulamento. Dada a natureza específica das instituições, órgãos e organismos da União abrangidos pelo âmbito de aplicação do presente regulamento, é conveniente designar a Autoridade Europeia para a Proteção de Dados como autoridade de fiscalização do mercado competente relativamente a essas instituições, órgãos e organismos. Tal não deverá prejudicar a designação das autoridades nacionais competentes pelos Estados-Membros. As atividades de fiscalização do mercado não deverão afetar a capacidade das entidades supervisionadas de desempenharem as suas funções de forma independente, quando essa independência for exigida pelo direito da União.

(157) O presente regulamento não prejudica as competências, as atribuições, os poderes nem a independência das autoridades ou organismos públicos nacionais competentes que supervisionam a aplicação do direito da União que protege direitos fundamentais, incluindo os organismos de promoção da igualdade e as autoridades de proteção de dados. Quando tal for necessário ao cumprimento do seu mandato, essas autoridades ou organismos públicos nacionais deverão também ter acesso à documentação elaborada por força do presente regulamento. Deverá ser estabelecido um procedimento de salvaguarda específico para assegurar uma aplicação adequada e atempada relativamente aos sistemas de IA que apresentem um risco para a saúde, a segurança e os direitos fundamentais. O procedimento aplicável a esses sistemas de IA que apresentam um risco deverá ser aplicado aos sistemas de IA de risco elevado que apresentem um risco, aos sistemas proibidos que tenham sido colocados no mercado, colocados em serviço ou utilizados em violação das disposições respeitantes a práticas proibidas estabelecidas no presente regulamento e aos sistemas de IA que tenham sido disponibilizados em violação dos requisitos de transparência estabelecidos no presente regulamento e que apresentem um risco.

(158) A legislação da União no domínio dos 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, inclusive 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 dos atos legais da União aplicáveis aos serviços financeiros, as autoridades competentes responsáveis pela supervisão e execução desses atos jurídicos, nomeadamente as autoridades competentes na aceção do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho[46] e as Diretivas 2008/48/CE[47], 2009/138/CE[48], 2013/36/UE[49], 2014/17/UE[50] e (UE) 2016/97[51] do Parlamento Europeu e do Conselho, deverão ser designadas, no âmbito das respetivas competências, 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 disponibilizados ou utilizados por instituições financeiras regulamentadas e supervisionadas, salvo se os Estados-Membros decidirem designar outra autoridade para desempenhar essas funções de fiscalização do mercado.

---

46 Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento e que altera o Regulamento (UE) n.º 648/2012 (JO L 176 de 27.6.2013, p. 1).

47 Diretiva 2008/48/CE do Parlamento Europeu e do Conselho, de 23 de abril de 2008, relativa a contratos de crédito aos consumidores e que revoga a Diretiva 87/102/CEE do Conselho, JO L 133 de 22.5.2008, p. 66.

48 Diretiva 2009/138/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, relativa ao acesso à atividade de seguros e resseguros e ao seu exercício (Solvência II) (JO L 335 de 17.12.2009, p. 1).

49 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).

50 Diretiva 2014/17/UE do Parlamento Europeu e do Conselho, de 4 de fevereiro de 2014, relativa aos contratos de crédito aos consumidores para imóveis de habitação e que altera as Diretivas 2008/48/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010 (JO L 60 de 28.2.2014, p. 34).

51 Diretiva (UE) 2016/97 do Parlamento Europeu e do Conselho, de 20 de janeiro de 2016, sobre a distribuição de seguros (JO L 26 de 2.2.2016, p. 19).

Essas autoridades competentes deverão dispor de todos os poderes ao abrigo do presente regulamento e do Regulamento (UE) 2019/1020 para fazer cumprir os requisitos e obrigações do presente regulamento, incluindo poderes para levar a cabo atividades de fiscalização do mercado *ex post* que possam ser integradas, se for caso disso, nos seus mecanismos e procedimentos de supervisão existentes ao abrigo do direito da União aplicável no domínio dos serviços financeiros. É apropriado definir que, ao atuarem como autoridades de fiscalização do mercado ao abrigo do presente regulamento, as autoridades nacionais responsáveis por supervisionar as instituições de crédito regulamentadas pela Diretiva 2013/36/UE, que participam no Mecanismo Único de Supervisão estabelecido pelo Regulamento (UE) n.º 1024/2013 do Conselho[52], deverão comunicar sem demora ao Banco Central Europeu todas as informações identificadas no âmbito das suas atividades de fiscalização do mercado que possam ser de interesse potencial para as atribuições de supervisão prudencial do Banco Central Europeu especificadas nesse regulamento. A fim de reforçar a coerência entre o presente regulamento e as regras aplicáveis às instituições de crédito regulamentadas pela Diretiva 2013/36/UE, também é apropriado integrar algumas das obrigações processuais dos prestadores relativas à gestão de riscos, ao acompanhamento pós-comercialização e à documentação nas obrigações e procedimentos em vigor por força da referida diretiva. No intuito de evitar sobreposições, também deverão ser previstas derrogações limitadas no respeitante ao sistema de gestão da qualidade dos prestadores e à obrigação de controlo imposta aos responsáveis pela implantação de sistemas de IA de risco elevado, contanto que tal se aplique a instituições de crédito regulamentadas pela Diretiva 2013/36/UE. Deverá aplicar-se o mesmo regime às empresas de seguros e de resseguros e às sociedades gestoras de participações no setor dos seguros nos termos da Diretiva 2009/138/CE, aos mediadores de seguros nos termos da Diretiva (UE) 2016/97 e a outros tipos de instituições financeiras sujeitas a requisitos em matéria governação, mecanismos ou processos internos estabelecidos nos termos do direito da União aplicável no domínio dos serviços financeiros, a fim de assegurar a coerência e a igualdade de tratamento no setor financeiro.

---

52 Regulamento (UE) n.º 1024/2013 do Conselho, de 15 de outubro de 2013, que confere ao BCE atribuições específicas no que diz respeito às políticas relativas à supervisão prudencial das instituições de crédito (JO L 287 de 29.10.2013, p. 63).

(159) Todas as autoridades de fiscalização do mercado dos sistemas de IA de risco elevado enumerados no domínio da biométrica, conforme enumerado num anexo do presente regulamento, na medida em que esses sistemas sejam utilizados para fins de aplicação da lei, da migração, do asilo e da gestão do controlo das fronteiras, ou para a administração da justiça e processos democráticos, deverão dispor de poderes de investigação e de correção eficazes, incluindo, pelo menos, o poder de aceder a todos os dados pessoais que estão a ser tratados e a todas as informações necessárias ao desempenho das suas funções. As autoridades de fiscalização do mercado deverão poder exercer os seus poderes atuando com total independência. Quaisquer limitações ao seu acesso a dados operacionais sensíveis nos termos do presente regulamento não deverão prejudicar os poderes que lhes são conferidos pela Diretiva (UE) 2016/680. Nenhuma exclusão da divulgação de dados às autoridades nacionais de proteção de dados ao abrigo do presente regulamento deverá afetar os atuais ou futuros poderes dessas autoridades fora do âmbito de aplicação do presente regulamento.

(160) As autoridades de fiscalização do mercado e a Comissão deverão poder propor atividades conjuntas, incluindo investigações conjuntas, a realizar quer pelas autoridades de fiscalização do mercado quer pelas autoridades de fiscalização do mercado em conjunto com a Comissão, que tenham por objetivo promover a conformidade, identificar situações de não conformidade, sensibilizar e disponibilizar orientações em relação ao presente regulamento no que diz respeito a categorias específicas de sistemas de IA de risco elevado consideradas como apresentando um risco grave em dois ou mais Estados-Membros. As atividades conjuntas para promover a conformidade deverão ser realizadas em conformidade com o artigo 9.º do Regulamento (UE) 2019/1020. O Serviço para a IA deverá prestar apoio à coordenação de investigações conjuntas.

(161) É necessário clarificar as responsabilidades e competências a nível da União e a nível nacional no que diz respeito aos sistemas de IA que se baseiam em modelos de IA de finalidade geral. A fim de evitar a sobreposição de competências, sempre que um sistema de IA se baseie num modelo de IA de finalidade geral e o modelo e o sistema sejam disponibilizados pelo mesmo prestador, a supervisão deverá ter lugar a nível da União através do Serviço para a IA, o qual deverá ter os poderes de uma autoridade de fiscalização do mercado na aceção do Regulamento (UE) 2019/1020 para esse efeito. Em todos os outros casos, os responsáveis pela supervisão dos sistemas de IA continuam a ser as autoridades nacionais de fiscalização do mercado. No entanto, para os sistemas de IA de finalidade geral que possam ser utilizados diretamente pelos responsáveis pela implantação para, pelo menos, uma finalidade classificada como sendo de risco elevado, as autoridades de fiscalização do mercado deverão cooperar com o Serviço para a IA na realização de avaliações da conformidade e informar o Comité e outras autoridades de fiscalização do mercado em conformidade. Além disso, as autoridades de fiscalização do mercado deverão poder solicitar assistência ao Serviço para a IA sempre que a autoridade de fiscalização do mercado não seja capaz de concluir uma investigação sobre um sistema de IA de risco elevado devido à sua impossibilidade de aceder a determinadas informações relacionadas com o modelo de IA de finalidade geral no qual o sistema de IA de risco elevado se baseia. Nesses casos, o procedimento relativo à assistência mútua em casos transfronteiriços previsto no capítulo VI do Regulamento (UE) 2019/1020 deverá aplicar-se *mutatis mutandis*.

(162) A fim de utilizar da melhor forma os conhecimentos especializados centralizados da União e as sinergias a nível da União, os poderes de supervisão e execução das obrigações dos prestadores de modelos de IA de finalidade geral deverão ser da competência da Comissão. O Serviço para a IA deverá poder realizar todas as ações necessárias para acompanhar a execução efetiva do presente regulamento no que diz respeito aos modelos de IA de finalidade geral. Deverá poder investigar eventuais infrações às regras aplicáveis aos prestadores de modelos de IA de finalidade geral, tanto por sua própria iniciativa, na sequência dos resultados das suas atividades de acompanhamento, como a pedido das autoridades de fiscalização do mercado, em conformidade com as condições estabelecidas no presente regulamento. A fim de apoiar um acompanhamento eficaz do Serviço para a IA, este deverá prever a possibilidade de os prestadores a jusante apresentarem queixas sobre possíveis infrações às regras aplicáveis aos prestadores de modelos e sistemas de IA de finalidade geral.

(163) Com vista a complementar os sistemas de governação aplicáveis a modelos de IA de finalidade geral, o painel científico deverá apoiar as atividades de acompanhamento do Serviço para a IA e pode, em certos casos, emitir alertas qualificados ao Serviço para a IA que desencadeiem seguimentos, como investigações. Tal deverá ser o caso se o painel científico tiver razões para suspeitar que um modelo de IA de finalidade geral representa um risco concreto e identificável a nível da União. Além disso, deverá ser esse o caso se o painel científico tiver motivos para suspeitar que um modelo de IA de finalidade geral cumpre os critérios que conduziriam a uma classificação como modelo de IA de finalidade geral com risco sistémico. A fim de dotar o painel científico das informações necessárias para o desempenho dessas funções, deverá existir um mecanismo através do qual o painel científico possa solicitar à Comissão que exija documentação ou informações a um prestador.

(164) O Serviço para a IA deverá poder tomar as medidas necessárias para fiscalizar a execução efetiva e o cumprimento das obrigações dos prestadores de modelos de IA de finalidade geral estabelecidas no presente regulamento. O Serviço para a IA deverá poder investigar eventuais infrações em conformidade com os poderes previstos no presente regulamento, nomeadamente solicitando documentação e informações, realizando avaliações, bem como solicitando medidas aos prestadores de modelos de IA de finalidade geral. Na realização das avaliações, a fim de recorrer a conhecimentos especializados independentes, o Serviço para a IA deverá poder envolver peritos independentes para realizar as avaliações em seu nome. O cumprimento das obrigações deverá ser executório, nomeadamente através de pedidos de adoção de medidas adequadas, incluindo medidas de redução dos riscos em caso de riscos sistémicos identificados, bem como através da restrição da disponibilização no mercado, da retirada ou da recolha do modelo. A título de salvaguarda, sempre que seja necessário para além dos direitos processuais previstos no presente regulamento, os prestadores de modelos de IA de finalidade geral deverão gozar dos direitos processuais previstos no artigo 18.º do Regulamento (UE) 2019/1020, que deverão ser aplicáveis *mutatis mutandis*, sem prejuízo de direitos processuais mais específicos previstos no presente regulamento.

(165) 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 IA ética e de confiança na União. Os prestadores de sistemas de IA que não sejam de risco elevado deverão ser incentivados a criar códigos de conduta, incluindo mecanismos de governação conexos, destinados a promover a aplicação voluntária de alguns ou de todos os requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado, adaptados à finalidade prevista dos sistemas e ao menor risco envolvido e tendo em conta as soluções técnicas disponíveis e as boas práticas da indústria, como modelos e cartões de dados. Os prestadores e, se for caso disso, os responsáveis pela implantação de todos os sistemas de IA, de risco elevado ou não, e dos modelos de IA deverão também ser incentivados a aplicar, numa base voluntária, requisitos adicionais relacionados, por exemplo, com os elementos das Orientações Éticas da União para uma IA de Confiança, a sustentabilidade ambiental, as medidas de literacia no domínio da IA, a conceção e o desenvolvimento inclusivos e diversificados de sistemas de IA, incluindo a atenção às pessoas vulneráveis e a acessibilidade das pessoas com deficiência, a participação das partes interessadas com a participação, conforme adequado, das partes interessadas pertinentes, como as organizações empresariais e da sociedade civil, o meio académico, as organizações de investigação, os sindicatos e as organizações de defesa dos consumidores na conceção e desenvolvimento de sistemas de IA, e a diversidade das equipas de desenvolvimento, incluindo o equilíbrio entre homens e mulheres. A fim de assegurar que sejam eficazes, os códigos de conduta voluntários deverão basear-se em objetivos claros e em indicadores-chave de desempenho para medir a consecução desses objetivos. Deverão também ser desenvolvidos de forma inclusiva, conforme adequado, com a participação das partes interessadas pertinentes, como as organizações empresariais e da sociedade civil, o meio académico, as organizações de investigação, os sindicatos e as organizações de defesa dos consumidores. A Comissão pode desenvolver iniciativas, nomeadamente de natureza setorial, para facilitar a redução de obstáculos técnicos que impeçam o intercâmbio transfronteiriço de dados para o desenvolvimento da IA, inclusive em matéria de infraestruturas de acesso aos dados e de interoperabilidade semântica e técnica dos diferentes tipos de dados.

(166) 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 aplicáveis a sistemas de IA de risco elevado, sejam seguros quando são colocados no mercado ou colocados em serviço. A fim de contribuir para alcançar esse objetivo, o Regulamento (UE) 2023/988 do Parlamento Europeu e do Conselho[53] deverá ser aplicado como uma rede de segurança.

(167) 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 deverão respeitar a confidencialidade das informações e dos dados obtidos no exercício das suas funções, em conformidade com o direito da União ou o direito nacional. Deverão desempenhar as suas funções e atividades de modo a proteger, em especial, os direitos de propriedade intelectual, as informações comerciais de caráter confidencial e os segredos comerciais, a execução efetiva do presente regulamento, os interesses públicos e nacionais em matéria de segurança, a integridade dos processos penais e administrativos e a integridade das informações classificadas.

---

[53] Regulamento (UE) 2023/988 do Parlamento Europeu e do Conselho, de 10 de maio de 2023, relativo à segurança geral dos produtos, que altera o Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho e a Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho e que revoga a Diretiva 2001/95/CE do Parlamento Europeu e do Conselho e a Diretiva 87/357/CEE do Conselho (JO L 135 de 23.5.2023, p. 1).

(168) O cumprimento do presente regulamento deverá ter força executória através da imposição de sanções e de outras medidas de execução. Os Estados-Membros deverão tomar todas as medidas necessárias para assegurar a aplicação das disposições do presente regulamento, inclusive estabelecendo sanções efetivas, proporcionadas e dissuasivas aplicáveis em caso de violação dessas disposições, e a respeito do princípio *ne bis in idem*. A fim de reforçar e harmonizar as sanções administrativas em caso de infração ao presente regulamento, deverão ser estabelecidos os limites máximos para a fixação de coimas para determinadas infrações específicas. Ao avaliar o montante das coimas, os Estados-Membros deverão, em cada caso individual, ter em conta todas as circunstâncias relevantes da situação específica, prestando a devida atenção à natureza, à gravidade e à duração da infração e às suas consequências, bem como à dimensão do prestador, em particular se o prestador for uma PME, incluindo uma empresa em fase de arranque. A Autoridade Europeia para a Proteção de Dados deverá ter competências para impor coimas às instituições, órgãos e organismos da União que se enquadram no âmbito do presente regulamento.

(169) O cumprimento das obrigações impostas aos prestadores de modelos de IA de finalidade geral nos termos do presente regulamento deverá ter força executória, nomeadamente, através de coimas. Para o efeito, deverão também ser estabelecidos níveis adequados de coimas em caso de infração dessas obrigações, incluindo o incumprimento das medidas solicitadas pela Comissão nos termos do presente regulamento, sob reserva de prazos de prescrição adequados, de acordo com o princípio da proporcionalidade. Todas as decisões tomadas pela Comissão ao abrigo do presente regulamento estão sujeitas a fiscalização pelo Tribunal de Justiça da União Europeia nos termos do TFUE, incluindo a plena jurisdição do Tribunal de Justiça da União Europeia no que diz respeito às sanções nos termos do artigo 261.º do TFUE.

(170) O direito da União e o direito nacional já preveem vias de recurso eficazes para as pessoas singulares e coletivas cujos direitos e liberdades sejam afetados negativamente pela utilização de sistemas de IA. Sem prejuízo dessas vias, qualquer pessoa singular ou coletiva que tenha motivos para considerar que houve uma infração do presente regulamento deverá ter o direito de apresentar uma queixa à autoridade de fiscalização do mercado competente.

(171) As pessoas afetadas deverão ter o direito de obter explicações quando uma decisão do responsável pela implantação tenha por base principalmente os resultados de determinados sistemas de IA de risco elevado abrangidos pelo âmbito de aplicação do presente regulamento, e quando essa decisão produzir efeitos jurídicos ou analogamente afetar num grau significativo essas pessoas, de uma forma que considerem ter repercussões negativas na sua saúde, segurança ou direitos fundamentais. Essas explicações deverão ser claras e pertinentes e constituir uma base sobre a qual as pessoas afetadas possam exercer os seus direitos. O direito à obtenção de explicações não deverá aplicar-se à utilização de sistemas de IA para os quais decorram do direito da União ou do direito nacional exceções ou restrições e deverá aplicar-se apenas na medida em que não esteja já previsto no direito da União.

(172) As pessoas que atuam como denunciantes de infrações ao presente regulamento deverão ser protegidas ao abrigo do direito da União. A Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho[54] deverá, por conseguinte, aplicar-se à denúncia de infrações ao presente regulamento e à proteção das pessoas que denunciam essas infrações.

---

[54] Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho, de 23 de outubro de 2019, relativa à proteção das pessoas que denunciam violações do direito da União (JO L 305 de 26.11.2019, p. 17).

(173) A fim de assegurar que o regime regulamentar possa ser adaptado sempre que necessário, o poder de adotar atos nos termos do artigo 290.º do TFUE deverá ser delegado na Comissão para que possa alterar as condições nas quais um sistema de IA não é para ser considerado de risco elevado, a lista dos sistemas de IA de risco elevado, as disposições relativas à documentação técnica, o conteúdo da declaração UE de conformidade, as disposições relativas aos procedimentos de avaliação da conformidade, as disposições que estabelecem os sistemas de IA de risco elevado aos quais se deverá aplicar o procedimento de avaliação da conformidade baseado na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica, o limiar e os parâmetros de referência e os indicadores, inclusive complementando esses parâmetros de referência e indicadores, nas regras para a classificação de modelos de IA de finalidade geral com risco sistémico, os critérios para a designação de modelos de IA de finalidade geral com risco sistémico, a documentação técnica para os prestadores de modelos de IA de finalidade geral e informações em matéria de transparência para os prestadores de modelos de IA de finalidade geral. 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[55]. 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.

[55] JO L 123 de 12.5.2016, p. 1.

(174) Tendo em conta a rápida evolução tecnológica e os conhecimentos técnicos necessários para a aplicação efetiva do presente regulamento, a Comissão deverá avaliar e rever o presente regulamento até … [cinco anos a contar da data de entrada em vigor do presente regulamento] e, posteriormente, de quatro em quatro anos, e apresentar um relatório ao Parlamento Europeu e ao Conselho. Além disso, tendo em conta as implicações para o âmbito de aplicação do presente regulamento, uma vez por ano a Comissão deverá efetuar uma avaliação da necessidade de alterar a lista de sistemas de IA de risco elevado e a lista de práticas proibidas. Além disso, até … [quatro anos a contar da data de entrada em vigor do presente regulamento] e, posteriormente, de quatro em quatro anos, a Comissão deverá avaliar e apresentar um relatório ao Parlamento Europeu e ao Conselho sobre a necessidade de alterar os a lista de domínios de risco elevado do anexo do presente regulamento, os sistemas de IA abrangidos pelas obrigações de transparência, a eficácia do sistema de supervisão e governação e os progressos realizados no desenvolvimento de produtos de normalização sobre o desenvolvimento eficiente do ponto de vista energético de modelos de IA de finalidade geral, incluindo a necessidade de medidas ou ações adicionais. Por fim, até ... [quatro anos a contar da data de entrada em vigor do presente regulamento] e, posteriormente, de três em três anos, a Comissão deverá avaliar o impacto e a eficácia dos códigos de conduta voluntários, a fim de fomentar a aplicação dos requisitos estabelecidos para sistemas de IA de risco elevado a sistemas de IA que não sejam de risco elevado e, possivelmente, de outros requisitos adicionais para esses sistemas de IA.

(175) 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[56].

(176) Atendendo a que o objetivo do presente regulamento, a saber, melhorar o funcionamento do mercado interno e promover a adoção de uma IA centrada no ser humano e de confiança, assegurando simultaneamente um elevado nível de proteção da saúde, da segurança e dos direitos fundamentais consagrados na Carta, incluindo a democracia, o Estado de direito e a proteção do ambiente contra os efeitos nocivos dos sistemas de IA na União e apoiando a inovação, não pode ser suficientemente alcançado pelos Estados-Membros mas 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. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar esse objetivo.

---

[56] 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).

(177) A fim de garantir a segurança jurídica, assegurar um período de adaptação adequado para os operadores e evitar perturbações do mercado, nomeadamente assegurando a continuidade da utilização dos sistemas de IA, é conveniente que o presente regulamento só seja aplicável aos sistemas de IA de risco elevado que tenham sido colocados no mercado ou colocados em serviço antes da data geral de aplicação do mesmo, se, a partir dessa data, esses sistemas sofrerem alterações significativas na sua conceção ou finalidade prevista. É conveniente clarificar que, a este respeito, o conceito de alteração significativa deverá ser entendido como equivalente, em substância, ao conceito de modificação substancial, que é utilizado apenas no que diz respeito aos sistemas de IA de risco elevado, nos termos do presente regulamento. A título excecional e à luz da responsabilização pública, os operadores de sistemas de IA que são componentes dos sistemas informáticos de grande escala estabelecidos pelos atos jurídicos enumerados num anexo do presente regulamento e os operadores de sistemas de IA de risco elevado concebidos para serem utilizados por autoridades públicas deverão, respetivamente, tomar as medidas necessárias para cumprir os requisitos do presente regulamento até ao final de 2030 e até … [seis anos a contar da data de entrada em vigor do presente regulamento].

(178) Os prestadores de sistemas de IA de risco elevado são incentivados a começar a cumprir, numa base voluntária, as obrigações pertinentes previstas no presente regulamento já durante o período de transição.

(179) O presente regulamento é aplicável a partir de ... [dois anos a contar da data de entrada em vigor do presente regulamento]. No entanto, tendo em conta o risco inaceitável associado à utilização da IA de determinadas formas, as proibições bem como as disposições gerais do presente regulamento deverão aplicar-se já a partir de ... [seis meses a contar da entrada em vigor do presente regulamento]. Embora o pleno efeito dessas proibições decorra do estabelecimento da governação e da execução do presente regulamento, a antecipação da aplicação das proibições é importante para ter em conta riscos inaceitáveis e para ter efeitos noutros procedimentos, como no direito civil. Além disso, as estruturas relacionadas com a governação e o sistema de avaliação da conformidade deverão estar operacionais antes de … [dois anos a contar da data de entrada em vigor do presente regulamento], pelo que as disposições relativas aos organismos notificados e à estrutura de governação deverão aplicar-se a partir de … [12 meses a contar da data de entrada em vigor do presente regulamento]. Tendo em conta o ritmo acelerado da evolução tecnológica e da adoção de modelos de IA de finalidade geral, as obrigações dos prestadores de modelos de IA de finalidade geral deverão aplicar-se a partir de ... [12 meses a contar da data de entrada em vigor do presente regulamento]. Códigos de práticas deverão estar prontos até ... [nove meses a contar da data de entrada em vigor do presente regulamento], com vista a permitir que os prestadores demonstrem o cumprimento atempadamente. O Serviço para a IA deverá assegurar que as regras e procedimentos de classificação estejam atualizados à luz da evolução tecnológica. Além disso, os Estados-Membros deverão estabelecer as regras em matéria de sanções, incluindo coimas, e notificá-las à Comissão, bem como assegurar a sua aplicação de forma efetiva e adequada à data de aplicação do presente regulamento. Como tal, as disposições relativas às sanções deverão aplicar-se a partir de … [12 meses a contar da data de entrada em vigor do presente regulamento].

(180) 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.ºs 1 e 2, do Regulamento (UE) 2018/1725, e emitiram parecer em 18 de junho de 2021,

ADOTARAM O PRESENTE REGULAMENTO:

Capítulo I
Disposições gerais

Artigo 1.º
Objeto

1. A finalidade do presente regulamento é melhorar o funcionamento do mercado interno e promover a adoção de uma inteligência artificial (IA) centrada no ser humano e de confiança, assegurando simultaneamente um elevado nível de proteção da saúde, da segurança e dos direitos fundamentais consagrados na Carta, incluindo a democracia, o Estado de direito e a proteção do ambiente, contra os efeitos nocivos dos sistemas de IA na União, bem como apoiar a inovação.

2. O presente regulamento estabelece:

   a) Regras harmonizadas para a colocação no mercado, a colocação em serviço e a utilização de sistemas de IA na União;

   b) Proibições de certas práticas de IA;

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

   d) Regras de transparência harmonizadas para determinados sistemas de IA;

   e) Regras harmonizadas para a colocação no mercado de modelos de IA de finalidade geral;

f) Regras relativas ao acompanhamento do mercado, à fiscalização do mercado, à governação e à aplicação da lei;

g) Medidas de apoio à inovação, com especial ênfase nas PME, incluindo as empresas em fase de arranque.

Artigo 2.º

Âmbito

1. O presente regulamento é aplicável a:

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

b) Responsáveis pela implantação de sistemas de IA que tenham o seu local de estabelecimento ou que estejam localizados na União;

c) Prestadores e responsáveis pela implantação de sistemas de IA que tenham o seu local de estabelecimento ou estejam localizados num país terceiro, se o resultado produzido pelo sistema de IA for utilizado na União;

d) Importadores e distribuidores de sistemas de IA;

e) Fabricantes de produtos que coloquem no mercado ou coloquem em serviço um sistema de IA juntamente com o seu produto e sob o seu próprio nome ou a sua própria marca;

f) Mandatários dos prestadores que não estejam estabelecidos na União;

g) Pessoas afetadas localizadas na União.

2. Aos sistemas de IA classificados como sistemas de IA de risco elevado em conformidade com o artigo 6.º, n.º 1, relacionados com os produtos abrangidos pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I, secção B, apenas é aplicável o artigo 6.º, n.º 1, os artigos 102.º a 109.º e o artigo 112.º. O artigo 57.º só é aplicável na medida em que os requisitos aplicáveis aos sistemas de IA de risco elevado previstos no presente regulamento tenham sido integrados na referida legislação de harmonização da União.

3. O presente regulamento não se aplica a domínios não abrangidos pelo âmbito de aplicação do direito da União nem afeta, em caso algum, as competências dos Estados-Membros em matéria de segurança nacional, independentemente do tipo de entidade designada pelos Estados-Membros para desempenhar as funções relacionadas com essas competências.

O presente regulamento não se aplica aos sistemas de IA se e na medida em que tiverem sido colocados no mercado, colocados em serviço ou utilizados, com ou sem modificações, exclusivamente para finalidades militares, de defesa ou de segurança nacional, independentemente do tipo de entidade que realiza essas atividades.

O presente regulamento não se aplica aos sistemas de IA que não tenham sido colocados no mercado ou colocados em serviço na União, se os seus resultados forem utilizados na União exclusivamente para finalidades militares, de defesa ou de segurança nacional, independentemente do tipo de entidade que realiza essas atividades.

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 da cooperação internacional ou de acordos internacionais para efeitos de cooperação policial e judiciária com a União ou com um ou vários Estados-Membros, sob condição de esse país terceiro ou organização internacional apresentar salvaguardas adequadas em matéria de proteção de direitos e liberdades fundamentais das pessoas.

5. O presente regulamento não afeta a aplicação das disposições relativas à responsabilidade dos prestadores de serviços intermediários estabelecidas no capítulo II do Regulamento (UE) 2022/2065.

6. O presente regulamento não se aplica a sistemas de IA ou modelos de IA, incluindo os respetivos resultados, especificamente desenvolvidos e colocados em serviço exclusivamente para fins de investigação e desenvolvimento científicos.

7. O direito da União em matéria de proteção de dados pessoais, privacidade e confidencialidade das comunicações aplica-se aos dados pessoais tratados em virtude dos direitos e obrigações estabelecidos no presente regulamento. O presente regulamento não afeta o disposto nos Regulamentos (UE) 2016/679 ou (UE) 2018/1725 nem nas Diretivas 2002/58/CE ou (UE) 2016/680, sem prejuízo do disposto no artigo 10.º, n.º 5, e no artigo 59.º do presente regulamento.

8. O presente regulamento não se aplica às atividades de investigação, testagem ou desenvolvimento relativas a sistemas de IA ou modelos de IA antes de serem colocados no mercado ou colocados em serviço. Tais atividades devem ser realizadas em conformidade com direito da União aplicável. A testagem em condições reais não é abrangida por essa exclusão.

9. O presente regulamento não prejudica as regras estabelecidas por outros atos legislativos da União relacionados com a proteção dos consumidores e a segurança dos produtos.

10. O presente regulamento não se aplica às obrigações dos responsáveis pela implantação que sejam pessoas singulares que utilizam os sistemas de IA no âmbito de uma atividade puramente pessoal de caráter não profissional.

11. O presente regulamento não impede a União nem os Estados-Membros de manterem ou introduzirem disposições legislativas, regulamentares ou administrativas mais favoráveis para os trabalhadores em termos de proteção dos seus direitos no que diz respeito à utilização de sistemas de IA por empregadores, nem de incentivarem ou permitirem a aplicação de convenções coletivas mais favoráveis para os trabalhadores.

12. O presente regulamento não se aplica aos sistemas de IA lançados ao abrigo de licenças gratuitas e de código aberto, a menos que sejam colocados no mercado ou colocados em serviço como sistemas de IA de risco elevado ou que sejam sistemas de IA abrangidos pelo âmbito de aplicação dos artigos 5.º ou 50.º.

Artigo 3.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Sistema de IA», um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais;

2) «Risco», a combinação da probabilidade de ocorrência de danos com a gravidade desses danos;

3) «Prestador», uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que desenvolva, ou mande desenvolver, um sistema de IA ou um modelo de IA de finalidade geral e o coloque no mercado, ou coloque o sistema de IA em serviço sob o seu próprio nome ou a sua própria marca, a título oneroso ou gratuito;

4) «Responsável pela implantação», uma pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que utilize um sistema de IA sob a sua própria autoridade, 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 localizada ou estabelecida na União que tenha recebido e aceitado um mandato escrito de um prestador de um sistema de IA ou de um modelo de IA de finalidade geral para cumprir e executar em seu nome, respetivamente, as obrigações e os procedimentos previstos no presente regulamento;

6) «Importador», uma pessoa singular ou coletiva localizada ou estabelecida na União que coloca no mercado um sistema de IA que ostenta o nome ou a marca de uma pessoa singular ou coletiva estabelecida num país terceiro;

7) «Distribuidor», uma pessoa singular ou coletiva inserida na cadeia de distribuição, distinta do prestador e do importador, que disponibiliza um sistema de IA no mercado da União;

8) «Operador», um prestador, fabricante de produtos, responsável pela implantação, mandatário, importador ou distribuidor;

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

10) «Disponibilização no mercado», o fornecimento de um sistema de IA ou de um modelo de IA de finalidade geral 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, diretamente ao responsável pela implantação ou para utilização própria, de um sistema de IA para a primeira utilização na União com a finalidade prevista;

12) «Finalidade prevista», a utilização a que o prestador destina o sistema de IA, incluindo o contexto específico e as condições de utilização, conforme especificado nas informações facultadas pelo prestador 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 um comportamento humano razoavelmente previsível ou de uma interação razoavelmente previsível com outros sistemas, incluindo outros sistemas de IA;

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

15) «Instruções de utilização», as informações facultadas pelo prestador para esclarecer responsável pela implantação, em especial, sobre a finalidade prevista e a utilização correta de um sistema de IA;

16) «Recolha de um sistema de IA», qualquer medida destinada a obter a devolução ao prestador de um sistema de IA disponibilizado aos responsáveis pela implantação ou a colocar esse sistema fora de serviço ou a desativá-lo;

17) «Retirada de um sistema de IA», qualquer medida destinada a impedir a disponibilização no mercado de um sistema de IA presente na cadeia de distribuição;

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 demonstrar se estão preenchidos os requisitos relacionados com um sistema de IA de risco elevado estabelecidos no capítulo III, secção 2;

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 notificado nos termos do presente regulamento ou de outra legislação de harmonização da União pertinente;

23) «Modificação substancial», uma alteração do sistema de IA após a sua colocação no mercado ou colocação em serviço, que não tenha sido prevista ou planeada pelo prestador na avaliação da conformidade inicial e que, consequentemente, afete a conformidade do sistema de IA com os requisitos estabelecidos no capítulo II, secção 2, do presente regulamento, ou modifique a finalidade prevista relativamente à qual o sistema de IA foi avaliado;

24) «Marcação CE», a marcação pela qual um prestador atesta que um sistema de IA está em conformidade com os requisitos estabelecidos no capítulo III, secção 2, e noutros atos aplicáveis enumerados na lista da legislação de harmonização da União que prevejam a aposição dessa marcação;

25) «Sistema de acompanhamento pós-comercialização», todas as atividades empreendidas pelos prestadores de sistemas de IA para recolher e analisar dados sobre a experiência adquirida com a utilização de sistemas de IA por eles colocados no mercado ou colocados em serviço, com vista a identificar a eventual necessidade de aplicar imediatamente as eventuais medidas corretivas ou preventivas necessárias;

26) «Autoridade de fiscalização do mercado», a autoridade nacional que realiza as atividades e toma as medidas 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) «Especificação comum», um conjunto de especificações técnicas, definidas no artigo 2.º, ponto 4, do Regulamento (UE) n.º 1025/2012, que proporcionam os meios para cumprir certos requisitos estabelecidos 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;

30) «Dados de validação», os dados utilizados para realizar uma avaliação do sistema de IA treinado e ajustar os seus parâmetros não passíveis de serem aprendidos e o seu processo de aprendizagem, a fim de, entre outras coisas, evitar um subajustamento ou um sobreajustamento;

31) «Conjunto de dados de validação», um conjunto de dados separado ou parte de um conjunto de dados de treino, sob forma de uma divisão fixa ou variável;

32) «Dados de teste», os dados utilizados para realizar uma avaliação independente do sistema de IA, a fim de confirmar o desempenho esperado desse sistema antes da sua colocação no mercado ou colocação em serviço;

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

34) «Dados biométricos», dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;

35) «Identificação biométrica», o reconhecimento automatizado de características humanas físicas, fisiológicas, comportamentais ou psicológicas para efeitos de determinação da identidade de uma pessoa singular, comparando os dados biométricos dessa pessoa com os dados biométricos de pessoas armazenados numa base de dados;

36) «Verificação biométrica», a verificação automatizada, «um para um», incluindo a autenticação, da identidade de pessoas singulares por meio da comparação dos seus dados biométricos com dados biométricos previamente facultados;

37) «Categorias especiais de dados pessoais», as categorias de dados pessoais a que se referem 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;

38) «Dados operacionais sensíveis», dados operacionais relacionados com atividades de prevenção, deteção, investigação ou repressão de infrações penais, cuja divulgação possa comprometer a integridade de processos penais;

39) «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;

40) «Sistema de categorização biométrica», um sistema de IA destinado a afetar pessoas singulares a categorias específicas com base nos seus dados biométricos, a menos que seja acessório a outro serviço comercial e estritamente necessário por razões técnicas objetivas;

41) «Sistema de identificação biométrica à distância», um sistema de IA concebido para identificar pessoas singulares, sem a sua participação ativa, normalmente à distância, por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência;

42) «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, que engloba não apenas a identificação instantânea, mas também a identificação com ligeiro atraso, a fim de evitar que as regras sejam contornadas;

43) «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;

44) «Espaço acessível ao público», qualquer espaço físico, público ou privado, acessível a um número indeterminado de pessoas singulares, independentemente da eventual aplicação de condições de acesso específicas e independentemente das eventuais restrições de capacidade;

45) «Autoridade responsável pela aplicação da lei»:

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 designado pelo direito de um Estado-Membro para exercer autoridade pública e poderes públicos para efeitos de prevenção, investigação, deteção ou pelo exercício da ação penal relativo a infrações penais ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção das mesmas;

46) «Aplicação da lei», as atividades realizadas por autoridades responsáveis pela aplicação da lei ou em nome destas 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;

47) «Serviço para a IA», a atribuição da Comissão de contribuir para a aplicação, o acompanhamento e a supervisão dos sistemas de IA, dos modelos de IA de finalidade geral, e da governação da IA prevista na Decisão da Comissão de 24 de janeiro de 2024; as referências ao Serviço para a IA no presente regulamento devem ser entendidas como referências à Comissão;

48) «Autoridade nacional competente», uma autoridade notificadora ou uma autoridade de fiscalização do mercado; no que diz respeito aos sistemas de IA colocados em serviço ou utilizados pelas instituições, agências, serviços e organismos da União, quaisquer referências às autoridades nacionais competentes ou às autoridades de fiscalização do mercado no presente regulamento devem ser entendidas como referências à Autoridade Europeia para a Proteção de Dados;

49) «Incidente grave», qualquer incidente ou anomalia num sistema de IA que, direta ou indiretamente, tenha alguma das seguintes consequências:

a) A morte de uma pessoa ou danos graves para a saúde de uma pessoa;

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

c) A infração das obrigações decorrentes do direito da União destinadas a proteger os direitos fundamentais;

d) Danos graves a bens ou ao ambiente;

50) «Dados pessoais», os dados pessoais na aceção do artigo 4.º, ponto 1, do Regulamento (UE) 2016/679;

51) «Dados não pessoais», os dados que não sejam dados pessoais na aceção do artigo 4.º, ponto 1), do Regulamento (UE) 2016/679;

52) «Definição de perfis», a definição de perfis na aceção do artigo 4.º, ponto 4), do Regulamento (UE) 2016/679;

53) «Plano de testagem em condições reais», um documento que descreve os objetivos, a metodologia, o âmbito geográfico, populacional e temporal, o acompanhamento, a organização e a realização dos testes em condições reais;

54) «Plano do ambiente de testagem», um documento acordado entre o prestador participante e a autoridade competente, que descreve os objetivos, as condições, o calendário, a metodologia e os requisitos aplicáveis às atividades realizadas no ambiente de testagem;

55) «Ambiente de testagem da regulamentação da IA», um modelo controlado, criado por uma autoridade competente, que oferece aos prestadores ou potenciais prestadores de sistemas de IA a possibilidade de desenvolver, treinar, validar e testar, se for caso disso em condições reais, um sistema de IA inovador, de acordo com um plano do ambiente de testagem, durante um período limitado sob supervisão regulamentar;

56) «Literacia no domínio da IA», as competências, os conhecimentos e a compreensão que permitem que os prestadores, os responsáveis pela implantação e as pessoas afetadas, tendo em conta os respetivos direitos e obrigações no contexto do presente regulamento, procedam à implantação dos sistemas de IA com conhecimento de causa e tomem consciência das oportunidades e dos riscos inerentes à IA, bem como dos eventuais danos que a IA pode causar;

57) «Testagem em condições reais», a testagem temporária de um sistema de IA para a sua finalidade prevista em condições reais, fora de um laboratório ou de outro ambiente simulado, com vista a recolher dados fiáveis e sólidos e a avaliar e verificar a conformidade do sistema de IA com os requisitos do presente regulamento e não se considera como colocação do sistema de IA no mercado nem colocação do sistema de IA em serviço na aceção do presente regulamento, desde que estejam preenchidas todas as condições estabelecidas no artigo 57.º ou no artigo 60.º;

58) «Participante», para efeitos de testagem em condições reais, uma pessoa singular que participa na testagem em condições reais;

59) «Consentimento informado», a expressão livre, específica, inequívoca e voluntária, por parte do participante, da sua vontade de participar numa dada testagem em condições reais, depois de ter sido informado de todos os aspetos da testagem que sejam relevantes para a sua decisão de participar;

60) «Falsificações profundas», conteúdos de imagem, áudio ou vídeo gerados ou manipulados por IA, que sejam semelhantes a pessoas, objetos, locais, entidades ou acontecimentos reais, e que possam levar uma pessoa a crer, erroneamente, que são autênticos ou verdadeiros;

61) «Infração generalizada», uma ação ou omissão contrária à legislação da União que protege os interesses das pessoas, e que:

a) Tenha prejudicado, ou seja suscetível de prejudicar, os interesses coletivos de pessoas que residam em, pelo menos, dois Estados-Membros que não o Estado-Membro no qual:

i) o ato ou omissão tenha tido origem ou sido cometido,

ii) o prestador em causa ou, se aplicável, o seu mandatário esteja estabelecido, ou

iii) o responsável pela implantação esteja estabelecido, caso a violação seja cometida por este;

b) Tenha prejudicado, ou seja suscetível de prejudicar, os interesses coletivos das pessoas e tenha características comuns, inclusive a mesma prática ilegal ou a violação de um mesmo interesse, e que seja cometida pelo mesmo operador em, pelo menos, três Estados-Membros em simultâneo;

62) «Infraestrutura crítica», uma infraestrutura crítica na aceção do artigo 2.º, ponto 4), da Diretiva (UE) 2022/2557;

63) «Modelo de IA de finalidade geral», um modelo de IA, inclusive se for treinado com uma grande quantidade de dados utilizando a autossupervisão em escala, que apresenta uma generalidade significativa e é capaz de executar de forma competente uma vasta gama de tarefas distintas, independentemente da forma como o modelo é colocado no mercado, e que pode ser integrado numa variedade de sistemas ou aplicações a jusante, exceto os modelos de IA que são utilizados para atividades de investigação, desenvolvimento ou criação de protótipos antes de serem colocados no mercado;

64) «Capacidades de elevado impacto», capacidades que correspondem ou excedem as capacidades registadas nos modelos de IA de finalidade geral mais avançados;

65) «Risco sistémico», um risco específico das capacidades de elevado impacto dos modelos de IA de finalidade geral que têm um impacto significativo no mercado da União devido ao seu alcance ou devido a efeitos negativos reais ou razoavelmente previsíveis na saúde pública, na segurança, na segurança pública, nos direitos fundamentais ou na sociedade no seu conjunto, que se pode propagar em escala ao longo da cadeia de valor;

66) «Sistema de IA de finalidade geral», um sistema de IA baseado num modelo de IA de finalidade geral, e com a capacidade de servir para diversas finalidades, tanto para utilização direta como para integração noutros sistemas de IA;

67) «Operação de vírgula flutuante», qualquer operação matemática ou atribuição que envolva números em vírgula flutuante, que são um subconjunto dos números reais normalmente representados em computadores por um número inteiro de precisão fixa escalado por um expoente inteiro de uma base fixa;

68) «Prestador a jusante», um prestador de um sistema de IA, incluindo um sistema de IA de finalidade geral, que integra um modelo de IA, independentemente de o modelo de IA ser disponibilizado por si próprio e verticalmente integrado ou ser disponibilizado por outra entidade com base em relações contratuais.

Artigo 4.º

Literacia no domínio da IA

Os prestadores e os responsáveis pela implantação de sistemas de IA adotam medidas para garantir, na medida do possível, que o seu pessoal e outras pessoas envolvidas na operação e utilização de sistemas de IA em seu nome dispõem de um nível suficiente de literacia no domínio da IA, tendo em conta os seus conhecimentos técnicos, experiência, qualificações académicas e formação e o contexto em que os sistemas de IA serão utilizados, bem como as pessoas ou grupos de pessoas visadas por essa utilização.

Capítulo II
Práticas de IA proibidas

Artigo 5.º

Práticas de IA proibidas

1. Estão proibidas as seguintes práticas de IA:

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, ou técnicas manifestamente manipuladoras ou enganadoras, com o objetivo ou o efeito de distorcer substancialmente o comportamento de uma pessoa ou de um grupo de pessoas prejudicando de forma considerável a sua capacidade de tomar uma decisão informada e levando, assim, a que tomem uma decisão que, caso contrário, não tomariam, de uma forma que cause ou seja razoavelmente suscetível de causar danos significativos a essa ou a outra pessoa, ou a um grupo de pessoas;

b) A colocação no mercado, a colocação em serviço ou a utilização de um sistema de IA que explore vulnerabilidades de uma pessoa singular ou de um grupo específico de pessoas devidas à sua idade, incapacidade ou situação socioeconómica específica, com o objetivo ou o efeito de distorcer substancialmente o comportamento dessa pessoa ou de uma pessoa pertencente a esse grupo de uma forma que cause ou seja razoavelmente suscetível de causar danos significativos a essa ou a outra pessoa;

c) A colocação no mercado, a colocação em serviço ou a utilização de sistemas de IA para avaliação ou classificação de pessoas singulares ou grupos de pessoas durante um certo período com base no seu comportamento social ou em características de personalidade ou pessoais, conhecidas, inferidas ou previsíveis, em que a classificação social conduza a uma das seguintes situações ou a ambas:

i) tratamento prejudicial ou desfavorável de certas pessoas singulares ou grupos de pessoas 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 de pessoas que seja injustificado ou desproporcionado face ao seu comportamento social ou à gravidade do mesmo;

d) A colocação no mercado, a colocação em serviço para esta finalidade específica ou a utilização de um sistema de IA para a realização de avaliações de risco de pessoas singulares a fim de avaliar ou prever o risco de uma pessoa singular cometer uma infração penal, com base exclusivamente na definição de perfis de uma pessoa singular ou na avaliação dos seus traços e características de personalidade. Esta proibição não se aplica aos sistemas de IA utilizados para apoiar a avaliação humana do envolvimento de uma pessoa numa atividade criminosa, que já se baseia em factos objetivos e verificáveis diretamente ligados a uma atividade criminosa;

e) A colocação no mercado, a colocação em serviço para esta finalidade específica ou a utilização de sistemas de IA que criam ou expandem bases de dados de reconhecimento facial através da recolha aleatória de imagens faciais a partir da Internet ou de imagens de televisão em circuito fechado (TVCF);

f) A colocação no mercado, a colocação em serviço para esta finalidade específica ou a utilização de sistemas de IA para inferir emoções de uma pessoa singular no local de trabalho e nas instituições de ensino, exceto nos casos em que o sistema de IA se destine a ser instalado ou introduzido no mercado por razões médicas ou de segurança;

g) A colocação no mercado, a colocação em serviço para este fim específico, ou a utilização de sistemas de categorização biométrica que classifiquem individualmente as pessoas singulares com base nos seus dados biométricos para deduzir ou inferir a sua raça, opiniões políticas, filiação sindical, convicções religiosas ou filosóficas, vida sexual ou orientação sexual; esta proibição não abrange rotulagens nem filtragens de conjuntos de dados biométricos legalmente adquiridos, tais como imagens, com base em dados biométricos ou na categorização de dados biométricos no domínio da aplicação da lei;

h) A utilização de sistemas de identificação biométrica à distância em «tempo real» em espaços acessíveis ao público para efeitos de aplicação da lei, a menos e na medida em que essa utilização seja estritamente necessária para um dos seguintes fins:

   i) busca seletiva de vítimas específicas de rapto, tráfico de seres humanos ou exploração sexual de seres humanos, bem como a busca por pessoas desaparecidas,

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

iii) a localização ou identificação de uma pessoa suspeita de ter cometido uma infração penal, para efeitos da realização de uma investigação criminal, ou instauração de ação penal ou execução de uma sanção penal por alguma das infrações referidas no anexo II e puníveis no Estado-Membro em causa com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a quatro anos.

A alínea h) do primeiro parágrafo não prejudica o disposto no artigo 9.º do Regulamento (UE) 2016/679 no que respeita ao tratamento de dados biométricos para outros fins que não a aplicação da lei.

2. A utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de aplicação da lei com vista a alcançar qualquer um dos fins previstos no n.º 1, primeiro parágrafo, alínea h), deve ser implantada para os fins descritos na referida alínea, apenas com a finalidade de confirmar a identidade da pessoa especificamente visada e 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 danos 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 aplicação da lei com vista a alcançar qualquer um dos objetivos referidos no n.º 1, primeiro parágrafo, alínea h), do presente artigo deve observar salvaguardas e condições necessárias e proporcionadas em conformidade com o direito nacional que autoriza tal utilização, nomeadamente no respeitante a limitações temporais, geográficas e das pessoas visadas. A utilização de um sistema de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público só é autorizada se a autoridade responsáveis pela aplicação da lei tiver concluído uma avaliação de impacto sobre os direitos fundamentais, conforme previsto no artigo 27.º, e tiver registado o sistema na base de dados da UE em conformidade com o artigo 49.º. No entanto, em casos de urgência devidamente justificados, a utilização desses sistemas pode ser iniciada sem o registo na base de dados da UE, desde que esse registo seja concluído sem demora injustificada.

3. No tocante ao n.º 1, primeiro parágrafo, alínea h), e ao n.º 2, cada utilização de um sistema de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de aplicação da lei está sujeita a autorização prévia concedida por uma autoridade judiciária, ou uma autoridade administrativa independente cuja decisão seja vinculativa, 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 5. Contudo, numa situação de urgência devidamente justificada, a utilização do sistema pode ser iniciada sem uma autorização, desde que essa autorização seja solicitada sem demora injustificada, o mais tardar no prazo de 24 horas. Se o pedido de autorização for rejeitado, a utilização do sistema é suspensa com efeito imediato, e todos os dados, bem como os resultados dessa utilização, são imediatamente descartados e eliminados.

A autoridade judiciária competente, ou uma autoridade administrativa independente cuja decisão seja vinculativa, apenas concede 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, primeiro parágrafo, alínea h), conforme identificado no pedido, e, em especial, se limita ao estritamente necessário no que diz respeito ao período de tempo e ao âmbito geográfico e pessoal. Ao decidir sobre o pedido, a autoridade judiciária ou administrativa competente tem em conta os elementos referidos no n.º 2. As decisões que produzam efeitos jurídicos adversos sobre uma pessoa não podem ser tomadas exclusivamente com base nos resultados saídos do sistema de identificação biométrica à distância «em tempo real».

4. Sem prejuízo do disposto no n.º 3, cada utilização de um sistema de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de aplicação da lei é notificada à autoridade de fiscalização do mercado pertinente e à autoridade nacional de proteção de dados, em conformidade com as regras nacionais a que se refere o n.º 5. A notificação deve conter, no mínimo, as informações especificadas no n.º 6 e não pode incluir dados operacionais sensíveis.

5. 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 fins de aplicação da lei dentro dos limites e sob as condições enumeradas no n.º 1, primeiro parágrafo, alínea h), e nos n.os 2 e 3. Os Estados-Membros em causa estabelecem na sua legislação nacional as regras de execução aplicáveis ao pedido, à emissão e ao exercício das autorizações a que se refere o n.º 3, bem como à supervisão e comunicação das mesmas. Essas regras especificam igualmente para quais dos objetivos enumerados no n.º 1, primeiro parágrafo, alínea h), inclusive para quais das infrações penais referidas na subalínea iii) da referida alínea, as autoridades competentes podem ser autorizadas a usar esses sistemas para efeitos de aplicação da lei. Os Estados-Membros notificam essas regras à Comissão o mais tardar 30 dias após a sua adoção. Os Estados-Membros podem introduzir, em conformidade com o direito da União, legislação mais restritiva sobre a utilização de sistemas de identificação biométrica à distância.

6. As autoridades nacionais de fiscalização do mercado e as autoridades nacionais de proteção de dados dos Estados-Membros que tenham sido notificadas da utilização de sistemas de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de aplicação da lei nos termos do n.º 4 apresentam à Comissão relatórios anuais sobre essa utilização. Para o efeito, a Comissão disponibiliza aos Estados-Membros e às autoridades nacionais de fiscalização do mercado e de proteção de dados um modelo que inclua informações sobre o número de decisões tomadas pelas autoridades judiciárias competentes, ou por uma autoridade administrativa independente cuja decisão seja vinculativa, após os pedidos de autorização nos termos do n.º 3, bem como sobre o seu resultado.

7. A Comissão publica relatórios anuais sobre a utilização de sistemas de identificação biométrica à distância em tempo real em espaços acessíveis ao público para efeitos de aplicação da lei, baseados em dados agregados nos Estados-Membros com base nos relatórios anuais a que se refere o n.º 6. Esses relatórios anuais não podem incluir dados operacionais sensíveis sobre as atividades de aplicação da lei conexas.

8. O presente artigo não afeta as proibições aplicáveis sempre que uma prática de IA infrinja outra legislação da União.

Capítulo III

Sistemas de IA de risco elevado

SECÇÃO 1

CLASSIFICAÇÃO DE SISTEMAS DE IA COMO SENDO DE RISCO ELEVADO

Artigo 6.º

Regras para a classificação de sistemas de IA 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 sempre que se estejam preenchidas ambas as seguintes condições:

   a) O sistema de IA destina-se a ser utilizado como um componente de segurança de um produto ou o sistema de IA é, ele próprio, um produto abrangido pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I;

b) O produto cujo componente de segurança nos termos da alínea a) é o sistema de IA, ou o próprio sistema de IA enquanto produto, tem de ser sujeito a uma avaliação da conformidade por terceiros com vista à sua colocação no mercado ou colocação em serviço nos termos dos atos enumerados na lista da legislação de harmonização da União constante do anexo I.

2. Além dos sistemas de IA de risco elevado a que se refere o n.º 1, os sistemas de IA a que se refere o anexo III são também considerados de risco elevado.

3. Em derrogação do n.º 2, um sistema de IA a que se refere o Anexo III não pode ser considerado de risco elevado se não representar um risco significativo de danos para a saúde, a segurança ou os direitos fundamentais das pessoas singulares, nomeadamente se não influenciarem de forma significativa o resultado da tomada de decisões.

O primeiro parágrafo aplica-se nos casos em que estiverem preenchidas quaisquer das seguintes condições:

a) O sistema de IA destina-se a desempenhar uma tarefa processual restrita;

b) O sistema de IA destina-se a melhorar o resultado de uma atividade humana previamente concluída;

c) O sistema de IA destina-se a detetar padrões de tomada de decisões ou desvios em relação a padrões de tomada de decisões anteriores e não se destina a substituir nem influenciar uma avaliação humana previamente concluída, sem que se proceda a uma verificação adequada por um ser humano; ou

d) O sistema de IA destina-se a executar uma tarefa preparatória no contexto de uma avaliação pertinente para efeitos dos casos de utilização enumerados no anexo III.

Não obstante o primeiro parágrafo, os sistemas de IA a que se refere o anexo III devem ser sempre considerados de risco elevado nos casos em que executarem a definição de perfis de pessoas singulares.

4. Um prestador que considere que um dos sistemas de IA a que se refere o anexo III não é de risco elevado deve documentar a sua avaliação antes de esse sistema ser colocado no mercado ou colocado em serviço. Esse prestador está sujeito à obrigação de registo prevista no artigo 49.º, n.º 2. A pedido das autoridades nacionais competentes, o prestador deve facultar a documentação da avaliação.

5. Após consulta do Comité Europeu para a Inteligência Artificial («Comité»), e o mais tardar até ... [18 meses a contar da data de entrada em vigor do presente regulamento], a Comissão disponibiliza orientações que especifiquem a aplicação prática do presente artigo em conformidade com o artigo 96.º, juntamente com uma lista exaustiva de exemplos práticos de casos de utilização de sistemas de IA de risco elevado e de risco não elevado.

6. A Comissão fica habilitada a adotar atos delegados os termos do artigo 97.º para alterar o n.º 3, segundo parágrafo, do presente artigo no que diz respeito a aditar novas condições para além das que aí se encontram previstas, ou a alterar essas condições, se existirem provas concretas e fiáveis da existência de sistemas de IA que sejam abrangidos pelo âmbito de aplicação do anexo III mas não apresentem um risco significativo de danos para a saúde, a segurança ou os direitos fundamentais das pessoas singulares.

7. A Comissão adota atos delegados nos termos do artigo 97.º no que diz respeito à alteração do n.º 3, segundo parágrafo, do presente artigo, para suprimir qualquer uma das condições aí previstas, caso existam provas concretas e fiáveis de que tal é necessário para manter o nível de proteção da saúde, da segurança e dos direitos fundamentais previsto no presente regulamento.

8. Qualquer alteração às condições estabelecidas no n.º 3, segundo parágrafo, adotadas nos termos dos n.ºs 6 e 7 do presente artigo, não pode diminuir o nível geral de proteção da saúde, da segurança e dos direitos fundamentais previsto no presente regulamento e assegura a coerência com os atos delegados adotados nos termos do artigo 7.º, n.º 1, e tem em conta a evolução tecnológica e do mercado.

Artigo 7.º

Alterações ao anexo III

1. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 97.º para alterar o anexo III, aditando ou modificando casos de utilização de sistemas de IA de risco elevado sempre que estejam preenchidas ambas as seguintes condições:

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

   b) Os sistemas de IA representam um risco de danos para a saúde e a segurança ou de repercussões negativas nos direitos fundamentais, e esse risco é equivalente ou superior ao risco de danos ou repercussões negativas representado pelos sistemas de IA de risco elevado já referidos no anexo III.

2. Ao avaliar a condição prevista no n.º 1, alínea b), a Comissão tem em conta 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) A natureza e a quantidade dos dados tratados e utilizados pelo sistema de IA e, em particular, o facto de serem tratadas categorias especiais de dados pessoais;

d) A medida em que o sistema de IA atua de forma autónoma e a possibilidade de um ser humano anular decisões ou recomendações que possam causar danos;

e) A medida em que a utilização de um sistema de IA já tenha causado danos para a saúde e a segurança, tenha tido repercussões negativas nos direitos fundamentais ou tenha suscitado preocupações significativas quanto à probabilidade de esses danos ou essas repercussões negativas ocorrerem, conforme demonstrado, por exemplo, por relatórios ou alegações documentadas apresentados às autoridades nacionais competentes, ou por outros relatórios, consoante o caso;

f) A potencial dimensão desses danos ou dessas repercussões negativas, nomeadamente em termos de intensidade e de capacidade para afetar várias pessoas, ou para afetar de forma desproporcionada um determinado grupo de pessoas;

g) A medida em que as pessoas que sofreram potenciais danos ou repercussões negativas dependem dos resultados produzidos por um sistema de IA, em especial se, por razões práticas ou jurídicas, não lhes for razoavelmente possível autoexcluir-se desse resultado;

h) A medida em que existe um desequilíbrio em termos de poder ou em que as pessoas que sofreram potenciais danos ou repercussões negativas se encontram numa posição vulnerável em relação ao responsável pela implantação de um sistema de IA, em particular por motivos relacionados com o estatuto, a autoridade, o conhecimento, as circunstâncias económicas ou sociais, ou a idade;

i) A medida em que os resultados produzidos com o envolvimento de um sistema de IA são facilmente corrigíveis ou reversíveis, tendo em conta as soluções técnicas disponíveis para os corrigir ou reverter, sendo que os resultados com uma repercussão negativa na saúde, na segurança ou nos direitos fundamentais não podem ser considerados como facilmente corrigíveis ou reversíveis;

j) A magnitude e a probabilidade dos benefícios da implantação do sistema de IA para as pessoas, os grupos ou a sociedade em geral, incluindo possíveis melhorias na segurança dos produtos;

k) A medida em que o direito 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.

3. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 97.º para alterar a lista do anexo III suprimindo sistemas de IA de risco elevado sempre que estejam preenchidas ambas as seguintes condições:

a) O sistema de IA de risco elevado em causa deixa de representar um risco significativo para os direitos fundamentais, a saúde ou a segurança, tendo em conta os critérios enumerados no n.º 2;

b) A supressão não diminui o nível geral de proteção da saúde, da segurança e dos direitos fundamentais ao abrigo do direito da União.

SECÇÃO 2

REQUISITOS APLICÁVEIS AOS SISTEMAS DE IA DE RISCO ELEVADO

Artigo 8.º

Cumprimento dos requisitos

1. Os sistemas de IA de risco elevado devem cumprir os requisitos estabelecidos na presente secção, tendo em conta a sua finalidade prevista, bem como o estado da arte geralmente reconhecido em matéria de IA e de tecnologias conexas. O sistema de gestão de riscos a que se refere o artigo 9.º deve ser tido em conta para efeitos de cumprimento desses requisitos.

2. Sempre que um produto contenha um sistema de IA ao qual se aplicam os requisitos do presente regulamento, bem como os requisitos dos atos enumerados na lista da legislação de harmonização da União constante do anexo I, secção A, os prestadores são responsáveis por assegurar que o seu produto está em plena conformidade com todos os requisitos aplicáveis ao abrigo da legislação de harmonização da União. Ao assegurar a conformidade dos sistemas de IA de risco elevado a que se refere o n.º 1 com os requisitos estabelecidos na presente secção, e a fim de assegurar a coerência, evitar duplicações e minimizar os encargos adicionais, os prestadores têm a possibilidade de integrar, conforme adequado, os processos de testagem e comunicação de informações necessários, bem como as informações e a documentação necessárias, por si disponibilizados relativamente ao seu produto na documentação e nos procedimentos já existentes exigidos pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I, secção A.

Artigo 9.º

Sistema de gestão de riscos

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

2. O sistema de gestão de riscos é entendido como um processo iterativo contínuo, planeado e executado ao longo de todo o ciclo de vida de um sistema de IA de risco elevado, que requer revisões e atualizações sistemáticas regulares. Deve compreender as seguintes etapas:

   a) A identificação e análise dos riscos conhecidos e razoavelmente previsíveis que o sistema de IA de risco elevado pode representar para a saúde, a segurança ou os direitos fundamentais quando é utilizado em conformidade com a sua finalidade prevista;

b) A estimativa e avaliação dos riscos que podem surgir quando o sistema de IA de risco elevado é utilizado em conformidade com a sua finalidade prevista e em condições de utilização indevida razoavelmente previsível;

c) A avaliação de outros riscos que possam surgir, com base na análise dos dados recolhidos por meio do sistema de acompanhamento pós-comercialização a que se refere o artigo 72.º;

d) A adoção de medidas adequadas e específicas de gestão de riscos concebidas para fazer face aos riscos identificados nos termos da alínea a).

3. O presente artigo faz referência apenas aos riscos que possam ser razoavelmente atenuados ou eliminados aquando do desenvolvimento ou da conceção do sistema de IA de risco elevado ou por meio da prestação de informações técnicas adequadas.

4. As medidas de gestão de riscos a que se refere o n.º 2, alínea d), devem ter em devida consideração os efeitos e a eventual interação resultantes da aplicação combinada dos requisitos estabelecidos na presente secção, com vista a minimizar os riscos de forma mais eficaz e, ao mesmo tempo, alcançar um equilíbrio adequado na aplicação das medidas destinadas a cumprir esses requisitos.

5. As medidas de gestão de riscos a que se refere o n.º 2, alínea d), devem ser de molde a fazer com que o risco residual pertinente associado a cada perigo, bem como o risco residual global dos sistemas de IA de risco elevado, sejam considerados aceitáveis.

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

a) Eliminação ou redução dos riscos identificados e avaliados nos termos do n.º 2, tanto quanto tecnicamente viável através da conceção e do desenvolvimento adequados do sistema de IA de risco elevado;

b) Se for caso disso, adoção de medidas de atenuação e controlo adequadas para fazer face aos riscos que não possam ser eliminados;

c) Prestação das informações exigidas nos termos do artigo 13.º e, se for caso disso, formação dos responsáveis pela implantação.

Com vista à 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 responsável pela implantação possua e o contexto presumível em que o sistema se destina a ser utilizado.

6. Os sistemas de IA de risco elevado são sujeitos a testes a fim de se identificarem as medidas de gestão de riscos específicas mais adequadas. Os testes asseguram que os sistemas de IA de risco elevado funcionam de forma coerente com a sua finalidade prevista e cumprem os requisitos estabelecidos na presente secção.

7. Os procedimentos de teste podem incluir a testagem em condições reais, em conformidade com o artigo 60.

8. 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 com base em parâmetros e limiares probabilísticos previamente definidos que sejam adequados à finalidade prevista do sistema de IA de risco elevado.

9. Ao implementarem o sistema de gestão de riscos tal como previsto nos n.os 1 a 7, os prestadores ponderam se, tendo em conta a sua finalidade prevista, existe a probabilidade de o sistema de IA de risco elevado ter repercussões negativas sobre pessoas com menos de 18 anos e, se for o caso, outros grupos vulneráveis.

10. Para os prestadores de sistemas de IA de risco elevado sujeitos a requisitos relativos aos processos internos de gestão de riscos nos termos da legislação setorial aplicável da União, os aspetos descritos nos n.os 1 a 9 podem fazer parte dos procedimentos de gestão de riscos estabelecidos nos termos dessa legislação ou ser combinados com esses procedimentos.

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 a que se referem os n.os 2 a 5, sempre que esses conjuntos de dados sejam utilizados.

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

a) Às escolhas de conceção pertinentes;

b) A processos de recolha de dados e à origem dos dados e, no caso dos dados pessoais, à finalidade original da recolha desses dados;

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

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

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

f) Ao exame para detetar eventuais enviesamentos suscetíveis de afetar a saúde e a segurança das pessoas, de ter repercussões negativas nos direitos fundamentais ou de resultar em discriminações proibidas pelo direito da União, especialmente quando os resultados obtidos a partir dos dados influenciam os dados de entrada para operações futuras;

g) Às medidas adequadas para detetar, prevenir e atenuar eventuais enviesamentos identificados nos termos da alínea f);

h) À identificação de lacunas ou deficiências pertinentes dos dados que impeçam o cumprimento do presente regulamento e de possíveis soluções para as mesmas.

3. Os conjuntos de dados de treino, validação e teste devem ser pertinentes, suficientemente representativos e, tanto quanto possível, isentos de erros e completos, tendo em conta a finalidade prevista. Devem ter as propriedades estatísticas adequadas, nomeadamente, quando aplicável, no tocante às pessoas ou grupos de pessoas em relação às quais se destina a utilização do sistema de IA de risco elevado. Essas 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 devem ter em conta, na medida do necessário para a finalidade prevista, as características ou os elementos que são idiossincráticos do enquadramento geográfico, contextual, 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 a deteção e a correção de enviesamentos em relação aos sistemas de IA de risco elevado em conformidade com o n.º 2, alíneas f) e g), do presente artigo, os prestadores desses sistemas podem, excecionalmente, tratar categorias especiais de dados pessoais, sob reserva de garantias adequadas dos direitos e liberdades fundamentais das pessoas singulares. Para além das disposições estabelecidas nos Regulamentos (UE) 2016/679 e (UE) 2018/1725 e na Diretiva (UE) 2016/680, todas as seguintes condições para que esse tratamento ocorra devem ser cumpridas:

   a) A deteção e a correção de enviesamentos não podem ser eficazmente efetuadas através do tratamento de outros dados, nomeadamente dados sintéticos ou anonimizados;

b) As categorias especiais de dados pessoais estão sujeitas a limitações técnicas em matéria de reutilização dos dados pessoais e às mais avançadas medidas de segurança e preservação da privacidade, incluindo a pseudonimização;

c) As categorias especiais de dados pessoais estão sujeitas a medidas destinadas a assegurar que os dados pessoais tratados estejam seguros, protegidos e sujeitos a garantias adequadas, incluindo controlos rigorosos e uma documentação criteriosa do acesso a esses dados, a fim de evitar uma utilização abusiva e assegurar que apenas tenham acesso a esses dados as pessoas autorizadas e com as devidas obrigações de confidencialidade;

d) As categorias especiais de dados pessoais não são transmitidos nem transferidos para terceiros, nem de outra forma consultados por esses terceiros;

e) As categorias especiais de dados pessoais são eliminadas assim que o enviesamento tenha sido corrigido ou que os dados pessoais atinjam o fim do respetivo período de conservação, consoante o que ocorrer primeiro;

f) Os registos das atividades de tratamento nos termos do Regulamento (UE) 2016/679, do Regulamento (UE) 2018/1725 e da Diretiva (UE) 2016/680 incluem os motivos pelos quais o tratamento de categorias especiais de dados pessoais foi estritamente necessário para detetar e corrigir enviesamentos e os motivos pelos quais não foi possível alcançar esse objetivo através do tratamento de outros dados.

6. Para o desenvolvimento de sistemas de IA de risco elevado que não utilizam técnicas que envolvem o treino de modelos de IA, os n.os 2 a 5 aplicam-se apenas aos conjuntos de dados de teste.

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 deve ser mantida atualizada.

   A documentação técnica deve ser elaborada de maneira que demonstre que o sistema de IA de risco elevado cumpre os requisitos estabelecidos na presente secção e deve facultar às autoridades nacionais competentes e aos organismos notificados, de forma clara e completa, 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. As PME, incluindo as empresas em fase de arranque, podem facultar os elementos da documentação técnica especificados no anexo IV de forma simplificada. Para o efeito, a Comissão deve criar um formulário de documentação técnica simplificado destinado às necessidades das pequenas e microempresas. Caso uma PME, nomeadamente uma empresa em fase de arranque, opte por prestar as informações exigidas no anexo IV de forma simplificada, deve utilizar o formulário a que se refere o presente número. Os organismos notificados devem aceitar o formulário para efeitos de avaliação da conformidade.

2. Aquando da colocação no mercado ou da colocação em serviço de um sistema de IA de risco elevado relacionado com um produto abrangido pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I, secção A, deve ser elaborada uma documentação técnica única que contenha todas as informações previstas no n.º 1, bem como as informações exigidas nos termos desses atos jurídicos.

3. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 97.º para alterar o anexo IV, se for caso disso, com vista a assegurar que, tendo em conta a evolução técnica, a documentação técnica faculte todas as informações necessárias para aferir a conformidade do sistema com os requisitos estabelecidos na presente secção.

Artigo 12.º

Manutenção de registos

1. Os sistemas de IA de risco elevado devem permitir tecnicamente o registo automático de eventos («registos») durante a vida útil do sistema.

2. A fim de assegurar um nível de rastreabilidade do funcionamento de um sistema de IA de risco elevado adequado à finalidade prevista do sistema, as capacidades de registo devem permitir o registo de eventos pertinentes para:

   a) A identificação de situações que possam dar azo a que o sistema de IA de risco elevado apresente um risco na aceção do artigo 79.º, n.º 1, ou dar origem a uma modificação substancial;

   b) A facilitação do acompanhamento pós-comercialização a que se refere o artigo 72.º; e

   c) O controlo do funcionamento dos sistemas de IA de risco elevado a que se refere o artigo 26.º, n.º 5.

3. 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 incluir, 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 a que se refere o artigo 14.º, n.º 5.

Artigo 13.º

Transparência e prestação de informações aos responsáveis pela implantação

1. Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de maneira a assegurar que o seu funcionamento seja suficientemente transparente para permitir aos responsáveis pela implantação interpretar os resultados do sistema e utilizá-los de forma adequada. Deve ser garantido um tipo e um grau adequado de transparência com vista a garantir o cumprimento das obrigações pertinentes que incumbem ao prestador e ao responsável pela implantação por força da secção 3.

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

3. As instruções de utilização devem incluir, pelo menos, as seguintes informações:

a) A identidade e os dados de contacto do prestador 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 sua finalidade prevista,

ii) o nível de exatidão – incluindo os seus parâmetros –, de solidez e de cibersegurança a que se refere o artigo 15.º usado como referência para testar e validar o sistema de IA de risco elevado 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 previsível, que possa causar os riscos a que se refere o artigo 9.º, n.º 2, para a saúde e a segurança ou para os direitos fundamentais,

iv) se for caso disso, as capacidades técnicas e as características do sistema de IA de risco elevado que sejam pertinentes para explicar os seus resultados,

v) quando oportuno, o seu desempenho em relação a determinadas pessoas ou grupos de pessoas específicos em que o sistema se destina a ser utilizado,

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

vii) se for caso disso, informações que permitam aos responsáveis pela implantação interpretar os resultados do sistema de IA de risco elevado e utilizá-los adequadamente;

c) As alterações do sistema de IA de risco elevado e do seu desempenho que tenham sido predeterminadas pelo prestador 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 de risco elevado pelos responsáveis pela implantação;

e) Os recursos computacionais e de **hardware** necessários, a vida útil esperada do sistema de IA de risco elevado e quaisquer medidas de manutenção e assistência necessárias, incluindo a sua frequência, para assegurar o correto funcionamento desse sistema de IA, inclusive no tocante a atualizações do software;

f) Sempre que pertinente, uma descrição dos mecanismos incluídos no sistema de IA de risco elevado que permita aos responsáveis pela implantação recolher, armazenar e interpretar corretamente os registos, em conformidade com o artigo 12.º.

Artigo 14.º

Supervisão humana

1. Os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de modo a poderem, nomeadamente por meio de ferramentas de interface homem-máquina apropriadas, ser eficazmente supervisionados por pessoas singulares durante o período em que estão em utilização.

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 previsível, em especial quando esses riscos persistem apesar da aplicação de outros requisitos estabelecidos na presente secção.

3. As medidas de supervisão humana devem ser consentâneas com os riscos, ao nível de autonomia e ao contexto de utilização do sistema de IA de risco elevado e a supervisão deve ser assegurada por meio de um ou de todos os seguintes tipos de medidas:

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

   b) Medidas identificadas pelo prestador antes de o sistema de IA de risco elevado ser colocado no mercado ou colocado em serviço e que se prestem a serem postas em prática pelo responsável pela implantação.

4. Para efeitos da aplicação dos n.os 1, 2 e 3, o sistema de IA de risco elevado deve ser disponibilizado ao responsável pela implantação de modo a que seja possível às pessoas singulares responsáveis pela supervisão humana, conforme adequado e de forma proporcionada:

   a) Compreender adequadamente as capacidades e limitações pertinentes do sistema de IA de risco elevado e conseguir controlar devidamente o seu funcionamento, nomeadamente a fim de detetar e corrigir anomalias, disfuncionalidades e desempenhos inesperados;

b) Estar conscientes da possível tendência para confiar automaticamente ou confiar excessivamente nos resultados produzidos pelo sistema de IA de risco elevado (enviesamento da automatização), em especial no que toca a sistemas de IA de risco elevado utilizados para prestar informações ou recomendações com vista à tomada de decisões por pessoas singulares;

c) Interpretar corretamente os resultados do sistema de IA de risco elevado, tendo em conta, por exemplo, as ferramentas e os métodos de interpretação disponíveis;

d) Decidir, em qualquer situação específica, não usar o sistema de IA de risco elevado ou ignorar, anular ou reverter os resultados do sistema de IA de risco elevado;

e) Intervir no funcionamento do sistema de IA de risco elevado ou interromper o sistema por meio de um botão de «paragem» ou de um procedimento similar que permita parar o sistema de modo seguro.

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 do presente artigo devem, além disso, permitir assegurar que nenhuma ação ou decisão seja tomada pelo responsável pela implantação com base na identificação resultante do sistema, salvo se a mesma tiver sido verificada e confirmada separadamente por, pelo menos, duas pessoas singulares com a competência, formação e autoridade necessárias.

O requisito de verificação separada por, pelo menos, duas pessoas singulares não se aplica aos sistemas de IA de risco elevado utilizados para efeitos de aplicação da lei, de migração, de controlo das fronteiras ou de asilo, em que o direito da União ou o direito nacional considere que a aplicação deste requisito é desproporcionada.

Artigo 15.º

Exatidão, solidez e cibersegurança

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

2. A fim de abordar os aspetos técnicos relativos à forma de medir os níveis adequados de exatidão e solidez estabelecidos no n.º 1, bem como quaisquer outros parâmetros de desempenho pertinentes, a Comissão, em cooperação com as partes interessadas e as organizações pertinentes, tais como as autoridades responsáveis pela metrologia e pela avaliação comparativa, incentiva, conforme adequado, o desenvolvimento de parâmetros de referência e metodologias de medição.

3. As instruções de utilização que acompanham os sistemas de IA de risco elevado devem declarar os níveis de exatidão e os parâmetros de exatidão aplicáveis.

4. Os sistemas de IA de risco elevado devem ser tão resistentes quanto possível 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 este respeito, devem ser tomadas medidas técnicas e organizativas.

   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 planos de segurança à prova de falhas.

Os sistemas de IA de risco elevado que continuam a aprender após serem colocados no mercado ou colocados em serviço são desenvolvidos de forma a eliminar ou reduzir, tanto quanto possível, o risco de resultados possivelmente enviesados que influenciem os dados de entrada de futuras operações (circuitos de realimentação), bem como a assegurar que esses resultados possivelmente enviesados sejam objeto de medidas de atenuação adequadas.

5. Os sistemas de IA de risco elevado devem ser resistentes a tentativas de terceiros não autorizados de alterar a sua utilização, os seus resultados ou seu 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 IA devem incluir, se for caso disso, medidas para prevenir, detetar, resolver e controlar, bem como dar resposta a ataques que visem manipular o conjunto de dados de treino (contaminação de dados) ou componentes pré-treinados utilizados no treino (contaminação de modelos), dados de entrada concebidos para fazer com que o modelo de IA cometa um erro (exemplos antagónicos ou evasão de modelos), ataques de confidencialidade ou falhas do modelo.

SECÇÃO 3

OBRIGAÇÕES DOS PRESTADORES E DOS RESPONSÁVEIS PELA IMPLANTAÇÃO DE SISTEMAS DE INTELIGÊNCIA ARTIFICIAL DE RISCO ELEVADO E DE OUTRAS PARTES

Artigo 16.º

Obrigações dos prestadores de sistemas de inteligência artificial de risco elevado

Os prestadores de sistemas de IA de risco elevado devem:

a) Assegurar que os seus sistemas de IA de risco elevado cumpram os requisitos estabelecidos na secção 2;

b) Indicar no sistema de IA de risco elevado ou, se tal não for possível, na embalagem ou na documentação que o acompanha, consoante o caso, o seu nome, o nome comercial registado ou a marca registada e o endereço no qual podem ser contactados;

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

d) Conservar a documentação nos termos do artigo 18.º;

e) Quando tal esteja sob o seu controlo, manter os registos gerados automaticamente pelos sistemas de IA de risco elevado que disponibilizam, conforme previsto no artigo 19.º;

f) Assegurar que o sistema de IA de risco elevado seja sujeito ao procedimento de avaliação da conformidade aplicável, tal como previsto no artigo 43.º, antes da colocação no mercado ou da colocação em serviço;

g) Elaborar uma declaração UE de conformidade, nos termos do artigo 47.º;

h) Apor a marcação CE no sistema de IA de risco elevado ou, se tal não for possível, na embalagem ou na documentação que o acompanha, para indicar a conformidade com o presente regulamento, nos termos do artigo 48.º;

i) Respeitar as obrigações de registo a que se refere o artigo 49.º, n.º 1;

j) Adotar as medidas corretivas necessárias e prestar as informações, tal como estabelecido no artigo 20.º;

k) Mediante pedido fundamentado de uma autoridade nacional competente, demonstrar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos na secção 2;

l) Assegurar que o sistema de IA de risco elevado cumpra os requisitos de acessibilidade em conformidade com as Diretivas (UE) 2016/2102 e (UE) 2019/882.

Artigo 17.º

Sistema de gestão da qualidade

1. Os prestadores 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 maneira sistemática e ordenada, sob a forma de políticas, procedimentos e instruções escritos, e 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, ou não abrangerem todos os requisitos pertinentes estabelecidos na secção 2, os meios a usar para assegurar que o sistema de IA de risco elevado cumpra esses requisitos;

f) Sistemas e procedimentos de gestão de dados, incluindo aquisição de dados, 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 72.º;

i) Procedimentos de comunicação de um incidente grave em conformidade com o artigo 73.º;

j) A gestão da comunicação com autoridades nacionais competentes, outras autoridades pertinentes, incluindo as que disponibilizam ou apoiam 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 pertinente;

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

m) Um regime 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 prestador. Os prestadores devem, em qualquer caso, respeitar o grau de rigor e o nível de proteção necessários para garantir a conformidade dos seus sistemas de IA de risco elevado com o presente regulamento.

3. Os prestadores de sistemas de IA de risco elevado sujeitos a obrigações relativas aos sistemas de gestão da qualidade ou a uma função equivalente nos termos da legislação setorial aplicável da União podem incluir os aspetos enumerados no n.º 1 como parte dos sistemas de gestão da qualidade estabelecidos nos termos dessa legislação.

4. Para os prestadores que sejam instituições financeiras sujeitas a requisitos em matéria de governação, mecanismos ou processos internos nos termos do direito da União no domínio dos serviços financeiros, considera-se que a obrigação de criar um sistema de gestão da qualidade, com exceção do n.º 1, alíneas g), h) e i) do presente artigo, é satisfeita mediante o cumprimento das regras em matéria de governação, mecanismos ou processos internos nos termos do direito da União aplicável no domínio dos serviços financeiros. Para o efeito, devem ser tidas em conta as eventuais normas harmonizadas a que se refere o artigo 40.º.

Artigo 18.º

Manutenção de documentação

1. O prestador 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 de risco elevado:

   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 UE de conformidade a que se refere o artigo 47.º.

2. Cada Estado-Membro determina as condições em que a documentação a que se refere o n.º 1 permanece à disposição das autoridades nacionais competentes durante o período indicado nesse número, nos casos em que um prestador ou o seu mandatário estabelecido no seu território falir ou cessar a sua atividade antes do termo desse período.

3. Os prestadores que sejam instituições financeiras sujeitas a requisitos em matéria de governação, mecanismos ou processos internos nos termos do direito da União no domínio dos serviços financeiros devem manter a documentação técnica como parte da documentação conservada nos termos do direito da União aplicável no domínio dos serviços financeiros.

Artigo 19.º

Registos gerados automaticamente

1. Os prestadores de sistemas de IA de risco elevado devem manter os registos, a que se refere o artigo 12.º, n.º 1, gerados automaticamente pelos seus sistemas de IA de risco elevado, desde que esses registos estejam sob o seu controlo. Sem prejuízo do direito da União ou do direito nacional aplicável, os registos devem ser conservados por um período adequado à finalidade prevista do sistema de IA de risco elevado, de pelo menos seis meses, salvo disposição em contrário no direito da União ou do direito nacional aplicável, em especial no direito da União em matéria de proteção de dados pessoais.

2. Os prestadores que sejam instituições financeiras sujeitas a requisitos em matéria de governação, mecanismos ou processos internos nos termos do direito da União no domínio dos serviços financeiros devem manter os registos gerados automaticamente pelos sistemas de IA de risco elevado que disponibilizam como parte da documentação conservada nos termos da legislação aplicável no domínio dos serviços financeiros.

Artigo 20.º

Medidas corretivas e dever de informação

1. Os prestadores 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 imediatamente tomar as medidas corretivas necessárias para repor a conformidade do sistema em questão, proceder à sua retirada, desativação ou à recolha do mesmo, consoante o caso. Devem informar do facto os distribuidores do sistema de IA de risco elevado em questão e, se for caso disso, os responsáveis pela implantação, o mandatário e os importadores.

2. Se o sistema de IA de risco elevado apresentar um risco na aceção do artigo 79.º, n.º 1, e o prestador tomar conhecimento desse risco, o prestador deve imediatamente investigar as causas, em colaboração com o responsável pela implantação que tenha comunicado informações a esse respeito, se for o caso, e informar as autoridades de fiscalização do mercado competentes para o sistema de IA de elevado risco em causa e, se for o caso, o organismo notificado que emitiu um certificado para o sistema de IA de risco elevado em conformidade com o artigo 44.º, em especial sobre a natureza da não conformidade e as medidas corretivas tomadas.

Artigo 21.º

Cooperação com as autoridades competentes

1. Os prestadores de sistemas de IA de risco elevado devem, mediante pedido fundamentado de uma autoridade 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 na secção 2, numa língua que possa ser facilmente compreendida pela autoridade numa das línguas oficiais das instituições da União indicada pelo Estado-Membro em questão.

2. Mediante pedido fundamentado de uma autoridade competente, os prestadores devem igualmente conceder a essa autoridade, consoante o caso, o acesso aos registos gerados automaticamente do sistema de IA de risco elevado a que se refere o artigo 12.º, n.º 1, desde que esses registos estejam sob o seu controlo.

3. Todas as informações que uma autoridade competente obtenha nos termos do presente artigo devem ser tratadas nos termos das obrigações de confidencialidade estabelecidas no artigo 78.º.

Artigo 22.º

Mandatários dos prestadores de sistemas de IA de risco elevado

1. Antes de disponibilizarem os seus sistemas de IA de risco elevado no mercado da União, os prestadores estabelecidos em países terceiros devem, através de mandato escrito, designar um mandatário estabelecido na União.

2. O prestador deve habilitar o seu mandatário a desempenhar as funções especificadas no mandato conferido pelo prestador.

3. O mandatário deve desempenhar as funções especificadas no mandato conferido pelo prestador. Mediante pedido, o mandatário deve apresentar uma cópia do mandato às autoridades de fiscalização do mercado, numa das línguas oficiais das instituições da União indicada pela autoridade competente. Para efeitos do presente regulamento, o mandato habilita o mandatário a desempenhar as seguintes funções:

   a) Verificar se a declaração UE de conformidade referida no artigo 47.º e a documentação técnica a que se refere o artigo 11.º foram elaboradas e se o prestador efetuou um procedimento de avaliação da conformidade adequado;

   b) Manter à disposição das autoridades competentes e das autoridades ou organismos nacionais a que se refere o artigo 74.º, n.º 10, durante os dez anos subsequentes à data de colocação no mercado ou colocação em serviço do sistema de IA de risco elevado, os dados de contacto do prestador que designou o mandatário, uma cópia da declaração UE de conformidade referida no artigo 47.º, a documentação técnica e, se aplicável, o certificado emitido pelo organismo notificado;

   c) Prestar a uma autoridade competente, mediante pedido fundamentado, todas as informações e documentação, inclusive aquelas a que se refere a alínea b) do presente parágrafo, necessárias para demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos na secção 2 do presente título, incluindo o acesso aos registos, conforme referido no artigo 12.º, n.º 1, gerados automaticamente pelo sistema de IA de risco elevado, desde que esses registos estejam sob o controlo do prestador;

d) Cooperar com as autoridades competentes, mediante pedido fundamentado, em qualquer ação que estas empreendam em relação ao sistema de IA de risco elevado, nomeadamente para reduzir e atenuar os riscos colocados pelo mesmo;

e) Se for o caso, cumprir as obrigações de registo a que se refere o artigo 49.º, n.º 1, ou, se o registo for efetuado pelo próprio prestador, assegurar que as informações a que se refere o ponto 3 da secção A do anexo VIII, estejam corretas.

O mandato habilita o mandatário a ser contactado, em complemento ou em alternativa ao prestador, pelas autoridades competentes, sobre todas as questões relacionadas com a garantia do cumprimento do presente regulamento.

4. O mandatário põe termo ao mandato se considerar ou tiver razões para considerar que o prestador age de forma contrária às obrigações que lhe incumbem por força do presente regulamento. Nesse caso, informa de imediato a pertinente autoridade de fiscalização do mercado, bem como, se for caso disso, o organismo notificado pertinente, da cessação do mandato e da respetiva justificação.

Artigo 23.º

Obrigações dos importadores

1. Antes de colocarem um sistema de IA de risco elevado no mercado, os importadores devem assegurar-se de que o sistema está em conformidade com o presente regulamento, verificando se:

a) O prestador do sistema de IA de risco elevado realizou o procedimento de avaliação da conformidade pertinente a que se refere o artigo 43.º;

b) O prestador elaborou a documentação técnica em conformidade com o artigo 11.º e o anexo IV;

c) O sistema ostenta a marcação CE exigida e está acompanhado da declaração UE de conformidade referida no artigo 47.º e das instruções de utilização;

d) O prestador designou um mandatário em conformidade com o artigo 22.º, n.º 1.

2. Se um importador tiver motivos suficientes para crer que um sistema de IA de risco elevado não está em conformidade com o presente regulamento, ou é falsificado ou acompanhado de documentação falsificada, não pode colocar o sistema no mercado enquanto não for reposta a conformidade. Se o sistema de IA de risco elevado apresentar um risco na aceção do artigo 79.º, n.º 1, o importador deve informar desse facto o prestador do sistema, os mandatários e as autoridades de fiscalização do mercado.

3. Os importadores devem indicar o seu nome, nome comercial registado ou marca registada e endereço no qual podem ser contactados no sistema de IA de risco elevado e na respetiva embalagem ou na documentação que o acompanha, quando aplicável.

4. Enquanto um sistema de IA de risco elevado estiver sob a responsabilidade dos importadores, estes devem assegurar que as condições de armazenamento ou de transporte, se for caso disso, não prejudicam a conformidade do sistema com os requisitos enunciados na secção 2.

5. Os importadores devem conservar, durante os dez anos subsequentes à data de colocação no mercado ou colocação em serviço do sistema de IA de risco elevado, uma cópia do certificado emitido pelo organismo notificado, quando aplicável, das instruções de utilização e da declaração UE de conformidade referida no artigo 47.º.

6. Os importadores devem prestar às pertinentes autoridades competentes, mediante pedido fundamentado, todas as informações e documentação necessárias, inclusive as referidas no n.º 5, para demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos na secção 2, numa língua que possa ser facilmente compreendida pelas autoridades. Para o efeito, asseguram igualmente que a documentação técnica possa ser disponibilizada a essas autoridades.

7. Os importadores devem cooperar com as pertinentes autoridades competentes em todas as medidas que essas autoridades tomarem em relação a um sistema de IA de risco elevado colocados no mercado pelos importadores, nomeadamente para reduzir ou atenuar o risco colocado pelo sistema.

Artigo 24.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 CE exigida, se está acompanhado de uma cópia da declaração UE de conformidade referida no artigo 47.º e das instruções de utilização e se o prestador e o importador desse sistema, consoante o caso, cumpriram as suas obrigações estabelecidas no artigo 16.º, alíneas b) e c) e no artigo 23.º, n.º 3.

2. Se um distribuidor considerar ou tiver motivos para crer, com base nas informações que possui, que um sistema de IA de risco elevado não está em conformidade com os requisitos estabelecidos na secção 2, não pode disponibilizar esse sistema de IA de risco elevado no mercado enquanto não for reposta a conformidade com os referidos requisitos. Além disso, se o sistema de IA de risco elevado apresentar um risco na aceção do artigo 79.º, n.º 1, o distribuidor deve informar desse facto o prestador 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 que as condições de armazenamento ou de transporte, se for caso disso, não prejudiquem a conformidade do sistema com os requisitos enunciados na secção 2.

4. Um distribuidor que considere ou tenha motivos para crer, com base nas informações que possui, que um sistema de IA de risco elevado que disponibilizou no mercado não está em conformidade com os requisitos estabelecidos na secção 2 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 prestador, o importador ou qualquer operador envolvido, consoante o caso, tome essas medidas corretivas. Se um sistema de IA de risco elevado apresentar um risco na aceção do artigo 79.º, n.º 1, o distribuidor deve informar imediatamente desse facto o prestador ou o importador do sistema e as autoridades competentes para o sistema de IA de risco elevado em causa, apresentando dados, sobretudo no que se refere à não conformidade e às medidas corretivas tomadas.

5. Mediante pedido fundamentado de uma pertinente autoridade competente, os distribuidores de um sistema de IA de risco elevado prestam a essa autoridade todas as informações e documentação relativas às suas atividades previstas nos n.os 1 a 4 que sejam necessárias para demonstrar a conformidade desse sistema com os requisitos estabelecidos na secção 2.

6. Os distribuidores devem cooperar com as pertinentes autoridades competentes em todas as medidas que essas autoridades tomarem em relação a um sistema de IA de risco elevado disponibilizado no mercado pelos distribuidores, nomeadamente para reduzir ou atenuar o risco colocado pelo sistema.

Artigo 25.º

Responsabilidades ao longo da cadeia de valor da IA

1. Qualquer distribuidor, importador, responsável pela implantação ou outro terceiro é considerado um prestador de um sistema de IA de risco elevado para efeitos do presente regulamento e fica sujeito às obrigações dos prestadores estabelecidas no artigo 16.º em qualquer uma das seguintes circunstâncias:

   a) Se colocar o seu nome ou marca num sistema de IA de risco elevado já colocado no mercado ou colocado em serviço, sem prejuízo de disposições contratuais que estipulem uma atribuição diferente das obrigações;

   b) Se introduzir uma modificação substancial num sistema de IA de risco elevado que já tenha sido colocado no mercado ou colocado em serviço, de forma que o mesmo continue a ser um sistema de IA de risco elevado nos termos do artigo 6.º;

c) Se modificar a finalidade prevista de um sistema de IA, incluindo um sistema de IA de finalidade geral, que não tenha sido classificado como sendo de risco elevado e que já tenha sido colocado no mercado ou colocado em serviço, de forma que o sistema de IA em causa se torne um sistema de IA de risco elevado nos termos do artigo 6.º.

2. Sempre que se verificarem as circunstâncias a que se refere o n.º 1, o prestador que inicialmente colocou no mercado ou colocou em serviço o sistema de IA deixa de ser considerado um prestador desse sistema de IA específico para efeitos do presente regulamento. Esse prestador inicial deve cooperar estreitamente com novos prestadores, disponibilizar as informações necessárias e facultar o acesso técnico e a assistência razoavelmente esperados e necessários para o cumprimento das obrigações estabelecidas no presente regulamento, em especial no que diz respeito ao cumprimento da avaliação da conformidade dos sistemas de IA de risco elevado. O presente número não se aplica nos casos em que o prestador inicial tenha especificado claramente que o seu sistema de IA não deve ser alterado para um sistema de IA de risco elevado, não estando assim sujeito à obrigação de entregar a documentação.

3. No caso dos sistemas de IA de risco elevado que sejam componentes de segurança de produtos abrangidos pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I, secção A, o fabricante desses produtos é considerado o prestador do sistema de IA de risco elevado e fica sujeito às obrigações estabelecidas no artigo 16.º, caso se verifique uma das seguintes circunstâncias:

a) O sistema de IA de risco elevado é colocado no mercado juntamente com o produto sob o nome ou marca do fabricante do produto;

b) O sistema de IA de risco elevado é colocado em serviço sob o nome ou marca do fabricante do produto, depois de o produto ter sido colocado no mercado.

4. O prestador de um sistema de IA de risco elevado e o terceiro que disponibilize um sistema de IA, ferramentas, serviços, componentes ou processos que sejam utilizados ou integrados num sistema de IA de risco elevado devem, mediante acordo escrito, especificar as informações necessárias, as capacidades, o acesso técnico e demais assistência, com base no estado da arte geralmente reconhecido, a fim de permitir que o prestador do sistema de IA de risco elevado cumpra plenamente as obrigações estabelecidas no presente regulamento. O presente número não se aplica a terceiros que disponibilizem ao público ferramentas, serviços, processos ou componentes que não sejam modelos de IA de finalidade geral, ao abrigo de uma licença gratuita e aberta.

O Serviço para a IA pode desenvolver e recomendar modelos de cláusulas contratuais voluntários entre prestadores de sistemas de IA de risco elevado e terceiros que disponibilizem ferramentas, serviços, componentes ou processos utilizados ou integrados em sistemas de IA de risco elevado. Ao elaborar esses modelos de cláusulas voluntários, o Serviço para a IA deve ter em conta eventuais requisitos contratuais aplicáveis em setores ou casos comerciais específicos. Os modelos de cláusulas voluntários devem ser publicados e disponibilizados gratuitamente num formato eletrónico facilmente utilizável.

5. Os n.os 2 e 3 não prejudicam a necessidade de respeitar e proteger os direitos de propriedade intelectual, as informações comerciais de caráter confidencial e os segredos comerciais, em conformidade com o direito da União e o direito nacional.

Artigo 26.º

Obrigações dos responsáveis pela implantação de sistemas de IA de risco elevado

1. Os responsáveis pela implantação de sistemas de IA de risco elevado devem tomar medidas técnicas e organizativas adequadas para garantir que utilizam esses sistemas de acordo com as instruções de utilização que os acompanham, nos termos dos n.os 3 e 6.

2. Os responsáveis pela implantação devem atribuir a supervisão humana a pessoas singulares que possuam as competências, a formação e a autoridade necessárias, bem como o apoio necessário.

3. As obrigações estabelecidas nos n.os 1 e 2 não excluem outras obrigações do responsável pela implantação previstas no direito da União ou no direito nacional nem prejudicam a liberdade do responsável pela implantação para organizar os seus próprios recursos e atividades para efeitos de aplicação das medidas de supervisão humana indicadas pelo prestador.

4. Sem prejuízo do disposto nos n.os 1 e 2, na medida em que o responsável pela implantação exercer controlo sobre os dados de entrada, deve assegurar que os dados de entrada sejam pertinentes e suficientemente representativos tendo em vista a finalidade prevista do sistema de IA de risco elevado.

5. Os responsáveis pela implantação devem controlar o funcionamento do sistema de IA de risco elevado com base nas instruções de utilização e, se for caso disso, informam os prestadores em conformidade com o artigo 72.º. Se os responsáveis pela implantação tiverem motivos para considerar que a utilização do sistema de IA de risco elevado de acordo com as instruções pode conduzir a que aquele sistema de IA represente um risco na aceção do artigo 79.º, n.º 1, devem informar, sem demora injustificada, o prestador ou distribuidor e a autoridade de fiscalização do mercado competente e suspender a utilização do sistema. Sempre que os responsáveis pela implantação tenham identificado um incidente grave, devem também informar imediatamente desse incidente, em primeiro lugar, o prestador e, em seguida, o importador ou distribuidor e as autoridades de fiscalização do mercado competentes. Se o responsável pela implantação não conseguir entrar em contacto com o prestador, aplica-se, *mutatis mutandis*, o artigo 73.º. Esta obrigação não abrange os dados operacionais sensíveis dos responsáveis pela implantação de sistemas de IA que sejam autoridades responsáveis pela aplicação da lei.

Para os responsáveis pela implantação que sejam instituições financeiras sujeitas a requisitos em matéria de governação, mecanismos ou processos internos nos termos do direito da União no domínio dos serviços financeiros, considera-se que a obrigação de controlo estabelecida no primeiro parágrafo é satisfeita mediante o cumprimento das regras em matéria de governação, mecanismos ou processos internos nos termos da legislação aplicável no domínio dos serviços financeiros.

6. Os responsáveis pela implantação 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, por um período adequado à finalidade prevista do sistema de IA de risco elevado, de pelo menos seis meses, salvo disposição em contrário no direito da União ou no direito nacional aplicável, em especial no direito da União em matéria de proteção de dados pessoais.

Os responsáveis pela implantação que sejam instituições financeiras sujeitas a requisitos em matéria de governação, mecanismos ou processos internos nos termos do direito da União no domínio dos serviços financeiros devem manter os registos como parte da documentação conservada nos termos do direito da União aplicável no domínio dos serviços financeiros.

7. Antes da colocação em serviço ou da utilização de um sistema de IA de risco elevado no local de trabalho, os responsáveis pela implantação que sejam empregadores devem informar os representantes dos trabalhadores e os trabalhadores afetados de que estarão sujeitos à utilização do sistema de IA de risco elevado. Essas informações devem ser prestadas, se for o caso, em conformidade com as regras e os procedimentos estabelecidos na legislação e nas práticas da União e nacionais em matéria de informação dos trabalhadores e dos seus representantes.

8. Os responsáveis pela implantação de sistemas de IA de risco elevado que sejam autoridades públicas ou instituições, órgãos ou organismos da União devem cumprir as obrigações de registo referidas no artigo 49.º. Se esses responsáveis pela implantação verificarem que o sistema de IA de risco elevado que tencionam utilizar não foi registado na base de dados da UE a que se refere o artigo 71.º, não podem utilizar esse sistema e devem informar o prestador ou o distribuidor.

9. Se for o caso, os responsáveis pela implantação de sistemas de IA de risco elevado devem usar as informações recebidas nos termos do artigo 13.º do presente regulamento 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.

10. Sem prejuízo da Diretiva (UE) 2016/680, no âmbito de uma investigação seletiva de uma pessoa suspeita ou condenada por ter cometido uma infração penal, o responsável pela implantação de um sistema de IA de risco elevado destinado à identificação biométrica à distância em diferido deve solicitar uma autorização, prévia ou sem demora injustificada e no prazo máximo de 48 horas, a uma autoridade judiciária ou uma autoridade administrativa cuja decisão seja vinculativa e esteja sujeita a controlo jurisdicional, para a utilização desse sistema, exceto quando este seja utilizado para a identificação inicial de um potencial suspeito com base em factos objetivos e verificáveis diretamente relacionados com a infração. Cada utilização deve limitar-se ao estritamente necessário para a investigação de uma infração penal específica.

Se a autorização solicitada nos termos do primeiro parágrafo for rejeitada, a utilização do sistema de identificação biométrica à distância em diferido associado a essa autorização solicitada deve ser interrompida com efeitos imediatos e os dados pessoais relacionados com a utilização do sistema de IA de risco elevado para o qual a autorização foi solicitada devem ser apagados.

Em nenhuma circunstância esse sistema de IA de risco elevado destinado à identificação biométrica à distância em diferido pode ser utilizado para fins de aplicação da lei de forma não seletiva, sem qualquer ligação a uma infração penal, a um processo penal, a uma ameaça real e presente ou real e previsível de uma infração penal ou à busca de uma determinada pessoa desaparecida. Deve garantir-se que nenhuma decisão que produza efeitos jurídicos prejudiciais a uma pessoa possa ser tomada pelas autoridades responsáveis pela aplicação da lei exclusivamente com base nos resultados destes sistemas de identificação biométrica à distância em diferido.

O presente número não prejudica o artigo 9.º do Regulamento (UE) 2016/679 nem o artigo 10.º da Diretiva (UE) 2016/680 no que diz respeito ao tratamento de dados biométricos.

Independentemente da finalidade ou do responsável pela implantação, cada utilização destes sistemas de IA de risco elevado deve ser registada na documentação policial pertinente e disponibilizada à autoridade de fiscalização do mercado competente e à autoridade nacional de proteção de dados, mediante pedido, excluindo a divulgação de dados operacionais sensíveis relacionados com a aplicação da lei. O presente parágrafo não prejudica os poderes conferidos pela Diretiva (UE) 2016/680 às autoridades de controlo.

Os responsáveis pela implantação devem apresentar relatórios anuais às autoridades nacionais de fiscalização do mercado e às autoridades nacionais de proteção de dados competentes sobre a utilização que dão dos sistemas de identificação biométrica à distância em diferido, excluindo a divulgação de dados operacionais sensíveis relacionados com a aplicação da lei. Os relatórios podem ser agregados para abranger mais do que uma implantação.

Os Estados-Membros podem introduzir, em conformidade com o direito da União, legislação mais restritiva sobre a utilização de sistemas de identificação biométrica à distância em diferido.

11. Sem prejuízo do artigo 50.º do presente regulamento, os responsáveis pela implantação de sistemas de IA de risco elevado referidos no anexo III, que tomam decisões ou ajudam a tomar decisões relacionadas com pessoas singulares, devem informar as pessoas singulares de que estão sujeitas à utilização do sistema de IA de risco elevado. Para os sistemas de IA de risco elevado utilizados para fins de aplicação da lei, aplica-se o artigo 13.º da Diretiva (UE) 2016/680.

12. Os responsáveis pela implantação devem cooperar com as autoridades competentes em todas as medidas que essas autoridades tomarem em relação a um sistema de IA de risco elevado, a fim de aplicar o presente regulamento.

Artigo 27.º

Avaliação de impacto dos sistemas de IA de risco elevado sobre os direitos fundamentais

1. Antes de implementarem um sistema de IA de risco elevado a que se refere o artigo 6.º, n.º 2, à exceção dos sistemas de IA de risco elevado destinados a ser utilizados nos domínios enumerados no anexo III, ponto 2, os responsáveis pela implantação que sejam organismos de direito público, ou entidades privadas que prestam serviços públicos e responsáveis pela implantação de sistemas de IA de risco elevado a que se refere o anexo III, ponto 5, alíneas b) e c), devem executar uma avaliação do impacto que a utilização desse sistema possa ter nos direitos fundamentais. Para o efeito, os responsáveis pela implantação executam uma avaliação que inclua:

   a) Uma descrição dos processos do responsável pela implantação em que o sistema de IA de risco elevado seja utilizado de acordo com a sua finalidade prevista;

   b) Uma descrição do período em que o sistema de IA de risco elevado se destina a ser utilizado e com que frequência;

c) As categorias de pessoas singulares e grupos suscetíveis de serem afetados no contexto específico de utilização do sistema;

d) Os riscos específicos de danos suscetíveis de terem impacto nas categorias de pessoas singulares ou grupos de pessoas identificadas nos termos da alínea c) do presente número, tendo em conta as informações facultadas pelo prestador nos termos do artigo 13.º;

e) Uma descrição da aplicação das medidas de supervisão humana de acordo com as instruções de utilização;

f) As medidas a tomar caso esses riscos se materializem, incluindo as disposições relativas à governação interna e aos mecanismos de apresentação de queixas.

2. A obrigação estabelecida no n.º 1 aplica-se à primeira utilização do sistema de IA de risco elevado. O responsável pela implantação pode, em casos semelhantes, basear-se em avaliações de impacto sobre os direitos fundamentais efetuadas anteriormente ou em avaliações de impacto existentes realizadas pelo prestador. Se, durante a utilização do sistema de IA de risco elevado, o responsável pela implantação considerar que algum dos elementos enumerados no n.º 1 se alterou ou deixou de estar atualizado, deve tomar as medidas necessárias para atualizar as informações.

3. Uma vez realizada a avaliação de impacto a que se refere o n.º 1 do presente artigo, o responsável pela implantação deve notificar a autoridade de fiscalização do mercado dos resultados da avaliação, apresentando o modelo preenchido a que se refere o n.º 5 do presente artigo como parte da notificação. No caso referido no artigo 46.º, n.º 1, os responsáveis pela implantação podem ser dispensados desta obrigação de notificação.

4. Se alguma das obrigações previstas no presente artigo já tiver sido cumprida através da avaliação de impacto sobre a proteção de dados realizada nos termos do artigo 35.º do Regulamento (UE) 2016/679 ou do artigo 27.º da Diretiva (UE) 2016/680, a avaliação de impacto sobre os direitos fundamentais a que se refere o n.º 1 do presente artigo deve complementar essa avaliação de impacto sobre a proteção de dados.

5. O Serviço para a IA deve desenvolver um modelo para um questionário, nomeadamente através de um sistema automatizado, a fim de facilitar aos responsáveis pela implantação o cumprimento simplificado das obrigações do presente artigo.

SECÇÃO 4

AUTORIDADES NOTIFICADORAS E ORGANISMOS NOTIFICADOS

Artigo 28.º

Autoridades notificadoras

1. Cada Estado-Membro deve designar ou criar pelo menos 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 por fiscalizar esses organismos. Esses procedimentos devem ser desenvolvidos através da cooperação entre as autoridades notificadoras de todos os Estados-Membros.

2. Os Estados-Membros podem decidir que a avaliação e a fiscalização a que se refere o n.º 1 sejam efetuados por um organismo nacional de acreditação, na aceção e nos termos do Regulamento (CE) n.º 765/2008.

3. As autoridades notificadoras devem ser criadas, estar organizadas e funcionar de modo a garantir 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 ou exercer qualquer atividade que seja da competência dos organismos de avaliação da conformidade, nem propor ou prestar quaisquer serviços de consultoria com caráter comercial ou em regime de concorrência.

6. As autoridades notificadoras devem proteger a confidencialidade das informações que obtêm, em conformidade com o artigo 78.º.

7. As autoridades notificadoras devem dispor de recursos humanos com competência técnica em número adequado para o correto desempenho das suas funções. O pessoal com competência técnica deve dispor dos conhecimentos especializados necessários, consoante o caso, para o exercício das suas funções, em domínios como as tecnologias da informação, a IA e o direito, incluindo a supervisão dos direitos fundamentais.

Artigo 29.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 dos tipos de sistemas de IA em relação aos quais o organismo de avaliação da conformidade 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 31.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 apresentar à autoridade notificadora todas as provas documentais necessárias à verificação, ao reconhecimento e ao controlo regular da sua conformidade com os requisitos estabelecidos no artigo 31.º.

4. 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. O organismo notificado deve atualizar a documentação a que se referem os n.os 2 e 3 do presente artigo sempre que ocorram alterações pertinentes, a fim de permitir que a autoridade responsável pelos organismos notificados controle e verifique o cumprimento permanente de todos os requisitos estabelecidos no artigo 31.º.

Artigo 30.º

Procedimento de notificação

1. As autoridades notificadoras apenas podem notificar os organismos de avaliação da conformidade que cumpram os requisitos previstos no artigo 31.º.

2. As autoridades notificadoras devem notificar a Comissão e os restantes Estados-Membros sobre cada organismo de avaliação da conformidade a que se refere o n.º 1 utilizando o instrumento de notificação eletrónica criado e gerido pela Comissão.

3. A notificação a que se refere o n.º 2 do presente artigo deve incluir informações pormenorizadas sobre as atividades de avaliação da conformidade, o módulo ou módulos de avaliação da conformidade, os tipos de sistemas de IA em causa, e a declaração de competência pertinente. Caso a notificação não se baseie no certificado de acreditação a que se refere o artigo 29.º, n.º 2, a autoridade notificadora deve apresentar à Comissão e aos outros Estados-Membros provas documentais que atestem a competência do organismo de avaliação da conformidade e as disposições introduzidas para assegurar que o organismo seja acompanhado periodicamente e continue a cumprir os requisitos estabelecidos no artigo 31.º.

4. O organismo de avaliação da conformidade em causa apenas pode executar as atividades reservadas a organismos notificados se nem a Comissão nem os outros Estados-Membros tiverem formulado objeções nas duas semanas seguintes a uma notificação por uma autoridade notificadora, se esta incluir um certificado de acreditação a que se refere o artigo 29.º, n.º 2, ou nos dois meses seguintes a uma notificação por uma autoridade notificadora, se esta incluir as provas documentais a que se refere o artigo 29.º, n.º 3.

5. Caso sejam formuladas objeções, a Comissão deve proceder, sem demora, a consultas com os Estados-Membros pertinentes e o organismo de avaliação da conformidade. Tendo em conta essas consultas, a Comissão decide se a autorização se justifica. A Comissão designa o Estado-Membro em causa e o organismo de avaliação da conformidade pertinente como destinatários da decisão.

Artigo 31.º

Requisitos aplicáveis aos organismos notificados

1. Os organismos notificados devem ser constituídos nos termos da lei nacional de um Estado-Membro e ser dotados de personalidade jurídica.

2. Os organismos notificados devem satisfazer os requisitos em termos de organização, gestão da qualidade, recursos e processos que sejam necessários para o desempenho das suas funções, bem como requisitos de cibersegurança adequados.

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

4. Os organismos notificados devem ser independentes do prestador 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 outros operadores que tenham um interesse económico nos sistemas de IA de risco elevado que são avaliados, bem como nos dos concorrentes do prestador. Esta exigência não impede a utilização de sistemas de IA de risco elevado avaliados que sejam necessários para a atividade do organismo de avaliação da conformidade, nem a sua utilização para fins pessoais.

5. Os organismos de avaliação da conformidade, os seus quadros superiores e o pessoal encarregado de desempenhar as suas funções de avaliação da conformidade não podem intervir diretamente na conceção, no desenvolvimento, na comercialização ou na utilização de sistemas de IA de risco elevado, nem ser mandatários das pessoas envolvidas nessas atividades. Não podem igualmente exercer qualquer atividade que possa comprometer a independência da sua apreciação ou a sua integridade no desempenho das atividades de avaliação da conformidade para as quais são notificados. Esta disposição aplica-se, nomeadamente, aos serviços de consultoria.

6. 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 suscetíveis de salvaguardar essa imparcialidade e de promover e aplicar os princípios da imparcialidade em toda a sua organização, a todo o seu pessoal e em todas as suas atividades de avaliação.

7. 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, nos termos do artigo 78.º, a confidencialidade das informações de que tenham conhecimento durante a realização das atividades de avaliação da conformidade, salvo se a divulgação dessas informações 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 desempenho das suas funções no âmbito do presente regulamento, exceto em relação às autoridades notificadoras do Estado-Membro em que exerce as suas atividades.

8. Os organismos notificados devem dispor de procedimentos relativos ao exercício de atividades que tenham em devida conta a dimensão de um prestador, o setor em que opera, a sua estrutura e o grau de complexidade do sistema de IA em causa.

9. 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 onde se encontram estabelecidos nos termos da legislação nacional ou que o próprio Estado-Membro seja diretamente responsável pela avaliação da conformidade.

10. Os organismos notificados devem ser capazes de desempenhar todas as funções que lhes incumbem nos termos do presente regulamento com a maior integridade profissional e a competência exigida no domínio específico, quer essas funções sejam desempenhadas pelos próprios, quer em seu nome e sob a sua responsabilidade.

11. Os organismos notificados devem dispor de competências internas suficientes para poderem avaliar eficazmente as funções desempenhadas em seu nome por partes externas. Os organismos notificados devem dispor permanentemente de suficiente pessoal do domínio administrativo, técnico, jurídico e científico com experiência e conhecimentos relativos aos tipos de sistemas de IA em apreço, aos dados e à computação de dados e aos requisitos estabelecidos na secção 2.

12. Os organismos notificados devem participar em atividades de coordenação nos termos do artigo 38.º. Além disso, devem participar, diretamente ou por meio de representantes, em organizações europeias de normalização, ou assegurar que conhecem as normas aplicáveis e mantêm atualizado esse conhecimento.

Artigo 32.º

Presunção da conformidade com os requisitos aplicáveis aos organismos notificados

Presume-se que os organismos de avaliação da conformidade que provem a sua conformidade com os critérios estabelecidos nas normas harmonizadas aplicáveis, ou em partes destas, cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia* cumprem os requisitos previstos no artigo 31.º, contanto que as referidas normas harmonizadas contemplem esses requisitos.

Artigo 33.º

Filiais dos organismos notificados e subcontratação

1. Sempre que um organismo notificado subcontratar funções específicas relacionadas com a avaliação da conformidade ou recorrer a uma filial, deve assegurar que o subcontratante ou a filial cumpra os requisitos previstos no artigo 31.º e informar desse facto a autoridade notificadora.

2. Os organismos notificados assumem plena responsabilidade pelas funções que lhes incumbem que sejam desempenhadas por quaisquer subcontratantes ou filiais.

3. As atividades só podem ser exercidas por um subcontratante ou por uma filial mediante acordo do prestador. Os organismos notificados devem disponibilizar ao público uma lista das suas filiais.

4. Os documentos pertinentes respeitantes à avaliação das qualificações do subcontratante ou da filial e ao trabalho efetuado por estes nos termos do presente regulamento devem ser mantidos à disposição da autoridade notificadora durante um período de cinco anos a contar da data de termo da subcontratação.

Artigo 34.º

Obrigações operacionais dos organismos notificados

1. Os organismos notificados devem verificar a conformidade dos sistemas de IA de risco elevado de acordo com os procedimentos de avaliação da conformidade estabelecidos no artigo 43.º.

2. Os organismos notificados devem, no exercício das suas atividades, evitar encargos desnecessários para os prestadores e ter em devida conta a dimensão do prestador, o setor em que opera, a sua estrutura e o grau de complexidade do sistema de IA de risco elevado em causa, em especial com vista a minimizar os encargos administrativos e os custos de conformidade para as micro e pequenas empresas na aceção da Recomendação 2003/361/CE. Os organismos notificados devem, contudo, respeitar o grau de rigor e o nível de proteção exigidos para que o sistema de IA de risco elevado cumpra os requisitos do presente regulamento.

3. Os organismos notificados devem disponibilizar e, mediante pedido, apresentar toda a documentação importante, incluindo a documentação elaborada pelos prestadores, à autoridade notificadora a que se refere o artigo 28.º para que essa autoridade possa exercer as suas atividades de avaliação, designação, notificação e controlo e ainda para facilitar a avaliação descrita na presente secção.

Artigo 35.º

Números de identificação e listas de organismos notificados

1. A Comissão atribui um número de identificação único a cada organismo notificado, mesmo que um organismo seja notificado ao abrigo de mais do que um ato da União.

2. A Comissão publica a lista de organismos notificados ao abrigo do presente regulamento, incluindo os seus números de identificação e as atividades em relação às quais foram notificados. A Comissão deve assegurar que essa lista se mantém atualizada.

Artigo 36.º

Alterações das notificações

1. A autoridade notificadora deve notificar a Comissão e os outros Estados-Membros de todas as alterações pertinentes da notificação de um organismo notificado através do instrumento de notificação eletrónica a que se refere o artigo 30.º, n.º 2.

2. Os procedimentos estabelecidos nos artigos 29.º e 30.º aplicam-se ao alargamento do âmbito da notificação.

No que respeita às alterações da notificação que não digam respeito ao alargamento do seu âmbito de aplicação, são aplicáveis os procedimentos estabelecidos nos n.ºs 3 a 9.

3. Caso um organismo notificado decida cessar as suas atividades de avaliação da conformidade, informa a autoridade notificadora e os prestadores em causa o mais rapidamente possível e, em caso de cessação planeada, pelo menos um ano antes de cessar as atividades. Os certificados do organismo notificado podem manter-se válidos durante um período de nove meses após a cessação das atividades do organismo notificado, desde que outro organismo notificado confirme por escrito que assumirá a responsabilidade pelos sistemas de IA de risco elevado abrangidos por esses certificados. Esse outro organismo notificado efetua uma avaliação completa dos sistemas de IA de risco elevado em causa até ao final do período de nove meses, antes de emitir novos certificados para esses sistemas. Se o organismo notificado tiver cessado a sua atividade, a autoridade notificadora deve retirar a designação.

4. Caso uma autoridade notificadora tenha motivos suficientes para considerar que um organismo notificado deixou de cumprir os requisitos estabelecidos no artigo 31.º, ou que não cumpre as suas obrigações, deve imediatamente investigar a matéria com a máxima diligência. Nesse contexto, a autoridade notificadora deve informar o organismo notificado em causa sobre as objeções formuladas e dar-lhe a possibilidade de apresentar as suas observações. Caso a autoridade notificadora conclua que o organismo notificado deixou de cumprir os requisitos estabelecidos no artigo 31.º, ou que não cumpre as suas obrigações, deve restringir, suspender ou retirar a designação, consoante o caso, em função da gravidade do incumprimento desses requisitos ou dessas obrigações. A autoridade notificadora deve informar imediatamente a Comissão e os restantes Estados-Membros deste facto.

5. Caso a sua designação tenha sido suspendida, restringida ou revogada, na totalidade ou em parte, o organismo notificado informa os prestadores em causa o mais tardar no prazo de dez dias.

6. Em caso de restrição, suspensão ou retirada de uma designação, a autoridade notificadora deve tomar as medidas necessárias para assegurar que os processos do organismo notificado são conservados e para os disponibilizar às autoridades notificadoras noutros Estados-Membros e às autoridades de fiscalização do mercado, se estas o solicitarem.

7. Em caso de restrição, suspensão ou retirada de uma designação, a autoridade notificadora:

   a) Avalia o impacto nos certificados emitidos pelo organismo notificado;

   b) Apresenta à Comissão e aos outros Estados-Membros um relatório sobre as suas conclusões no prazo de três meses após ter notificado das alterações à designação;

c) Determina que o organismo notificado suspenda ou retire, num prazo razoável por ela determinado, os certificados indevidamente emitidos, a fim de garantir a conformidade contínua dos sistemas de IA de risco elevado no mercado;

d) Informa a Comissão e os Estados-Membros dos certificados para os quais exigiu a suspensão ou retirada;

e) Presta às autoridades nacionais competentes do Estado-Membro em que o prestador tem a sua sede social todas as informações pertinentes sobre os certificados para os quais exigiu a suspensão ou retirada; essas autoridades devem tomar as medidas adequadas que se revelem necessárias para evitar potenciais riscos para a saúde, a segurança ou os direitos fundamentais.

8. Com exceção dos certificados indevidamente emitidos, e caso uma designação tenha sido suspendida ou restringida, os certificados permanecem válidos nas seguintes circunstâncias:

a) Quando a autoridade notificadora tiver confirmado, no prazo de um mês a contar da suspensão ou restrição, que, no que respeita aos certificados afetados pela suspensão ou restrição, não existem riscos para a saúde, a segurança ou os direitos fundamentais, e tiver estabelecido um prazo para as ações previstas para corrigir a suspensão ou restrição; ou

b) Quando a autoridade notificadora tiver confirmado que, durante o período de suspensão ou restrição, não serão emitidos, alterados nem reemitidos certificados relevantes para a suspensão, e indicar se o organismo notificado tem capacidade para continuar a assumir, durante o período de suspensão ou restrição, o controlo e a responsabilidade pelos certificados já emitidos; caso a autoridade notificadora determine que o organismo notificado não tem capacidade para apoiar os certificados já emitidos, o prestador do sistema abrangido pelo certificado deve confirmar por escrito às autoridades nacionais competentes do Estado-Membro em que tem a sua sede social, no prazo de três meses a contar da suspensão ou restrição, que outro organismo notificado qualificado exerce temporariamente as funções do organismo notificado de assunção do controlo e da responsabilidade pelos certificados durante o período de suspensão ou restrição.

9. Com exceção dos certificados emitidos indevidamente, e sempre que a designação tenha sido retirada, os certificados permanecem válidos por um período de nove meses nas seguintes circunstâncias:

a) Se a autoridade nacional competente do Estado-Membro em que o prestador do sistema de IA de risco elevado abrangido pelo certificado tem a sua sede social tiver confirmado que não existem riscos associados aos sistemas de IA de risco elevado em causa para a saúde, a segurança ou os direitos fundamentais; e

b) Se um outro organismo notificado tiver confirmado por escrito que assumirá de imediato a responsabilidade por esses sistemas de IA e concluir a respetiva avaliação no prazo de doze meses a contar da retirada da designação.

Nas circunstâncias referidas no primeiro parágrafo, a autoridade nacional competente do Estado-Membro em que o prestador do sistema abrangido pelo certificado tem a sua sede social pode prorrogar a validade provisória dos certificados por novos períodos de três meses, até um máximo de 12 meses no total.

A autoridade nacional competente ou o organismo notificado que assumir as funções do organismo notificado ao qual se aplica a alteração da designação informa imediatamente desse facto a Comissão, os outros Estados-Membros e os demais organismos notificados.

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 da competência de um organismo notificado ou do cumprimento continuado dos requisitos estabelecidos no artigo 31.º e das responsabilidades aplicáveis por parte de um organismo notificado.

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

3. A Comissão garante que todas as informações sensíveis obtidas no decurso das suas investigações nos termos do presente artigo sejam tratadas de forma confidencial em conformidade com o artigo 78.º.

4. Caso verifique que um organismo notificado não cumpre ou deixou de cumprir os requisitos aplicáveis à sua notificação, a Comissão informa o Estado-Membro notificador do facto e solicita-lhe que tome as medidas corretivas necessárias, incluindo, se for caso disso, a suspensão ou retirada da notificação. Se o Estado-Membro não tomar as medidas corretivas necessárias, a Comissão pode, por meio de um ato de execução, suspender, restringir ou retirar a designação. O referido ato de execução é adotado de acordo com o procedimento de exame a que se refere o artigo 98.º, n.º 2.

Artigo 38.º

Coordenação dos organismos notificados

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

2. Cada autoridade notificadora deve assegurar que os organismos por si notificados participem, diretamente ou por meio de representantes designados, nos trabalhos de um grupo a que se refere o n.º 1.

3. A Comissão deve proporcionar o intercâmbio de conhecimentos especializados e de boas práticas entre as autoridades notificadoras.

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, desde que cumpram os requisitos previstos no artigo 31.º ou garantam um nível de cumprimento equivalente.

Secção 5

Normas, avaliação da conformidade, certificados, registo

Artigo 40.º

Normas harmonizadas e produtos de normalização

1. Presume-se que os sistemas de IA de risco elevado ou os modelos de IA de finalidade geral que estão em conformidade com normas harmonizadas, ou com partes destas, cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia* nos termos do Regulamento (UE) n.º 1025/2012, são conformes com os requisitos estabelecidos na secção 2 do presente capítulo, ou, consoante o caso, com as obrigações estabelecidas nas secções 2 e 3 do capítulo V do presente regulamento, desde que tais normas abranjam esses requisitos ou obrigações.

2. Nos termos do artigo 10.º do Regulamento (UE) n.º 1025/2012, a Comissão emite, sem demora injustificada, pedidos de normalização que abranjam todos os requisitos estabelecidos na secção 2 do presente capítulo e, conforme aplicável, pedidos de normalização que abranjam as obrigações estabelecidas nas secções 2 e 3 do capítulo V do presente regulamento. Os pedidos de normalização devem também solicitar produtos respeitantes aos processos de comunicação e documentação para melhorar o desempenho dos sistemas de IA em termos de recursos, como a redução do consumo de energia e de outros recursos do sistema de IA de risco elevado durante o seu ciclo de vida, e respeitantes ao desenvolvimento eficiente do ponto de vista energético de modelos de IA de finalidade geral. Ao preparar um pedido de normalização, a Comissão deve consultar o Comité e as partes interessadas pertinentes, incluindo o fórum consultivo.

Ao enviar um pedido de normalização a uma organização europeia de normalização, a Comissão deve especificar que as normas têm de ser claras, coerentes, nomeadamente com as normas desenvolvidas nos vários setores para os produtos abrangidos pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I, e que se destinam a assegurar que os sistemas de IA de risco elevado ou modelos de IA de finalidade geral colocados no mercado ou colocados em serviço na União cumprem os requisitos ou obrigações pertinentes estabelecidos no presente regulamento.

A Comissão deve solicitar às organizações europeias de normalização que apresentem provas dos seus melhores esforços para cumprir os objetivos referidos no primeiro e segundo parágrafos do presente número, em conformidade com o artigo 24.º do Regulamento (UE) n.º 1025/2012.

3. Os participantes no processo de normalização devem procurar promover o investimento e a inovação no domínio da IA, nomeadamente através do aumento da segurança jurídica, bem como a competitividade e o crescimento do mercado da União, contribuir para o reforço da cooperação mundial em matéria de normalização, tendo em conta as normas internacionais existentes no domínio da IA que sejam compatíveis com os valores, os direitos fundamentais e os interesses da União, e reforçar a governação multilateral, assegurando uma representação equilibrada dos interesses e a participação efetiva de todas as partes interessadas pertinentes, em conformidade com os artigos 5.º, 6.º e 7.º do Regulamento (UE) n.º 1025/2012.

Artigo 41.º

Especificações comuns

1. A Comissão pode adotar atos de execução que estabeleçam especificações comuns para os requisitos estabelecidos na secção 2 do presente capítulo, ou, se for caso disso, para as obrigações estabelecidas nas secções 2 e 3 do capítulo V, se estiverem preenchidas as seguintes condições:

   a) A Comissão pediu, nos termos do artigo 10.º, n.º 1, do Regulamento (UE) n.º 1025/2012, a uma ou mais organizações europeias de normalização que elaborassem uma norma harmonizada para os requisitos estabelecidos na secção 2 do presente capítulo, ou, conforme aplicável, para as obrigações estabelecidas nas secções 2 e 3 do capítulo V, e:

      i) o pedido não foi aceite por nenhuma das organizações europeias de normalização, ou

ii) as normas harmonizadas relativas a esse pedido não foram entregues no prazo fixado em conformidade com o artigo 10.º, n.º 1, do Regulamento (UE) n.º 1025/2012, ou

iii) as normas harmonizadas pertinentes não dão resposta suficiente às preocupações em matéria de direitos fundamentais, ou

iv) as normas harmonizadas não cumprem o pedido; e

b) Não se encontra publicada no *Jornal Oficial da União Europeia* qualquer referência a normas harmonizadas que abranjam os requisitos referidos na secção 2 do presente capítulo ou, conforme aplicável, para as obrigações referidas nas secções 2 e 3 do capítulo V, em conformidade com o Regulamento (UE) n.º 1025/2012, e não se prevê a publicação de tal referência dentro de um prazo razoável.

Quando elaborar as especificações comuns, a Comissão deverá consultar o fórum consultivo a que se refere o artigo 67.º.

Os atos de execução a que se refere o primeiro parágrafo do presente número são adotados de acordo com o procedimento de exame a que se refere o artigo 98.º, n.º 2.

2. Antes de elaborar um projeto de ato de execução, a Comissão informa o comité a que se refere o artigo 22.º do Regulamento (UE) n.º 1025/2012 de que considera que estão preenchidas as condições estabelecidas no n.º 1 do presente artigo.

3. Presume-se que os sistemas de IA de risco elevado ou os modelos de IA de finalidade geral que estão em conformidade com as especificações comuns a que se refere o n.º 1, ou com partes dessas especificações, são conformes com os requisitos estabelecidos na secção 2 do presente capítulo, ou, conforme aplicável, que cumprem as obrigações referidas nas secções 2 e 3 do capítulo V, desde que tais especificações comuns abranjam esses requisitos ou essas obrigações.

4. Sempre que uma norma harmonizada seja adotada por uma organização europeia de normalização e a publicação da sua referência no *Jornal Oficial da União Europeia* seja proposta à Comissão, esta última avalia a norma harmonizada nos termos do Regulamento (UE) n.º 1025/2012. Quando a referência a uma norma harmonizada é publicada no *Jornal Oficial da União Europeia*, a Comissão revoga os atos de execução a que se refere o n.º 1, ou partes desses atos de execução que abranjam os mesmos requisitos estabelecidos na secção 2 do presente capítulo ou, conforme aplicável, as mesmas obrigações estabelecidas nas secções 2 e 3 do capítulo V.

5. Os prestadores de sistemas de IA de risco elevado ou os modelos de IA de finalidade geral que não cumprirem as especificações comuns a que se refere o n.º 1 devem justificar devidamente que adotaram soluções técnicas que cumprem os requisitos referidos na secção 2 do presente capítulo, ou, conforme aplicável, as obrigações estabelecidas nas secções 2 e 3 do capítulo V, a um nível, no mínimo, equivalente.

6. Caso um Estado-Membro considere que uma especificação comum não cumpre inteiramente os requisitos estabelecidos na secção 2 ou, conforme aplicável, as obrigações estabelecidas nas secções 2 e 3 do capítulo V, informa a Comissão desse facto, apresentando uma explicação pormenorizada. A Comissão avalia essas informações e, se for caso disso, altera o ato de execução que estabelece a especificação comum em causa.

Artigo 42.º

Presunção de conformidade com determinados requisitos

1. Presume-se que os sistemas de IA de risco elevado que foram treinados e testados com recurso a dados que refletem o cenário geográfico, comportamental, contextual ou funcional específico no qual se destinam a ser utilizados são conformes com os requisitos pertinentes estabelecidos 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 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, se, ao demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos na secção 2, o prestador tiver aplicado as normas harmonizadas a que se refere o artigo 40.º, ou, se for caso disso, as especificações comuns a que se refere o artigo 41.º, o prestador deve optar por um dos seguintes procedimentos:

   a) O controlo interno a que se refere o anexo VI; ou

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

   Ao demonstrar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos na secção 2, o prestador deve seguir o procedimento de avaliação da conformidade estabelecido no anexo VII quando:

   a) Não existam as normas harmonizadas a que se refere o artigo 40.º e não estejam disponíveis as especificações comuns a que se refere o artigo 41.º;

   b) O prestador não tenha aplicado, ou tenha aplicado apenas parcialmente, a norma harmonizada;

   c) Existam as especificações comuns a que se refere a alínea a), mas o prestador não as tenha aplicado;

d) Uma ou mais das normas harmonizadas a que se refere a alínea a) tenham sido publicadas com uma restrição, e apenas no tocante à parte da norma que foi objeto da restrição.

Para efeitos do procedimento de avaliação da conformidade a que se refere o anexo VII, o prestador pode escolher qualquer um dos organismos notificados. Contudo, caso o sistema de IA de risco elevado se destine a ser colocado em serviço por autoridades competentes em matéria de aplicação da lei, imigração ou asilo ou por instituições, órgãos e organismos da UE, a autoridade de fiscalização do mercado a que se refere o artigo 74.º, n.os 8 ou 9, consoante aplicável, atua como organismo notificado.

2. Em relação aos sistemas de IA de risco elevado enumerados no anexo III, pontos 2 a 8, os prestadores 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.

3. Em relação aos sistemas de IA de risco elevado abrangidos pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I, secção A, o prestador deve seguir o procedimento de avaliação da conformidade aplicável nos termos desses atos jurídicos. Os requisitos estabelecidos na secção 2 do presente capítulo 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 nos termos dos referidos atos jurídicos ficam habilitados a verificar a conformidade dos sistemas de IA de risco elevado com os requisitos estabelecidos na secção 2, contanto que a conformidade desses organismos notificados com os requisitos estabelecidos no artigo 31.º, n.os 4, 5, 10 e 11, tenha sido avaliada no contexto do procedimento de notificação previsto nesses atos jurídicos.

Sempre que um ato jurídico enumerado na secção A do anexo I permita que o fabricante do produto renuncie a uma avaliação da conformidade por terceiros, desde que esse fabricante tenha aplicado todas as normas harmonizadas que abrangem os requisitos previstos nesses atos, o fabricante apenas pode recorrer a 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 todos os requisitos estabelecidos na secção 2 do presente capítulo.

4. Os sistemas de IA de risco elevado que já tenham sido sujeitos a um procedimento de avaliação da conformidade devem ser sujeitos a um novo procedimento de avaliação da conformidade caso sejam substancialmente modificados, independentemente de o sistema modificado se destinar a distribuição ulterior ou continuar a ser utilizado pelo atual responsável pela implantação.

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

5. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 97.º para alterar os anexos VI e VII atualizando-os à luz da evolução técnica.

6. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 97.º para alterar os n.os 1 e 2 do presente artigo, a fim de sujeitar os sistemas de IA de risco elevado a que se refere o anexo III, pontos 2 a 8, à totalidade, ou a parte, do procedimento de avaliação da conformidade a que se refere o anexo VII. 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 no que toca à prevenção ou minimização dos riscos que esses sistemas representam para a saúde e a segurança e para a proteção dos direitos fundamentais, bem como a disponibilidade de capacidades e recursos adequados nos organismos notificados.

Artigo 44.º

Certificados

1. Os certificados emitidos pelos organismos notificados em conformidade com o anexo VII devem ser redigidos numa língua que possa ser facilmente compreendida pelas autoridades competentes do Estado-Membro em que o organismo notificado estiver estabelecido.

2. Os certificados são válidos pelo período neles indicado, que não pode exceder cinco anos para os sistemas de IA abrangidos pelo anexo I e quatro anos para os sistemas de IA abrangidos pelo anexo III. A pedido do prestador, a validade de um certificado pode ser prorrogada por novos períodos não superiores a cinco anos para os sistemas de IA abrangidos pelo anexo I e a quatro anos para os sistemas de IA abrangidos pelo anexo III, com base numa reavaliação segundo os procedimentos de avaliação da conformidade aplicáveis. Os eventuais aditamentos a um certificado permanecem válidos, desde que o certificado a que dizem respeito seja válido.

3. Se verificar que um sistema de IA deixou de cumprir os requisitos estabelecidos na secção 2, o organismo notificado deve suspender, retirar ou restringir o certificado emitido, tendo em conta o princípio da proporcionalidade, a não ser que o prestador do sistema assegure o cumprimento desses requisitos tomando as medidas corretivas necessárias num prazo adequado estabelecido pelo organismo notificado. O organismo notificado deve fundamentar a sua decisão.

Deve prever-se um procedimento de recurso das decisões dos organismos notificados, incluindo sobre os certificados de conformidade emitidos.

Artigo 45.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 de sistemas de gestão da qualidade emitidos em conformidade 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 do anexo VII;

c) 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 exercidas no âmbito da respetiva notificação e quaisquer outras atividades exercidas, nomeadamente atividades transfronteiriças 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, mediante pedido, as aprovações que tenha concedido a sistemas de qualidade;

b) Os certificados da União de avaliação da documentação técnica ou quaisquer suplementos dos mesmos que tenha recusado, retirado, suspendido ou restringido e, mediante 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 e relativas aos mesmos tipos de sistemas de IA informações importantes sobre questões relativas aos resultados negativos e, mediante pedido, aos resultados positivos dos procedimentos de avaliação da conformidade.

4. Os organismos notificados devem proteger a confidencialidade das informações que obtêm, em conformidade com o artigo 78.º.

Artigo 46.º

Derrogação do procedimento de avaliação da conformidade

1. Em derrogação do artigo 43.º e mediante pedido devidamente justificado, 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 ou de proteção de ativos industriais e infraestruturas essenciais. Essa autorização é concedida por um período limitado enquanto estiverem em curso os procedimentos de avaliação da conformidade necessários, tendo em conta as razões excecionais que justificam a derrogação. Esses procedimentos devem ser concluídos sem demora injustificada.

2. Em situações de urgência devidamente justificadas por motivos excecionais de segurança pública ou em caso de ameaça específica, substancial e iminente para a vida ou a segurança física de pessoas singulares, as autoridades responsáveis pela aplicação da lei ou as autoridades da proteção civil podem colocar em serviço um sistema de IA de risco elevado específico sem a autorização a se refere o n.º 1, desde que essa autorização seja solicitada durante ou após a utilização, sem demora injustificada. Se a autorização a que se refere o n.º 1 for recusada, a utilização do sistema de IA de risco elevado deve ser suspensa com efeito imediato e todos os resultados dessa utilização devem ser imediatamente descartados.

3. A autorização a que se refere o n.º 1 só deve ser concedida se a autoridade de fiscalização do mercado concluir que o sistema de IA de risco elevado cumpre os requisitos da secção 2. A autoridade de fiscalização do mercado deve informar a Comissão e os outros Estados-Membros sobre as autorizações concedidas nos termos dos n.ºs 1 e 2. Esta obrigação não abrange os dados operacionais sensíveis relativos às atividades das autoridades responsáveis pela aplicação da lei.

4. Se, no prazo de 15 dias a contar da receção da informação a que se refere o n.º 3, nem os Estados-Membros nem a Comissão tiverem formulado 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 autorização é justificada.

5. Se, nos 15 dias subsequentes à receção da notificação a que se refere o n.º 3, um Estado-Membro formular 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 sobre a conformidade do sistema a que se refere o n.º 3 é infundada, a Comissão procede sem demora a consultas com o Estado-Membro em causa. Os operadores em causa devem ser consultados e ter a possibilidade de apresentar as suas observações. Tendo em conta essas consultas, a Comissão decide se a autorização se justifica. A Comissão designa o Estado-Membro e os operadores em causa como destinatários da decisão.

6. Se a Comissão considerar que a autorização é injustificada, a autoridade de fiscalização do mercado do Estado-Membro em causa deve retirá-la.

7. No caso dos sistemas de IA de risco elevado relacionados com produtos abrangidos pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I, secção A, só são aplicáveis as derrogações à avaliação da conformidade previstas nessa mesma legislação.

Artigo 47.º

Declaração UE de conformidade

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

2. A declaração UE de conformidade deve mencionar que o sistema de IA de risco elevado em causa cumpre os requisitos estabelecidos na secção 2. A declaração UE de conformidade deve conter as informações indicadas no anexo V e ser traduzida para uma língua que possa ser facilmente compreendida pelas autoridades nacionais competentes dos Estados-Membros em que o sistema de IA de risco elevado seja colocado no mercado ou disponibilizado.

3. Se os sistemas de IA de risco elevado estiverem sujeitos a outra legislação de harmonização da União que também exija uma declaração UE de conformidade, deve ser elaborada uma única declaração UE de conformidade respeitante a todo o direito da União 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 UE de conformidade, o prestador assume a responsabilidade pelo cumprimento dos requisitos estabelecidos na secção 2. O prestador deve manter a declaração UE de conformidade atualizada na medida do necessário.

5. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 97.º para alterar o anexo V através da atualização do conteúdo da declaração UE de conformidade estabelecido nesse anexo, a fim de introduzir elementos que se tornem necessários à luz da evolução técnica.

Artigo 48.º

Marcação CE

1. A marcação CE está sujeita aos princípios gerais enunciados no artigo 30.º do Regulamento (CE) n.º 765/2008.

2. No caso dos sistemas de IA de risco elevado disponibilizados digitalmente, só deve ser utilizada uma marcação CE digital se esta for facilmente acessível através da interface a partir da qual se acede a esse sistema ou através de um código legível por máquina facilmente acessível ou por outros meios eletrónicos.

3. A marcação CE deve ser aposta de modo visível, legível e indelével nos 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 for mais adequado.

4. Quando aplicável, a marcação CE deve ser acompanhada do número de identificação do organismo notificado responsável pelos procedimentos de avaliação da conformidade estabelecidos no artigo 43.º. O número de identificação do organismo notificado deve ser aposto pelo próprio organismo ou, segundo as suas instruções, pelo prestador ou pelo seu mandatário. O número de identificação deve ser também indicado em todo o material promocional que mencione que o sistema de IA de risco elevado cumpre os requisitos aplicáveis à marcação CE.

5. Caso os sistemas de IA de risco elevado sejam objeto de outro direito da União que também preveja a aposição da marcação CE, essa marcação deve indicar que os sistemas de IA de risco elevado cumprem igualmente os requisitos desse outro direito.

Artigo 49.º

Registo

1. Antes da colocação no mercado ou da colocação em serviço de um sistema de IA de risco elevado enumerado no anexo III, com exceção dos sistemas de IA de risco elevado a que se refere o anexo III, ponto 2, o prestador ou, se for caso disso, o mandatário deve registar-se e registar o seu sistema na base de dados da UE a que se refere o artigo 71.º.

2. Antes da colocação no mercado ou da colocação em serviço de um sistema de IA relativamente ao qual o prestador tenha concluído que não é de risco elevado nos termos do artigo 6.º, n.º 3, esse prestador ou, se for caso disso, o mandatário deve registar-se e registar esse sistema na base de dados da UE a que se refere o artigo 71.º.

3. Antes de colocarem em serviço ou utilizarem um dos sistemas de IA de risco elevado enumerados no anexo III, com exceção dos sistemas de IA de risco elevado enumerados no ponto 2 do anexo III, os responsáveis pela implantação que sejam autoridades públicas, instituições, órgãos ou organismos da União ou pessoas que atuem em seu nome devem registar-se, selecionar o sistema e registar a sua utilização na base de dados da UE a que se refere o artigo 71.º.

4. No caso dos sistemas de IA de risco elevado a que se refere o anexo III, pontos 1, 6 e 7, nos domínios da aplicação da lei, da migração, do asilo e da gestão do controlo das fronteiras, o registo referido nos n.os 1, 2 e 3 do presente artigo deve ser efetuado numa secção segura e não pública da base de dados da UE a que se refere o artigo 71.º e incluir apenas as seguintes informações, conforme aplicável, a que se referem:

   a) O anexo VIII, secção A, pontos 1 a 10, com exceção dos pontos 6, 8 e 9;

   b) O anexo VIII, secção B, pontos 1 a 5 e pontos 8 e 9;

   c) O anexo VIII, secção C, pontos 1 a 3;

   d) O anexo IX, pontos 1, 2, 3 e 5.

Só a Comissão e as autoridades nacionais referidas no artigo 74.º, n.º 8, têm acesso às respetivas secções restritas da base de dados da UE a que se refere o primeiro parágrafo do presente número.

5. Os sistemas de IA de risco elevado a que se refere o anexo III, ponto 2, devem ser registados a nível nacional.

Capítulo IV
Obrigações de transparência aplicáveis aos prestadores e responsáveis pela implantação de determinados sistemas de Inteligência Artificial

Artigo 50.º

Obrigações de transparência aplicáveis aos prestadores e responsáveis pela implantação de determinados sistemas de inteligência artificial

1. Os prestadores devem assegurar que os sistemas de IA destinados a interagir diretamente com pessoas singulares sejam concebidos e desenvolvidos de maneira que as pessoas singulares em causa sejam informadas de que estão a interagir com um sistema de IA, salvo se tal for óbvio do ponto de vista de uma pessoa singular razoavelmente informada, atenta e advertida, tendo em conta as circunstâncias e o contexto de utilização. Esta obrigação não se aplica a sistemas de IA legalmente autorizados para detetar, prevenir, investigar ou reprimir infrações penais, sob reserva de garantias adequadas dos direitos e liberdades de terceiros, salvo se esses sistemas estiverem disponíveis ao público para denunciar uma infração penal.

2. Os prestadores de sistemas de IA, incluindo sistemas de IA de finalidade geral, que geram conteúdos sintéticos de áudio, imagem, vídeo ou texto, devem assegurar que os resultados do sistema de IA sejam marcados num formato legível por máquina e detetáveis como tendo sido artificialmente gerados ou manipulados. Os prestadores devem assegurar que as suas soluções técnicas são eficazes, interoperáveis, sólidas e fiáveis, na medida em que tal seja tecnicamente viável, tendo em conta as especificidades e limitações dos vários tipos de conteúdos, os custos de aplicação e o estado da arte geralmente reconhecido, tal como estiver refletido em normas técnicas pertinentes. Esta obrigação não se aplica na medida em que os sistemas de IA desempenhem uma função de apoio à edição normalizada ou não alterem substancialmente os dados de entrada disponibilizados pelo responsável pela implantação ou a semântica dos mesmos, ou quando a sua utilização for autorizada por lei para detetar, prevenir, investigar e reprimir infrações penais.

3. Os responsáveis pela implantação de um sistema de reconhecimento de emoções ou de um sistema de categorização biométrica devem informar as pessoas expostas a esse sistema do seu funcionamento e tratar os dados pessoais em conformidade com os Regulamentos (UE) 2016/679, e (UE) 2018/1725 e a Diretiva (UE) 2016/680, conforme aplicável. Esta obrigação não se aplica aos sistemas de IA usados para categorização biométrica e reconhecimento de emoções legalmente autorizados para detetar, prevenir ou investigar infrações penais, sob reserva de garantias adequadas dos direitos e liberdades de terceiros, e nos termos do direito da União.

4. Os responsáveis pela implantação de um sistema de IA que gere ou manipule conteúdos de imagem, áudio ou vídeo que constituam uma falsificação profunda devem revelar que os conteúdos foram artificialmente gerados ou manipulados. Esta obrigação não se aplica se a utilização for autorizada por lei para detetar, prevenir, investigar ou reprimir infrações penais. Sempre que os conteúdos façam parte de um programa ou obra de natureza manifestamente artística, criativa, satírica, ficcional ou análoga, as obrigações de transparência estabelecidas no presente número limitam-se à divulgação da existência desses conteúdos gerados ou manipulados, de uma forma adequada que não prejudique a exibição ou a fruição da obra.

Os responsáveis pela implantação de um sistema de IA que gere ou manipule texto publicado com o objetivo de informar o público sobre questões de interesse público devem revelar que o texto foi artificialmente gerado ou manipulado. Esta obrigação não se aplica se a utilização for autorizada por lei para detetar, prevenir, investigar e reprimir infrações penais ou se os conteúdos gerados por IA tiverem sido objeto de um processo de análise humana ou de controlo editorial e se uma pessoa singular ou coletiva for responsável editorial pela publicação do conteúdo.

5. As informações a que se referem os n.os 1 a 4 são prestadas às pessoas singulares em causa de forma clara e percetível o mais tardar aquando da primeira interação ou exposição. As informações devem estar em conformidade com os requisitos de acessibilidade aplicáveis.

6. Os n.os 1 a 4 não afetam os requisitos e obrigações estabelecidos no capítulo III e não prejudicam outras obrigações de transparência aplicáveis aos responsáveis pela implantação de sistemas de IA estabelecidas no direito da União ou no direito nacional.

7. O Serviço para a IA incentiva e facilita a elaboração a nível da União de códigos de práticas para facilitar a aplicação efetiva das obrigações em matéria de deteção e rotulagem de conteúdos artificialmente gerados ou manipulados. A Comissão pode adotar atos de execução para aprovar esses códigos de práticas em conformidade com o procedimento previsto no artigo 56.º, n.º 6. Se considerar que o código não é adequado, a Comissão pode adotar um ato de execução que especifique as regras comuns para a aplicação dessas obrigações, em conformidade com o procedimento de exame previsto no artigo 98.º, n.º 2.

Capítulo V
Modelos de IA de finalidade geral

SECÇÃO 1
REGRAS DE CLASSIFICAÇÃO

Artigo 51.º
Classificação de modelos de IA de finalidade geral como modelos de IA de finalidade geral com risco sistémico

1. Um modelo de IA de finalidade geral é classificado como modelo de IA de finalidade geral com risco sistémico se preencher qualquer uma das seguintes condições:

   a) Ter capacidades de elevado impacto avaliadas com base em ferramentas e metodologias técnicas adequadas, incluindo indicadores e parâmetros de referência;

b) Ter capacidades ou um impacto equivalentes às estabelecidas na alínea a), tendo em conta os critérios estabelecidos no anexo XIII, com base numa decisão da Comissão, *ex officio* ou na sequência de um alerta qualificado do painel científico.

2. Presume-se que um modelo de IA de finalidade geral tem capacidades de elevado impacto nos termos do n.º 1, alínea a), quando a quantidade acumulada de cálculo utilizado para o seu treino, medido em operações de vírgula flutuante por segundo, for superior a 10^{25}.

3. A Comissão adota atos delegados nos termos do artigo 97.º para alterar os limiares enumerados nos n.os 1 e 2 do presente artigo, bem como para complementar os parâmetros de referência e os indicadores à luz da evolução tecnológica, tais como melhorias algorítmicas ou uma maior eficiência do hardware, se necessário, para que esses limiares reflitam o estado da arte.

Artigo 52.º

Procedimento

1. Sempre que um modelo de IA de finalidade geral preencha a condição a que se refere o artigo 51.º, n.º 1, alínea a), o prestador em causa notifica a Comissão sem demora e, em qualquer caso, no prazo de duas semanas a contar da data em que preencheu esse requisito ou da data em que se soube que esse requisito vai ser preenchido. Essa notificação deve incluir as informações necessárias para demonstrar que o requisito em causa foi preenchido. Se a Comissão tomar conhecimento de um modelo de IA de finalidade geral que apresente riscos sistémicos dos quais não tenha sido notificada, pode decidir designá-lo como um modelo com risco sistémico.

2. O prestador de um modelo de IA de finalidade geral que preencha as condições a que se refere o artigo 51.º, n.º 1, alínea a), pode apresentar, com a sua notificação, argumentos suficientemente fundamentados para demonstrar que, excecionalmente, embora preencha esse requisito, o modelo de IA de finalidade geral não apresenta, devido às suas características específicas, riscos sistémicos e, por conseguinte, não deverá ser classificado como um modelo de IA de finalidade geral com risco sistémico.

3. Se concluir que os argumentos apresentados nos termos do n.º 2 não estão suficientemente fundamentados e que o prestador em causa não conseguiu demonstrar que o modelo de IA de finalidade geral não apresenta, devido às suas características específicas, riscos sistémicos, a Comissão rejeita esses argumentos e o modelo de IA de finalidade geral é considerado um modelo de IA de finalidade geral com risco sistémico.

4. A Comissão pode designar um modelo de IA de finalidade geral como apresentando riscos sistémicos, *ex officio* ou na sequência de um alerta qualificado do painel científico nos termos do artigo 90.º, n.º 1, alínea a), com base nos critérios estabelecidos no anexo XIII.

A Comissão fica habilitada a adotar atos delegados nos termos do artigo 97.º para alterar o anexo XIII através da especificação e atualização dos critérios estabelecidos nesse anexo.

5. Mediante pedido fundamentado de um prestador cujo modelo tenha sido designado como modelo de IA de finalidade geral com risco sistémico nos termos do n.º 4, a Comissão tem em conta o pedido e pode decidir reavaliar se o modelo de IA de finalidade geral ainda pode ser considerado como apresentando riscos sistémicos com base nos critérios estabelecidos no anexo XIII. Um tal pedido deve conter razões objetivas, detalhadas e novas que tenham surgido desde a decisão relativa à designação. Os prestadores podem solicitar uma reavaliação decorridos no mínimo seis meses após a decisão relativa à designação. Se, na sequência da sua reavaliação, a Comissão decidir manter a designação de modelo de IA de finalidade geral com risco sistémico, os prestadores podem solicitar uma reavaliação decorridos no mínimo seis meses após essa decisão.

6. A Comissão assegura a publicação de uma lista de modelos de IA de finalidade geral com risco sistémico e mantém-na atualizada, sem prejuízo da necessidade de observar e proteger os direitos de propriedade intelectual e as informações comerciais de caráter confidencial ou segredos comerciais, em conformidade com o direito da União e o direito nacional.

SECÇÃO 2

OBRIGAÇÕES DOS PRESTADORES DE MODELOS DE IA DE FINALIDADE GERAL

Artigo 53.º

Obrigações dos prestadores de modelos de IA de finalidade geral

1. Os prestadores de modelos de IA de finalidade geral devem:

   a) Elaborar e manter atualizada a documentação técnica do modelo, incluindo o seu processo de treino e de testagem e os resultados da sua avaliação, que deve conter, no mínimo, as informações previstas no anexo XI, a fim de a facultarem, mediante pedido, ao Serviço para a IA e às autoridades nacionais competentes;

   b) Elaborar, manter atualizadas e disponibilizar informações e documentação aos prestadores de sistemas de IA que pretendam integrar o modelo de IA de finalidade geral nos seus sistemas de IA. Sem prejuízo da necessidade de respeitar e proteger os direitos de propriedade intelectual e as informações comerciais de caráter confidencial ou segredos comerciais, em conformidade com o direito da União e o direito nacional, as informações e documentação devem:

      i) permitir que os prestadores de sistemas de IA tenham uma boa compreensão das capacidades e limitações do modelo de IA de finalidade geral e cumpram as suas obrigações nos termos do presente regulamento, e

      ii) conter, no mínimo, os elementos previstos no anexo XII;

c) Aplicar uma política para dar cumprimento ao direito da União em matéria de direitos de autor e direitos conexos e, em especial, identificar e cumprir, nomeadamente através de tecnologias de ponta, uma reserva de direitos expressa nos termos do artigo 4.º, n.º 3, da Diretiva (UE) 2019/790;

d) Elaborar e disponibilizar ao público um resumo suficientemente pormenorizado sobre os conteúdos utilizados para o treino do modelo de IA de finalidade geral, de acordo com um modelo facultado pelo Serviço para a IA.

2. As obrigações estabelecidas no n.º 1, alíneas a) e b), não se aplicam aos prestadores de modelos de IA lançados ao abrigo de uma licença gratuita e aberta que permita o acesso, a utilização, a modificação e a distribuição do modelo, e cujos parâmetros, incluindo as ponderações, as informações sobre a arquitetura do modelo e as informações sobre a utilização do modelo, sejam disponibilizados ao público. Esta exceção não se aplica a modelos de IA de finalidade geral com riscos sistémicos.

3. Os prestadores de modelos de IA de finalidade geral devem cooperar na medida do necessário com a Comissão e as autoridades nacionais competentes no exercício das suas competências e poderes nos termos do presente regulamento.

4. Os prestadores de modelos de IA de finalidade geral podem basear-se em códigos de práticas na aceção do artigo 56.º para demonstrarem o cumprimento das obrigações previstas no n.º 1 do presente artigo, até que seja publicada uma norma harmonizada. O cumprimento das normas europeias harmonizadas concede aos prestadores a presunção de cumprimento, na medida que essas normas abranjam essas obrigações. Os prestadores de modelos de IA de finalidade geral que não cumpram um código de práticas aprovado ou que não cumpram uma norma europeia harmonizada devem demonstrar meios de conformidade alternativos adequados para avaliação pela Comissão.

5. A fim de facilitar o cumprimento do anexo XI, nomeadamente do ponto 2, alíneas d) e e), a Comissão fica habilitada a adotar atos delegados em conformidade com o artigo 97.º a fim de especificar as metodologias de medição e cálculo, com vista a permitir documentação comparável e verificável.

6. A Comissão fica habilitada a adotar atos delegados nos termos do artigo 97.º, n.º 2, para alterar os anexos XI e XII à luz da evolução tecnológica.

7. Todas as informações ou documentação obtidas nos termos do presente artigo, nomeadamente segredos comerciais, são tratadas em conformidade com as obrigações de confidencialidade estabelecidas no artigo 78.º.

Artigo 54.º

Mandatários dos prestadores de modelos de IA de finalidade geral

1. Antes de colocarem um modelo de IA de finalidade geral no mercado da União, os prestadores estabelecidos em países terceiros devem, mediante mandato escrito, designar um mandatário estabelecido na União.

2. O prestador deve habilitar o seu mandatário a desempenhar as funções especificadas no mandato conferido pelo prestador.

3. O mandatário deve desempenhar as funções especificadas no mandato conferido pelo prestador. Mediante pedido, o mandatário fornece ao Serviço para a IA uma cópia do mandato numa das línguas oficiais das instituições da União. Para efeitos do presente regulamento, o mandato habilita o mandatário a exercer as seguintes funções:

   a) Verificar se a documentação técnica especificada no anexo XI foi elaborada e se todas as obrigações referidas no artigo 53.º e, se for caso disso, no artigo 55.º, foram cumpridas pelo prestador;

   b) Conservar uma cópia da documentação técnica especificada no anexo XI, que deve ficar ao dispor do Serviço para a IA e das autoridades nacionais competentes por um período de dez anos após a colocação no mercado do modelo de IA de finalidade geral, e os dados de contacto do prestador que designou o mandatário;

   c) Prestar ao Serviço para a IA, mediante pedido fundamentado, todas as informações e documentação, incluindo a documentação e dados a que se refere a alínea b), necessária para demonstrar o cumprimento com as obrigações previstas no presente capítulo;

   d) Cooperar com o Serviço para a IA e as autoridades competentes, mediante pedido fundamentado, em qualquer medida que estas tomem em relação ao modelo de IA de finalidade geral, inclusive quando o modelo esteja integrado em sistemas de IA colocados no mercado ou colocados em serviço na União.

4. O mandato habilita o mandatário a ser contactado, em complemento ou em alternativa ao prestador, pelo Serviço para a IA ou pelas autoridades competentes, sobre todas as questões relacionadas com a garantia da conformidade com o presente regulamento.

5. O mandatário põe termo ao mandato se considerar ou tiver razões para considerar que o prestador age de forma contrária às obrigações que lhe incumbem por força do presente regulamento. Nesse caso, informa também imediatamente o Serviço para a IA da cessação do mandato e dos respetivos motivos.

6. A obrigação estabelecida no presente artigo não se aplica aos prestadores de modelos de IA de finalidade geral lançados ao abrigo de uma licença gratuita e de fonte aberta que permita o acesso, a utilização, a modificação e a distribuição do modelo, e cujos parâmetros, incluindo as ponderações, as informações sobre a arquitetura do modelo e as informações sobre a utilização do modelo, sejam disponibilizados ao público, a menos que os modelos de IA de finalidade geral apresentem riscos sistémicos.

SECÇÃO 3

OBRIGAÇÕES DOS PRESTADORES DE MODELOS DE IA DE FINALIDADE GERAL COM RISCO SISTÉMICO

Artigo 55.º

Obrigações dos prestadores de modelos de IA de finalidade geral com risco sistémico

1. Para além das obrigações enumeradas nos artigos 53.º e 54.º, os prestadores de modelos de IA de finalidade geral com risco sistémico devem:

   a) Realizar a avaliação do modelo em conformidade com protocolos e instrumentos normalizados que reflitam o estado da arte, incluindo a realização e documentação de testagens antagónicas do modelo, com vista a identificar e atenuar os riscos sistémicos;

   b) Avaliar e atenuar eventuais riscos sistémicos a nível da União, incluindo as respetivas fontes, que possam resultar do desenvolvimento, da colocação no mercado ou da utilização de modelos de IA de finalidade geral com risco sistémico;

   c) Acompanhar, documentar e comunicar, sem demora injustificada, ao Serviço para a IA e, se for caso disso, às autoridades nacionais competentes, as informações pertinentes sobre incidentes graves e eventuais medidas corretivas para os resolver;

   d) Assegurar um nível adequado de proteção em termos de cibersegurança para o modelo de IA de finalidade geral com risco sistémico e a infraestrutura física do modelo.

2. Os prestadores de modelos de IA de finalidade geral com risco sistémico podem basear-se em códigos de práticas na aceção do artigo 56.º para demonstrarem o cumprimento das obrigações previstas no n.º 1 do presente artigo, até que seja publicada uma norma harmonizada. O cumprimento das normas europeias harmonizadas concede aos prestadores a presunção de cumprimento, na medida que essas normas abranjam essas obrigações. Os prestadores de modelos de IA de finalidade geral com risco sistémico que não cumpram um código de práticas aprovado ou que não cumpram uma norma europeia harmonizada devem demonstrar meios de conformidade alternativos adequados para avaliação pela Comissão.

3. Todas as informações ou documentação obtidas nos termos do presente artigo, nomeadamente segredos comerciais, são tratadas em conformidade com as obrigações de confidencialidade estabelecidas no artigo 78.º.

SECÇÃO 4

CÓDIGOS DE PRÁTICAS

Artigo 56.º

Códigos de práticas

1. O Serviço para a IA incentiva e facilita a elaboração de códigos de práticas a nível da União a fim de contribuir para a correta aplicação do presente regulamento, tendo em conta as abordagens internacionais.

2. O Serviço para a IA e o Comité procuram assegurar que os códigos de práticas abranjam, pelo menos, as obrigações previstas nos artigos 53.º e 55.º, incluindo os seguintes elementos:

a) Os meios para assegurar que as informações referidas no artigo 53.º, n.º 1, alíneas a) e b), sejam mantidas atualizadas à luz da evolução tecnológica e do mercado;

b) O nível de pormenor adequado para o resumo dos conteúdos utilizados no treino;

c) A identificação do tipo e da natureza dos riscos sistémicos ao nível da União, incluindo as respetivas fontes, se for caso disso;

d) As medidas, procedimentos e modalidades de avaliação e gestão dos riscos sistémicos a nível da União, incluindo a respetiva documentação, que devem ser proporcionados em relação aos riscos, ter em conta a sua gravidade e probabilidade e ter em conta os desafios específicos da resposta a esses riscos à luz das possíveis formas como podem surgir e materializar-se ao longo da cadeia de valor da IA.

3. O Serviço para a IA pode convidar todos os prestadores de modelos de IA de finalidade geral, bem como as autoridades nacionais competentes, a participar na elaboração de códigos de práticas. As organizações da sociedade civil, a indústria, o meio académico e outras partes interessadas pertinentes, tais como prestadores a jusante e peritos independentes, podem apoiar o processo.

4. O Serviço para a IA e o Comité procuram assegurar que os códigos de práticas definam claramente os seus objetivos específicos e contenham compromissos ou medidas, incluindo, se adequado, indicadores-chave de desempenho, para assegurar a consecução desses objetivos, e que tenham devidamente em conta as necessidades e os interesses de todas as partes interessadas, incluindo as pessoas afetadas, a nível da União.

5. O Serviço para a IA procura assegurar que os participantes nos códigos de práticas lhe comuniquem regularmente a execução dos compromissos e das medidas tomadas e os seus resultados, nomeadamente, se adequado, em função dos indicadores-chave de desempenho. Os indicadores-chave de desempenho e os compromissos em matéria de comunicação de informações devem refletir as diferenças entre os vários participantes em termos de dimensão e capacidade.

6. O Serviço para a IA e o Comité acompanham e avaliam regularmente a consecução dos objetivos dos códigos de práticas pelos participantes e o seu contributo para a correta aplicação do presente regulamento. O Serviço para a IA e o Comité avaliam se os códigos de práticas abrangem as obrigações previstas nos artigos 53.º e 55.º, e acompanham e avaliam regularmente a consecução dos seus objetivos. O Serviço para a IA e o Comité publicam a sua avaliação da adequação dos códigos de práticas.

   A Comissão pode, por meio de um ato de execução, aprovar um código de práticas e conferir-lhe uma validade geral na União. O referido ato de execução é adotado de acordo com o procedimento de exame a que se refere o artigo 98.º, n.º 2.

7. O Serviço para a IA pode convidar os prestadores de modelos de IA de finalidade geral a aderirem aos códigos de práticas. Para os prestadores de modelos de IA de finalidade geral que não apresentem riscos sistémicos, esta adesão pode limitar-se às obrigações previstas no artigo 53.º, a menos que declarem explicitamente o seu interesse em aderir à integralidade do código.

8. Se for caso disso, o Serviço para a IA também incentiva e facilita a revisão e a adaptação dos códigos de práticas, em especial à luz das normas emergentes. O Serviço para a IA presta assistência na avaliação das normas disponíveis.

9. Os códigos de práticas devem estar prontos o mais tardar até ... [nove meses a contar da data de entrada em vigor do presente regulamento]. O Serviço para a IA toma as medidas necessárias, nomeadamente convidando os prestadores nos termos do n.º 7.

Se, até ... [12 meses a contar da data de entrada em vigor], não puder ser finalizado um código de práticas, ou se o Serviço para a IA considerar que tal não é adequado na sequência da sua avaliação nos termos do n.º 6 do presente artigo, a Comissão pode estabelecer, por meio de atos de execução, regras comuns para a execução das obrigações previstas nos artigos 53.º e 55.º, incluindo os elementos referidos no n.º 2 do presente artigo. Os referidos atos de execução são adotados de acordo com o procedimento de exame a que se refere o artigo 98.º, n.º 2.

Capítulo VI
Medidas de apoio à inovação

Artigo 57.º

Ambientes de testagem da regulamentação da inteligência artificial

1. Os Estados-Membros asseguram que as respetivas autoridades competentes criam pelo menos um ambiente de testagem da regulamentação da IA a nível nacional, que deve estar operacional até ... [24 meses a contar da data de entrada em vigor do presente regulamento]. Esse ambiente de testagem também pode ser criado em conjunto com as autoridades competentes de outros Estados-Membros. A Comissão pode prestar apoio técnico, aconselhamento e ferramentas para a criação e o funcionamento de ambientes de testagem da regulamentação da IA.

   A obrigação prevista no primeiro parágrafo pode também ser cumprida através da participação num ambiente de testagem existente, desde que essa participação proporcione um nível equivalente de cobertura nacional para os Estados-Membros participantes.

2. Podem também ser criados ambientes de testagem da regulamentação da IA a nível regional ou local ou em conjunto com as autoridades competentes de outros Estados-Membros.

3. A Autoridade Europeia para a Proteção de Dados pode igualmente criar um ambiente de testagem da regulamentação da IA para as instituições, órgãos e organismos da União e exercer as funções e as atribuições das autoridades nacionais competentes em conformidade com o presente capítulo.

4. Os Estados-Membros asseguram que as autoridades competentes a que se referem os n.os 1 e 2 afetam recursos suficientes para cumprir o disposto no presente artigo de forma eficaz e atempada. Se for caso disso, as autoridades nacionais competentes devem cooperar com outras autoridades pertinentes e podem permitir a participação de outros intervenientes no ecossistema da IA. O presente artigo não afeta outros ambientes de testagem da regulamentação criados ao abrigo do direito da União ou do direito nacional. Os Estados-Membros asseguram um nível adequado de cooperação entre as autoridades que supervisionam esses outros ambientes de testagem e as autoridades nacionais competentes.

5. Os ambientes de testagem da regulamentação da IA estabelecidos nos termos do n.º 1 devem proporcionar um ambiente controlado que promova a inovação e facilite o desenvolvimento, a testagem e a validação de sistemas inovadores de IA por um tempo limitado, antes da sua colocação no mercado ou colocação em serviço nos termos de um plano específico acordado entre os prestadores ou os potenciais prestadores e a autoridade competente. Esses ambientes de testagem podem incluir testagem nas condições reais aí supervisionada.

6. As autoridades competentes disponibilizam, se for caso disso, orientações, supervisão e apoio no ambiente de testagem da regulamentação da IA, com vista a identificar riscos, em especial para os direitos fundamentais, a saúde e a segurança, a efetuar testes, e a aplicar medidas de atenuação e verificar a sua eficácia em relação às obrigações e requisitos do presente regulamento e, se for caso disso, de outras disposições do direito da União e nacional supervisionada no ambiente de testagem.

7. As autoridades competentes disponibilizam aos prestadores e potenciais prestadores participantes no ambiente de testagem da regulamentação da IA orientações sobre as expectativas regulamentares e a forma de cumprir os requisitos e obrigações estabelecidos no presente regulamento.

A pedido do prestador ou potencial prestador do sistema de IA, a autoridade competente apresenta uma prova escrita das atividades realizadas com êxito no ambiente de testagem. A autoridade competente também apresenta um relatório de saída que descreva pormenorizadamente as atividades realizadas no ambiente de testagem e as respetivas conclusões e resultados de aprendizagem. Os prestadores podem utilizar essa documentação para demonstrar que estão em conformidade com o presente regulamento através do processo de avaliação da conformidade ou das atividades de fiscalização do mercado pertinentes. A este respeito, as autoridades de fiscalização do mercado e os organismos notificados devem ter em conta de forma positiva os relatórios de saída e as provas escritas apresentadas pela autoridade nacional competente, a fim de acelerar na medida do razoável os procedimentos de avaliação da conformidade.

8. Sob reserva das disposições em matéria de confidencialidade previstas no artigo 78.º, e com o acordo do prestador ou potencial prestador, a Comissão e o Comité ficam autorizados a aceder aos relatórios de saída e têm-nos em conta, se for caso disso, no exercício das suas funções nos termos do presente regulamento. Se tanto o prestador ou o potencial prestador como a autoridade nacional competente derem o seu acordo explícito, o relatório de saída pode ser disponibilizado ao público através da plataforma única de informação a que se refere o presente artigo.

9. O estabelecimento de ambientes de testagem da regulamentação da IA visa contribuir para os seguintes objetivos:

   a) Melhorar a segurança jurídica para assegurar a conformidade regulamentar com o presente regulamento ou, se for caso disso, outras disposições pertinentes do direito da União e do direito nacional;

   b) Apoiar a partilha de boas práticas através da cooperação com as autoridades envolvidas no ambiente de testagem da regulamentação da IA;

c) Promover a inovação e a competitividade e facilitar o desenvolvimento de um ecossistema da IA;

d) Contribuir para uma aprendizagem regulamentar baseada em dados concretos;

e) Facilitar e acelerar o acesso dos sistemas de IA ao mercado da União, em especial quando disponibilizados por PME, incluindo empresas em fase de arranque.

10. As autoridades nacionais competentes asseguram que, na medida em que os sistemas de IA inovadores envolvam o tratamento de dados pessoais ou de outro modo se enquadrem 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 ou autoridades competentes sejam associadas ao funcionamento do ambiente de testagem da regulamentação da IA e implicadas na supervisão desses aspetos, na medida das respetivas atribuições e poderes.

11. Os ambientes de testagem da regulamentação da IA não afetam os poderes de supervisão ou de correção das autoridades competentes que supervisionam os ambientes de testagem, inclusive a nível local ou regional. A identificação de quaisquer riscos significativos para a saúde e a segurança e os direitos fundamentais durante o desenvolvimento e a testagem desses sistemas de IA deve resultar em medidas adequadas de atenuação. As autoridades nacionais competentes ficam habilitadas a suspender temporária ou permanentemente o processo de testagem ou a participação no ambiente de testagem se não for possível uma atenuação eficaz, e informam o Serviço para a IA dessa decisão. As autoridades nacionais competentes devem exercer os seus poderes de supervisão de forma flexível, dentro dos limites da do direito pertinente, utilizando os seus poderes discricionários quando aplicam disposições jurídicas em relação a um projeto específico de ambiente de testagem da regulamentação da IA, com o objetivo de apoiar a inovação no domínio da IA na União.

12. Os prestadores e potenciais prestadores que participam no ambiente de testagem da regulamentação da IA continuam a ser responsáveis, nos termos do direito da União e do direito nacional aplicável em matéria de responsabilidade, por quaisquer danos infligidos a terceiros em resultado da experimentação que ocorre no ambiente de testagem. No entanto, desde que os potenciais prestadores respeitem o plano específico e os termos e condições da sua participação e sigam de boa-fé as orientações dadas pelas autoridades nacionais competentes, as autoridades não aplicam coimas por infrações ao presente regulamento. Sempre que outras autoridades competentes responsáveis por outras disposições do direito da União e do direito nacional e da União tenham estado ativamente envolvidas na supervisão do sistema de IA no ambiente de testagem e tenham disponibilizado orientações em matéria de conformidade, não podem ser impostas coimas relativamente a essa lei.

13. Os ambientes de testagem da regulamentação da IA são concebidos e aplicados de forma a facilitar, se for caso disso, a cooperação transfronteiriça entre as autoridades nacionais competentes.

14. As autoridades nacionais competentes coordenam as suas atividades e cooperam no âmbito do Comité.

15. As autoridades nacionais competentes informam o Serviço para a IA e o Comité acerca da criação de um ambiente de testagem e podem solicitar-lhes apoio e orientação. O Serviço para a IA disponibiliza ao público e mantém atualizada uma lista dos ambientes de testagem previstos e existentes, a fim de incentivar uma maior interação nos ambientes de testagem da regulamentação da IA e na cooperação transfronteiriça.

16. As autoridades nacionais competentes apresentam relatórios anuais ao Serviço para a IA e ao Comité, um ano após a criação do ambiente de testagem da regulamentação da IA e, posteriormente, todos os anos até à sua cessação, bem como um relatório final. Esses relatórios devem prestar informações sobre o progresso e os resultados da aplicação desses ambientes de testagem – incluindo boas práticas, incidentes, ensinamentos retirados e recomendações sobre a sua configuração – e, se for caso disso, sobre a aplicação e possível revisão do presente regulamento, incluindo os seus atos delegados e de execução, e sobre a aplicação supervisionada pelas autoridades competentes no âmbito do ambiente de testagem de outra legislação da União. As autoridades nacionais competentes disponibilizam ao público, em linha, esses relatórios ou resumos anuais. A Comissão tem em conta, se for caso disso, os relatórios anuais no exercício das suas funções nos termos do presente regulamento.

17. A Comissão desenvolve uma interface única e específica que contém todas as informações pertinentes relacionadas com os ambientes de testagem da regulamentação da IA, a fim de permitir que as partes interessadas interajam com esses mesmos ambientes e peçam informações às autoridades competentes, bem como para que peçam orientações não vinculativas sobre a conformidade de produtos, serviços e modelos de negócios inovadores que integrem tecnologias de IA, em conformidade com o artigo 62.º, n.º 1, alínea c). A Comissão coordena-se proativamente com as autoridades nacionais competentes, quando pertinente.

Artigo 58.º

Modalidades pormenorizadas dos ambientes de testagem da regulamentação da IA e o respetivo funcionamento

1. A fim de evitar a fragmentação em toda a União, a Comissão adota atos de execução que especifiquem as modalidades pormenorizadas para a criação, desenvolvimento, implementação, funcionamento e supervisão dos ambientes de testagem da regulamentação da IA. Os atos de execução incluem princípios comuns sobre os seguintes elementos:

   a) A elegibilidade e os critérios de seleção para a participação no ambiente de testagem da regulamentação da IA;

   b) Os procedimentos para a candidatura, participação, monitorização, saída e cessação do ambiente de testagem da regulamentação da IA, incluindo o plano do ambiente de testagem e o relatório de saída;

   c) Os termos e condições aplicáveis aos participantes.

   Os referidos atos de execução são adotados de acordo com o procedimento de exame a que se refere o artigo 98.º, n.º 2.

2. Os atos de execução a que se referem o n.º 1 asseguram:

   a) Que os ambientes de testagem da regulamentação da IA estejam abertos a qualquer prestador ou potencial prestador de um sistema de IA que apresente um pedido nesse sentido e que preencha os critérios de elegibilidade e seleção, que devem ser transparentes e equitativos, e que essas autoridades nacionais competentes informem os requerentes da sua decisão no prazo de três meses a contar da apresentação do pedido;

b) Que os ambientes de testagem da regulamentação da IA facultem um acesso amplo e em condições de igualdade e acompanhem a procura de participação; prestadores e os potenciais prestadores possam também apresentar pedidos em parceria com responsáveis pela implantação e outros terceiros pertinentes;

c) Que as modalidades pormenorizadas e as condições relativas aos ambientes de testagem da regulamentação da IA apoiem, na medida do possível, a flexibilidade das autoridades nacionais competentes para estabelecerem e operarem os seus ambientes de testagem da regulamentação da IA;

d) Que o acesso aos ambientes de testagem da regulamentação da IA seja gratuito para as PME, incluindo as empresas em fase de arranque, sem prejuízo dos custos excecionais que as autoridades nacionais competentes possam recuperar de forma justa e proporcionada;

e) Que os prestadores e os potenciais prestadores possam cumprir com maior facilidade, através dos resultados de aprendizagem dos ambientes de testagem da regulamentação da IA, as obrigações de avaliação da conformidade previstas no presente regulamento e que seja facilitada a aplicação voluntária dos códigos de conduta a que se refere o artigo 95.º;

f) Que os ambientes de testagem da regulamentação da IA facilitem a participação de outros intervenientes pertinentes no ecossistema da IA, como os organismos notificados e as organizações de normalização, as PME, incluindo as empresas em fase de arranque, as empresas, os inovadores, as instalações de testagem e experimentação, os laboratórios de investigação e experimentação e os polos de inovação digital europeus, os centros de excelência e os investigadores individuais, a fim de permitir e facilitar a cooperação com os setores público e privado;

g) Que os procedimentos, processos e requisitos administrativos para a aplicação, seleção, participação e saída do ambiente de testagem da regulamentação da IA sejam simples, facilmente compreensíveis e comunicados claramente, a fim de facilitar a participação das PME, incluindo as empresas em fase de arranque, com capacidades jurídicas e administrativas limitadas, e sejam simplificados em toda a União para evitar a fragmentação; e que a participação num ambiente de testagem da regulamentação da IA criado por um Estado-Membro ou pela Autoridade Europeia para a Proteção de Dados seja mútua e uniformemente reconhecida e tenha os mesmos efeitos jurídicos em toda a União;

h) Que a participação no ambiente de testagem da regulamentação da IA seja limitada a um período adequado à complexidade e dimensão do projeto, e que poderá ser prorrogado pela autoridade nacional competente;

i) Que os ambientes de testagem da regulamentação da IA facilitem o desenvolvimento de instrumentos e de infraestruturas para testar, comparar, avaliar e explicar as dimensões dos sistemas de IA pertinentes para a aprendizagem regulamentar, como a exatidão, a robustez e a cibersegurança, bem como de medidas para atenuar os riscos para os direitos fundamentais e a sociedade em geral.

3. Os potenciais prestadores nos ambientes de testagem da regulamentação da IA, especialmente as PME e as empresas em fase de arranque, devem ser direcionados, se for caso disso, para os serviços de pré-implantação – como serviços de orientação sobre a aplicação do presente regulamento – e para outros serviços que apresentem um valor acrescentado, como a ajuda para os documentos de normalização e à certificação, as instalações de testagem e experimentação, os polos de inovação digital europeus e os centros de excelência.

4. Sempre que ponderem autorizar a testagem em condições reais supervisionada no âmbito de um ambiente de testagem da regulamentação da IA criado ao abrigo do presente artigo, as autoridades nacionais competentes devem acordar especificamente os termos e condições dessa testagem e, em especial, as salvaguardas adequadas com os participantes com vista a proteger os direitos fundamentais, a saúde e a segurança. Se for caso disso, cooperam com outras autoridades nacionais competentes com vista a assegurar práticas coerentes em toda a União.

Artigo 59.º

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

1. No ambiente de testagem da regulamentação da IA, os dados pessoais legalmente recolhidos para outras finalidades podem ser tratados exclusivamente com vista a desenvolver, treinar e testar certos sistemas de IA no ambiente de testagem, quando estiverem preenchidas todas as seguintes condições:

   a) Os sistemas de IA são desenvolvidos para salvaguarda de um interesse público substancial por uma autoridade pública ou outra pessoa singular ou coletiva e num ou mais dos seguintes domínios:

      i) segurança pública e saúde pública, nomeadamente a deteção, o diagnóstico, a prevenção, o controlo e o tratamento e a melhoria dos sistemas de cuidados de saúde,

      ii) um elevado nível de proteção e melhoria da qualidade do ambiente, a proteção da biodiversidade, a proteção contra a poluição, medidas de transição ecológica, medidas de atenuação das alterações climáticas e de adaptação às mesmas;

iii) sustentabilidade energética,

iv) segurança e resiliência dos sistemas e da mobilidade, das infraestruturas críticas e das redes de transportes,

v) eficiência e qualidade da administração pública e dos serviços públicos;

b) Os dados tratados são necessários para cumprir um ou vários dos requisitos a que se refere o capítulo III, secção 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 determinar, tal como previsto no artigo 35.º do Regulamento (UE) 2016/679 e no artigo 39.º do Regulamento (UE) 2018/1725, se pode surgir durante a experimentação no ambiente de testagem um elevado risco para os direitos e as liberdades, bem como identificar mecanismos de resposta para atenuar prontamente esses riscos e, se necessário, interromper o tratamento dos dados;

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 do potencial prestador, sendo apenas acessíveis a pessoas autorizadas;

e) Os prestadores só podem partilhar os dados inicialmente recolhidos se essa partilha estiver em conformidade com a legislação da União em matéria de proteção de dados; os dados pessoais armazenados no ambiente de testagem não podem ser partilhados fora do ambiente de testagem;

f) Nenhum tratamento de dados pessoais no contexto do ambiente de testagem dá origem a medidas ou decisões que afetem os titulares dos dados, ou afeta a aplicação dos seus direitos consagrados no direito da União em matéria de proteção de dados pessoais;

g) Todos os dados pessoais tratados no contexto do ambiente de testagem são protegidos por meio de medidas técnicas e organizativas adequadas e apagados assim que a participação no ambiente de testagem terminar ou assim 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, salvo disposição em contrário no direito da União ou no direito nacional;

i) É conservada como parte da documentação técnica a que se refere o anexo IV, 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;

j) É publicada no sítio Web das autoridades competentes uma breve síntese do projeto de IA desenvolvido no ambiente de testagem, incluindo os seus objetivos e resultados esperados; esta obrigação não abrange dados operacionais sensíveis relacionados com as atividades das autoridades competentes em matéria de aplicação da lei, controlo das fronteiras, imigração ou asilo.

2. 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, sob o controlo e a responsabilidade das autoridades responsáveis pela aplicação da lei, o tratamento de dados pessoais em ambientes de testagem da regulamentação da IA baseia-se no direito da União ou nacional específica e está sujeito às mesmas condições cumulativas a que se refere o n.º 1.

3. O n.º 1 não prejudica o direito da União ou o direito nacional que exclua o tratamento de dados pessoais para outras finalidades que não as explicitamente mencionadas nessa legislação, nem o direito da União ou o direito nacional que estabeleça a base para o tratamento de dados pessoais necessário para efeitos de desenvolvimento, testagem ou treino de sistemas de IA inovadores nem qualquer outra base jurídica, em conformidade com o direito da União em matéria de proteção de dados pessoais.

Artigo 60.º

Testagem de sistemas de IA de risco elevado em condições reais fora dos ambientes de testagem da regulamentação da IA

1. A testagem de sistemas de IA de risco elevado em condições reais fora dos ambientes de testagem da regulamentação da IA pode ser realizada por prestadores ou potenciais prestadores dos sistemas de IA de risco elevado enumerados no anexo III, em conformidade com o presente artigo e com o plano de testagem em condições reais a que se refere o presente artigo, sem prejuízo das proibições previstas no artigo 5.º.

   A Comissão, por meio de atos de execução, especifica os elementos pormenorizados do plano de testagem em condições reais. Esses atos de execução são adotados de acordo com o procedimento de exame a que se refere o artigo 98.º, n.º 2.

O presente número não prejudica o direito da União nem o direito nacional relativo à testagem em condições reais de sistemas de IA de risco elevado relacionados com produtos abrangidos pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I.

2. Os prestadores ou potenciais prestadores podem testar os sistemas de IA de risco elevado a que se refere o anexo III em condições reais em qualquer momento antes da colocação no mercado ou da colocação em serviço do sistema de IA, isoladamente ou em parceria com um ou mais responsáveis pela implantação ou potenciais responsáveis pela implantação.

3. A testagem de sistemas de IA de risco elevado em condições reais ao abrigo do presente artigo não prejudica qualquer análise ética que seja exigida pelo direito da União ou pelo direito nacional.

4. Os prestadores ou potenciais prestadores só podem realizar a testagem em condições reais se estiverem preenchidas todas as seguintes condições:

a) O prestador ou potencial prestador elaborou um plano de testagem em condições reais e apresentou-o à autoridade de fiscalização do mercado do Estado-Membro onde se vai realizar a testagem em condições reais;

b) A autoridade de fiscalização do mercado do Estado-Membro onde se vai realizar a testagem em condições reais aprovou a testagem em condições reais e o plano de testagem em condições reais; se a autoridade de fiscalização do mercado não der uma resposta no prazo de 30 dias, considera-se que as testagens em condições reais e o plano de testagem foram aprovados; nos casos em que a legislação nacional não preveja uma aprovação tácita, a testagem em condições reais continua a estar sujeita a uma autorização;

c) O prestador ou potencial prestador, com exceção dos prestadores ou potenciais prestadores dos sistemas de IA de risco elevado a que se refere o anexo III, pontos 1, 6 e 7, nos domínios da aplicação da lei, da migração, do asilo e da gestão do controlo das fronteiras, e dos sistemas de IA de risco elevado a que se refere o anexo III, ponto 2, registou a testagem em condições reais em conformidade com o artigo 71.º, n.º 4, com um número único de identificação a nível da União e com as informações especificadas no anexo IX; o prestador ou potencial prestador dos sistemas de IA de risco elevado a que se refere o anexo III, pontos 1, 6 e 7, nos domínios da aplicação da lei, da migração, do asilo e da gestão do controlo das fronteiras, registou a testagem em condições reais na secção não pública da base de dados da UE em conformidade com o artigo 49.º, n.º 4, com um número único de identificação a nível da União e com as informações aí especificadas; o prestador ou potencial prestado de sistemas de IA de risco elevado referido no anexo III, ponto 2, registou a testagem em condições reais em conformidade com o artigo 49.º, n.º 5;

d) O prestador ou potencial prestador que realiza a testagem em condições reais está estabelecido na União ou nomeou um representante legal que está estabelecido na União;

e) Os dados recolhidos e tratados para efeitos de testagem em condições reais não são transferidos para países terceiros, a menos que sejam aplicadas as garantias adequadas e aplicáveis nos termos do direito da União;

f) A testagem em condições reais não dura mais tempo do que o necessário para atingir os seus objetivos e, em qualquer caso, não excede seis meses, que podem ser prorrogados por um período de mais seis meses, sob reserva de notificação prévia do prestador ou potencial prestador à autoridade de fiscalização do mercado, acompanhada de uma explicação da necessidade dessa prorrogação;

g) Os participantes na testagem em condições reais que sejam pessoas que pertençam a grupos vulneráveis devido à sua idade ou deficiência estão devidamente protegidos;

h) Sempre que um prestador ou potencial prestador organizar a testagem em condições reais em colaboração com um ou mais responsáveis ou potenciais responsáveis pela implantação, estes últimos são informados de todos os aspetos da testagem que sejam pertinentes para a sua decisão de participar e recebem as instruções de utilização pertinentes do sistema de IA a que se refere o artigo 13.º; o prestador ou potencial prestador e o responsável pela implantação ou potencial responsável pela implantação celebram um acordo que especifique as suas funções e responsabilidades, a fim de assegurar o cumprimento das disposições relativas à testagem em condições reais nos termos do presente regulamento e de outras disposições aplicáveis do direito da União e do direito nacional;

i) Os participantes na testagem em condições reais deram o seu consentimento informado em conformidade com o artigo 61.º ou, no caso das autoridades responsáveis pela aplicação da lei, se a obtenção do consentimento informado impedir que o sistema de IA seja testado, a testagem propriamente dita e os resultados da testagem em condições reais não têm um efeito negativo sobre os participantes e os seus dados pessoais são apagados depois de realizada a testagem;

j) A testagem em condições reais é efetivamente supervisionada pelo prestador ou potencial prestador, bem como pelos responsáveis ou potenciais responsáveis pela implantação, por intermédio de pessoas que tenham as devidas qualificações no domínio em causa, bem como a capacidade, a formação e a autoridade necessárias para desempenhar as respetivas funções;

k) As previsões, recomendações ou decisões do sistema de IA podem ser efetivamente revertidas e ignoradas.

5. Os participantes na testagem em condições reais, ou o seu representante legalmente autorizado, consoante o caso, podem, sem que daí decorra qualquer prejuízo e sem terem que apresentar qualquer justificação, retirar-se da testagem a qualquer momento retirando para tal o seu consentimento informado e solicitando o apagamento imediato e permanente dos seus dados pessoais. A retirada do consentimento informado não afeta as atividades já realizadas.

6. Em conformidade com o artigo 75.º, os Estados-Membros conferem às suas autoridades de fiscalização do mercado os poderes para exigir aos prestadores e potenciais prestadores a prestação de informações, para realizarem inspeções à distância ou no local sem aviso prévio e para efetuarem verificações da forma como é realizada a testagem em condições reais e dos sistemas de IA de risco elevado conexos. As autoridades de fiscalização do mercado utilizam esses poderes para garantir o desenvolvimento seguro da testagem em condições reais.

7. Todos os incidentes graves identificados durante a testagem em condições reais são comunicados à autoridade nacional de fiscalização do mercado em conformidade com o artigo 73.º. O prestador ou potencial prestador deve adotar medidas de atenuação imediatas ou, na sua falta, suspender a testagem em condições reais até que essa atenuação tenha lugar ou, se tal não acontecer, cessar a testagem. O prestador ou potencial prestador deve estabelecer um procedimento para a rápida recolha do sistema de IA após a cessação da testagem em condições reais.

8. O prestador ou potencial prestador deve notificar a autoridade nacional de fiscalização do mercado do Estado-Membro onde se realiza a testagem em condições reais da suspensão ou cessação da testagem em condições reais e dos resultados finais.

9. O prestador ou potencial prestador é responsável, nos termos do direito da União e do direito nacional aplicável em matéria de responsabilidade, pelos danos causados no decurso da sua testagem em condições reais.

Artigo 61.º

Consentimento informado para participar em testagens em condições reais fora dos ambientes de testagem da regulamentação da IA

1. Para efeitos de testagem em condições reais nos termos do artigo 60.º, o consentimento informado deve ser dado livremente pelos participantes na testagem antes da sua participação nessa testagem e depois de lhe terem sido devidamente prestadas informações concisas, claras, pertinentes e compreensíveis sobre:

   a) A natureza e os objetivos da testagem em condições reais e os eventuais incómodos que possam estar ligados à sua participação na testagem;

   b) As condições em que a testagem em condições reais vai realizar-se, incluindo a duração prevista da sua participação na testagem;

   c) Os seus direitos e garantias no tocante à sua participação, em particular o seu direito de recusar a participação na testagem em condições reais e o direito de se retirar da mesma em qualquer altura sem que daí decorra qualquer prejuízo e sem ter de dar qualquer justificação;

   d) As modalidades para solicitar que as previsões, recomendações ou decisões do sistema de IA sejam revertidas ou ignoradas;

   e) O número único de identificação a nível da União da testagem em condições reais, em conformidade com o artigo 60.º, n.º 4, alínea c), e os dados de contacto do prestador, ou do seu representante legal, junto do qual podem ser obtidas mais informações.

2. O consentimento informado deve ser datado e documentado e deve dele ser dado um exemplar aos participantes na testagem ou ao seu representante legal.

Artigo 62.º

Medidas para prestadores e responsáveis pela implantação, em especial PME, incluindo empresas em fase de arranque

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

a) Proporcionar às PME, incluindo as empresas em fase de arranque, com sede social ou sucursal na União, acesso prioritário aos ambientes de testagem da regulamentação da IA, desde que cumpram as condições de elegibilidade e os critérios de seleção; o acesso prioritário não obsta a que outras PME, incluindo empresas em fase de arranque, que não as referidas no presente número, tenham acesso ao ambiente de testagem da regulamentação da IA, desde que também preencham as condições de elegibilidade e os critérios de seleção;

b) Organizar atividades de sensibilização e de formação específicas sobre a aplicação do presente regulamento adaptadas às necessidades das PME, incluindo as empresas em fase de arranque, dos responsáveis pela implantação e, conforme adequado, das autoridades públicas locais;

c) Utilizar os canais específicos existentes e, se for caso disso, criar canais novos para a comunicação com as PME, incluindo as empresas em fase de arranque, os responsável pela implantação, outros inovadores e, conforme adequado, as autoridades públicas locais, com vista a prestar aconselhamento e responder a perguntas sobre a aplicação do presente regulamento, inclusive no que diz respeito à participação em ambientes de testagem da regulamentação da IA;

d) Facilitar a participação das PME e de outras partes interessadas relevantes no processo de desenvolvimento da normalização;

2. Os interesses e as necessidades específicas dos prestadores que são PME, incluindo as empresas em fase de arranque, devem ser tidos 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, à dimensão do mercado e demais indicadores pertinentes.

3. O Serviço para a IA deve empreender as seguintes ações:

a) Disponibilizar modelos normalizados para os domínios abrangidos pelo presente regulamento, conforme especificado pelo Comité no seu pedido;

b) Desenvolver e manter uma plataforma única de informação que faculte a todos os operadores em toda a União informações de fácil utilização a respeito do presente regulamento;

c) Organizar campanhas de comunicação adequadas para sensibilizar para as obrigações decorrentes do presente regulamento;

d) Avaliar e promover a convergência das boas práticas nos processos de adjudicação de contratos públicos em relação aos sistemas de IA.

Artigo 63.º

Derrogações aplicáveis a operadores específicos

1. As microempresas, na aceção da Recomendação 2003/361/CE, podem preencher determinados requisitos do sistema de gestão da qualidade exigidos pelo artigo 17.º do presente regulamento de forma simplificada, desde que não tenham empresas parceiras ou empresas associadas na aceção dessa recomendação. Para o efeito, a Comissão elabora orientações sobre os elementos do sistema de gestão da qualidade que podem ser cumpridos de forma simplificada tendo em conta as necessidades das microempresas, sem afetar o nível de proteção ou a necessidade de conformidade com os requisitos aplicáveis aos sistemas de IA de risco elevado.

2. O n.º 1 do presente artigo não pode ser interpretado no sentido de isentar esses operadores do cumprimento de quaisquer outros requisitos ou obrigações estabelecidos no presente regulamento, incluindo os estabelecidos nos artigos 9.º, 10.º, 11.º, 12.º, 13.º, 14.º, 15.º, 72.º e 73.º.

Capítulo VII
Governação

SECÇÃO 1
GOVERNAÇÃO A NÍVEL DA UNIÃO

Artigo 64.º

Serviço para a IA

1. A Comissão desenvolve os conhecimentos especializados e as capacidades da União no domínio da IA por intermédio do Serviço para a IA.

2. Os Estados-Membros facilitam o exercício das atribuições confiadas ao Serviço para a IA, tal como refletido no presente regulamento.

Artigo 65.º

Criação e estrutura do Comité Europeu para a Inteligência Artificial

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

2. O Comité é composto por um representante de cada Estado-Membro. A Autoridade Europeia para a Proteção de Dados participa na qualidade de observador. O Serviço para a IA participa igualmente nas reuniões do Comité, mas não participa nas votações. O Comité pode convidar para as reuniões, caso a caso, outras autoridades, organismos ou peritos nacionais e da União, sempre que as questões debatidas sejam pertinentes para os mesmos.

3. Cada representante é designado pelo respetivo Estado-Membro por um período de três anos, renovável uma vez.

4. Os Estados-Membros asseguram que os seus representantes no Comité:

   a) Disponham das competências e poderes pertinentes no seu Estado-Membro, de modo a contribuir ativamente para o desempenho das funções do Comité a que se refere o artigo 66.º;

   b) Sejam designados como ponto de contacto único para o Comité e, se for caso disso, tendo em conta as necessidades dos Estados-Membros, como ponto de contacto único para as partes interessadas;

   c) Estejam habilitados a facilitar a coerência e a coordenação entre as autoridades nacionais competentes nos respetivos Estados-Membros no que diz respeito à aplicação do presente regulamento, nomeadamente através da recolha de dados e informações pertinentes para efeitos do desempenho das suas funções no Comité.

5. Os representantes designados dos Estados-Membros adotam o regulamento interno do Comité por maioria de dois terços. O regulamento interno estabelece, em especial, os procedimentos para o processo de seleção, a duração do mandato e as especificações das funções do presidente, as modalidades pormenorizadas de votação e a organização das atividades do Comité e dos seus subgrupos.

6. O Comité deve criar dois subgrupos permanentes para proporcionar uma plataforma de cooperação e intercâmbio entre as autoridades de fiscalização do mercado e para notificar as autoridades sobre questões relacionadas com a fiscalização do mercado e os organismos notificados respetivamente.

O subgrupo permanente para a fiscalização do mercado deverá atuar como grupo de cooperação administrativa (ADCO) para efeitos do presente regulamento, na aceção do artigo 30.º do Regulamento (UE) 2019/1020.

O Comité pode constituir outros subgrupos permanentes ou temporários consoante adequado para fins de análise de questões específicas. Se for caso disso, os representantes do fórum consultivo a que se refere o artigo 67.º podem ser convidados para esses subgrupos ou para reuniões específicas desses subgrupos na qualidade de observadores.

7. O Comité deve estar organizado e funcionar de modo a salvaguardar a objetividade e a imparcialidade das suas atividades.

8. O Comité é presidido por um dos representantes dos Estados-Membros. O Serviço para a IA disponibiliza o secretariado ao Comité, convoca as reuniões mediante pedido do presidente e prepara a ordem de trabalhos em conformidade com as funções do Comité nos termos do presente regulamento e com o seu regulamento interno.

Artigo 66.º

Funções do Comité

O Comité presta aconselhamento e assistência à Comissão e aos Estados-Membros a fim de facilitar a aplicação coerente e eficaz do presente regulamento. Para o efeito, o Comité pode, em especial:

a) Contribuir para a coordenação entre as autoridades nacionais competentes responsáveis pela aplicação do presente regulamento e, em cooperação com as autoridades de fiscalização do mercado em causa e sob reserva do acordo destas, apoiar as atividades conjuntas das autoridades de fiscalização do mercado a que se refere o artigo 74.º, n.º 11;

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

c) Prestar aconselhamento sobre a aplicação do presente regulamento, em especial no que diz respeito à aplicação das regras relativas aos modelos de IA de finalidade geral;

d) Contribuir para a harmonização das práticas administrativas nos Estados-Membros, nomeadamente no que diz respeito à derrogação dos procedimentos de avaliação da conformidade a que se refere o artigo 46.º, ao funcionamento dos ambientes de testagem da regulamentação da IA e à testagem em condições reais a que se referem os artigos 57.º, 59.º e 60.º;

e) A pedido da Comissão ou por sua própria iniciativa, emitir recomendações e pareceres escritos sobre quaisquer matérias pertinentes relacionadas com a execução do presente regulamento e com a sua aplicação coerente e eficaz, incluindo:

i) a elaboração e a aplicação de códigos de conduta e códigos de práticas nos termos do presente regulamento, bem como das orientações da Comissão,

ii) a avaliação e a revisão do presente regulamento nos termos do artigo 112.º, nomeadamente no que diz respeito aos relatórios de incidentes graves a que se refere o artigo 73.º e ao funcionamento da base de dados da UE a que se refere o artigo 71.º, à preparação dos atos delegados ou de execução e ao eventual alinhamento do presente regulamento com legislação de harmonização da União enumerada no anexo I,

iii) as especificações técnicas ou normas existentes relativas aos requisitos estabelecidos no capítulo III, secção 2,

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

v) tendências tais como a competitividade europeia a nível mundial no domínio da IA, a adoção da IA na União e o desenvolvimento de competências digitais,

vi) as tendências da evolução da tipologia das cadeias de valor da IA, em especial no que toca às implicações daí resultantes em termos de responsabilização,

vii) a eventual necessidade de alterar o anexo III, em conformidade com o artigo 7.º, e a eventual necessidade de uma possível revisão do artigo 5.º, nos termos do artigo 112.º, tendo em conta os dados pertinentes disponíveis e a mais recente evolução tecnológica;

f) Apoiar a Comissão na promoção da literacia no domínio da IA, da sensibilização e da compreensão do público relativamente aos benefícios, aos riscos, às garantias e aos direitos e obrigações associados à utilização de sistemas de IA;

g) Facilitar o desenvolvimento de critérios comuns e um entendimento comum entre os operadores do mercado e as autoridades competentes dos conceitos pertinentes previstos no presente regulamento, inclusive contribuindo para o desenvolvimento de parâmetros de referência;

h) Cooperar, conforme adequado, com outras instituições, órgãos e organismos da União, bem como grupos de peritos e redes pertinentes da União, em especial nos domínios da segurança dos produtos, da cibersegurança, da concorrência, dos serviços digitais e de comunicação social, dos serviços financeiros, da defesa dos consumidores, dos dados e da proteção dos direitos fundamentais;

i) Contribuir para uma cooperação eficaz com as autoridades competentes de países terceiros e com organizações internacionais;

j) Prestar assistência às autoridades nacionais competentes e à Comissão no desenvolvimento dos conhecimentos técnicos e organizacionais necessários para a execução do presente regulamento, nomeadamente contribuindo para a avaliação das necessidades de formação do pessoal dos Estados-Membros envolvido na execução do presente regulamento;

k) Ajudar o Serviço para a IA a apoiar as autoridades nacionais competentes na criação e no desenvolvimento de ambientes de testagem da regulamentação da IA e facilitar a cooperação e a partilha de informações entre os ambientes de testagem da regulamentação da IA;

l) Contribuir para a elaboração da documentação de orientação pertinente e prestar aconselhamento nesta matéria;

m) Aconselhar a Comissão em relação a questões internacionais no domínio da IA;

n) Dar pareceres à Comissão sobre os alertas qualificados relativos a modelos de IA de finalidade geral;

o) Receber pareceres dos Estados-Membros sobre alertas qualificados relativos a modelos de IA de finalidade geral e sobre as experiências e práticas nacionais em matéria de acompanhamento e execução dos sistemas de IA, em especial os sistemas que integram os modelos de IA de finalidade geral.

Artigo 67.º

Fórum consultivo

1. É criado um fórum consultivo para facultar conhecimentos técnicos especializados e aconselhar o Comité e a Comissão, e contribuir para o exercício das respetivas funções nos termos do presente regulamento.

2. A composição do fórum consultivo deve representar uma seleção equilibrada de partes interessadas, incluindo a indústria, as empresas em fase de arranque, as PME, a sociedade civil e o meio académico. A composição do fórum consultivo deve ser equilibrada no que diz respeito aos interesses comerciais e não comerciais e, dentro da categoria dos interesses comerciais, no que diz respeito às PME e às outras empresas.

3. A Comissão nomeia os membros do fórum consultivo, em conformidade com os critérios estabelecidos no n.º 2, de entre as partes interessadas com conhecimentos especializados reconhecidos no domínio da IA.

4. O mandato dos membros do fórum consultivo é de dois anos, podendo ser prorrogado por um período não superior a quatro anos.

5. A Agência dos Direitos Fundamentais da União Europeia, a ENISA, o Comité Europeu de Normalização (CEN), o Comité Europeu de Normalização Eletrotécnica (CENELEC) e o Instituto Europeu de Normalização das Telecomunicações (ETSI) são membros permanentes do fórum consultivo.

6. O fórum consultivo elabora o seu regulamento interno. O fórum consultivo elege dois copresidentes de entre os seus membros, de acordo com os critérios estabelecidos no n.º 2. O mandato dos copresidentes é de dois anos, renovável uma vez.

7. O fórum consultivo reúne-se pelo menos duas vezes por ano. Pode convidar peritos e outras partes interessadas para as suas reuniões.

8. O fórum consultivo pode elaborar pareceres, recomendações e contributos escritos mediante pedido do Comité ou da Comissão.

9. O fórum consultivo pode criar subgrupos permanentes ou temporários, conforme adequado para o exame de questões específicas relacionadas com os objetivos do presente regulamento.

10. O fórum consultivo elabora um relatório anual sobre as suas atividades. Esse relatório é disponibilizado ao público.

Artigo 68.º

Painel científico de peritos independentes

1. A Comissão adota, por meio de um ato de execução, disposições relativas à criação de um painel científico de peritos independentes (o «painel científico») destinado a apoiar as atividades de execução nos termos do presente regulamento. O referido ato de execução é adotado de acordo com o procedimento de exame a que se refere o artigo 98.º, n.º 2.

2. O painel científico é composto por peritos selecionados pela Comissão com base em conhecimentos científicos ou técnicos atualizados no domínio da IA necessários para o exercício das funções previstas no n.º 3, e deve poder demonstrar que preenche todas as seguintes condições:

   a) Conhecimentos e competências específicos e conhecimentos científicos ou técnicos no domínio da IA;

   b) Independência relativamente a qualquer prestador de sistemas de IA ou de modelos de IA de finalidade geral;

   c) Capacidade para realizar atividades de forma diligente, precisa e objetiva. A Comissão, em consulta com o Comité, determina o número de peritos do painel de acordo com as necessidades e assegura uma representação equitativa em termos de género e no plano geográfico.

3. O painel científico aconselha e apoia o Serviço para a IA, em especial no que diz respeito às seguintes funções:

a) Apoiar a aplicação e execução do presente regulamento no que diz respeito aos modelos e sistemas de IA de finalidade geral, em particular:

i) alertando o Serviço para a IA para eventuais riscos sistémicos a nível da União dos modelos de IA de finalidade geral, em conformidade com o artigo 90.º,

ii) contribuindo para o desenvolvimento de instrumentos e metodologias de avaliação das capacidades dos modelos e sistemas de IA de finalidade geral, nomeadamente através de parâmetros de referência,

iii) prestando aconselhamento sobre a classificação dos modelos de IA de finalidade geral com risco sistémico,

iv) prestando aconselhamento sobre a classificação de vários modelos e sistemas de IA de finalidade geral,

v) contribuindo para o desenvolvimento de instrumentos e modelos;

b) Apoiar as autoridades de fiscalização do mercado no seu trabalho, a pedido destas;

c) Apoiar as atividades de fiscalização do mercado transfronteiriças a que se refere o artigo 74.º, n.º 11, sem prejuízo dos poderes das autoridades de fiscalização do mercado;

d) Apoiar o Serviço para a IA no exercício das suas funções no contexto do procedimento de salvaguarda da União prevista no artigo 81.º.

4. Os peritos do painel científico desempenham as suas funções com imparcialidade e objetividade e garantem a confidencialidade das informações e dos dados obtidos no desempenho das suas funções e atividades. Não solicitam nem aceitam instruções de ninguém no exercício das suas funções nos termos do n.º 3. Cada um dos peritos apresenta uma declaração de interesses, que é disponibilizada ao público. O Serviço para a IA cria sistemas e procedimentos para gerir e evitar ativamente potenciais conflitos de interesses.

5. O ato de execução a que se refere o n.º 1 deve incluir disposições sobre as condições, os procedimentos e as modalidades pormenorizadas segundo as quais o painel científico e os seus membros emitem alertas e solicitam a assistência do Serviço para a IA no desempenho das funções do painel científico.

Artigo 69.º

Acesso dos Estados-Membros ao grupo de peritos

1. Os Estados-Membros podem recorrer a peritos do painel científico para apoiar as suas atividades de execução ao abrigo do presente regulamento.

2. Os Estados-Membros podem ser obrigados a pagar honorários pelo aconselhamento e apoio prestados pelos peritos. A estrutura e o nível dos honorários, bem como a escala e a estrutura das despesas reembolsáveis, são definidos no ato de execução a que se refere o artigo 68.º, n.º 1, tendo em conta os objetivos de uma aplicação adequada do presente regulamento, a relação custo-eficácia e a necessidade de assegurar um acesso efetivo a peritos para todos os Estados-Membros.

3. A Comissão facilita o acesso atempado dos Estados-Membros aos peritos, conforme necessário, e assegura que a combinação das atividades de apoio realizadas pelas estruturas de apoio à testagem da IA a nível da União nos termos do artigo 84.º e pelos peritos nos termos do presente artigo seja organizada de forma eficiente e proporcione o melhor valor acrescentado possível.

SECÇÃO 2

AUTORIDADES NACIONAIS COMPETENTES

Artigo 70.º

Designação das autoridades nacionais competentes e dos pontos de contacto únicos

1. Cada Estado-Membro cria ou designa pelo menos uma autoridade notificadora e pelo menos uma autoridade de fiscalização do mercado para efeitos do presente regulamento como autoridades nacionais competentes. Essas autoridades nacionais competentes exercem os seus poderes de forma independente, imparcial e sem enviesamentos, a fim de salvaguardar a objetividade das suas atividades e funções e de assegurar a aplicação e execução do presente regulamento. Os membros dessas autoridades abstêm-se de praticar qualquer ato incompatível com a natureza das suas funções. Desde que esses princípios sejam respeitados, tais atividades e funções podem ser desempenhadas por uma ou mais autoridades designadas, de acordo com as necessidades organizativas do Estado-Membro.

2. Os Estados-Membros comunicam à Comissão a identidade das autoridades notificadoras e das autoridades de fiscalização do mercado, bem como as funções dessas autoridades e quaisquer alterações subsequentes das mesmas. Os Estados-Membros disponibilizam ao público informações sobre a forma como as autoridades competentes e os pontos de contacto únicos podem ser contactados, através de meios de comunicação eletrónica, até ... [12 meses a contar a data de entrada em vigor do presente regulamento]. Os Estados-Membros designam uma autoridade de fiscalização do mercado para atuar como ponto de contacto único para efeitos do presente regulamento e notificam a Comissão da identidade do ponto de contacto único. A Comissão disponibiliza ao público uma lista dos pontos de contacto únicos.

3. Os Estados-Membros asseguram que as suas autoridades nacionais competentes dispõem dos recursos técnicos, financeiros e humanos adequados e das infraestruturas para desempenhar eficazmente as funções que lhes incumbem nos termos do presente regulamento. Em especial, as autoridades nacionais competentes devem dispor permanentemente de pessoal suficiente cujas competências e conhecimentos especializados incluam uma compreensão profunda das tecnologias de IA, dos dados e da computação de dados, da proteção de dados pessoais, da cibersegurança, dos direitos fundamentais e dos riscos para a saúde e a segurança, bem como um conhecimento das normas e dos requisitos legais em vigor. Os Estados-Membros avaliam e, se necessário, atualizam anualmente os requisitos em matéria de competências e de recursos a que se refere o presente número.

4. As autoridades nacionais competentes devem tomar medidas adequadas para assegurar um nível adequado de cibersegurança.

5. No desempenho das suas funções, as autoridades nacionais competentes atuam em conformidade com as obrigações de confidencialidade estabelecidas no artigo 78.º.

6. Até ... [um ano a contar da data de entrada em vigor do presente regulamento] e, posteriormente, de dois em dois anos, os Estados-Membros informam a 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.

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

8. As autoridades nacionais competentes podem disponibilizar orientações e prestar aconselhamento sobre a execução do presente regulamento, em especial às PME, incluindo as empresas em fase de arranque, tendo em conta as orientações e o aconselhamento do Comité e da Comissão, conforme adequado. Sempre que as autoridades nacionais competentes pretendam disponibilizar orientações e prestar aconselhamento em relação a um sistema de IA em domínios abrangidos por outras disposições do direito da União, as autoridades nacionais competentes ao abrigo do direito da União devem ser consultadas, conforme adequado.

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

Capítulo VIII

Base de dados da UE relativa a sistemas de IA de risco elevado

Artigo 71.º

Base de dados da UE relativa a sistemas de IA de risco elevado enumerados no anexo III

1. A Comissão, em colaboração com os Estados-Membros, cria e mantém uma base de dados da UE que contenha as informações a que se referem os n.os 2 e 3 do presente artigo relativas aos sistemas de IA de risco elevado a que se refere o artigo 6.º, n.º 2, que estejam registados em conformidade com os artigos 49.º e 60.º e aos sistemas de IA que não são considerados de risco elevado nos termos do artigo 6.º, n.º 3, e que se encontram registados em conformidade com o artigos 6.º, n.º 4 e artigo 49.º. Ao definir as especificações funcionais dessa base de dados, a Comissão consulta os peritos pertinentes e, ao atualizar as especificações funcionais dessa base de dados, a Comissão consulta o Comité.

2. Os dados enumerados no anexo VIII, secções A e B, são introduzidos na base de dados da UE pelo prestador ou, se aplicável, pelo mandatário.

3. Os dados enumerados no anexo VIII, secção C, são introduzidos na base de dados da UE pelos responsáveis pela implantação que sejam autoridades públicas ou instituições, órgãos, organismos da União, ou que atuem em seu nome, em conformidade com o artigo 49.º, n.os 3 e 4.

4. Com exceção da secção a que se referem o artigo 49.º, n.º 4, e o artigo 60.º, n.º 4, alínea c), as informações contidas na base de dados da UE registadas em conformidade com o artigo 49.º devem ser acessíveis e disponibilizadas ao público de forma facilmente utilizável. As informações devem ser facilmente navegáveis e legíveis por máquina. As informações registadas em conformidade com o artigo 60.º só devem ser acessíveis às autoridades de fiscalização do mercado e à Comissão, a menos que o prestador ou potencial prestador tenha dado o seu consentimento para tornar essas informações igualmente acessíveis ao público.

5. 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 prestador ou o responsável pela implantação, conforme o caso.

6. A Comissão é o responsável pelo tratamento da base de dados da UE. A Comissão disponibiliza aos prestadores, potenciais prestadores e responsáveis pela implantação o apoio técnico e administrativo adequado. A base de dados da UE deve cumprir os requisitos de acessibilidade aplicáveis.

Capítulo IX
Acompanhamento pós-comercialização, partilha de informações, e fiscalização do mercado

SECÇÃO 1
ACOMPANHAMENTO PÓS-COMERCIALIZAÇÃO

Artigo 72.º

Acompanhamento pós-comercialização pelos prestadores e plano de acompanhamento pós- comercialização aplicável a sistemas de IA de risco elevado

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

2. O sistema de acompanhamento pós-comercialização recolhe, documenta e analisa de forma ativa e sistemática dados pertinentes quer facultados pelos responsáveis pela implantação quer recolhidos por meio de outras fontes sobre o desempenho dos sistemas de IA de risco elevado ao longo da sua vida útil, e que permitam ao prestador avaliar a contínua conformidade dos sistemas de IA com os requisitos estabelecidos no capítulo III, secção 2. Se for caso disso, o acompanhamento pós-comercialização inclui uma análise da interação com outros sistemas de IA. Esta obrigação não abrange os dados operacionais sensíveis dos responsáveis pela implantação que sejam autoridades responsáveis pela aplicação da lei.

3. O sistema de acompanhamento pós-comercialização deve basear-se num plano de acompanhamento pós-comercialização. O plano de acompanhamento pós-comercialização deve fazer parte da documentação técnica a que se refere o 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 até ... [18 meses a contar da entrada em vigor do presente regulamento]. O referido ato de execução é adotado de acordo com o procedimento de exame a que se refere o artigo 98.º, n.º 2.

4. No respeitante aos sistemas de IA de risco elevado abrangidos pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I, secção A, relativamente aos quais já se encontram estabelecidos um sistema e um plano de acompanhamento pós-comercialização ao abrigo dessa legislação, a fim de assegurar a coerência, evitar duplicações e minimizar encargos adicionais, os prestadores têm a opção de integrar, se for caso disso, os elementos necessários descritos nos n.os 1, 2 e 3, utilizando o modelo referido no n.º 3, nos sistemas e nos planos já existentes ao abrigo dessa legislação, desde que se atinja um nível de proteção equivalente.

O primeiro parágrafo do presente número também é aplicável aos sistemas de IA de risco elevado a que se refere o anexo III, ponto 5, colocados no mercado ou colocados em serviço por instituições financeiras e que estejam sujeitos a requisitos em matéria de governação, mecanismos ou processos internos nos termos do direito da União no domínio dos serviços financeiros.

SECÇÃO 2

PARTILHA DE INFORMAÇÕES SOBRE INCIDENTES GRAVES

Artigo 73.º

Comunicação de incidentes graves

1. Os prestadores de sistemas de IA de risco elevado colocados no mercado da União devem comunicar os incidentes graves às autoridades de fiscalização do mercado dos Estados-Membros onde esses incidentes ocorrerem.

2. A comunicação a que se refere o n.º 1 deve ser efetuada imediatamente após o prestador ter determinado uma relação causal, ou a probabilidade razoável de que exista uma relação causal, entre o sistema de IA e o incidente grave e, em qualquer caso, o mais tardar 15 dias após o prestador ou, se for caso disso, o responsável pela implantação ter tomado conhecimento do incidente grave.

   O prazo para efetuar a comunicação a que se refere o primeiro parágrafo deve ter em conta a severidade do incidente grave.

3. Não obstante o disposto no n.º 2 do presente artigo, em caso de infração generalizada ou incidente grave na aceção do artigo 3.º, ponto 49, alínea b), a comunicação a que se refere o n.º 1 do presente artigo é apresentada imediatamente e, o mais tardar, dois dias após o prestador ou, se for caso disso, o responsável pela implantação ter tomado conhecimento desse incidente.

4. Não obstante o disposto no n.º 2, em caso de morte de uma pessoa, a denúncia deve ser apresentada imediatamente após o prestador ou o responsável pela implantação ter determinado uma relação causal, ou logo que suspeite de uma relação causal, entre o sistema de IA de risco elevado e o incidente grave, mas o mais tardar dez dias após a data em que o prestador ou, se for caso disso, o responsável pela implantação tomou conhecimento do incidente grave.

5. Sempre que necessário, a fim de assegurar a comunicação atempada, o prestador ou, se for caso disso, o responsável pela implantação pode apresentar um relatório inicial incompleto, seguido de um relatório completo.

6. Na sequência da comunicação de um incidente grave nos termos do n.º 1, o prestador procede, sem demora, à investigação necessária a respeito desse incidente grave e do sistema de IA em causa. Tal inclui uma avaliação de risco do incidente e medidas corretivas.

   O prestador coopera com as autoridades competentes e, se pertinente, com o organismo notificado em causa durante a investigação a que se refere o primeiro parágrafo, e não realiza qualquer investigação que implique a alteração do sistema de IA em causa de um modo que possa afetar qualquer posterior avaliação das causas do incidente antes de informar as autoridades competentes de tal ação.

7. Após receção de uma notificação relacionada com um incidente grave a que se refere o artigo 3.º, ponto 49, alínea c), a autoridade de fiscalização do mercado pertinente deve informar as autoridades ou os organismos públicos nacionais a que se refere o artigo 77.º, n.º 1. A Comissão elabora orientações específicas para facilitar o cumprimento das obrigações previstas no n.º 1 do presente artigo. As referidas orientações são publicadas até ... [12 meses a contar da entrada em vigor do presente regulamento] e são avaliadas periodicamente.

8. A autoridade de fiscalização do mercado toma as medidas adequadas, tal como previsto no artigo 19.º do Regulamento (UE) 2019/1020, no prazo de sete dias a contar da data de receção da notificação a que se refere o n.º 1 do presente artigo e segue os procedimentos de notificação previstos no referido regulamento.

9. Relativamente aos sistemas de IA de risco elevado referidos no anexo III colocados no mercado ou colocados em serviço por prestadores que estejam sujeitos a instrumentos legislativos da União que estabeleçam obrigações de comunicação equivalentes às descritas no presente regulamento, a notificação de incidentes graves limita-se aos mencionados no artigo 3.º, ponto 49, alínea c).

10. 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 limita-se aos casos referidos no artigo 3.º, ponto 49, alínea c), do presente regulamento e é feita à autoridade nacional competente escolhida para o efeito pelos Estados-Membros em que ocorreu o incidente.

11. As autoridades nacionais competentes notificam imediatamente a Comissão de qualquer incidente grave, independentemente de terem ou não tomado medidas a seu respeito, em conformidade com o artigo 20.º do Regulamento (UE) 2019/1020.

SECÇÃO 3

EXECUÇÃO

Artigo 74.º

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

1. O Regulamento (UE) 2019/1020 é aplicável aos sistemas de IA abrangidos pelo presente regulamento. 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 artigo 2.º, n.º 1, 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 de aplicação do presente regulamento.

2. No âmbito das suas obrigações de comunicação nos termos do artigo 34.º, n.º 4, do Regulamento (UE) 2019/1020, as autoridades de fiscalização do mercado comunicam anualmente à Comissão e às autoridades nacionais competentes em matéria de concorrência todas as informações identificadas no decurso de atividades de fiscalização do mercado que possam ser de interesse potencial para a aplicação do direito da União em matéria de regras de concorrência. Também informam anualmente a Comissão sobre a utilização de práticas proibidas ocorridas durante esse ano e sobre as medidas tomadas.

3. No caso dos sistemas de IA de risco elevado abrangidos pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I, secção A, a autoridade de fiscalização do mercado para efeitos do presente regulamento é a autoridade responsável pelas atividades de fiscalização do mercado designada nos termos desses atos jurídicos.

Em derrogação do disposto no primeiro parágrafo, e nas circunstâncias adequadas, os Estados-Membros podem designar outra autoridade competente para atuar como autoridade de fiscalização do mercado, desde que assegurem a coordenação com as autoridades setoriais de fiscalização do mercado competentes responsáveis pela aplicação da legislação de harmonização da União enumerada no anexo I.

4. Os procedimentos a que se referem os artigos 79.º a 83.º do presente regulamento não se aplicam aos sistemas de IA relacionados com produtos abrangidos pelos atos enumerados na lista da legislação de harmonização da União constante do anexo I, secção A, se esses atos jurídicos já previrem procedimentos que assegurem um nível de proteção equivalente e tiverem o mesmo objetivo. Nesse caso, aplicam-se os procedimentos setoriais pertinentes.

5. Sem prejuízo dos poderes das autoridades de fiscalização do mercado nos termos do artigo 14.º do Regulamento (UE) 2019/1020, a fim de assegurar a execução efetiva do presente regulamento, as autoridades de fiscalização do mercado podem exercer à distância, conforme adequado, os poderes a que se refere o artigo 14.º, n.º 4, alíneas d) e j), do Regulamento (UE) 2019/1020.

6. No caso dos sistemas de IA de risco elevado colocados no mercado, colocados em serviço ou utilizados por instituições financeiras regulamentadas pela legislação da União no domínio dos serviços financeiros, a autoridade de fiscalização do mercado para efeitos do presente regulamento é a autoridade nacional responsável pela supervisão financeira dessas instituições ao abrigo da referida legislação, na medida em que a colocação no mercado, a colocação em serviço ou a utilização do sistema de IA esteja diretamente relacionada com a prestação desses serviços financeiros.

7. Em derrogação do n.º 6, nas circunstâncias adequadas e desde que assegurada a coordenação, o Estado-Membro pode identificar outra autoridade competente como autoridade de fiscalização do mercado para efeitos do presente regulamento.

As autoridades nacionais de fiscalização do mercado que supervisionam as instituições de crédito regulamentadas pela Diretiva 2013/36/UE e que participam no Mecanismo Único de Supervisão estabelecido pelo Regulamento (UE) n.º 1024/2013 devem comunicar sem demora ao Banco Central Europeu todas as informações identificadas no âmbito das suas atividades de fiscalização do mercado que possam ser de interesse potencial para as atribuições de supervisão prudencial do Banco Central Europeu especificadas nesse regulamento.

8. Para os sistemas de IA de risco elevado enumerados no anexo III, ponto 1, do presente regulamento, na medida em que os sistemas sejam utilizados para efeitos de aplicação da lei, gestão das fronteiras, justiça e democracia, e para os sistemas de IA de risco elevado enumerados no anexo III, pontos 6, 7 e 8, do presente regulamento, os Estados-Membros designam como autoridades de fiscalização do mercado para efeitos do presente regulamento as autoridades de controlo competentes em matéria de proteção de dados nos termos do Regulamento (UE) 2016/679 ou da Diretiva (UE) 2016/680, ou qualquer outra autoridade designada nas mesmas condições estabelecidas nos artigos 41.º a 44.º da Diretiva (UE) 2016/680. As atividades de fiscalização do mercado em nada afetam a independência das autoridades judiciárias nem se ingerem nas atividades destas últimas no exercício das suas funções judiciárias.

9. Sempre que as instituições, órgãos e organismos da União sejam abrangidos pelo âmbito do presente regulamento, a Autoridade Europeia para a Proteção de Dados atua como a autoridade de fiscalização do mercado dos mesmos, exceto em relação ao Tribunal de Justiça da União Europeia no exercício das suas funções jurisdicionais.

10. 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 dos atos enumerados na lista da legislação de harmonização da União constante do anexo I ou de outras disposições do direito da União suscetíveis de serem aplicáveis aos sistemas de IA de risco elevado a que se refere o anexo III.

11. As autoridades de fiscalização do mercado e a Comissão podem propor atividades conjuntas, incluindo investigações conjuntas, a realizar quer pelas autoridades de fiscalização do mercado quer pelas autoridades de fiscalização do mercado em conjunto com a Comissão, que tenham por objetivo promover a conformidade, identificar situações de não conformidade, sensibilizar ou disponibilizar orientações em relação ao presente regulamento no que diz respeito a categorias específicas de sistemas de IA de risco elevado consideradas como apresentando um risco grave em dois ou mais Estados-Membros, em conformidade com o artigo 9.º do Regulamento (UE) 2019/1020. O Serviço para a IA presta apoio à coordenação de investigações conjuntas.

12. Sem prejuízo dos poderes previstos no Regulamento (UE) 2019/1020, e sempre que pertinente e limitado ao necessário para o desempenho das suas funções, os prestadores devem conceder às autoridades de fiscalização do mercado total acesso à documentação, bem como aos conjuntos de dados de treino, validação e teste utilizados para o desenvolvimento dos sistemas de IA de risco elevado, inclusive, se for caso disso e sob reserva de salvaguardas de segurança, através de interfaces de programação de aplicações ou outros meios e ferramentas técnicas pertinentes que possibilitem o acesso remoto.

13. Deve ser concedido às autoridades de fiscalização do mercado o acesso ao código-fonte dos sistemas de IA de risco elevado mediante pedido fundamentado e apenas se estiverem preenchidas ambas as condições que se seguem:

    a) O acesso ao código-fonte é necessário para avaliar a conformidade de um sistema de IA de risco elevado com os requisitos estabelecidos no capítulo III, secção 2; e,

    b) Os procedimentos de testagem ou auditoria e as verificações com base nos dados e na documentação apresentados pelo prestador foram esgotados ou revelaram-se insuficientes.

14. Todas as informações ou documentação obtidas pelas autoridades de fiscalização do mercado devem ser tratadas em conformidade com as obrigações de confidencialidade estabelecidas no artigo 78.º.

Artigo 75.º

Assistência mútua, fiscalização do mercado e controlo dos sistemas de IA de finalidade geral

1. Sempre que um sistema de IA se baseie num modelo de IA de finalidade geral e o modelo e o sistema sejam desenvolvidos pelo mesmo prestador, o Serviço para a IA tem poderes para acompanhar e supervisionar a conformidade desse sistema de IA com as obrigações previstas no presente regulamento. Para desempenhar as suas funções de acompanhamento e supervisão, o Serviço para a IA dispõe de todos os poderes de uma autoridade de fiscalização do mercado previstos na presente secção e no Regulamento (UE) 2019/1020.

2. Caso tenham motivos suficientes para considerar que os sistemas de IA de finalidade geral que podem ser utilizados diretamente pelos responsáveis pela implantação para, pelo menos, uma finalidade classificada como sendo de risco elevado nos termos do presente regulamento não estão em conformidade com os requisitos estabelecidos no presente regulamento, as autoridades de fiscalização do mercado competentes cooperam com o Serviço para a IA no sentido de realizar avaliações da conformidade e informam a esse respeito o Comité e outras autoridades de fiscalização do mercado.

3. Quando uma autoridade de fiscalização do mercado não estiver em condições de concluir a sua investigação sobre o sistema de IA de risco elevado devido à sua incapacidade de aceder a determinadas informações relacionadas com o modelo de IA de finalidade geral, apesar de ter envidado todos os esforços adequados para obter essas informações, pode apresentar um pedido fundamentado ao Serviço para a IA a fim de que o acesso a essas informações seja garantido. Nesse caso, o Serviço para a IA presta à autoridade requerente sem demora e, em qualquer caso, no prazo máximo de 30 dias, todas as informações que o Serviço para a IA considere pertinentes para determinar se um sistema de IA de risco elevado não está conforme. As autoridades de fiscalização do mercado protegem a confidencialidade das informações que obtêm, em conformidade com o artigo 78.º do presente regulamento. O procedimento previsto no capítulo VI do Regulamento (UE) 2019/1020 é aplicável *mutatis mutandis*.

Artigo 76.º

Supervisão da testagem em condições reais pelas autoridades de fiscalização do mercado

1. As autoridades de fiscalização do mercado devem ter competências e poderes para assegurar que a testagem em condições reais está em conformidade com o presente regulamento.

2. Sempre que seja realizada uma testagem em condições reais para sistemas de IA supervisionados no âmbito de um ambiente de testagem da regulamentação da IA nos termos do artigo 58.º, as autoridades de fiscalização do mercado devem verificar a conformidade com o artigo 60.º no âmbito da sua função de supervisão do ambiente de testagem da regulamentação da IA. Essas autoridades podem, conforme adequado, permitir que a testagem em condições reais seja realizada pelo prestador ou potencial prestador em derrogação das condições estabelecidas no artigo 60.º, n.º 4, alíneas f) e g).

3. Se a autoridade de fiscalização do mercado for informada pelo prestador, pelo potencial prestador ou por terceiros de um incidente grave ou tiver outros motivos para considerar que as condições estabelecidas nos artigos 60.º e 61.º não estão preenchidas, pode tomar uma das seguintes decisões no seu território, conforme adequado:

   a) Suspender ou cessar a testagem em condições reais;

   b) Solicitar ao prestador ou potencial prestador e aos responsáveis pela implantação ou potenciais responsáveis pela implantação que alterem qualquer um dos aspetos da testagem em condições reais.

4. Se a autoridade de fiscalização do mercado tiver tomado uma das decisões referidas no n.º 3 do presente artigo ou formulado uma objeção na aceção do artigo 60.º, n.º 4, alínea b), a decisão ou objeção deve indicar os motivos da mesma e a forma como o prestador ou potencial prestador podem contestar a decisão ou objeção.

5. Se for caso disso, sempre que uma autoridade de fiscalização do mercado tomar uma das decisões referidas no n.º 3, deve comunicar os seus motivos às autoridades de fiscalização do mercado dos outros Estados-Membros em que o sistema de IA tenha sido testado em conformidade com o plano de testagem.

Artigo 77.º

Poderes das autoridades responsáveis pela proteção dos direitos fundamentais

1. As autoridades ou organismos públicos nacionais que supervisionam ou asseguram o respeito das obrigações previstas na legislação da União que protege os direitos fundamentais, incluindo o direito à não discriminação, no que se refere à utilização de sistemas de IA de risco elevado referidos no anexo III, têm poderes para solicitar e aceder a toda a documentação elaborada ou mantida nos termos do presente regulamento numa língua e formato acessíveis nos casos em que o acesso a essa documentação for necessário para o exercício dos seus mandatos 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.

2. Até ... [três meses a contar da entrada em vigor do presente regulamento], cada Estado-Membro deve fazer uma lista das autoridades ou organismos públicos a que se refere o n.º 1 e tornar essa lista acessível ao público. Os Estados-Membros devem notificar a lista à Comissão e aos outros Estados-Membros e mantê-la atualizada.

3. Se a documentação a que se refere o n.º 1 não for suficiente para determinar se ocorreu uma infração das obrigações impostas pela legislação da União que protege os direitos fundamentais, a autoridade ou organismo público a que se refere o n.º 1 pode apresentar um pedido fundamentado à autoridade de fiscalização do mercado para organizar a testagem do sistema de IA de risco elevado com recurso a meios técnicos. A autoridade de fiscalização do mercado deve organizar a testagem com a estreita participação da autoridade ou organismo público requerente num prazo razoável após o pedido.

4. Todas as informações ou documentação que as autoridades ou organismos públicos nacionais a que se refere o n.º 1 do presente artigo obtenham devem ser tratadas em conformidade com as obrigações de confidencialidade estabelecidas no artigo 78.º.

Artigo 78.º

Confidencialidade

1. A Comissão, as autoridades de fiscalização do mercado e os organismos notificados e qualquer outra pessoa singular ou coletiva envolvida na aplicação do presente regulamento respeitam, nos termos do direito da União ou nacional, a confidencialidade das informações e dos dados obtidos no exercício das suas funções e atividades de modo a proteger, em especial:

   a) Os direitos de propriedade intelectual e as informações comerciais de caráter confidencial ou os 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 (UE) 2016/943 do Parlamento Europeu e do Conselho[57];

   b) A execução efetiva do presente regulamento, em especial no que diz respeito à realização de inspeções, investigações ou auditorias;

   c) Os interesses públicos e nacionais em matéria de segurança;

   d) A condução de processos penais ou administrativos;

[57] Diretiva (UE) 2016/943 do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativa à proteção de know-how e de informações comerciais confidenciais (segredos comerciais) contra a sua aquisição, utilização e divulgação ilegais (JO L 157 de 15.6.2016, p. 1).

e) As informações classificadas nos termos do direito da União ou do direito nacional.

2. As autoridades envolvidas na aplicação do presente regulamento nos termos do n.º 1 solicitam apenas os dados que sejam estritamente necessários para a avaliação do risco apresentado pelos sistemas de IA e para o exercício dos seus poderes nos termos do presente regulamento e do Regulamento (UE) 2019/1020. Adotam medidas de cibersegurança adequadas e eficazes para proteger a segurança e a confidencialidade das informações e dos dados obtidos e apagam os dados recolhidos logo que estes deixem de ser necessários para a finalidade para a qual foram obtidos, em conformidade com o direito da União ou o direito nacional aplicável.

3. Sem prejuízo do n.os 1 e 2, as informações trocadas a título confidencial entre autoridades nacionais competentes ou entre as autoridades nacionais competentes e a Comissão não podem ser divulgadas sem serem previamente consultados a autoridade nacional competente de origem e o responsável pela implantação, caso os sistemas de IA de risco elevado a que se refere o anexo III, pontos 1, 6 ou 7, sejam utilizados por autoridades competentes em matéria de aplicação da lei, controlo das fronteiras, imigração ou asilo e caso tal divulgação prejudique interesses públicos e nacionais em matéria de segurança. Este intercâmbio de informações não abrange os dados operacionais sensíveis relacionados com as atividades das autoridades competentes em matéria de aplicação da lei, controlo das fronteiras, imigração ou asilo.

Se as autoridades competentes em matéria de aplicação da lei, imigração ou asilo forem os prestadores de sistemas de IA de risco elevado a que se refere o anexo III, pontos 1, 6 ou 7, a documentação técnica a que se refere o anexo IV deve permanecer nas instalações dessas autoridades. As referidas autoridades devem assegurar que as autoridades de fiscalização do mercado a que se refere o artigo 74.º, n.os 8 e 9, conforme aplicável, 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 de credenciação de segurança adequado.

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

5. A Comissão e os Estados-Membros podem, quando necessário e no respeito das disposições pertinentes de acordos internacionais e comerciais, trocar informações confidenciais com as autoridades reguladoras de países terceiros com as quais tenham celebrado acordos de confidencialidade bilaterais ou multilaterais que garantam um nível adequado de confidencialidade.

Artigo 79.º

Procedimento a nível nacional aplicável aos sistemas de IA que apresentam um risco

1. Entende-se por sistemas de IA que apresentam um risco um «produto que apresenta um risco» na aceção do artigo 3.º, ponto 19, do Regulamento (UE) 2019/1020, na medida em que apresentem riscos para a saúde ou a segurança ou para os direitos fundamentais das pessoas.

2. Se a autoridade de fiscalização do mercado de um Estado-Membro tiver motivo suficiente para considerar que um sistema de IA apresenta um risco a que se refere o n.º 1 do presente artigo, avalia o sistema de IA em causa no que diz respeito à conformidade do mesmo com todos os requisitos e obrigações previstos no presente regulamento. Deve ser dada especial atenção aos sistemas de IA que apresentem um risco para os grupos vulneráveis. Se forem identificados riscos para os direitos fundamentais, a autoridade de fiscalização do mercado também deve informar as autoridades ou os organismos públicos nacionais competentes a que se refere o artigo 77.º, n.º 1, e com eles cooperar plenamente. Os operadores pertinentes cooperam na medida do necessário com a autoridade de fiscalização do mercado e as outras autoridades ou organismos públicos nacionais a que se refere o artigo 77.º, n.º 1.

Se, no decurso dessa avaliação, a autoridade de fiscalização do mercado ou, se for caso disso, a autoridade de fiscalização do mercado em cooperação com a autoridade publica nacional a que se refere o artigo 77.º, n.º 1, verificar que o sistema de IA não cumpre os requisitos e as obrigações previstos no presente regulamento, exige sem demora injustificada ao operador pertinente 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 que pode ser fixado pela autoridade de fiscalização do mercado e, em todo o caso, no prazo máximo de quinze dias úteis ou no prazo previsto na legislação de harmonização da União pertinente, consoante o que for mais curto.

A autoridade de fiscalização do mercado deve informar desse facto o organismo notificado competente. O artigo 18.º do Regulamento (UE) 2019/1020 é aplicável às medidas a que se refere o segundo parágrafo do presente número.

3. Se a autoridade de fiscalização do mercado considerar que a não conformidade não se limita ao respetivo território nacional, deve comunicar sem demora injustificada 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 a que se refere o n.º 2, a autoridade de fiscalização do mercado deve tomar todas as medidas provisórias adequadas para proibir ou restringir a disponibilização ou colocação em serviço do sistema de IA no respetivo mercado nacional, para retirar o produto ou o sistema de IA autónomo desse mercado ou para o recolher. A referida autoridade notifica sem demora justificada a Comissão e os outros Estados-Membros da adoção de tais medidas.

6. A notificação a que se refere o n.º 5 deve conter todas as informações disponíveis, em especial as informações necessárias à identificação do sistema de IA não conforme, a origem do sistema de IA e a cadeia de distribuição, a natureza da alegada não conformidade e o risco conexo, a natureza e a duração das medidas nacionais adotadas, bem como os argumentos apresentados pelo operador em causa. As autoridades de fiscalização do mercado devem, nomeadamente, indicar se a não conformidade se deve a um ou vários dos seguintes motivos:

   a) Incumprimento da proibição das práticas de IA a que se refere o artigo 5.º;

   b) Incumprimento, por parte do sistema de IA de risco elevado, dos requisitos estabelecidos no capítulo III, secção 2;

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

d) Incumprimento do artigo 50.º.

7. As autoridades de fiscalização do mercado, com exceção da autoridade de fiscalização do mercado do Estado-Membro que desencadeou o procedimento, devem informar sem demora injustificada 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 da notificação a que se refere o n.º 5 do presente artigo, nem uma autoridade de supervisão do mercado de um Estado-Membro nem a Comissão tiverem formulado objeções à medida provisória tomada por uma autoridade de supervisão do mercado de um outro 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. O prazo de três meses referido no presente número é reduzido para 30 dias em caso de incumprimento da proibição das práticas de IA a que se refere o artigo 5.º do presente regulamento.

9. As autoridades de fiscalização do mercado garantem que sejam tomadas as medidas restritivas adequadas relativas ao produto ou ao sistema de IA em causa, como a retirada do produto ou do sistema de IA do respetivo mercado, sem demora injustificada.

Artigo 80.º

Procedimento aplicável aos sistemas de IA classificados pelo prestador como não sendo de risco elevado em aplicação do anexo III

1. Sempre que uma autoridade de fiscalização do mercado tenha motivo suficiente para considerar que um sistema de IA, classificado pelo prestador como não sendo de risco elevado nos termos do artigo 6.º, n.º 3, é de risco elevado, a autoridade de fiscalização do mercado realiza uma avaliação do sistema de IA em causa no que diz respeito à sua classificação como sistema de IA de risco elevado, com base nas condições estabelecidas no artigo 6.º, n.º 3, e nas orientações da Comissão.

2. Se, no decurso dessa avaliação, a autoridade de fiscalização do mercado considerar que o sistema de IA em causa é de risco elevado, exige ao prestador em causa, sem demora injustificada, que tome todas as medidas necessárias para assegurar a conformidade do sistema de IA com os requisitos e obrigações estabelecidos no presente regulamento, e que tome as medidas corretivas adequadas num prazo que pode ser fixado pela autoridade de fiscalização do mercado.

3. Se a autoridade de fiscalização do mercado considerar que a utilização do sistema de IA em causa não se restringe ao respetivo território nacional, comunica sem demora injustificada à Comissão e aos outros Estados-Membros os resultados da avaliação e as medidas que exigiu que o operador tomasse.

4. O prestador garante que sejam tomadas todas as medidas necessárias para assegurar a conformidade do sistema de IA com os requisitos e obrigações estabelecidos no presente regulamento. Se o prestador de um sistema de IA em causa não tornar o sistema de IA conforme com esses requisitos e obrigações no prazo referido no n.º 2 do presente artigo, esse prestador fica sujeito a coimas em conformidade com o artigo 99.º.

5. O prestador garante a aplicação de todas as medidas corretivas adequadas relativamente aos sistemas de IA em causa por si disponibilizados no mercado da União.

6. Se o prestador do sistema de IA em causa não tomar as medidas corretivas adequadas no prazo referido no n.º 2 do presente artigo, aplicam-se as disposições do artigo 79.º, n.os 5 a 9.

7. Se, no decurso da avaliação nos termos do n.º 1 do presente artigo, a autoridade de fiscalização do mercado concluir que o prestador classificou erradamente o sistema de IA como não sendo de risco elevado para contornar a aplicação dos requisitos previstos no capítulo III, secção 2, esse prestador fica sujeito a coimas em conformidade com o artigo 99.º.

8. No exercício dos seus poderes de acompanhamento da aplicação do presente artigo e em conformidade com o artigo 11.º do Regulamento (UE) 2019/1020, as autoridades de fiscalização do mercado podem efetuar verificações adequadas, tendo em conta, em especial, as informações armazenadas na base de dados da UE a que se refere o artigo 71.º do presente regulamento.

Artigo 81.º

Procedimento de salvaguarda da União

1. Se, no prazo de três meses após a receção da notificação a que se refere o artigo 79.º, n.º 5, ou no prazo de 30 dias em caso de incumprimento da proibição das práticas de IA a que se refere o artigo 5.º, a autoridade de fiscalização do mercado de um Estado-Membro formular objeções a uma medida tomada por outra autoridade de fiscalização do mercado, ou a Comissão considerar que a medida é contrária ao direito da União, a Comissão procede sem demora injustificada a consultas com a autoridade de fiscalização do mercado do Estado-Membro e o operador ou operadores em causa e avalia a medida nacional. Em função dos resultados dessa avaliação, a Comissão decide, no prazo de seis meses, ou no prazo de 60 dias em caso de incumprimento da proibição das práticas de IA a que se refere o artigo 5.º, a contar da notificação a que se refere o artigo 79.º, n.º 5, se a medida nacional é justificada, e notifica a sua decisão à autoridade de fiscalização do mercado do Estado-Membro em causa. A Comissão informa todas as outras autoridades de fiscalização do mercado da sua decisão.

2. Se a Comissão considerar que a medida tomada pelo Estado-Membro em causa é justificada, todos os Estados-Membros devem garantir que tomam medidas restritivas adequadas relativamente ao sistema de IA em causa, como exigir a retirada do sistema de IA do seu mercado sem demora injustificada, e informam a Comissão em conformidade. Se a Comissão considerar que a medida nacional é injustificada, o Estado-Membro em causa retira a medida e informa a Comissão em conformidade.

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 a que se referem os 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 82.º

Sistemas de IA conformes que apresentam um risco

1. Se, uma vez realizada a avaliação prevista no artigo 79.º, após consulta da autoridade de fiscalização do mercado em causa a que se refere o artigo 77.º, n.º 1, a autoridade de fiscalização do mercado de um Estado-Membro concluir que, embora cumpra o presente regulamento, um sistema de IA de risco elevado apresenta um risco para a saúde, a segurança ou os direitos fundamentais ou outros aspetos de proteção do interesse público, exige ao operador correspondente que tome sem demora injustificada, num prazo que pode ser fixado pela autoridade, todas as medidas adequadas para assegurar que, quando for colocado no mercado ou colocado em serviço, o sistema de IA em causa já não apresenta esse risco.

2. O prestador ou outro operador pertinente deve assegurar que a medida corretiva seja tomada relativamente a todos os sistemas de IA em causa que tenha disponibilizado no mercado da União, no prazo fixado pela autoridade de fiscalização do mercado do Estado-Membro a que se refere o n.º 1.

3. Os Estados-Membros informam imediatamente a Comissão e os restantes Estados-Membros da conclusão a que se refere o n.º 1. As informações prestadas devem incluir todos os dados disponíveis, em particular os dados necessários à identificação do sistema de IA em causa, a origem e a cadeia de distribuição do sistema de IA, a natureza do risco e a natureza e duração das medidas nacionais adotadas.

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

5. A Comissão comunica de imediato a sua decisão aos Estados-Membros em causa e aos operadores pertinentes. A Comissão informa igualmente os outros Estados-Membros.

Artigo 83.º

Não conformidade formal

1. Se a autoridade de fiscalização do mercado de um Estado-Membro chegar a uma das conclusões a seguir enunciadas, deve exigir ao prestador em causa que ponha termo à não conformidade em causa, num prazo que pode ser fixado pela autoridade:

   a) A marcação CE foi aposta em violação do disposto no artigo 48.º;

   b) Não foi aposta a marcação CE;

   c) Não foi elaborada uma declaração UE de conformidade referida no artigo 47.º;

d) Não foi elaborada corretamente uma declaração UE de conformidade referida no artigo 47.º;

e) Não foi efetuado o registo na base de dados da UE referido no artigo 71.º;

f) Não foi nomeado, quando aplicável, nenhum mandatário;

g) A documentação técnica não está disponível.

2. Se a não conformidade a que se refere o n.º 1 persistir, a autoridade de fiscalização do mercado do Estado-Membro em causa toma as medidas adequadas e proporcionadas 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 sem demora.

Artigo 84.º

Estruturas da União de apoio à testagem da IA

1. A Comissão designa uma ou mais estruturas da União de apoio à testagem para desempenhar as atividades enumeradas no artigo 21.º, n.º 6, do Regulamento (UE) 2019/1020 no domínio da IA.

2. Sem prejuízo das atividades a que se refere o n.º 1, as estruturas da União de apoio à testagem da IA também prestam aconselhamento técnico ou científico independente a pedido do Comité, da Comissão ou das autoridades de fiscalização do mercado.

SECÇÃO 4

VIAS DE RECURSO

Artigo 85.º

Direito de apresentar queixa a uma autoridade de fiscalização do mercado

Sem prejuízo de outras vias de recurso administrativas ou judiciais, qualquer pessoa singular ou coletiva que tenha motivos para considerar que houve uma infração às disposições do presente regulamento pode apresentar uma queixa à autoridade de fiscalização do mercado competente.

Em conformidade com o Regulamento (UE) 2019/1020, essas queixas devem ser tidas em conta para efeitos da realização das atividades de fiscalização do mercado e tratadas em conformidade com os procedimentos específicos estabelecidos para o efeito pelas autoridades de fiscalização do mercado.

Artigo 86.º

Direito a explicações sobre as decisões individuais

1. Qualquer pessoa afetada sujeita a uma decisão tomada pelo responsável pela implantação com base nos resultados de um sistema de IA de risco elevado enumerado no anexo III, com exceção dos sistemas enumerados no ponto 2 desse anexo, e que produza efeitos jurídicos ou analogamente afete num grau significativo essa pessoa, de forma que considere ter repercussões negativas na sua saúde, segurança ou direitos fundamentais, tem o direito de obter do responsável pela implantação explicações claras e pertinentes sobre o papel do sistema de IA no processo de tomada de decisão e sobre os principais elementos da decisão tomada.

2. O n.º 1 não se aplica à utilização de sistemas de IA para os quais as exceções ou restrições à obrigação prevista nesse número decorram do direito da União ou do direito nacional em conformidade com o direito da União.

3. O presente artigo só é aplicável na medida em que o direito a que se refere o n.º 1 não esteja estipulado em contrário no direito da União.

Artigo 87.º

Denúncia de infrações e proteção dos denunciantes

A Diretiva (UE) 2019/1937 aplica-se à denúncia de infrações ao presente regulamento e à proteção das pessoas que denunciam essas infrações.

SECÇÃO 5

SUPERVISÃO, INVESTIGAÇÃO, EXECUÇÃO E CONTROLO NO QUE RESPEITA A PRESTADORES DE MODELOS DE IA DE FINALIDADE GERAL

Artigo 88.º

Execução das obrigações dos prestadores de modelos de IA de finalidade geral

1. A Comissão dispõe de poderes exclusivos para supervisionar e fazer cumprir o disposto no capítulo V, tendo em conta as garantias processuais previstas no artigo 94.º. A Comissão confia a execução destas funções ao Serviço para a IA, sem prejuízo dos poderes de organização da Comissão e da repartição de competências entre os Estados-Membros e a União com base nos Tratados.

2. Sem prejuízo do disposto no artigo 75.º, n.º 3, as autoridades de fiscalização do mercado podem solicitar à Comissão que exerça os poderes previstos na presente secção, sempre que tal seja necessário e proporcionado para ajudar no desempenho das suas funções nos termos do presente regulamento.

Artigo 89.º

Medidas de acompanhamento

1. Para efeitos do desempenho das funções que lhe são confiadas nos termos da presente secção, o Serviço para a IA pode tomar as medidas necessárias para acompanhar a execução e o cumprimento efetivos do presente regulamento pelos prestadores de modelos de IA de finalidade geral, incluindo a observância de códigos de práticas aprovados.

2. Os prestadores a jusante têm o direito de apresentar uma queixa alegando uma infração ao presente regulamento. A queixa deve ser devidamente fundamentada e indicar, pelo menos:

   a) O ponto de contacto do prestador do modelo de IA de finalidade geral em causa;

   b) A descrição dos factos pertinentes, as disposições aplicáveis do presente regulamento e o motivo pelo qual o prestador a jusante considera que o prestador do modelo de IA de finalidade geral em causa infringiu o presente regulamento;

   c) Quaisquer outras informações que o prestador a jusante que tiver enviado o pedido considere pertinentes, incluindo, consoante o caso, informações que tenha recolhido por sua própria iniciativa.

Artigo 90.º

Alertas de riscos sistémicos emitidos pelo painel científico

1. O painel científico pode emitir um alerta qualificado ao serviço para a IA se tiver motivos para suspeitar que:

   a) Um modelo de IA de finalidade geral apresenta um risco concreto identificável a nível da União; ou

   b) Um modelo de IA de finalidade geral preenche as condições a que se refere o artigo 51.º.

2. Na sequência desse alerta qualificado, a Comissão, através do Serviço para a IA e após ter informado o Comité, pode exercer os poderes estabelecidos na presente secção para efeitos de avaliação da questão. O Serviço para a IA informa o Comité de qualquer medida em conformidade com os artigos 91.º a 94.º.

3. Um alerta qualificado deve ser devidamente fundamentado e indicar, pelo menos:

   a) O ponto de contacto do prestador do modelo de IA de finalidade geral com risco sistémico em causa;

   b) Uma descrição dos factos pertinentes e dos motivos para o alerta do painel científico;

   c) Quaisquer outras informações que o painel científico considere pertinentes, incluindo, consoante o caso, informações que tenha recolhido por sua própria iniciativa.

Artigo 91.º

Poder para solicitar documentação e informações

1. A Comissão pode solicitar ao prestador do modelo de IA de finalidade geral em causa que apresente a documentação elaborada pelo prestador em conformidade com os artigos 53.º e 55.º ou quaisquer informações adicionais necessárias para efeitos de avaliação da conformidade do prestador com o presente regulamento.

2. Antes de enviar o pedido de informações, o Serviço para a IA pode iniciar um diálogo estruturado com o prestador do modelo de IA de finalidade geral.

3. Mediante pedido devidamente fundamentado do painel científico, a Comissão pode apresentar um pedido de informações a um prestador de um modelo de IA de finalidade geral, sempre que o acesso à informação seja necessário e proporcionado para o desempenho das funções do painel científico no âmbito do artigo 68.º, n.º 2.

4. O pedido de informações indica a base jurídica e a finalidade do pedido, especifica que informações são necessárias, fixa o prazo em que as informações devem ser prestadas e indica as coimas previstas no artigo 101.º pela prestação de informações incorretas, incompletas ou enganosas.

5. O prestador do modelo de IA de finalidade geral em causa, ou o seu representante, presta as informações solicitadas. Caso se trate de pessoas coletivas, empresas ou associações de empresas, ou caso o prestador não tenha personalidade jurídica, as pessoas autorizadas a representá-las nos termos da lei ou dos respetivos estatutos prestam as informações solicitadas em nome do prestador do modelo de IA de finalidade geral em causa. Os advogados devidamente mandatados podem prestar as informações solicitadas em nome dos seus clientes. Contudo, os clientes são plenamente responsáveis em caso de prestação de informações incompletas, incorretas ou enganosas.

Artigo 92.º

Poder para realizar avaliações

1. O Serviço para a IA, após consulta do Comité, pode realizar avaliações do modelo de IA de finalidade geral em causa para:

   a) Avaliar o cumprimento, por parte do prestador, das obrigações decorrentes do presente regulamento, caso as informações recolhidas nos termos do artigo 91.º sejam insuficientes; ou,

   b) Investigar os riscos sistémicos a nível da União de modelos de IA de finalidade geral com risco sistémico, em especial na sequência de um alerta qualificado do painel científico em conformidade com o artigo 90.º, n.º 1, alínea a).

2. A Comissão pode decidir nomear peritos independentes para realizar avaliações em seu nome, incluindo peritos do painel científico criado nos termos do artigo 68.º. Os peritos independentes nomeados para exercer esta atribuição devem satisfazer os critérios enunciados no artigo 68.º, n.º 2.

3. Para efeitos do n.º 1, a Comissão pode solicitar o acesso ao modelo de IA de finalidade geral em causa através IPA ou de outros meios e ferramentas técnicas adequadas, incluindo o código-fonte.

4. O pedido de acesso indica a base jurídica, a finalidade e os motivos do pedido e fixa o prazo em que o acesso deve ser concedido, e as coimas previstas no artigo 101.º por não disponibilização do acesso.

5. Os prestadores do modelo de IA de finalidade geral em causa ou o seu representante, presta as informações solicitadas. No caso de pessoas coletivas, empresas ou associações de empresas, ou, caso os prestadores não tenham personalidade jurídica, as pessoas autorizadas a representá-las nos termos da lei ou dos respetivos estatutos, disponibilizam o acesso solicitado em nome do prestador do modelo de IA de finalidade geral em causa.

6. A Comissão adota atos de execução que estabelecem as modalidades pormenorizadas e as condições das avaliações, incluindo as modalidades pormenorizadas da participação de peritos independentes, e o procedimento de seleção destes últimos. Os referidos atos de execução são adotados de acordo com o procedimento de exame a que se refere o artigo 98.º, n.º 2.

7. Antes de solicitar o acesso ao modelo de IA de finalidade geral em causa, o Serviço para a IA pode iniciar um diálogo estruturado com o prestador do modelo de IA de finalidade geral para recolher mais informações sobre as testagens internas do modelo, as salvaguardas internas para prevenir riscos sistémicos e outros procedimentos e medidas internos que o prestador tenha tomado para atenuar esses riscos.

Artigo 93.º

Poder para solicitar medidas

1. Sempre que necessário e adequado, a Comissão pode solicitar aos prestadores que:

   a) Tomem medidas adequadas para cumprir as obrigações estabelecidas nos artigos 53.º e 54.º;

   b) Apliquem medidas de atenuação, caso a avaliação efetuada em conformidade com o artigo 92.º tenha suscitado preocupações sérias e fundamentadas quanto à existência de um risco sistémico a nível da União;

   c) Restrinjam a disponibilização no mercado, retirem ou recolham o modelo.

2. Antes de ser solicitada uma medida, o Serviço para a IA pode iniciar um diálogo estruturado com o prestador do modelo de IA de finalidade geral.

3. Se, durante o diálogo estruturado a que se refere o n.º 2, o prestador do modelo de IA de finalidade geral com risco sistémico se propuser a assumir compromissos no sentido de aplicar medidas de atenuação para fazer face a um risco sistémico a nível da União, a Comissão pode, mediante decisão, tornar esses compromissos vinculativos e declarar que não existem outros motivos para tomar medidas.

Artigo 94.º

Direitos processuais dos operadores económicos do modelo de IA de finalidade geral

O artigo 18.º do Regulamento (UE) 2019/1020 aplica-se, *mutatis mutandis*, aos prestadores do modelo de IA de finalidade geral, sem prejuízo de direitos processuais mais específicos previstos no presente regulamento.

Capítulo X

Códigos de conduta e orientações

Artigo 95.º

Códigos de conduta para a aplicação voluntária de requisitos específicos

1. O Serviço para a IA e os Estados-Membros promovem e facilitam a elaboração de códigos de conduta, incluindo os mecanismos de governação conexos, destinados a incentivar a aplicação voluntária de alguns ou de todos os requisitos estabelecidos no capítulo III, secção 2, a sistemas de IA que não sejam sistemas de IA de risco elevado, tendo em conta as soluções técnicas disponíveis e as boas práticas do setor que permitam a aplicação desses requisitos.

2. O Serviço para a IA e os Estados-Membros facilitam a elaboração de códigos de conduta relativos à aplicação voluntária, inclusive pelos responsáveis pela implantação, de requisitos específicos a todos os sistemas de IA, com base em objetivos claros e indicadores-chave de desempenho para medir a consecução desses objetivos, nomeadamente elementos como, entre outros:

a) Elementos aplicáveis das Orientações Éticas da União para uma IA de Confiança;

b) Avaliar e minimizar o impacto dos sistemas de IA na sustentabilidade ambiental, nomeadamente no que diz respeito à programação e às técnicas de conceção, treino e utilização da IA eficientes do ponto de vista energético;

c) Promover a literacia no domínio da IA, em especial das pessoas que lidam com o desenvolvimento, o funcionamento e a utilização da IA;

d) Facilitar uma conceção inclusiva e diversificada dos sistemas de IA, nomeadamente através da constituição de equipas de desenvolvimento inclusivas e diversificadas e da promoção da participação das partes interessadas nesse processo;

e) Avaliar e prevenir as repercussões negativas dos sistemas de IA nas pessoas vulneráveis ou nos grupos de pessoas vulneráveis, inclusive no que diz respeito à acessibilidade para pessoas com deficiências, bem como na igualdade de género.

3. Os códigos de conduta podem ser elaborados por prestadores ou responsáveis pela implantação de sistemas de IA a título individual ou por organizações que os representem, ou ambos, nomeadamente com a participação de quaisquer partes interessadas e das respetivas organizações representativas, incluindo organizações da sociedade civil e o meio académico. Os códigos de conduta podem abranger um ou mais sistemas de IA, tendo em conta a semelhança da finalidade prevista desses sistemas.

4. O Serviço para a IA e os Estados-Membros têm em conta as necessidades e os interesses específicos das PME, incluindo as empresas em fase de arranque, quando incentivam e facilitam a elaboração de códigos de conduta.

Artigo 96.º

Orientações da Comissão sobre a execução do presente regulamento

1. A Comissão elabora orientações sobre a execução prática do presente regulamento e, em especial, sobre:

   a) A aplicação dos requisitos e obrigações a que se referem os artigos 8.º a 15.º e o artigo 25.º;

   b) As práticas proibidas a que se refere o artigo 5.º;

   c) A execução prática das disposições relativas a alterações substanciais;

   d) A execução prática das obrigações de transparência estabelecidas no artigo 50.º;

e) As informações pormenorizadas sobre a relação do presente regulamento com os atos enumerados na lista da legislação de harmonização da União constante do anexo I, bem como com outras disposições pertinentes do direito da União, nomeadamente no que diz respeito à coerência na sua aplicação;

f) A aplicação da definição de um sistema de IA estabelecida no artigo 3.º, ponto 1.

Ao emitir essas orientações, a Comissão deve prestar especial atenção às necessidades das PME, incluindo as empresas em fase de arranque, das autoridades públicas locais e dos setores mais suscetíveis de serem afetados pelo presente regulamento.

As orientações a que se refere o primeiro parágrafo do presente número devem ter devidamente em conta o estado da arte geralmente reconhecido em matéria de IA, bem como as normas harmonizadas e especificações comuns pertinentes a que se referem os artigos 40.º e 41.º, ou as normas harmonizadas ou especificações técnicas estabelecidas nos termos da legislação de harmonização da União.

2. A pedido dos Estados-Membros ou do Serviço para a IA, ou por sua própria iniciativa, a Comissão atualiza as orientações previamente adotadas quando tal for considerado necessário.

CAPÍTULO XI

Delegação de poderes e procedimento de comité

Artigo 97.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 a que se refere o artigo 6.º, n.ºs 6 e 7, o artigo 7.º, n.os 1 e 3, o artigo 11.º, n.º 3, o artigo 43.º, n.os 5 e 6, o artigo 47.º, n.º 5, o artigo 51.º, n.º 3, o artigo 52.º, n.º 4, e o artigo 53.º, n.os 5 e 6, é conferido à Comissão por um prazo de cinco anos a contar de ... [data de entrada em vigor do presente regulamento]. A Comissão elabora um relatório relativo à delegação de poderes pelo menos nove meses antes do final do prazo de cinco anos. A delegação de poderes é tacitamente prorrogada por períodos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem pelo menos três meses antes do final de cada prazo.

3. A delegação de poderes a que se refere o artigo 6.º, n.ºs 6 e 7, o artigo 7.º, n.os 1 e 3, o artigo 11.º, n.º 3, o artigo 43.º, n.os 5 e 6, o artigo 47.º, n.º 5, o artigo 51.º, n.º 3, o artigo 52.º, n.º 4, e o artigo 53.º, n.os 5 e 6, 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. Antes de adotar um ato delegado, a Comissão consulta os peritos designados por cada Estado-Membro de acordo com os princípios estabelecidos no Acordo Interinstitucional, de 13 de abril de 2016, sobre legislar melhor.

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

6. Os atos delegados adotados nos termos do artigo 6.º, n.ºs 6 ou 7, do artigo 7.º, n.os 1 ou 3, do artigo 11.º, n.º 3, do artigo 43.º, n.os 5 ou 6, do artigo 47.º, n.º 5, do artigo 51.º, n.º 3, do artigo 52.º, n.º 4, ou do artigo 53.º, n.os 5 ou 6, 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 98.º

Procedimento de comité

1. A Comissão é assistida por um comité. Esse 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.

Capítulo XII

Sanções

Artigo 99.º

Sanções

1. Em conformidade com os termos e as condições previstos no presente regulamento, os Estados-Membros determinam o regime de sanções e outras medidas de execução, que podem também incluir advertências e medidas não pecuniárias, aplicável em caso de infração do presente regulamento por parte dos operadores, e tomam todas as medidas necessárias para garantir que o mesmo é aplicado correta e eficazmente, tendo, por isso, em conta as orientações emitidas pela Comissão em conformidade com o artigo 96.º. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas. Devem ter em conta os interesses das PME, incluindo as empresas em fase de arranque, e a respetiva viabilidade económica.

2. Os Estados-Membros notificam sem demora a Comissão do regime de sanções e de outras medidas de execução a que se refere o n.º 1, o mais tardar até à data de início da sua aplicação, bem como de qualquer alteração subsequente das mesmas.

3. O incumprimento da proibição das práticas de IA a que se refere o artigo 5.º fica sujeito a coimas num montante que pode ir até 35 000 000 EUR ou, se o infrator for uma empresa, até 7 % do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado.

4. A não conformidade com quaisquer das seguintes disposições relacionadas com operadores ou organismos notificados que não os estabelecidos no artigo 5.º fica sujeita a coimas até 15 000 000 EUR ou, se o infrator for uma empresa, até 3 % do seu volume de negócios anual a nível mundial no exercício anterior, consoante o que for mais elevado:

a) As obrigações dos prestadores nos termos dos artigo 16.º;

b) As obrigações dos mandatários nos termos do artigo 22.º;

c) As obrigações dos importadores nos termos do artigo 23.º;

d) As obrigações dos distribuidores nos termos do artigo 24.º;

e) As obrigações dos responsáveis pela implantação nos termos do artigo 26.º;

f) Os requisitos e obrigações dos organismos notificados nos termos do artigo 31.º, do artigo 33.º, n.os 1, 3 e 4, e do artigo 34.º;

g) As obrigações de transparência para os prestadores e responsáveis pela implantação nos termos do artigo 50.º.

5. A prestação de informações incorretas, incompletas ou falaciosas aos organismos notificados ou às autoridades nacionais competentes em resposta a um pedido fica sujeita a coimas num montante que pode ir até 7 500 000 EUR ou, se o infrator for uma empresa, até 1 % do seu volume de negócios anual total a nível mundial no exercício anterior, consoante o que for mais elevado.

6. No caso das PME, incluindo as empresas em fase de arranque, cada coima a que se refere o presente artigo não pode exceder as percentagens ou o montante a que se referem os n.os 3, 4 e 5, consoante o que for mais baixo.

7. Ao decidir sobre a aplicação de uma coima e ao determinar o montante da mesma em cada caso, devem ser tidas em conta, em cada caso, todas as circunstâncias pertinentes da situação específica, bem como, conforme adequado, os seguintes elementos:

a) A natureza, a gravidade e a duração da infração e das suas consequências, tendo em conta a finalidade do sistema de IA, bem como, se for caso disso, o número de pessoas afetadas e o nível de danos por elas sofridos;

b) O facto de outras autoridades de fiscalização do mercado já terem ou não aplicado coimas ao mesmo operador pela mesma infração;

c) O facto de outras autoridades já terem ou não aplicado coimas ao mesmo operador por infrações a outras disposições do direito da União ou do direito nacional, quando tais infrações resultarem da mesma atividade ou omissão que constitua uma infração pertinente ao presente regulamento;

d) A dimensão, o volume de negócios anual e a quota de mercado do operador que cometeu a infração;

e) Qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como os benefícios financeiros obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração;

f) O grau de cooperação com as autoridades nacionais competentes, a fim de sanar a infração e atenuar os seus eventuais efeitos adversos;

g) O grau de responsabilidade do operador tendo em conta as medidas técnicas e organizacionais que aplicou;

h) A forma como as autoridades nacionais competentes tomaram conhecimento da infração, em especial se foram notificadas pelo operador e, em caso afirmativo, em que medida o operador o fez;

i) O caráter doloso ou negligente da infração;

j) As medidas tomadas pelo operador para atenuar os danos sofridos pelas pessoas afetadas.

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

9. Em função do ordenamento jurídico dos Estados-Membros, as regras relativas às coimas podem ser aplicadas de maneira que as coimas sejam aplicadas pelos tribunais nacionais competentes ou por outros organismos, conforme aplicável nesses Estados-Membros. A aplicação dessas regras nesses Estados-Membros deve ter um efeito equivalente.

10. O exercício das competências ao abrigo do presente artigo fica sujeito às garantias processuais adequadas nos termos do direito da União e do direito nacional, incluindo o direito à ação judicial e a um processo equitativo.

11. Os Estados-Membros comunicam anualmente à Comissão as coimas que tenham aplicado durante esse ano, em conformidade com o presente artigo, bem como quaisquer litígios ou processos judiciais conexos.

Artigo 100.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 de aplicação do presente regulamento. Ao decidir da aplicação de uma coima e ao determinar o montante da mesma em cada caso, 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, tendo em conta a finalidade do sistema de IA em causa, bem como, quando necessário, o número de pessoas afetadas e o nível de danos por elas sofridos;

   b) O grau de responsabilidade da instituição, órgão ou organismo da União, tendo em conta as medidas técnicas e organizacionais que aplicaram;

   c) Qualquer medida tomada pela instituição, órgão ou organismo da União para atenuar os danos sofridos pelas pessoas afetadas;

   d) O grau de 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 das 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;

e) Quaisquer infrações similares anteriormente cometidas pela instituição, órgão ou organismo da União;

f) A forma como a Autoridade Europeia para a Proteção de Dados tomou conhecimento da infração, em especial se a instituição, órgão ou organismo da União a notificou e, em caso afirmativo, em que medida o fez;

g) O orçamento anual da instituição, órgão ou organismo da União.

2. O incumprimento da proibição das práticas de IA a que se refere o artigo 5.º fica sujeito a coimas num montante que pode ascender a 1 500 000 EUR.

3. A não conformidade do sistema de IA com quaisquer requisitos ou obrigações impostos por força do presente regulamento, que não os estabelecidos no artigo 5.º, fica sujeita a coimas num montante que pode ascender a 750 000 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 ser ouvida 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 aos quais as partes em causa tenham podido apresentar observações. Os queixosos, caso existam, devem ser estreitamente associados ao processo.

5. Os direitos de defesa das partes em causa devem ser plenamente respeitados ao longo do processo. As partes interessadas têm o direito de aceder ao processo da Autoridade Europeia para a Proteção de Dados, sob reserva do interesse legítimo das pessoas singulares ou das empresas relativamente à proteção dos respetivos dados pessoais ou segredos comerciais.

6. Os fundos recolhidos em resultado da aplicação das coimas previstas no presente artigo contribuem para o orçamento geral da União. As coimas não devem afetar a eficácia do funcionamento da instituição, órgão ou organismo da União alvo de aplicação de coimas.

7. A Autoridade Europeia para a Proteção de Dados comunica anualmente à Comissão as coimas que tenha aplicado nos termos do presente artigo, bem como quaisquer litígios e processos judiciais que tenha iniciado.

Artigo 101.º

Coimas aplicáveis aos prestadores de modelos de IA de finalidade geral

1. A Comissão pode aplicar aos prestadores de modelos de IA de finalidade geral coimas não superiores a 3 % do seu volume de negócios anual total a nível mundial no exercício financeiro anterior ou a 15 000 000 EUR, consoante o que for mais elevado, quando considerar que o prestador, dolosamente ou por negligência:

   a) Infringiu as disposições aplicáveis do presente regulamento;

   b) Não deu seguimento a um pedido de documentos ou informações nos termos do artigo 91.º, ou prestou informações incorretas, incompletas ou enganosas;

c) Não cumpriu uma medida solicitada nos termos do artigo 93.º;

d) Não disponibilizou à Comissão o acesso ao modelo de IA de finalidade geral ou ao modelo de IA de finalidade geral com risco sistémico para efeitos da realização de uma avaliação nos termos do artigo 92.º.

Na fixação do montante da coima ou da sanção pecuniária compulsória, deve atender-se à natureza, à gravidade e à duração da infração, tendo em devida conta os princípios da proporcionalidade e da adequação. A Comissão deve ter igualmente em conta os compromissos assumidos em conformidade com o artigo 93.º, n.º 3, ou assumidos nos códigos de práticas pertinentes em conformidade com o artigo 56.º.

2. Antes de adotar a decisão nos termos do n.º 1, a Comissão comunica as suas conclusões preliminares ao prestador do modelo de IA de finalidade geral e dá-lhe a oportunidade de ser ouvido.

3. As coimas aplicadas nos termos do presente artigo devem ser efetivas, proporcionadas e dissuasivas.

4. As informações sobre as coimas aplicadas ao abrigo do presente artigo também são comunicadas ao Comité, conforme adequado.

5. O Tribunal de Justiça da União Europeia tem competência de plena jurisdição para apreciar recursos das decisões em que a Comissão tenha aplicado uma coima ao abrigo do presente artigo, podendo anular a coima ou reduzir ou aumentar o seu valor.

6. A Comissão adota atos de execução que contenham as modalidades pormenorizadas e as garantias processuais dos processos tendo em vista a eventual adoção de decisões nos termos do n.º 1 do presente artigo. Os referidos atos de execução são adotados de acordo com o procedimento de exame a que se refere o artigo 98.º, n.º 2.

Capítulo XIII
Disposições finais

Artigo 102.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) 2024/... do Parlamento Europeu e do Conselho[*+], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção 2, desse regulamento.

---

[*] Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho, de ..., que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (JO L ..., ELI: ...).».

[+] JO: Inserir no texto o número do presente Regulamento (2021/0106(COD)) e completar a nota de rodapé correspondente.

Artigo 103.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) 2024/... do Parlamento Europeu e do Conselho[*+], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção 2, desse regulamento.

---

[*] Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho de ... que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (JO L ..., ELI: ...).».

[+] JO: Inserir no texto o número do presente regulamento (2021/0106(COD)) e completar a nota de rodapé correspondente.

Artigo 104.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) 2024/... do Parlamento Europeu e do Conselho[*+], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção 2, desse regulamento.

---

[*] Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho, de ..., que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (JO L ..., ELI: ...).».

[+] JO: Inserir no texto o número do presente regulamento (2021/0106(COD)) e completar a nota de rodapé correspondente.

Artigo 105.º

Alteração da Diretiva 2014/90/UE

Ao artigo 8.º da Diretiva 2014/90/UE, é aditado o seguinte número:

«5. No tocante aos sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho[*+], ao realizar as suas atividades nos termos do n.º 1 e ao adotar especificações técnicas e normas de ensaio em conformidade com os n.os 2 e 3, a Comissão tem em conta os requisitos estabelecidos no capítulo III, secção 2, desse regulamento.

---

[*] Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho de ... que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (JO L ..., ELI: ...).».

[+] JO: Inserir no texto o número do presente regulamento (2021/0106(COD)) e completar a nota de rodapé correspondente.

Artigo 106.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) 2024/... do Parlamento Europeu e do Conselho[*+], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção 2, desse regulamento.

---

* Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho de ... que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (JO L ..., ELI: ...).».

+ JO: Inserir no texto o número do presente regulamento (2021/0106(COD)) e completar a nota de rodapé correspondente.

Artigo 107.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) 2024/... do Parlamento Europeu e do Conselho[*+], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção 2, desse regulamento.

---

[*] Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho de ... que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (JO L ..., ELI: ...).».

[+] JO: Inserir no texto o número do presente Regulamento (2021/0106(COD)) e completar a nota de rodapé correspondente.

Artigo 108.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) 2024/... do Parlamento Europeu e do Conselho[*+], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção 2, desse regulamento.

---

[*] Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho, de ..., que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (JO L ..., ELI: ...).»;

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) 2024/...[++], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção 2, desse regulamento.»;

[+] JO: Inserir no texto o número do presente regulamento (2021/0106(COD)) e completar a nota de rodapé correspondente.

[++], [++] JO: Inserir o número do presente regulamento (2021/0106(COD)).

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) 2024/...[+], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção2, 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) 2024/...[+], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção 2, desse regulamento.»;

5) Ao artigo 57.º, é aditado o seguinte parágrafo:

«Na adoção desses atos de execução relativamente a sistemas de inteligência artificial que constituem componentes de segurança na aceção do Regulamento (UE) 2024/...[+], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção 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) 2024/...[+], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção 2, desse regulamento.».

[+] JO: Inserir o número do presente regulamento (2021/0106(COD)).

[+] JO: Inserir o número do presente regulamento (2021/0106(COD)).

Artigo 109.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) 2024/... do Parlamento Europeu e do Conselho[*++], devem ser tidos em conta os requisitos estabelecidos no capítulo III, secção 2, desse regulamento.

---

[*] Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho, de ..., que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (JO L ..., ELI: ...).».

[++] JO: Inserir no texto o número do presente regulamento (2021/0106(COD)) e completar a nota de rodapé correspondente.

Artigo 110.º

Alteração da Diretiva (UE) 2020/1828

Ao anexo I da Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho[58], é aditado o seguinte ponto:

«68) Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho[+], de ..., que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial) (JO L ..., ELI: ...)».

Artigo 111.º

Sistemas de inteligência artificial já colocados no mercado ou colocados em serviço e modelos de IA de finalidade geral já colocados no mercado

1. Sem prejuízo da aplicação do artigo 5.º, tal como referido no artigo 113.º, n.º 3, alínea a), os sistemas de IA que sejam componentes de sistemas informáticos de grande escala criados pelos atos jurídicos enumerados no anexo X que tenham sido colocados no mercado ou colocados em serviço antes de ... [36 meses a contar da data de entrada em vigor do presente regulamento] devem ser tornados conformes com o presente regulamento até 31 de dezembro de 2030.

---

58 Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho, de 25 de novembro de 2020, relativa a ações coletivas para proteção dos interesses coletivos dos consumidores e que revoga a Diretiva 2009/22/CE (JO L 409 de 4.12.2020, p. 1).

[+] JO: Inserir no texto a data e o número da diretiva que consta do presente regulamento.

Os requisitos estabelecidos no presente regulamento devem ser tidos em conta na avaliação de cada um dos sistemas informáticos de grande escala criados pelos atos jurídicos enumerados no anexo X, a realizar como previsto nesses atos jurídicos e sempre que esses atos jurídicos sejam substituídos ou alterados.

2. Sem prejuízo da aplicação do artigo 5.º, tal como referido no artigo 113.º, n.º 3, alínea a), o presente regulamento só se aplica aos operadores de sistemas de IA de risco elevado, excluindo os sistemas a que se refere o n.º 1 do presente artigo, que tenham sido colocados no mercado ou colocados em serviço antes de ... [24 meses a contar da data de entrada em vigor do presente regulamento], se, após essa data, os referidos sistemas forem sujeitos a alterações significativas em termos de conceção. Em qualquer caso, os prestadores e os responsáveis pela implantação de sistemas de IA de risco elevado concebidos para serem utilizados por autoridades públicas, tomam as medidas necessárias para cumprir os requisitos e com as obrigações previstos no presente regulamento até ... [seis anos a contar da data de entrada em vigor do presente regulamento].

3. Os prestadores de modelos de IA de finalidade geral que tenham sido colocados no mercado antes de ... [12 meses a contar da data de entrada em vigor do presente regulamento] tomam as medidas necessárias para cumprir as obrigações estabelecidas no presente regulamento até ... [36 meses a contar da data de entrada em vigor do presente regulamento].

Artigo 112.º

Avaliação e reexame

1. A Comissão avalia a necessidade de alterar a lista que consta do anexo III e a lista das práticas de IA proibidas prevista no artigo 5.º, uma vez por ano após a entrada em vigor do presente regulamento e até ao final do prazo da delegação de poderes prevista no artigo 97.º. A Comissão apresenta os resultados dessa avaliação ao Parlamento Europeu e ao Conselho.

2. Até ... [quatro anos a contar da data de entrada em vigor do presente regulamento] e, posteriormente, de quatro em quatro anos, a Comissão avalia e apresenta ao Parlamento Europeu e ao Conselho um relatório sobre o seguinte:

   a) A necessidade de alterações que alarguem as rubricas existentes ou acrescentem novas rubricas no anexo III;

   b) Alterações à lista de sistemas de IA que, nos termos do artigo 50.º, exigem medidas de transparência adicionais;

   c) Alterações que aumentem a eficácia do sistema de supervisão e governação.

3. Até … [cinco anos a contar da data de entrada em vigor do presente regulamento] e, posteriormente, de quatro em quatro anos, a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e reexame do presente regulamento. O relatório deve incluir uma avaliação da estrutura de execução e da eventual necessidade de um organismo da União para resolver as deficiências identificadas. Com base nas conclusões, esse relatório é acompanhado, quando adequado, de uma proposta de alteração do presente regulamento. Os relatórios devem ser divulgados ao público.

4. Os relatórios a que se refere o n.º 2 devem dar especial atenção ao seguinte:

a) A situação das autoridades nacionais competentes em termos de recursos financeiros, técnicos e humanos necessários para desempenhar eficazmente as funções que lhes foram atribuídas nos termos do presente regulamento;

b) O estado das sanções, nomeadamente das coimas a que se refere o artigo 99.º, n.º 1, aplicadas pelos Estados-Membros em consequência de infrações ao presente regulamento;

c) Normas harmonizadas adotadas e especificações comuns elaboradas para apoiar o presente regulamento;

d) O número de empresas que entram no mercado após o início da aplicação do presente regulamento e quantas delas são PME.

5. Até ... [quatro anos a contar da data de entrada em vigor do presente regulamento], a Comissão avalia o funcionamento do Serviço para a IA, a questão de saber se foram atribuídos ao Serviço para a IA poderes e competências suficientes para o desempenho das suas funções e se, para a correta aplicação e execução do presente regulamento, seria pertinente e necessário reforçar o Serviço para a IA e os seus poderes de execução, bem como aumentar os seus recursos. A Comissão apresenta um relatório sobre a sua avaliação ao Parlamento Europeu e ao Conselho.

6. Até ... [quatro anos a contar da data de entrada em vigor do presente regulamento] e, posteriormente, de quatro em quatro anos, a Comissão apresenta um relatório sobre a análise dos progressos realizados no desenvolvimento de produtos de normalização sobre o desenvolvimento eficiente do ponto de vista energético de modelos de IA de finalidade geral e avalia a necessidade de novas medidas ou ações, incluindo medidas ou ações vinculativas. O relatório é apresentado ao Parlamento Europeu e ao Conselho e é tornado público.

7. Até ... [quatro anos a contar da data de entrada em vigor do presente regulamento] e, posteriormente, de três em três anos, a Comissão avalia o impacto e a eficácia dos códigos de conduta voluntários destinados a fomentar a aplicação dos requisitos estabelecidos no capítulo III, secção 2, a sistemas de IA que não sejam sistemas de IA de risco elevado e, eventualmente, de outros requisitos adicionais a sistemas de IA que não sejam sistemas de IA de risco elevado, inclusive no que diz respeito à sustentabilidade ambiental.

8. Para efeitos do disposto nos n.os 1 a 7, o Comité, os Estados-Membros e as autoridades nacionais competentes devem facultar à Comissão, sem demora injustificada, as informações que esta solicitar.

9. Ao efetuar as avaliações e os reexames a que se referem os n.os 1 a 7, a Comissão tem em consideração as posições e as conclusões do Comité, do Parlamento Europeu, do Conselho e de outros organismos ou fontes pertinentes.

10. Se necessário, a Comissão apresenta propostas adequadas com vista a alterar o presente regulamento, atendendo, em especial, à evolução das tecnologias, ao efeito dos sistemas de IA na saúde, na segurança e nos direitos fundamentais e aos progressos da sociedade da informação.

11. Para orientar as avaliações e os reexames referidos nos n.os 1 a 7 do presente artigo, o Serviço para a IA compromete-se a desenvolver uma metodologia objetiva e participativa para a avaliação dos níveis de risco com base nos critérios estabelecidos nos artigos pertinentes e a inclusão de novos sistemas:

a) Na lista constante do anexo III, incluindo a extensão dos domínios existentes ou o aditamento de novos domínios nesse anexo;

b) Na lista das práticas proibidas que consta do artigo 5.º; e

c) Na lista dos sistemas de IA que, nos termos do artigo 50.º, exigem medidas de transparência adicionais.

12. Qualquer alteração do presente regulamento nos termos do n.º 10, ou de atos delegados ou de execução pertinentes, que incida sobre os atos enumerados na lista da legislação setorial de harmonização da União constante do anexo I, secção B, deve ter em conta as especificidades regulamentares de cada setor e os mecanismos aplicáveis em matéria de governação, avaliação da conformidade e de execução, bem como as autoridades previstas nos mesmos.

13. Até ... [sete anos a contar da data de entrada em vigor do presente regulamento], a Comissão procede a uma avaliação da execução do presente regulamento e apresenta um relatório da avaliação ao Parlamento Europeu, ao Conselho e ao Comité Económico e Social Europeu, tendo em conta os primeiros anos de aplicação do presente regulamento. Com base nas conclusões, tal relatório deve, quando adequado, ser acompanhado de uma proposta de alteração do presente regulamento no que diz respeito à estrutura de execução e à necessidade de um organismo da União para resolver quaisquer deficiências identificadas.

Artigo 113.º

Entrada em vigor e aplicação

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é aplicável a partir de ... [24 meses a contar da data de entrada em vigor do presente regulamento].

Contudo:

a) Os capítulos I e II são aplicáveis a partir de ... [seis meses a contar da data de entrada em vigor do presente regulamento];

b) O capítulo III, secção 4, o capítulo V, o capítulo VII e o capítulo XII e o artigo 78.º são aplicáveis a partir de ... [12 meses a contar da data de entrada em vigor do presente regulamento], com exceção do artigo 101.º;

c) O artigo 6.º, n.º 1, e as obrigações correspondentes previstas no presente regulamento são aplicáveis a partir de ... [36 meses a contar da data de 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 …, em …

Pelo Parlamento Europeu	*Pelo Conselho*
A Presidente	*O Presidente / A Presidente*

ANEXO I

Lista da legislação de harmonização da União

Secção A – Lista da legislação de harmonização da União baseada no novo regime jurídico

1. Diretiva 2006/42/CE do Parlamento Europeu e do Conselho, de 17 de maio de 2006, relativa às máquinas e que altera a Diretiva 95/16/CE (JO L 157 de 9.6.2006, p. 24) [revogada pelo Regulamento Máquinas];

2. Diretiva 2009/48/CE do Parlamento Europeu e do Conselho, de 18 de junho de 2009, relativa à segurança dos brinquedos (JO L 170 de 30.6.2009, p. 1);

3. Diretiva 2013/53/UE do Parlamento Europeu e do Conselho, de 20 de novembro de 2013, relativa às embarcações de recreio e às motas de água e que revoga a Diretiva 94/25/CE (JO L 354 de 28.12.2013, p. 90);

4. Diretiva 2014/33/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante a ascensores e componentes de segurança para ascensores (JO L 96 de 29.3.2014, p. 251);

5. Diretiva 2014/34/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à harmonização da legislação dos Estados-Membros relativa a aparelhos e sistemas de proteção destinados a ser utilizados em atmosferas potencialmente explosivas (JO L 96 de 29.3.2014, p. 309);

6. Diretiva 2014/53/UE do Parlamento Europeu e do Conselho, de 16 de abril de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos de rádio no mercado e que revoga a Diretiva 1999/5/CE (JO L 153 de 22.5.2014, p. 62);

7. Diretiva 2014/68/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa à harmonização da legislação dos Estados-Membros respeitante à disponibilização de equipamentos sob pressão no mercado (JO L 189 de 27.6.2014, p. 164);

8. Regulamento (UE) 2016/424 do Parlamento Europeu e do Conselho, de 9 de março de 2016, relativo às instalações por cabo e que revoga a Diretiva 2000/9/CE (JO L 81 de 31.3.2016, p. 1);

9. Regulamento (UE) 2016/425 do Parlamento Europeu e do Conselho, de 9 de março de 2016, relativo aos equipamentos de proteção individual e que revoga a Diretiva 89/686/CEE do Conselho (JO L 81 de 31.3.2016, p. 51);

10. Regulamento (UE) 2016/426 do Parlamento Europeu e do Conselho, de 9 de março de 2016, relativo aos aparelhos a gás e que revoga a Diretiva 2009/142/CE (JO L 81 de 31.3.2016, p. 99);

11. 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);

12. 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).

Secção B – Lista de outra legislação de harmonização da União

13. 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);

14. 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);

15. 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);

16. 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);

17. 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);

18. 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);

19. 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) n.º 2015/166 da Comissão (JO L 325 de 16.12.2019, p. 1);

20. 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), no que se refere ao projeto, fabrico e colocação no mercado de aeronaves a que se refere o artigo 2.º, n.º 1, alíneas a) e b), na parte relativa a aeronaves não tripuladas e aos seus motores, hélices, peças e equipamento de controlo remoto.

ANEXO II

Lista das infrações penais a que se refere o artigo 5.º, n.º 1,
primeiro parágrafo, alínea h), subalínea iii)

Infrações penais a que se refere o artigo 5.º, n.º 1, primeiro parágrafo, alínea h), subalínea iii):

– Terrorismo;

– Tráfico de seres humanos;

– Exploração sexual de crianças e pornografia infantil;

– Tráfico de estupefacientes e substâncias psicotrópicas;

– Tráfico de armas, munições ou explosivos;

– Homicídio, ofensas corporais graves;

– Tráfico de órgãos ou tecidos humanos;

– Tráfico de materiais nucleares ou radioativos;

– Rapto, sequestro ou tomada de reféns;

– Crimes abrangidos pela jurisdição do Tribunal Penal Internacional;

– Desvio de aviões ou navios;

– Violação;

– Criminalidade ambiental;

– Roubo organizado ou à mão armada;

– Sabotagem;

– Participação numa organização criminosa envolvida numa ou mais das infrações acima enumeradas.

ANEXO III

Sistemas de IA de risco elevado a que se refere o artigo 6.º, n.º 2

Os sistemas de IA de risco elevado a que se refere o artigo 6.º, n.º 2, são os sistemas de IA incluídos num dos domínios a seguir enumerados:

1. Dados biométricos, na medida em que a sua utilização seja permitida ao abrigo do direito da União ou do direito nacional aplicável:

   a) Sistemas de identificação biométrica à distância.

      Não inclui os sistemas de IA concebidos para serem utilizados para verificação biométrica com o único propósito de confirmar que uma determinada pessoa singular é a pessoa que alega ser;

   b) Sistemas de IA concebidos para serem utilizados para categorização biométrica, de acordo com atributos ou características sensíveis ou protegidos com base na inferência desses atributos ou características;

   c) Sistemas de IA concebidos para serem utilizados para o reconhecimento de emoções.

2. Infraestruturas críticas: sistemas de IA concebidos para serem utilizados como componentes de segurança na gestão e no controlo de infraestruturas digitais críticas, do trânsito rodoviário ou das redes de abastecimento de água, gás, aquecimento ou eletricidade.

3. Educação e formação profissional:

   a) Sistemas de IA concebidos para serem utilizados para determinar o acesso ou a admissão ou a afetação de pessoas singulares a instituições de ensino e de formação profissional de todos os níveis;

   b) Sistemas de IA concebidos para serem utilizados para avaliar os resultados da aprendizagem, nomeadamente quando esses resultados são utilizados para orientar o processo de aprendizagem de pessoas singulares em instituições de ensino e de formação profissional de todos os níveis;

   c) Sistemas de IA concebidos para serem utilizados para efeitos de avaliação do nível de educação adequado que as pessoas receberão ou a que poderão ter acesso no contexto de instituições de ensino e formação profissional ou nessas instituições de todos os níveis;

   d) Sistemas de IA concebidos para serem utilizados para efeitos de controlo e deteção de práticas proibidas por parte de estudantes durante testes no contexto de instituições de ensino e formação profissional ou nessas instituições de todos os níveis.

4. Emprego, gestão de trabalhadores e acesso ao emprego por conta própria:

   a) Sistemas de IA concebidos para serem utilizados no recrutamento ou na seleção de pessoas singulares, nomeadamente para colocar anúncios de emprego direcionados, analisar e filtrar candidaturas a ofertas de emprego e avaliar os candidatos;

b) Sistemas de IA concebidos para serem utilizados na tomada de decisões que afetem os termos das relações de trabalho, a promoção ou a cessação das relações contratuais de trabalho, na atribuição de tarefas com base em comportamentos individuais, traços ou características pessoais, ou no controlo e avaliação do desempenho e da conduta de pessoas que são partes nessas relações.

5. Acesso a serviços privados essenciais e a serviços e prestações públicos essenciais, bem como o usufruto dos mesmos:

a) Sistemas de IA concebidos para serem utilizados por autoridades públicas, ou em seu nome, para avaliar a elegibilidade de pessoas singulares para terem acesso a prestações e serviços de assistência pública essenciais, incluindo serviços de cuidados de saúde, bem como para conceder, reduzir, revogar ou recuperar o acesso a tais prestações e serviços;

b) Sistemas de IA concebidos para serem utilizados para avaliar a capacidade de solvabilidade de pessoas singulares ou estabelecer a sua classificação de crédito, com exceção dos sistemas de IA utilizados para efeitos de deteção de fraude financeira;

c) Sistemas de IA concebidos para serem utilizados nas avaliações de risco e na fixação de preços em relação a pessoas singulares no caso de seguros de vida e de saúde;

d) Sistemas de IA concebidos para avaliar e classificar chamadas de emergência efetuadas por pessoas singulares ou para serem utilizados no envio, ou no estabelecimento de prioridades no envio, de serviços de primeira resposta a emergências, incluindo polícia, bombeiros e assistência médica, bem como sistemas de triagem de pacientes dos sistemas de cuidados de saúde de emergência.

6. Aplicação da lei, na medida em que a sua utilização seja permitida nos termos do direito da União ou do direito nacional aplicável:

a) Sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei, ou em seu nome, ou por instituições, órgãos ou organismos da União em apoio das autoridades responsáveis pela aplicação da lei, ou em seu nome, para avaliar o risco de uma pessoa singular vir a ser vítima de infrações penais;

b) Sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei, ou em seu nome, ou por instituições, órgãos ou organismos da União em apoio das autoridades responsáveis pela aplicação da lei, como polígrafos ou instrumentos semelhantes;

c) Sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei, ou em seu nome, ou por instituições, órgãos ou organismos da União em apoio das autoridades responsáveis pela aplicação da lei para avaliar a fiabilidade dos elementos de prova no decurso da investigação ou ação penal relativas a infrações penais;

d) Sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei, ou em seu nome, ou por instituições, órgãos ou organismos da União em apoio das autoridades responsáveis pela aplicação da lei para avaliar o risco de uma pessoa singular cometer uma infração penal ou reincidir não exclusivamente com base na definição de perfis de pessoas singulares na aceção do artigo 3.º, ponto 4, da Diretiva (UE) 2016/680, ou para avaliar os traços e características da personalidade ou o comportamento criminal passado de pessoas singulares ou grupos;

e) Sistemas de IA concebidos para serem utilizados por autoridades responsáveis pela aplicação da lei, ou em seu nome, ou por instituições, órgãos ou organismos da União em apoio das autoridades responsáveis pela aplicação da lei para definir o perfil de pessoas singulares na aceção do artigo 3.º, ponto 4, da Diretiva (UE) 2016/680, no decurso da deteção, investigação ou ação penal relativas a infrações penais.

7. Gestão da migração, do asilo e do controlo das fronteiras, na medida em que a sua utilização seja permitida nos termos do direito da União ou do direito nacional aplicável:

a) Sistemas de IA concebidos para serem utilizados por autoridades públicas competentes ou instituições, órgãos ou organismos da União, ou em seu nome, como polígrafos e instrumentos semelhantes;

b) Sistemas de IA concebidos para serem utilizados por autoridades públicas competentes, ou em seu nome, ou por instituições, órgãos ou organismos da União para avaliar os riscos, incluindo um risco para a segurança, um risco de migração irregular ou um risco para a saúde, que uma pessoa singular que pretenda entrar ou tenha entrado no território de um Estado-Membro represente;

c) Sistemas de IA concebidos para serem utilizados por autoridades públicas competentes, ou em seu nome, ou por instituições, órgãos ou organismos da União para auxiliar as autoridades públicas competentes na análise de pedidos de asilo, de visto e de autorização de residência e das queixas conexas, no que toca à elegibilidade das pessoas singulares que requerem determinado estatuto, nomeadamente nas avaliações conexas da fiabilidade dos elementos de prova;

d) Sistemas de IA concebidos para serem utilizados por autoridades públicas competentes ou por instituições, órgãos ou organismos da União, ou em seu nome, no contexto da gestão da migração, do asilo ou do controlo das fronteiras, para efeitos de deteção, reconhecimento ou identificação de pessoas singulares, com exceção da verificação de documentos de viagem.

8. Administração da justiça e processos democráticos:

a) Sistemas de IA concebidos para serem utilizados por uma autoridade judiciária, ou em seu nome, para auxiliar uma autoridade judiciária na investigação e na interpretação de factos e do direito, bem como na aplicação da lei a um conjunto específico de factos, ou para serem utilizados de forma similar na resolução alternativa de litígios;

b) Sistemas de IA concebidos para serem utilizados para influenciar o resultado de uma eleição ou referendo ou o comportamento eleitoral de pessoas singulares no exercício do seu direito de voto em eleições ou referendos. Não estão incluídos os sistemas de IA a cujos resultados as pessoas singulares não estejam diretamente expostas, como as ferramentas utilizadas para organizar, otimizar e estruturar campanhas políticas do ponto de vista administrativo e logístico.

ANEXO IV

Documentação técnica a que se refere o artigo 11.º, n.º 1

A documentação técnica a que se refere o artigo 11.º, n.º 1, deve conter, pelo menos, as informações indicadas a seguir, consoante aplicável ao sistema de IA em causa:

1. Uma descrição geral do sistema de IA, incluindo:

   a) A sua finalidade prevista, o nome do prestador e a versão do sistema que reflete a sua relação com versões anteriores;

   b) A forma como o sistema de IA interage ou pode ser utilizado para interagir com hardware ou software, inclusive com outros sistemas de IA, que não faça parte do próprio sistema de IA, se aplicável;

   c) As versões do *software* ou *firmware* pertinente e todos os requisitos relacionados com a atualização das versões;

   d) A descrição de todas as formas sob as quais o sistema de IA é colocado no mercado ou colocado em serviço, tais como pacotes de software integrados em hardware, descarregamentos ou interfaces de programação de aplicações;

   e) A descrição do hardware no qual se pretende executar o sistema de IA;

   f) Se o sistema de IA for uma componente de produtos, fotografias ou ilustrações que mostrem características externas, a marcação e a disposição interna desses produtos;

g) Uma descrição básica da interface de utilizador facultada ao responsável pela implantação;

h) Instruções de utilização destinadas ao responsável pela implantação e uma descrição básica da interface de utilizador facultada ao responsável pela implantação, se aplicável;

2. Uma descrição pormenorizada dos elementos do sistema de IA e do respetivo processo de desenvolvimento, incluindo:

a) Os métodos utilizados e os passos dados com vista ao desenvolvimento do sistema de IA, incluindo, se for caso disso, o recurso a sistemas ou ferramentas previamente treinados disponibilizados por terceiros e a forma como estes foram utilizados, integrados ou modificados pelo prestador;

b) As especificações de conceção do sistema, a saber, a lógica geral do sistema de IA e dos algoritmos; as principais opções de conceção, nomeadamente a lógica subjacente e os pressupostos utilizados, também no respeitante às pessoas ou grupos de pessoas em que o sistema se destina a ser utilizado; as principais opções de classificação; o que se pretende otimizar com o sistema e a importância dos diferentes parâmetros; a descrição dos resultados esperados e a qualidade dos resultados do sistema; as decisões acerca de eventuais concessões no tocante às soluções técnicas adotadas para cumprir os requisitos definidos no capítulo III, secção 2;

c) A descrição da arquitetura do sistema, explicando de que forma os componentes de software se utilizam ou se alimentam mutuamente e como se integram no processamento global; os recursos computacionais utilizados para desenvolver, treinar, testar e validar o sistema de IA;

d) Se for caso disso, os requisitos de dados em termos de folhas de dados que descrevam as metodologias e técnicas de treino e os conjuntos de dados de treino utilizados, incluindo uma descrição geral desses conjuntos de dados, informações sobre a sua proveniência, o seu âmbito e as suas principais características; a forma como os dados foram obtidos e selecionados; procedimentos de rotulagem (p. ex., para aprendizagem supervisionada), metodologias de limpeza de dados (por ex., deteção de valores atípicos);

e) Análise das medidas de supervisão humana necessárias em conformidade com o artigo 14.º, incluindo uma análise das soluções técnicas necessárias para facilitar a interpretação dos resultados dos sistemas de IA pelos responsáveis pela implantação, em conformidade com o artigo 13.º, n.º 3, alínea d);

f) Se aplicável, uma descrição pormenorizada das alterações predeterminadas do sistema de IA e do seu desempenho, juntamente com todas as informações pertinentes relacionadas com as soluções técnicas adotadas para assegurar a conformidade contínua do sistema de IA com os requisitos aplicáveis estabelecidos no capítulo III, secção 2;

g) Os procedimentos de validação e testagem aplicados, incluindo informações sobre os dados de validação e de teste utilizados e as principais características desses dados; os parâmetros utilizados para aferir a exatidão, a solidez e a conformidade com outros requisitos aplicáveis estabelecidos no capítulo III, secção 2, bem como potenciais impactos discriminatórios; registos dos testes e todos os relatórios de teste datados e assinados pelas pessoas responsáveis, inclusive no respeitante às alterações predeterminadas a que se refere a alínea f);

h) As medidas de cibersegurança adotadas;

3. Informações pormenorizadas sobre o acompanhamento, o funcionamento e o controlo do sistema de IA, especialmente no que diz respeito: às suas capacidades e limitações de desempenho, incluindo os níveis de exatidão no tocante a pessoas ou grupos de pessoas específicos em que o sistema se destina a ser utilizado e o nível geral esperado de exatidão em relação à finalidade prevista; aos resultados não pretendidos mas previsíveis e às fontes de riscos para a saúde e a segurança, os direitos fundamentais e a proteção contra a discriminação atendendo à finalidade prevista do sistema de IA; às medidas de supervisão humana necessárias em conformidade com o artigo 14.º, incluindo as soluções técnicas adotadas para facilitar a interpretação dos resultados dos sistemas de IA pelos responsáveis pela implantação; às especificações relativas aos dados de entrada, consoante apropriado;

4. Uma descrição da adequação dos parâmetros de desempenho destinada ao sistema de IA específico;

5. Uma descrição pormenorizada do sistema de gestão de riscos em conformidade com o artigo 9.º;

6. A descrição das alterações pertinentes introduzidas pelo prestador no sistema ao longo do seu ciclo de vida;

7. Uma lista das normas harmonizadas aplicadas total ou parcialmente, cujas referências tenham sido publicadas no *Jornal Oficial da União Europeia*; caso não tenham sido aplicadas tais normas harmonizadas, uma descrição pormenorizada das soluções adotadas para cumprir os requisitos estabelecidos no capítulo III, secção 2, incluindo uma lista das outras normas e especificações técnicas aplicáveis que tenham sido aplicadas;

8. Uma cópia da declaração UE de conformidade referida no artigo 47.º;

9. Uma descrição pormenorizada do sistema existente para avaliar o desempenho do sistema de IA na fase de pós-comercialização em conformidade com o artigo 72.º, incluindo o plano de acompanhamento pós-comercialização a que se refere o artigo 72.º, n.º 3.

ANEXO V

Declaração UE de conformidade

A declaração UE de conformidade a que se refere o artigo 47.º deve conter todas as seguintes informações:

1. Nome e tipo do sistema de IA e quaisquer outras referências inequívocas que permitam identificar e rastrear o sistema de IA;

2. Nome e endereço do prestador ou, se aplicável, do mandatário;

3. Menção de que a declaração UE de conformidade, referida no artigo 47.º, é emitida sob a exclusiva responsabilidade do prestador;

4. Menção que ateste que o sistema de IA é conforme com o presente regulamento e, se for caso disso, outras disposições pertinentes do direito da União que prevejam a emissão da declaração UE de conformidade referida no artigo 47.º;

5. Sempre que um sistema de IA implique o tratamento de dados pessoais, uma menção de que esse sistema de IA cumpre o disposto nos Regulamentos (UE) 2016/679 e (UE) 2018/1725 e na Diretiva (UE) 2016/680;

6. Referências a todas as normas harmonizadas pertinentes utilizadas ou a outras especificações comuns em relação às quais é declarada a conformidade;

7. Se aplicável, nome e número de identificação do organismo notificado, descrição do procedimento de avaliação da conformidade adotado e identificação do certificado emitido;

8. Local e data de emissão da declaração, nome e cargo da pessoa que assina, bem como indicação da pessoa em nome de quem se assina, e assinatura.

ANEXO VI

Procedimento de avaliação da conformidade baseado no controlo interno

1. O procedimento de avaliação da conformidade baseado no controlo interno é o descrito nos pontos 2, 3 e 4.

2. O prestador verifica se o sistema de gestão da qualidade aplicado se encontra em conformidade com os requisitos do artigo 17.º.

3. O prestador analisa as informações contidas na documentação técnica para determinar a conformidade do sistema de IA com os requisitos essenciais aplicáveis estabelecidos no capítulo III, secção 2.

4. O prestador também verifica se o processo de conceção e desenvolvimento do sistema de IA e do seu acompanhamento pós-comercialização a que se refere o artigo 72.º estão de acordo com a documentação técnica.

ANEXO VII

Conformidade baseada numa avaliação do sistema de gestão da qualidade
e numa avaliação da documentação técnica

1. Introdução

A conformidade baseada numa avaliação do sistema de gestão da qualidade e numa avaliação da documentação técnica é o procedimento de avaliação da conformidade descrito nos pontos 2 a 5.

2. Generalidades

O sistema de gestão da qualidade aprovado para efeitos de conceção, desenvolvimento e testagem de sistemas de IA nos termos do artigo 17.º é analisado em conformidade com o ponto 3 e está sujeito à fiscalização especificada no ponto 5. A documentação técnica do sistema de IA é analisada em conformidade com o ponto 4.

3. Sistema de gestão da qualidade

3.1. O pedido do prestador inclui:

a) O nome e o endereço do prestador e, se for apresentado por um mandatário, também o nome e o endereço deste último;

b) A lista dos sistemas de IA abrangidos pelo mesmo sistema de gestão da qualidade;

c) A documentação técnica de cada sistema de IA abrangido pelo mesmo sistema de gestão da qualidade;

d) A documentação relativa ao sistema de gestão da qualidade, que deve abranger todos os aspetos enunciados no artigo 17.º;

e) Uma descrição dos procedimentos em vigor para assegurar a adequação e eficácia do sistema de gestão da qualidade;

f) Uma declaração escrita em como o mesmo pedido não foi apresentado a nenhum outro organismo notificado.

3.2. O sistema de gestão da qualidade é avaliado pelo organismo notificado, que determina se esse sistema cumpre os requisitos a que se refere o artigo 17.º.

A decisão é notificada ao prestador ou ao seu mandatário.

A notificação inclui as conclusões da avaliação do sistema de gestão da qualidade e a decisão de avaliação fundamentada.

3.3. O prestador deve continuar a aplicar e a manter o sistema de gestão da qualidade aprovado de maneira que este permaneça adequado e eficiente.

3.4. O prestador deve comunicar ao organismo notificado qualquer alteração planeada do sistema de gestão da qualidade aprovado ou da lista de sistemas de IA abrangidos por este último.

As alterações propostas são analisadas pelo organismo notificado, a quem cabe decidir se o sistema de gestão da qualidade alterado continua a satisfazer os requisitos enunciados no ponto 3.2 ou se será necessário proceder a nova avaliação.

O organismo notificado notifica o prestador da sua decisão. A notificação inclui as conclusões da análise das alterações e a decisão de avaliação fundamentada.

4. Controlo da documentação técnica

4.1. Além do pedido a que se refere o ponto 3, o prestador deve apresentar junto de um organismo notificado da sua escolha um pedido de avaliação da documentação técnica relativa ao sistema de IA que o prestador tenciona colocar no mercado ou colocar em serviço e que seja abrangido pelo sistema de gestão da qualidade a que se refere o ponto 3.

4.2. O pedido deve incluir:

a) O nome e o endereço do prestador;

b) Uma declaração escrita em como o mesmo pedido não foi apresentado a nenhum outro organismo notificado;

c) A documentação técnica referida no anexo IV.

4.3. O organismo notificado deve analisar a documentação técnica. Sempre que pertinente, e dentro dos limites do necessário para o desempenho das suas funções, deve ser concedido ao organismo notificado total acesso aos conjuntos de dados de treino, validação e teste utilizados, inclusive, se for caso disso e sob reserva de salvaguardas de segurança, através de IPA ou outros meios e ferramentas técnicas pertinentes que possibilitem o acesso remoto.

4.4. Ao analisar a documentação técnica, o organismo notificado pode exigir que o prestador apresente mais provas ou realize mais testes a fim de permitir uma adequada avaliação da conformidade do sistema de IA com os requisitos estabelecidos no capítulo III, secção 2. Se os testes realizados pelo prestador não satisfizerem o organismo notificado, deve o próprio organismo notificado realizar diretamente os testes adequados que sejam necessários.

4.5. Sempre que necessário para avaliar a conformidade do sistema de IA de risco elevado com os requisitos estabelecidos no capítulo III, secção 2, depois de todas as outras formas razoáveis de verificação da conformidade terem sido esgotadas ou se revelarem insuficientes, e mediante pedido fundamentado, deve também ser concedido ao organismo notificado o acesso aos modelos de treino e treinados do sistema de IA, incluindo os seus parâmetros pertinentes. Esse acesso está sujeito à legislação da União em vigor em matéria de proteção da propriedade intelectual e dos segredos comerciais.

4.6. A decisão do organismo notificado é notificada ao prestador ou ao seu mandatário. A notificação deve incluir as conclusões da avaliação da documentação técnica e a decisão de avaliação fundamentada.

Se o sistema de IA estiver em conformidade com os requisitos estabelecidos no capítulo III, secção 2, o organismo notificado deve emitir um certificado da União de avaliação da documentação técnica. Esse certificado deve indicar o nome e o endereço do prestador, as conclusões do exame, as (eventuais) condições da sua validade e os dados necessários à identificação do sistema de IA.

O certificado e os seus anexos devem conter todas as informações necessárias para permitir a avaliação da conformidade do sistema de IA e o controlo do sistema de IA durante a utilização, se aplicável.

Se o sistema de IA não estiver em conformidade com os requisitos estabelecidos no capítulo III, secção 2, o organismo notificado deve recusar a emissão de um certificado da União de avaliação da documentação técnica e informar o requerente desse facto, fundamentando pormenorizadamente os motivos da sua recusa.

Se o sistema de IA não cumprir o requisito relativo aos dados utilizados para o treinar, será necessário voltar a treinar o sistema de IA antes da apresentação de um pedido de nova avaliação da conformidade. Nesse caso, a decisão de avaliação fundamentada pela qual o organismo notificado recusa a emissão do certificado da União de avaliação da documentação técnica deve incluir considerações específicas sobre a qualidade dos dados utilizados para treinar o sistema de IA, nomeadamente as razões da não conformidade.

4.7. Todas as alterações do sistema de IA que possam afetar a conformidade do sistema de IA com os requisitos ou com a finalidade prevista devem ser examinadas pelo organismo notificado que emitiu o certificado da União de avaliação da documentação técnica. O prestador informa o referido organismo notificado se tencionar introduzir alterações como as supramencionadas ou se, de algum outro modo, tiver conhecimento da ocorrência dessas alterações. As alterações previstas são examinadas pelo organismo notificado, a quem cabe decidir se essas alterações tornam necessária uma nova avaliação da conformidade nos termos do artigo 43.º, n.º 4, ou se a situação pode ser resolvida com um aditamento ao certificado da União de avaliação da documentação técnica. Neste último caso, o organismo notificado examina as alterações, notifica o prestador da sua decisão e, se as alterações forem aprovadas, emite ao prestador um aditamento ao certificado da União de avaliação da documentação técnica.

5. Fiscalização do sistema de gestão da qualidade aprovado

5.1. O objetivo da fiscalização realizada pelo organismo notificado a que se refere o ponto 3 é garantir que o prestador cumpre devidamente os termos e as condições do sistema de gestão da qualidade aprovado.

5.2. Para efeitos de avaliação, o prestador deve autorizar o organismo notificado a aceder às instalações onde decorre a conceção, o desenvolvimento e a testagem dos sistemas de IA. O prestador deve igualmente partilhar com o organismo notificado todas as informações necessárias.

5.3. O organismo notificado efetua auditorias periódicas para se certificar de que o prestador mantém e aplica o sistema de gestão da qualidade e faculta ao prestador um relatório de auditoria. No contexto das referidas auditorias, o organismo notificado pode realizar testes adicionais aos sistemas de IA em relação aos quais foi emitido um certificado da União de avaliação da documentação técnica.

ANEXO VIII

Informações a apresentar aquando do registo
de sistemas de IA de risco elevado em conformidade com o artigo 49.º

Secção A – Informações a apresentar pelos prestadores de sistemas de IA de risco elevado em conformidade com o artigo 49.º, n.º 1

As informações a seguir indicadas devem ser fornecidas e, subsequentemente, mantidas atualizadas no respeitante a sistemas de IA de risco elevado a registar em conformidade com o artigo 49.º, n.º 1:

1. Nome, endereço e dados de contacto do prestador;

2. Se as informações forem apresentadas por outra pessoa em nome do prestador, nome, endereço e contactos dessa pessoa;

3. Nome, endereço e contactos do mandatário, se aplicável;

4. Designação comercial do sistema de IA e quaisquer outras referências inequívocas que permitam identificar e rastrear o sistema de IA;

5. Descrição da finalidade prevista do sistema de IA e dos componentes e funções apoiados através deste sistema de IA;

6. Uma descrição básica e concisa das informações utilizadas pelo sistema (dados, entradas) e a sua lógica de funcionamento;

7. Estado do sistema de IA (no mercado ou em serviço; já não se encontra no mercado/em serviço; retirado);

8. Tipo, número e data de validade do certificado emitido pelo organismo notificado e o nome ou número de identificação desse organismo notificado, se aplicável;

9. Uma cópia digitalizada do certificado a que se refere o ponto 8, se aplicável;

10. Todos os Estados-Membros em que o sistema de IA foi colocado no mercado, foi colocado em serviço ou disponibilizado na União;

11. Uma cópia da declaração UE de conformidade a que se refere o artigo 47.º;

12. Instruções de utilização em formato eletrónico; esta informação não é fornecida no que respeita a sistemas de IA de risco elevado nos domínios da aplicação da lei ou da gestão da migração, do asilo e do controlo das fronteiras, referidos no anexo III, pontos 1, 6 e 7;

13. Endereço URL para informações adicionais (opcional).

Secção B – Informações a apresentar pelos prestadores de sistemas de IA de risco elevado nos termos do artigo 49.º, n.º 2

As informações a seguir indicadas devem ser fornecidas e, subsequentemente, mantidas atualizadas no respeitante a sistemas de IA a registar em conformidade com o artigo 49.º, n.º 2:

1. Nome, endereço e dados de contacto do prestador;

2. Se as informações forem apresentadas por outra pessoa em nome do prestador, nome, endereço e contactos dessa pessoa;

3. Nome, endereço e contactos do mandatário, se aplicável;

4. Designação comercial do sistema de IA e quaisquer outras referências inequívocas que permitam identificar e rastrear o sistema de IA;

5. Descrição da finalidade prevista do sistema de IA;

6. A condição ou condições no âmbito do artigo 6.º, n.º 3, com base nas quais o sistema de IA é considerado como não sendo de risco elevado;

7. Breve síntese dos motivos com base nos quais o sistema de IA é considerado como não sendo de risco elevado na aplicação do procedimento previsto no artigo 6.º, n.º 3;

8. Estado do sistema de IA (no mercado ou em serviço; já não se encontra no mercado/em serviço; retirado);

9. Todos os Estados-Membros em que o sistema de IA foi colocado no mercado ou colocado em serviço ou disponibilizado na União.

Secção C – Informações a apresentar pelos responsáveis pela implantação de sistemas de IA de risco elevado em conformidade com o artigo 49.º, n.º 3

As informações a seguir indicadas devem ser fornecidas e, subsequentemente, mantidas atualizadas no respeitante a sistemas de IA de risco elevado a registar em conformidade com o artigo 49.º:

1. Nome, endereço e dados de contacto do responsável pela implantação;

2. Nome, endereço e dados de contacto da pessoa que apresenta informações em nome do responsável pela implantação;

3. O URL da entrada do sistema de IA na base de dados da UE pelo seu prestador;

4. Uma síntese das conclusões da avaliação do impacto sobre os direitos fundamentais realizada nos termos do artigo 27;

5. Uma síntese da avaliação do impacto sobre a proteção de dados realizada em conformidade com o artigo 35.º do Regulamento (UE) 2016/679 ou com o artigo 27.º da Diretiva (UE) 2016/680, conforme especificado no artigo 26.º, n.º 8, do presente regulamento, se aplicável.

ANEXO IX

Informações a apresentar aquando do registo dos sistemas de IA de risco elevado enumerados no anexo III em relação à testagem em condições reais em conformidade com o artigo 60.º.

As informações a seguir indicadas devem ser prestadas e, subsequentemente, mantidas atualizadas no respeitante à testagem em condições reais a efetuar em conformidade com o artigo 60.º:

1. Número único de identificação a nível da União da testagem em condições reais;

2. Nome e contactos do prestador ou potencial prestador e dos responsáveis pela implantação envolvidos na testagem em condições reais;

3. Uma breve descrição do sistema de IA, da sua finalidade prevista e outras informações necessárias para a identificação do sistema;

4. Um resumo das principais características do plano de testagem em condições reais;

5. Informações sobre a suspensão ou cessação da testagem em condições reais.

ANEXO X

Atos legislativos da União relativos a sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça

1. Sistema de Informação de Schengen

a) Regulamento (UE) 2018/1860 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo à utilização do Sistema de Informação de Schengen para efeitos de regresso dos nacionais de países terceiros em situação irregular (JO L 312 de 7.12.2018, p. 1).

b) Regulamento (UE) 2018/1861 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio dos controlos de fronteira, e que altera a Convenção de Aplicação do Acordo de Schengen e altera e revoga o Regulamento (CE) n.º 1987/2006 (JO L 312 de 7.12.2018, p. 14).

c) Regulamento (UE) 2018/1862 do Parlamento Europeu e do Conselho, de 28 de novembro de 2018, relativo ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen (SIS) no domínio da cooperação policial e da cooperação judiciária em matéria penal, e que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1986/2006 do Parlamento Europeu e do Conselho e a Decisão 2010/261/UE da Comissão (JO L 312 de 7.12.2018, p. 56).

2. Sistema de Informação sobre Vistos

a) Regulamento (UE) 2021/1133 do Parlamento Europeu e do Conselho, de 7 de julho de 2021, que altera os Regulamentos (UE) n.º 603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 e (UE) 2019/818 no que respeita ao estabelecimento das condições de acesso a outros sistemas de informação da UE para efeitos do Sistema de Informação sobre Vistos (JO L 248 de 13.7.2021, p. 1).

b) Regulamento (UE) 2021/1134 do Parlamento Europeu e do Conselho, de 7 de julho de 2021, que altera os Regulamentos (CE) n.º 767/2008, (CE) n.º 810/2009, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1860, (UE) 2018/1861, (UE) 2019/817 e (UE) 2019/1896 do Parlamento Europeu e do Conselho e que revoga as Decisões 2004/512/CE e 2008/633/JAI do Conselho, para efeitos de reforma do Sistema de Informação sobre Vistos (JO L 248 de 13.7.2021, p. 11).

3. Eurodac

Regulamento (UE) 2024/... do Parlamento Europeu e do Conselho relativo à criação do sistema «Eurodac» de comparação de dados biométricos para efeitos da aplicação efetiva dos Regulamentos (UE) 2024/... e (UE) 2024/... do Parlamento Europeu e do Conselho e da Diretiva 2001/55/CE do Conselho, para identificação de nacionais de países terceiros e apátridas em situação irregular, e de pedidos de comparação com os dados Eurodac apresentados pelas autoridades responsáveis dos Estados-Membros e pela Europol para fins de aplicação da lei, que altera os Regulamentos (UE) 2018/1240 e (UE) 2019/818 do Parlamento Europeu e do Conselho e revoga o Regulamento (UE) n.º 603/2013 do Parlamento Europeu e do Conselho[+].

4. Sistema de Entrada/Saída

Regulamento (UE) 2017/2226 do Parlamento Europeu e do Conselho, de 30 de novembro de 2017, que estabelece o Sistema de Entrada/Saída (SES) para registo dos dados das entradas e saídas e dos dados das recusas de entrada dos nacionais de países terceiros aquando da passagem das fronteiras externas dos Estados-Membros, que determina as condições de acesso ao SES para efeitos de aplicação da lei, e que altera a Convenção de Aplicação do Acordo de Schengen e os Regulamentos (CE) n.º 767/2008 e (UE) n.º 1077/2011 (JO L 327 de 9.12.2017, p. 20).

[+] JO: Inserir no texto o número do regulamento que consta do documento PE-CONS 15/24 (2016/0132(COD)) e inserir na nota de rodapé o número, a data, o título e a referência do JO desse regulamento.

5. Sistema Europeu de Informação e Autorização de Viagem

a) Regulamento (UE) 2018/1240 do Parlamento Europeu e do Conselho, de 12 de setembro de 2018, que cria um Sistema Europeu de Informação e Autorização de Viagem (ETIAS) e altera os Regulamentos (UE) n.º 1077/2011, (UE) n.º 515/2014, (UE) 2016/399, (UE) 2016/1624 e (UE) 2017/2226 (JO L 236 de 19.9.2018, p. 1).

b) Regulamento (UE) 2018/1241 do Parlamento Europeu e do Conselho, de 12 de setembro de 2018, que altera o Regulamento (UE) 2016/794 para efeitos da criação de um Sistema Europeu de Informação e Autorização de Viagem (ETIAS) (JO L 236 de 19.9.2018, p. 72).

6. Sistema Europeu de Informação sobre Registos Criminais de nacionais de países terceiros e de apátridas

Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que cria um sistema centralizado para a determinação dos Estados-Membros que possuem informações sobre condenações de nacionais de países terceiros e de apátridas (ECRIS-TCN) tendo em vista completar o Sistema Europeu de Informação sobre Registos Criminais e que altera o Regulamento (UE) 2018/1726 (JO L 135 de 22.5.2019, p. 1).

7. Interoperabilidade

a) Regulamento (UE) 2019/817 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho, e as Decisões 2004/512/CE e 2008/633/JAI do Conselho (JO L 135 de 22.5.2019, p. 27).

b) Regulamento (UE) 2019/818 do Parlamento Europeu e do Conselho, de 20 de maio de 2019, relativo à criação de um regime de interoperabilidade entre os sistemas de informação da UE no domínio da cooperação policial e judiciária, asilo e migração, e que altera os Regulamentos (UE) 2018/1726, (UE) 2018/1862 e (UE) 2019/816 (JO L 135 de 22.5.2019, p. 85).

ANEXO XI

Documentação técnica a que se refere o artigo 53.º, n.º 1, alínea a) – documentação técnica para os prestadores de modelos de IA de finalidade geral

Secção 1

Informações a apresentar por todos os prestadores de modelos de IA de finalidade geral

A documentação técnica a que se refere o artigo 53.º, n.º 1, alínea a), deve conter, pelo menos, as informações indicadas a seguir, consoante aplicável à dimensão e ao perfil de risco do modelo:

1. Uma descrição geral do modelo de IA de finalidade geral, incluindo:

   a) As tarefas que o modelo se destina a desempenhar e o tipo e a natureza dos sistemas de IA em que pode ser integrado;

   b) As políticas de utilização aceitáveis aplicáveis;

   c) A data de lançamento e os métodos de distribuição;

   d) A arquitetura e o número de parâmetros;

   e) A modalidade (p. ex.: texto, imagem) e formato das entradas e saídas;

   f) A licença.

2. Uma descrição pormenorizada dos elementos do modelo a que se refere o ponto 1, e as informações pertinentes sobre o processo de desenvolvimento, incluindo os seguintes elementos:

a) Os meios técnicos (p. ex., instruções de utilização, infraestruturas, ferramentas) necessários para que o modelo de IA de finalidade geral seja integrado nos sistemas de IA;

b) As especificações de conceção do modelo e do processo de treino, incluindo as metodologias e técnicas de treino, as principais opções de conceção, incluindo a fundamentação e os pressupostos assumidos; o que se pretende otimizar com o modelo e a importância dos diferentes parâmetros, se aplicável;

c) Informações sobre os dados utilizados para treino, testagem e validação, se aplicável, incluindo o tipo e a proveniência dos dados e as metodologias de curadoria (p. ex., limpeza, filtragem, etc.), o número de pontos de dados, o seu âmbito e as principais características; a forma como os dados foram obtidos e selecionados, bem como todas as outras medidas para detetar a inadequação das fontes de dados e dos métodos para detetar enviesamentos identificáveis, se aplicável;

d) Os recursos computacionais utilizados para treinar o modelo (p. ex., o número de operações de vírgula flutuante), o tempo de treino e outros dados pertinentes relacionados com a formação;

e) O consumo de energia conhecido ou estimado do modelo.

No que diz respeito à alínea e), se o consumo de energia do modelo for desconhecido, o consumo de energia pode basear-se em informações sobre os recursos computacionais utilizados.

Secção 2

Informações adicionais a prestar

pelos prestadores de modelos de IA de finalidade geral com risco sistémico

1. Uma descrição pormenorizada das estratégias de avaliação, incluindo os resultados da avaliação, com base nos protocolos e ferramentas de avaliação públicos disponíveis ou noutras metodologias de avaliação. As estratégias de avaliação devem incluir critérios de avaliação, parâmetros e a metodologia de identificação de limitações.

2. Se aplicável, uma descrição pormenorizada das medidas adotadas para efeitos de realização de testagens antagónicas internas e/ou externas (p. ex., simulação de ataques), adaptações do modelo, incluindo alinhamento e ajustes.

3. Se aplicável, uma descrição pormenorizada da arquitetura do sistema, explicando de que forma os componentes de software se utilizam ou se alimentam mutuamente e como se integram no processamento global.

ANEXO XII

Informações em matéria de transparência a que se refere o artigo 53.º, n.º 1, alínea b) – documentação técnica para os prestadores de modelos de IA de finalidade geral destinada aos prestadores a jusante que integrem o modelo no seu sistema de IA

As informações a que se refere o artigo 53.º, n.º 1, alínea b) devem incluir, pelo menos, o seguinte:

1. Uma descrição geral do modelo de IA de finalidade geral, incluindo:

   a) As tarefas que o modelo se destina a desempenhar e o tipo e a natureza dos sistemas de IA em que pode ser integrado;

   b) As políticas de utilização aceitáveis aplicáveis;

   c) A data de lançamento e os métodos de distribuição;

   d) De que forma o modelo interage ou pode ser utilizado para interagir com hardware ou software que não faça parte do próprio modelo, quando aplicável;

   e) As versões do software pertinente relacionadas com a utilização do modelo de IA de finalidade geral, se aplicável;

   f) A arquitetura e o número de parâmetros;

   g) A modalidade (p. ex.: texto, imagem) e o formato das entradas e saídas;

   h) A licença para o modelo.

2. Uma descrição dos elementos do modelo e do respetivo processo de desenvolvimento, incluindo:

a) Os meios técnicos (p. ex., instruções de utilização, infraestruturas, ferramentas) necessários para que o modelo de IA de finalidade geral seja integrado nos sistemas de IA;

b) A modalidade (p. ex.: texto, imagem, etc.) e o formato das entradas e saídas e a sua dimensão máxima (p. ex., comprimento da janela de contexto, etc.);

c) Informações sobre os dados utilizados para o treino, a testagem e a validação, se aplicável, incluindo o tipo e a proveniência dos dados e as metodologias de curadoria.

ANEXO XIII

Critérios para a designação de modelos de IA de finalidade geral
com risco sistémico a que se refere o artigo 51.º

A fim de determinar que um modelo de IA de finalidade geral tem capacidades ou um impacto equivalentes aos previstos no artigo 51.º, n.º 1, alínea a), a Comissão deve ter em conta os seguintes critérios:

a) O número de parâmetros do modelo;

b) A qualidade ou dimensão do conjunto de dados, por exemplo, medida através de *tokens*;

c) A quantidade de cálculo utilizada para o treino do modelo, medida em operações de vírgula flutuante ou indicada por uma combinação de outras variáveis, como o custo estimado do treino, o tempo estimado necessário para o treino ou o consumo estimado de energia para o treino;

d) As modalidades de entrada e de saída do modelo, tais como texto para texto (grandes modelos linguísticos), texto para imagem, multimodalidade e limiares de ponta para determinar as capacidades de elevado impacto para cada modalidade, bem como o tipo específico de entradas e saídas (p. ex., sequências biológicas);

e) Os parâmetros de referência e avaliações das capacidades do modelo, nomeadamente tendo em conta o número de tarefas sem treino adicional, a adaptabilidade à aprendizagem de tarefas novas e distintas, o seu nível de autonomia e escalabilidade e as ferramentas a que tem acesso;

f) Se tem um elevado impacto no mercado interno devido ao seu alcance, o que se presume quando tiver sido disponibilizado a, pelo menos, 10 000 utilizadores empresariais registados estabelecidos na União;

g) O número de utilizadores finais registados.