2024/1689

12.7.2024

REGULAMENTO (UE) 2024/1689 DO PARLAMENTO EUROPEU E DO CONSELHO

13 de junho de 2024

que estabelece regras harmonizadas sobre inteligência artificial e altera o Regulamento (CE) n.º$_{qualquer}$300/2008, (UE) n.º$_{qualquer}$167/2013, (UE) n.º$_{qualquer}$168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828
(Regulamento de Inteligência Artificial)

(Texto relevante para o 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 a transmissão do projecto de acto 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),

De acordo com o processo legislativo ordinário (4),

Considerando o seguinte:

(1) O objetivo do presente regulamento é melhorar o funcionamento do mercado interno, estabelecendo um quadro jurídico uniforme, em especial 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 inteligência artificial (IA) centrada no ser humano e fiável, assegurando simultaneamente um elevado nível de proteção da saúde, da segurança e dos direitos fundamentais consagrados na Carta dos Direitos Fundamentais da União Europeia («a Carta»), incluindo a democracia, o Estado de direito e a proteção do ambiente, protegendo contra os efeitos nocivos dos sistemas de IA na União, bem como apoiando a inovação. O presente regulamento garante a livre circulação transfronteiriça de bens e serviços baseados em IA, impedindo assim os Estados-Membros de imporem restrições ao desenvolvimento, à comercialização e à utilização de sistemas de IA, salvo se expressamente autorizado pelo presente Regulamento.

(2) Este regulamento deve ser implementado de acordo com os valores da União consagrados na Carta, facilitando a proteção das pessoas singulares, das empresas, da democracia, do Estado de direito e da proteção ambiental, ao mesmo tempo que impulsiona a inovação e o emprego e torna a União líder na adoção de IA fiável.

(3) Os sistemas de IA podem ser facilmente implantados em uma ampla gama de setores da economia e em muitas partes da sociedade, inclusive além-fronteiras, e podem circular facilmente por toda a União. Alguns Estados-Membros já consideraram adotar regras nacionais para garantir que a IA seja confiável e segura e seja desenvolvida e utilizada em conformidade com as obrigações de direitos fundamentais. Regras nacionais divergentes podem levar à fragmentação do mercado interno e reduzir a segurança jurídica para operadores que desenvolvem, importam ou usam sistemas de IA. Por conseguinte, é necessário garantir um nível elevado e consistente de proteção em toda a União, a fim de alcançar uma IA fiável, bem como evitar divergências que dificultem a livre circulação, a inovação, a implementação e a adoção no mercado interno de sistemas de IA e

(1) DO C 517 de 22.12.2021, p. 56. (2) DO C 115 de 11.3.2022, p. 5. (3) DO 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 21 de maio de 2024.

produtos e serviços relacionados, estabelecendo obrigações uniformes para os operadores e garantindo a proteção uniforme dos objetivos primordiais de interesse geral e dos direitos dos indivíduos em todo o mercado interno, com base no artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE). Na medida em que o presente regulamento contém regras específicas para a proteção de indivíduos em relação ao tratamento de dados pessoais que restringem a utilização de sistemas de IA para identificação biométrica remota para fins de aplicação da lei, a utilização de sistemas de IA para realizar avaliações de risco de pessoas singulares para fins de aplicação da lei e a utilização de sistemas de IA para categorização biométrica para fins de aplicação da lei, é adequado basear o presente regulamento, no que diz respeito a essas regras específicas, no artigo 16.º do TFUE. À luz destas regras específicas e do recurso ao artigo 16.º do TFUE, é adequado consultar o Comité Europeu para a Proteção de Dados.

(4) IA é um conjunto de tecnologias em rápida evolução que contribui para gerar benefícios econômicos, ambientais e sociais muito diversos em todos os setores econômicos e atividades sociais. O uso da IA pode fornecer vantagens competitivas essenciais às empresas e facilitar a obtenção de resultados sociais e ambientais positivos nas áreas de saúde, agricultura, segurança alimentar, educação e treinamento, mídia, esporte, cultura, gestão de infraestrutura, energia, transporte e logística, serviços públicos, segurança, justiça, eficiência energética e de recursos, monitoramento ambiental, conservação e restauração da biodiversidade e ecossistemas, e mitigação e adaptação às mudanças climáticas, entre outros, melhorando a previsão, otimizando operações e alocação de recursos e personalizando soluções digitais disponíveis ao público e às organizações.

(5) Ao mesmo tempo, dependendo das circunstâncias relacionadas com a sua aplicação específica, utilização e nível de desenvolvimento tecnológico, a IA pode criar riscos e prejudicar os interesses públicos e os direitos fundamentais protegidos pelo direito da União. Esses danos podem ser tangíveis ou intangíveis e incluem danos físicos, psicológicos, sociais ou econômicos.

(6) Dado o impacto significativo que a IA pode ter na sociedade e a necessidade de criar confiança, é É essencial que a IA e o seu quadro regulamentar sejam desenvolvidos de acordo com os valores da União consagrados no artigo 2.º do Tratado da União Europeia (TUE), os direitos e liberdades fundamentais consagrados nos Tratados e, em conformidade com o artigo 6.º do TUE, na Carta. Como pré-requisito, a IA deve ser uma tecnologia centrada no ser humano. Além disso, deve ser uma ferramenta para as pessoas e ter como objetivo final aumentar o bem-estar humano.

(7) Devem ser estabelecidas regras comuns para sistemas de IA de alto risco, a fim de garantir um nível alto e consistente de proteção dos interesses públicos no que diz respeito à saúde, segurança e direitos fundamentais. Essas regras devem ser consistentes com a Carta, não discriminatórias e alinhadas com os compromissos comerciais internacionais da União. Eles também devem levar em consideração a Declaração Europeia sobre Direitos Digitais e Princípios para a Década Digital e as Diretrizes Éticas para uma IA Confiável do Grupo Independente de Peritos de Alto Nível sobre Inteligência Artificial.

(8) Consequentemente, é necessário um quadro jurídico da UE que estabeleça regras de IA harmonizadas para promover o desenvolvimento, a utilização e a adoção de IA no mercado interno, ao mesmo tempo que proporciona um elevado nível de proteção dos interesses públicos, como a saúde e a segurança, e a proteção dos direitos fundamentais, incluindo a democracia, o Estado de direito e a proteção ambiental, reconhecidos e protegidos pela legislação da UE. Para atingir este objetivo, é adequado estabelecer regras que regulem a colocação no mercado, a colocação em funcionamento e a utilização de determinados sistemas de IA, o que garantirá o bom funcionamento do mercado interno e permitirá que tais sistemas beneficiem do princípio da livre circulação de bens e serviços. Essas regras devem ser claras e fortes na proteção dos direitos fundamentais, apoiando novas soluções inovadoras, permitindo um ecossistema europeu de atores públicos e privados que criem sistemas de IA alinhados aos valores da UE e liberando o potencial da transformação digital em todas as regiões da UE. Ao estabelecer tais regras, bem como medidas de apoio à inovação com especial enfoque nas pequenas e médias empresas (PME), incluindo as start-ups, o presente regulamento apoia o objetivo de promover a abordagem europeia centrada no ser humano à IA e de ser líder mundial no desenvolvimento de IA segura, fiável e ética, tal como indicado pelo Conselho Europeu ([5]), e assegura a protecção dos princípios éticos, tal como especificamente solicitado pelo Parlamento Europeu ([6]).

([5]) Conselho Europeu, Reunião extraordinária do Conselho Europeu (1-2 de outubro de 2020) – Conclusões, EUCO 13/20, 2020, p. 6.
([6]) Resolução do Parlamento Europeu de 20 de outubro de 2020 com recomendações à Comissão sobre um quadro para os aspetos éticos da inteligência artificial, da robótica e das tecnologias conexas [2020/2012(INL)].

(9) Devem ser estabelecidas regras harmonizadas para a colocação no mercado, a entrada em serviço e a utilização de sistemas de IA de alto risco, em conformidade com o Regulamento (CE) n.º 1999/2003.qualquer765/2008 do Parlamento Europeu e do Conselho (7), Decisão n.ºqualquer768/2008/CE do Parlamento Europeu e do Conselho (8) e o Regulamento (UE) 2019/1020 do Parlamento Europeu e do Conselho (9) (a seguir designado por «novo quadro legislativo»). As regras harmonizadas estabelecidas no presente regulamento devem ser aplicadas a todos os setores e, em consonância com o novo quadro legislativo, não devem prejudicar a legislação da União em vigor, em especial em matéria de proteção de dados, proteção do consumidor, direitos fundamentais, emprego, proteção dos trabalhadores e segurança dos produtos, que é complementada pelo presente regulamento. Consequentemente, todos os direitos e recursos concedidos pela legislação da UE aos consumidores e outras pessoas que possam ser negativamente afetadas pelos sistemas de IA permanecem inalterados e continuam a ser plenamente aplicáveis, incluindo no que diz respeito à reparação de quaisquer danos nos termos da Diretiva 85/374/CEE do Conselho (10). 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 ou o direito laboral nacional – em conformidade com o direito da União – relativo ao emprego e às condições de trabalho, incluindo a saúde e a segurança no trabalho e a relação entre empregadores e empregados. O presente regulamento também não deverá afetar de forma alguma o exercício dos direitos fundamentais reconhecidos nos Estados-Membros e a nível da União, incluindo o direito ou a liberdade de greve ou de tomar outras medidas previstas nos sistemas específicos de relações laborais dos Estados-Membros e o direito de negociar, celebrar e aplicar acordos coletivos ou de levar a cabo ações coletivas em conformidade com a legislação nacional. O presente regulamento não deverá afetar as disposições destinadas a melhorar as condições de trabalho no trabalho em plataformas digitais estabelecidas numa Diretiva do Parlamento Europeu e do Conselho relativa à melhoria das condições de trabalho no trabalho em plataformas digitais. Além disso, o presente regulamento visa reforçar a eficácia dos direitos e recursos 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 ao abrigo do presente regulamento deverão aplicar-se sem prejuízo da legislação nacional que, em conformidade com o direito da União, tenha o efeito de limitar a utilização de determinados sistemas de IA quando essa legislação não se enquadra no âmbito do presente regulamento ou prossiga objetivos legítimos de interesse público diferentes dos prosseguidos pelo presente regulamento. Por exemplo, este Regulamento não deve afetar a legislação laboral nacional nem a legislação relativa à proteção de menores, ou seja, pessoas com menos de dezoito anos, que têm em conta o Comentário Geral n.º 1.qualquer25 (2021) da Convenção das Nações Unidas sobre os Direitos da Criança sobre os direitos da criança em relação ao ambiente digital, na medida em que não sejam específicos dos sistemas de IA e persigam outros objetivos legítimos de interesse público.

(10) O direito fundamental à protecção de dados pessoais é garantido, nomeadamente, pelo Regulamento (UE) 2016/679 (11) e (UE) 2018/1725 (12) do Parlamento Europeu e do Conselho e a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho (13). Além disso, a Directiva 2002/58/CE do Parlamento Europeu e do Conselho (14) protege a privacidade e a confidencialidade das comunicações, estabelecendo também condições para qualquer armazenamento de dados pessoais e não pessoais em equipamentos terminais, e acesso a partir deles. Esses atos legislativos da União formam a base para o processamento de dados sustentável e responsável, inclusive quando os conjuntos de dados contêm uma mistura de dados pessoais e não pessoais. O presente regulamento não prejudica a aplicação da legislação da União em vigor que rege o tratamento de dados pessoais, incluindo as funções e os poderes das autoridades de controlo independentes competentes para monitorizar o cumprimento desses instrumentos. Também não afeta as obrigações dos provedores e dos responsáveis pela implantação de sistemas de IA em sua função de controladores ou processadores de dados.

(7) Regulamento (CE) n.ºqualquer765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e revoga o Regulamento (CEE) n.º 146/2008.qualquer339/93 (JO L 218 de 13.8.2008, p. 30).

(8) Decisão n.ºqualquer768/2008/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 do Conselho (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 1020/2009 e (CE) n.º 1020/2009/CE.qualquer765/2008 e (UE) n.qualquer 305/2011 (JO L 169 de 25.6.2019, p. 1).

(10) Directiva 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 por danos causados por produtos defeituosos (JO L 210 de 7.8.1985, p. 29).

(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, pelos órgãos e organismos da União e à livre circulação desses dados e que revoga o Regulamento (CE) n.º 1725/2018.qualquer45/2001 e Decisão n.ºqualquer1247/2002/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 (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 setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37).

decorrentes da legislação da União ou nacional relativa à proteção de dados pessoais, na medida em que a conceção, o desenvolvimento ou a utilização de sistemas de IA envolvam o tratamento de dados pessoais. Deve também ser esclarecido que os titulares dos dados continuam a usufruir de todos os direitos e garantias que lhes são conferidos pela referida Lei da União, incluindo direitos relacionados com decisões individuais totalmente automatizadas, como a definição de perfis. As regras harmonizadas para a colocação no mercado, a colocação em funcionamento e a utilização de sistemas de IA estabelecidas ao abrigo do presente regulamento deverão facilitar a implementação eficaz e permitir o exercício de direitos e outras vias de recurso dos titulares de dados garantidos pela legislação da União relativa à proteção de dados pessoais, bem como outros direitos fundamentais.

(11) O presente regulamento deverá ser interpretado sem prejuízo das disposições do Regulamento (UE) 2022/2065 do Parlamento Europeu e do Conselho ([15]) relativas à responsabilidade dos prestadores de serviços intermediários.

(12) O conceito de "sistema de IA" deve ser claramente definido no presente regulamento e estreitamente alinhado com o trabalho das organizações internacionais que lidam com IA, a fim de garantir a segurança jurídica e facilitar a convergência internacional e a ampla aceitação, ao mesmo tempo que proporciona a flexibilidade necessária para acomodar os rápidos desenvolvimentos tecnológicos neste domínio. Além disso, a definição deve ser baseada nas principais características dos sistemas de IA que os distinguem dos sistemas de computador.Programasou abordagens de programação tradicionais e mais simples, e não devem incluir sistemas baseados em regras definidas exclusivamente por pessoas físicas para executar operações automaticamente. Uma característica fundamental dos sistemas de IA são suas capacidades de inferência. Essa capacidade de inferência se refere ao processo de obtenção de resultados de saída, como previsões, conteúdo, recomendações ou decisões, que podem influenciar ambientes físicos e virtuais, e à capacidade dos sistemas de IA de deduzir modelos ou algoritmos, ou ambos, a partir de informações ou dados de entrada. Técnicas que permitem inferência ao construir um sistema de IA incluem estratégias de aprendizado de máquina que aprendem com dados como atingir determinados objetivos e estratégias baseadas em lógica e conhecimento que inferem a partir de conhecimento codificado ou de uma representação simbólica da tarefa a ser resolvida. A capacidade de inferência de um sistema de IA transcende o processamento básico de dados, permitindo aprendizado, raciocínio ou modelagem. O termo “baseado em máquina” se refere ao fato de que sistemas de IA rodam em máquinas. A referência a objetivos explícitos ou implícitos sublinha que sistemas de IA podem operar de acordo com objetivos definidos explícitos ou objetivos implícitos. Os objetivos do sistema de IA podem ser diferentes da finalidade pretendida do sistema de IA em um contexto específico. Para efeitos do presente regulamento, os ambientes devem ser entendidos como os contextos em que os sistemas de IA operam, enquanto os resultados de saída gerados pelo sistema de IA refletem as diferentes funções desempenhadas pelos sistemas de IA e incluem previsões, conteúdos, recomendações ou decisões. Os sistemas de IA são projetados para operar com vários níveis de autonomia, o que significa que eles podem agir com algum grau de independência da intervenção humana e têm algumas capacidades de operar sem intervenção humana. A capacidade adaptativa que um sistema de IA pode exibir após a implantação refere-se às capacidades de autoaprendizagem que permitem que o sistema mude durante o uso. Os sistemas de IA podem ser usados de forma independente ou como componentes de um produto, independentemente de o sistema fazer parte fisicamente do produto (incorporado) ou contribuir para a funcionalidade do produto sem fazer parte dele (não incorporado).

(13) O conceito de "controlador de implantação", conforme referido no presente regulamento, deve ser interpretado como qualquer pessoa singular ou coletiva, incluindo qualquer autoridade, organismo, gabinete ou agência pública, que utilize um sistema de IA sob sua própria autoridade, exceto quando sua utilização ocorrer no contexto de uma atividade pessoal e não profissional. Dependendo do tipo de sistema de IA, o uso do sistema pode afetar pessoas diferentes da pessoa responsável por implantá-lo.

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

(15) O conceito de «identificação biométrica» a que se refere o presente regulamento deverá ser definido como o reconhecimento automatizado de características físicas, fisiológicas ou comportamentais de uma pessoa, como rosto, movimento dos olhos, formato do corpo, voz, entonação, marcha, postura, frequência cardíaca, pressão arterial, odor ou características de digitação, a fim de determinar a identidade de um indivíduo comparando seus dados biométricos com dados biométricos de indivíduos armazenados em um banco de dados de referência, independentemente de o indivíduo ter dado consentimento ou não. Estão excluídos os sistemas de IA destinados à verificação biométrica, o que inclui autenticação, cujo único propósito é confirmar que uma pessoa física específica é quem ela afirma ser, bem como a identidade de uma pessoa física com o único propósito de conceder-lhe acesso a um serviço, desbloquear um dispositivo ou ter acesso seguro a um local.

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

(16) O conceito de «categorização biométrica» referido no presente regulamento deverá ser definido como a inclusão de pessoas singulares em categorias específicas com base nos seus dados biométricos. Essas categorias específicas podem se referir a aspectos como sexo, idade, cor do cabelo, cor dos olhos, tatuagens, traços comportamentais ou de personalidade, idioma, religião, filiação a uma minoria nacional ou orientação sexual ou política. Isto não inclui sistemas de categorização biométrica que sejam um recurso puramente acessório intrinsecamente vinculado a outro serviço comercial, o que significa que o recurso não pode, por razões técnicas objetivas, ser usado sem o serviço principal e que a integração de tal recurso ou funcionalidade não é um meio de contornar a aplicabilidade das regras deste regulamento. Por exemplo, filtros que classificam características faciais ou corporais usados em mercados online podem constituir um recurso acessório, pois só podem ser usados em conexão com o serviço principal, que é vender um produto permitindo que o consumidor visualize como ele ficaria nele e o ajude a tomar uma decisão de compra. Filtros usados em serviços de redes sociais que classificam características faciais ou corporais para que os usuários possam adicionar ou modificar imagens ou vídeos também podem ser considerados um recurso acessório, já que tais filtros não podem ser usados sem o serviço principal da rede social, que é o compartilhamento de conteúdo online.

(17) O conceito de «sistema de identificação biométrica remota», tal como referido no presente regulamento, deverá ser definido funcionalmente como um sistema de IA destinado a identificar pessoas singulares sem a sua participação ativa, normalmente de forma remota, através da comparação dos seus dados biométricos com os de uma base de dados de referência, independentemente da tecnologia, dos processos ou dos tipos de dados biométricos específicos utilizados. Esses sistemas remotos de identificação biométrica são frequentemente usados para detectar várias pessoas ou seu comportamento simultaneamente, a fim de simplificar consideravelmente a identificação de pessoas sem sua participação ativa. Estão excluídos os sistemas de IA destinados à verificação biométrica, o que inclui autenticação, cujo único propósito é confirmar que uma pessoa física específica é quem ela afirma ser, bem como a identidade de uma pessoa física com o único propósito de conceder-lhe acesso a um serviço, desbloquear um dispositivo ou ter acesso seguro a um local. Essa exclusão é justificada pelo fato de que tais sistemas provavelmente terão um impacto menor nos direitos fundamentais das pessoas físicas do que os sistemas de identificação biométrica remota que podem ser usados para processar os dados biométricos de um grande número de pessoas sem sua participação ativa. No caso de sistemas “em tempo real”, a coleta de dados biométricos, a comparação e a identificação ocorrem de forma instantânea, quase instantânea ou, em qualquer caso, sem atrasos significativos. Neste sentido, não deverá existir qualquer possibilidade de contornar as regras estabelecidas no presente regulamento relativamente à utilização “em tempo real” dos sistemas de IA em causa, gerando atrasos mínimos. Os sistemas "em tempo real" envolvem o uso de materiais "ao vivo" ou "quase ao vivo", como gravações de vídeo, gerados por uma câmera ou outro dispositivo com funções semelhantes. Em contraste, em sistemas "atrasados", os dados biométricos já foram coletados e a comparação e a identificação ocorrem com um atraso significativo. Para tanto, são utilizados materiais como imagens ou gravações de vídeo captadas por câmeras de circuito fechado de televisão ou dispositivos particulares, geradas antes da utilização do sistema em relação aos indivíduos afetados.

(18) O conceito de «sistema de reconhecimento de emoções», tal como referido no presente regulamento, deve ser definido como um sistema de IA destinado a distinguir ou inferir as emoções ou intenções de pessoas singulares a partir dos seus dados biométricos. O conceito se refere a emoções ou intenções como felicidade, tristeza, indignação, surpresa, desgosto, constrangimento, entusiasmo, vergonha, desprezo, satisfação e diversão. Não inclui estados físicos como dor ou fadiga, como, por exemplo, os sistemas usados para detectar fadiga em pilotos ou motoristas profissionais para evitar acidentes. Também não inclui a mera detecção de expressões, gestos ou movimentos que sejam óbvios, a menos que sejam usados para distinguir ou deduzir emoções. Essas expressões podem ser expressões faciais básicas, como uma carranca ou um sorriso; gestos como movimentos das mãos, braços ou cabeça, ou características da voz de uma pessoa, como uma voz elevada ou um sussurro.

(19) Para efeitos do presente regulamento, o conceito de «espaço acessível ao público» deverá ser entendido como referindo-se a qualquer espaço físico que possa ser acedido por um número indeterminado de pessoas singulares, independentemente de ser de propriedade privada ou pública e independentemente da atividade para a qual o espaço possa ser utilizado, quer se trate de atividades comerciais, por exemplo, lojas, restaurantes, cafés; prestação de serviços, por exemplo, bancários, atividades profissionais, hotelaria; esportes, por exemplo, piscinas, academias, estádios; transporte, por exemplo, estações de ônibus, metrô e trem, aeroportos, meios de transporte; entretenimento, por exemplo, cinemas, teatros, museus, salas de concerto, salas de conferências; instalações recreativas ou de outro tipo, por exemplo, vias e praças públicas, parques, florestas, parques infantis. Da mesma forma, um espaço deve ser considerado de acesso público se, independentemente de eventuais restrições de capacidade ou de segurança, o acesso estiver sujeito a determinadas condições previamente definidas e que possam ser cumpridas por um número indeterminado de pessoas, como a aquisição de um bilhete ou de um título de transporte, a inscrição prévia ou a idade determinada. Pelo contrário, um espaço não deve ser considerado publicamente acessível se for acessível apenas a determinadas pessoas singulares definidas, seja em virtude de legislação da União ou nacional diretamente relacionada com a segurança pública, seja em virtude de uma manifestação clara da vontade da pessoa que exerce a autoridade.

relevantes para esse espaço. A possibilidade real de acesso, como uma porta destrancada ou um portão aberto, não significa por si só que o espaço seja publicamente acessível se houver indicações ou circunstâncias que sugiram o contrário, como placas proibindo ou restringindo o acesso. As instalações da empresa e da fábrica, bem como escritórios e locais de trabalho destinados ao acesso apenas de funcionários e prestadores de serviços relevantes, não são espaços de acesso público. Prisões e áreas onde são realizadas inspeções de fronteira não devem ser incluídas em áreas públicas. Alguns espaços podem incluir áreas de acesso público e áreas de acesso não público, como aeroportos ou o saguão de um edifício residencial privado que leva a um consultório médico. Espaços online não são lugares de acesso público, pois não são espaços físicos. No entanto, é preciso determinar caso a caso se um espaço é de acesso público ou não, levando em consideração as particularidades da situação específica.

(20) Para obter os maiores benefícios dos sistemas de IA, protegendo ao mesmo tempo os direitos
Para garantir que a alfabetização em IA seja um elemento essencial dos direitos humanos fundamentais, da saúde e da segurança, e para permitir o controle democrático, a alfabetização em IA deve equipar fornecedores, implantadores e indivíduos afetados com os conceitos necessários para tomar decisões informadas sobre sistemas de IA. Esses conceitos podem variar dependendo do contexto relevante e incluem uma compreensão da aplicação correta de elementos técnicos durante a fase de desenvolvimento do sistema de IA, as medidas a serem aplicadas durante seu uso, formas apropriadas de interpretar os resultados de saída do sistema de IA e, no caso de indivíduos afetados, o conhecimento necessário para entender como as decisões tomadas com a ajuda da IA terão impacto sobre eles. No contexto da implementação deste Regulamento, a literacia em IA deve fornecer a todos os intervenientes relevantes na cadeia de valor da IA o conhecimento necessário para garantir o cumprimento adequado e a implementação correta. Além disso, a implementação generalizada de medidas de literacia em IA e a introdução de ações de acompanhamento adequadas poderiam contribuir para melhorar as condições de trabalho e, em última análise, apoiar o caminho de consolidação e inovação de uma IA fiável na União. O Conselho Europeu de Inteligência Artificial (doravante designado por «Conselho da IA») deverá apoiar a Comissão na promoção de ferramentas de literacia em IA, na sensibilização do público e na compreensão dos benefícios, riscos, salvaguardas, direitos e obrigações relacionados com a utilização de sistemas de IA. Em cooperação com as partes interessadas relevantes, a Comissão e os Estados-Membros devem facilitar o desenvolvimento de códigos de conduta voluntários para promover a literacia em IA entre os envolvidos no desenvolvimento, operação e utilização da IA.

(21) A fim de garantir condições de concorrência equitativas e a proteção efetiva dos direitos e liberdades dos indivíduos em toda a União, as regras estabelecidas no presente regulamento devem aplicar-se aos fornecedores de sistemas de IA sem discriminação, independentemente de estarem estabelecidos na União ou num país terceiro, e aos responsáveis pela implementação de sistemas de IA estabelecidos na União.

(22) Devido à sua natureza digital, alguns sistemas de IA devem ser abrangidos pelo âmbito de aplicação do presente regulamento, mesmo que não sejam colocados no mercado, colocados em serviço ou utilizados na União. Isto acontece, por exemplo, quando um operador estabelecido na União assina um contrato com um operador estabelecido num país terceiro para a prestação de determinados serviços relacionados com uma atividade a ser realizada por um sistema de IA que seria considerada de alto risco. Nessas circunstâncias, o sistema de IA utilizado num país terceiro pelo operador poderia processar dados recolhidos legalmente na União e transferidos do seu território, e fornecer ao operador contratante localizado na União os resultados de saída gerados por esse sistema de IA como resultado desse processamento, sem que o sistema de IA em questão fosse colocado no mercado, colocado em serviço ou utilizado na União.
A fim de evitar a evasão do presente regulamento e garantir a proteção efetiva das pessoas singulares localizadas na União, o presente regulamento deverá também aplicar-se aos prestadores e aos controladores da implantação de sistemas de IA estabelecidos num país terceiro, na medida em que os resultados gerados por tais sistemas se destinem à utilização na União. No entanto, a fim de levar em conta os acordos existentes e as necessidades especiais de cooperação futura com parceiros estrangeiros com os quais são trocadas informações e provas, o presente regulamento não deverá aplicar-se às autoridades públicas de um país terceiro ou a organizações internacionais quando atuarem no âmbito de acordos internacionais ou de cooperação celebrados a nível nacional ou da União para efeitos de cooperação policial e judiciária com a União ou os seus Estados-Membros, se o país terceiro ou a organização internacional em causa oferecer garantias suficientes no que diz respeito à proteção dos direitos e liberdades fundamentais das pessoas. Quando apropriado, isso pode incluir as atividades de entidades às quais países terceiros confiaram tarefas específicas em apoio a essa cooperação policial e judiciária. Tais estruturas ou acordos de cooperação foram estabelecidos bilateralmente entre Estados-Membros e países terceiros ou entre a União Europeia, a Europol e outros organismos da União e países terceiros e organizações internacionais. As autoridades competentes para supervisionar a aplicação da lei e as autoridades judiciais ao abrigo do presente regulamento deverão avaliar se tais quadros de cooperação ou acordos internacionais incluem garantias suficientes no que diz respeito à proteção dos direitos e liberdades fundamentais dos indivíduos. As autoridades nacionais e as instituições, órgãos, gabinetes e agências da União que são destinatários desses resultados e que os utilizam dentro da União continuam a ser responsáveis por garantir que a sua utilização da informação é efetuada de forma atempada.

as informações estão em conformidade com o direito da União. Quando, no futuro, tais acordos internacionais forem revistos ou novos forem celebrados, as partes contratantes deverão envidar todos os esforços para garantir que tais acordos estejam em conformidade com os requisitos do presente regulamento.

(23) O presente regulamento deverá também aplicar-se às instituições, organismos, gabinetes e agências da União quando estes atuem como prestadores ou como responsáveis pela implementação 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 modificações, para fins militares, de defesa ou de segurança nacional, deverão ser excluídos do âmbito do presente regulamento, independentemente do tipo de entidade que realiza essas atividades, por exemplo, se é uma entidade pública ou privada. No que diz respeito a fins militares e de defesa, tal 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 política de defesa comum da União referidas no Título V, Capítulo 2, do TUE, que estão sujeitas ao direito internacional público, que constitui, portanto, o quadro jurídico mais adequado para a regulamentação dos sistemas de IA no contexto da utilização de força letal e de outros sistemas de IA no contexto de atividades militares e de defesa. No que diz respeito a fins de segurança nacional, a exclusão justifica-se tanto pelo facto de a segurança nacional continuar a ser da responsabilidade exclusiva dos Estados-Membros, em conformidade com o artigo 4.º, n.º 2, do TUE, como pela natureza específica e pelas necessidades operacionais das atividades de segurança nacional e pelas regras nacionais específicas aplicáveis a tais 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 fosse utilizado temporária ou permanentemente fora dessas áreas para outros fins (por exemplo, para fins civis ou humanitários, aplicação da lei ou segurança pública), esse sistema estaria abrangido pelo âmbito de aplicação do presente regulamento. Nesse caso, a entidade que utiliza o sistema de IA para fins que não sejam militares, de defesa ou de segurança nacional deve garantir que o sistema de IA cumpre o presente regulamento, a menos que o sistema já o faça. Sistemas de IA colocados no mercado ou em serviço para uma finalidade excluída, nomeadamente fins militares, de defesa ou de segurança nacional, e uma ou mais finalidades não excluídas, como fins civis ou de aplicação da lei, estão abrangidas pelo âmbito de aplicação do presente Regulamento e os fornecedores desses sistemas devem garantir o cumprimento do presente Regulamento. Nesses casos, o facto de um sistema de IA poder estar abrangido pelo âmbito de aplicação do presente regulamento não deverá afetar a possibilidade de entidades que realizam atividades militares, de defesa e de segurança nacional, independentemente do tipo de entidade que realiza essas atividades, utilizarem sistemas de IA para fins militares, de defesa e de segurança nacional, cuja utilização está 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) Este regulamento deve apoiar a inovação, respeitar a liberdade científica e não prejudicar a atividade de investigação e desenvolvimento. Portanto, é necessário excluir do seu escopo sistemas e modelos de IA especificamente desenvolvidos e colocados em serviço exclusivamente para fins de pesquisa e desenvolvimento científico. Além disso, é necessário garantir que o presente regulamento não afete de outra forma a investigação científica e o desenvolvimento de sistemas ou modelos de IA antes da sua colocação no mercado ou da sua entrada em serviço. No que diz respeito à atividade de investigação, ensaio e desenvolvimento orientada para produtos relacionados com sistemas ou modelos de IA, as disposições do presente regulamento também não deverão aplicar-se antes de tais sistemas e modelos serem colocados em serviço ou no mercado. Esta exclusão não prejudica a obrigação de cumprir o presente regulamento quando um sistema de IA abrangido pelo âmbito de aplicação do mesmo é colocado no mercado ou colocado em serviço em resultado dessa atividade de investigação e desenvolvimento, nem a aplicação de disposições relativas a ambientes de teste de IA controlados e a testes em condições reais. Além disso, sem prejuízo da exclusão de sistemas de IA especificamente desenvolvidos e colocados em serviço exclusivamente para fins de investigação e desenvolvimento científico, qualquer outro sistema de IA que possa ser utilizado para realizar qualquer atividade de investigação e desenvolvimento deverá continuar sujeito às disposições do presente regulamento. Em qualquer caso, todas as atividades de pesquisa e desenvolvimento devem ser realizadas de acordo com padrões éticos e profissionais reconhecidos para pesquisa científica e com a legislação aplicável da União.

(26) Para estabelecer um conjunto proporcional e eficaz de regras vinculativas para sistemas de IA, é necessária uma abordagem claramente definida e baseada em riscos, adaptando o tipo e o conteúdo das regras. a intensidade e o alcance dos riscos que os sistemas de IA em questão podem gerar. É, portanto, necessário proibir certas práticas inaceitáveis de IA, definir os requisitos a serem cumpridos pelos sistemas de IA de alto risco e as obrigações aplicáveis aos operadores relevantes, bem como impor obrigações de transparência a certos sistemas de IA.

(27) Embora a abordagem baseada no risco constitua a base para um conjunto de regras vinculativas proporcionais e eficazes, é É importante relembrar as Diretrizes Éticas para IA Confiável de 2019, desenvolvidas pelo Grupo Independente de Peritos de Alto Nível sobre IA estabelecido pela Comissão. Nessas diretrizes, o Grupo de Especialistas de Alto Nível em IA desenvolveu sete princípios éticos não vinculativos para IA que visam ajudar a garantir a confiabilidade e a base ética da IA. Os sete princípios são: ação e supervisão humana; solidez técnica e segurança; privacidade e gestão de 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 outro ato aplicável do direito da União, essas diretrizes contribuem para a concepção de uma IA coerente, confiável e centrada no ser humano, em consonância com a Carta e os valores em que a União se funda. De acordo com as diretrizes do Grupo de Peritos de Alto Nível sobre IA, "ação e supervisão humanas" significa que os sistemas de IA são desenvolvidos e usados como uma ferramenta a serviço das pessoas, que respeita a dignidade humana e a autonomia pessoal e que opera de uma forma que pode ser adequadamente controlada e monitorada por humanos. "Robustez e segurança técnicas" significa que os sistemas de IA são desenvolvidos e usados de uma forma que seja robusta a problemas e resiliente a tentativas de alterar o uso ou a operação do sistema de IA para permitir o uso ilegal por terceiros e minimizar danos não intencionais. "Privacidade e gerenciamento de dados" significa que os sistemas de IA são desenvolvidos e usados em conformidade com os padrões de privacidade e proteção de dados, ao mesmo tempo em que lidam com dados que atendem a padrões rigorosos em termos de qualidade e integridade. Transparência significa que os sistemas de IA são desenvolvidos e usados de uma forma que permite rastreabilidade e explicabilidade adequadas, ao mesmo tempo em que conscientiza as pessoas de que estão se comunicando ou interagindo com um sistema de IA e informa adequadamente os responsáveis pela implantação sobre as capacidades e limitações desse sistema de IA e os indivíduos afetados sobre seus direitos. 'Diversidade, não discriminação e justiça' significa que os sistemas de IA são desenvolvidos e utilizados de uma forma que inclui diversos intervenientes e promove a igualdade de acesso, a igualdade de género e a diversidade cultural, evitando simultaneamente efeitos discriminatórios e preconceitos injustos proibidos pela legislação da União ou nacional. "Bem-estar social e ambiental" significa que os sistemas de IA são desenvolvidos e utilizados de forma sustentável e amiga do ambiente, bem como para o benefício de todos os seres humanos,ao mesmo tempo em que monitora e avalia os efeitos de longo prazo nas pessoas, na sociedade e na democracia. A aplicação desses princípios deve ser traduzida, sempre que possível, no design e no uso de modelos de IA. Em qualquer caso, deverão servir de base para o desenvolvimento de códigos de conduta ao abrigo do presente regulamento. Todas as partes interessadas, incluindo a indústria, a academia, a sociedade civil e organizações de normalização, são incentivadas a considerar, conforme apropriado, princípios éticos para o desenvolvimento de padrões voluntários e melhores práticas.

(28) Além dos muitos usos benéficos da IA, ela também pode ser mal utilizada e fornecer novas ferramentas poderosas para manipulação, exploração e controle social. Tais práticas são extremamente prejudiciais e erradas e devem ser proibidas, pois vão contra os valores da União de respeito à dignidade humana, liberdade, igualdade, democracia e Estado de direito e os direitos fundamentais consagrados na Carta, como o direito à não discriminação, à proteção de dados e à privacidade e os direitos da criança.

(29) Técnicas de manipulação possibilitadas pela IA podem ser usadas para persuadir pessoas a se envolverem em comportamentos indesejáveis ou para induzi-las a tomar decisões de uma forma que enfraqueça e prejudique sua autonomia, tomada de decisão e capacidade de escolher livremente. Eles são particularmente perigosos e, portanto, a colocação no mercado, a colocação em serviço ou a utilização de determinados sistemas de IA com o objetivo ou a finalidade de alterar substancialmente o comportamento humano, com probabilidade de causar danos substanciais, em particular danos com efeitos adversos suficientemente significativos na saúde física ou mental ou nos interesses financeiros, deve ser proibida. Esses sistemas de IA usam componentes subliminares, como estímulos de áudio, imagem ou vídeo que os humanos não conseguem perceber (pois tais estímulos estão além da percepção humana) ou outras técnicas manipuladoras ou enganosas que prejudicam ou prejudicam a autonomia, a tomada de decisões ou a capacidade dos humanos de escolher livremente, de maneiras que os humanos não têm conhecimento dessas técnicas ou, quando têm conhecimento delas, ainda podem ser enganados ou incapazes de controlá-las ou resistir a elas. Isso poderia ser facilitado, por exemplo, por interfaces cérebro-máquina ou realidade virtual, uma vez que permitem um maior grau de controle sobre quais estímulos são apresentados às pessoas, a ponto de poderem alterar substancialmente seu comportamento de uma forma que cause danos consideráveis. Além disso, os sistemas de IA também podem explorar de outras formas as vulnerabilidades de uma pessoa ou de um grupo específico de pessoas decorrentes da sua idade, deficiência na aceção da Diretiva (UE) 2019/882 do Parlamento Europeu e do Conselho ([16]) ou uma situação social ou econômica específica que provavelmente aumentará sua vulnerabilidade à exploração, como viver em extrema pobreza ou pertencer a minorias étnicas ou religiosas. Esses sistemas de IA podem ser colocados no mercado, colocados em serviço ou usados com o objetivo ou o efeito de alterar substancialmente o comportamento de um indivíduo e de uma forma que cause, ou seja razoavelmente provável que cause, danos substanciais a esse indivíduo ou a outro indivíduo ou grupo de indivíduos, incluindo danos que podem se acumular ao longo do tempo, e, portanto, devem ser proibidos. Não se pode presumir que exista

([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).

a intenção de interromper o comportamento se a interrupção for resultado de fatores externos ao sistema de IA que estão além do controle do provedor ou implementador, ou seja, fatores que não são razoavelmente previsíveis e, portanto, não podem ser mitigados pelo provedor ou implementador do sistema de IA. Em qualquer caso, não é necessário que o provedor ou a pessoa responsável pela implantação tenha a intenção de causar danos consideráveis, desde que tais danos resultem de práticas manipuladoras ou exploradoras que a IA permite. A proibição de tais práticas de IA complementa as disposições da Diretiva 2005/29/CE do Parlamento Europeu e do Conselho (17), em especial a proibição, em quaisquer circunstâncias, de práticas comerciais desleais que causem danos económicos ou financeiros aos consumidores, quer sejam estabelecidas através de sistemas de IA ou de outra forma. A proibição de práticas manipuladoras e exploradoras estabelecida no presente Regulamento não deve afetar práticas lícitas no contexto de tratamento médico, como tratamento psicológico de doenças mentais ou reabilitação física, quando tais práticas forem realizadas de acordo com a legislação aplicável e as normas médicas, por exemplo, com o consentimento expresso das pessoas ou dos seus representantes legais. Da mesma forma, práticas comerciais comuns e legítimas (por exemplo, em publicidade) que estejam em conformidade com a lei aplicável não devem ser consideradas, por si só, práticas manipulativas prejudiciais permitidas pela IA.

(30) Os sistemas de categorização biométrica baseados em dados biométricos de pessoas singulares devem ser proibidos, como o rosto ou as impressões digitais de uma pessoa física, para deduzir ou inferir opiniões políticas, filiação sindical, crenças religiosas ou filosóficas, raça, vida sexual ou orientação sexual de uma pessoa física. Esta proibição não deve aplicar-se à rotulagem, filtragem ou categorização legal de conjuntos de dados biométricos adquiridos em conformidade com a legislação da União ou nacional com base em dados biométricos, como a classificação de imagens com base na cor do cabelo ou dos olhos, que podem ser utilizadas, por exemplo, no domínio da aplicação da lei.

(31) Sistemas de IA que permitem que agentes públicos ou privados realizem pontuação de cidadãos podem ter resultados discriminatórios e levar à exclusão de certos grupos. Eles podem comprometer o direito à dignidade e à não discriminação e os valores de igualdade e justiça. Esses sistemas de IA avaliam ou classificam indivíduos ou grupos de indivíduos com base em múltiplos pontos de dados relacionados ao seu comportamento social em múltiplos contextos ou em características pessoais ou de personalidade conhecidas, inferidas ou previstas ao longo de determinados períodos de tempo. A pontuação do cidadão resultante de tais sistemas de IA pode levar a um tratamento prejudicial ou desfavorável de certos indivíduos ou grupos inteiros em contextos sociais que não estão relacionados ao contexto em que os dados foram originalmente gerados ou coletados, ou a um tratamento prejudicial que seja desproporcional ou injustificado em relação à seriedade de seu comportamento social. Portanto, os sistemas de IA que se envolvem em tais práticas de pontuação inaceitáveis e resultam em resultados tão prejudiciais ou desfavoráveis devem ser banidos. Esta proibição não deverá afetar as práticas legais de avaliação de pessoas singulares realizadas para uma finalidade específica, em conformidade com o direito da União e o direito nacional.

(32) A utilização de sistemas de IA para identificação biométrica remota "em tempo real" de pessoas singulares em espaços públicos, com o objetivo de garantir o cumprimento da lei, infringe de forma particularmente grave os direitos e liberdades das pessoas em causa, uma vez que pode afetar a vida privada de uma grande parte da população, criar a sensação de estar sob vigilância constante e desencorajar indiretamente os cidadãos de exercerem a sua liberdade de reunião e outros direitos fundamentais. Imprecisões técnicas em sistemas de IA destinados à identificação biométrica remota de pessoas físicas podem levar a resultados tendenciosos e ter efeitos discriminatórios. Esses potenciais resultados tendenciosos e efeitos discriminatórios são particularmente relevantes em relação à idade, etnia, raça, sexo ou deficiência. Além disso, a imediatez das consequências e as oportunidades limitadas de verificações ou correções adicionais relacionadas ao uso de sistemas que operam em "tempo real" aumentam o risco que eles representam para os direitos e liberdades das pessoas afetadas por ou no contexto de atividades de aplicação da lei.

(33) Consequentemente, o uso de tais sistemas para fins de garantir o cumprimento da lei deve ser proibido. exceto em situações enumeradas de forma limitada e definidas com precisão, nas quais seu uso seja estritamente necessário para atingir um interesse público essencial cuja importância supere os riscos. Essas situações incluem a busca por vítimas específicas de um crime, incluindo pessoas desaparecidas; certas ameaças à vida ou à segurança física de pessoas singulares ou ameaças de ataques terroristas; e a localização ou identificação dos autores ou suspeitos das infrações enumeradas num anexo ao presente regulamento, sempre que tais infrações sejam puníveis no Estado-Membro em causa com uma pena ou uma multa.

(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 1017/2005.qualquer2006/2004 do Parlamento Europeu e do Conselho («Diretiva relativa às práticas comerciais desleais») (JO L 149 de 11.6.2005, p. 22).

medidas de segurança privativas de liberdade com uma duração máxima de pelo menos quatro anos, tal como definidas na legislação desse Estado-Membro. Estabelecer tal limite para uma pena de prisão ou medida de segurança sob a legislação nacional ajuda a garantir que o crime seja grave o suficiente para justificar o uso de sistemas remotos de identificação biométrica "em tempo real". Além disso, a lista de infracções constante do anexo ao presente regulamento baseia-se nas trinta e duas infracções enumeradas na Decisão-Quadro 2002/584/JAI do Conselho ([18]), embora deva ser notado que, na prática, alguns são provavelmente mais relevantes do que outros no sentido de que é previsível que o uso da identificação biométrica remota "em tempo real" possa ser necessário e proporcional em graus muito diferentes para localizar ou identificar os autores ou suspeitos das diferentes infrações listadas, e que é provável que haja diferenças na gravidade, probabilidade e magnitude do dano ou potenciais consequências negativas. Uma ameaça iminente à vida ou à segurança física de pessoas singulares também poderá surgir de uma perturbação grave de infraestruturas críticas, tal como definido no artigo 2.º, ponto 4, da Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho ([19]), quando a interrupção ou destruição de tais infraestruturas críticas representar uma ameaça iminente à vida ou à segurança física de uma pessoa, inclusive prejudicando gravemente o fornecimento de produtos básicos à população ou o exercício da função essencial do Estado. Além disso, o presente regulamento deverá preservar a capacidade das autoridades responsáveis pela aplicação da lei, pelo controlo de fronteiras, pela imigração ou pelo asilo de efetuarem controlos de identidade na presença da pessoa em causa, em conformidade com as condições estabelecidas na legislação da União e nacional para tais controlos. Em particular, as autoridades responsáveis pela aplicação da lei, pelo controlo de fronteiras, pela imigração ou pelo asilo deverão poder utilizar sistemas de informação, em conformidade com o direito da União ou nacional, para identificar pessoas que, durante um controlo de identidade, se recusem a ser identificadas ou não consigam declarar ou provar a sua identidade, sem que o presente regulamento exija a obtenção de autorização prévia. Pode ser, por exemplo, uma pessoa envolvida em um crime que não quer revelar sua identidade às autoridades policiais ou que não pode fazê-lo devido a um acidente ou a uma condição médica.

(34) A fim de garantir que tais sistemas sejam utilizados de forma responsável e proporcionada, é também importante prever que, nas situações enumeradas de forma limitada e precisamente definidas, sejam tidos em conta determinados elementos, nomeadamente no que diz respeito à natureza da situação que dá origem ao pedido, as consequências que seu uso pode ter sobre os direitos e liberdades de todas as pessoas envolvidas, e as garantias e condições que acompanham seu uso. Além disso, a utilização de sistemas remotos de identificação biométrica "em tempo real" em espaços de acesso público para fins de aplicação da lei deve ser realizada exclusivamente para confirmar a identidade da pessoa que é o alvo específico e deve ser limitada ao estritamente necessário em termos de período de tempo, bem como de âmbito geográfico e pessoal, levando em consideração, em particular, evidências ou indícios relativos a ameaças, vítimas ou perpetradores. O uso do sistema de identificação biométrica remota em tempo real em espaços de acesso público só deve ser autorizado se a autoridade policial competente tiver realizado uma avaliação de impacto sobre os direitos fundamentais e, salvo disposição em contrário do presente regulamento, tiver registrado o sistema no banco de dados estabelecido pelo presente regulamento. O banco de dados de pessoas de referência deve ser apropriado para cada caso de uso em cada uma das situações mencionadas acima.

(35) Qualquer utilização de um sistema de identificação biométrica remota “em tempo real” em espaços de acesso público para efeitos de garantia do cumprimento da lei deve ter sido expressa e especificamente autorizada por uma autoridade judicial ou uma autoridade administrativa independente de um Estado-Membro e cuja decisão seja vinculativa. Em princípio, tal autorização deve ser obtida antes de utilizar o sistema de IA para identificar uma ou mais pessoas. Deverão ser permitidas exceções a esta regra em situações devidamente justificadas por motivos de urgência, nomeadamente quando a necessidade de utilização dos sistemas em questão for tão imperiosa que seja efetiva e objetivamente impossível obter autorização antes de começar a utilizar o sistema de IA. Em tais situações de emergência, a utilização deve limitar-se ao mínimo necessário e satisfazer as garantias e condições adequadas, de acordo com as disposições da legislação nacional e conforme apropriado em cada caso específico de utilização urgente pela autoridade que garante o cumprimento da lei. Além disso, em tais situações, as autoridades responsáveis pela aplicação da lei devem solicitar tal autorização e expor as razões pelas quais não puderam fazê-lo antes, sem demora injustificada e, no máximo, no prazo de vinte e quatro horas. Se tal autorização for recusada, o uso de sistemas de identificação biométrica em tempo real vinculados à autorização deverá ser descontinuado com efeito imediato e todos os dados relacionados a tal uso deverão ser descartados e excluídos. Esses dados incluem dados de entrada adquiridos diretamente por um sistema de IA durante o uso desse sistema, bem como resultados e informações de saída desse uso vinculados a essa autorização. Não deve incluir informações de entrada legalmente adquiridas de acordo com outro ato de direito nacional ou da União. Em qualquer caso, não deverá ser tomada nenhuma decisão que produza efeitos

([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).

([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).

consequências legais adversas para uma pessoa apenas com base nos resultados do sistema de identificação biométrica remota.

(36) Para desempenhar as suas funções em conformidade com os requisitos estabelecidos no presente regulamento, bem como nas regras nacionais, cada utilização do sistema de identificação biométrica em tempo real deverá ser notificada à autoridade de fiscalização do mercado relevante e à autoridade nacional de proteção de dados. As autoridades de fiscalização do mercado e as autoridades nacionais de proteção de dados que tenham recebido uma notificação devem apresentar à Comissão um relatório anual sobre a utilização de sistemas de identificação biométrica em tempo real.

(37) Por outro lado, é conveniente prever, no âmbito do quadro abrangente estabelecido pelo presente regulamento, que essa utilização no território de um Estado-Membro, em conformidade com o presente regulamento, só deverá ser possível quando e na medida em que o Estado-Membro em causa tenha decidido prever expressamente a possibilidade de autorizar tal nas regras pormenorizadas da sua legislação nacional. Consequentemente, ao abrigo do presente regulamento, os Estados-Membros continuam a ser livres de não oferecer esta possibilidade de todo ou de a oferecer apenas em relação a algumas das finalidades que podem justificar uma utilização autorizada ao abrigo do presente regulamento. Essas regras nacionais devem ser notificadas à Comissão no prazo de trinta dias após sua adoção.

(38) A utilização de sistemas de IA para identificação biométrica remota em tempo real de pessoas singulares em espaços públicos com a finalidade de garantir o cumprimento da Lei implica necessariamente o tratamento de dados biométricos. As regras do presente regulamento que proíbem, com certas excepções, tal utilização, com base no artigo 16.º do TFUE, deverão aplicar-se na medida em quelex especialistano que diz respeito às regras relativas ao tratamento de dados biométricos estabelecidas no artigo 10.º da Diretiva (UE) 2016/680, que regula de forma abrangente essa utilização e o tratamento dos dados biométricos correspondentes. Por conseguinte, tal utilização e tratamento só deverão ser possíveis na medida em que sejam compatíveis com o quadro estabelecido pelo presente regulamento, sem deixar margem, fora desse quadro, para que as autoridades competentes, quando atuarem para fins de aplicação da lei, utilizem esses sistemas e tratem esses dados nos casos previstos no artigo 10.º da Diretiva (UE) 2016/680. A este respeito, o presente regulamento não se destina a fornecer a base jurídica para o tratamento de dados pessoais nos termos do artigo 8.º da Diretiva (UE) 2016/680. No entanto, a utilização de sistemas de identificação biométrica remota em tempo real em espaços de acesso público para fins que não sejam a aplicação da lei, incluindo por autoridades competentes, não deverá estar sujeita ao quadro específico estabelecido pelo presente regulamento no que diz respeito à utilização de tais sistemas para fins de aplicação da lei. Consequentemente, a sua utilização para fins que não sejam a garantia do cumprimento da lei não deverá estar sujeita à exigência de obtenção de uma autorização prevista no presente regulamento ou às regras de execução aplicáveis da legislação nacional que possam dar efeito a tal autorização.

(39) Qualquer tratamento de dados biométricos e outros dados pessoais associado à utilização de sistemas de IA para identificação biométrica, exceto o associado à utilização de sistemas remotos de identificação biométrica em tempo real em espaços de acesso público para efeitos de garantia do cumprimento da lei regulada pelo presente Regulamento, deve continuar a cumprir todos os requisitos decorrentes do artigo 10.º da Diretiva (UE) 2016/680. 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 para fins que não sejam a aplicação da lei, sujeito às exceções limitadas previstas nesses artigos. Na aplicação do artigo 9.º, n.º 1, do Regulamento (UE) 2016/679, a utilização da identificação biométrica remota para fins diversos da garantia do cumprimento da lei já foi objeto de decisões de proibição por parte das autoridades nacionais de proteção de dados.

(40) Nos termos do artigo 6.ºBisdo Protocolo n.º$_{qualquer}$Português 21 sobre a posição do Reino Unido e da Irlanda relativamente ao espaço de liberdade, segurança e justiça, anexa ao TUE e ao TFUE, as regras estabelecidas no artigo 5.º, n.º 1, alínea g), na medida em que se apliquem à utilização de sistemas de categorização biométrica para atividades no domínio da cooperação policial e da cooperação judiciária em matéria penal, no artigo 5.º, n.º 1, alínea d), na medida em que se apliquem à utilização de sistemas de IA abrangidos pelo âmbito de aplicação desse artigo, no artigo 5.º, n.º 1, alínea h), n.ºs 2 a 6, e no artigo 26.º, n.º 10, do presente regulamento, adotado com base no artigo 16.º do TFUE e relativo ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação da Parte III, Título V, Capítulos 4 ou 5 do referido Tratado, são vinculativas para a Irlanda apenas na medida em que as regras relativas ao presente regulamento sejam vinculativas para a Irlanda. da União que regula as formas de cooperação judiciária em matéria penal e a cooperação policial, no âmbito das quais devem ser respeitadas as disposições estabelecidas com base no artigo 16.º do TFUE.

(41) De acordo com o disposto nos artigos 2 e 2Bisdo Protocolo n.º$_{qualquer}$22 sobre a posição da Dinamarca, anexo ao TUE e ao TFUE, as regras estabelecidas no artigo 5.º, n.º 1, alínea g), na medida em que se apliquem à utilização de sistemas de categorização biométrica para atividades no domínio da cooperação policial e da cooperação judiciária em matéria penal, no artigo 5.º, n.º 1, alínea d), na medida em que se apliquem à utilização de sistemas de IA abrangidos pelo âmbito de aplicação desse artigo, no artigo 5.º,

O parágrafo 1, primeiro parágrafo, alínea h), os parágrafos 2 a 6 e o artigo 26(10) do presente regulamento, adotados com base no artigo 16.º do TFUE e que dizem respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação da Parte III, Título V, Capítulos 4 ou 5 do referido Tratado, não são vinculativos nem aplicáveis à Dinamarca.

(42) Em consonância com a presunção de inocência, as pessoas singulares na União devem ser sempre julgadas com base no seu comportamento real. Pessoas físicas nunca devem ser julgadas com base em comportamentos previstos por uma IA com base apenas em seus perfis, traços de personalidade ou características, como nacionalidade, local de nascimento, local de residência, número de filhos, nível de endividamento ou tipo de veículo, sem uma avaliação humana e sem que haja uma suspeita razoável, baseada em fatos objetivos verificáveis, de que a referida pessoa esteja envolvida em atividades criminosas. Portanto, as avaliações de risco realizadas em relação a pessoas físicas para avaliar a probabilidade de que cometam um crime ou para prever a prática de um crime real ou potencial com base apenas no perfil dessas pessoas físicas ou na avaliação de seus traços e características de personalidade devem ser proibidas. Em qualquer caso, esta proibição não se refere nem diz respeito a análises de risco que não sejam baseadas na criação de perfis de indivíduos ou nos traços de personalidade e características dos indivíduos, como sistemas de IA que usam análise de risco para avaliar a probabilidade de fraude financeira por empresas com base em transações suspeitas ou ferramentas de análise de risco para prever a probabilidade de detecção de narcóticos e mercadorias ilícitas pelas autoridades alfandegárias, por exemplo, com base em rotas de tráfico conhecidas.

(43) A colocação no mercado, a colocação em serviço para essa finalidade ou a utilização de sistemas de IA que criem ou expandam bancos de dados de reconhecimento facial por meio da extração não seletiva de imagens faciais da Internet ou de imagens de CFTV devem ser proibidas, pois tais práticas exacerbam sentimentos de vigilância em massa e podem levar a graves violações de direitos fundamentais, incluindo o direito à privacidade.

(44) Há uma preocupação considerável sobre a base científica dos sistemas de IA que buscam detectar ou inferir emoções, especialmente porque a expressão das emoções varia consideravelmente entre culturas e situações, e até mesmo dentro da mesma pessoa. Algumas das principais deficiências desses sistemas são confiabilidade limitada, falta de especificidade e generalização limitada. Portanto, os sistemas de IA que detectam ou inferem as emoções ou intenções de pessoas físicas a partir de seus dados biométricos podem ter resultados discriminatórios e podem invadir os direitos e liberdades dos indivíduos em questão. Dado o desequilíbrio de poder no local de trabalho ou na educação, combinado com a natureza intrusiva desses sistemas, esses sistemas podem levar a um tratamento prejudicial ou desfavorável de certos indivíduos ou grupos inteiros. Portanto, a colocação no mercado, o comissionamento e a utilização de sistemas de IA destinados a detectar o estado emocional das pessoas em situações relacionadas ao local de trabalho e à educação devem ser proibidos. Tal proibição não deve ser aplicada a sistemas de IA colocados no mercado estritamente para fins médicos ou de segurança, como sistemas destinados ao uso terapêutico.

(45) O presente regulamento não deverá afetar práticas proibidas pelo direito da União, incluindo o direito da União em matéria de proteção de dados, o direito da não discriminação, o direito da proteção do consumidor e o direito da concorrência.

(46) A colocação no mercado da União, a colocação em serviço ou a utilização de sistemas de IA de alto risco devem estar sujeitas ao cumprimento, por parte do utilizador, de determinados requisitos obrigatórios, que devem garantir que os sistemas de IA de alto risco disponíveis na União ou cujos resultados sejam utilizados na União não representam riscos inaceitáveis para interesses públicos importantes da União, tal como reconhecidos e protegidos pelo direito da União. Com base no novo quadro legislativo, tal como esclarecido na Comunicação da Comissão intitulada "Guia Azul sobre a implementação das regras da UE em matéria de produtos, 2022" ([20]), a regra geral é que mais do que um ato jurídico de legislação de harmonização da União, como o Regulamento (UE) 2017/745 ([21]) e (UE) 2017/746 ([22]) do Parlamento Europeu e do Conselho ou da Directiva 2006/42/CE do Parlamento Europeu e do Conselho ([23]) pode ser aplicada a um produto, uma vez que a colocação no mercado ou a entrada em serviço só pode ocorrer quando o produto estiver em conformidade com toda a legislação de harmonização aplicável da União. A fim de

([20]) DO 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 1018/2009 e o Regulamento (CE) n.º 1018/2009.qualquer178/2002 e Regulamento (CE) n.ºqualquer1223/2009 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 de diagnósticoem vitroe 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).

A fim de garantir a coerência e evitar encargos ou custos administrativos desnecessários, os fornecedores de um produto que contenha um ou mais sistemas de IA de alto risco, aos quais se aplicam os requisitos do presente regulamento e da legislação de harmonização da União enumerados num anexo ao presente regulamento, devem ser flexíveis no que diz respeito às decisões operacionais sobre como garantir a conformidade de um produto que contenha um ou mais sistemas de IA com todos os requisitos aplicáveis da legislação de harmonização da União de forma otimizada. A classificação de um sistema de IA como de "alto risco" deve ser limitada aos sistemas de IA que tenham um efeito prejudicial significativo na saúde, na segurança e nos direitos fundamentais das pessoas na União, e essa limitação deve minimizar quaisquer potenciais restrições ao comércio internacional.

(47) Os sistemas de IA podem ter um efeito adverso na saúde e segurança humanas, principalmente quando operam como componentes de segurança do produto. Em consonância com os objetivos da legislação de harmonização da União para facilitar a livre circulação de produtos no mercado interno e garantir que apenas produtos seguros e conformes cheguem ao mercado, é importante prevenir e mitigar adequadamente quaisquer riscos de segurança que um produto como um todo possa representar devido aos seus componentes digitais, que podem incluir sistemas de IA. Por exemplo, robôs cada vez mais autônomos usados em fábricas ou para fins de assistência e cuidados pessoais devem ser capazes de operar e executar suas funções com segurança em ambientes complexos. Da mesma forma, no setor da saúde, onde pode haver impactos particularmente significativos na vida e na saúde, sistemas de diagnóstico e suporte à decisão cada vez mais sofisticados devem ser confiáveis e precisos.

(48) A magnitude das consequências adversas de um sistema de IA para os direitos fundamentais protegidos pela Carta é particularmente importante ao classificar um sistema de IA como de alto risco. Estes direitos incluem o direito à dignidade humana, o respeito pela vida privada e familiar, a proteção de dados pessoais, a liberdade de expressão e informação, a liberdade de reunião e associação, o direito à não discriminação, o direito à educação, a proteção do consumidor, os direitos dos trabalhadores, os direitos das pessoas com deficiência, a igualdade entre homens e mulheres, os direitos de propriedade intelectual, o direito à proteção judicial efetiva e a um juiz imparcial, os direitos de defesa e a presunção de inocência, e o direito à boa administração. Além desses direitos, vale destacar que as crianças têm direitos específicos consagrados no Artigo 24 da Carta e na Convenção das Nações Unidas sobre os Direitos da Criança, que são desenvolvidos com mais detalhes no Comentário Geral n.º 1.qualquer25 da Convenção das Nações Unidas sobre os Direitos da Criança sobre os direitos das crianças em relação ao ambiente digital. Ambos os instrumentos exigem que as vulnerabilidades das crianças sejam levadas em consideração e que elas recebam a proteção e a assistência necessárias ao seu bem-estar. Ao avaliar a gravidade dos danos que um sistema de IA pode causar, inclusive no que diz respeito à saúde e à segurança humanas, o direito fundamental a um alto nível de proteção ambiental consagrado na Carta e implementado nas políticas da União também deve ser levado em consideração.

(49) Em relação aos sistemas de IA de alto risco que são componentes de segurança de produtos ou sistemas, ou que são eles próprios produtos ou sistemas abrangidos pelo âmbito do Regulamento (CE) n.ºqualquer300/2008 do Parlamento Europeu e do Conselho (24), Regulamento (UE) n.ºqualquer167/2013 do Parlamento Europeu e do Conselho (25), Regulamento (UE) n.ºqualquer 168/2013 do Parlamento Europeu e do Conselho (26), Diretiva 2014/90/UE do Parlamento Europeu e do Conselho (27), Diretiva (UE) 2016/797 do Parlamento Europeu e do Conselho (28), Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho (29), Regulamento (UE) 2018/1139 do Parlamento Europeu e

(24) Regulamento (CE) n.ºqualquer300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008, relativa a regras comuns para a segurança da aviação civil e que revoga o Regulamento (CE) n.º 300/2008.qualquer2320/2002 (JO L 97 de 9.4.2008, p. 72).

(25) Regulamento (UE) n.ºqualquer167/2013 do Parlamento Europeu e do Conselho, de 5 de fevereiro de 2013, relativo à homologação de veículos agrícolas ou florestais e à fiscalização do mercado desses veículos (JO L 60 de 2.3.2013, p. 1).

(26) Regulamento (UE) n.ºqualquer168/2013 do Parlamento Europeu e do Conselho, de 15 de janeiro de 2013, relativo à homologação de veículos de duas ou três rodas e de quadriciclos e à fiscalização do mercado desses veículos (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).

(29) Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho, de 30 de maio de 2018, relativo à homologação e fiscalização do mercado de veículos motorizados e seus reboques, e de sistemas, componentes e unidades técnicas destinadas a esses veículos, que altera os Regulamentos (CE) n.º 1189/2008 e (CE) n.º 1189/2008 e revoga ...qualquer715/2007 e (CE) n.º.qualquer595/2009 e que revoga a Diretiva 2007/46/CE (JO L 151 de 14.6.2018, p. 1).

do Conselho (30), e o Regulamento (UE) 2019/2144 do Parlamento Europeu e do Conselho (31), é adequado alterar esses atos para garantir que, ao adotar atos delegados ou de execução relevantes baseados neles, a Comissão tenha em conta os requisitos obrigatórios para sistemas de IA de alto risco previstos no presente regulamento, tendo em conta as especificidades técnicas e regulamentares dos diferentes setores e sem interferir nos mecanismos e autoridades de governação, avaliação da conformidade e execução existentes, estabelecidos nesses atos.

(50) Para sistemas de IA que são componentes de segurança de produtos, ou são produtos em si mesmos, e se enquadram no escopo de determinados atos legislativos de harmonização da União listados em um anexo ao presente regulamento, é apropriado classificá-los como de alto risco nos termos do presente regulamento se o produto em questão estiver sujeito a um procedimento de avaliação da conformidade com um organismo de avaliação da conformidade de terceiros, de acordo com esses atos legislativos de harmonização da União. Esses produtos são, em particular, máquinas, brinquedos, elevadores, equipamentos e sistemas de proteção para uso em atmosferas potencialmente explosivas, equipamentos de rádio, equipamentos de pressão, equipamentos para barcos de recreio, instalações de transporte por cabo, aparelhos que queimam combustíveis gasosos, dispositivos médicos, dispositivos médicos de diagnóstico.em vitro,automotivo e aviação.

(51) O facto de um sistema de IA ser classificado como de alto risco ao abrigo do presente regulamento não significa necessariamente que o produto do qual é um componente de segurança, ou o próprio sistema de IA enquanto produto, seja considerado de «alto risco» de acordo com os critérios estabelecidos na legislação de harmonização da União aplicável ao produto. É o caso, em particular, dos Regulamentos (UE) 2017/745 e (UE) 2017/746, que preveem a avaliação da conformidade por terceiros de produtos de médio e alto risco.

(52) No que diz respeito aos sistemas de IA autónomos, nomeadamente os sistemas de IA de alto risco que não são componentes de segurança dos produtos ou são produtos em si mesmos, devem ser classificados como de alto risco se, à luz da sua finalidade pretendida, apresentarem um elevado risco de danos para a saúde e a segurança ou para os direitos fundamentais das pessoas, tendo em conta tanto a gravidade dos danos potenciais como a probabilidade de ocorrência de danos, e forem utilizados em várias áreas predefinidas especificadas no presente regulamento. Para identificar tais sistemas, são utilizados a mesma metodologia e os mesmos critérios previstos na possível futura alteração da lista de sistemas de IA de alto risco, que a Comissão deverá ter poderes para adotar, por meio de atos delegados, a fim de ter em conta o ritmo acelerado do desenvolvimento tecnológico, bem como as possíveis alterações na utilização dos sistemas de IA.

(53) Também é importante esclarecer que pode haver casos específicos em que os sistemas de IA abrangidos por áreas predefinidas especificadas no presente regulamento não representam um risco significativo de dano aos interesses jurídicos abrangidos por essas áreas, uma vez que não influenciam substancialmente a tomada de decisões ou não prejudicam substancialmente esses interesses. Para efeitos do presente regulamento, um sistema de IA que não influencia substancialmente o resultado da tomada de decisões deverá significar um sistema de IA que não afeta a substância e, consequentemente, o resultado da tomada de decisões, quer sejam humanas ou automatizadas. Um sistema de IA que não influencia substancialmente o resultado da tomada de decisão pode incluir situações em que uma ou mais das seguintes condições são atendidas. A primeira dessas condições deve ser que o sistema de IA se destine a executar uma tarefa processual delimitada, como um sistema de IA que transforma dados não estruturados em dados estruturados, um sistema de IA que classifica documentos recebidos em categorias ou um sistema de IA que é usado para detectar duplicatas em um grande número de aplicativos. A natureza dessas tarefas é tão restrita e limitada que elas apresentam apenas riscos limitados que não são aumentados pelo uso de um sistema de IA em um contexto que um anexo ao presente regulamento especifica como um uso de alto risco. A segunda condição deve ser que a tarefa executada pelo sistema de IA tenha como objetivo melhorar o resultado de uma atividade

(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 e altera os Regulamentos (CE) n.º 1139/2018 e (CE) n.º 1139/2018...qualquer2111/2005, (CE) n.º.qualquer1008/2008, (UE) n.ºqualquer996/2010 e (UE) n.qualquer376/2014 e Diretivas 2014/30/UE e 2014/53/UE do Parlamento Europeu e do Conselho e Regulamentos (CE) n.ºqualquer552/2004 e (CE) n.º.qualquer216/2008 do Parlamento Europeu e do Conselho e Regulamento (CEE) n.ºqualquer3922/91 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 para veículos a motor e seus reboques, e sistemas, componentes e unidades técnicas separadas destinados a esses veículos, no que diz respeito à sua segurança geral e à proteção dos ocupantes dos veículos e dos utilizadores vulneráveis da estrada, que altera o Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho e revoga os Regulamentos (CE) n.º 1899/2002 e (CE) n.º 1899/2002.qualquer78/2009, (CE) n.ºqualquer79/2009 e (CE) n.º.qualquer661/2009 do Parlamento Europeu e do Conselho e Regulamento (CE) n.ºqualquer631/2009, (UE) n.ºqualquer406/2010, (UE) n.ºqualquer672/2010, (UE) n.ºqualquer1003/2010, (UE) n.ºqualquer1005/2010, (UE) n.ºqualquer1008/2010, (UE) n.ºqualquer1009/2010, (UE) n.ºqualquer19/2011, (UE) n.qualquer109/2011, (UE) n.ºqualquer458/2011, (UE) n.ºqualquer65/2012, (UE) n.ºqualquer130/2012, (UE) n.ºqualquer347/2012, (UE) n.ºqualquer351/2012, (UE) n.ºqualquer1230/2012 e (UE) 2015/166 da Comissão (JO L 325 de 16.12.2019, p. 1).

testes prévios realizados por um ser humano, que possam ser relevantes para efeitos das utilizações de alto risco enumeradas num anexo ao presente regulamento. Dadas essas características, o sistema de IA apenas acrescenta um nível adicional à atividade humana, acarretando assim menos riscos. Essa condição se aplicaria, por exemplo, a sistemas de IA destinados a melhorar a linguagem utilizada em documentos já escritos, por exemplo, no que diz respeito ao uso de um tom profissional ou de um registro linguístico acadêmico ou à adaptação do texto a uma comunicação de marca específica. A terceira condição deve ser que o sistema de IA tenha como objetivo detectar padrões de tomada de decisão ou desvios de padrões de tomada de decisão anteriores. O risco seria menor porque o sistema de IA é usado após uma avaliação humana prévia e não tem a intenção de substituí-lo ou influenciá-lo sem a devida revisão por um humano. Por exemplo, os sistemas de IA deste tipo incluem aqueles que podem ser usados para verificara posteriori se um professor pode ter se desviado de seu padrão de classificação prescrito, a fim de chamar a atenção para quaisquer inconsistências ou anomalias. A quarta condição deve ser que o sistema de IA se destine a executar uma tarefa que seja apenas preparatória para uma avaliação relevante para os fins dos sistemas de IA listados no anexo do presente regulamento, pelo que o impacto potencial dos resultados do sistema seria muito baixo em termos de representar um risco para a avaliação subsequente. Isso inclui, entre outras coisas, soluções inteligentes para gerenciamento de arquivos, incluindo diversas funções como indexação, pesquisa, processamento de texto e fala, ou vinculação de dados a outras fontes de dados, ou sistemas de IA usados para a tradução de documentos iniciais. Em qualquer caso, os sistemas de IA utilizados em casos de alto risco enumerados num anexo ao presente regulamento devem ser considerados como apresentando um risco significativo de comprometer a saúde e a segurança ou os direitos fundamentais se o sistema de IA envolver a definição de perfis na aceção do artigo 4.º, n.º 4, do Regulamento (UE) 2016/679, do artigo 3.º, n.º 4, da Diretiva (UE) 2016/680 ou do artigo 3.º, n.º 5, do Regulamento (UE) 2018/1725. Para garantir a rastreabilidade e a transparência, os fornecedores que, com base nas condições acima, considerem que um sistema de IA não é de alto risco, devem preparar a documentação de avaliação antes da colocação no mercado ou da entrada em serviço desse sistema de IA e fornecê-la às autoridades nacionais competentes mediante solicitação. Esses provedores devem ser obrigados a registrar o sistema no banco de dados da UE criado ao abrigo do presente regulamento. A fim de fornecer orientações adicionais sobre a aplicação prática das condições em que os sistemas de IA listados num anexo ao presente regulamento não são, excepcionalmente, considerados de alto risco, a Comissão deverá, após consulta ao Conselho da IA, fornecer orientações que especifiquem essa aplicação prática, complementadas por uma lista exaustiva de exemplos práticos de casos de utilização de sistemas de IA de alto risco e de risco não elevado.

(54) Como os dados biométricos constituem uma categoria de dados pessoais sensíveis, vários casos de uso crítico de sistemas biométricos devem ser classificados como de alto risco, na medida em que seu uso seja permitido pela legislação nacional e da União aplicável. Imprecisões técnicas em sistemas de IA destinados à identificação biométrica remota de pessoas físicas podem levar a resultados tendenciosos e ter efeitos discriminatórios. O risco de tais resultados tendenciosos e efeitos discriminatórios é particularmente relevante no que diz respeito à idade, etnia, raça, sexo ou deficiência. Os sistemas de identificação biométrica remota devem, portanto, ser classificados como de alto risco devido aos riscos que acarretam. Estão excluídos desta classificação os sistemas de IA destinados à verificação biométrica, o que inclui a autenticação, cujo único propósito é confirmar que uma pessoa física específica é quem afirma ser, bem como confirmar a identidade de uma pessoa física com o único propósito de conceder acesso a um serviço, desbloquear um dispositivo ou ter acesso seguro a um local. Além disso, os sistemas de IA destinados a serem utilizados para categorização biométrica de acordo com atributos ou características sensíveis protegidos pelo artigo 9.º, n.º 1, do Regulamento (UE) 2016/679 com base em dados biométricos, na medida em que não sejam proibidos ao abrigo do presente regulamento, bem como os sistemas de reconhecimento de emoções que não sejam proibidos ao abrigo do presente regulamento, devem ser classificados como de alto risco. Sistemas biométricos destinados a serem usados exclusivamente para fins de viabilização de medidas de segurança cibernética e proteção de dados pessoais não devem ser considerados sistemas de IA de alto risco.

(55) No que diz respeito à gestão e operação de infraestruturas críticas, os sistemas de IA destinados a serem utilizados como componentes de segurança na gestão e operação de infraestruturas digitais críticas enumeradas no ponto 8 do anexo da Diretiva (UE) 2022/2557 devem ser classificados como de alto risco; tráfego rodoviário e fornecimento de água, gás, aquecimento e eletricidade, uma vez que uma falha ou mau funcionamento desses componentes pode colocar em risco a vida e a saúde das pessoas em grande escala e interromper significativamente o desenvolvimento normal das atividades sociais e econômicas. Componentes de segurança de infraestrutura crítica, como infraestrutura digital crítica, são sistemas usados para proteger diretamente a integridade física da infraestrutura crítica ou a saúde e a segurança de pessoas e propriedades, mas não são necessários para a operação do sistema. A falha ou defeito de

A operação desses componentes pode levar diretamente a riscos à integridade física de infraestruturas críticas e, portanto, a riscos à saúde e segurança de pessoas e bens. Componentes destinados a serem usados exclusivamente para fins de segurança cibernética não devem ser considerados componentes de segurança. Os componentes de segurança dessas infraestruturas críticas incluem sistemas de controle de pressão de água ou sistemas de controle de alarme de incêndio em centros de computação em nuvem.

(56) A implantação de sistemas de IA na educação é importante para promover educação e treinamento digitais de alta qualidade e permitir que todos os alunos e professores adquiram e compartilhem as habilidades e competências digitais necessárias, incluindo alfabetização midiática e pensamento crítico, para participar ativamente da economia, da sociedade e dos processos democráticos. No entanto, os sistemas de IA usados na educação ou treinamento vocacional, e em particular aqueles que determinam o acesso ou admissão, alocam indivíduos entre diferentes instituições ou programas educacionais e de treinamento vocacional em todos os níveis, avaliam os resultados de aprendizagem dos indivíduos, avaliam o nível apropriado de educação de um indivíduo e influenciam substancialmente o nível de educação e treinamento que os indivíduos receberão ou poderão acessar, ou monitoram e detectam comportamentos proibidos por alunos durante os testes, devem ser classificados como de alto risco, pois podem decidir o caminho educacional e profissional de um indivíduo e, consequentemente, podem afetar sua capacidade de garantir um meio de vida. Quando não são projetados e usados corretamente, esses sistemas podem ser particularmente intrusivos e violar o direito à educação e à formação, e o direito de não ser discriminado, além de perpetuar padrões históricos de discriminação, por exemplo, contra mulheres, certas faixas etárias, pessoas com deficiência ou pessoas de uma determinada origem racial ou étnica ou com uma determinada orientação sexual.

(57) Os sistemas de IA utilizados nas áreas de emprego, gestão da força de trabalho e acesso ao trabalho autônomo, em especial para recrutamento e seleção de pessoal, para tomada de decisões que afetam os termos e condições de relações de trabalho, promoção e rescisão de relações de trabalho contratuais, para atribuição de tarefas com base no comportamento individual ou em traços ou características pessoais e para monitoramento ou avaliação de indivíduos dentro de relações de trabalho contratuais, também devem ser classificados como de alto risco, pois podem afetar significativamente as perspectivas futuras de emprego, a subsistência desses indivíduos e os direitos dos trabalhadores. As relações de emprego contratuais devem incluir significativamente funcionários e pessoas que prestam serviços por meio de plataformas, conforme descrito no Programa de Trabalho de 2021 da Comissão. Esses sistemas podem perpetuar padrões históricos de discriminação, por exemplo, contra mulheres, certas faixas etárias, pessoas com deficiência ou pessoas de origens raciais ou étnicas específicas ou com uma orientação sexual específica, ao longo do processo de recrutamento e na avaliação, promoção ou retenção de pessoas em relações de emprego contratuais. Os sistemas de IA usados para monitorar o desempenho e o comportamento desses indivíduos também podem prejudicar seus direitos fundamentais à proteção de dados pessoais e privacidade.

(58) O acesso e o usufruto de certos serviços e benefícios essenciais, tanto públicos quanto privados, que são necessários para que as pessoas participem plenamente da sociedade ou melhorem seu padrão de vida, é outra área em que atenção especial deve ser dada ao uso de sistemas de IA. Em particular, as pessoas singulares que solicitam ou recebem de autoridades públicas benefícios e serviços essenciais de assistência pública, nomeadamente serviços de saúde, benefícios de segurança social, serviços sociais que asseguram proteção em casos como maternidade, doença, acidentes de trabalho, dependência ou velhice e perda de emprego, assistência social e assistência habitacional, são frequentemente dependentes de tais benefícios e serviços e encontram-se geralmente numa posição vulnerável face às autoridades responsáveis. O uso de sistemas de IA para decidir se as autoridades devem conceder, negar, reduzir ou revogar tais benefícios e serviços ou reivindicar seu reembolso, incluindo decidir, por exemplo, se os beneficiários têm direito legítimo a tais benefícios e serviços, pode ter um impacto significativo nos meios de subsistência das pessoas e violar seus direitos fundamentais, como o direito à proteção social, à não discriminação, à dignidade humana ou à proteção judicial efetiva, e, portanto, deve ser classificado como de alto risco. No entanto, este regulamento não deve impedir o desenvolvimento e a utilização de abordagens inovadoras no governo, que poderiam beneficiar de uma maior utilização de sistemas de IA conformes e seguros, desde que tais sistemas não representem um risco elevado para pessoas singulares e coletivas. Além disso, os sistemas de IA usados para avaliar a classificação de crédito ou a solvência de indivíduos devem ser classificados como de alto risco, pois decidem se esses indivíduos podem acessar recursos financeiros ou serviços essenciais, como moradia, eletricidade e telecomunicações. Os sistemas de IA usados para tais propósitos podem discriminar certos indivíduos ou grupos e perpetuar padrões históricos de discriminação, como com base na origem racial ou étnica, gênero, deficiência, idade ou orientação sexual, ou gerar novas formas de discriminação. No entanto, os sistemas de IA previstos pela legislação da União com vista a detetar fraudes na prestação de serviços financeiros e, para efeitos prudenciais, a calcular os requisitos de capital das instituições de crédito e das empresas de seguros não deverão ser considerados de alto risco ao abrigo do presente regulamento. Além do mais,

Sistemas de IA destinados a serem utilizados para avaliação de riscos e precificação em relação a

O uso de apólices de seguro de vida e saúde por indivíduos também pode ter um impacto significativo nos meios de subsistência das pessoas e, se não for adequadamente projetado, desenvolvido e usado, pode violar seus direitos fundamentais e ter consequências sérias para a vida e a saúde das pessoas, como exclusão financeira e discriminação. Por fim, os sistemas de IA usados para avaliar e classificar chamadas de emergência de indivíduos ou para despachar ou priorizar o envio de socorristas em situações de emergência, incluindo polícia, bombeiros e serviços médicos, bem como sistemas de triagem de pacientes para assistência médica de emergência, também devem ser considerados de alto risco, pois tomam decisões em situações extremamente críticas para a vida e a saúde das pessoas e de seus bens.

(59) Dado seu papel e responsabilidade, as ações das autoridades policiais que envolvem certos usos de sistemas de IA são caracterizadas por um desequilíbrio significativo de poder e podem levar à vigilância, prisão ou privação de liberdade de uma pessoa física, além de ter outros efeitos negativos sobre os direitos fundamentais consagrados na Carta. Em particular, se o sistema de IA não for treinado com dados de boa qualidade, não atender aos requisitos adequados em termos de desempenho, precisão ou robustez, ou não for adequadamente projetado e testado antes de ser introduzido no mercado ou colocado em serviço, ele poderá ter como alvo indivíduos de forma discriminatória, incorreta ou injusta. Além disso, poderia impedir o exercício de direitos processuais fundamentais importantes, como o direito à proteção judicial efetiva e a um juiz imparcial, bem como o direito à defesa e à presunção de inocência, principalmente quando tais sistemas de IA não são suficientemente transparentes, explicáveis ou bem documentados. Portanto, na medida em que seu uso seja permitido pela legislação nacional e da União aplicável, é adequado classificar como de alto risco uma série de sistemas de IA destinados a serem usados para fins de execução, onde sua precisão, confiabilidade e transparência são particularmente importantes para evitar consequências adversas, manter a confiança pública e garantir responsabilização e recursos eficazes.
Tendo em conta a natureza das atividades e os riscos associados, esses sistemas de IA de alto risco devem incluir, em particular, sistemas de IA destinados a serem utilizados por ou em nome de autoridades responsáveis pela aplicação da lei ou por instituições, órgãos, gabinetes ou agências da União em apoio às autoridades responsáveis pela aplicação da lei, para avaliar o risco de uma pessoa singular se tornar vítima de um crime, como testes de polígrafo e outras ferramentas semelhantes, para avaliar a fiabilidade das provas durante a investigação ou a acusação de infrações penais e, na medida em que não seja proibido pelo presente regulamento, para avaliar o risco de uma pessoa singular cometer uma infração penal ou reincidir, não apenas com base na definição de perfis de pessoas singulares ou na avaliação de traços e características de personalidade ou comportamento criminoso passado de pessoas singulares ou grupos de pessoas, ou para definição de perfis durante a deteção, investigação ou acusação de infrações penais. Os sistemas de IA especificamente destinados ao uso em processos administrativos por autoridades fiscais e aduaneiras e unidades de inteligência financeira que realizam tarefas administrativas de análise de informações de acordo com a lei da União contra a lavagem de dinheiro não devem ser classificados como sistemas de IA de alto risco usados por autoridades policiais para fins de prevenção, detecção, investigação e repressão de infrações penais. O uso de ferramentas de IA por autoridades policiais e outras autoridades relevantes não deve se tornar um fator de desigualdade ou exclusão. Não se deve ignorar o impacto do uso de ferramentas de IA nos direitos de defesa dos suspeitos, em particular a dificuldade em obter informações significativas sobre o funcionamento de tais sistemas e a consequente dificuldade em contestar seus resultados em tribunal, em especial por pessoas físicas sob investigação.

(60) Os sistemas de IA utilizados na gestão de migração, asilo e controle de fronteiras afetam pessoas que muitas vezes se encontram em situação particularmente vulnerável e que dependem do resultado das ações das autoridades públicas competentes. Por esse motivo, é extremamente importante que os sistemas de IA utilizados nesses contextos sejam precisos, não discriminatórios e transparentes, a fim de garantir que os direitos fundamentais dos indivíduos em questão sejam respeitados, e em particular seu direito à livre circulação, à não discriminação, à privacidade pessoal e à proteção de dados pessoais, à proteção internacional e à boa administração. Por conseguinte, é adequado classificar como de alto risco, na medida em que a sua utilização seja permitida pela legislação da União e nacional, os sistemas de IA destinados a serem utilizados por ou em nome de autoridades públicas competentes ou por instituições, organismos, gabinetes ou agências da União que desempenhem tarefas no domínio da migração, do asilo e da gestão do controlo de fronteiras, tais como polígrafos e instrumentos semelhantes, para avaliar determinados riscos colocados por pessoas singulares que entram no território de um Estado-Membro ou que solicitam um visto ou asilo, para auxiliar as autoridades públicas competentes no exame, incluindo a avaliação conexa da fiabilidade das provas, dos pedidos de asilo, vistos e autorizações de residência, bem como de reivindicações conexas em relação ao objetivo de determinar se as pessoas singulares requerentes preenchem os requisitos para que o seu pedido seja deferido, para efeitos de deteção, reconhecimento ou identificação de pessoas singulares no contexto da gestão da migração, do asilo e do controlo de fronteiras, com exceção da verificação de documentos de viagem. Os sistemas de IA no domínio da gestão da migração, do asilo e do controlo de fronteiras sujeitos ao presente regulamento deverão cumprir os requisitos processuais relevantes estabelecidos no Regulamento (CE) n.º 1099/2008.qualquer810/2009 do Parlamento Europeu e do

Conselho (32), Diretiva 2013/32/UE do Parlamento Europeu e do Conselho (33) e outras legislações relevantes da União. O uso de sistemas de IA na gestão de migração, asilo e controle de fronteiras não deve, em nenhuma circunstância, ser usado pelos Estados-Membros ou instituições, órgãos, escritórios ou agências da União como um meio de contornar suas obrigações internacionais sob a Convenção das Nações Unidas relativa ao Estatuto dos Refugiados, feita em Genebra em 28 de julho de 1951, conforme alterada pelo Protocolo de 31 de janeiro de 1967. Também não deve ser usado para infringir de forma alguma o princípio de não repulsão, nem para negar vias legais seguras e eficazes de acesso ao território da União, incluindo o direito à proteção internacional.

(61) Certos sistemas de IA destinados à administração da justiça e aos processos democráticos devem ser classificados como de alto risco, uma vez que podem ter efeitos potencialmente significativos na democracia, no Estado de direito, nas liberdades individuais e no direito à proteção judicial efetiva e a um juiz imparcial. Em particular, para abordar o risco de potencial enviesamento, erro e opacidade, os sistemas de IA destinados a serem utilizados por ou em nome de uma autoridade judicial para auxiliar as autoridades judiciais na investigação e interpretação de fatos e da lei e na aplicação da lei a fatos específicos devem ser classificados como de alto risco. Os sistemas de IA destinados a serem usados por órgãos de resolução alternativa de disputas para tais propósitos também devem ser considerados de alto risco, quando os resultados dos procedimentos de resolução alternativa de disputas tiverem efeitos legais para as partes. O uso de ferramentas de IA pode dar suporte ao poder de decisão dos juízes ou à independência judicial, mas não deve substituí-los: a tomada de decisão final deve continuar sendo uma atividade humana. No entanto, a classificação dos sistemas de IA como de alto risco não deve ser estendida aos sistemas de IA destinados a atividades administrativas puramente acessórias que não afetam a administração da justiça em si em casos específicos, como a anonimização ou pseudonimização de decisões judiciais, documentos ou dados, a comunicação entre funcionários ou tarefas administrativas.

(62) Sem prejuízo das regras previstas no Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho (34), e para fazer face aos riscos de interferência externa indevida no direito de voto consagrado no artigo 39.º da Carta e de efeitos adversos na democracia e no Estado de direito, os sistemas de IA destinados a influenciar o resultado de uma eleição ou de um referendo, ou o comportamento eleitoral de pessoas singulares quando exercem o seu voto em eleições ou referendos, devem ser classificados como sistemas de IA de alto risco, com exceção dos sistemas de IA a cujos resultados as pessoas singulares não estão diretamente expostas, como as ferramentas utilizadas para organizar, otimizar e estruturar campanhas políticas de um ponto de vista administrativo e logístico.

(63) O fato de um sistema de IA ser classificado como um sistema de IA de alto risco ao abrigo do presente regulamento não deve ser interpretado como uma indicação de que sua utilização é lícita ao abrigo de outros atos do direito da União ou do direito nacional compatível com o direito da União, por exemplo, no que diz respeito à proteção de dados pessoais ou à utilização de polígrafos e ferramentas semelhantes ou outros sistemas para detetar o estado emocional de pessoas singulares. Qualquer utilização deste tipo deverá continuar a ser efetuada exclusivamente de acordo com os requisitos relevantes decorrentes da Carta e dos atos aplicáveis do direito secundário da União e do direito nacional. O presente regulamento não deve ser entendido como constituindo uma base jurídica para o tratamento de dados pessoais, incluindo categorias especiais de dados pessoais, quando aplicável, salvo se o presente regulamento dispuser especificamente o contrário.

(64) A fim de mitigar os riscos representados pelos sistemas de IA de alto risco colocados no mercado ou em serviço, e para garantir um alto nível de confiabilidade, devem ser aplicados requisitos obrigatórios aos sistemas de IA de alto risco que levem em consideração a finalidade pretendida e o contexto de uso do sistema de IA e estejam alinhados com o sistema de gerenciamento de risco a ser estabelecido pelo provedor. As medidas tomadas pelos prestadores para cumprir os requisitos obrigatórios do presente regulamento devem levar em conta o estado da arte geralmente reconhecido no campo da IA, ser proporcionais e eficazes para atingir os objetivos do presente regulamento. Com base no novo quadro legislativo, conforme esclarecido na Comunicação da Comissão intitulada "Guia Azul sobre a implementação das regras de produtos da UE, 2022", a regra geral é que mais de um ato jurídico da legislação de harmonização da União pode ser aplicável a um produto, uma vez que a colocação no mercado ou a entrada em serviço só pode ocorrer quando o produto estiver em conformidade com 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 daqueles abrangidos pela legislação de harmonização da União em vigor e, portanto, os requisitos do presente regulamento complementariam o atual conjunto de legislação de harmonização da União. Por exemplo, máquinas ou dispositivos médicos que incorporem um sistema de IA podem apresentar riscos que não são abordados pela

(32) Regulamento (CE) n.ºqualquer810/2009 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 de proteção internacional (JO L 180 de 29.6.2013, p. 60).

(34) Regulamento (UE) 2024/900 do Parlamento Europeu e do Conselho, de 13 de março de 2024, relativo à transparência e à segmentação na publicidade política (JO L 2024/900, 20.3.2024, ELI: http://data.europa.eu/eli/reg/2024/900/oj).

requisitos essenciais de saúde e segurança estabelecidos na legislação harmonizada da União pertinente, uma vez que essa legislação setorial não aborda os riscos específicos dos sistemas de IA. Isso requer a aplicação simultânea e complementar de vários atos legislativos. A fim de garantir a coerência e evitar encargos administrativos e custos desnecessários, os fornecedores de um produto que contenha um ou mais sistemas de IA de alto risco, aos quais se aplicam os requisitos do presente regulamento e dos atos legislativos de harmonização da União baseados no novo quadro legislativo e enumerados num anexo ao presente regulamento, devem ser flexíveis no que diz respeito às decisões operacionais sobre como garantir a conformidade de um produto que contenha um ou mais sistemas de IA com todos os requisitos aplicáveis da legislação harmonizada da União de forma otimizada. Essa flexibilidade pode significar, por exemplo, a decisão do fornecedor de integrar parte dos processos de teste e relatórios necessários, bem como as informações e a documentação exigidas por este regulamento, na documentação e nos procedimentos já existentes exigidos pelos atuais atos legislativos de harmonização da União, baseados no novo quadro legislativo e listados em um anexo ao presente regulamento. Isso não deve, de forma alguma, prejudicar a obrigação do fornecedor de cumprir todos os requisitos aplicáveis.

(65) O sistema de gerenciamento de riscos deve consistir em um processo iterativo contínuo que seja planejado e executado durante todo o ciclo de vida do sistema de IA de alto risco. Tal processo deve ter como objetivo detectar e mitigar riscos relevantes representados pelos sistemas de IA à saúde, à segurança e aos direitos fundamentais. O sistema de gestão de riscos deve ser revisado e atualizado regularmente para garantir sua eficácia contínua e para assegurar a justificativa e a documentação de quaisquer decisões e ações significativas tomadas sob este Regulamento. Este processo deve garantir que o provedor determine os riscos ou efeitos negativos e implemente medidas de mitigação para riscos conhecidos e razoavelmente previsíveis dos sistemas de IA para a saúde, segurança e direitos fundamentais, levando em consideração sua finalidade pretendida e uso indevido razoavelmente previsível, incluindo riscos potenciais decorrentes da interação entre o sistema de IA e o ambiente em que opera. O sistema de gerenciamento de riscos deve adotar as medidas de gerenciamento de riscos mais apropriadas à luz do atual estado da arte em IA. Ao determinar as medidas de gerenciamento de risco mais apropriadas, o fornecedor deve documentar e explicar as escolhas feitas e, quando apropriado, envolver especialistas externos e partes interessadas. Ao determinar o uso indevido razoavelmente previsível de sistemas de IA de alto risco, o provedor deve levar em consideração os usos de sistemas de IA que, embora não diretamente abrangidos pela finalidade pretendida ou definidos nas instruções de uso, podem ser razoavelmente esperados como resultado de comportamento humano facilmente previsível no contexto das características específicas e do uso de um sistema de IA específico. Quaisquer circunstâncias conhecidas ou previsíveis associadas ao uso do sistema de IA de alto risco de acordo com a finalidade pretendida ou com uso indevido razoavelmente previsível que possa dar origem a riscos à saúde e segurança ou aos direitos fundamentais devem ser incluídas nas instruções de uso fornecidas pelo fornecedor. O objetivo é garantir que o implantador esteja ciente desses riscos e os leve em consideração ao usar o sistema de IA de alto risco. A identificação e implementação de medidas de mitigação de riscos em caso de utilização indevida previsível ao abrigo do presente regulamento não deverá exigir, para as resolver, formação adicional específica para o sistema de IA de alto risco por parte do fornecedor, a fim de resolver utilizações indevidas previsíveis. No entanto, os provedores são incentivados a considerar tais medidas de treinamento adicionais para mitigar o uso indevido razoavelmente previsível, quando necessário e apropriado.

(66) Requisitos relativos à gestão de riscos, qualidade e relevância dos conjuntos de dados utilizados, documentação técnica e manutenção de registros, transparência e comunicação de informações aos responsáveis pela implantação, supervisão humana, robustez e conformidade devem ser aplicados a sistemas de IA de alto risco. precisão e segurança cibernética. Tais requisitos são necessários para mitigar efetivamente os riscos à saúde, à segurança e aos direitos fundamentais. Na ausência de medidas menos restritivas ao comércio razoavelmente disponíveis, tais requisitos não constituem restrições injustificadas ao comércio.

(67) Dados de alta qualidade e acesso a dados de alta qualidade desempenham um papel essencial no fornecimento de estrutura e na garantia do funcionamento de muitos sistemas de IA, em particular ao empregar técnicas que envolvem treinamento de modelos, com vistas a garantir que o sistema de IA de alto risco opere conforme o esperado e com segurança e não se torne uma fonte de qualquer forma de discriminação proibida pela legislação da União. Práticas adequadas de governança e gerenciamento de dados devem ser implementadas para garantir conjuntos de dados de alta qualidade para treinamento, validação e testes. Os conjuntos de dados para treinamento, validação e teste, incluindo rótulos, devem ser relevantes, suficientemente representativos e, na maior medida possível, livres de erros e completos, tendo em vista a finalidade pretendida do sistema. Para facilitar o cumprimento da legislação da União sobre proteção de dados, como o Regulamento (UE) 2016/679, as práticas de gestão e governação de dados devem incluir, no caso de dados pessoais, transparência sobre a finalidade original da coleta de dados. Os conjuntos de dados devem ter propriedades estatísticas apropriadas, inclusive no que diz respeito às pessoas ou grupos de pessoas em relação às quais o sistema de IA de alto risco se destina a ser usado, com atenção especial à mitigação de potenciais vieses nos conjuntos de dados que possam afetar a saúde e a segurança de pessoas físicas, ter impactos negativos nos direitos fundamentais ou dar origem a qualquer outro tipo de dano.

discriminação proibida pela legislação da União, especialmente quando os dados de saída influenciam as informações de entrada para transações futuras (ciclos de feedback). Vieses, por exemplo, podem ser inerentes aos conjuntos de dados subjacentes, especialmente ao usar dados históricos, ou gerados quando os sistemas são implantados em ambientes do mundo real. Os resultados dos sistemas de IA dependem desses preconceitos inerentes, que tendem a aumentar gradualmente e, assim, perpetuar e amplificar a discriminação existente, particularmente com relação a indivíduos pertencentes a certos grupos vulneráveis, incluindo grupos raciais ou étnicos. O requisito de que os conjuntos de dados sejam, na maior medida possível, completos e livres de erros não deve afetar o uso de técnicas de proteção de privacidade no contexto do desenvolvimento e teste de sistemas de IA. Em particular, os conjuntos de dados devem levar em conta, na medida exigida pela finalidade pretendida, as características, os elementos ou as características particulares do ambiente geográfico, contextual, comportamental ou funcional específico no qual o sistema de IA se destina a ser utilizado. Os requisitos relacionados à governança de dados podem ser atendidos por meio do uso de terceiros que ofereçam serviços de conformidade certificados, incluindo verificação de governança de dados, integridade de conjuntos de dados e práticas de treinamento, validação e teste de dados, na medida em que a conformidade com os requisitos de dados deste Regulamento seja garantida.

(68) Para poder desenvolver e avaliar sistemas de IA de alto risco, certos intervenientes, como fornecedores, organismos notificados e outras entidades relevantes, como os Centros Europeus de Inovação Digital, instalações de teste e experimentação e investigadores, devem ter acesso e poder utilizar conjuntos de dados de alta qualidade nos seus domínios de atividade relacionados com o presente regulamento. Os espaços comuns de dados europeus estabelecidos pela Comissão e a facilitação do compartilhamento de dados entre empresas e com governos no interesse público serão essenciais para fornecer acesso confiável, responsável e não discriminatório a dados de alta qualidade para treinar, validar e testar sistemas de IA. Por exemplo, no campo da saúde, o Espaço Europeu de Dados de Saúde facilitará o acesso não discriminatório a dados de saúde e o treinamento de algoritmos de IA com base nesses conjuntos de dados de forma segura, oportuna, transparente, confiável e respeitadora da privacidade, com governança institucional adequada. Autoridades competentes relevantes, incluindo as setoriais, que fornecem ou facilitam o acesso aos dados também podem apoiar o fornecimento de dados de alta qualidade para treinar, validar e testar sistemas de IA.

(69) O direito à privacidade e à proteção dos dados pessoais deve ser garantido durante todo o ciclo de vida dos dados. Sistema de IA. A este respeito, os princípios de minimização de dados e de proteção de dados desde a conceção e por defeito, tal como estabelecidos na legislação da União em matéria de proteção de dados, são aplicáveis quando são processados dados pessoais. As medidas tomadas pelos provedores para garantir a conformidade com esses princípios podem incluir não apenas a anonimização e a criptografia, mas também o uso de tecnologia que permita que algoritmos sejam aplicados aos dados e que sistemas de IA sejam treinados sem a necessidade de transmissão entre partes ou cópia de dados brutos ou estruturados, sem prejuízo dos requisitos de governança de dados estabelecidos neste Regulamento.

(70) A fim de proteger os direitos de terceiros contra a discriminação que possa resultar de preconceitos nos sistemas de IA, os prestadores devem – a título excecional, na medida estritamente necessária para garantir a deteção e correção de preconceitos associados a sistemas de IA de alto risco, sujeitos a salvaguardas adequadas para os direitos e liberdades fundamentais das pessoas singulares e após 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 – poder tratar também categorias especiais de dados pessoais, como uma questão de interesse público essencial 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) Para permitir a rastreabilidade dos sistemas de IA de alto risco, verificar a sua conformidade com os requisitos do presente regulamento, monitorizar o seu desempenho e efetuar a vigilância pós-comercialização, é essencial dispor de informações compreensíveis sobre a forma como foram desenvolvidos e sobre o seu desempenho ao longo do seu ciclo de vida. Para tanto, devem ser mantidos registros e deve estar disponível documentação técnica contendo as informações necessárias para avaliar se o sistema de IA em questão atende aos requisitos relevantes e para facilitar a vigilância pós-comercialização. Essas informações devem incluir as características gerais, capacidades e limitações do sistema e os algoritmos, dados e processos de treinamento, teste e validação utilizados, bem como documentação sobre o sistema de gerenciamento de riscos relevante, preparada de forma clara e completa. A documentação técnica deve ser mantida adequadamente atualizada durante toda a vida útil do sistema de IA. Além disso, os sistemas de IA de alto risco devem permitir tecnicamente o registro automático de eventos, usando arquivos de log, durante toda a vida útil do sistema.

(72) A fim de abordar as preocupações relacionadas com a opacidade e a complexidade de determinados sistemas de IA e ajudar os implementadores a cumprirem as suas obrigações ao abrigo do presente regulamento, deverá ser exigida transparência aos sistemas de IA de alto risco antes de serem colocados no mercado ou em serviço. Os sistemas de IA de alto risco devem ser projetados de forma que permitam que os implantadores entendam como o sistema de IA funciona, avaliem sua funcionalidade e entendam seus pontos fortes e limitações. Os sistemas de IA de alto risco devem ser acompanhados de informações apropriadas na forma de instruções de uso. Essas informações devem incluir as características, capacidades e limitações da operação do sistema de IA. Isso incluiria informações sobre circunstâncias potenciais conhecidas e previsíveis relacionadas ao uso do sistema de IA de alto risco, incluindo quaisquer ações do implantador capazes de influenciar o comportamento e a operação do sistema, sob as quais o sistema de IA pode dar origem a riscos à saúde, segurança e direitos fundamentais, sobre mudanças predeterminadas e avaliadas para conformidade pelo provedor e sobre medidas relevantes de supervisão humana, incluindo medidas para facilitar a interpretação dos resultados de saída do sistema de IA pelos implantadores. A transparência, incluindo instruções de uso que acompanham os sistemas de IA, deve ajudar os implantadores a usar o sistema e tomar decisões informadas. Os responsáveis pela implantação devem, entre outras coisas, estar mais bem posicionados para fazer a escolha correta do sistema que pretendem utilizar à luz das obrigações que lhes são aplicáveis, ser informados sobre os usos pretendidos e excluídos e utilizar o sistema de IA corretamente e conforme apropriado. A fim de melhorar a legibilidade e a acessibilidade das informações incluídas nas instruções de uso, exemplos ilustrativos, por exemplo, sobre limitações e sobre usos pretendidos e excluídos do sistema de IA, devem ser incluídos, quando apropriado. Os fornecedores devem garantir que toda a documentação, incluindo instruções de uso, contenha informações significativas, abrangentes, acessíveis e compreensíveis, levando em consideração as necessidades previsíveis e o conhecimento dos implantadores pretendidos. As instruções de utilização devem ser disponibilizadas numa linguagem facilmente compreensível pelos mobilizadores previstos, conforme decidido pelo Estado-Membro em causa.

(73) Os sistemas de IA de alto risco devem ser projetados e desenvolvidos de forma que pessoas físicas possam monitorar sua operação, garantir que sejam usados conforme pretendido e que seus impactos sejam abordados durante todo o ciclo de vida do sistema. Para isso, o fornecedor do sistema deve definir medidas adequadas de monitoramento humano antes de sua introdução no mercado ou comissionamento. Quando apropriado, tais medidas devem garantir, em particular, que o sistema esteja sujeito a limitações operacionais incorporadas no próprio sistema que não possam ser anuladas pelo sistema, que seja responsivo a um operador humano e que qualquer pessoa física encarregada da supervisão humana tenha as habilidades, o treinamento e a autoridade necessários para desempenhar essa função. Também é essencial, conforme apropriado, garantir que os sistemas de IA de alto risco incluam mecanismos para orientar e informar as pessoas físicas encarregadas da supervisão humana para que tomem decisões informadas sobre se, quando e como intervir, a fim de evitar consequências ou riscos negativos, ou para interromper o sistema se ele não funcionar conforme o esperado. Dadas as enormes consequências para os indivíduos no caso de uma correspondência incorreta feita por certos sistemas de identificação biométrica, é apropriado estabelecer um requisito para uma supervisão humana aprimorada para tais sistemas, de modo que o implantador não possa agir ou tomar qualquer decisão com base na identificação gerada pelo sistema, a menos que tenha sido verificada e confirmada separadamente por pelo menos duas pessoas físicas. Essas pessoas podem vir de uma ou mais entidades e incluir a pessoa que opera ou usa o sistema. Este requisito não deve criar encargos ou atrasos desnecessários e pode ser suficiente que as verificações realizadas separadamente por diferentes pessoas sejam automaticamente registradas nos registros gerados pelo sistema. Dadas as especificidades das áreas de aplicação da lei, migração, controlo de fronteiras e asilo, esse requisito não deverá aplicar-se quando a sua aplicação for considerada desproporcional ao abrigo do direito nacional ou da União.

(74) Os sistemas de IA de alto risco devem operar de forma consistente durante todo o seu ciclo de vida e exibir um nível apropriado de precisão, robustez e segurança cibernética, à luz da finalidade pretendida e de acordo com o estado da arte geralmente reconhecido. A Comissão e as organizações e partes interessadas relevantes são incentivadas a dar a devida consideração à mitigação dos riscos e impactos negativos do sistema de IA. O nível pretendido de parâmetros operacionais deve ser declarado nas instruções de uso que acompanham os sistemas de IA. Os fornecedores são incentivados a comunicar essas informações aos responsáveis pela implantação de forma clara e facilmente compreensível, sem mal-entendidos ou declarações enganosas. Direito da União em matéria de metrologia legal, incluindo a Diretiva 2014/31/UE ([35]) e 2014/32/UE ([36]) do Parlamento Europeu e do Conselho, visa garantir a precisão das medições e contribuir para a transparência e a equidade das transações comerciais. Nesse contexto, em cooperação com as partes interessadas e organizações relevantes, como autoridades de metrologia e de avaliação comparativa, a Comissão deve incentivar, conforme apropriado, o desenvolvimento de avaliações comparativas e metodologias de medição para sistemas de IA. Ao fazê-lo, a Comissão deve tomar nota e interagir com parceiros internacionais que trabalham em metrologia e indicadores de medição relevantes relacionados à IA.

([35]) Diretiva 2014/31/UE do Parlamento Europeu e do Conselho, de 26 de fevereiro de 2014, relativa à harmonização das legislações dos Estados-Membros respeitantes à colocação no mercado de instrumentos de pesagem não automáticos (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 das legislações dos Estados-Membros respeitantes à comercialização de instrumentos de medição (JO L 96 de 29.3.2014, p. 149).

(75) A robustez técnica é um requisito fundamental para sistemas de IA de alto risco, que devem ser resilientes a comportamentos prejudiciais ou indesejáveis que podem surgir de limitações nos sistemas ou no ambiente em que operam (por exemplo, erros, bugs, inconsistências ou situações inesperadas). Portanto, medidas técnicas e organizacionais devem ser tomadas para garantir a robustez dos sistemas de IA de alto risco, por exemplo, projetando e desenvolvendo soluções técnicas adequadas para prevenir ou minimizar esse comportamento prejudicial ou indesejável. Essas soluções técnicas podem incluir, por exemplo, mecanismos que permitam ao sistema interromper com segurança sua operação (planos de prevenção de falhas) na presença de determinadas anomalias ou quando a operação ocorrer fora de certos limites pré-determinados. A não adoção de medidas de proteção contra esses riscos pode ter consequências de segurança ou impactar negativamente direitos fundamentais, por exemplo, devido a decisões erradas ou resultados errôneos ou tendenciosos gerados pelo sistema de IA.

(76) A segurança cibernética é essencial para garantir que os sistemas de IA sejam resistentes às ações de terceiros mal-intencionados que, ao explorar vulnerabilidades do sistema, tentam alterar seu uso, comportamento ou operação ou comprometer suas propriedades de segurança. Os ataques cibernéticos contra sistemas de IA podem ter como alvo ativos de IA específicos, como conjuntos de dados de treinamento (por exemplo, envenenamento de dados) ou modelos treinados (por exemplo, ataques adversários ou inferência de associação).
ou explorar vulnerabilidades nos ativos digitais do sistema de IA ou na infraestrutura de TIC subjacente. Portanto, para garantir um nível de segurança cibernética adequado aos riscos, os provedores de sistemas de IA de alto risco devem tomar medidas adequadas, como controles de segurança, levando também em consideração, quando apropriado, a infraestrutura de TIC subjacente.

(77) Sem prejuízo dos requisitos relacionados com a robustez e a precisão estabelecidos no presente regulamento, os sistemas de IA de alto risco abrangidos pelo âmbito de um regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança para produtos que contenham elementos digitais, em conformidade com esse regulamento, podem demonstrar a conformidade com os requisitos de cibersegurança do presente regulamento através do cumprimento dos requisitos essenciais de cibersegurança estabelecidos nesse regulamento. Quando os sistemas de IA de alto risco cumprem os requisitos essenciais de segurança cibernética de um Regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de segurança cibernética para produtos que contenham elementos digitais, deve presumir-se que cumprem os requisitos de segurança cibernética do presente regulamento na medida em que a satisfação desses requisitos seja demonstrada na declaração de conformidade da UE emitida nos termos desse regulamento, ou em partes da mesma. Para esse fim, a avaliação dos riscos de segurança cibernética associados a um produto com elementos digitais classificado como um sistema de IA de alto risco nos termos do presente regulamento, realizada nos termos de um regulamento do Parlamento Europeu e do Conselho sobre requisitos horizontais de segurança cibernética para produtos com elementos digitais, deve levar em consideração os riscos para a resiliência cibernética de um sistema de IA no que diz respeito a tentativas de terceiros não autorizados de alterar sua utilização, comportamento ou operação, incluindo vulnerabilidades específicas da IA, como envenenamento de dados ou ataques adversários, bem como, quando aplicável, riscos para os direitos fundamentais, conforme exigido pelo presente regulamento.

(78) O procedimento de avaliação da conformidade estabelecido no presente regulamento deverá ser aplicado em relação aos requisitos essenciais de cibersegurança de um produto com elementos digitais regulamentado por um Regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança para produtos com elementos digitais e classificado como um sistema de IA de alto risco ao abrigo do presente regulamento. No entanto, esta regra não deve levar a uma redução no nível de garantia exigido para produtos críticos com elementos digitais sujeitos a um Regulamento do Parlamento Europeu e do Conselho sobre requisitos horizontais de segurança cibernética para produtos com elementos digitais. Por conseguinte, em derrogação ao presente regulamento, os sistemas de IA de alto risco abrangidos pelo âmbito do presente regulamento e que também são considerados produtos críticos importantes com elementos digitais ao abrigo de um Regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança para produtos com elementos digitais e aos quais se aplica o procedimento de avaliação da conformidade com base no controlo interno estabelecido num anexo ao presente regulamento estão sujeitos às disposições de um Regulamento do Parlamento Europeu e do Conselho relativo aos requisitos horizontais de cibersegurança para produtos com elementos digitais para avaliação da conformidade no que diz respeito aos requisitos essenciais de cibersegurança desse regulamento. Nesse caso, em relação a todos os outros aspetos abrangidos pelo âmbito de aplicação do presente regulamento, deverão aplicar-se as disposições do anexo VI do presente regulamento relativas à avaliação da conformidade com base no controlo interno. Tendo em conta a competência e a experiência da Agência da União Europeia para a Cibersegurança (ENISA) na política de cibersegurança e as tarefas que lhe são conferidas pelo Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho ([37]), a Comissão 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.°qualquer526/2013 («Regulamento sobre a Cibersegurança») (JO L 151 de 7.6.2019, p. 15).

(79) É adequado que uma pessoa singular ou coletiva específica, definida como o fornecedor, assuma a responsabilidade associada à colocação no mercado ou à colocação em serviço de um sistema de IA de alto risco, independentemente de essa pessoa singular ou coletiva ser ou não quem concebeu ou desenvolveu o sistema.

(80) Como signatários da Convenção sobre os Direitos das Pessoas com Deficiência, a União e todos os Estados-Membros são legalmente obrigados a proteger as pessoas com deficiência contra a discriminação e a promover a sua igualdade, a garantir que as pessoas com deficiência tenham acesso, em igualdade de condições com as demais, às tecnologias e sistemas de informação e comunicação, e a garantir o respeito pela privacidade das pessoas com deficiência. Dada a crescente importância e uso de sistemas de IA, a aplicação dos princípios de design universal a todas as novas tecnologias e serviços deve garantir acesso total e igualitário para todas as pessoas que podem ser afetadas ou usar tecnologias de IA, incluindo pessoas com deficiência, de uma maneira que leve totalmente em consideração sua dignidade e diversidade inerentes. É, portanto, essencial que os prestadores garantam o cumprimento integral dos requisitos de acessibilidade, incluindo a Diretiva (UE) 2016/2102 do Parlamento Europeu e do Conselho ([38]) e a Diretiva (UE) 2019/882. Os fornecedores devem garantir a conformidade com esses requisitos desde o projeto. Portanto, as medidas necessárias devem ser integradas, tanto quanto possível, ao design de sistemas de IA de alto risco.

(81) O fornecedor deve estabelecer um sistema de gestão de qualidade robusto, garantir que o procedimento de avaliação de conformidade necessário seja seguido, preparar a documentação relevante e estabelecer um sistema robusto de vigilância pós-comercialização. Os fornecedores de sistemas de IA de alto risco que estejam sujeitos a obrigações relacionadas com sistemas de gestão da qualidade ao abrigo da legislação setorial da União aplicável deverão ter a possibilidade de integrar os elementos do sistema de gestão da qualidade estabelecidos no presente regulamento no sistema de gestão da qualidade estabelecido nessa legislação setorial da União. A complementaridade entre o presente regulamento e a legislação setorial vigente na União também deverá ser tida em conta em futuras atividades de normalização ou em quaisquer orientações adotadas pela Comissão a este respeito. As autoridades públicas que colocam sistemas de IA de alto risco em serviço para seu próprio uso podem adotar e implementar regras que regem o sistema de gestão da qualidade no âmbito do sistema de gestão da qualidade adotado a nível nacional ou regional, conforme o caso, levando em consideração as particularidades do setor e as competências e organização da autoridade pública em questão.

(82) Para permitir a implementação deste regulamento e proporcionar condições equitativas aos operadores, é importante garantir que uma pessoa estabelecida na União possa, em quaisquer circunstâncias, fornecer às autoridades todas as informações necessárias sobre a conformidade de um sistema de IA, tendo em conta as diferentes formas pelas quais os produtos digitais podem ser oferecidos. Portanto, antes de colocarem os seus sistemas de IA no mercado da União, os prestadores estabelecidos fora do seu território devem nomear, por meio de um mandato escrito, um representante autorizado localizado na União. O representante autorizado desempenha um papel fundamental para garantir a conformidade dos sistemas de IA de alto risco colocados no mercado ou em serviço na União por fornecedores não estabelecidos na União e atua como pessoa de contato estabelecida na União.

(83) Considerando a natureza e a complexidade da cadeia de valor dos sistemas de IA e de acordo com o novo quadro legislativo, é essencial garantir a segurança jurídica e facilitar o cumprimento do presente Regulamento. Portanto, é necessário esclarecer o papel e as obrigações específicas dos operadores relevantes em toda a cadeia de valor, como importadores e distribuidores, que podem contribuir para o desenvolvimento de sistemas de IA. Em determinadas situações, esses operadores podem desempenhar mais de uma função ao mesmo tempo e, portanto, devem cumprir cumulativamente todas as obrigações relevantes associadas a essas funções. Por exemplo, um operador pode atuar como distribuidor e importador ao mesmo tempo.

(84) Para garantir a segurança jurídica, é necessário esclarecer que, sob certas condições específicas, qualquer distribuidor, importador, implantador ou outro terceiro deve ser considerado um fornecedor de um sistema de IA de alto risco e, portanto, deve assumir todas as obrigações relevantes. Este seria o caso se, por exemplo, essa pessoa colocasse seu nome ou marca registrada em um sistema de IA de alto risco já colocado no mercado ou em serviço, sem prejuízo de acordos contratuais que estipulassem outra distribuição de obrigações.
Este também seria o caso se essa Parte modificasse substancialmente um sistema de IA de alto risco que já tenha sido colocado no mercado ou em serviço, de tal forma que o sistema modificado continue sendo um sistema de IA de alto risco, de acordo com o presente Regulamento, ou se modificasse a finalidade pretendida de um sistema de IA, como um sistema de IA de uso geral, que já tenha sido colocado no mercado ou em serviço e não seja classificado como um sistema de alto risco, de tal forma que o sistema modificado se torne um sistema de IA de alto risco, de acordo com o presente Regulamento. Estas disposições deverão aplicar-se sem prejuízo de disposições mais específicas estabelecidas em determinados atos legislativos de harmonização da União com base no novo quadro legislativo a aplicar em conjunto com o presente regulamento. Por exemplo, o

([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 dos organismos do setor público (JO L 327 de 2.12.2016, p. 1).

O artigo 16.º, n.º 2, do Regulamento (UE) 2017/745, que prevê que determinadas alterações não devem ser consideradas modificações de um dispositivo que possam afetar a conformidade com os requisitos aplicáveis, deve continuar a aplicar-se aos sistemas de IA de alto risco que sejam dispositivos médicos na aceção desse regulamento.

(85) Os sistemas de IA de uso geral podem ser usados como sistemas de IA de alto risco por conta própria ou ser componentes de sistemas de IA de alto risco. Por conseguinte, devido à sua natureza particular e a fim de assegurar uma partilha justa de responsabilidades ao longo de toda a cadeia de valor, os fornecedores desses sistemas, independentemente de poderem ser utilizados como sistemas de IA de alto risco por outros fornecedores ou como componentes de sistemas de IA de alto risco, e salvo disposição em contrário no presente regulamento, devem cooperar estreitamente com os fornecedores dos sistemas de IA de alto risco relevantes, a fim de lhes permitir cumprir as obrigações relevantes ao abrigo do presente regulamento.
bem como com as autoridades competentes estabelecidas nos termos do presente Regulamento.

(86) Sempre que, nas condições estabelecidas no presente regulamento, o fornecedor que inicialmente colocou o sistema de IA no mercado ou o colocou em serviço deixar de ser considerado fornecedor para efeitos do presente regulamento, e sempre que esse fornecedor não tenha expressamente excluído a transformação do sistema de IA num sistema de IA de alto risco, o primeiro fornecedor deve, no entanto, cooperar estreitamente, fornecer as informações necessárias e fornecer o acesso técnico ou outra assistência que possa ser razoavelmente esperada e que seja 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 alto risco.

(87) Além disso, quando um sistema de IA de alto risco que seja um componente de segurança de um produto abrangido pelo âmbito de um ato legislativo de harmonização da União com base no novo quadro legislativo não for colocado no mercado ou colocado em serviço independentemente do produto, o fabricante do produto, conforme definido no ato legislativo relevante, deverá cumprir as obrigações impostas ao fornecedor pelo presente regulamento e, em particular, deverá garantir que o sistema de IA incorporado no produto final cumpra os requisitos do presente regulamento.

(88) Ao longo da cadeia de valor da IA, diversas partes geralmente fornecem não apenas sistemas, ferramentas e serviços de IA, mas também componentes ou processos que o fornecedor incorpora ao sistema de IA para vários propósitos, como treinamento de modelos, retreinamento de modelos, teste e avaliação de modelos, integração ao sistema de IA e assim por diante.Programasou outros aspectos do desenvolvimento do modelo. Essas partes desempenham um papel importante na cadeia de valor em relação ao fornecedor do sistema de IA de alto risco no qual seus sistemas, ferramentas, serviços, componentes ou processos de IA estão integrados e devem fornecer a esse fornecedor, por meio de acordo por escrito, as informações, capacidades, acesso técnico e outra assistência necessária, levando em consideração o estado da arte geralmente reconhecido, para permitir que o fornecedor cumpra integralmente as obrigações estabelecidas no presente regulamento, sem comprometer seus próprios direitos de propriedade intelectual ou segredos comerciais.

(89) Terceiros que disponibilizam publicamente ferramentas, serviços, processos ou componentes de IA que não sejam modelos de IA de uso geral não devem ser obrigados a cumprir requisitos relacionados a responsabilidades ao longo da cadeia de valor da IA, em particular no que diz respeito ao provedor que usou ou integrou tais ferramentas, serviços, processos ou componentes de IA, onde o acesso a tais ferramentas, serviços, processos ou componentes de IA está sujeito a uma licença gratuita e de código aberto. No entanto, os desenvolvedores de ferramentas, serviços, processos ou componentes de IA gratuitos e de código aberto que não sejam modelos de IA de uso geral devem ser incentivados a aplicar práticas de documentação amplamente adotadas, como cartões de modelo e folhas de dados, como forma de acelerar a troca de informações ao longo da cadeia de valor da IA, permitindo a promoção de sistemas de IA confiáveis na União.

(90) A Comissão poderia desenvolver e recomendar cláusulas contratuais padrão voluntárias entre fornecedores de sistemas de IA de alto risco e terceiros que forneçam ferramentas, serviços, componentes ou processos a serem usados ou integrados em sistemas de IA de alto risco, a fim de facilitar a cooperação ao longo da cadeia de valor. Ao desenvolver essas cláusulas contratuais padrão voluntárias, a Comissão também deve levar em consideração possíveis requisitos contratuais aplicáveis em determinados setores ou modelos de negócios.

(91) Dadas as características dos sistemas de IA e os riscos que a sua utilização acarreta para a segurança e os direitos fundamentais, também no que se refere à necessidade de garantir um acompanhamento adequado do funcionamento de um sistema de IA num ambiente real, é conveniente estabelecer as responsabilidades específicas dos responsáveis pela sua implementação. Em particular, os implantadores devem tomar medidas técnicas e organizacionais adequadas para garantir que usam sistemas de IA de alto risco de acordo com as instruções de uso. Além disso, outras obrigações precisam ser definidas em relação ao monitoramento da operação dos sistemas de IA e à manutenção de registros, conforme apropriado. Além disso, os responsáveis pela implementação deverão garantir que as pessoas responsáveis pela implementação das instruções de utilização e pela supervisão humana estabelecidas no presente regulamento tenham as competências necessárias, em especial um nível adequado de literacia,

treinamento e autoridade em IA para executar adequadamente essas tarefas. Tais obrigações não devem prejudicar outras obrigações que o implantador tenha em relação a sistemas de IA de alto risco, nos termos da legislação nacional ou da União.

(92) O presente regulamento não prejudica a obrigação dos empregadores de informar ou de informar e consultar os trabalhadores ou os seus representantes, nos termos da legislação ou das práticas da União ou nacionais, incluindo a Diretiva 2002/14/CE do Parlamento Europeu e do Conselho ([39]), sobre a decisão de colocar em serviço ou utilizar sistemas de IA. Os trabalhadores e seus representantes devem ser informados sobre a implantação planejada de sistemas de IA de alto risco no local de trabalho, mesmo que as condições das obrigações de informação acima mencionadas ou das obrigações de informação e consulta previstas em outros instrumentos legais não sejam cumpridas. Além disso, este direito à informação é acessório e necessário para o objetivo de proteção dos direitos fundamentais subjacentes ao presente Regulamento. Por conseguinte, deverá ser estabelecido no presente regulamento um requisito de informação para este efeito, sem afetar quaisquer direitos existentes dos trabalhadores.

(93) Embora os riscos associados aos sistemas de IA possam surgir de seu design, os riscos também podem surgir da maneira como são usados. Os responsáveis pela implantação de um sistema de IA de alto risco desempenham, portanto, um papel fundamental na garantia da proteção dos direitos fundamentais, como complemento às obrigações do fornecedor no desenvolvimento do sistema de IA. Os implantadores estão em melhor posição para entender o uso específico que o sistema de IA de alto risco terá e, portanto, podem detectar riscos potenciais significativos que não foram previstos na fase de desenvolvimento, tendo uma compreensão mais precisa do contexto de uso e dos indivíduos ou grupos de indivíduos que provavelmente serão afetados, incluindo grupos vulneráveis. Os responsáveis pela implementação de sistemas de IA de alto risco enumerados num anexo ao presente regulamento também desempenham um papel fundamental na informação das pessoas singulares e, ao tomarem decisões ou prestarem assistência na tomada de decisões relativas a pessoas singulares, devem, quando aplicável, informar as pessoas singulares de que são objeto da utilização de um sistema de IA de alto risco. Essas informações devem incluir a finalidade pretendida e o tipo de decisões que estão sendo tomadas. O responsável pela mobilização deverá também informar as pessoas singulares sobre o seu direito a uma explicação ao abrigo do presente regulamento. No que diz respeito aos sistemas de IA de alto risco utilizados para fins de execução, essa obrigação deverá ser implementada em conformidade com o artigo 13.º da Diretiva (UE) 2016/680.

(94) Qualquer processamento de dados biométricos em conexão com o uso de um sistema de IA para identificação biométrica para fins de aplicação da lei deve estar em conformidade com o Artigo 10 da Diretiva (UE) 2016/680, que permite tal processamento somente quando estritamente necessário, sujeito a salvaguardas adequadas para os direitos e liberdades do titular dos dados e quando autorizado pela legislação da União ou do Estado-Membro. Tal utilização, quando autorizada, deve também respeitar os princípios estabelecidos no artigo 4.º, n.º 1, da Diretiva (UE) 2016/680, tais como, entre outros, o tratamento lícito e leal, a transparência, a limitação da finalidade, a exatidão e a limitação do período de conservação.

(95) Sem prejuízo da legislação aplicável da União, em especial o Regulamento (UE) 2016/679 e a Diretiva (UE) 2016/680, tendo em conta a natureza intrusiva dos sistemas de identificação biométrica diferida remota, a utilização de tais sistemas deverá estar sujeita a salvaguardas. Os sistemas de identificação biométrica remota devem ser sempre utilizados de forma proporcional e legítima, na medida do estritamente necessário e, portanto, de forma seletiva em relação às pessoas a serem identificadas, à localização e ao escopo temporal e com base em um conjunto limitado de dados de gravações de vídeo obtidas legalmente. Em qualquer caso, os sistemas de identificação biométrica remota não devem ser utilizados no contexto de garantia do cumprimento da lei de forma que ocorra vigilância indiscriminada. As condições para a identificação biométrica remota de forma diferida não devem, em caso algum, servir para contornar as condições de proibição e as exceções estritas aplicáveis à identificação biométrica remota em tempo real.

(96) Para garantir efetivamente a proteção dos direitos fundamentais, os responsáveis pela implantação de sistemas de IA de alto risco que sejam organismos de direito público ou entidades privadas que prestem serviços públicos, e os responsáveis pela implantação de determinados sistemas de IA de alto risco listados num anexo ao presente regulamento, como entidades bancárias ou seguradoras, devem realizar uma avaliação de impacto nos direitos fundamentais antes da sua implantação. Alguns serviços importantes para as pessoas que são de natureza pública também podem ser prestados por entidades privadas. As entidades privadas que prestam esses serviços públicos estão vinculadas a funções de interesse público, por exemplo, nas áreas de educação, saúde, serviços sociais, habitação e administração da justiça. O objetivo da avaliação de impacto sobre direitos fundamentais é que o implementador identifique os riscos específicos aos direitos de indivíduos ou grupos de indivíduos que provavelmente serão afetados e defina as medidas a serem tomadas caso esses riscos se materializem. A avaliação de impacto deve

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

ser realizada antes da implantação do sistema de IA de alto risco e deve ser atualizada quando o implantador considerar que algum dos fatores relevantes mudou. A avaliação de impacto deve identificar os processos relevantes do implementador nos quais o sistema de IA de alto risco será usado de acordo com sua finalidade pretendida e deve incluir uma descrição do período e da frequência em que o sistema deve ser usado, bem como as categorias específicas de pessoas físicas e grupos de pessoas que provavelmente serão afetadas pelo uso do sistema de IA de alto risco naquele contexto específico de uso. A avaliação também deve identificar os riscos específicos de danos que podem afetar os direitos fundamentais de tais indivíduos ou grupos. Ao realizar esta avaliação, o implementador deve levar em consideração informações relevantes para uma avaliação de impacto adequada, incluindo, por exemplo, informações fornecidas pelo fornecedor do sistema de IA de alto risco nas instruções de uso. À luz dos riscos identificados, os implantadores devem determinar as medidas a serem tomadas caso tais riscos se materializem, incluindo, por exemplo, sistemas de governança para aquele contexto de uso específico, como mecanismos de supervisão humana de acordo com as instruções de uso, tratamento de reclamações e procedimentos de reparação, pois estes podem ser essenciais para mitigar riscos aos direitos fundamentais em casos de uso específicos. Após a conclusão de tal avaliação de impacto, o implantador deve notificar a autoridade de vigilância de mercado relevante. Quando apropriado, para reunir informações relevantes necessárias para realizar a avaliação de impacto, os responsáveis pela implantação de um sistema de IA de alto risco, em particular quando o sistema de IA for usado no setor público, podem envolver as partes interessadas relevantes, como representantes de grupos de pessoas que provavelmente serão afetadas pelo sistema de IA, especialistas independentes ou organizações da sociedade civil, na realização dessas avaliações de impacto e na concepção das medidas a serem tomadas caso os riscos se materializem. O Gabinete Europeu de Inteligência Artificial (a seguir designado por «Gabinete de IA») deverá desenvolver um modelo de questionário para facilitar o cumprimento e reduzir os encargos administrativos para os responsáveis pela implementação.

(97) O conceito de modelos de IA de uso geral deve ser claramente definido e diferenciado do conceito de sistemas de IA para garantir a segurança jurídica. A definição deve ser baseada nas características funcionais essenciais de um modelo de IA de propósito geral, em particular a generalidade e a capacidade de executar com competência uma ampla variedade de tarefas diferenciadas. Esses modelos geralmente são treinados usando grandes volumes de dados e por meio de uma variedade de métodos, como aprendizado autossupervisionado, não supervisionado ou por reforço. Modelos de IA de uso geral podem ser introduzidos no mercado de diversas maneiras, por exemplo, por meio de bibliotecas, interfaces de programação de aplicativos (APIs), como download direto ou como cópia física. Esses modelos podem ser modificados ou refinados e transformados em novos modelos. Embora os modelos de IA sejam componentes essenciais dos sistemas de IA, eles não constituem sistemas de IA por si só. Os modelos de IA exigem a adição de outros componentes, como uma interface de usuário, para se tornarem sistemas de IA. Os modelos de IA geralmente são incorporados e fazem parte dos sistemas de IA. O presente regulamento estabelece regras específicas para modelos de IA de uso geral e para modelos de IA de uso geral que impliquem riscos sistémicos, as quais também deverão ser aplicáveis quando estes modelos estiverem integrados num sistema de IA ou fizerem parte de um sistema de IA. Deve-se entender que as obrigações dos provedores de modelos de IA de uso geral devem ser aplicadas quando os modelos de IA de uso geral forem introduzidos no mercado. Quando o fornecedor de um modelo de IA de uso geral integra um modelo proprietário em um sistema de IA proprietário que é colocado no mercado ou colocado em serviço, esse modelo deve ser considerado como tendo sido colocado no mercado e, portanto, as obrigações estabelecidas no presente regulamento em relação aos modelos devem continuar a ser aplicáveis, além daquelas estabelecidas em relação aos sistemas de IA. Em qualquer caso, as obrigações estabelecidas em relação aos modelos não devem ser aplicadas quando um modelo proprietário for utilizado em processos puramente internos que não sejam essenciais para fornecer um produto ou serviço a terceiros e os direitos das pessoas físicas não sejam afetados. Considerando seu potencial para causar efeitos negativos significativos,

Os modelos de IA de uso geral com risco sistémico deverão estar sempre sujeitos às obrigações relevantes estabelecidas no presente regulamento. A definição não deve incluir modelos de IA usados antes da introdução no mercado apenas para atividades de pesquisa, desenvolvimento e prototipagem. O acima exposto não prejudica a obrigação de cumprimento das disposições do presente regulamento quando, após a realização dessas atividades, o modelo for colocado no mercado.

(98) Embora a generalidade de um modelo também possa ser determinada, entre outras coisas, por um conjunto de parâmetros, modelos que têm pelo menos um bilhão de parâmetros e foram treinados em um grande volume de dados usando autossupervisão em escala devem ser considerados como tendo um grau significativo de generalidade e executando com competência uma ampla variedade de tarefas discretas.

(99) Grandes modelos de IA generativa são um exemplo típico de um modelo de IA de propósito geral, pois permitem a geração flexível de conteúdo, por exemplo, em formato de texto, áudio, imagem ou vídeo, que pode ser facilmente adaptado a uma ampla gama de tarefas diferenciadas.

(100) Quando um modelo de IA de uso geral é integrado ou faz parte de um sistema de IA, este sistema deve ser considerado um sistema de IA de uso geral quando, devido a esta integração, o sistema tem a capacidade de servir múltiplos propósitos. Um sistema de IA de uso geral pode ser usado diretamente e integrado a outros sistemas de IA.

(101) Os fornecedores de modelos de IA para fins gerais têm um papel e uma responsabilidade específicos ao longo da cadeia de valor da IA, uma vez que os modelos que fornecem podem constituir a base de vários sistemas a jusante, que são frequentemente fornecidos por fornecedores 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 ao abrigo do presente regulamento ou de outros regulamentos. Portanto, medidas de transparência proporcionais devem ser colocadas em prática, incluindo o desenvolvimento e a manutenção de documentação atualizada e o fornecimento de informações sobre o modelo de IA de uso geral para uso por provedores posteriores. O fornecedor do modelo de IA de uso geral deve desenvolver e manter documentação técnica atualizada para disponibilizá-la, mediante solicitação, ao Escritório de IA e às autoridades nacionais competentes. Os elementos mínimos que tal documentação deve conter devem ser estabelecidos em anexos específicos ao presente Regulamento. A Comissão deverá ter poderes para alterar esses anexos por meio de atos delegados, à luz da evolução tecnológica.

(102) OPrograma se dados, incluindo modelos, divulgados sob uma licença livre e de código aberto que permite compartilhamento aberto e acesso do usuário, ou versões modificadas desses dados. Programase esses dados, ou a livre utilização, modificação e redistribuição desses dados, podem contribuir para a investigação e a inovação no mercado e podem oferecer oportunidades de crescimento significativas para a economia da União. Modelos de IA de uso geral divulgados sob uma licença gratuita e de código aberto devem ser considerados para garantir altos níveis de transparência e abertura se seus parâmetros, incluindo pesos, informações sobre a arquitetura do modelo e informações sobre o uso do modelo, forem disponibilizados publicamente. A licença deve ser considerada livre e de código aberto quando permite aos usuários executar, copiar, distribuir, estudar, modificar e melhorar o Programase dados, incluindo modelos, desde que o fornecedor original do modelo seja citado, se condições de distribuição idênticas ou comparáveis forem respeitadas.

(103) Os componentes de IA livres e de código aberto incluem:Programase dados, incluindo modelos e modelos de IA de uso geral, ferramentas, serviços e processos de um sistema de IA. Componentes de IA gratuitos e de código aberto podem ser entregues por meio de diferentes canais, incluindo a possibilidade de desenvolvê-los em repositórios abertos. Para efeitos do presente regulamento, os componentes de IA que são fornecidos mediante pagamento ou monetizados de outra forma, como através da prestação de apoio técnico ou de outros serviços relacionados com o componente de IA, seja através de uma plataforma de pagamento ou de um prestador de serviços, serão considerados como tais componentes.Programasou por outros meios, ou utilizando dados pessoais para fins que não estejam relacionados exclusivamente com a melhoria da segurança, compatibilidade ou interoperabilidade dosoftware,Exceto no caso de transações entre microempresas, elas não devem ser elegíveis para as exceções previstas para componentes de IA gratuitos e de código aberto. A disponibilidade de um componente de IA por meio de repositórios abertos não deve, por si só, constituir monetização.

(104) Os fornecedores de modelos de IA para fins gerais divulgados ao abrigo de uma licença livre e de código aberto cujos parâmetros, incluindo pesos, informações sobre a arquitetura do modelo e informações sobre a utilização do modelo, sejam disponibilizados publicamente devem estar sujeitos a exceções aos requisitos de transparência impostos aos modelos de IA para fins gerais, a menos que possam ser considerados como apresentando um risco sistémico, caso em que o facto de o modelo ser transparente e ser acompanhado de uma licença de código aberto não deve ser considerado uma razão suficiente para que seja isento das obrigações estabelecidas no presente regulamento. Em qualquer caso, uma vez que a divulgação de modelos de IA para fins gerais ao abrigo de uma licença livre e de código aberto não revela necessariamente informações substanciais sobre o conjunto de dados utilizado para treinar ou ajustar o modelo ou sobre a forma como foi garantida a conformidade com a legislação em matéria de direitos de autor, a exceção prevista para modelos de IA para fins gerais em relação à conformidade com os requisitos de transparência não deve isentar da obrigação de fornecer um resumo do conteúdo utilizado para treinar o modelo ou da obrigação de adotar orientações para a conformidade com a legislação da União em matéria de direitos de autor, em especial para identificar e respeitar a reserva de direitos prevista no artigo 4.º, n.º 3, da Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho (40).

(105) Modelos de IA de uso geral, em particular modelos de IA generativos de grande dimensão, capazes de gerar texto, Imagens e outros conteúdos apresentam oportunidades únicas de inovação, mas também desafiam artistas, autores e outros criadores e a maneira como seu conteúdo criativo é criado, distribuído, usado e consumido. O desenvolvimento e o treinamento desses modelos exigem acesso a grandes quantidades de texto, imagens, vídeos e outros dados. Técnicas de mineração de texto e dados podem ser amplamente utilizadas neste contexto para a recuperação e análise de tal conteúdo, que pode ser protegido por direitos autorais e direitos conexos. Qualquer uso de conteúdo protegido por direitos autorais requer a permissão do detentor dos direitos autorais, a menos que exceções e limitações de direitos autorais aplicáveis se apliquem. A Diretiva (UE) 2019/790 introduziu exceções e limitações que permitem reproduções e extrações de obras e outros materiais para fins de mineração de texto e dados em determinadas circunstâncias. Com arranjo

(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).

De acordo com essas regras, os detentores de direitos autorais podem optar por reservar seus direitos em relação às suas obras ou outras execuções, a fim de impedir a prospecção de textos e dados, a menos que sua finalidade seja a pesquisa científica. Quando o detentor dos direitos autorais tiver reservado adequadamente o direito de excluir, os provedores de modelos de IA de uso geral devem obter a permissão do detentor dos direitos autorais para conduzir mineração de texto e dados em tais obras.

(106) Os fornecedores que colocam modelos de IA para fins gerais no mercado da União devem garantir o cumprimento das obrigações relevantes estabelecidas no presente regulamento. Para esse efeito, os fornecedores de modelos de IA de uso geral devem adotar diretrizes para a conformidade com a legislação da União em matéria de direitos de autor e direitos conexos, em especial para detetar 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 fornecedor que coloque um modelo de IA de uso geral no mercado da União deve cumprir esta obrigação, independentemente da jurisdição em que ocorrem os atos de direitos autorais relevantes que sustentam o treinamento de tais modelos de IA de uso geral. Esta medida é necessária para garantir condições equitativas entre os fornecedores de modelos de IA de uso geral, o que impede que um fornecedor obtenha uma vantagem competitiva no mercado da União ao aplicar regras de direitos autorais menos rigorosas do que as previstas na União.

(107) A fim de aumentar a transparência relativamente aos dados utilizados no pré-treino e no treino de modelos de IA de uso geral, incluindo textos e dados protegidos por lei de direitos de autor, é adequado que os fornecedores desses modelos desenvolvam e disponibilizem publicamente um resumo suficientemente detalhado do conteúdo utilizado para o treino do modelo de IA de uso geral. Este resumo deve levar em conta a necessidade de proteger segredos comerciais e informações comerciais confidenciais, sendo, ao mesmo tempo, abrangente em escopo e não tecnicamente detalhado, a fim de facilitar que as partes com interesses legítimos, incluindo detentores de direitos autorais, exerçam e façam valer seus direitos sob a legislação da União, por exemplo, listando os principais conjuntos ou coleções de dados que foram usados para treinar o modelo, como arquivos ou bancos de dados de big data privados ou públicos, e fornecendo uma explicação descritiva de outras fontes de dados usadas. É apropriado que o IA Office forneça um modelo para o resumo, que deve ser simples e eficaz e permitir que o provedor forneça o resumo necessário de forma descritiva.

(108) No que diz respeito às obrigações impostas aos fornecedores de modelos de IA para fins gerais de adotarem diretrizes para a conformidade com a legislação da União em matéria de direitos de autor e de disponibilizarem publicamente um resumo do conteúdo utilizado para a formação, o Instituto de IA deverá monitorizar se o fornecedor cumpriu essas obrigações sem verificar ou efetuar uma avaliação trabalho a trabalho dos dados de formação para efeitos de conformidade com os direitos de autor. O presente regulamento não afeta o cumprimento das regras de direitos de autor previstas no direito da União.

(109) O cumprimento das obrigações aplicáveis aos fornecedores de modelos de IA para fins gerais deverá ser proporcional e adequado ao tipo de fornecedor de modelos. Pessoas que desenvolvem ou utilizam modelos para fins de pesquisa não profissionais ou científicas devem ser isentas da obrigação de cumprimento. No entanto, essas pessoas devem ser incentivadas a cumprir esses requisitos voluntariamente. Sem prejuízo da legislação da União sobre direitos autorais, o cumprimento dessas obrigações deve levar em conta o tamanho do provedor e permitir formas simplificadas de conformidade para PMEs, incluindo start-ups, o que não deve implicar custos excessivos ou desencorajar o uso de tais modelos. No caso de modificação ou ajuste de um modelo, as obrigações dos fornecedores de modelos de IA de uso geral devem limitar-se a essa modificação ou a esses ajustes, por exemplo, complementando a documentação técnica existente com informações sobre as modificações, incluindo novas fontes de dados de treinamento, para cumprir as obrigações da cadeia de valor estabelecidas no presente regulamento.

(110) Os modelos de IA para fins gerais podem representar riscos sistémicos, por exemplo, quaisquer efeitos negativos reais ou razoavelmente previsíveis em relação a acidentes graves, perturbações de setores críticos e consequências graves para a saúde e segurança públicas, quaisquer efeitos negativos reais ou razoavelmente previsíveis nos processos democráticos e na segurança pública e económica ou a divulgação de conteúdos ilegais, falsos ou discriminatórios. Deve-se entender que os riscos sistêmicos aumentam com as capacidades e o alcance dos modelos, podem surgir ao longo do ciclo de vida do modelo e são influenciados por condições de uso indevido, confiabilidade do modelo, justiça e segurança do modelo, nível de autonomia do modelo, seu acesso a ferramentas, modalidades novas ou combinadas, estratégias de disseminação e distribuição, possibilidade de remoção de salvaguardas e outros fatores. Em particular, as abordagens internacionais até à data estabeleceram a necessidade de prestar atenção aos riscos decorrentes de potenciais problemas de utilização indevida intencional ou de controlo relacionados com a harmonização com a intenção humana não intencional, com os riscos químicos, biológicos, radiológicos e nucleares, bem como com as formas como as barreiras à entrada podem ser reduzidas, bem como com as

para o desenvolvimento, design, aquisição ou uso de armas; capacidades cibernéticas ofensivas, como as formas pelas quais vulnerabilidades podem ser descobertas, exploradas ou usadas operacionalmente; os efeitos da interação e uso de ferramentas, incluindo, por exemplo, a capacidade de controlar sistemas físicos e interferir na operação de infraestrutura crítica; os riscos decorrentes de modelos que fazem cópias de si mesmos ou "auto-replicam" ou treinam outros modelos; as formas pelas quais os modelos podem dar origem a preconceitos e discriminação prejudiciais que representam riscos para indivíduos, comunidades ou sociedades; a facilitação de desinformação ou violação de privacidade, que ameaçam valores democráticos e direitos humanos; o risco de que um único evento possa desencadear uma reação em cadeia com efeitos negativos significativos que podem até afetar uma cidade inteira, um campo inteiro de atividade ou uma comunidade inteira.

(111) É adequado estabelecer uma metodologia para a classificação de modelos de IA de uso geral como modelos de IA de uso geral com riscos sistémicos. Como os riscos sistêmicos surgem de capacidades particularmente altas, um modelo de IA de uso geral deve ser considerado como apresentando riscos sistêmicos se tiver capacidades de alto impacto – avaliadas usando ferramentas e metodologias técnicas apropriadas – ou impactos significativos no mercado interno devido ao seu escopo. Capacidades de alto impacto em modelos de IA de uso geral são capacidades que correspondem ou excedem as capacidades demonstradas pelos modelos de IA de uso geral mais avançados. A introdução de um modelo no mercado ou as interações dos responsáveis pela sua implantação com ele permitem uma melhor compreensão de todas as suas capacidades. De acordo com o estado da arte no momento da entrada em vigor do presente regulamento, a quantidade cumulativa de computação utilizada para treinar o modelo de IA de uso geral, medida em operações de ponto flutuante, é uma das aproximações relevantes para as capacidades do modelo. A quantidade cumulativa de computação usada para treinamento inclui cálculos usados em várias atividades e métodos destinados a melhorar as capacidades do modelo antes da implantação, como pré-treinamento, geração de dados sintéticos e execução de ajustes finos. Portanto, deve ser definido um limite inicial de operações de ponto flutuante que, se atingido por um modelo de IA de uso geral, resultaria na presunção de que o modelo é um modelo de IA de uso geral com riscos sistêmicos. Esse limite deve ser ajustado para refletir mudanças tecnológicas e industriais, como melhorias algorítmicas ou maior eficiência de hardware, e deve ser complementado por benchmarks e indicadores de capacidade do modelo. Para informar isso, o AI Office deve se envolver com a comunidade científica, a indústria, a sociedade civil e outros especialistas. Limites, bem como ferramentas e referências para avaliar capacidades de alto impacto, devem ser capazes de prever de forma confiável a generalidade, as capacidades e o risco sistêmico associado aos modelos de IA de uso geral, e podem levar em consideração como o modelo será introduzido no mercado ou o número de usuários que ele pode impactar. Para complementar este sistema, a Comissão deve poder adotar decisões individuais que designem um modelo de IA de uso geral como um modelo de IA de uso geral com risco sistémico, se for determinado que tal modelo tem capacidades ou impactos equivalentes aos refletidos pelo limiar estabelecido.Essa decisão deve ser tomada levando em consideração uma avaliação geral dos critérios para a designação de modelos de IA de uso geral com risco sistémico estabelecidos em um anexo ao presente regulamento, como a qualidade ou o tamanho do conjunto de dados de treinamento, o número de profissionais e usuários finais, seus modos de entrada e saída, seu nível de autonomia e escalabilidade ou as ferramentas às quais têm acesso. Mediante solicitação fundamentada de um provedor cujo modelo foi designado como um modelo de IA de uso geral com risco sistêmico, a Comissão deve levar em consideração a solicitação e pode decidir reavaliar se o modelo de IA de uso geral pode continuar a ser considerado como apresentando riscos sistêmicos.

(112) É também necessário clarificar um procedimento para classificar um modelo de IA de uso geral com riscos sistémicos. Um modelo de IA de uso geral que atenda ao limite aplicável para capacidades de alto impacto deve ser presumido como um modelo de IA de uso geral com risco sistêmico. O provedor deve enviar uma notificação ao AI Office no máximo duas semanas após os requisitos serem atendidos ou se tornar conhecido que um modelo de IA de uso geral atenderá aos requisitos que levam à presunção. Isso é especialmente relevante em relação ao limite de operações de ponto flutuante, uma vez que o treinamento de modelos de IA de uso geral exige um planejamento considerável, incluindo pré-alocação de recursos computacionais e, portanto, os provedores de modelos de IA de uso geral podem saber se seu modelo atingirá o limite antes do final do treinamento. No contexto dessa notificação, o provedor deve ser capaz de demonstrar que, devido às suas características específicas, um modelo de IA de uso geral não apresenta riscos sistêmicos excepcionalmente e, portanto, não deve ser classificado como um modelo de IA de uso geral com riscos sistêmicos. Essas informações são valiosas para que o AI Office antecipe a introdução de modelos de IA de uso geral com riscos sistêmicos no mercado e para que os fornecedores comecem a colaborar com o AI Office em um estágio inicial. Essas informações são especialmente importantes quando se planeja divulgar um modelo de IA de uso geral, como

modelo de código aberto, uma vez que, após a divulgação de modelos de código aberto, poderá ser mais difícil implementar as medidas necessárias para garantir o cumprimento das obrigações estabelecidas no presente Regulamento.

(113) Se a Comissão considerar que um modelo de IA para fins gerais do qual não tinha conhecimento ou que não lhe foi notificado pelo fornecedor relevante pode ser classificado como um modelo de IA para fins gerais com risco sistémico, a Comissão deverá ser habilitada a designá-lo. Além das atividades de supervisão do AI Office, um sistema de alerta qualificado deve garantir que o AI Office seja informado pelo grupo de especialistas científicos sobre a existência de modelos de IA de uso geral que podem ser classificados como modelos de IA de uso geral com risco sistêmico.

(114) Os fornecedores de modelos de IA para fins gerais que apresentem riscos sistémicos deverão estar sujeitos, para além das obrigações impostas aos fornecedores de modelos de IA para fins gerais, a obrigações destinadas a detetar e atenuar esses riscos e a garantir um nível adequado de proteção da cibersegurança, independentemente de tais modelos serem oferecidos como modelos autónomos ou integrados em sistemas ou produtos de IA. Para atingir esses objetivos, o presente regulamento deverá exigir que os fornecedores realizem as avaliações necessárias dos modelos, em especial antes da primeira colocação no mercado, e, por exemplo, realizem e documentem testes de simulação adversarial, incluindo, quando adequado, por meio de testes externos independentes ou testes internos. Além disso, os provedores de modelos de IA de uso geral com riscos sistêmicos devem avaliar e mitigar continuamente os riscos sistêmicos, por exemplo, estabelecendo políticas de gerenciamento de riscos, como processos de responsabilização e governança, implementando vigilância pós-comercialização, tomando medidas apropriadas durante todo o ciclo de vida do modelo e cooperando com os atores relevantes ao longo da cadeia de valor da IA.

(115) Os fornecedores de modelos de IA para fins gerais com riscos sistémicos devem avaliar e atenuar os potenciais riscos sistémicos. Se, apesar dos esforços para detectar e prevenir riscos relacionados a um modelo de IA de uso geral que possa apresentar riscos sistêmicos, o desenvolvimento ou uso do modelo resultar em um incidente grave, o fornecedor do modelo de IA de uso geral deverá, sem demora injustificada, acompanhar o incidente e comunicar todas as informações relevantes e possíveis medidas corretivas à Comissão e às autoridades nacionais competentes. Além disso, os provedores devem garantir que o modelo e sua infraestrutura física, se aplicável, tenham um nível adequado de proteção de segurança cibernética durante todo o ciclo de vida do modelo. A proteção da segurança cibernética relacionada a riscos sistêmicos associados ao uso ou ataques maliciosos deve levar em conta vazamentos acidentais de modelos, divulgações não autorizadas, evasão de medidas de segurança e defesa contra ataques cibernéticos, acesso não autorizado ou roubo de modelos. Essa proteção poderia ser facilitada pela proteção dos pesos do modelo, algoritmos, servidores e conjuntos de dados, por exemplo, por meio de medidas de segurança operacional para segurança da informação, medidas específicas de segurança cibernética, soluções técnicas apropriadas e estabelecidas e controles de acesso cibernético e físico, dependendo das circunstâncias relevantes e dos riscos existentes.

(116) O Gabinete de IA deverá incentivar e facilitar o desenvolvimento, a revisão e a adaptação de códigos de boas práticas, levando em conta abordagens internacionais. Todos os provedores de modelos de IA de uso geral podem ser convidados a participar. Para garantir que os códigos de boas práticas reflitam o estado atual da arte e levem em conta diferentes perspectivas, o Escritório de IA deve colaborar com as autoridades nacionais competentes relevantes e, quando apropriado, pode consultar organizações da sociedade civil e outras partes interessadas e especialistas relevantes, incluindo o Grupo de Peritos Científicos, sobre o desenvolvimento de tais códigos. Os códigos de prática devem incluir obrigações para provedores de modelos de IA de uso geral e para modelos de IA de uso geral que apresentem riscos sistêmicos. Além disso, no que diz respeito aos riscos sistémicos, os códigos de práticas devem ajudar a estabelecer uma taxonomia de riscos que estabeleça o tipo e a natureza dos riscos sistémicos a nível da União, incluindo as suas fontes. Os códigos de boas práticas também devem se concentrar em medidas específicas de avaliação e redução de riscos.

(117) Os códigos de boas práticas deverão ser um instrumento fundamental para o cumprimento adequado das obrigações previstas no presente regulamento para os fornecedores de modelos de IA para fins gerais. Os fornecedores devem poder confiar em códigos de boas práticas para demonstrar conformidade com as obrigações. Por meio de atos de execução, a Comissão pode decidir adotar um código de boas práticas e dar-lhe validade geral na União ou, alternativamente, estabelecer regras comuns para a implementação das obrigações relevantes se, no momento em que o presente regulamento se tornar aplicável, um código de boas práticas não tiver sido finalizado ou não for considerado adequado pelo AI Office. Uma vez que foi

Uma vez que uma norma harmonizada tenha sido publicada e seja considerada pelo IA Office como adequada para cobrir as obrigações relevantes, a conformidade com uma norma harmonizada europeia deve dar aos fornecedores a presunção de conformidade. Além disso, os provedores de modelos de IA de uso geral devem ser capazes de demonstrar conformidade usando meios alternativos apropriados se códigos de boas práticas ou padrões harmonizados não estiverem disponíveis, ou se eles optarem por não confiar neles.

(118) O presente regulamento regula os sistemas e modelos de IA impondo determinados requisitos e obrigações aos intervenientes relevantes no mercado que os colocam no mercado, os colocam em serviço ou os utilizam na União, complementando assim as obrigações dos prestadores de serviços intermediários que integram esses sistemas ou modelos nos seus serviços, regulamentados pelo Regulamento (UE) 2022/2065. Na medida em que tais sistemas ou modelos estejam integrados em plataformas online muito grandes ou em motores de busca online muito grandes que tenham sido designados, eles estão sujeitos ao quadro de gestão de riscos estabelecido no Regulamento (UE) 2022/2065. Consequentemente, as obrigações relevantes ao abrigo do presente regulamento devem ser presumidas como tendo sido cumpridas, a menos que surjam riscos sistémicos significativos não abrangidos pelo Regulamento (UE) 2022/2065 e sejam detetados nesses modelos. Neste contexto, os fornecedores de plataformas online de grande dimensão e de motores de busca online de grande dimensão são obrigados para avaliar potenciais riscos sistêmicos decorrentes do design, operação e uso de seus serviços, incluindo como o design de sistemas algorítmicos usados no serviço pode contribuir para tais riscos, bem como riscos sistêmicos decorrentes de potencial uso indevido. Esses provedores também são obrigados a adotar medidas adequadas de redução de riscos, respeitando os direitos fundamentais.

(119) Tendo em conta o ritmo rápido da inovação e da evolução tecnológica dos serviços digitais abrangidos pelo âmbito de aplicação de diferentes instrumentos do direito da União, tendo em conta, nomeadamente, a utilização e a perceção dos seus destinatários, os sistemas de IA sujeitos ao presente regulamento podem ser fornecidos como serviços intermediários, ou partes dos mesmos, na aceção do Regulamento (UE) 2022/2065, que deverá ser interpretado de forma tecnologicamente neutra. Por exemplo, os sistemas de IA podem ser usados para fornecer mecanismos de busca on-line, em particular na medida em que um sistema de IA, como um chatbot on-line, pesquisa, em princípio, todos os sites e, em seguida, incorpora os resultados ao seu conhecimento existente e usa o conhecimento atualizado para gerar uma única informação de saída que combina diferentes fontes de informação.

(120) Além disso, as obrigações impostas aos prestadores e aos responsáveis pela implementação de determinados sistemas de IA no presente regulamento, destinadas a permitir a deteção e a divulgação de resultados gerados ou manipulados artificialmente por esses sistemas, são particularmente relevantes para facilitar a aplicação efetiva do Regulamento (UE) 2022/2065. Isto aplica-se em particular às obrigações dos fornecedores de plataformas online muito grandes ou de motores de busca online muito grandes de detetar e mitigar riscos sistémicos que possam surgir da divulgação de conteúdos gerados ou manipulados artificialmente, em particular o risco de efeitos negativos reais ou previsíveis nos processos democráticos, no discurso cívico e nos processos eleitorais, incluindo através da desinformação.

(121) A normalização deverá desempenhar um papel fundamental no fornecimento de soluções técnicas aos fornecedores para garantir o cumprimento do presente regulamento, em consonância com o estado atual da técnica, a fim de promover a inovação, bem como a competitividade e o crescimento no mercado único. Conformidade com as normas harmonizadas definidas no artigo 2.º, ponto 1, alínea c), do Regulamento (UE) n.º[qualquer]1025/2012 do Parlamento Europeu e do Conselho ([41]), que geralmente se espera que reflitam o estado atual da arte, devem ser um meio para os fornecedores demonstrarem a conformidade com os requisitos deste regulamento. Por conseguinte, deve ser incentivada uma representação equilibrada dos interesses de todas as partes interessadas relevantes, em particular as PME, as organizações de consumidores e as partes interessadas sociais e ambientais, na definição de normas, em conformidade com os artigos 5.º e 6.º do Regulamento (UE) n.º 1799/2008.[qualquer] 1025/2012. Para facilitar o cumprimento, a Comissão deve emitir pedidos de normalização sem demora injustificada. Ao preparar o pedido de padronização, a Comissão deve consultar o Fórum Consultivo e o Conselho de IA para obter conhecimentos especializados relevantes. Contudo, na ausência de referências relevantes a normas harmonizadas, a Comissão deverá poder estabelecer, por meio de atos de execução e após consulta ao fórum consultivo, especificações comuns para determinados requisitos previstos no presente regulamento. As especificações comuns devem ser uma solução alternativa excepcional para facilitar a obrigação do fornecedor de cumprir os requisitos do presente regulamento quando nenhuma das organizações europeias de normalização tiver aceitado o pedido de normalização, quando as normas harmonizadas relevantes não abordarem suficientemente as preocupações com os direitos fundamentais, quando as normas harmonizadas não atenderem ao pedido ou quando houver atrasos na adoção de uma norma harmonizada adequada. Quando tais atrasos na adopção de uma norma harmonizada se devem à complexidade técnica dessa norma, a

([41]) Regulamento (UE) n.º[qualquer]1025/2012 do Parlamento Europeu e do Conselho, de 25 de outubro de 2012, relativa 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 1025/2012 do Parlamento Europeu e do Conselho.[qualquer]1673/2006/CE do Parlamento Europeu e do Conselho (JO L 316 de 14.11.2012, p. 12).

A Comissão deve levar isso em consideração antes de considerar o estabelecimento de especificações comuns. A Comissão é incentivada a cooperar com parceiros internacionais e organismos internacionais de normalização ao desenvolver especificações comuns.

(122) É adequado que, sem prejuízo da utilização de normas harmonizadas e de especificações comuns, os fornecedores de um sistema de IA de alto risco que tenha sido treinado e testado com dados que refletem o ambiente geográfico, comportamental, contextual ou funcional específico em que o sistema de IA se destina a ser utilizado sejam presumidos como cumpridores da medida relevante prevista no requisito de governação de dados estabelecido no presente regulamento. Sem prejuízo dos requisitos relacionados com a robustez e a precisão estabelecidos no presente regulamento, em conformidade com o artigo 54.º, n.º 3, do Regulamento (UE) 2019/881, os sistemas de IA de alto risco que tenham uma certificação ou uma declaração de conformidade ao abrigo de um regime de certificação de cibersegurança nos termos desse regulamento e cujas referências tenham sido publicadas noJornal Oficial da União Europeiacumprir o requisito de segurança cibernética do presente regulamento na medida em que o certificado de segurança cibernética ou a declaração de conformidade, ou partes dos mesmos, atendam a esse requisito. Isto não prejudica a natureza voluntária deste esquema de segurança cibernética.

(123) A fim de garantir que os sistemas de IA de alto risco sejam altamente fiáveis, esses sistemas deverão ser sujeitos a uma avaliação da conformidade antes de serem colocados no mercado ou em serviço.

(124) A fim de minimizar os encargos para os operadores e evitar possíveis duplicações, é adequado, no caso dos sistemas de IA de alto risco associados a produtos regulamentados pela legislação de harmonização da União em vigor com base no novo quadro legislativo, que a conformidade desses sistemas de IA com os requisitos estabelecidos no presente regulamento seja avaliada no âmbito da avaliação da conformidade já prevista nessa legislação. Por conseguinte, a aplicabilidade dos requisitos do presente regulamento não deverá afetar a lógica específica, a metodologia ou a estrutura geral da avaliação da conformidade prevista nos atos legislativos de harmonização da União pertinentes.

(125) Dada a complexidade dos sistemas de IA de alto risco e os riscos a eles associados, é importante desenvolver um procedimento adequado de avaliação da conformidade para sistemas de IA de alto risco que envolvam organismos notificados, designado por «avaliação da conformidade por terceiros». No entanto, dada a experiência atual dos profissionais que realizam a certificação pré-comercialização no domínio da segurança dos produtos e a natureza diferente dos riscos envolvidos, é adequado limitar, pelo menos na fase inicial de aplicação do presente regulamento, o âmbito das avaliações externas da conformidade aos sistemas de IA de alto risco que não estejam associados aos produtos. Assim, geralmente é o provedor que deve realizar a avaliação de conformidade de tais sistemas sob sua própria responsabilidade, com a única exceção dos sistemas de IA destinados a serem usados para biometria.

(126) Para poderem realizar avaliações de conformidade por terceiros quando tal for exigido, as autoridades nacionais competentes deverão notificar os organismos notificados nos termos do presente regulamento, desde que estes cumpram uma série de requisitos, nomeadamente no que se refere à sua independência, às suas competências e à ausência de conflitos de interesses, bem como aos requisitos adequados em matéria de cibersegurança. As autoridades nacionais competentes devem enviar a notificação desses organismos à Comissão e aos outros Estados-Membros através do sistema de notificação eletrónica desenvolvido e gerido pela Comissão em conformidade com o artigo R23 do Anexo I da Decisão n.º 166/2004.qualquer768/2008/CE.

(127) Em consonância com os compromissos assumidos pela União no âmbito do Acordo da Organização Mundial do Comércio sobre Obstáculos Técnicos ao Comércio, é adequado facilitar o reconhecimento mútuo dos resultados das avaliações de conformidade efetuadas pelos organismos de avaliação da conformidade competentes, independentemente do território em que estejam 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 a União tenha celebrado um acordo para esse efeito. Neste contexto, a Comissão deverá explorar ativamente possíveis instrumentos internacionais para este fim e, em particular, procurar celebrar acordos de reconhecimento mútuo com países terceiros.

(128) Em consonância com o conceito comummente estabelecido de «modificação substancial» de produtos abrangidos pela legislação de harmonização da União, é adequado que, sempre que ocorra uma alteração que possa afetar a conformidade de um sistema de IA de alto risco com o presente regulamento (por exemplo, uma alteração no sistema operativo ou na arquitetura),software)ou quando a finalidade pretendida do sistema muda, esse sistema de IA é considerado um novo sistema de IA que deve passar por uma nova avaliação de conformidade. No entanto, as alterações ao algoritmo e ao funcionamento dos sistemas de IA que continuam a "aprender" depois de serem colocados no mercado ou colocados em serviço, nomeadamente através da adaptação automática da forma como desempenham as suas funções, não devem constituir uma modificação substancial, desde que tais alterações tenham sido pré-determinadas pelo fornecedor e tenham sido avaliadas no momento da avaliação da conformidade.

(129) Os sistemas de IA de alto risco deverão ostentar a marcação CE para atestar a sua conformidade com o presente regulamento e, assim, poder circular livremente no mercado interno. Para sistemas de IA de alto risco incorporados em um produto, uma marcação CE física deve ser afixada, que pode ser complementada por uma marcação CE digital. Para sistemas de IA de alto risco que são fornecidos apenas digitalmente, uma marcação CE digital deve ser usada. Os Estados-Membros não devem criar barreiras injustificadas à colocação no mercado ou à colocação em serviço de sistemas de IA de alto risco que cumpram os requisitos estabelecidos no presente regulamento e ostentem a marcação CE.

(130) Em determinadas condições, a rápida disponibilidade de tecnologias inovadoras pode ser crucial para a saúde e a segurança humanas, para a protecção ambiental e para a atenuação das alterações climáticas, bem como para a sociedade em geral. É, portanto, adequado que as autoridades de fiscalização do mercado possam autorizar, por motivos excecionais de segurança pública ou com vista à proteção da vida e da saúde das pessoas singulares, do ambiente e dos ativos críticos da indústria e das infraestruturas, a colocação no mercado ou a colocação em serviço de sistemas de IA que não tenham sido sujeitos a uma avaliação da conformidade. Em situações devidamente justificadas previstas no presente regulamento, as autoridades responsáveis pela aplicação da lei ou as autoridades de proteção civil podem colocar em serviço um sistema de IA especificamente de risco elevado sem autorização da autoridade de fiscalização do mercado, desde que a autorização seja solicitada durante ou após a utilização, sem demora injustificada.

(131) A fim de facilitar o trabalho da Comissão e dos Estados-Membros no domínio da IA e aumentar a transparência para o público, os fornecedores de sistemas de IA de alto risco que não estejam associados a produtos abrangidos pelo âmbito de aplicação da legislação de harmonização da União pertinente e aplicável e os fornecedores que considerem que qualquer um dos sistemas de IA enumerados nos casos de utilização de alto risco num anexo ao presente regulamento não é de alto risco com base numa derrogação deverão ser obrigados a registar-se e a registar informações sobre os seus sistemas de IA numa base de dados da UE, que será criada e gerida pela Comissão. Antes de utilizar um sistema de IA listado nos casos de uso de alto risco em um anexo ao presente regulamento, os responsáveis pela implantação de sistemas de IA de alto risco que sejam autoridades, órgãos ou agências públicas devem se registrar nesse banco de dados e selecionar o sistema que pretendem utilizar. Outros responsáveis pela implantação devem poder realizar esse registro de forma voluntária. Esta seção do banco de dados da UE deve ser acessível ao público e gratuita, as informações devem ser fáceis de navegar e devem ser compreensíveis e legíveis por máquinas. A base de dados da UE também deve ser de fácil utilização, por exemplo, disponibilizando funcionalidades de pesquisa, nomeadamente através de palavras-chave, permitindo ao público em geral encontrar as informações a submeter para o registo de sistemas de IA de alto risco e relacionadas com os casos de utilização de sistemas de IA de alto risco definidos num anexo ao presente regulamento, aos quais correspondem os sistemas de IA de alto risco. Quaisquer modificações substanciais em sistemas de IA de alto risco também devem ser registradas no banco de dados da UE. Para sistemas de IA de alto risco no campo da aplicação da lei e migração, asilo e gestão de controle de fronteiras, as obrigações de registro devem ser cumpridas em uma seção segura e não pública do banco de dados da UE. O acesso a essa seção deve ser estritamente limitado à Comissão e às autoridades de fiscalização do mercado no que diz respeito à sua seção nacional desse banco de dados. Sistemas de IA de alto risco no campo de infraestrutura crítica só precisam ser registrados em nível nacional. A Comissão deve ser a controladora do banco de dados da UE, em conformidade com o Regulamento (UE) 2018/1725. Para garantir a plena funcionalidade do banco de dados da UE quando estiver operacional, o procedimento para sua criação deve incluir o desenvolvimento de especificações funcionais pela Comissão e a elaboração de um relatório de auditoria independente.Ao exercer suas funções como controladora do banco de dados da UE, a Comissão deve levar em consideração os riscos de segurança cibernética. Para maximizar a disponibilidade e a utilização da base de dados da UE pelo público, a base de dados da UE e as informações fornecidas através dela devem cumprir os requisitos estabelecidos na Diretiva (UE) 2019/882.

(132) Certos sistemas de IA destinados a interagir com pessoas singulares ou a gerar conteúdos podem apresentar riscos específicos de representação ou de engano, independentemente de preencherem ou não as condições para serem considerados de alto risco. A utilização destes sistemas deverá, por conseguinte, estar sujeita, em determinadas circunstâncias, a obrigações específicas de transparência, sem prejuízo dos requisitos e obrigações aplicáveis. para sistemas de IA de alto risco e para exceções específicas para levar em conta as necessidades especiais da aplicação da lei. Em particular, as pessoas singulares devem ser informadas de que estão a interagir com um sistema de IA, exceto quando tal for óbvio do ponto de vista de uma pessoa singular naturalmente informada e razoavelmente atenta e percetiva, tendo em conta as circunstâncias e o contexto de utilização. Ao aplicar esta obrigação, devem ser tidas em conta as características das pessoas singulares pertencentes a grupos vulneráveis devido à sua idade ou deficiência, na medida em que o sistema de IA também se destina a interagir com esses grupos. Além disso, os indivíduos devem ser notificados quando forem expostos a sistemas de IA que, por meio do processamento de seus dados biométricos, podem determinar ou inferir suas emoções ou intenções ou incluí-los em categorias específicas. Essas categorias específicas podem se referir a aspectos como gênero, idade, cor do cabelo, cor dos olhos, tatuagens, traços pessoais, origem étnica ou preferências e interesses pessoais. Essas informações e notificações devem ser fornecidas em formatos acessíveis a pessoas com deficiência.

(133) Uma variedade de sistemas de IA pode gerar grandes quantidades de conteúdo sintético que é cada vez mais difícil para as pessoas distinguirem do conteúdo autêntico gerado por humanos. A ampla disponibilidade e as capacidades crescentes desses sistemas têm implicações significativas para a integridade e a confiança no ecossistema de informações, aumentando os riscos de desinformação e manipulação em larga escala, fraude, roubo de identidade e engano do consumidor. Tendo em vista esses efeitos, o rápido desenvolvimento tecnológico e a necessidade de novos métodos e técnicas para garantir a rastreabilidade da origem das informações, é apropriado exigir que os provedores de tais sistemas integrem soluções técnicas que permitam marcar, em um formato legível por máquina, e detectar que o resultado de saída foi gerado ou manipulado por um sistema de IA e não por um ser humano. Tais técnicas e métodos devem ser suficientemente confiáveis, interoperáveis, eficazes e robustos, na medida em que seja tecnicamente viável, levando em consideração as técnicas disponíveis ou uma combinação dessas técnicas, como marca d'água, identificação de metadados, métodos criptográficos para demonstrar a procedência e autenticidade do conteúdo, métodos de registro, impressão digital ou outras técnicas, conforme apropriado. Ao implementar esta obrigação, os provedores também devem levar em consideração as especificidades e limitações dos diferentes tipos de conteúdo e os desenvolvimentos tecnológicos e de mercado relevantes nessa área, conforme refletido no estado da arte geralmente reconhecido. Tais técnicas e métodos podem ser implementados no nível do sistema de IA ou no nível do modelo de IA, incluindo modelos de IA de uso geral que geram conteúdo, facilitando assim o cumprimento desta obrigação pelo provedor a jusante do sistema de IA. Para garantir a proporcionalidade, é adequado prever que esta obrigação de marcação não se aplica aos sistemas de IA que desempenham uma função de suporte de edição padrão ou não alteram substancialmente os dados de entrada fornecidos pelo implementador ou sua semântica.

(134) Além das soluções técnicas utilizadas pelos fornecedores de sistemas de IA, os implementadores que utilizam um sistema de IA para gerar ou manipular conteúdos de imagem, áudio ou vídeo gerados ou manipulados pela IA que se assemelham substancialmente a pessoas, objetos, lugares, entidades ou eventos reais e que podem induzir uma pessoa a acreditar que são autênticos ou fiéis à realidade (ultraspoofing) devem também tornar público, de forma clara e distinguível, que esse conteúdo foi criado ou manipulado artificialmente, rotulando os resultados de saída gerados pela IA em conformidade e indicando a sua origem artificial. O cumprimento desta obrigação de transparência não deve ser interpretado como uma indicação de que o uso do sistema de IA ou seus resultados impedem o direito à liberdade de expressão e o direito à liberdade das artes e das ciências, garantidos pela Carta, em particular quando o conteúdo faz parte de uma obra ou programa manifestamente criativo, satírico, artístico, ficcional ou similar, sujeito a salvaguardas adequadas para os direitos e liberdades de terceiros. Nesses casos, a obrigação de transparência em relação às personificações prevista no presente Regulamento limita-se à divulgação da existência de tais conteúdos gerados ou manipulados de forma adequada que não prejudique a apresentação e a fruição da obra, incluindo a sua exploração e utilização normais, preservando a utilidade e a qualidade da obra. Além disso, uma obrigação de divulgação semelhante também deve ser prevista em relação ao texto gerado ou manipulado por IA, na medida em que seja publicado com a finalidade de informar o público sobre questões de interesse público, a menos que o conteúdo gerado por IA tenha sido submetido a um processo de revisão humana ou controle editorial e uma pessoa física ou jurídica exerça 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 o desenvolvimento de códigos de boas práticas à escala da União, a fim de facilitar a aplicação efetiva das obrigações relativas à deteção e rotulagem de conteúdos gerados ou manipulados artificialmente, incluindo para apoiar disposições práticas para tornar os mecanismos de deteção acessíveis, quando adequado, e para facilitar a cooperação com outros intervenientes na cadeia de valor, através da divulgação de conteúdos ou da verificação da sua autenticidade e proveniência, a fim de permitir ao público distinguir eficazmente os conteúdos gerados por IA.

(136) As obrigações impostas aos prestadores e aos responsáveis pela implementação de determinados sistemas de IA no presente regulamento, destinadas a permitir a deteção e a divulgação de resultados gerados ou manipulados artificialmente por esses sistemas, são particularmente relevantes para facilitar a aplicação efetiva do Regulamento (UE) 2022/2065. Isto aplica-se em particular às obrigações dos fornecedores de plataformas online muito grandes ou de motores de busca online muito grandes de detetar e mitigar riscos sistémicos que possam surgir da divulgação de conteúdos gerados ou manipulados artificialmente, em particular o risco de efeitos negativos reais ou previsíveis nos processos democráticos, no discurso cívico e nos processos eleitorais, como através da desinformação. O requisito de rotular o conteúdo gerado pelos sistemas de IA ao abrigo do presente regulamento não prejudica a obrigação, nos termos do artigo 16.º, n.º 6, do Regulamento (UE) 2022/2065, de os prestadores de serviços de alojamento processarem as notificações que recebem sobre conteúdos ilegais ao abrigo do artigo 16.º, n.º 1, do referido regulamento, e não deverá influenciar a avaliação e a decisão sobre o caráter ilegal do conteúdo em questão. Tal avaliação deve ser feita exclusivamente com referência às regras que regem a legalidade do conteúdo.

(137) O cumprimento das obrigações de transparência aplicáveis aos sistemas de IA abrangidos pelo âmbito de aplicação do presente regulamento não deverá ser interpretado como um indicador de que a utilização do sistema de IA ou dos seus resultados é lícita ao abrigo do presente regulamento ou de outras disposições do direito da União e dos Estados-Membros, e não deverá prejudicar outras obrigações de transparência aplicáveis aos responsáveis pelo tratamento da implantação de sistemas de IA estabelecidas no direito da União ou nacional.

(138) A IA é uma família de tecnologias em rápida evolução que requer supervisão regulamentar e um espaço seguro e controlado para experimentação, bem como a garantia de inovação responsável e a integração de salvaguardas éticas adequadas e medidas de mitigação de riscos. Para alcançar um quadro jurídico que promova a inovação, resista ao teste do tempo e seja resiliente a perturbações, os Estados-Membros devem garantir que as suas autoridades nacionais competentes estabeleçam pelo menos um ambiente de testes nacional de IA que facilite o desenvolvimento e o teste de sistemas de IA inovadores sob supervisão regulamentar rigorosa antes de serem colocados no mercado ou colocados em serviço. Os Estados-Membros também poderão cumprir esta obrigação participando em áreas de teste controladas existentes ou estabelecendo uma área de teste em conjunto com as autoridades competentes de um ou mais Estados-Membros, desde que essa participação proporcione um nível equivalente de cobertura nacional para os Estados-Membros participantes. Os sandboxes de IA podem ser configurados fisicamente, digitalmente ou de forma híbrida e podem hospedar produtos físicos e digitais. As autoridades que os criam também devem garantir que as sandboxes de IA controladas tenham recursos adequados para sua operação, incluindo recursos financeiros e humanos.

(139) Os ambientes de teste de IA deverão ter como objetivo impulsionar a inovação no domínio da IA, através do estabelecimento de um ambiente de experimentação e de testes controlados na fase de desenvolvimento e de pré-comercialização, com vista a garantir que os sistemas de IA inovadores cumprem o presente regulamento e outras disposições pertinentes do direito da União e nacional. Além disso, os sandboxes de IA devem ter como objetivo aumentar a segurança jurídica para os inovadores e apoiar a supervisão e a compreensão das autoridades competentes sobre as oportunidades, os riscos emergentes e as consequências do uso da IA, facilitar o aprendizado regulatório por autoridades e empresas, inclusive com vistas a futuras adaptações da estrutura legal, apoiar a cooperação e o intercâmbio de melhores práticas com as autoridades envolvidas no sandbox e acelerar o acesso ao mercado, inclusive removendo barreiras para pequenas e médias empresas, incluindo startups. Áreas de testes controladas para IA devem estar amplamente disponíveis em toda a União e deve ser dada especial atenção para torná-las acessíveis às PME, incluindo as start-ups. A participação no sandbox de IA deve se concentrar em questões que criam incerteza jurídica e, portanto, dificultam que fornecedores e potenciais fornecedores inovem e experimentem IA na União e contribuam para o aprendizado regulatório baseado em evidências. Portanto, a supervisão dos sistemas de IA no sandbox de IA deve abranger seu desenvolvimento, treinamento, testes e validação antes de sua introdução no mercado ou colocação em serviço, bem como o conceito de "modificação substancial" e sua materialização, o que pode exigir um novo procedimento de avaliação da conformidade. Qualquer risco significativo detectado durante o processo de desenvolvimento e teste desses sistemas de IA deve levar à adoção de medidas de mitigação apropriadas e, na sua falta, à suspensão do processo de desenvolvimento e teste. Quando apropriado, as autoridades nacionais competentes que criam sandboxes de IA devem cooperar com outras autoridades relevantes, incluindo aquelas que supervisionam a proteção dos direitos fundamentais, e podem acomodar outros atores no ecossistema de IA, como organizações nacionais ou europeias de normalização, organismos notificados, instalações de teste e experimentação, laboratórios de pesquisa e experimentação, centros europeus de inovação digital e organizações relevantes de partes interessadas e da sociedade civil. A fim de assegurar uma aplicação uniforme em toda a União e alcançar economias de escala,É apropriado estabelecer padrões comuns para a criação de sandboxes de IA controlados, bem como uma estrutura para cooperação entre as autoridades relevantes envolvidas na supervisão de tais sandboxes. Os sandboxes de IA estabelecidos ao abrigo do presente regulamento não deverão prejudicar outros atos legislativos que permitam o estabelecimento de outros sandboxes destinados a garantir o cumprimento de atos legislativos que não o presente regulamento. Quando apropriado, as autoridades competentes relevantes responsáveis por outras áreas de teste controladas devem considerar os benefícios de também utilizá-las para garantir a conformidade com o presente regulamento pelos sistemas de IA. Sujeito a acordo entre as autoridades nacionais competentes e os participantes do AI Sandbox, os testes no mundo real também podem ser gerenciados e supervisionados dentro do AI Sandbox.

(140) O presente regulamento deverá fornecer a base jurídica para que os prestadores e potenciais prestadores na área restrita de IA utilizem dados pessoais recolhidos para outros fins, a fim de desenvolver determinados sistemas de IA no interesse público na área restrita de IA, apenas sob determinadas condições, em conformidade com os artigos 6.º, n.º 4, e 9.º, n.º 2, alínea g), do Regulamento (UE) 2016/679 e os artigos 5.º, 6.º e 10.º do Regulamento (UE) 2018/1725, e sem prejuízo dos artigos 4.º, n.º 2, e 10.º da Diretiva (UE) 2016/680. As outras obrigações dos controladores e os direitos dos titulares dos dados nos termos do Regulamento (UE) 2016/679, do Regulamento (UE) 2018/1725 e da Diretiva (UE) 2016/680 permanecem aplicáveis. Em particular, o presente regulamento não deverá constituir uma base jurídica na acepção 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. Fornecedores e potenciais fornecedores no sandbox de IA controlado devem fornecer salvaguardas adequadas e cooperar com, e também de acordo com, as autoridades relevantes, e agir prontamente e de boa-fé para mitigar adequadamente quaisquer riscos significativos à segurança, saúde e direitos fundamentais que sejam identificados e possam surgir durante o desenvolvimento, testes e experimentação no sandbox de IA controlado.

(141) A fim de acelerar o processo de desenvolvimento e colocação no mercado de sistemas de IA de alto risco enumerados num anexo ao presente regulamento, é importante que os fornecedores ou potenciais fornecedores desses sistemas possam também beneficiar de um regime específico para testar esses sistemas em condições reais, sem participarem numa área de testes de IA. Contudo, em tais casos, tendo em conta as possíveis consequências desses testes para pessoas singulares, deverá assegurar-se que o Regulamento prevê salvaguardas e condições adequadas e suficientes para fornecedores ou potenciais fornecedores. Essas salvaguardas devem incluir, entre outras coisas, a busca de consentimento informado de pessoas físicas para participar de testes em condições reais, exceto no que diz respeito à garantia do cumprimento da lei quando a tentativa de obter consentimento informado impediria que o sistema de IA fosse testado. O consentimento dos sujeitos para participar de tais testes sob este Regulamento é distinto e não prejudica o consentimento dos titulares dos dados para o processamento de seus dados pessoais sob a legislação de proteção de dados aplicável. Também é importante minimizar os riscos e permitir a supervisão por autoridades competentes e, portanto, exigir que os fornecedores em potencial enviem à autoridade de fiscalização de mercado competente um plano para o teste no mundo real, registrem o teste nas seções específicas do banco de dados da UE, sujeito a algumas exceções limitadas, estabeleçam limitações no período durante o qual o teste pode ser realizado e exijam salvaguardas adicionais para pessoas pertencentes a certos grupos vulneráveis, bem como um acordo por escrito definindo as funções e responsabilidades dos fornecedores em potencial e dos responsáveis pela implantação e supervisão eficaz por pessoal competente envolvido no teste no mundo real. Além disso, devem ser fornecidas salvaguardas adicionais para garantir que as previsões, recomendações ou decisões do sistema de IA possam ser efetivamente revertidas e descartadas e que os dados pessoais sejam protegidos e apagados quando os sujeitos retirarem seu consentimento para participar do teste, sem prejuízo de seus direitos como titulares de dados sob a legislação de proteção de dados da União. No que diz respeito à transferência de dados, é também adequado prever que os dados recolhidos e tratados para efeitos de testes em condições reais só sejam transferidos para países terceiros onde existam salvaguardas adequadas e aplicáveis ao abrigo do direito da União, em especial,de acordo com as bases para a transferência de dados pessoais previstas na legislação da União em matéria de proteção de dados e, no que diz respeito aos dados não pessoais, existem salvaguardas adequadas ao abrigo da legislação da União, como o Regulamento (UE) 2022/868 ([42]) e (UE) 2023/2854 ([43]) do Parlamento Europeu e do Conselho.

(142) A fim de garantir que a IA conduza a resultados sociais e ambientais positivos, os Estados-Membros são encorajados a apoiar e a promover a investigação e o desenvolvimento de soluções de IA que apoiem esses resultados, como soluções baseadas em IA para aumentar a acessibilidade das pessoas com deficiência, para abordar as desigualdades socioeconómicas ou para cumprir objetivos ambientais, através da atribuição de recursos suficientes, incluindo fundos públicos e da União, e, quando adequado e desde que os critérios de elegibilidade e seleção sejam cumpridos, tendo em conta, em especial, os projetos que prosseguem esses objetivos. Tais projetos devem ser baseados no princípio da cooperação interdisciplinar entre desenvolvedores de IA, especialistas em desigualdade e não discriminação, acessibilidade e direitos do consumidor, questões ambientais e digitais, bem como representantes da academia.

(143) A fim de promover e proteger a inovação, é importante ter em especial consideração os interesses das PME, incluindo startups, sejam elas fornecedoras ou implantadoras de sistemas de IA. Para tal, os Estados-Membros deverão desenvolver iniciativas nas áreas da sensibilização e da comunicação de informações, entre outros aspetos, dirigidas a estes operadores. Os Estados-Membros devem proporcionar às PME, incluindo as start-ups, com sede social ou sucursal na União acesso prioritário a áreas de teste controladas para IA, desde que cumpram as condições de elegibilidade e os critérios de seleção e sem impedir que outros fornecedores e potenciais fornecedores acedam às áreas de teste controladas, desde que cumpram as mesmas condições e critérios. Os Estados-Membros devem utilizar os canais existentes e estabelecer, quando apropriado, novos canais de comunicação específicos com as PME, incluindo start-ups, implementadoras, outros inovadores e, quando apropriado, autoridades públicas locais, para apoiar as PME ao longo do seu percurso de desenvolvimento, fornecendo orientações e respondendo a perguntas sobre a aplicação do presente regulamento. Quando apropriado, esses canais devem trabalhar juntos para criar sinergias e garantir consistência em suas orientações para PMEs, incluindo startups e implantadores. Além disso, os Estados-Membros devem incentivar a participação de PME e outras partes interessadas relevantes nos processos de desenvolvimento de normalização. Os organismos notificados também devem levar em consideração as necessidades e os interesses específicos dos usuários.

([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 sobre a 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 para o acesso e a utilização equitativos de dados e que altera o Regulamento (UE) 2017/2394 e a Diretiva (UE) 2020/1828 (Regulamento sobre Dados) (JO L 2023/2854, 22.12.2023, ELI: http://data.europa.eu/eli/reg/2023/2854/oj).

fornecedores que sejam PMEs, incluindo start-ups, ao definir as taxas aplicáveis às avaliações de conformidade. A Comissão deve avaliar regularmente os custos de certificação e conformidade para PMEs, incluindo start-ups, por meio de consultas transparentes, e deve trabalhar com os Estados-Membros para reduzir esses custos. Por exemplo, os custos de tradução associados à documentação obrigatória e à comunicação com as autoridades podem ser consideráveis para fornecedores e outros operadores, especialmente os menores. Na medida do possível, os Estados-Membros devem garantir que um dos idiomas em que aceitam que os prestadores apresentem a documentação relevante e que pode ser usado para comunicação com os operadores seja amplamente conhecido pelo maior número possível de implantadores transfronteiriços. A fim de atender às necessidades específicas das PME, incluindo as start-ups, a Comissão deverá fornecer modelos normalizados para as áreas abrangidas pelo presente regulamento, mediante solicitação do Conselho da IA. Além disso, a Comissão deve complementar os esforços dos Estados-Membros, disponibilizando uma plataforma de informação única com informações de fácil utilização sobre este regulamento para todos os prestadores e implementadores, organizando campanhas de comunicação adequadas para aumentar a sensibilização para as obrigações decorrentes deste regulamento e avaliando e promovendo a convergência das melhores práticas nos procedimentos de contratação pública relativos aos sistemas de IA. As médias empresas que foram recentemente consideradas pequenas empresas na acepção do Anexo à Recomendação 2003/361/CE da Comissão ([44]) devem ter acesso a tais medidas de apoio, uma vez que essas novas empresas de média dimensão podem, por vezes, não dispor dos recursos jurídicos nem da formação necessários para garantir a compreensão e o cumprimento adequados do presente regulamento.

(144) A fim de promover e proteger a inovação, a plataforma de IA a pedido e todos os programas e projetos de financiamento relevantes da União, como o programa Europa Digital ou o Horizonte Europa, executados pela Comissão e pelos Estados-Membros a nível nacional ou da União, deverão, sempre que adequado, contribuir para a concretização dos objetivos do presente regulamento.

(145) A fim de minimizar os riscos de implementação decorrentes da falta de conhecimento e experiência do mercado, e com o objetivo de facilitar o cumprimento das obrigações que lhes são impostas pelos prestadores, em especial as PME, incluindo as empresas em fase de arranque, e pelos organismos notificados ao abrigo do presente regulamento, a plataforma de IA a pedido, os Polos Europeus de Inovação Digital e as instalações de ensaio e experimentação criadas pela Comissão e pelos Estados-Membros a nível nacional ou da União deverão contribuir para a implementação do presente regulamento. Em particular, a plataforma de IA sob demanda, os Centros Europeus de Inovação Digital e as instalações de testes e experimentação podem fornecer aos fornecedores e organismos notificados assistência técnica e científica dentro de suas respectivas missões e esferas de competência.

(146) Além disso, tendo em conta a dimensão muito reduzida de alguns operadores e a fim de assegurar a proporcionalidade em relação aos custos da inovação, é adequado permitir que as microempresas cumpram uma das obrigações mais onerosas, nomeadamente a criação de um sistema de gestão da qualidade, de forma simplificada, o que reduziria os encargos administrativos e os custos para essas empresas sem afetar o nível de proteção ou a necessidade de cumprir os requisitos aplicáveis aos sistemas de IA de alto risco. A Comissão deve elaborar diretrizes para especificar os elementos do sistema de gestão da qualidade que as microempresas devem cumprir dessa maneira simplificada.

(147) É conveniente que a Comissão facilite, na medida do possível, o acesso às instalações de ensaio e experimentais por parte de organismos, grupos ou laboratórios estabelecidos ou acreditados ao abrigo da legislação de harmonização pertinente da União e que desempenhem funções no âmbito da avaliação da conformidade de produtos ou dispositivos abrangidos por essa legislação. É o caso, em particular, dos painéis de peritos, dos laboratórios especializados e dos laboratórios de referência no domínio dos dispositivos médicos, em conformidade com os Regulamentos (UE) 2017/745 e (UE) 2017/746.

(148) O presente regulamento deverá estabelecer um quadro de governação que permita a coordenação e o apoio à sua implementação a nível nacional, o reforço de capacidades a nível da União e a integração das partes interessadas no domínio da IA. A implementação e execução efetivas deste regulamento exigem um quadro de governação que permita a coordenação e a aquisição de conhecimentos especializados centrais a nível da União. O Gabinete de IA foi criado pela Decisão da Comissão ([45]) e sua missão é desenvolver a expertise e as capacidades da União no campo da IA e contribuir para a implementação da legislação da União sobre IA. Os Estados-Membros devem facilitar as tarefas do Gabinete de IA com vista a apoiar o desenvolvimento de conhecimentos especializados e capacidades a nível da União e a reforçar o funcionamento do mercado único digital. Além disso, deve ser criado um Conselho da IA, composto por representantes dos Estados-Membros, um grupo de peritos científicos para integrar a comunidade científica e um fórum consultivo para facilitar a contribuição das partes interessadas na implementação do presente regulamento, a nível da União e nacional. O desenvolvimento do conhecimento

([44]) Recomendação 2003/361/CE 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).
([45]) Decisão da Comissão de 24 de janeiro de 2024 que cria o Gabinete Europeu de Inteligência Artificial (C/2024/390).

Os recursos e capacidades especializados da União também devem incluir o uso de recursos e conhecimentos especializados existentes, em especial por meio de sinergias com estruturas criadas no contexto da implementação, a nível da União, de outros atos legislativos e sinergias com iniciativas relacionadas a nível da União, como a Empresa Comum EuroHPC e as instalações de teste e experimentação de IA no âmbito do programa Europa Digital.

(149) Deverá ser criado um Conselho da IA para facilitar a aplicação harmoniosa, eficaz e harmonizada do presente regulamento. O Conselho de IA deve refletir os diversos interesses do ecossistema de IA e ser composto por representantes dos Estados-Membros. O Conselho de IA será encarregado de uma variedade de tarefas consultivas. Entre outras coisas, deve emitir pareceres, recomendações e relatórios consultivos ou contribuir para orientações sobre questões relacionadas com a aplicação do presente regulamento, incluindo no que diz respeito à implementação, especificações técnicas ou normas existentes em relação aos requisitos estabelecidos no presente regulamento, e aconselhar a Comissão e os Estados-Membros, bem como as suas autoridades nacionais competentes, sobre questões específicas relacionadas com a IA. A fim de proporcionar flexibilidade aos Estados-Membros na nomeação dos seus representantes para o Conselho da IA, qualquer pessoa pertencente a uma entidade pública que tenha as competências e poderes relevantes para facilitar a coordenação a nível nacional e contribuir para o cumprimento das tarefas do Conselho da IA pode ser nomeada como representante. O Conselho da IA deve estabelecer dois subgrupos permanentes para fornecer uma plataforma para cooperação e intercâmbio entre autoridades de fiscalização de mercado e autoridades notificadoras sobre questões relacionadas, respectivamente, à fiscalização de mercado e aos organismos notificados. O subgrupo permanente de fiscalização do mercado deve atuar como um grupo de cooperação administrativa (ADCO) para o presente regulamento, na aceção do artigo 30.º do Regulamento (UE) 2019/1020. Nos termos do artigo 33.º do referido regulamento, a Comissão deve apoiar as atividades do subgrupo permanente de fiscalização do mercado através da realização de avaliações ou estudos de mercado,
em especial com vista a identificar os aspetos do presente regulamento que exigem uma coordenação específica e urgente entre as autoridades de fiscalização do mercado. O Conselho da IA pode estabelecer outros subgrupos permanentes ou temporários, conforme apropriado, para examinar questões específicas. O Conselho da IA também deverá cooperar, conforme apropriado, com os organismos, grupos de peritos e redes relevantes da União que atuam no contexto da legislação relevante da União, incluindo, em especial, aqueles que atuam ao abrigo da legislação relevante da União sobre dados e 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 o Conselho de Administração e a Comissão e fornecer-lhes conhecimentos técnicos especializados. A fim de assegurar uma representação diversificada e equilibrada das partes interessadas, tendo em conta os interesses comerciais e não comerciais e, dentro da categoria de interesses comerciais, no que diz respeito PMEs e outras empresas, o fórum consultivo deve incluir, entre outros, a indústria, as start-ups, as PMEs, o meio académico, a sociedade civil, em particular os parceiros sociais, bem como 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 Normas de Telecomunicações (ETSI).

(151) A fim de apoiar a execução e a execução do presente regulamento, em especial as atividades de supervisão do Gabinete de IA no que diz respeito aos modelos de IA para fins gerais, deverá ser criado um grupo de peritos científicos composto por peritos independentes. Os peritos independentes que constituem o grupo de peritos científicos devem ser selecionados com base em conhecimentos científicos ou técnicos atualizados no domínio da IA e devem desempenhar as suas funções de forma imparcial e objetiva, bem como garantir a confidencialidade das informações e dos dados obtidos no exercício das suas funções e atividades. A fim de permitir o reforço das capacidades nacionais necessárias à aplicação eficaz do presente regulamento, os Estados-Membros deverão poder solicitar o apoio dos peritos que constituem o grupo científico para as suas atividades de aplicação.

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

(153) Os Estados-Membros desempenham um papel fundamental na aplicação e execução do presente regulamento. A este respeito, cada Estado-Membro deve designar pelo menos uma autoridade notificadora e pelo menos uma autoridade de fiscalização do mercado como autoridades nacionais competentes responsáveis pela supervisão da sua aplicação e execução. Os Estados-Membros podem decidir designar qualquer tipo de entidade pública para desempenhar as tarefas das autoridades nacionais competentes, na aceção do presente regulamento, de acordo com as suas características e necessidades organizacionais nacionais específicas. A fim de aumentar a eficiência organizacional nos Estados-Membros e estabelecer um único ponto de contacto oficial com o público e outras partes interessadas a nível dos Estados-Membros e da União, cada Estado-Membro deve designar uma autoridade de fiscalização do mercado para atuar como ponto de contacto único.

(154) As autoridades nacionais competentes devem exercer os seus poderes de forma independente, imparcial e objectiva, a fim de preservar os princípios de objetividade das suas atividades e funções e de assegurar a aplicação e execução do presente Regulamento. Os membros destas autoridades devem abster-se de qualquer ato incompatível com a natureza das suas funções e estar sujeitos às regras de confidencialidade estabelecidas no presente Regulamento.

(155) Todos os fornecedores de sistemas de IA de alto risco deverão dispor de um sistema de vigilância pós-comercialização, com vista a garantir que podem ter em conta a experiência adquirida com a utilização desses sistemas, a fim de melhorar os seus sistemas e o processo de conceção e desenvolvimento, ou que podem tomar medidas corretivas em tempo útil. Quando apropriado, a vigilância pós-comercialização deve incluir a análise da interação com outros sistemas de IA, incluindo outros dispositivos esoftware.A vigilância pós-comercialização não deve cobrir dados operacionais confidenciais de implantadores de sistemas de IA que são autoridades policiais. Este sistema também é essencial para garantir que os riscos potenciais decorrentes de sistemas de IA que continuam a "aprender" após sua introdução no mercado ou comissionamento sejam abordados de forma mais eficiente e oportuna. Neste contexto, os prestadores também devem ser obrigados a ter um sistema para comunicar às autoridades competentes qualquer incidente grave associado à utilização dos seus sistemas de IA, entendido como um incidente ou defeito que resulte em morte ou danos graves para a saúde, uma perturbação grave e irreversível na gestão ou operação de infraestruturas críticas, incumprimento de obrigações ao abrigo da legislação da União destinada a proteger direitos fundamentais ou danos graves à propriedade ou ao ambiente.

(156) A fim de assegurar o cumprimento adequado e efetivo dos requisitos e obrigações previstos no presente regulamento, que constitui legislação de harmonização da União, o sistema relativo à fiscalização do mercado e à conformidade dos produtos estabelecido pelo Regulamento (UE) 2019/1020 deverá ser integralmente aplicado. As autoridades de fiscalização do mercado designadas nos termos do presente regulamento devem ter todos os poderes de execução estabelecidos no presente regulamento e no Regulamento (UE) 2019/1020 e devem 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 ou obrigações específicas ao abrigo do presente regulamento, as autoridades de fiscalização do mercado podem tomar medidas em relação a todos os sistemas de IA quando estes apresentem um risco em conformidade com o presente regulamento. Devido à natureza específica das instituições, órgãos, gabinetes e agências da União abrangidos pelo âmbito de aplicação do presente regulamento, é adequado designar a Autoridade Europeia para a Proteção de Dados como a autoridade de fiscalização do mercado competente para os mesmos. Isto não deverá prejudicar a designação de 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, sempre que tal independência seja exigida pela legislação da União.

(157) O presente regulamento não prejudica as competências, tarefas, poderes e independência das autoridades ou organismos públicos nacionais competentes que supervisionam a aplicação do direito da União que protege os direitos fundamentais, incluindo os organismos responsáveis pela igualdade e as autoridades de proteção de dados. Sempre que necessário para o seu mandato, essas autoridades ou organismos públicos nacionais deverão também ter acesso a qualquer documentação criada ao abrigo do presente regulamento. Um procedimento de salvaguarda específico deve ser estabelecido para garantir a aplicação adequada e oportuna contra sistemas de IA que representam um risco à saúde, à segurança ou aos direitos fundamentais. O procedimento relativo a tais sistemas de IA que apresentem um risco deverá aplicar-se aos sistemas de IA de alto risco que apresentem um risco, aos sistemas proibidos que tenham sido colocados no mercado, colocados em serviço ou utilizados em violação das práticas proibidas estabelecidas no presente regulamento e aos sistemas de IA que tenham sido colocados no mercado em violação dos requisitos de transparência estabelecidos no presente regulamento e que apresentem um risco.

(158) A legislação da União sobre serviços financeiros contém regras e requisitos em matéria de governação interna e de gestão de riscos que as instituições financeiras regulamentadas devem cumprir quando prestam esses serviços, incluindo quando utilizam sistemas de IA. A fim de assegurar a aplicação e execução coerentes das obrigações estabelecidas no presente regulamento e das regras e requisitos relevantes dos atos jurídicos da União relativos aos serviços financeiros, deverão ser designadas autoridades competentes para supervisionar e executar esses atos jurídicos, em especial as autoridades competentes definidas no Regulamento (UE) n.º 1999/2002.qualquer575/2013 do Parlamento Europeu e do Conselho (46) e as Directivas 2008/48/CE (47), 2009/138/CE (48),

(46) Regulamento (UE) n.ºqualquer575/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e que altera o Regulamento (UE) n.º 575/2013.qualquer648/2012 (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).

2013/36/UE (49), 2014/17/UE (50) e (UE) 2016/97 (51) do Parlamento Europeu e do Conselho, no âmbito das respetivas competências, como autoridades competentes responsáveis pela supervisão da aplicação do presente regulamento, incluindo no que diz respeito às atividades de fiscalização do mercado, em relação aos sistemas de IA fornecidos ou utilizados por instituições financeiras regulamentadas e supervisionadas, a menos que os Estados-Membros decidam designar outra autoridade para desempenhar estas tarefas de fiscalização do mercado. Essas autoridades competentes devem ter todos os poderes previstos no presente regulamento e no Regulamento (UE) 2019/1020 para fazer cumprir os requisitos e obrigações do presente regulamento, incluindo os poderes para realizar atividades de fiscalização do mercado. ex postque podem ser integrados, quando apropriado, nos seus mecanismos e procedimentos de supervisão existentes ao abrigo da legislação relevante da União em matéria de serviços financeiros. É adequado prever que, ao atuarem como autoridades de fiscalização do mercado ao abrigo do presente regulamento, as autoridades nacionais responsáveis pela supervisão das instituições de crédito regulamentadas ao abrigo da Diretiva 2013/36/UE que participam no Mecanismo Único de Supervisão estabelecido pelo Regulamento (UE) n.º 107/2013 sejam obrigadas a atuar como autoridades de fiscalização do mercado ao abrigo do presente regulamento.qualquer1024/2013 do Conselho (52) comunicar sem demora ao Banco Central Europeu quaisquer informações obtidas no decurso das suas atividades de vigilância do mercado que possam ser relevantes para as tarefas 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 reguladas pela Diretiva 2013/36/UE, é também adequado integrar algumas das obrigações processuais dos prestadores relativas à gestão de riscos, à vigilância pós-comercialização e à documentação nas obrigações e procedimentos em vigor ao abrigo da Diretiva 2013/36/UE. A fim de evitar sobreposições, devem também ser previstas exceções limitadas em relação ao sistema de gestão da qualidade dos fornecedores e à obrigação de monitorização imposta aos responsáveis pela implementação de sistemas de IA de alto risco, na medida em que estas se apliquem às instituições de crédito regulamentadas pela Diretiva 2013/36/UE. O mesmo regime deve ser aplicado às empresas de seguros e resseguros e às sociedades holding de seguros regulamentadas pela Diretiva 2009/138/CE, aos intermediários de seguros regulamentados pela Diretiva (UE) 2016/97 e a outros tipos de instituições financeiras sujeitas a requisitos de governação, sistemas ou processos internos estabelecidos pela legislação relevante da União em matéria de serviços financeiros, a fim de garantir a coerência e a igualdade de tratamento no setor financeiro.

(159) Cada autoridade de fiscalização do mercado para sistemas de IA de alto risco no domínio da biometria enumerados num anexo ao presente regulamento, na medida em que tais sistemas sejam utilizados para fins de aplicação da lei, de gestão da migração, do asilo e do controlo de fronteiras, ou de administração da justiça e de processos democráticos, deverá ter poderes de investigação e correção eficazes, incluindo, pelo menos, o poder de obter acesso a todos os dados pessoais que estejam a ser tratados e a todas as informações necessárias ao desempenho das suas funções. As autoridades de fiscalização do mercado devem poder exercer seus poderes agindo com total independência. Qualquer limitação ao seu acesso a dados operacionais sensíveis ao abrigo do presente regulamento não deverá prejudicar os poderes que lhes são conferidos pela Diretiva (UE) 2016/680. Qualquer exclusão da divulgação de dados às autoridades nacionais de proteção de dados ao abrigo do presente regulamento não deverá afetar os poderes atuais ou futuros dessas autoridades que vão além do âmbito do presente regulamento.

(160) As autoridades de fiscalização do mercado e a Comissão deverão poder propor actividades conjuntas, incluindo investigações conjuntas, a serem realizadas pelas autoridades de fiscalização do mercado ou pelas autoridades de fiscalização do mercado em conjunto com a Comissão, com o objetivo de promover o cumprimento, detetar o incumprimento, sensibilizar e fornecer orientações em relação ao presente regulamento no que diz respeito a categorias específicas de sistemas de IA de alto risco que apresentam um risco grave em dois ou mais Estados-Membros. Essas atividades conjuntas para promover o cumprimento devem ser realizadas em conformidade com o artigo 9.º do Regulamento (UE) 2019/1020. O Gabinete de Inteligência Artificial deve fornecer apoio de coordenação para investigações conjuntas.

(161) É necessário clarificar as responsabilidades e competências a nível da União e nacional no que diz respeito aos sistemas de IA baseados em modelos de IA para fins gerais. Para evitar a sobreposição de competências, quando um sistema de IA é baseado num modelo de IA de uso geral e o modelo e o sistema são fornecidos pelo

(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, 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 a 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 1799/2008.qualquer1093/2010 (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, relativa à distribuição de seguros (JO L 26 de 2.2.2016, p. 19).

(52) Regulamento (UE) n.ºqualquer1024/2013 do Conselho, de 15 de outubro de 2013, que confere ao Banco Central Europeu atribuições específicas no que diz respeito às políticas relacionadas com a supervisão prudencial das instituições de crédito (JO L 287 de 29.10.2013, p. 1).

pág. 63).

mesmo prestador, a supervisão deverá ser efetuada a nível da União através do Gabinete de IA, que deverá ter para estes efeitos as competências de uma autoridade de fiscalização do mercado na aceção do Regulamento (UE) 2019/1020. Em todos os outros casos, as autoridades nacionais de fiscalização do mercado serão responsáveis pela supervisão dos sistemas de IA. No entanto, para sistemas de IA de uso geral que podem ser usados diretamente por implantadores para pelo menos uma finalidade classificada como de alto risco, as autoridades de fiscalização de mercado devem cooperar com o AI Office para realizar avaliações de conformidade e relatar sobre elas ao AI Council e outras autoridades de fiscalização de mercado. Além disso, as autoridades de fiscalização do mercado devem poder solicitar a assistência do Gabinete de IA quando a autoridade de fiscalização do mercado não conseguir concluir uma investigação sobre um sistema de IA de alto risco devido à sua incapacidade de aceder a determinadas informações relativas ao modelo de IA de uso geral no qual o sistema de IA de alto risco se baseia. Nesses casos, deve-se aplicarmutatis mutandiso procedimento de assistência mútua transfronteiriça previsto no Capítulo VI do Regulamento (UE) 2019/1020.

(162) A fim de tirar o máximo partido da centralização de conhecimentos especializados e das sinergias daí resultantes a nível da União, a Comissão deverá dispor de poderes para supervisionar e monitorizar o cumprimento das obrigações dos fornecedores de modelos de IA para fins gerais. O Gabinete de IA deverá poder realizar todas as ações necessárias para monitorizar a aplicação efetiva do presente regulamento no que diz respeito aos modelos de IA de uso geral. Deverá poder investigar potenciais violações das regras relativas aos fornecedores de modelos de IA para fins gerais, tanto por iniciativa própria, na sequência dos resultados das suas atividades de supervisão, como a pedido das autoridades de fiscalização do mercado, em conformidade com as condições estabelecidas no presente regulamento. Para promover uma supervisão eficaz, o AI Office deve prever a possibilidade de fornecedores a jusante apresentarem reclamações sobre potenciais violações das regras relativas a fornecedores de sistemas e modelos de IA de uso geral.

(163) A fim de complementar os sistemas de governação dos modelos de IA de uso geral, o grupo de peritos científicos deverá contribuir para as atividades de supervisão do Gabinete de IA e, em certos casos, poderá fornecer alertas qualificados ao Gabinete de IA, desencadeando ações de acompanhamento, como investigações. Este deve ser o caso quando o grupo de peritos científicos tiver motivos para suspeitar que um modelo de IA de uso geral apresenta um risco específico e identificável a nível da União. Este também deve ser o caso quando o grupo de especialistas científicos tiver motivos para suspeitar que um modelo de IA de uso geral atende aos critérios que levariam à sua classificação como um modelo de IA de uso geral com risco sistêmico. Para fornecer ao grupo de peritos científicos as informações necessárias para o desempenho dessas funções, deve haver um mecanismo que permita ao grupo de peritos científicos solicitar à Comissão que solicite documentação ou informações de um fornecedor.

(164) O Instituto de IA deverá poder tomar as medidas necessárias para monitorizar a implementação efetiva e o cumprimento das obrigações dos fornecedores de modelos de IA para fins gerais estabelecidas no presente regulamento. O Gabinete de IA deverá poder investigar potenciais infrações de acordo com os poderes previstos no presente regulamento, por exemplo, solicitando documentação e informações, realizando avaliações e solicitando medidas aos fornecedores de modelos de IA de uso geral. Ao realizar avaliações, para ter experiência independente, o IA Office deve poder recorrer a especialistas independentes para realizar avaliações em seu nome. O cumprimento das obrigações deve ser possível por meio, entre outros, de solicitações de medidas apropriadas, incluindo medidas de mitigação de riscos quando forem identificados riscos sistêmicos, bem como restrição de comercialização, retirada ou recolhimento do modelo. Como salvaguarda, sempre que necessário, além dos direitos processuais previstos no presente regulamento, os fornecedores de modelos de IA para fins gerais deverão ter os direitos processuais previstos no artigo 18.º do Regulamento (UE) 2019/1020, que deverão ser aplicáveismutatis mutandis,sem prejuízo dos direitos processuais mais específicos previstos no presente regulamento.

(165) O desenvolvimento de sistemas de IA que não sejam sistemas de IA de alto risco, em conformidade com os requisitos estabelecidos no presente regulamento, pode conduzir a uma adoção mais ampla de IA ética e fiável na União. Os provedores de sistemas de IA de risco não alto devem ser encorajados a criar códigos de conduta, incluindo mecanismos de governança apropriados, visando encorajar a implementação voluntária de todos ou parte dos requisitos aplicáveis a sistemas de IA de risco alto, adaptados levando em conta a finalidade pretendida dos sistemas e o menor risco representado e levando em conta as soluções técnicas disponíveis e as melhores práticas do setor, como cartões de modelo e de dados. Os provedores também devem ser encorajados e, quando apropriado, os responsáveis pela implementação de todos os sistemas de IA, sejam eles de alto risco ou não, e modelos de IA, para aplicar, numa base voluntária, requisitos adicionais relacionados, por exemplo, com os elementos das Diretrizes Éticas da União para uma IA Fiável, a sustentabilidade ambiental, as medidas de literacia em

no campo da IA, inclusão e diversidade na concepção e desenvolvimento de sistemas de IA, incluindo a consideração de pessoas vulneráveis e acessibilidade para pessoas com deficiência; envolvimento das partes interessadas, envolvendo, conforme apropriado, partes interessadas relevantes, como organizações empresariais e da sociedade civil, academia, órgãos de pesquisa, sindicatos e organizações de proteção ao consumidor, na concepção e desenvolvimento de sistemas de IA; e diversidade de equipes de desenvolvimento, inclusive no que diz respeito à paridade de gênero. Para garantir a eficácia dos códigos de conduta voluntários, eles devem ser baseados em objetivos claros e indicadores-chave de desempenho que permitam mensurar o alcance desses objetivos. Eles também devem ser desenvolvidos de forma inclusiva, quando apropriado, com o envolvimento de partes interessadas relevantes, como organizações empresariais e da sociedade civil, academia, órgãos de pesquisa, sindicatos e organizações de proteção ao consumidor. A Comissão poderia formular iniciativas, inclusive em nível setorial, destinadas a facilitar a redução de barreiras técnicas ao intercâmbio transfronteiriço de dados para o desenvolvimento da IA, inclusive em relação à infraestrutura de acesso a dados e à interoperabilidade semântica e técnica de diferentes tipos de dados.

(166) É importante que os sistemas de IA associados a produtos que não são considerados de alto risco pelo presente regulamento e que, por conseguinte, não são obrigados a cumprir os requisitos estabelecidos para os sistemas de IA de alto risco sejam, No entanto, eles são seguros quando introduzidos no mercado ou colocados em serviço. Para contribuir para este objectivo, o Regulamento (UE) 2023/988 do Parlamento Europeu e do Conselho ([53]).

(167) 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 nacional, a fim de assegurar uma cooperação fiável e construtiva entre as autoridades competentes a nível da União e nacional. Devem desempenhar as suas funções e atividades de forma a proteger, em particular, os direitos de propriedade intelectual e industrial, as informações comerciais confidenciais e os segredos comerciais, a implementação eficaz deste Regulamento, os interesses da segurança pública e nacional, a integridade dos processos penais e administrativos e a integridade das informações classificadas.

(168) O cumprimento do presente regulamento deverá ser executável através da imposição de sanções e de outras medidas coercivas. Os Estados-Membros deverão tomar todas as medidas necessárias para garantir a aplicação das disposições do presente regulamento, nomeadamente através da previsão de sanções eficazes, proporcionais e dissuasivas para as infracções, e respeitar o princípio daninguém menos que o mesmo.A fim de reforçar e harmonizar as sanções administrativas por infrações ao presente regulamento, deverão ser estabelecidos limites para a imposição de coimas administrativas no caso de determinadas infrações específicas. Ao determinar o montante das multas, os Estados-Membros devem ter em conta, em cada caso individual, todas as circunstâncias relevantes da situação em questão, tendo em conta, em especial, a natureza, a gravidade e a duração da infração e as suas consequências, bem como a dimensão do fornecedor, em especial se se trata de uma PME ou de uma start-up. A Autoridade Europeia para a Proteção de Dados deverá ter poderes para impor coimas às instituições, organismos, gabinetes e agências da União abrangidos pelo âmbito de aplicação do presente regulamento.

(169) Deverá ser possível impor o cumprimento das obrigações impostas ao abrigo do presente regulamento aos fornecedores de modelos de IA para fins gerais, nomeadamente através da imposição de coimas. Para esse efeito, deverão também ser previstas multas de montante adequado em caso de incumprimento dessas obrigações, incluindo o incumprimento das medidas solicitadas pela Comissão nos termos do presente regulamento, sujeitas aos prazos de prescrição relevantes, em conformidade com o princípio da proporcionalidade. Todas as decisões tomadas pela Comissão ao abrigo do presente regulamento estão sujeitas a revisão pelo Tribunal de Justiça da União Europeia, em conformidade com as disposições do TFUE, incluindo a jurisdição ilimitada do Tribunal sobre sanções ao abrigo do artigo 261.º do TFUE.

(170) O direito da União e o direito nacional já preveem soluções eficazes para as pessoas singulares e coletivas cujos direitos e liberdades são afetados negativamente pela utilização de sistemas de IA. Sem prejuízo dessas soluções, qualquer pessoa singular ou coletiva que tenha motivos para crer que houve uma violação 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 uma explicação quando a decisão de um mobilizador se basear principalmente nos resultados de determinados sistemas de IA de alto risco abrangidos pelo âmbito de aplicação do presente regulamento e quando essa decisão produzir efeitos jurídicos.

([53]) Regulamento (UE) 2023/988 do Parlamento Europeu e do Conselho, de 10 de maio de 2023, relativo à segurança geral dos produtos e que altera o Regulamento (UE) n.º 1099/2008 e o Regulamento (UE) n.º 1099/2008 e/ou o Parlamento Europeu e do Conselho, de 10 de maio de 2023, relativo à segurança geral dos produtos e que altera ... qualquer 1025/2012 do Parlamento Europeu e do Conselho e 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).

ou afeta significativamente essas pessoas de forma semelhante, de modo que elas considerem que isso tem um efeito negativo em sua saúde, segurança ou direitos fundamentais. Esta explicação deve ser clara e significativa e servir de base para que as pessoas afetadas exerçam seus direitos. O direito de obter uma explicação não deve aplicar-se à utilização de sistemas de IA para os quais existam exceções ou restrições ao abrigo do direito da União ou nacional, e deve aplicar-se apenas na medida em que este direito ainda não esteja previsto no direito da União.

(172) As pessoas que denunciam violações do presente regulamento deverão ser protegidas pelo direito da União. Por conseguinte, ao comunicar violações do presente regulamento e no que diz respeito à proteção das pessoas que comunicam tais violações, a Diretiva (UE) 2019/1937 do Parlamento Europeu e do Conselho ([54]).

(173) A fim de assegurar que o quadro regulamentar possa ser adaptado quando necessário, o poder de adotar atos em conformidade com o artigo 290.º do TFUE deverá ser delegado na Comissão para alterar as condições em que um sistema de IA não deve ser considerado um sistema de alto risco, a lista de sistemas de IA de alto risco, as disposições relativas à documentação técnica, o conteúdo da declaração de conformidade da UE, as disposições sobre os procedimentos de avaliação da conformidade, as disposições que estabelecem a quais sistemas de IA de alto risco o procedimento de avaliação da conformidade com base na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica deve ser aplicado, o limite, os parâmetros de referência e os indicadores, incluindo a possibilidade de complementar tais parâmetros de referência e indicadores, as regras para classificar modelos de IA de uso geral com risco sistêmico, os critérios para classificar um modelo como um modelo de IA de uso geral com risco sistêmico, a documentação técnica para provedores de modelos de IA de uso geral e as informações de transparência para provedores de modelos de IA de uso geral. É particularmente importante que a Comissão proceda às consultas adequadas durante a fase preparatória, em especial com peritos, e que essas consultas sejam conduzidas em conformidade com os princípios estabelecidos no Acordo Interinstitucional de 13 de abril de 2016 sobre legislar melhor ([55]). Em particular, para garantir a igualdade de participação na preparação de atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os seus peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratam da preparação de atos delegados.

(174) Tendo em conta a rápida evolução tecnológica e o conhecimento necessário para a aplicação eficaz do presente regulamento, a Comissão deverá avaliar e rever o presente regulamento até 2 de agosto de 2029 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 do presente regulamento, a Comissão deverá realizar uma avaliação da necessidade de alterar a lista de sistemas de IA de alto risco e a lista de práticas proibidas uma vez por ano. Além disso, até 2 de agosto de 2028 e, posteriormente, de quatro em quatro anos, a Comissão deve avaliar e comunicar ao Parlamento Europeu e ao Conselho a necessidade de alterar a lista de áreas de alto risco estabelecida no anexo do presente regulamento, os sistemas de IA abrangidos pelo âmbito das obrigações de transparência, a eficácia do sistema de supervisão e governação e o progresso no desenvolvimento de documentos de normalização sobre o desenvolvimento energeticamente eficiente de modelos de IA de uso geral, incluindo a necessidade de medidas ou ações adicionais. Finalmente,
Até 2 de agosto de 2028 e a cada três anos a partir de então, a Comissão deve avaliar o impacto e a eficácia dos códigos de conduta voluntários para incentivar a aplicação dos requisitos definidos para sistemas de IA de alto risco a sistemas de IA que não sejam sistemas de IA de alto risco e possivelmente requisitos adicionais para tais sistemas de IA.

(175) A fim de assegurar condições uniformes para a execução do presente regulamento, deverão ser atribuídas competências de execução à Comissão. Estes poderes devem ser exercidos em conformidade com o Regulamento (UE) n.qualquer182/2011 do Parlamento Europeu e do Conselho ([56]).

(176) Atendendo a que o objectivo do presente regulamento, nomeadamente melhorar o funcionamento do mercado interno e promover a adopção de uma IA centrada no ser humano e fiável, assegurando simultaneamente um elevado nível de protecção da saúde, da segurança e dos direitos fundamentais consagrados na Carta, incluindo a democracia, o Estado de direito e a protecção ambiental, contra os efeitos nocivos dos sistemas de IA na União, bem como apoiando a inovação, não pode ser suficientemente alcançada pelos Estados-Membros, mas pode, devido à sua escala e aos seus efeitos, ser mais bem alcançada ao nível da União, a União pode

([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).
([55]) JO L 123 de 12.5.2016, p. 1.
([56]) Regulamento (UE) n.ºqualquer182/2011 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).

adotar medidas, em conformidade com o princípio da subsidiariedade estabelecido no artigo 5.º do TUE. Em conformidade com o princípio da proporcionalidade estabelecido no mesmo artigo, o presente regulamento não excede o necessário para atingir esse objetivo.

(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 utilização contínua dos sistemas de IA, é adequado que o presente regulamento se aplique aos sistemas de IA de alto risco que tenham sido colocados no mercado ou em serviço antes da data geral de aplicação do presente regulamento, apenas se, a partir dessa data, esses sistemas forem sujeitos a alterações significativas na sua conceção ou finalidade prevista. Deve ser esclarecido que, A este respeito, o conceito de "alteração significativa" deverá ser entendido como sendo equivalente em substância ao de "modificação substancial", que é utilizado apenas no que diz respeito aos sistemas de IA de alto risco, em conformidade com o presente regulamento. A título de exceção e para efeitos de responsabilização pública, os operadores de sistemas de IA que sejam componentes de sistemas informáticos de grande escala estabelecidos por atos jurídicos enumerados num anexo ao presente regulamento e os operadores de sistemas de IA de alto risco destinados à utilização por autoridades públicas deverão, respetivamente, tomar as medidas necessárias para cumprir os requisitos do presente regulamento até ao final de 2030 e, o mais tardar, até 2 de agosto de 2030.

(178) Os fornecedores de sistemas de IA de alto risco são encorajados a começar a cumprir, numa base voluntária, as obrigações relevantes do presente regulamento já durante o período de transição.

(179) O presente regulamento deverá ser aplicável a partir de 2 de agosto de 2026. No entanto, tendo em conta o risco inaceitável associado a determinadas formas de utilização da IA, as proibições, bem como as disposições gerais do presente regulamento, deverão ser aplicáveis já em 2 de fevereiro de 2025. Embora essas proibições não entrem em vigor até depois do estabelecimento da governação e da aplicação do presente regulamento, é importante antecipar a aplicação das proibições, a fim de ter em conta riscos inaceitáveis e de acomodar outros procedimentos, por exemplo, na área do direito civil. Além disso, a infraestrutura relacionada à governança e o sistema de avaliação de conformidade devem estar operacionais até essa data, de modo que as disposições relativas aos organismos notificados e à estrutura de governança devem ser aplicadas a partir de 2 de agosto de 2026. Considerando os rápidos desenvolvimentos tecnológicos e o alto ritmo de adoção de modelos de IA de uso geral, as obrigações para provedores de modelos de IA de uso geral devem ser aplicadas a partir de 2 de agosto de 2025. Os códigos de melhores práticas devem ser finalizados até 2 de maio de 2025 para permitir que os provedores demonstrem conformidade com suas obrigações dentro do prazo planejado. O AI Office deve garantir que os padrões e procedimentos de classificação sejam mantidos atualizados com os desenvolvimentos tecnológicos. Os Estados-Membros devem também estabelecer e informar a Comissão sobre as regras relativas às sanções, incluindo multas administrativas, e garantir que estas são aplicadas de forma adequada e eficaz até à data de aplicação do presente regulamento. As disposições sobre sanções devem, portanto, ser aplicadas a partir de 2 de agosto de 2025.

(180) A Autoridade Europeia para a Proteção de Dados e o Comité Europeu para a Proteção de Dados, que foram consultados nos termos do artigo 42.º, n.os 1 e 2, do Regulamento (UE) 2018/1725, emitiram o seu parecer conjunto em 18 de junho de 2021.

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1

Objeto

1. O objetivo do presente regulamento é melhorar o funcionamento do mercado interno e promover a adoção de inteligência artificial (IA) centrada no ser humano e confiável, garantindo ao mesmo tempo 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 ambiental, contra os efeitos nocivos dos sistemas de IA («sistemas de IA») na União e apoiando a inovação.

2. O presente regulamento dispõe:

(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 alto risco e obrigações para os operadores desses sistemas;

(d) regras de transparência harmonizadas aplicáveis a determinados sistemas de IA;

(e) normas harmonizadas para a colocação no mercado de modelos de IA para fins gerais;

(f) regras sobre monitorização do mercado, vigilância do mercado, governação e garantia de conformidade;

g) medidas de apoio à inovação, com especial atenção às PME, incluindo as start-ups.

Artigo 2

Âmbito de aplicação

1. O presente regulamento aplica-se a:

(a) prestadores que coloquem no mercado ou em serviço sistemas de IA ou que coloquem no mercado modelos de IA para utilização geral na União, independentemente de esses prestadores estarem estabelecidos ou localizados na União ou num país terceiro;

(b) os responsáveis pela implementação de sistemas de IA estabelecidos ou localizados na União;

(c) prestadores e responsáveis pela implementação de sistemas de IA que estejam estabelecidos ou localizados num país terceiro, onde os resultados gerados pelo sistema de IA sejam utilizados na União;

d) importadores e distribuidores de sistemas de IA;

(e) fabricantes de produtos que colocam no mercado ou em serviço um sistema de IA juntamente com o seu produto e sob o seu próprio nome ou marca;

(f) representantes autorizados de fornecedores que não estejam estabelecidos na União;

(g) pessoas afetadas localizadas na União.

2. Para sistemas de IA classificados como sistemas de IA de alto risco de acordo com o Artigo 6(1) e relacionados com produtos regulados pelos atos legislativos de harmonização da União listados na Secção B do Anexo I, apenas o Artigo 6(1), os Artigos 102 a 109 e o Artigo 112 serão aplicáveis. O Artigo 57 será aplicável apenas na medida em que os requisitos para sistemas de IA de alto risco ao abrigo do presente Regulamento tenham sido integrados nesses atos legislativos de harmonização da União.

3. O presente regulamento não se aplica a domínios que não sejam abrangidos pelo âmbito de aplicação do direito da União e não afeta, em caso algum, as competências dos Estados-Membros em matéria de segurança nacional, independentemente do tipo de entidade à qual os Estados-Membros tenham confiado a execução de tarefas relacionadas com essas competências.

O presente regulamento não se aplica aos sistemas de IA que, e na medida em que, sejam colocados no mercado, colocados em serviço ou utilizados, com ou sem modificações, exclusivamente para fins 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 sejam colocados no mercado ou em serviço na União, caso os seus resultados sejam utilizados na União exclusivamente para fins militares, de defesa ou de segurança nacional, independentemente do tipo de entidade que realiza essas atividades.

4. O presente regulamento não se aplica às autoridades públicas de países terceiros ou às organizações internacionais abrangidas pelo âmbito de aplicação do presente regulamento nos termos do n.º 1, caso essas autoridades ou organizações utilizem sistemas de IA no âmbito de acordos ou de cooperação internacionais para efeitos de aplicação da lei e de cooperação judiciária com a União ou com um ou mais Estados-Membros, desde que esse país terceiro ou organização internacional ofereça garantias suficientes no que diz respeito à proteção dos 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 aos sistemas ou modelos de IA, incluindo os seus resultados, desenvolvidos e colocados em serviço especificamente para fins de investigação e desenvolvimento científico.

7. A legislação da União relativa à proteção de dados pessoais, à privacidade e à confidencialidade das comunicações aplica-se aos dados pessoais tratados em relação aos direitos e obrigações estabelecidos no presente regulamento. O presente regulamento não afeta os Regulamentos (UE) 2016/679 ou (UE) 2018/1725 nem as Diretivas 2002/58/CE ou (UE) 2016/680, sem prejuízo do artigo 10.º, n.º 5, e do artigo 59.º do presente regulamento.

8. O presente regulamento não se aplica a quaisquer atividades de investigação, ensaio ou desenvolvimento relacionadas com sistemas de IA ou modelos de IA antes da sua colocação no mercado ou entrada em serviço. Essas atividades serão realizadas de acordo com a legislação aplicável da União. Testes em condições reais não serão cobertos por esta exclusão.

9. O presente regulamento não prejudica as regras estabelecidas por outros atos jurídicos da União relativos à proteção do consumidor e à segurança dos produtos.

10. O presente regulamento não se aplica às obrigações dos implantadores que sejam pessoas singulares que utilizem sistemas de IA no exercício de uma atividade puramente pessoal e não profissional.

11. O presente regulamento não impede a União ou os Estados-Membros de manterem ou introduzirem leis, regulamentos ou disposições administrativas mais favoráveis aos trabalhadores no que diz respeito à proteção dos seus direitos no que diz respeito à utilização de sistemas de IA pelos empregadores ou que incentivem ou permitam a aplicação de convenções coletivas mais favoráveis aos trabalhadores.

12. O presente regulamento não se aplica aos sistemas de IA divulgados ao abrigo de licenças livres e de código aberto, a menos que sejam colocados no mercado ou em serviço como sistemas de IA de alto risco ou como sistemas de IA abrangidos pelo âmbito de aplicação do artigo 5.º ou do artigo 50.º.

Artigo 3

Definições

Para efeitos do presente regulamento, entende-se por:

1) «Sistema de IA» significa um sistema baseado em máquinas que é concebido para operar com diferentes níveis de autonomia e que pode apresentar capacidade de adaptação após a implementação, e que, para fins explícitos ou implícitos, infere a partir das informações de entrada que recebe como gerar resultados de saída, tais como previsões, conteúdos, recomendações ou decisões, que podem influenciar ambientes físicos ou virtuais;

2) «risco» significa a combinação da probabilidade de ocorrência de danos e da gravidade desses danos;

3) «provedor» significa uma pessoa singular ou coletiva, autoridade pública, organismo, agência ou organismo que desenvolve um sistema de IA de uso geral ou um modelo de IA ou para o qual um sistema de IA de uso geral ou um modelo de IA é desenvolvido e o coloca no mercado ou coloca o sistema de IA em serviço sob o seu próprio nome ou marca, seja mediante pagamento ou gratuitamente;

4) «controlador de implementação» significa uma pessoa singular ou coletiva, autoridade pública, organismo, serviço ou agência que utiliza um sistema de IA sob a sua própria autoridade, exceto quando a sua utilização se realiza no âmbito de uma atividade pessoal e não profissional;

5) «representante autorizado» significa uma pessoa singular ou coletiva localizada ou estabelecida na União que recebeu e aceitou um mandato escrito de um fornecedor de um sistema de IA ou de um modelo de IA para fins gerais para cumprir as obrigações e executar os procedimentos estabelecidos no presente regulamento em nome desse fornecedor;

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

7) «distribuidor» significa uma pessoa singular ou coletiva, parte da cadeia de abastecimento, que não seja o fornecedor ou o importador, que coloca um sistema de IA no mercado da União;

8) «operador» significa um fornecedor, fabricante de produtos, implementador, representante autorizado, importador ou distribuidor;

9) «Colocação no mercado», a primeira colocação no mercado da União de um sistema de IA ou de um modelo de IA para fins gerais;

10) «Colocação no mercado» significa o fornecimento de um sistema de IA para fins gerais ou de um modelo de IA para distribuição ou utilização no mercado da União no decurso de uma atividade comercial, mediante pagamento ou gratuitamente;

11) «colocação em serviço» significa o fornecimento de um sistema de IA para a sua primeira utilização diretamente ao implantador ou para sua própria utilização na União para o fim a que se destina;

12) «finalidade pretendida» significa a utilização para a qual um fornecedor concebe um sistema de IA, incluindo o contexto e as condições de utilização específicos, tal como fornecidos pelo fornecedor nas instruções de utilização, nos materiais e declarações promocionais e de vendas, e na documentação técnica;

13) «utilização indevida razoavelmente previsível» significa a utilização de um sistema de IA de uma forma que não está em conformidade com a sua finalidade pretendida, mas que pode resultar do comportamento humano ou da interação com outros sistemas, incluindo outros sistemas de IA, que é razoavelmente previsível;

14) «componente de segurança» significa um componente de um produto ou sistema de IA que desempenha uma função de segurança para esse produto ou sistema de IA, ou cuja falha ou mau funcionamento põe em perigo a saúde e a segurança de pessoas ou bens;

15) «instruções de utilização» significa informações fornecidas pelo fornecedor para informar o responsável pelo tratamento sobre a implementação, em particular, sobre a finalidade pretendida e a utilização correta de um sistema de IA;

16) «recuperação de um sistema de IA» significa qualquer medida destinada a obter a devolução ao fornecedor de um sistema de IA disponibilizado aos responsáveis pela sua implementação, tornando-o inutilizável ou impossibilitando a sua utilização;

17) «retirada de um sistema de IA» significa qualquer medida destinada a impedir a colocação no mercado de um sistema de IA que esteja na cadeia de abastecimento;

18) «desempenho de um sistema de IA» significa a capacidade de um sistema de IA atingir a finalidade pretendida;

19) «autoridade notificadora» significa a autoridade nacional responsável por estabelecer e executar os procedimentos necessários para a avaliação, designação e notificação dos organismos de avaliação da conformidade e para a sua supervisão;

20) «avaliação da conformidade» significa o processo através do qual se demonstra se os requisitos estabelecidos no Capítulo III, Secção 2, foram cumpridos em relação a um sistema de IA de alto risco;

21) «organismo de avaliação da conformidade» significa um organismo que realiza atividades de avaliação da conformidade por terceiros, tais como ensaios, certificação e inspeção;

22) «organismo notificado» significa um organismo de avaliação da conformidade notificado em conformidade com o presente regulamento e outros atos pertinentes da legislação de harmonização da União;

(23) «modificação substancial» significa uma alteração a um sistema de IA após a sua colocação no mercado ou entrada em serviço, que não foi prevista ou planeada na avaliação de conformidade inicial efetuada pelo fornecedor e que afeta a conformidade do sistema de IA com os requisitos estabelecidos no Capítulo III, Secção 2, ou que resulta numa alteração à finalidade pretendida para a qual o sistema de IA em causa foi avaliado;

24) «Marcação CE» significa uma marcação através da qual um fornecedor indica que um sistema de IA cumpre os requisitos estabelecidos no Capítulo III, Secção 2, e outros atos aplicáveis da legislação de harmonização da União que preveem a sua colocação;

(25) «vigilância pós-comercialização» significa quaisquer atividades realizadas por fornecedores de sistemas de IA destinadas a recolher e analisar a experiência adquirida com a utilização de sistemas de IA que colocam no mercado ou em serviço, com vista a identificar a potencial necessidade de implementação imediata de quaisquer medidas corretivas ou preventivas necessárias;

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

27) «norma harmonizada» significa uma norma harmonizada tal como definida no artigo 2.º, n.º 1, alínea c), do Regulamento (UE) n.qualquer1025/2012;

28) «especificação comum» significa um conjunto de especificações técnicas tal como definido no artigo 2.º(4) do Regulamento (UE) n.ºqualquer1025/2012 que prevê meios para cumprir determinados requisitos estabelecidos no presente Regulamento;

29) «dados de treino» significa dados utilizados para treinar um sistema de IA através do ajuste dos seus parâmetros treináveis;

30) «dados de validação» significa dados utilizados para fornecer uma avaliação do sistema de IA treinado e para adaptar os seus parâmetros não treináveis e o seu processo de aprendizagem para, entre outros, evitar o subajuste ou o sobreajuste;

31) «conjunto de dados de validação» significa um conjunto de dados independente ou uma parte do conjunto de dados de treino, obtido por uma divisão fixa ou variável;

32) «dados de teste» significa dados utilizados para fornecer uma avaliação independente do sistema de IA, a fim de confirmar o desempenho pretendido desse sistema antes de ser colocado no mercado ou em serviço;

33) «dados de entrada» significa dados fornecidos ou obtidos diretamente por um sistema de IA a partir dos quais produz um resultado de saída;

34) «dados biométricos» são dados pessoais obtidos através de um tratamento técnico específico e relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, tais como imagens faciais ou dados dactiloscópicos;

35) «identificação biométrica» significa o reconhecimento automatizado de características físicas, fisiológicas, comportamentais ou psicológicas de uma pessoa singular com o objetivo de determinar a identidade de uma pessoa singular através da comparação dos seus dados biométricos com dados biométricos de indivíduos conservados numa base de dados;

36) «verificação biométrica» significa a verificação automatizada individual, incluindo a autenticação, da identidade de pessoas singulares através da comparação dos seus dados biométricos com dados biométricos previamente fornecidos;

37) «categorias especiais de dados pessoais» significa as categorias de dados pessoais referidas no artigo 9.º, n.º 1, do Regulamento (UE) 2016/679, no artigo 10.º da Diretiva (UE) 2016/680 e no artigo 10.º, n.º 1, do Regulamento (UE) 2018/1725;

38) «dados operacionais sensíveis» significa dados operacionais relacionados com a prevenção, detecção, investigação ou repressão de infrações penais, cuja divulgação possa pôr em risco a integridade dos processos penais;

39) «sistema de reconhecimento de emoções» significa um sistema de IA destinado a distinguir ou inferir as emoções ou intenções de pessoas singulares a partir dos seus dados biométricos;

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

41) «sistema de identificação biométrica remota» significa um sistema de IA destinado a identificar pessoas singulares sem a sua participação ativa e, normalmente, remotamente, através da comparação dos seus dados biométricos com os contidos numa base de dados de referência;

42) «sistema de identificação biométrica remota em tempo real» significa um sistema de identificação biométrica remota, no qual a recolha de dados biométricos, a comparação e a identificação ocorrem sem atrasos significativos; Abrange não apenas a identificação instantânea, mas também, para evitar evasões, atrasos mínimos limitados;

43) «sistema de identificação biométrica remota retardada» significa qualquer sistema de identificação biométrica remota que não seja um sistema de identificação biométrica remota em tempo real;

44) «espaço acessível ao público» significa qualquer lugar físico, privado ou público, que pode ser acedido por um número indeterminado de pessoas singulares, independentemente de determinadas condições de acesso terem de ser cumpridas e independentemente de quaisquer restrições de capacidade;

45) "autoridade responsável pela aplicação da lei":

(a) qualquer autoridade pública competente para a prevenção, investigação, detecção ou repressão de infracções penais ou a execução de sanções penais, incluindo a protecção contra ameaças à segurança pública e a sua prevenção, ou

(b) qualquer outro organismo ou entidade a que a legislação do Estado-Membro tenha confiado o exercício da autoridade pública e dos poderes públicos para efeitos de prevenção, investigação, detecção ou repressão de infracções penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública;

46) «aplicação da lei» significa atividades realizadas por ou em nome de autoridades responsáveis pela aplicação da lei para a prevenção, investigação, deteção ou repressão de infrações penais ou a execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção dessas ameaças;

(47) «Gabinete de IA» significa o papel da Comissão no sentido de contribuir para a implementação, monitorização e supervisão de sistemas de IA e modelos de IA para fins gerais, bem como para a governação da IA, tal como previsto na Decisão da Comissão de 24 de janeiro de 2024; As referências no presente regulamento ao Instituto de Auditoria Interna devem ser interpretadas como referências à Comissão;

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

49) «incidente grave» significa um incidente ou mau funcionamento de um sistema de IA que, direta ou indiretamente, resulte em qualquer uma das seguintes consequências:

a) a morte de uma pessoa ou lesão grave à sua saúde;

b) uma perturbação grave e irreversível na gestão ou operação de infraestruturas críticas;

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

d) danos graves à propriedade ou ao meio ambiente;

50) «dados pessoais» significa dados pessoais tal como definidos no ponto 1 do artigo 4.º do Regulamento (UE) 2016/679;

51) «dados não pessoais» significa dados que não sejam dados pessoais, tal como definidos no ponto 1 do artigo 4.º do Regulamento (UE) 2016/679;

52) «criação de perfis» significa a criação de perfis tal como definida no ponto (4) do artigo 4.º do Regulamento (UE) 2016/679;

53) «plano de teste no mundo real» significa um documento que descreve os objetivos, a metodologia, o âmbito geográfico, populacional e temporal, a monitorização, a organização e a condução do teste no mundo real;

54) «plano de sandbox» significa um documento acordado entre o prestador participante e a autoridade competente que descreve os objetivos, as condições, o calendário, a metodologia e os requisitos para as atividades realizadas no sandbox;

(55) «Sandbox de IA» significa um quadro controlado estabelecido por uma autoridade competente que oferece aos fornecedores e potenciais fornecedores de sistemas de IA a possibilidade de desenvolver, treinar, validar e testar, em condições reais, quando adequado, um sistema de IA inovador, de acordo com um plano de sandbox e por um período limitado, sob supervisão regulamentar;

(56) «Literacia em IA» significa as competências, os conhecimentos e a compreensão que permitem aos prestadores, aos mobilizadores e a outras pessoas afetadas, tendo em conta os respetivos direitos e obrigações no contexto do presente regulamento, efetuar uma implementação informada dos sistemas de IA e estar cientes das oportunidades e dos riscos colocados pela IA, bem como dos danos que esta pode causar;

(57) «Testes no mundo real» significa os testes temporários de um sistema de IA para a finalidade a que se destina, em condições reais, fora de um laboratório ou de outro ambiente de simulação, a fim de recolher dados sólidos e fiáveis e de avaliar e verificar a conformidade do sistema de IA com os requisitos do presente regulamento; se todas as condições estabelecidas no artigo 57.º ou 60.º forem cumpridas, o sistema de IA não será considerado colocado no mercado nem colocado em serviço, na aceção do presente regulamento;

58) «sujeito» significa, para efeitos do teste na vida real, uma pessoa singular que participa no teste na vida real;

59) «consentimento informado» significa a expressão livre, específica, inequívoca e voluntária por um sujeito da sua vontade de participar num determinado teste em condições da vida real, após ter sido informado de todos os aspetos do teste que são relevantes para a sua decisão de participar;

60) 'personificação profunda' significa conteúdo de imagem, áudio ou vídeo gerado ou manipulado por IA que se assemelha a pessoas, objetos, lugares, entidades ou eventos da vida real e que pode induzir uma pessoa a acreditar que são autênticos ou verdadeiros;

61) «Infracção generalizada» significa qualquer acto ou omissão contrário ao direito da União que proteja os interesses dos indivíduos e que:

(a) prejudicou ou é susceptível de prejudicar os interesses colectivos de pessoas que residem em pelo menos dois Estados-Membros que não aquele em que:

i) o ato ou omissão teve origem ou ocorreu,

ii) o fornecedor em questão ou, quando aplicável, o seu representante autorizado esteja localizado ou estabelecido, ou

iii) seja identificada a pessoa responsável pela mobilização no momento da prática da infração;

(b) prejudicou, prejudica ou é susceptível de prejudicar os interesses colectivos de indivíduos e tem características comuns – incluindo a mesma prática ilícita ou violação do mesmo interesse – e é cometida simultaneamente pelo mesmo operador em pelo menos três Estados-Membros;

62) «infraestrutura crítica» significa uma infraestrutura crítica tal como definida no ponto (4) do artigo 2.º da Diretiva (UE) 2022/2557;

(63) «Modelo de IA para fins gerais» significa um modelo de IA, incluindo um modelo treinado num grande volume de dados utilizando autossupervisão em larga escala, que apresenta um grau considerável de generalidade e é capaz de executar com competência uma grande variedade de tarefas diferentes, independentemente da forma como o modelo é introduzido no mercado, e que pode ser integrado numa variedade de sistemas ou aplicações a jusante, exceto no caso de modelos de IA que são utilizados para atividades de investigação, desenvolvimento ou prototipagem antes de serem introduzidos no mercado;

64) «capacidades de alto impacto» significa capacidades que correspondem ou excedem as capacidades demonstradas pelos modelos de IA de uso geral mais avançados;

(65) «Risco sistémico», um risco específico das capacidades de elevado impacto dos modelos de IA para fins gerais, que têm um impacto significativo no mercado da União devido ao seu âmbito ou aos seus efeitos negativos reais ou razoavelmente previsíveis na saúde pública, na segurança, na proteção pública, nos direitos fundamentais ou na sociedade no seu todo, e que pode propagar-se em grande escala por toda a cadeia de valor;

66) «sistema de IA de uso geral» significa um sistema de IA que se baseia num modelo de IA de uso geral e que pode servir uma variedade de propósitos, tanto para utilização direta como para integração noutros sistemas de IA;

67) 'operação de ponto flutuante' significa qualquer operação ou tarefa matemática que envolva números de ponto flutuante, que são um subconjunto de números reais normalmente representados em computadores por um inteiro de precisão fixa elevado pelo expoente inteiro de uma base fixa;

68) «provedor a jusante» significa um fornecedor de um sistema de IA, incluindo um sistema de IA de uso geral, que integra um modelo de IA, independentemente de o modelo de IA ser fornecido por si próprio e verticalmente integrado ou ser fornecido por outra entidade ao abrigo de relações contratuais.

Artigo 4º

Alfabetização em IA

Os provedores e implantadores de sistemas de IA devem tomar medidas para garantir que, na maior medida possível, seu pessoal e outras pessoas envolvidas em seu nome na operação e uso de sistemas de IA tenham um nível suficiente de conhecimento em IA, levando em consideração seu conhecimento técnico, experiência, educação e treinamento, bem como o contexto pretendido de uso dos sistemas de IA e as pessoas ou grupos de pessoas com as quais os sistemas de IA serão usados.

CAPÍTULO II

PRÁTICAS DE IA PROIBIDAS

Artigo 5º

Práticas de IA proibidas

1. As seguintes práticas de IA são proibidas:

(a) a colocação no mercado, a colocação em serviço ou a utilização de um sistema de IA que utilize técnicas subliminares que transcendam a consciência de uma pessoa ou técnicas deliberadamente manipuladoras ou enganosas com o objetivo ou efeito de alterar substancialmente o comportamento de uma pessoa ou de um grupo de pessoas, prejudicando assim significativamente a sua capacidade de tomar uma decisão informada e levando-as a tomar uma decisão que de outra forma não teriam tomado, de uma forma que cause, ou seja razoavelmente provável que cause, danos substanciais a essa pessoa, 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 qualquer vulnerabilidade de uma pessoa singular ou de um grupo específico de pessoas, resultante da sua idade ou deficiência, ou de uma situação social ou económica específica, com o propósito ou efeito de alterar 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 substanciais a essa pessoa ou a outra pessoa;

(c) a colocação no mercado, a colocação em serviço ou a utilização de sistemas de IA para avaliar ou classificar pessoas singulares ou grupos de pessoas durante um determinado período de tempo com base no seu comportamento social ou em características pessoais ou de personalidade conhecidas, inferidas ou previstas, de modo que a pontuação do cidadão resultante resulte numa ou mais das seguintes situações:

(i) tratamento prejudicial ou desfavorável de certos indivíduos ou grupos de indivíduos em contextos sociais não relacionados com os contextos em que os dados foram originalmente gerados ou recolhidos,

(ii) tratamento prejudicial ou desfavorável de certos indivíduos ou grupos de indivíduos que seja injustificado ou desproporcional ao seu comportamento social ou à gravidade desse comportamento;

(d) a colocação no mercado, a colocação em serviço para esse fim ou a utilização de um sistema de IA para realizar avaliações de risco de pessoas singulares, a fim de avaliar ou prever o risco de uma pessoa singular cometer uma infração penal com base unicamente na definição do perfil de uma pessoa singular ou numa 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 em atividades criminosas que já se baseie em factos objetivos e verificáveis diretamente relacionados com a atividade criminosa;

(e) a colocação no mercado, a colocação em serviço para esse fim específico ou a utilização de sistemas de IA que criem ou expandam bases de dados de reconhecimento facial através da extracção não selectiva de imagens faciais da Internet ou de circuitos fechados de televisão;

(f) a colocação no mercado, a colocação em serviço para esse fim específico ou a utilização de sistemas de IA para inferir as emoções de uma pessoa singular em locais de trabalho e estabelecimentos de ensino, exceto quando o sistema de IA se destina a ser instalado ou colocado no mercado por razões médicas ou de segurança;

(g) a colocação no mercado, a colocação em serviço para esse fim específico ou a utilização de sistemas de categorização biométrica que classifiquem individualmente pessoas singulares com base nos seus dados biométricos, a fim de deduzir ou inferir a sua raça, opiniões políticas, filiação sindical, crenças religiosas ou filosóficas, vida sexual ou orientação sexual; Esta proibição não inclui a rotulagem ou filtragem de conjuntos de dados biométricos adquiridos legalmente, como imagens, com base em dados biométricos ou a categorização de dados biométricos no campo da aplicação da lei;

(h) a utilização de sistemas remotos de identificação biométrica “em tempo real” em espaços públicos para efeitos de garantia do cumprimento da Lei, exceto e na medida em que tal utilização seja estritamente necessária para atingir um ou mais dos seguintes objetivos:

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

(ii) a prevenção de uma ameaça específica, significativa e iminente à vida ou à segurança física de pessoas singulares ou de uma ameaça genuína e presente ou real e previsível de um ataque terrorista,

(iii) a localização ou identificação de uma pessoa suspeita de ter cometido um crime para efeitos de investigação ou processo criminal ou de execução de uma sanção penal por qualquer um dos crimes referidos no Anexo II que sejam puníveis no Estado-Membro em causa com uma pena ou medida de segurança privativas de liberdade com uma duração máxima de, pelo menos, quatro anos.

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

2. A utilização de sistemas de identificação biométrica remota “em tempo real” em espaços de acesso público para efeitos de garantia do cumprimento da Lei para qualquer das finalidades referidas na alínea h) do primeiro parágrafo do n.º 1 deve ser efetuada para os efeitos previstos nessa alínea, unicamente para confirmar a identidade da pessoa que constitui o alvo específico e deve ter em conta os seguintes aspetos:

(a) a natureza da situação que dá origem à possível utilização e, em particular, a gravidade, a probabilidade e a magnitude dos danos que resultariam se o sistema não fosse utilizado;

(b) as consequências que a utilização do sistema teria sobre os direitos e liberdades das pessoas em causa e, em especial, a gravidade, a probabilidade e a magnitude dessas consequências.

Além disso, a utilização de sistemas remotos de identificação biométrica “em tempo real” em espaços de acesso público para efeitos de garantir o cumprimento da lei para qualquer uma das finalidades referidas na alínea h) do primeiro parágrafo do n.º 1 do presente artigo deverá respeitar as salvaguardas e condições necessárias e proporcionais em relação à utilização, em conformidade com a legislação nacional que autoriza essa utilização, em especial no que diz respeito às limitações temporais, geográficas e pessoais. O uso de um sistema de identificação biométrica remota "em tempo real" em espaços de acesso público só será autorizado se a autoridade responsável pela aplicação da lei tiver concluído uma avaliação de impacto sobre os direitos fundamentais, conforme previsto no artigo 27, e tiver registrado o sistema no banco de dados da UE, de acordo com o artigo 49. No entanto, em casos de urgência devidamente justificados, esses sistemas podem começar a ser usados sem registro no banco de dados da UE, desde que esse registro seja concluído sem demora injustificada.

3. Para efeitos da alínea h) do primeiro parágrafo do n.º 1 e do n.º 2, qualquer utilização de um sistema de identificação biométrica remota "em tempo real" em espaços de acesso público para efeitos de execução estará sujeita a autorização prévia de uma autoridade judicial ou de uma autoridade administrativa independente cuja decisão seja vinculativa para o Estado-Membro em que o sistema será utilizado, a qual será emitida mediante pedido fundamentado e de acordo com as regras pormenorizadas do direito nacional referidas no n.º 5. No entanto, numa situação de urgência devidamente justificada, a utilização de tal sistema pode ser iniciada sem autorização, desde que essa autorização seja solicitada sem demora injustificada, mas o mais tardar no prazo de 24 horas. Se tal permissão for recusada, o uso será descontinuado com efeito imediato e todos os dados, bem como os resultados e informações de saída gerados por tal uso, serão descartados e excluídos imediatamente.

A autoridade judicial competente ou uma autoridade administrativa independente cuja decisão seja vinculativa só concederá autorização se estiver convencida, com base em provas objetivas ou indicações claras que lhe sejam apresentadas, de que a utilização do sistema de identificação biométrica remota "em tempo real" é necessária e proporcional para atingir um dos objetivos especificados na alínea h) do primeiro parágrafo do n.º 1, que deverá ser indicado no pedido e, em particular, se limitar ao estritamente necessário no que diz respeito ao período de tempo, bem como ao âmbito geográfico e pessoal. Ao tomar uma decisão sobre a matéria, essa autoridade levará em consideração os aspectos mencionados no parágrafo 2.

A autoridade não pode adotar nenhuma decisão que produza efeitos jurídicos adversos para uma pessoa apenas com base nos resultados do sistema de identificação biométrica remota "em tempo real".

4. Sem prejuízo do disposto no parágrafo 3, qualquer utilização de um sistema de identificação biométrica remota “em tempo real” em espaços de acesso público para fins de execução deve ser notificada à autoridade de fiscalização do mercado relevante e à autoridade nacional de proteção de dados, de acordo com as regras nacionais referidas no parágrafo 5. A notificação deve conter, no mínimo, as informações especificadas no parágrafo 6 e não deve incluir dados operacionais sensíveis.

5. Os Estados-Membros podem decidir prever a possibilidade de autorizar, no todo ou em parte, a utilização de sistemas de identificação biométrica remotos «em tempo real» em espaços acessíveis ao público para efeitos de execução, dentro dos limites e nas condições estabelecidas na alínea h) do primeiro parágrafo do n.º 1, nos n.ºs 2 e 3. Os Estados-Membros em causa devem estabelecer na sua legislação nacional as regras pormenorizadas necessárias aplicáveis à aplicação, concessão e exercício das autorizações referidas no n.º 3, bem como à monitorização e comunicação de informações relacionadas com as mesmas. Essas regras devem também especificar para que fins, de entre os enumerados na alínea h) do primeiro parágrafo do n.º 1, e, quando adequado, em relação a que infracções referidas na alínea h)(iii), as autoridades competentes podem ser autorizadas a utilizar esses sistemas para fins de aplicação da lei. Os Estados-Membros devem notificar essas regras à Comissão no prazo máximo de 30 dias após a sua adoção. Os Estados-Membros podem, em conformidade com o direito da União, adotar leis mais restritivas sobre a utilização de sistemas de identificação biométrica remota.

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 remotos de identificação biométrica «em tempo real» em espaços de acesso público para efeitos de execução, nos termos do n.º 4, devem apresentar relatórios anuais à Comissão sobre essa utilização. Para o efeito, a Comissão deve fornecer aos Estados-Membros e às autoridades nacionais de fiscalização do mercado e de proteção de dados um modelo que contenha informações sobre o número de decisões tomadas pelas autoridades judiciais competentes ou por uma autoridade administrativa independente cuja decisão é vinculativa em relação aos pedidos de autorização, em conformidade com o n.º 3, bem como o seu resultado.

7. A Comissão publicará relatórios anuais sobre a utilização de sistemas remotos de identificação biométrica "em tempo real" em espaços acessíveis ao público para fins de execução, elaborados com base em dados agregados relativos aos Estados-Membros com base nos relatórios anuais referidos no n.º 6. Esses relatórios anuais não incluirão dados operacionais sensíveis das atividades de execução relacionadas.

8. O presente artigo não afeta as proibições aplicáveis quando uma prática de IA infringe outras disposições do direito da União.

CAPÍTULO III

SISTEMAS DE IA DE ALTO RISCO

SEÇÃO 1

Classificação dos sistemas de IA como sistemas de alto risco

Artigo 6º

Regras de classificação para sistemas de IA de alto risco

1. Independentemente de ter sido colocado no mercado ou em serviço sem estar integrado nos produtos referidos nas alíneas a) e b), um sistema de IA é considerado de alto risco quando preenche ambas as seguintes condições:

(a) o sistema de IA se destina a ser utilizado como um componente de segurança de um produto abrangido pelo âmbito de aplicação dos atos legislativos de harmonização da União enumerados no anexo I, ou o próprio sistema de IA é um desses produtos, e

(b) o produto do qual o sistema de IA é um componente de segurança nos termos da alínea a), ou o próprio sistema de IA enquanto produto, deve ser submetido a uma avaliação de conformidade por terceiros para a sua colocação no mercado ou entrada em serviço, em conformidade com os atos legislativos de harmonização da União enumerados no anexo I.

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

3. Não obstante o disposto no n.º 2, um sistema de IA referido no Anexo III não será considerado de alto risco se não representar um risco significativo de danos à saúde, à segurança ou aos direitos fundamentais das pessoas singulares, nomeadamente não influenciando substancialmente o resultado da tomada de decisões.

O primeiro parágrafo será aplicável quando se verificar qualquer uma das seguintes condições:

a) o sistema de IA se destina a executar uma tarefa processual limitada;

b) que o sistema de IA se destina a melhorar o resultado de uma atividade humana realizada anteriormente;

(c) o sistema de IA se destina a detectar padrões de tomada de decisão ou desvios de padrões anteriores de tomada de decisão e não se destina a substituir ou influenciar julgamentos humanos previamente feitos sem uma revisão humana adequada, ou

(d) o sistema de IA se destina a executar uma tarefa preparatória para uma avaliação que seja relevante para os fins dos casos de utilização enumerados no Anexo III.

Não obstante o primeiro parágrafo, os sistemas de IA referidos no Anexo III serão sempre considerados de alto risco quando o sistema de IA criar perfis de pessoas singulares.

4. Um fornecedor que considere que um sistema de IA referido no Anexo III não apresenta um risco elevado deve documentar a sua avaliação antes de o sistema de IA ser colocado no mercado ou em serviço. Tal prestador estará sujeito à obrigação de registo estabelecida no Artigo 49(2). A pedido das autoridades nacionais competentes, o prestador deverá fornecer a documentação da avaliação.

5. A Comissão, após consulta ao Conselho Europeu de Inteligência Artificial («Conselho da IA»), até 2 de fevereiro de 2026, fornecerá 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 alto risco e de risco não elevado.

6. A Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 97.º, para alterar o segundo parágrafo do n.º 3 do presente artigo, acrescentando novas condições ou alterando as estabelecidas nesse número, sempre que existam provas concretas e fiáveis da existência de sistemas de IA abrangidos pelo âmbito de aplicação do anexo III, mas que não representem um risco significativo de danos para a saúde, a segurança ou os direitos fundamentais das pessoas singulares.

7. A Comissão adota atos delegados, em conformidade com o artigo 97.º, para alterar o segundo parágrafo do n.º 3 do presente artigo, suprimindo qualquer das condições nele estabelecidas, sempre que existam provas específicas 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. Nenhuma alteração às condições estabelecidas no segundo parágrafo do n.º 3, adotada em conformidade com os n.ºs 6 e 7 do presente artigo, reduzirá o nível global de proteção da saúde, da segurança e dos direitos fundamentais previstos no presente regulamento, e qualquer alteração deverá assegurar a coerência com os atos delegados adotados nos termos do artigo 7.º, n.º 1, e ter em conta a evolução tecnológica e do mercado.

Artigo 7

Alterações ao Anexo III

1. A Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 97.º, para alterar o anexo III, acrescentando ou modificando casos de utilização para sistemas de IA de alto risco, sempre que sejam cumpridas ambas as seguintes condições:

(a) os sistemas de IA se destinam a ser utilizados em qualquer uma das áreas enumeradas no anexo III, e

(b) os sistemas de IA representam um risco de danos à saúde e à segurança ou de impactos negativos nos direitos fundamentais, e esse risco é equivalente ou superior ao risco de danos ou de impactos negativos representados pelos sistemas de IA de alto risco já mencionados no Anexo III.

2. Ao avaliar a condição referida no n.º 1, alínea b), a Comissão terá em conta os seguintes critérios:

a) a finalidade pretendida do sistema de IA;

b) a extensão em que um sistema de IA foi ou é provável que venha a ser utilizado;

(c) a natureza e a quantidade dos dados processados e utilizados pelo sistema de IA, em especial quando são processadas categorias especiais de dados pessoais;

(d) o grau de autonomia com que o sistema de IA atua e a possibilidade de um ser humano anular uma decisão ou recomendação que possa resultar em dano;

(e) a medida em que a utilização de um sistema de IA já causou danos à saúde e à segurança, teve impactos negativos nos direitos fundamentais ou deu origem a preocupações significativas quanto à probabilidade de tais danos ou impactos negativos, conforme demonstrado, por exemplo, por relatórios ou alegações documentados apresentados às autoridades nacionais competentes ou quaisquer outros relatórios, conforme apropriado;

(f) a extensão potencial de tais danos ou impactos negativos, em especial no que se refere à sua intensidade e ao seu potencial para afectar várias pessoas ou para afectar desproporcionalmente um determinado grupo de pessoas;

(g) a medida em que as pessoas que podem sofrer tais danos ou tais impactos negativos dependem do resultado gerado por um sistema de IA, em especial porque não é razoavelmente possível, por razões práticas ou legais, optar por não participar em tal resultado;

(h) a medida em que existe um desequilíbrio de poder ou as pessoas que podem sofrer tais danos ou impactos negativos se encontram numa posição de vulnerabilidade em relação à pessoa responsável pela implementação de um sistema de IA, em especial devido à sua situação, autoridade, conhecimento, circunstâncias económicas ou sociais, ou idade;

(i) a medida em que o resultado gerado através de um sistema de IA é facilmente corrigido ou revertido, tendo em conta as soluções técnicas disponíveis para o corrigir ou reverter e sem que os resultados que afetem negativamente a saúde, a segurança ou os direitos fundamentais sejam considerados fáceis de corrigir ou reverter;

(j) a probabilidade de a implementação do sistema de IA resultar em benefícios para indivíduos, comunidades ou sociedade em geral, e a magnitude desse benefício, incluindo potenciais melhorias na segurança do produto;

(k) a medida em que o direito da União aplicável prevê:

(i) soluções eficazes em relação aos riscos colocados por um sistema de IA, excluindo ações de indemnização,

(ii) medidas eficazes para prevenir ou reduzir significativamente tais riscos.

3. A Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 97.º, para alterar a lista do anexo III, suprimindo os sistemas de IA de alto risco, sempre que sejam cumpridas ambas as seguintes condições:

(a) os sistemas de IA de alto risco em causa já não representam riscos significativos para os direitos fundamentais, a saúde ou a segurança, tendo em conta os critérios enumerados no n.º 2;

(b) a supressão não reduz o nível geral de protecção da saúde, da segurança e dos direitos fundamentais ao abrigo do direito da União.

SEÇÃO 2

Requisitos para sistemas de IA de alto risco

Artigo 8

Conformidade com os requisitos

1. Os sistemas de IA de alto risco devem cumprir os requisitos estabelecidos na presente secção, tendo em conta as finalidades pretendidas, bem como o estado da arte geralmente reconhecido em matéria de IA e tecnologias relacionadas com IA. Ao garantir o cumprimento destes requisitos, deve ser tido em conta o sistema de gestão de riscos referido no artigo 9.º.

2. Sempre que um produto contenha um sistema de IA ao qual se apliquem os requisitos do presente regulamento, bem como os requisitos dos atos legislativos de harmonização da União enumerados na secção A do anexo I, os fornecedores serão responsáveis por garantir que o seu produto cumpre integralmente todos os requisitos aplicáveis ao abrigo dos atos legislativos de harmonização da União aplicáveis. A fim de garantir a conformidade dos sistemas de IA de alto risco referidos no parágrafo 1 com os requisitos estabelecidos na presente Seção, e para garantir a consistência, evitar duplicações e minimizar encargos adicionais, os fornecedores podem optar por integrar, conforme apropriado, os processos de teste e comunicação necessários, e as informações e documentação que fornecem em relação ao seu produto, na documentação e nos procedimentos existentes exigidos pela legislação de harmonização da União enumerados na Seção A do Anexo I.

Artigo 9

Sistema de gestão de riscos

1. Deve ser estabelecido, implementado, documentado e mantido um sistema de gestão de riscos em relação aos sistemas de IA de alto risco.

2. O sistema de gestão de riscos deve ser entendido como um processo iterativo contínuo planejado e executado ao longo do ciclo de vida de um sistema de IA de alto risco, que exigirá revisões e atualizações sistemáticas periódicas. Consistirá nas seguintes etapas:

(a) a determinação e análise dos riscos conhecidos e previsíveis que o sistema de IA de alto risco pode representar para a saúde, a segurança ou os direitos fundamentais quando o sistema de IA de alto risco é utilizado de acordo com a finalidade a que se destina;

(b) a estimativa e a avaliação dos riscos que podem surgir quando o sistema de IA de alto risco é utilizado de acordo com a sua finalidade prevista e quando está sujeito a uma utilização indevida razoavelmente previsível;

(c) a avaliação de outros riscos que possam surgir da análise dos dados recolhidos através do sistema de vigilância pós-comercialização referido no artigo 72.º;

(d) a adopção de medidas de gestão de riscos adequadas e específicas, concebidas para fazer face aos riscos identificados em conformidade com a alínea a).

3. Os riscos referidos no presente artigo são apenas aqueles que podem ser razoavelmente mitigados ou eliminados pelo desenvolvimento ou conceção do sistema de IA de alto risco ou pelo fornecimento de informações técnicas adequadas.

4. As medidas de gestão de riscos referidas na alínea d) do n.º 2 devem ter devidamente em conta os efeitos e a potencial interação resultante da aplicação combinada dos requisitos estabelecidos na presente secção, com vista a minimizar os riscos de forma mais eficaz, ao mesmo tempo que se alcança um equilíbrio adequado na aplicação de medidas para satisfazer esses requisitos.

5. As medidas de gestão de riscos referidas na alínea d) do n.º 2 devem considerar os riscos residuais relevantes associados a cada perigo como aceitáveis, bem como o risco residual global dos sistemas de IA de alto risco.

Ao determinar as medidas de gestão de risco mais adequadas, serão procurados os seguintes aspetos:

(a) eliminar ou reduzir os riscos identificados e avaliados em conformidade com o n.º 2, na medida em que seja tecnicamente viável, através da conceção e do desenvolvimento adequados do sistema de IA de alto risco;

b) implementar, quando apropriado, medidas de mitigação e controlo adequadas para fazer face aos riscos que não possam ser eliminados;

(c) fornecer as informações exigidas em conformidade com o artigo 13.º e, quando adequado, fornecer formação aos responsáveis pelo destacamento.

Com o objetivo de eliminar ou reduzir os riscos associados ao uso do sistema de IA de alto risco, deve-se levar em consideração o conhecimento técnico, a experiência, a educação e o treinamento esperados do implantador, bem como o contexto no qual o sistema deve ser usado.

6. Os sistemas de IA de alto risco serão submetidos a testes para determinar as medidas de gestão de risco mais adequadas e específicas. Esses testes devem verificar se os sistemas de IA de alto risco operam de forma consistente com a finalidade pretendida e atendem aos requisitos estabelecidos nesta Seção.

7. Os procedimentos de ensaio podem incluir ensaios em condições reais, em conformidade com o artigo 60.º.

8. Os testes de sistemas de IA de alto risco devem ser realizados, conforme apropriado, a qualquer momento durante o processo de desenvolvimento e, em qualquer caso, antes da sua introdução no mercado ou da sua colocação em serviço. Os testes serão realizados usando parâmetros de probabilidade predefinidos e limites apropriados para a finalidade pretendida do sistema de IA de alto risco.

9. Ao implementar o sistema de gestão de riscos previsto nos parágrafos 1 a 7, os prestadores devem prestar atenção se, tendo em conta a sua finalidade pretendida, o sistema de IA de alto risco é suscetível de afetar negativamente pessoas com menos de dezoito anos e, quando aplicável, outros grupos vulneráveis.

10. No caso de fornecedores de sistemas de IA de alto risco que estejam sujeitos a requisitos relativos a processos internos de gestão de riscos ao abrigo de outras disposições relevantes do direito da União, os aspetos previstos nos n.ºs 1 a 9 podem fazer parte dos procedimentos de gestão de riscos estabelecidos ao abrigo dessa legislação ou ser combinados com eles.

Artigo 10

Dados e governança de dados

1. Os sistemas de IA de alto risco que utilizem técnicas que envolvam o treino de modelos de IA com dados devem ser desenvolvidos utilizando conjuntos de dados de treino, validação e teste que cumpram os critérios de qualidade referidos nos parágrafos 2 a 5 sempre que tais conjuntos de dados sejam utilizados.

2. Os conjuntos de dados de treinamento, validação e teste devem estar sujeitos a práticas de governança e gestão de dados adequadas à finalidade pretendida do sistema de IA de alto risco. Essas práticas se concentrarão, em particular, no seguinte:

a) decisões de projeto relevantes;

b) os processos de coleta de dados e a origem dos dados e, no caso de dados pessoais, a finalidade original da coleta de dados;

c) as operações de tratamento necessárias à preparação dos dados, tais como anotação, etiquetagem, limpeza, atualização, enriquecimento e agregação;

d) a formulação de pressupostos, em particular no que diz respeito à informação que os dados pretendem medir e representar;

e) uma avaliação da disponibilidade, quantidade e adequação dos conjuntos de dados necessários;

(f) o exame de quaisquer preconceitos que possam afetar a saúde e a segurança das pessoas, afetar negativamente os direitos fundamentais ou dar origem a qualquer forma de discriminação proibida pelo direito da União, em especial quando os dados produzidos influenciam os dados introduzidos em transações futuras;

(g) medidas adequadas para detectar, prevenir e atenuar potenciais distorções detectadas em conformidade com a alínea f);

(h) a identificação de lacunas ou deficiências relevantes nos dados que impeçam o cumprimento do presente regulamento e a forma de as corrigir.

3. Os conjuntos de dados de treinamento, validação e teste devem ser relevantes, suficientemente representativos e, na maior medida possível, livres de erros e completos, tendo em vista a finalidade pretendida. Devem também ter propriedades estatísticas adequadas, por exemplo, quando adequado, no que diz respeito às pessoas ou grupos de pessoas em relação às quais o sistema de IA de alto risco se destina a ser utilizado. Os conjuntos de dados podem atender a essas características para cada conjunto de dados individualmente ou para uma combinação de conjuntos de dados.

4. Os conjuntos de dados devem ter em conta, na medida do necessário para a finalidade pretendida, as características ou elementos específicos do ambiente geográfico, contextual, comportamental ou funcional específico em que o sistema de IA de alto risco se destina a ser utilizado.

5. Na medida estritamente necessária para garantir a deteção e correção de enviesamentos associados a sistemas de IA de alto risco, em conformidade com as alíneas f) e g) do n.º 2 do presente artigo, os fornecedores desses sistemas podem, excepcionalmente, tratar categorias especiais de dados pessoais, desde que forneçam salvaguardas adequadas em relação aos direitos e liberdades fundamentais das pessoas singulares. Além das disposições estabelecidas nos Regulamentos (UE) 2016/679 e (UE) 2018/1725 e na Diretiva (UE) 2016/680, para que tal tratamento ocorra, todas as seguintes condições devem ser cumpridas:

a) que o tratamento de outros dados, como dados sintéticos ou anonimizados, não permite a deteção e correção eficazes de enviesamentos;

(b) que categorias especiais de dados pessoais estão sujeitas a limitações técnicas quanto à reutilização de dados pessoais e a medidas de segurança e proteção da privacidade de última geração, incluindo a pseudonimização;

(c) que categorias especiais de dados pessoais estejam sujeitas a medidas para garantir que os dados pessoais processados sejam protegidos e estejam sujeitos a salvaguardas adequadas, incluindo controlos rigorosos e documentação de acesso, a fim de evitar o uso indevido e garantir que apenas pessoas autorizadas tenham acesso a esses dados pessoais com obrigações de confidencialidade adequadas;

(d) que categorias especiais de dados pessoais não sejam transmitidas ou transferidas a terceiros e que estes não possam ter acesso aos mesmos de outra forma;

(e) que categorias especiais de dados pessoais sejam eliminadas quando a parcialidade tiver sido corrigida ou os dados pessoais tiverem atingido o fim do seu período de retenção, consoante o que ocorrer primeiro;

(f) os registos das atividades de tratamento nos termos dos Regulamentos (UE) 2016/679 e (UE) 2018/1725 e da Diretiva (UE) 2016/680 incluem as razões pelas quais o tratamento de categorias especiais de dados pessoais foi estritamente necessário para detetar e corrigir preconceitos e por que esse objetivo não pôde ser alcançado através do tratamento de outros dados.

6. Para o desenvolvimento de sistemas de IA de alto risco que não empreguem técnicas que envolvam o treinamento de modelos de IA, os parágrafos 2 a 5 serão aplicáveis apenas aos conjuntos de dados de teste.

Artigo 11

Documentação técnica

1. A documentação técnica de um sistema de IA de alto risco deve ser desenvolvida antes da sua introdução no mercado ou comissionamento e deve ser mantida atualizada.

A documentação técnica deve ser elaborada de modo a demonstrar que o sistema de IA de alto risco cumpre os requisitos estabelecidos na presente secção e a fornecer às autoridades nacionais competentes e aos organismos notificados as informações necessárias para avaliar a conformidade do sistema de IA com esses requisitos de forma clara e abrangente. Deve conter, no mínimo, os elementos referidos no Anexo IV. As PME, incluindo as start-ups, podem fornecer os elementos da documentação técnica especificados no Anexo IV de forma simplificada. Para esse fim, a Comissão estabelecerá um modelo simplificado de documentação técnica voltada para as necessidades das pequenas e microempresas. Sempre que uma PME, incluindo uma start-up, optar por fornecer as informações exigidas no Anexo IV de forma simplificada, deverá utilizar o formulário referido na presente secção. Os organismos notificados devem aceitar este formulário para fins de avaliação da conformidade.

2. Sempre que um sistema de IA de alto risco associado a um produto abrangido pelo âmbito dos atos legislativos de harmonização da União referidos na secção A do anexo I for colocado no mercado ou colocado em serviço, deve ser elaborado um conjunto único de documentos técnicos que contenha todas as informações referidas no n.º 1, bem como as informações exigidas por esses atos legislativos.

3. A Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 97.º, para alterar o anexo IV, sempre que necessário, a fim de assegurar que, tendo em conta a evolução técnica, a documentação técnica fornece todas as informações necessárias para avaliar se o sistema cumpre os requisitos estabelecidos na presente secção.

Artigo 12

Manutenção de registros

1. Os sistemas de IA de alto risco devem permitir tecnicamente o registro automático de eventos (doravante "arquivos de log") durante todo o ciclo de vida do sistema.

2. Para garantir um nível de rastreabilidade da operação do sistema de IA de alto risco que seja adequado à finalidade pretendida do sistema, as capacidades de registo devem permitir o registo de eventos relevantes para:

(a) a deteção de situações que possam levar a que o sistema de IA de alto risco apresente um risco na aceção do artigo 79.º(1) ou a uma alteração substancial;

(b) a facilitação da vigilância pós-comercialização referida no artigo 72.º, e

(c) a monitorização do funcionamento dos sistemas de IA de alto risco referidos no artigo 26.º, n.º 5.

3. Para os sistemas de IA de alto risco referidos na alínea a) do anexo III, ponto 1, as capacidades de registo devem incluir, pelo menos:

a) um registro do período de cada uso do sistema (a data e hora de início e a data e hora de término de cada uso);

b) a base de dados de referência com a qual o sistema comparou os dados de entrada;

c) os dados de entrada com os quais a pesquisa produziu uma correspondência;

(d) a identificação das pessoas singulares envolvidas na verificação dos resultados referidos no artigo 14.º, n.º 5.

Artigo 13

Transparência e comunicação de informações aos responsáveis pela implantação

1. Os sistemas de IA de alto risco devem ser concebidos e desenvolvidos de forma a garantir que operam com um nível de transparência suficiente para que os seus resultados sejam corretamente interpretados e utilizados pelos responsáveis pela sua implementação. Deve ser garantido um tipo e nível adequados de transparência para permitir que o provedor e o implantador cumpram as obrigações relevantes nos termos da Seção 3.

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

3. As instruções de utilização devem conter, no mínimo, as seguintes informações:

a) a identidade e os dados de contacto do fornecedor e, quando aplicável, do seu representante autorizado;

b) as características, capacidades e limitações do funcionamento do sistema de IA de alto risco, incluindo:

i) a sua finalidade pretendida,

(ii) o nível de precisão (incluindo os parâmetros para a sua medição), robustez e cibersegurança referido no artigo 15.º relativamente ao qual o sistema de IA de alto risco foi testado e validado e que pode ser esperado, bem como quaisquer circunstâncias conhecidas e previsíveis que possam afetar o nível esperado de precisão, robustez e cibersegurança,

(iii) quaisquer circunstâncias conhecidas ou previsíveis associadas à utilização do sistema de IA de alto risco de acordo com a sua finalidade pretendida ou a uma utilização indevida razoavelmente previsível, que possam dar origem a riscos para a saúde e a segurança ou para os direitos fundamentais referidos no artigo 9.º(2);

(iv) quando aplicável, as capacidades e características técnicas do sistema de IA de alto risco para fornecer informações relevantes para explicar os seus resultados,

(v) quando aplicável, a sua operação em relação a determinadas pessoas ou a determinados grupos de pessoas em relação às quais o sistema se destina a ser utilizado,

(vi) quando aplicável, especificações relativas aos dados de entrada, ou quaisquer outras informações relevantes relativas aos conjuntos de dados de formação, validação e teste utilizados, tendo em conta a finalidade pretendida do sistema de IA de alto risco,

(vii) quando aplicável, informações que permitam aos responsáveis pela implementação interpretar os resultados do sistema de IA de alto risco e utilizá-lo adequadamente;

(c) alterações ao sistema de IA de alto risco e ao seu funcionamento pré-determinadas pelo fornecedor no momento da avaliação inicial da conformidade, se aplicável;

(d) as medidas de supervisão humana referidas no artigo 14.º, incluindo medidas técnicas estabelecidas para facilitar a interpretação dos resultados dos sistemas de IA de alto risco pelos responsáveis pela sua implementação;

(e) os recursos informáticos e de hardware necessários, a vida útil esperada do sistema de IA de alto risco e as medidas de manutenção e cuidados necessárias (incluindo a sua frequência) para garantir o funcionamento adequado desse sistema, incluindo no que diz respeito às atualizações do sistema.programas;

(f) quando aplicável, uma descrição dos mecanismos incluídos no sistema de IA de alto risco que permitem aos responsáveis pela implementação recolher, armazenar e interpretar corretamente os ficheiros de registo, em conformidade com o artigo 12.º.

Artigo 14

Supervisão humana

1. Os sistemas de IA de alto risco devem ser concebidos e desenvolvidos de modo a poderem ser monitorizados eficazmente por pessoas singulares durante o período em que estiverem em utilização, nomeadamente através do fornecimento de ferramentas adequadas de interface homem-máquina.

2. O objetivo da supervisão humana será prevenir ou minimizar os riscos para a saúde, a segurança ou os direitos fundamentais que possam surgir quando um sistema de IA de alto risco for utilizado de acordo com a finalidade pretendida ou quando estiver sujeito a uma utilização indevida razoavelmente previsível, em particular quando tais riscos persistirem apesar da aplicação de outros requisitos estabelecidos na presente secção.

3. As medidas de supervisão devem ser proporcionais aos riscos, ao nível de autonomia e ao contexto de utilização do sistema de IA de alto risco e devem ser asseguradas por um dos seguintes tipos de medidas, ou por ambos:

(a) medidas que o fornecedor define e integra, sempre que tecnicamente viável, no sistema de IA de alto risco antes da sua introdução no mercado ou da sua colocação em serviço;

(b) medidas que o fornecedor define antes de o sistema de IA de alto risco ser colocado no mercado ou em serviço e que são adequadas para implementação pelo implementador.

4. Para efeitos da aplicação dos n.os 1, 2 e 3, o sistema de IA de alto risco deve ser oferecido ao responsável pela implantação de modo a que as pessoas singulares encarregadas da supervisão humana possam, conforme adequado e de forma proporcional:

(a) compreender adequadamente as capacidades e limitações relevantes do sistema de IA de alto risco e ser capaz de monitorizar adequadamente o seu funcionamento, por exemplo, com vista a detetar e resolver anomalias, avarias e comportamentos inesperados;

(b) estar ciente da tendência potencial para confiar automaticamente ou excessivamente nos resultados gerados por um sistema de IA de alto risco ("viés de automação"), em particular no caso dos sistemas que são utilizados para fornecer informações ou recomendações para efeitos de tomada de decisões por pessoas singulares;

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

d) decidir, em qualquer situação específica, não utilizar o sistema de IA de alto risco ou descartar, invalidar ou reverter os resultados de saída que ele gera;

e) intervir na operação do sistema de IA de alto risco ou interromper o sistema pressionando um botão de parada ou usando um procedimento semelhante que permita parar o sistema com segurança.

5. No caso de sistemas de IA de alto risco referidos na alínea a) do Anexo III, ponto 1, as medidas referidas no n.º 3 do presente artigo devem também garantir que o responsável pela implantação não atua nem toma qualquer decisão com base na identificação gerada pelo sistema, a menos que essa identificação tenha sido verificada e confirmada separadamente por, pelo menos, duas pessoas singulares com a competência, a formação e a autoridade necessárias.

O requisito de verificação por pelo menos duas pessoas singulares distintas não se aplica aos sistemas de IA de alto risco utilizados para fins de aplicação da lei, migração, controlo de fronteiras ou asilo, quando a aplicação deste requisito for considerada desproporcional ao abrigo do direito da União ou nacional.

Artigo 15

Precisão, robustez e segurança cibernética

1. Os sistemas de IA de alto risco devem ser concebidos e desenvolvidos para atingir um nível adequado de precisão, robustez e segurança cibernética e para ter um desempenho consistente nestes aspetos ao longo do seu ciclo de vida.

2. A fim de abordar os aspetos técnicos de como medir os níveis adequados de precisão e robustez estabelecidos no parágrafo 1 e quaisquer outros parâmetros de desempenho relevantes, a Comissão, em cooperação com as partes interessadas e organizações relevantes, como autoridades de metrologia e de avaliação comparativa, deve, conforme apropriado, promover o desenvolvimento de parâmetros de referência e metodologias de medição.

3. As instruções de utilização que acompanham os sistemas de IA de alto risco devem indicar os níveis de precisão desses sistemas, bem como os parâmetros relevantes para medir a sua precisão.

4. Os sistemas de IA de alto risco devem ser tão resilientes quanto possível em relação a erros, falhas ou inconsistências que possam surgir nos próprios sistemas ou no ambiente em que operam, em especial devido à sua interação com pessoas singulares ou outros sistemas. Serão tomadas medidas técnicas e organizacionais a este respeito.

A robustez de sistemas de IA de alto risco pode ser alcançada por meio de soluções de redundância técnica, como backups ou planos de failover.

Os sistemas de IA de alto risco que continuam a aprender após sua introdução no mercado ou comissionamento devem ser desenvolvidos de forma a eliminar ou reduzir, tanto quanto possível, o risco de que resultados de saída potencialmente tendenciosos influenciem as informações de entrada para operações futuras (ciclos de feedback) e a garantir que tais ciclos sejam adequadamente abordados por medidas apropriadas de mitigação de risco.

5. Os sistemas de IA de alto risco serão resistentes a tentativas de terceiros não autorizados de alterar seu uso, resultados de saída ou operação explorando vulnerabilidades no sistema.

Soluções técnicas destinadas a garantir a segurança cibernética de sistemas de IA de alto risco serão adequadas às circunstâncias e riscos relevantes.

Soluções técnicas para abordar vulnerabilidades específicas de IA incluirão, conforme apropriado, medidas para prevenir, detectar, combater, resolver e controlar ataques que tentem manipular o conjunto de dados de treinamento ("envenenamento de dados") ou componentes pré-treinados usados no treinamento ("envenenamento de modelo"), informações de entrada projetadas para fazer com que o modelo de IA cometa um erro ("exemplos adversários" ou "evasão de modelo"), ataques de confidencialidade ou defeitos no modelo.

SEÇÃO 3

Obrigações dos fornecedores e dos responsáveis pela implementação de sistemas de IA de alto risco e de outras partes

Artigo 16

Obrigações dos fornecedores de sistemas de IA de alto risco

Provedores de sistemas de IA de alto risco:

(a) garantir que os seus sistemas de IA de alto risco cumprem os requisitos definidos na secção 2;

(b) indicar no sistema de IA de alto risco ou, quando tal não for possível, na embalagem do sistema ou na documentação que o acompanha, conforme aplicável, o seu nome, nome comercial registado ou marca comercial e o seu endereço de contacto;

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

(d) conservar a documentação referida no artigo 18.º;

(e) quando sob o seu controlo, conservar ficheiros de registo gerados automaticamente pelos seus sistemas de IA de alto risco referidos no artigo 19.º;

(f) garantir que os sistemas de IA de alto risco sejam sujeitos ao procedimento de avaliação da conformidade relevante referido no artigo 43.º antes de serem colocados no mercado ou 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 alto risco ou, quando tal não for possível, na sua embalagem ou documentação que o acompanha, para indicar a conformidade com o presente regulamento, em conformidade com o artigo 48.º;

(i) cumprir as obrigações de registo referidas no artigo 49.º(1);

(j) tomar as medidas corretivas necessárias e fornecer as informações exigidas no artigo 20.º;

(k) demonstrar, mediante pedido fundamentado da autoridade nacional competente, a conformidade do sistema de IA de alto risco com os requisitos estabelecidos na secção 2;

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

Artigo 17

Sistema de gestão da qualidade

1. Os fornecedores de sistemas de IA de alto risco devem estabelecer um sistema de gestão da qualidade para garantir o cumprimento do presente regulamento. Este sistema deve ser registrado de forma sistemática e ordenada em documentação contendo as políticas, procedimentos e instruções e deve contemplar, no mínimo, os seguintes aspectos:

(a) uma estratégia para o cumprimento dos regulamentos, incluindo o cumprimento dos procedimentos de avaliação da conformidade e dos procedimentos para a gestão de modificações em sistemas de IA de alto risco;

(b) as técnicas, os procedimentos e as ações sistemáticas a utilizar na conceção, no controlo e na verificação da conceção do sistema de IA de alto risco;

(c) as técnicas, os procedimentos e as ações sistemáticas a utilizar no desenvolvimento do sistema de IA de alto risco e no seu controlo e garantia de qualidade;

(d) os procedimentos de revisão, teste e validação que serão realizados antes, durante e depois do desenvolvimento do sistema de IA de alto risco, bem como a frequência com que serão executados;

(e) as especificações técnicas, incluindo normas, a aplicar e, quando as normas harmonizadas relevantes não se aplicarem integralmente ou não abrangerem todos os requisitos relevantes estabelecidos na secção 2, os meios a utilizar para garantir que o sistema de IA de alto risco cumpre esses requisitos;

(f) sistemas e procedimentos de gestão de dados, incluindo a sua aquisição, recolha, análise, rotulagem, armazenamento, filtragem, prospeção, agregação, retenção e quaisquer outras operações relacionadas com dados realizadas antes e para a colocação no mercado ou a entrada em funcionamento de sistemas de IA de alto risco;

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

(h) o estabelecimento, a implementação e a manutenção de um sistema de vigilância pós-comercialização, em conformidade com o artigo 72.º;

(i) os procedimentos associados à notificação de um incidente grave nos termos do artigo 73.º;

(j) gerir a comunicação com as autoridades nacionais competentes, outras autoridades relevantes, incluindo aquelas que concedem ou facilitam o acesso aos dados, organismos notificados, outros operadores, clientes ou outras partes interessadas;

k) sistemas e procedimentos para manter registros de toda a documentação e informações relevantes;

l) gestão de recursos, incluindo medidas relacionadas com a segurança do fornecimento;

(m) um quadro de responsabilização que defina as responsabilidades da gestão e de outros funcionários em relação a todos os aspetos listados nesta secção.

2. A aplicação dos aspectos mencionados na seção 1 deve ser proporcional ao tamanho da organização do fornecedor. 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 alto risco com o presente regulamento.

3. Os fornecedores de sistemas de IA de alto risco que estejam sujeitos a obrigações relativas a sistemas de gestão da qualidade ou a uma função equivalente ao abrigo da legislação setorial relevante da União podem incluir os aspetos enumerados no n.º 1 como parte dos sistemas de gestão da qualidade ao abrigo dessa legislação.

4. Para os prestadores que sejam instituições financeiras sujeitas a requisitos relativos à sua governação, sistemas ou processos internos ao abrigo da legislação da União sobre serviços financeiros, a obrigação de estabelecer um sistema de gestão da qualidade será considerada cumprida, exceto em relação às alíneas g), h) e i) do n.º 1 do presente artigo, quando forem respeitadas as regras relativas aos sistemas ou processos de governação interna ao abrigo da legislação da União aplicável em matéria de serviços financeiros. Para este efeito, serão tidas em conta todas as normas harmonizadas referidas no artigo 40.º.

Artigo 18

Conservação de documentação

1. Durante um período de dez anos a contar da colocação no mercado ou da entrada em serviço do sistema de IA de alto risco, o fornecedor deve manter à disposição das autoridades nacionais competentes:

a) a documentação técnica referida no artigo 11.º;

(b) a documentação relativa ao sistema de gestão da qualidade referido no artigo 17.º;

c) documentação relativa às alterações aprovadas pelos organismos notificados, se aplicável;

(d) decisões e outros documentos emitidos por organismos notificados, quando aplicável;

(e) a declaração UE de conformidade referida no artigo 47.º.

2. Cada Estado-Membro determinará as condições em que a documentação referida no n.º 1 permanecerá à disposição das autoridades nacionais competentes durante o período referido nesse número nos casos em que um fornecedor ou o seu representante autorizado estabelecido no seu território entre em falência ou deixe de operar antes do final desse período.

3. Os prestadores que sejam instituições financeiras sujeitas a requisitos relativos à sua governação, sistemas ou processos internos ao abrigo da legislação da União sobre serviços financeiros devem manter a documentação técnica como parte da documentação mantida ao abrigo da legislação da União sobre serviços financeiros relevante.

Artigo 19

Arquivos de log gerados automaticamente

1. Os fornecedores de sistemas de IA de alto risco devem conservar os ficheiros de registo referidos no artigo 12.º, n.º 1, que são gerados automaticamente pelos sistemas de IA de alto risco, na medida em que tais ficheiros estejam sob o seu controlo. Sem prejuízo da legislação da União ou nacional aplicável, os ficheiros de registo devem ser conservados durante um período de tempo adequado à finalidade pretendida do sistema de IA de alto risco, pelo menos seis meses, salvo disposição em contrário da legislação da União ou nacional aplicável, em especial da legislação da União relativa à proteção de dados pessoais.

2. Os provedores que são instituições financeiras sujeitas a requisitos relacionados à sua governança, sistemas ou processos internos sob a lei de serviços financeiros da União devem manter arquivos de log gerados automaticamente por seus sistemas de IA de alto risco como parte da documentação mantida sob a lei de serviços financeiros relevante.

Artigo 20

Medidas corretivas e obrigações de comunicação

1. Os fornecedores de sistemas de IA de alto risco que considerem ou tenham motivos para considerar que um sistema de IA de alto risco que colocaram no mercado ou em serviço não está em conformidade com o presente regulamento devem tomar imediatamente as medidas corretivas necessárias para o tornar conforme, retirá-lo do mercado, desativá-lo ou recuperá-lo, conforme o caso. Deverão informar os distribuidores do sistema de IA de alto risco em questão e, quando aplicável, os responsáveis pela implementação, o representante autorizado e os importadores.

2. Sempre que um sistema de IA de alto risco apresentar um risco na aceção do artigo 79.º, n.º 1, e o fornecedor estiver ciente desse risco, o fornecedor deve investigar imediatamente as causas, em colaboração com o implementador que notificou o sistema, se aplicável, e informar as autoridades de fiscalização do mercado competentes para o sistema de IA de alto risco em causa e, se aplicável, o organismo notificado que emitiu um certificado para esse sistema, em conformidade com o artigo 44.º, em particular sobre a natureza da não conformidade e quaisquer medidas corretivas tomadas.

Artigo 21

Cooperação com autoridades competentes

1. Os fornecedores de sistemas de IA de alto risco devem, mediante solicitação fundamentada de uma autoridade competente, fornecer a essa autoridade todas as informações e documentação necessárias para demonstrar a conformidade do sistema de IA de alto risco com os requisitos estabelecidos na Seção 2, em um idioma que seja facilmente compreensível pela autoridade e que seja uma das línguas oficiais das instituições da União, conforme indicado pelo Estado-Membro em questão.

2. Mediante pedido fundamentado de uma autoridade competente, os prestadores devem também conceder a essa autoridade, quando adequado, acesso aos ficheiros de registo gerados automaticamente do sistema de IA de alto risco referido no artigo 12.º, n.º 1, na medida em que esses ficheiros estejam sob o seu controlo.

3. Qualquer informação obtida por uma autoridade competente nos termos do presente artigo será tratada de acordo com as obrigações de confidencialidade estabelecidas no artigo 78.º.

Artigo 22

Representantes autorizados de provedores de sistemas de IA de alto risco

1. Antes de colocarem os seus sistemas de IA de alto risco no mercado da União, os prestadores estabelecidos em países terceiros devem nomear, por meio de um mandato escrito, um representante autorizado estabelecido na União.

2. Os fornecedores devem permitir que seu representante autorizado execute as tarefas especificadas no mandato recebido do fornecedor.

3. Os representantes autorizados executarão as tarefas especificadas no mandato recebido do fornecedor. Devem fornecer às autoridades de fiscalização do mercado, mediante solicitação, uma cópia do mandato numa das línguas oficiais das instituições da União, conforme indicado pela autoridade competente. Para efeitos do presente regulamento, o mandato deve permitir ao representante autorizado desempenhar as seguintes tarefas:

(a) verificar se a declaração UE de conformidade referida no artigo 47.º e a documentação técnica referida no artigo 11.º foram elaboradas e se o fornecedor efetuou um procedimento de avaliação da conformidade adequado;

(b) manter à disposição das autoridades competentes e das autoridades ou organismos nacionais referidos no artigo 74.º, n.º 10, por um período de 10 anos a contar da colocação no mercado ou da entrada em serviço do sistema de IA de alto risco, os dados de contacto do fornecedor que nomeou o representante autorizado, 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) fornecer a uma autoridade competente, mediante pedido fundamentado, todas as informações e documentação, incluindo as referidas na alínea b) do presente número, necessárias para demonstrar a conformidade de um sistema de IA de alto risco com os requisitos estabelecidos na secção 2, incluindo o acesso aos ficheiros de registo referidos no artigo 12.º, n.º 1, gerados automaticamente por esse sistema, na medida em que esses ficheiros estejam sob o controlo do fornecedor;

(d) cooperar com as autoridades competentes, mediante pedido fundamentado, em todas as ações por estas empreendidas em relação ao sistema de IA de alto risco, em especial para reduzir e atenuar os riscos que este apresenta;

(e) quando aplicável, cumprir as obrigações de registo referidas no artigo 49.º(1) ou, quando o registo for efetuado pelo próprio prestador, garantir que as informações referidas na secção A, ponto 3, do anexo VIII estão corretas.

O mandato deve permitir que o representante autorizado seja contactado pelas autoridades competentes, além do fornecedor ou em substituição deste, relativamente a todas as questões relacionadas com a garantia do cumprimento do presente regulamento.

4. O representante autorizado deve rescindir o mandato se considerar ou tiver motivos para considerar que o fornecedor está em violação das suas obrigações nos termos do presente regulamento. Nesse caso, deverá também informar imediatamente a autoridade de fiscalização do mercado relevante e, se aplicável, o organismo notificado relevante da cessação do mandato e dos motivos desta medida.

Artigo 23

Obrigações dos importadores

1. Antes de colocarem um sistema de IA de alto risco no mercado, os importadores devem garantir que o sistema cumpre o presente regulamento, verificando se:

(a) o fornecedor do sistema de IA de alto risco tenha efetuado o procedimento de avaliação da conformidade relevante referido no artigo 43.º;

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

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

(d) o fornecedor tenha nomeado um representante autorizado em conformidade com o artigo 22(1).

2. Sempre que o importador tiver motivos razoáveis para considerar que um sistema de IA de alto risco não está em conformidade com o presente regulamento, foi falsificado ou está acompanhado de documentação falsificada, o importador não deve colocar o sistema no mercado até que a conformidade seja alcançada. Se o sistema de IA de alto risco apresentar um risco na aceção do artigo 79.º, n.º 1, o importador deve informar o fornecedor do sistema, os representantes autorizados e as autoridades de fiscalização do mercado.

3. Os importadores devem indicar, na embalagem do sistema de IA de alto risco ou na documentação que o acompanha, quando aplicável, o seu nome, nome comercial registado ou marca comercial e o seu endereço de contacto.

4. Enquanto responsáveis por um sistema de IA de alto risco, os importadores devem garantir que as condições de armazenamento ou transporte, quando aplicável, não comprometam a conformidade desse sistema com os requisitos estabelecidos na Seção 2.

5. Os importadores devem conservar, por um período de dez anos a contar da data em que o sistema de IA de alto risco for colocado no mercado ou em serviço, uma cópia do certificado emitido pelo organismo notificado, se aplicável, contendo as instruções de utilização e a declaração UE de conformidade referida no artigo 47.º.

6. Os importadores devem fornecer às autoridades competentes relevantes, mediante solicitação fundamentada, todas as informações e documentação, incluindo as referidas no parágrafo 5, necessárias para demonstrar a conformidade de um sistema de IA de alto risco com os requisitos estabelecidos na Seção 2, em um idioma facilmente compreensível por elas. Para esse efeito, devem também garantir que a documentação técnica possa ser disponibilizada a essas autoridades.

7. Os importadores devem cooperar com as autoridades competentes relevantes em quaisquer medidas por elas tomadas em relação a um sistema de IA de alto risco colocado no mercado pelos importadores, em especial para reduzir e mitigar os riscos por ele apresentados.

Artigo 24

Obrigações dos distribuidores

1. Antes de colocarem um sistema de IA de alto risco no mercado, os distribuidores devem verificar se este ostenta a marcação CE exigida, se é acompanhado de uma cópia da declaração UE de conformidade referida no artigo 47.º e das instruções de utilização, e se o fornecedor e o importador desse sistema, consoante o caso, cumpriram as suas obrigações nos termos do artigo 16.º, alíneas b) e c), e do artigo 23.º, n.º 3, respetivamente.

2. Se um distribuidor considerar ou tiver motivos para acreditar, com base nas informações em sua posse, que um sistema de IA de alto risco não cumpre os requisitos estabelecidos na Seção 2, ele não deverá colocá-lo no mercado até que tal conformidade seja alcançada. Além disso, se o sistema de IA de alto risco apresentar um risco na aceção do artigo 79.º(1), o distribuidor deve informar o fornecedor ou importador do sistema, conforme o caso.

3. Enquanto responsáveis por um sistema de IA de alto risco, os distribuidores devem garantir que as condições de armazenamento ou transporte, quando aplicáveis, não comprometam a conformidade do sistema com os requisitos estabelecidos na Seção 2.

4. Os distribuidores que considerem ou tenham motivos para considerar, com base nas informações em sua posse, que um sistema de IA de alto risco que colocaram no mercado não está em conformidade com os requisitos estabelecidos na Seção 2 devem tomar as medidas corretivas necessárias para colocá-lo em conformidade, retirá-lo do mercado ou recolhê-lo, ou devem garantir que o fornecedor, importador ou outro operador relevante, conforme o caso, tome tais medidas corretivas. Sempre que um sistema de IA de alto risco apresentar um risco na aceção do artigo 79.º, n.º 1, o seu distribuidor deve informar imediatamente o fornecedor ou importador do sistema e as autoridades competentes para o sistema de IA de alto risco em causa, fornecendo-lhe detalhes, em especial, sobre a não conformidade e quaisquer medidas corretivas tomadas.

5. Mediante solicitação fundamentada de uma autoridade competente relevante, os distribuidores de um sistema de IA de alto risco devem fornecer a essa autoridade todas as informações e documentação relacionadas às suas ações nos termos dos parágrafos 1 a 4 que sejam necessárias para demonstrar que o sistema cumpre os requisitos estabelecidos na Seção 2.

6. Os distribuidores devem cooperar com as autoridades competentes relevantes em quaisquer medidas que tomem em relação a um sistema de IA de alto risco colocado no mercado pelos distribuidores, em especial para reduzir ou atenuar os riscos que este apresenta.

Artigo 25

Responsabilidades em toda a cadeia de valor da IA

1. Qualquer distribuidor, importador, implementador ou terceiro será considerado um fornecedor de um sistema de IA de alto risco para efeitos do presente regulamento e estará sujeito às obrigações de fornecedor estabelecidas no artigo 16.º em qualquer uma das seguintes circunstâncias:

(a) quando colocar o seu nome ou marca registada num sistema de IA de alto risco previamente colocado no mercado ou em serviço, sem prejuízo de disposições contratuais que estipulem que as obrigações sejam atribuídas de outra forma;

(b) quando modificar substancialmente um sistema de IA de alto risco que já tenha sido colocado no mercado ou em serviço, de tal forma que continue a ser um sistema de IA de alto risco nos termos do artigo 6.º;

(c) quando modifica a finalidade pretendida de um sistema de IA, incluindo um sistema de IA para fins gerais, que não foi identificado como de alto risco e já foi colocado no mercado ou em serviço, de tal forma que o sistema de IA em causa se torna um sistema de IA de alto risco, em conformidade com o artigo 6.º.

2. Quando se aplicarem as circunstâncias referidas no n.º 1, o fornecedor que inicialmente colocou o sistema de IA no mercado ou o colocou em serviço deixa de ser considerado fornecedor desse sistema de IA específico para efeitos do presente regulamento. O fornecedor inicial deve cooperar estreitamente com os novos fornecedores e fornecer as informações necessárias, o acesso técnico ou outra assistência razoavelmente previsível, conforme necessário, para o cumprimento das obrigações estabelecidas no presente regulamento, em especial no que diz respeito à conformidade com a avaliação da conformidade dos sistemas de IA de alto risco. Esta seção não se aplica nos casos em que o fornecedor inicial indicou claramente que seu sistema de IA não deve ser transformado em um sistema de IA de alto risco e, portanto, não está sujeito à obrigação de fornecer documentação.

3. No caso de sistemas de IA de alto risco que sejam componentes de segurança de produtos abrangidos pelos atos legislativos de harmonização da União enumerados na secção A do anexo I, o fabricante do produto deve ser considerado um fornecedor do sistema de IA de alto risco e deve estar sujeito às obrigações previstas no artigo 16.º numa das seguintes circunstâncias:

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

b) o sistema de IA de alto risco é colocado em serviço sob o nome ou marca do fabricante do produto após o produto ter sido introduzido no mercado.

4. O fornecedor de um sistema de IA de alto risco e o terceiro que fornece um sistema de IA de alto risco, ferramentas, serviços, componentes ou processos que são usados ou integrados num sistema de IA de alto risco devem especificar, por acordo escrito, as informações, capacidades, acesso técnico e outra assistência que são necessárias, com base no estado da arte geralmente reconhecido, para que o fornecedor do sistema de IA de alto risco seja capaz de cumprir integralmente as obrigações estabelecidas no presente regulamento. Esta seção não se aplica a terceiros que disponibilizam ao público ferramentas, serviços, processos ou componentes que não sejam modelos de IA de uso geral sob uma licença gratuita e de código aberto.

O AI Office pode desenvolver e recomendar cláusulas contratuais padrão voluntárias entre provedores de sistemas de IA de alto risco e terceiros que fornecem ferramentas, serviços, componentes ou processos que são usados ou integrados em sistemas de IA de alto risco. Ao desenvolver tais cláusulas contratuais padrão voluntárias, o AI Office levará em consideração potenciais requisitos contratuais aplicáveis em determinados setores ou modelos de negócios. As cláusulas contratuais padrão voluntárias serão publicadas e disponibilizadas gratuitamente em um formato eletrônico de fácil utilização.

5. Os parágrafos 2 e 3 não prejudicam a necessidade de observar e proteger os direitos de propriedade intelectual e industrial, as informações comerciais confidenciais e os segredos comerciais, em conformidade com a legislação da União e nacional.

Artigo 26

Obrigações dos responsáveis pela implementação de sistemas de IA de alto risco

1. Os responsáveis pela implementação de sistemas de IA de alto risco devem tomar medidas técnicas e organizacionais adequadas para garantir que utilizam esses sistemas de acordo com as instruções de utilização que os acompanham, em conformidade com os n.ºs 3 e 6.

2. Os responsáveis pela mobilização devem confiar a supervisão humana a pessoas singulares que tenham a competência, a formação e a autoridade necessárias.

3. As obrigações estabelecidas nos n.os 1 e 2 não afetam quaisquer outras obrigações impostas aos responsáveis pela mobilização pela legislação da União ou nacional, nem a sua liberdade de organizar os seus próprios recursos e atividades, a fim de implementar as medidas de supervisão humana indicadas pelo prestador.

4. Sem prejuízo dos n.os 1 e 2, o responsável pela implantação deve garantir que os dados de entrada sejam relevantes e suficientemente representativos tendo em conta a finalidade pretendida do sistema de IA de alto risco, na medida em que exerça controlo sobre esses dados de entrada.

5. Os implantadores devem monitorizar o funcionamento do sistema de IA de alto risco com base nas instruções de utilização e, quando apropriado, informar os prestadores de acordo com o artigo 72.º. Sempre que os implantadores tenham motivos para considerar que a utilização do sistema de IA de alto risco de acordo com as suas instruções pode resultar num sistema de IA que representa um risco na aceção do artigo 79.º(1), devem, sem demora injustificada, informar o prestador ou distribuidor e a autoridade de fiscalização do mercado relevante e suspender a utilização desse sistema. Caso os responsáveis pela implantação do equipamento detectem um incidente grave, eles também deverão comunicar imediatamente o incidente, primeiro ao fornecedor, depois ao importador ou distribuidor e à autoridade de fiscalização do mercado relevante. Caso o responsável pela implantação não consiga entrar em contato com o provedor, será aplicado o Artigo 73.mutatis mutandis.Esta obrigação não abrangerá dados operacionais sensíveis dos responsáveis pela implantação de sistemas de IA, que são autoridades responsáveis por garantir o cumprimento da lei.

No caso de mobilizadores que sejam instituições financeiras sujeitas a requisitos relativos à sua governação, sistemas ou processos internos ao abrigo da legislação da União em matéria de serviços financeiros, a obrigação de supervisão prevista no primeiro parágrafo será considerada cumprida quando forem respeitadas as regras relativas aos sistemas, processos e disposições de governação interna, em conformidade com a legislação da União em matéria de serviços financeiros aplicável.

6. Os responsáveis pelo tratamento que implementam sistemas de IA de alto risco devem conservar os ficheiros de registo gerados automaticamente pelos sistemas de IA de alto risco, na medida em que tais ficheiros estejam sob o seu controlo, durante um período de tempo adequado à finalidade pretendida do sistema de IA de alto risco, pelo menos seis meses, salvo disposição em contrário da legislação da União ou nacional aplicável, em especial da legislação da União relativa à proteção de dados pessoais.

Os controladores de implantação que são instituições financeiras sujeitas a requisitos relacionados à sua governança, sistemas ou processos internos sob a lei de serviços financeiros da União devem manter os arquivos de log como parte da documentação mantida sob a lei de serviços financeiros da União.

7. Antes de implantar ou usar um sistema de IA de alto risco no local de trabalho, os implantadores que são empregadores devem informar os representantes dos funcionários e os trabalhadores afetados de que eles serão expostos ao uso do sistema de IA de alto risco. Estas informações serão fornecidas, quando adequado, de acordo com as regras e procedimentos estabelecidos na legislação da União e nacional e de acordo com as práticas relativas à informação aos trabalhadores e aos seus representantes.

8. Os responsáveis pela implantação de sistemas de IA de alto risco que sejam autoridades públicas ou instituições, órgãos, gabinetes e agências da União devem cumprir as obrigações de registo referidas no artigo 49.º. Caso esses implantadores verifiquem que o sistema de IA de alto risco que pretendem utilizar não foi registado na base de dados da UE referida no artigo 71.º, não devem utilizar esse sistema e devem informar o fornecedor ou distribuidor.

9. Quando aplicável, os responsáveis pelo tratamento que implementam sistemas de IA de alto risco devem utilizar as informações fornecidas nos termos do artigo 13.º do presente regulamento para cumprir a sua obrigação de realizar uma avaliação de impacto na 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. Não obstante a Diretiva (UE) 2016/680, no contexto de uma investigação cujo objetivo seja a busca seletiva de uma pessoa suspeita ou condenada por ter cometido um crime, a pessoa responsável pela implantação de um sistema de IA de alto risco para identificação biométrica remota de forma diferida deve solicitar,ex anteou sem demora injustificada e no prazo máximo de quarenta e oito horas, a uma autoridade judicial ou administrativa cujas decisões sejam vinculativas e sujeitas a revisão judicial, uma autorização para usar tal sistema, exceto quando for usado para a identificação inicial de um possível suspeito com base em fatos objetivos e verificáveis diretamente relacionados ao crime. Qualquer uso deve ser limitado ao estritamente necessário para investigar um crime específico.

No caso de ser negada a autorização prevista no primeiro parágrafo, o sistema de identificação biométrica remota objeto do pedido de autorização deixará de ser utilizado com efeitos imediatos e os dados pessoais associados à utilização do sistema de IA de alto risco para o qual a autorização foi solicitada serão eliminados.

Este sistema de IA de alto risco para identificação biométrica remota de forma diferida não poderá ser utilizado em nenhuma circunstância para fins de garantir o cumprimento da Lei de forma indiscriminada, sem qualquer relação com um crime, um processo criminal, uma ameaça real e presente ou real e previsível de crime, ou com a busca de uma pessoa desaparecida específica. Deve ser garantido que as autoridades responsáveis pela aplicação da lei não possam tomar nenhuma decisão que produza efeitos jurídicos adversos para uma pessoa apenas com base nos resultados de tais sistemas remotos de identificação biométrica diferida.

A presente secção não prejudica o disposto no artigo 9.º do Regulamento (UE) 2016/679 e no artigo 10.º da Diretiva (UE) 2016/680 para o tratamento de dados biométricos.

Independentemente da finalidade ou da pessoa responsável pela implantação, qualquer uso de tais sistemas de IA de alto risco deverá ser documentado no arquivo de aplicação da lei relevante e disponibilizado mediante solicitação à autoridade de vigilância de mercado relevante e à autoridade nacional de proteção de dados, excluindo a divulgação de dados operacionais sensíveis relacionados à garantia da conformidade com a lei. O presente parágrafo não prejudica os poderes conferidos às autoridades de supervisão pela Diretiva (UE) 2016/680.

Os responsáveis pela implantação deverão apresentar relatórios anuais à autoridade de fiscalização de mercado relevante e à autoridade nacional de proteção de dados sobre o uso de sistemas de identificação biométrica remota, excluindo a divulgação de dados operacionais sensíveis relacionados à garantia da conformidade com a Lei. Os relatórios podem ser agregados para abranger mais de uma implantação.

Os Estados-Membros podem, em conformidade com o direito da União, adotar leis mais restritivas sobre a utilização de sistemas de identificação biométrica remota e diferida.

11. Sem prejuízo do artigo 50.º do presente regulamento, os responsáveis pela implantação de sistemas de IA de alto risco referidos no anexo III que tomem decisões ou auxiliem na tomada de decisões relativas a pessoas singulares devem informar as pessoas singulares de que estão expostas à utilização de sistemas de IA de alto risco. Para sistemas de IA de alto risco utilizados para fins de execução, aplica-se o artigo 13.º da Diretiva (UE) 2016/680.

12. Os implantadores devem cooperar com as autoridades competentes relevantes em quaisquer medidas que tomem em relação ao sistema de IA de alto risco para efeitos de implementação do presente regulamento.

Artigo 27

Avaliação do impacto dos direitos fundamentais em sistemas de IA de alto risco

1. Antes de implementar um dos sistemas de IA de alto risco referidos no artigo 6.º, n.º 2, com exceção dos sistemas de IA de alto risco destinados a serem utilizados no domínio enumerado no ponto 2 do anexo III, os responsáveis pela implementação que sejam organismos de direito público, ou entidades privadas que prestem serviços públicos, e os responsáveis pela implementação dos sistemas de IA de alto risco referidos nas alíneas b) e c) do ponto 5 do anexo III, devem efetuar uma avaliação do impacto que a utilização desses sistemas pode ter nos direitos fundamentais. Para tal, os responsáveis pela implantação realizarão uma avaliação que consistirá em:

(a) uma descrição dos processos do implementador nos quais o sistema de IA de alto risco será utilizado de acordo com a sua finalidade pretendida;

b) uma descrição do período de tempo durante o qual se espera que cada sistema de IA de alto risco seja utilizado e da frequência com que se espera que seja utilizado;

c) as categorias de pessoas singulares e grupos que podem ser afetados pela sua utilização no contexto específico;

(d) os riscos específicos de danos que podem afetar as categorias de pessoas singulares e grupos determinados em conformidade com a alínea c) do presente número, tendo em conta as informações fornecidas pelo fornecedor em conformidade com o artigo 13.º;

e) descrição da aplicação das medidas de monitoramento humano, de acordo com as instruções de uso;

(f) as medidas a tomar no caso de tais riscos se materializarem, incluindo acordos de governação interna e mecanismos de reclamação.

2. A obrigação descrita no parágrafo 1 aplica-se à primeira utilização do sistema de IA de alto risco. Em casos semelhantes, o implementador pode confiar em avaliações de impacto sobre direitos fundamentais conduzidas anteriormente ou em avaliações de impacto existentes conduzidas por provedores. Se, durante a utilização do sistema de IA de alto risco, o responsável pela implantação considerar que algum dos elementos enumerados no n.º 1 sofreu alterações ou deixou de estar atualizado, o responsável pela implantação deverá tomar as medidas necessárias para atualizar as informações.

3. Uma vez efetuada a avaliação referida no n.º 1 do presente artigo, o responsável pela implementação deve comunicar os seus resultados à autoridade de fiscalização do mercado, apresentando o formulário preenchido referido no n.º 5 do presente artigo. No caso referido no artigo 46.º, n.º 1, os responsáveis pela mobilização poderão ser isentos desta obrigação de notificação.

4. Se alguma das obrigações estabelecidas no presente artigo já for cumprida pela 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 referida no n.º 1 do presente artigo complementará essa avaliação de impacto sobre a proteção de dados.

5. O Gabinete de IA deverá desenvolver um questionário modelo, inclusive por meio de uma ferramenta automatizada, para facilitar aos implantadores o cumprimento de suas obrigações nos termos deste artigo de forma simplificada.

SEÇÃO 4

Autoridades notificadoras e organismos notificados

Artigo 28

Autoridades notificadoras

1. Cada Estado-Membro deve nomear ou criar pelo menos uma autoridade notificadora que será responsável por estabelecer e executar os procedimentos necessários para a avaliação, designação e notificação dos organismos de avaliação da conformidade, bem como pela sua supervisão. Estes procedimentos serão desenvolvidos através da cooperação entre as autoridades notificadoras de todos os Estados-Membros.

2. Os Estados-Membros podem decidir que a avaliação e a supervisão referidas no n.º 1 serão realizadas por um organismo nacional de acreditação, na aceção do Regulamento (CE) n.º$_{qualquer}$765/2008 e em conformidade com este.

3. As autoridades notificadoras devem ser constituídas, organizadas e operar de modo a que não surjam conflitos de interesses com os organismos de avaliação da conformidade e a que a imparcialidade e a objetividade das suas atividades sejam garantidas.

4. As autoridades notificadoras devem ser organizadas de modo 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 devem oferecer nem realizar quaisquer atividades realizadas por organismos de avaliação da conformidade, nem quaisquer serviços de consultoria de natureza comercial ou concorrencial.

6. As autoridades notificadoras manterão a confidencialidade das informações obtidas, em conformidade com o disposto no artigo 78.º.

7. As autoridades notificadoras devem dispor de pessoal competente suficiente para desempenhar adequadamente as suas tarefas. Quando apropriado, a equipe relevante terá a experiência necessária para desempenhar suas funções em áreas como tecnologia da informação, IA e direito, incluindo o monitoramento de direitos fundamentais.

Artigo 29

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 em que estão estabelecidos.

2. O pedido de notificação deve ser acompanhado de uma descrição das atividades de avaliação da conformidade, dos módulos de avaliação da conformidade e dos tipos de sistemas de IA para os quais o organismo de avaliação da conformidade se considera competente, bem como de um certificado de acreditação, se houver, emitido por um organismo nacional de acreditação, declarando que o organismo de avaliação da conformidade cumpre os requisitos estabelecidos no artigo 31.º.

Serão acrescentados quaisquer documentos válidos relativos às designações existentes do organismo notificado requerente ao abrigo de qualquer outro ato da legislação de harmonização da União.

3. Se o organismo de avaliação da conformidade em causa não puder fornecer um certificado de acreditação, deverá fornecer à autoridade notificadora todas as provas documentais necessárias para verificar, reconhecer e monitorizar periodicamente o seu cumprimento dos requisitos estabelecidos no artigo 31.º.

4. No que diz respeito aos organismos notificados designados em conformidade com qualquer outra legislação de harmonização da União, todos os documentos e certificados associados a essas designações podem ser utilizados para apoiar o seu procedimento de designação ao abrigo do presente regulamento, conforme adequado. O organismo notificado deve atualizar a documentação referida nos n.os 2 e 3 do presente artigo sempre que ocorram alterações relevantes, para que a autoridade responsável pelos organismos notificados possa monitorizar e verificar se todos os requisitos estabelecidos no artigo 31.º continuam a ser cumpridos.

Artigo 30

Procedimento de notificação

1. As autoridades notificadoras só podem notificar os organismos de avaliação da conformidade que tenham cumprido os requisitos estabelecidos no artigo 31.º.

2. As autoridades notificadoras devem notificar a Comissão e os outros Estados-Membros, através do sistema de notificação eletrónica desenvolvido e gerido pela Comissão, de cada organismo de avaliação da conformidade referido no n.º 1.

3. A notificação referida no n.º 2 do presente artigo deve incluir informações detalhadas sobre as atividades de avaliação da conformidade, os módulos de avaliação da conformidade e os tipos de sistemas de IA afetados, bem como a certificação de competência relevante. Se a notificação não se basear no certificado de acreditação referido no artigo 29.º, n.º 2, a autoridade notificadora deve fornecer à Comissão e aos outros Estados-Membros provas documentais que demonstrem a competência do organismo de avaliação da conformidade e as disposições em vigor para garantir que o organismo é regularmente monitorizado e continua a cumprir os requisitos estabelecidos no artigo 31.º.

4. O organismo de avaliação da conformidade em causa só pode realizar as atividades de um organismo notificado se não for levantada qualquer objeção pela Comissão ou pelos outros Estados-Membros no prazo de duas semanas a contar da notificação por uma autoridade notificadora, caso esta inclua o certificado de acreditação referido no artigo 29.º, n.º 2, ou de dois meses a contar da notificação pela autoridade notificadora, caso esta inclua as provas documentais referidas no artigo 29.º, n.º 3.

5. Caso sejam levantadas objeções, a Comissão iniciará imediatamente consultas com os Estados-Membros relevantes e com o organismo de avaliação da conformidade. Tendo em conta o exposto, a Comissão transmitirá a sua decisão ao Estado-Membro em causa e ao organismo de avaliação da conformidade relevante.

Artigo 31

Requisitos para organismos notificados

1. Os organismos notificados devem ser estabelecidos de acordo com a legislação nacional dos Estados-Membros e devem ter personalidade jurídica.

2. Os organismos notificados devem cumprir os requisitos organizacionais, de gestão da qualidade, de recursos e de processo necessários ao desempenho das suas funções, bem como os requisitos adequados em matéria de cibersegurança.

3. A estrutura organizacional, a distribuição de responsabilidades, as linhas de comunicação e o funcionamento dos organismos notificados devem proporcionar confiança no seu desempenho e nos resultados das atividades de avaliação da conformidade realizadas pelos organismos notificados.

4. Os organismos notificados devem ser independentes do fornecedor de um sistema de IA de alto risco em relação ao qual realizam atividades de avaliação da conformidade. Os organismos notificados devem ser independentes de qualquer outro operador com interesse económico nos sistemas de IA de alto risco que estão a ser avaliados, bem como de qualquer concorrente do fornecedor. Isso não impede o uso de sistemas de IA de alto risco avaliados que sejam necessários para as atividades do organismo de avaliação da conformidade ou o uso de tais sistemas de alto risco para fins pessoais.

5. Os organismos de avaliação da conformidade, a sua alta direção e o pessoal responsável pela execução das tarefas de avaliação da conformidade não devem estar diretamente envolvidos na conceção, desenvolvimento, comercialização ou utilização de tais sistemas de IA de alto risco, nem devem representar as partes que realizam essas atividades. Além disso, não devem realizar nenhuma atividade que possa entrar em conflito com sua independência de julgamento ou sua integridade em relação às atividades de avaliação da conformidade para as quais foram notificados. Isso se aplicará especialmente aos serviços de consultoria.

6. Os organismos notificados devem ser organizados e geridos de modo a garantir a independência, a objetividade e a imparcialidade das suas atividades. Os organismos notificados devem documentar e implementar uma estrutura e procedimentos para garantir a imparcialidade e promover e implementar os princípios de imparcialidade em toda a sua organização, para todos os funcionários e em todas as suas atividades de avaliação.

7. Os organismos notificados devem ter procedimentos documentados para garantir que o seu pessoal, comités, subsidiárias, subcontratantes e todos os organismos associados ou pessoal de organismos externos mantenham, em conformidade com o artigo 78.º, a confidencialidade das informações que chegam à sua posse no desempenho das atividades de avaliação da conformidade, exceto nos casos em que a divulgação seja exigida por lei. O pessoal dos organismos notificados está vinculado ao sigilo profissional no que diz respeito a todas as informações obtidas no exercício das suas funções ao abrigo do presente regulamento, exceto em relação às autoridades notificadoras do Estado-Membro em que exercem as suas atividades.

8. Os organismos notificados devem dispor de procedimentos para a realização das suas atividades que tenham devidamente em conta a dimensão dos prestadores, o setor em que operam, 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, salvo se a responsabilidade for assumida pelo Estado-Membro em que estão estabelecidos ao abrigo da legislação nacional ou se o próprio Estado-Membro for diretamente responsável pela avaliação da conformidade.

10. Os organismos notificados devem ser capazes de executar todas as suas tarefas ao abrigo do presente regulamento com o mais elevado grau de integridade profissional e a competência técnica necessária no domínio específico, quer essas tarefas sejam executadas pelos próprios organismos notificados, quer em seu nome e sob a sua responsabilidade.

11. Os organismos notificados devem ter competência técnica interna suficiente para poderem avaliar eficazmente as tarefas realizadas em seu nome por intervenientes externos. O organismo notificado deve dispor permanentemente de pessoal administrativo, técnico, jurídico e científico suficiente com experiência e conhecimento dos tipos relevantes de sistemas de IA, dados e computação de dados e dos requisitos estabelecidos na Secção 2.

12. Os organismos notificados devem participar nas atividades de coordenação previstas no artigo 38.º. Devem também participar diretamente ou através de representação em organizações europeias de normalização, ou devem assegurar que são mantidos a par do estado atual das normas relevantes.

Artigo 32

Presunção de conformidade com os requisitos relativos aos organismos notificados

Sempre que um organismo de avaliação da conformidade demonstre o cumprimento dos critérios estabelecidos nas normas harmonizadas relevantes, ou partes das mesmas, cujas referências são publicadas noJornal Oficial da União Europeia,Presume-se que cumpre os requisitos estabelecidos no artigo 31.º na medida em que as normas harmonizadas aplicáveis prevejam esses mesmos requisitos.

Artigo 33

Filiais de organismos notificados e subcontratação

1. Sempre que um organismo notificado subcontratar tarefas específicas relacionadas com a avaliação da conformidade ou utilizar uma subsidiária, deve assegurar que o subcontratante ou a subsidiária cumprem os requisitos estabelecidos no artigo 31.º e informar desse facto a autoridade notificadora.

2. Os organismos notificados assumirão total responsabilidade pelas tarefas executadas por quaisquer subcontratantes ou subsidiárias.

3. As atividades só podem ser subcontratadas ou delegadas a uma subsidiária com o consentimento prévio do fornecedor. Os organismos notificados devem disponibilizar publicamente uma lista das suas subsidiárias.

4. Os documentos relevantes relativos à avaliação das qualificações do subcontratante ou da subsidiária e do trabalho por eles realizado ao abrigo do presente regulamento devem ser mantidos à disposição da autoridade notificadora por um período de cinco anos a contar da data de conclusão da subcontratação.

Artigo 34

Obrigações operacionais dos organismos notificados

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

2. Os organismos notificados devem evitar encargos desnecessários para os prestadores no exercício das suas atividades e devem ter devidamente em conta a dimensão do prestador, o setor em que opera, a sua estrutura e o grau de complexidade do sistema de IA de alto risco 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. O organismo notificado deve, contudo, respeitar o grau de rigor e o nível de proteção exigidos para que o sistema de IA de alto risco cumpra os requisitos do presente regulamento.

3. Os organismos notificados devem disponibilizar à autoridade notificadora referida no artigo 28.º e submeter-lhe, mediante pedido, toda a documentação relevante, incluindo a documentação dos fornecedores, a fim de permitir à autoridade notificadora referida no artigo 28.º realizar as suas atividades de avaliação, designação, notificação e monitorização e de facilitar a avaliação descrita na presente secção.

Artigo 35

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 de um ato da União.

2. A Comissão tornará pública a lista dos organismos notificados ao abrigo do presente regulamento, incluindo os seus números de identificação e as atividades para as quais foram notificados. A Comissão deve garantir que a lista seja mantida atualizada.

Artigo 36

Alterações nas notificações

1. A autoridade notificadora deve notificar a Comissão e os outros Estados-Membros de quaisquer alterações relevantes à notificação de um organismo notificado através do sistema de notificação eletrónica referido no artigo 30.º, n.º 2.

2. Os procedimentos previstos nos artigos 29.º e 30.º aplicam-se às extensões do âmbito da notificação.

Para modificações da notificação que não sejam extensões do seu âmbito, serão aplicáveis os procedimentos estabelecidos nos parágrafos 3 a 9.

3. Sempre que um organismo notificado decidir cessar as suas atividades de avaliação da conformidade, deverá informar a autoridade notificadora e os fornecedores em causa o mais rapidamente possível e, no caso de cessação planeada, pelo menos um ano antes de cessar as suas atividades. Os certificados do organismo notificado podem permanecer válidos por um período de nove meses após o organismo notificado cessar as suas atividades, desde que outro organismo notificado tenha confirmado por escrito que assumirá a responsabilidade pelos sistemas de IA de alto risco abrangidos por esses certificados. Este último organismo notificado realizará uma avaliação completa dos sistemas de IA de alto risco afetados antes do término deste período de nove meses e antes de emitir novos certificados para esses sistemas. Se o organismo notificado tiver cessado as suas atividades, a autoridade notificadora deverá retirar a designação.

4. Sempre que uma autoridade notificadora tiver motivos razoáveis para considerar que um organismo notificado deixou de cumprir os requisitos estabelecidos no artigo 31.º ou não está a cumprir as suas obrigações, a autoridade notificadora deve investigar o assunto sem demora e com a máxima diligência. Neste contexto, deve informar o organismo notificado em causa das objeções levantadas e dar-lhe a oportunidade de apresentar os seus pontos de vista. Se a autoridade notificadora concluir que o organismo notificado deixou de cumprir os requisitos estabelecidos no artigo 31.º ou não está a cumprir as suas obrigações, deverá limitar, suspender ou retirar a designação, conforme adequado, em função da gravidade do incumprimento desses requisitos ou obrigações. Deverá também informar imediatamente a Comissão e os outros Estados-Membros.

5. Caso a sua designação tenha sido suspensa, restringida ou retirada, no todo ou em parte, o organismo notificado deverá informar os fornecedores afetados no prazo de dez dias.

6. Em caso de limitação, suspensão ou retirada de uma designação, a autoridade notificadora deve tomar as medidas adequadas para garantir que os arquivos do organismo notificado em causa sejam conservados e para os disponibilizar às autoridades notificadoras de outros Estados-Membros e às autoridades de fiscalização do mercado, mediante pedido.

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

(a) avaliar o impacto nos certificados emitidos pelo organismo notificado;

(b) apresentar à Comissão e aos outros Estados-Membros um relatório com as suas conclusões no prazo de três meses a contar da notificação das alterações na designação;

(c) exigir que o organismo notificado suspenda ou retire, num prazo razoável determinado pela autoridade, quaisquer certificados emitidos indevidamente, a fim de garantir a conformidade contínua dos sistemas de IA de alto risco no mercado;

(d) informará a Comissão e os Estados-Membros dos certificados cuja suspensão ou retirada tiver solicitado;

(e) fornecer às autoridades nacionais competentes do Estado-Membro em que o fornecedor tem a sua sede social todas as informações relevantes relativas aos certificados cuja suspensão ou retirada solicitou; Esta autoridade tomará as medidas adequadas, sempre que necessário, para evitar um risco à saúde, à segurança ou aos direitos fundamentais.

8. Exceto no caso de certificados emitidos indevidamente, e quando uma designação tiver sido suspensa ou limitada, os certificados permanecerão válidos em uma das seguintes circunstâncias:

(a) quando, no prazo de um mês a contar da suspensão ou limitação, a autoridade notificadora tiver confirmado que não existe qualquer risco para a saúde, a segurança ou os direitos fundamentais em relação aos certificados afectados pela suspensão ou limitação e tiver estabelecido um calendário para a acção destinada a remediar a suspensão ou limitação, ou

(b) quando a autoridade notificadora tiver confirmado que não serão emitidos, alterados ou reemitidos quaisquer certificados relacionados com a suspensão durante o período da suspensão ou limitação, e declarar se o organismo notificado tem ou não capacidade, durante o período da suspensão ou limitação, para continuar a supervisionar e a ser responsável pelos certificados emitidos; Caso a autoridade notificadora determine que o organismo notificado não tem capacidade para dar suporte aos certificados emitidos, o fornecedor do sistema abrangido pelo certificado deverá 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 limitação, que outro organismo notificado qualificado assumirá temporariamente as funções do organismo notificado para monitorizar e ser responsável pelos certificados durante o período da suspensão ou limitação.

9. Exceto no caso de certificados emitidos indevidamente e quando uma designação tiver sido retirada, os certificados permanecerão válidos por nove meses nas seguintes circunstâncias:

(a) a autoridade nacional competente do Estado-Membro em que o fornecedor do sistema de IA de alto risco abrangido pelo certificado tem a sua sede social confirmou que não existe qualquer risco para a saúde, a segurança ou os direitos fundamentais associados ao sistema de IA de alto risco em questão, e

b) outro organismo notificado tenha confirmado por escrito que assumirá a responsabilidade imediata por tais sistemas de IA e conclua a sua 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 fornecedor do sistema abrangido pelo certificado tem a sua sede social pode prorrogar a validade provisória dos certificados por períodos adicionais de três meses, sem exceder doze meses no total.

A autoridade nacional competente ou o organismo notificado que assume as funções do organismo notificado afetado pela alteração da designação deve informar imediatamente a Comissão, os outros Estados-Membros e os outros organismos notificados.

Artigo 37

Questionando a competência dos organismos notificados

1. A Comissão deve, sempre que necessário, investigar quaisquer casos em que existam razões para duvidar da competência de um organismo notificado ou do cumprimento contínuo por um organismo notificado dos requisitos estabelecidos no artigo 31.º e das suas responsabilidades aplicáveis.

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

3. A Comissão assegurará o tratamento confidencial, em conformidade com o artigo 78.º, de todas as informações sensíveis recolhidas no decurso das suas investigações ao abrigo do presente artigo.

4. Caso a Comissão determine que um organismo notificado não cumpre ou deixou de cumprir os requisitos para a sua notificação, deverá informar o Estado-Membro notificador e solicitar-lhe que tome as medidas corretivas necessárias, incluindo a suspensão ou retirada da designação, quando necessário. Se o Estado-Membro não tomar as medidas corretivas necessárias, a Comissão pode, por meio de um ato de execução, suspender, limitar ou retirar a designação. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 98.º, n.º 2.

Artigo 38

Coordenação dos organismos notificados

1. A Comissão deve assegurar que seja estabelecida e mantida uma coordenação e cooperação adequadas entre os organismos notificados ativos nos procedimentos de avaliação da conformidade ao abrigo do presente regulamento, sob a forma de um grupo setorial de organismos notificados, em relação aos sistemas de IA de alto risco.

2. Cada autoridade notificadora deve assegurar que os organismos por ela notificados participem nos trabalhos do grupo referido no n.º 1, directamente ou através de representantes designados.

3. A Comissão deve providenciar a organização de intercâmbios de conhecimentos e de melhores práticas entre as autoridades notificadoras.

Artigo 39

Organismos de avaliação da conformidade de países terceiros

Os organismos de avaliação da conformidade estabelecidos ao abrigo da legislação de um país terceiro com o qual a União tenha celebrado um acordo podem ser autorizados a exercer as atividades de organismos notificados ao abrigo do presente regulamento, desde que cumpram os requisitos estabelecidos no artigo 31.º ou garantam um nível de conformidade equivalente.

SEÇÃO 5

Normas, avaliação de conformidade, certificados, registro

Artigo 40

Normas harmonizadas e documentos de normalização

1. Sistemas de IA de alto risco ou modelos de IA de uso geral que estejam em conformidade com normas harmonizadas, ou partes delas, cujas referências sejam publicadas noJornal Oficial da União Europeiade acordo com o Regulamento (UE) n.º$_{qualquer}$1025/2012 presume-se que cumpre os requisitos estabelecidos na Secção 2 do presente Capítulo ou, quando aplicável, as obrigações estabelecidas no Capítulo V, Secções 2 e 3 do presente Regulamento, na medida em que essas regras prevejam esses requisitos ou obrigações.

2. De acordo com o artigo 10.º do Regulamento (UE) n.º$_{qualquer}$1025/2012, a Comissão deve, sem demora injustificada, apresentar pedidos de normalização que abranjam todos os requisitos estabelecidos na Secção 2 do presente Capítulo e, quando adequado, pedidos de normalização que abranjam as obrigações estabelecidas no Capítulo V, Secções 2 e 3 do presente Regulamento. A solicitação de padronização também incluirá uma solicitação de documentos sobre processos de relatórios e documentação para melhorar o desempenho de eficiência de recursos dos sistemas de IA, como a redução do consumo de energia e outros recursos de sistemas de IA de alto risco durante seu ciclo de vida, bem como sobre o desenvolvimento de modelos de IA de uso geral com eficiência energética. Ao preparar um pedido de normalização, a Comissão deverá consultar o Conselho da IA e as partes interessadas relevantes, incluindo o Fórum Consultivo.

Ao dirigir um pedido de normalização às organizações europeias de normalização, a Comissão deve especificar que as normas devem ser claras, coerentes — incluindo com as normas desenvolvidas em vários setores para produtos abrangidos pelos atuais atos legislativos de harmonização da União enumerados no anexo I — e destinadas a garantir que os sistemas de IA de alto risco ou os modelos de IA para fins gerais colocados no mercado ou colocados em serviço na União cumpram os requisitos ou obrigações relevantes estabelecidos no presente regulamento.

A Comissão solicitará às organizações europeias de normalização que apresentem provas de que envidaram todos os esforços para atingir os objetivos referidos no primeiro e segundo parágrafos do presente número, em conformidade com o artigo 24.º do Regulamento (UE) n.º 1999/2003.$_{qualquer}$1025/2012.

3. Os participantes no processo de normalização devem procurar promover o investimento e a inovação na IA, nomeadamente através do aumento da segurança jurídica, bem como da competitividade e do crescimento do mercado da União, contribuir para o reforço da cooperação global a favor da normalização, tendo em conta as normas internacionais existentes no domínio da IA que sejam coerentes com os valores, os direitos fundamentais e os interesses da União, e reforçar a governação multilateral, assegurando uma representação equilibrada de interesses e a participação efetiva de todas as partes interessadas relevantes, em conformidade com os artigos 5.º, 6.º e 7.º do Regulamento (UE) n.º 1999/2002.$_{qualquer}$1025/2012.

Artigo 41

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, conforme o caso, para as obrigações estabelecidas no capítulo V, secções 2 e 3, desde que tenham sido cumpridas as seguintes condições:

(a) a Comissão solicitou, nos termos do artigo 10.º(1) do Regulamento (UE) n.º$_{qualquer}$1025/2012, a uma ou mais organizações europeias de normalização para desenvolver uma norma harmonizada para os requisitos estabelecidos na Secção 2 do presente Capítulo, ou, conforme o caso, para as obrigações estabelecidas no Capítulo V, Secções 2 e 3, e:

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

(ii) as normas harmonizadas que respondem a esse pedido não foram entregues dentro do prazo estabelecido em conformidade com o artigo 10.º(1) do Regulamento (UE) n.ºqualquer1025/2012, ou

(iii) as normas harmonizadas relevantes não abordam suficientemente as preocupações em matéria de direitos fundamentais, ou

iv) as normas harmonizadas não correspondem ao pedido, e

b) não foi publicado noJornal Oficial da União Europeianenhuma referência às normas harmonizadas que regem os requisitos estabelecidos na Secção 2 deste Capítulo, ou, conforme aplicável, as obrigações referidas no Capítulo V, Secções 2 e 3, em conformidade com o Regulamento (UE) n.ºqualquer1025/2012 e não se prevê a publicação dessa referência num prazo razoável.

Ao elaborar disposições comuns, a Comissão consultará o fórum consultivo referido no artigo 67.º.

Os atos de execução referidos no primeiro parágrafo do presente número são adotados pelo 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 referido no artigo 22.º do Regulamento (UE) n.º 1799/2003.qualquer1025/2012, que considera estarem reunidas as condições previstas no n.º 1 do presente artigo.

3. Os sistemas de IA de alto risco ou os modelos de IA de uso geral que cumpram as especificações comuns referidas no parágrafo 1, ou partes dessas especificações, serão presumidos como estando em conformidade com os requisitos estabelecidos na Seção 2 deste Capítulo ou, conforme aplicável, para fins de cumprimento das obrigações referidas no Capítulo V, Seções 2 e 3, na medida em que essas especificações comuns abordem esses requisitos ou essas obrigações.

4. Quando uma norma harmonizada é adoptada por uma organização europeia de normalização e proposta à Comissão para efeitos de publicação da sua referência noJornal Oficial da União Europeia,A Comissão avaliará a norma harmonizada de acordo com o Regulamento (UE) n.ºqualquer1025/2012. Quando a referência a uma norma harmonizada for publicada no Jornal Oficial da União Europeia,A Comissão revogará os atos de execução referidos no n.º 1, ou partes desses atos, que prevejam os mesmos requisitos estabelecidos na secção 2 do presente capítulo ou, conforme o caso, as mesmas obrigações estabelecidas no capítulo V, secções 2 e 3.

5. Caso os fornecedores de sistemas de IA de alto risco ou de modelos de IA de uso geral não cumpram as especificações comuns referidas no parágrafo 1, devem justificar devidamente que adotaram soluções técnicas que cumprem os requisitos referidos na Seção 2 do presente Capítulo ou, conforme aplicável, cumprem as obrigações estabelecidas no Capítulo V, Seções 2 e 3, a um nível pelo menos equivalente a estas.

6. Sempre que um Estado-Membro considerar que uma especificação comum não cumpre integralmente os requisitos estabelecidos na Secção 2 ou, conforme o caso, não cumpre as obrigações estabelecidas no Capítulo V, Secções 2 e 3, deverá informar a Comissão desse facto com uma explicação pormenorizada. A Comissão avaliará essas informações e, se for caso disso, alterará o ato de execução que estabelece a especificação comum em questão.

Artigo 42

Presunção de conformidade com certos requisitos

1. Os sistemas de IA de alto risco que tenham sido treinados e testados utilizando dados que refletem o ambiente geográfico, comportamental, contextual ou funcional específico em que se destinam a ser utilizados devem ser considerados conformes com os requisitos relevantes estabelecidos no artigo 10.º, n.º 4.

2. Sistemas de IA de alto risco que tenham um certificado ou uma declaração de conformidade ao abrigo de um regime de cibersegurança nos termos do Regulamento (UE) 2019/881, cujas referências são publicadas noJornal Oficial da União Europeiacumprir os requisitos de cibersegurança estabelecidos no artigo 15.º do presente regulamento, na medida em que o certificado de cibersegurança ou a declaração de conformidade, ou partes dos mesmos, atendam a esses requisitos.

Artigo 43

Avaliação de conformidade

1. Para os sistemas de IA de alto risco enumerados no ponto 1 do anexo III, quando, ao demonstrar a conformidade com os requisitos estabelecidos na secção 2 por um sistema de IA de alto risco, o fornecedor tiver aplicado as normas harmonizadas referidas no artigo 40.º ou, quando aplicável, as especificações comuns referidas no artigo 41.º, o fornecedor deve optar por um dos seguintes procedimentos de avaliação da conformidade:

a) a baseada no controlo interno, mencionada no Anexo VI, ou

(b) com base na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica, com a participação de um organismo notificado, mencionado no anexo VII.

Ao demonstrar a conformidade com os requisitos estabelecidos na Seção 2 por um sistema de IA de alto risco, o fornecedor deve cumprir o procedimento de avaliação da conformidade estabelecido no Anexo VII quando:

(a) as normas harmonizadas referidas no artigo 40.º não existem e as especificações comuns referidas no artigo 41.º não estão disponíveis;

b) o fornecedor não aplicou a norma harmonizada, ou aplicou apenas parte dela;

c) as especificações comuns referidas na alínea a) existem, mas o fornecedor não as aplicou;

(d) uma ou mais das normas harmonizadas referidas na alínea a) foram publicadas com uma limitação e apenas na parte da norma que é objecto da limitação.

Para efeitos do procedimento de avaliação da conformidade referido no Anexo VII, o fornecedor pode escolher qualquer um dos organismos notificados. No entanto, quando se espera que o sistema de IA de alto risco seja colocado em serviço por autoridades responsáveis pela aplicação da lei, autoridades de imigração ou autoridades de asilo, ou por instituições, organismos, gabinetes ou agências da União, a autoridade de fiscalização do mercado referida no artigo 74.º, n.º 8 ou (9), conforme o caso, deve atuar como organismo notificado.

2. Para os sistemas de IA de alto risco referidos no anexo III, pontos 2 a 8, os fornecedores devem cumprir o procedimento de avaliação da conformidade baseado no controlo interno referido no anexo VI, que não prevê o envolvimento de um organismo notificado.

3. No caso de sistemas de IA de alto risco regulamentados pelos atos legislativos de harmonização da União enumerados na secção A do anexo I, o fornecedor deve cumprir o procedimento de avaliação da conformidade relevante exigido por esses atos legislativos. Os requisitos estabelecidos na Secção 2 do presente Capítulo aplicam-se a esses sistemas de IA de alto risco e fazem parte dessa avaliação. Além disso, são aplicáveis os pontos 4.3, 4.4 e 4.5 do Anexo VII, bem como o ponto 4.6, quinto parágrafo, do mesmo Anexo.

Para efeitos dessa avaliação, os organismos notificados que tenham sido notificados nos termos desses atos legislativos terão o poder de monitorizar a conformidade dos sistemas de IA de alto risco com os requisitos estabelecidos na secção 2, desde 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 nos termos desses atos legislativos.

Quando um ato legislativo listado na Seção A do Anexo I permitir que o fabricante do produto dispense uma avaliação de conformidade por terceiros, desde que o fabricante tenha aplicado todas as normas harmonizadas que abrangem todos os requisitos relevantes, o fabricante só poderá usar esta opção se também tiver aplicado as normas harmonizadas ou, quando aplicável, as especificações comuns referidas no Artigo 41, que abrangem todos os requisitos estabelecidos na Seção 2 deste Capítulo.

4. Os sistemas de IA de alto risco que já tenham sido submetidos a um procedimento de avaliação da conformidade estarão sujeitos a um novo procedimento de avaliação da conformidade no caso de uma modificação substancial, independentemente de estar prevista uma distribuição adicional do sistema modificado ou de este continuar a ser utilizado pela pessoa responsável pela implementação atual.

Para sistemas de IA de alto risco que continuam a aprender depois de serem colocados no mercado ou em serviço, as alterações ao sistema de IA de alto risco e ao seu funcionamento que tenham sido pré-determinadas pelo fornecedor no momento da avaliação inicial da conformidade e estejam incluídas nas informações contidas na documentação técnica referida na alínea f) do anexo IV não constituem modificações substanciais.

5. A Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 97.º, para alterar os anexos VI e VII, atualizando-os à luz do progresso técnico.

6. A Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 97.º, para alterar os n.ºs 1 e 2 do presente artigo, a fim de sujeitar os sistemas de IA de alto risco referidos nos pontos 2 a 8 do anexo III ao procedimento de avaliação da conformidade referido no anexo VII ou partes deste. A Comissão adota esses atos delegados tendo em conta a eficácia do procedimento de avaliação da conformidade baseado no controlo interno referido no anexo VI na prevenção ou minimização dos riscos para a saúde, a segurança e a proteção dos direitos fundamentais colocados por esses sistemas, bem como a disponibilidade de capacidades e recursos adequados por parte dos organismos notificados.

Artigo 44

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 está estabelecido.

2. Os certificados serão válidos pelo período por eles indicado, que não poderá exceder cinco anos para os sistemas de IA referidos no Anexo I, e quatro anos para os sistemas de IA referidos no Anexo III. A pedido do fornecedor, a validade de um certificado pode ser prorrogada por períodos adicionais não superiores a cinco anos para os sistemas de IA referidos no Anexo I e a quatro anos para os sistemas de IA referidos no Anexo III, com base numa reavaliação de acordo com os procedimentos de avaliação da conformidade aplicáveis. Qualquer suplemento a um certificado permanecerá válido desde que o certificado que ele complementa seja válido.

3. Sempre que um organismo notificado verificar que um sistema de IA deixou de cumprir os requisitos estabelecidos na secção 2, deverá, tendo em conta o princípio da proporcionalidade, suspender ou retirar o certificado emitido ou impor-lhe restrições, a menos que o cumprimento desses requisitos seja garantido por medidas corretivas adequadas tomadas pelo fornecedor do sistema num prazo adequado determinado pelo organismo notificado. O organismo notificado deve fundamentar a sua decisão.

Haverá um procedimento de recurso contra as decisões dos organismos notificados, inclusive em relação aos certificados de conformidade emitidos.

Artigo 45

Obrigações de informação dos organismos notificados

1. Os organismos notificados devem informar a autoridade notificadora:

(a) qualquer certificado da União de avaliação da documentação técnica, qualquer suplemento a esses certificados e quaisquer aprovações de sistemas de gestão da qualidade emitidos em conformidade com os requisitos estabelecidos no anexo VII;

(b) qualquer recusa, restrição, suspensão ou retirada de um certificado União de avaliação de documentação técnica ou de uma aprovação de um sistema de gestão da qualidade emitido em conformidade com os requisitos estabelecidos no anexo VII;

c) qualquer circunstância que afete o escopo ou as condições da notificação;

(d) quaisquer pedidos de informação sobre atividades de avaliação da conformidade recebidos das autoridades de fiscalização do mercado;

(e) mediante solicitação, das atividades de avaliação da conformidade realizadas no âmbito da sua notificação e de quaisquer outras atividades realizadas, incluindo atividades transfronteiriças e subcontratação.

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

a) das aprovações de sistemas de gestão da qualidade que tenha recusado, suspendido ou retirado e, mediante solicitação, das aprovações de sistemas de gestão da qualidade que tenha emitido;

(b) Certificados da União de avaliação de documentação técnica ou suplementos a esses certificados que tenha recusado, retirado, suspenso ou restringido de outra forma e, mediante solicitação, quaisquer certificados ou suplementos aos mesmos que tenha emitido.

3. Cada organismo notificado deve fornecer a outros organismos notificados que realizem atividades de avaliação da conformidade semelhantes relacionadas com os mesmos tipos de sistemas de IA informações relevantes sobre questões relacionadas com resultados negativos e, mediante solicitação, positivos das avaliações da conformidade.

4. Os organismos notificados devem manter a confidencialidade das informações obtidas em conformidade com o artigo 78.º.

Artigo 46

Isenção do procedimento de avaliação da conformidade

1. Em derrogação do artigo 43.º e mediante pedido devidamente fundamentado, qualquer autoridade de fiscalização do mercado pode autorizar a colocação no mercado ou a entrada em serviço de sistemas específicos de IA de alto risco no território do Estado-Membro em causa por motivos excecionais de segurança pública ou para proteger a vida e a saúde humanas, o ambiente ou ativos industriais e de infraestruturas críticos. Essa autorização será concedida por um período limitado, enquanto os procedimentos necessários de avaliação da conformidade forem realizados, levando em consideração quaisquer razões excepcionais que justifiquem a isenção. A conclusão do processo em questão deverá ser alcançada sem demora injustificada.

2. Numa situação de emergência devidamente justificada por motivos excecionais de segurança pública ou em caso de ameaça específica, significativa e iminente à vida ou à segurança física de pessoas singulares, as autoridades responsáveis pela aplicação da lei ou as autoridades de proteção civil podem colocar em serviço um sistema de IA especificamente de alto risco sem a autorização referida no n.º 1, desde que tal autorização seja solicitada durante ou após a utilização, sem demora injustificada. Se a autorização referida no n.º 1 for recusada, a utilização do sistema de IA de alto risco será suspensa com efeitos imediatos e todos os resultados e informações produzidos por essa utilização serão imediatamente eliminados.

3. A autorização referida no n.º 1 só será emitida se a autoridade de fiscalização do mercado concluir que o sistema de IA de alto risco cumpre os requisitos estabelecidos na secção 2. A autoridade de fiscalização do mercado deve informar a Comissão e os outros Estados-Membros de qualquer autorização emitida em conformidade com os n.ºs 1 e 2. Esta obrigação não abrange dados operacionais sensíveis relacionados com as atividades das autoridades responsáveis pela execução.

4. Se, no prazo de 15 dias de calendário a contar da receção das informações referidas no n.º 3, nem o Estado-Membro nem a Comissão tiverem levantado objeções a uma autorização emitida por uma autoridade de fiscalização do mercado de um Estado-Membro nos termos do n.º 1, a autorização será considerada justificada.

5. Se, no prazo de 15 dias de calendário a contar da receção da notificação referida no n.º 3, um Estado-Membro levantar objeções contra uma autorização emitida por uma autoridade de fiscalização do mercado de outro Estado-Membro, ou se a Comissão considerar que a autorização infringe o direito da União ou que a conclusão dos Estados-Membros relativamente ao cumprimento do sistema referido no n.º 3 é infundada, a Comissão deve consultar o Estado-Membro em causa sem demora. Os operadores envolvidos serão consultados e terão a oportunidade de apresentar suas opiniões. À luz de tudo isto, a Comissão decidirá se a autorização é justificada ou não. A Comissão transmitirá a sua decisão ao Estado-Membro em causa e aos operadores relevantes.

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

7. Para sistemas de IA de alto risco associados a produtos regulamentados pelos atos legislativos de harmonização da União enumerados na secção A do anexo I, apenas se aplicam as isenções de avaliação da conformidade previstas nesses atos legislativos de harmonização da União.

Artigo 47

Declaração de conformidade da UE

1. O fornecedor deve elaborar uma declaração UE de conformidade por escrito, num formato legível por máquina, com uma assinatura eletrónica ou manuscrita, para cada sistema de IA de alto risco e mantê-la à disposição das autoridades nacionais competentes por um período de dez anos a partir do momento em que o sistema de IA de alto risco for colocado no mercado ou em serviço. A declaração de conformidade da UE deve especificar o sistema de IA de alto risco para o qual foi elaborada. Uma cópia da declaração de conformidade da UE deve ser fornecida às autoridades nacionais competentes, mediante solicitação.

2. A declaração de conformidade da UE deve declarar que o sistema de IA de alto risco em causa cumpre os requisitos estabelecidos na secção 2. A declaração de conformidade da UE deve conter as informações estabelecidas no anexo V e deve ser traduzida para uma língua que possa ser facilmente compreendida pelas autoridades nacionais competentes do(s) Estado(s)-Membro(s) em que o sistema de IA de alto risco é colocado no mercado ou disponibilizado no mercado.

3. Quando os sistemas de IA de alto risco estiverem sujeitos a outra legislação de harmonização da União que também exija uma declaração de conformidade da UE, deve ser elaborada uma única declaração de conformidade da UE no que diz respeito a toda a legislação da União aplicável ao sistema de IA de alto risco. A declaração deve conter todas as informações necessárias para determinar os atos legislativos de harmonização da União aos quais a declaração se refere.

4. Ao elaborar a declaração UE de conformidade, o fornecedor deve assumir a responsabilidade pelo cumprimento dos requisitos estabelecidos na Secção 2. O fornecedor deve manter a declaração UE de conformidade atualizada, conforme adequado.

5. A Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 97.º, para alterar o anexo V, atualizando o conteúdo da declaração UE de conformidade constante desse anexo, a fim de introduzir elementos que sejam necessários à luz do progresso técnico.

Artigo 48

Marcação CE

1. A marcação CE está sujeita aos princípios gerais estabelecidos no artigo 30.º do Regulamento (CE) n.º 101/2009. n.qualquer765/2008.

2. Para sistemas de IA de alto risco fornecidos digitalmente, a marcação CE digital só será utilizada se for facilmente acessível através da interface a partir da qual o sistema é acedido ou por meio de um código legível por máquina facilmente acessível ou outros meios eletrónicos.

3. A marcação CE deve ser afixada de forma visível, legível e indelével nos sistemas de IA de alto risco. Quando isso não for possível ou não puder ser garantido devido à natureza do sistema de IA de alto risco, deverá ser colocado na embalagem ou nos documentos que o acompanham, conforme apropriado.

4. Quando apropriado, a marcação CE deve ser seguida 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 notificado ou, segundo as suas instruções, pelo fornecedor ou pelo seu representante autorizado. O número de identificação também aparecerá em todo o material publicitário mencionando que o sistema de IA de alto risco atende aos requisitos de marcação CE.

5. Quando os sistemas de IA de alto risco estiverem sujeitos a outras disposições do direito da União que também exijam a aposição da marcação CE, a marcação CE deve indicar que os sistemas de IA de alto risco também cumprem os requisitos dessas outras disposições.

Artigo 49

Registro

1. Antes de colocar no mercado ou em serviço um sistema de IA de alto risco enumerado no anexo III, com exceção dos sistemas de IA de alto risco enumerados no ponto 2 do anexo III, o fornecedor ou, se aplicável, o representante autorizado, deve registar o seu sistema e a si próprio na base de dados da UE referida no artigo 71.º.

2. Antes de colocar no mercado ou em serviço um sistema de IA que o fornecedor tenha concluído não ser de alto risco, em conformidade com o artigo 6.º, n.º 3, esse fornecedor ou, se aplicável, o representante autorizado, deve registar ele próprio esse sistema na base de dados da UE referida no artigo 71.º.

3. Antes de colocar em serviço ou utilizar um sistema de IA de alto risco enumerado no anexo III, com exceção dos sistemas de IA de alto risco referidos no ponto 2 do anexo III, os responsáveis pela implementação de sistemas de IA de alto risco que sejam autoridades, instituições, organismos, gabinetes ou agências públicas da União, ou pessoas que atuem em seu nome, devem registar, selecionar o sistema e registar a sua utilização na base de dados da UE referida no artigo 71.º.

4. No caso de sistemas de IA de alto risco referidos nos pontos 1, 6 e 7 do anexo III, nos domínios da aplicação da lei, da migração, do asilo e da gestão do controlo de 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 referida no artigo 71.º e deve incluir apenas as informações, conforme aplicável, referidas:

(a) Anexo VIII, Secção A, pontos 1 a 10, com excepção dos pontos 6, 8 e 9;

(b) Anexo VIII, Secção B, pontos 1 a 5 e pontos 8 e 9;

(c) Anexo VIII, Secção C, pontos 1 a 3;

(d) Anexo IX, pontos 1, 2, 3 e 5.

Apenas a Comissão e as autoridades nacionais referidas no artigo 74.º, n.º 8, terão acesso às respetivas secções restritas da base de dados da UE enumeradas no primeiro parágrafo do presente número.

5. Os sistemas de IA de alto risco referidos no anexo III, ponto 2, devem ser registados a nível nacional.

CAPÍTULO IV

OBRIGAÇÕES DE TRANSPARÊNCIA DOS FORNECEDORES E DOS RESPONSÁVEIS PELA DISTRIBUIÇÃO DE DETERMINADOS PRODUTOS SISTEMAS DE IA

Artigo 50

Obrigações de transparência para fornecedores e responsáveis pela implementação de determinados sistemas de IA

1. Os fornecedores devem garantir que os sistemas de IA destinados a interagir diretamente com pessoas singulares sejam concebidos e desenvolvidos de modo a que as pessoas singulares em causa sejam informadas de que estão a interagir com um sistema de IA, exceto quando tal for óbvio do ponto de vista de uma pessoa singular razoavelmente informada, atenta e criteriosa, tendo em conta as circunstâncias e o contexto de utilização. Esta obrigação não se aplica aos sistemas de IA autorizados por lei a detetar, prevenir, investigar ou processar infrações penais, sujeitos a salvaguardas adequadas dos direitos e liberdades de terceiros, a menos que tais sistemas estejam publicamente disponíveis para denunciar uma infração penal.

2. Os provedores de sistemas de IA, incluindo sistemas de IA de uso geral, que geram conteúdo sintético de áudio, imagem, vídeo ou texto devem garantir que os resultados de saída do sistema de IA sejam marcados em um formato legível por máquina e que seja possível detectar que eles foram gerados ou manipulados artificialmente. Os provedores devem garantir que suas soluções técnicas sejam eficientes, interoperáveis, robustas e confiáveis na medida em que seja tecnicamente viável, levando em consideração as particularidades e limitações dos vários tipos de conteúdo, os custos de implementação e o estado da arte geralmente reconhecido, conforme refletido nas normas técnicas relevantes. Esta obrigação não se aplica na medida em que os sistemas de IA desempenhem uma função de suporte de edição padrão ou não alterem substancialmente os dados de entrada fornecidos pelo implantador ou sua semântica, ou quando estiverem autorizados por lei a detectar, prevenir, investigar ou processar infrações penais.

3. Os responsáveis pela implementação de um sistema de reconhecimento de emoções ou de um sistema de categorização biométrica devem informar as pessoas singulares a ele expostas sobre o funcionamento do sistema e devem tratar os seus 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 utilizados para categorização biométrica e reconhecimento de emoções que tenham sido autorizados por lei para detetar, prevenir e investigar infrações penais, sujeitos a salvaguardas adequadas dos direitos e liberdades de terceiros e em conformidade com o direito da União.

4. Os responsáveis pela implantação de um sistema de IA que gere ou manipule imagens ou conteúdo de áudio ou vídeo que constitua representação profunda tornarão público que esses conteúdos ou imagens foram gerados ou manipulados artificialmente. Esta obrigação não se aplica quando a lei autoriza a sua utilização para detectar, prevenir, investigar ou processar crimes. Quando o conteúdo fizer parte de uma obra ou programa manifestamente criativo, satírico, artístico, ficcional ou similar, as obrigações de transparência estabelecidas nesta seção serão limitadas à obrigação de tornar pública a existência de tal conteúdo gerado ou manipulado artificialmente de forma apropriada que não impeça a exibição ou a fruição da obra.

Os responsáveis pela implantação de um sistema de IA que gera ou manipula texto publicado com a finalidade de informar o público sobre assuntos de interesse público divulgarão que o texto foi gerado ou manipulado artificialmente. Esta obrigação não se aplica quando o uso é autorizado por lei para detectar, prevenir, investigar ou processar infrações penais, ou quando o conteúdo gerado por IA foi sujeito a revisão humana ou controle editorial e quando uma pessoa física ou jurídica tem responsabilidade editorial pela publicação do conteúdo.

5. As informações referidas nos n.os 1 a 4 devem ser fornecidas às pessoas singulares em causa de forma clara e distinguível, o mais tardar por ocasião da primeira interação ou exposição. As informações estarão em conformidade com os requisitos de acessibilidade aplicáveis.

6. Os parágrafos 1 a 4 não afetam os requisitos e obrigações estabelecidos no Capítulo III e não prejudicam outras obrigações de transparência previstas no direito da União ou nacional para os responsáveis pelo tratamento que implementam sistemas de IA.

7. O Gabinete de IA deve incentivar e facilitar o desenvolvimento de códigos de boas práticas em toda a União para promover a implementação efetiva das obrigações relativas à deteção e rotulagem de conteúdos gerados ou manipulados artificialmente. A Comissão pode adotar atos de execução para aprovar tais códigos de boas práticas de acordo com o procedimento estabelecido no Artigo 56(6). Se considerar que o código não é adequado, a Comissão pode adotar um ato de execução especificando regras comuns para o cumprimento dessas obrigações de acordo com o procedimento de exame estabelecido no Artigo 98(2).

CAPÍTULO V

MODELOS DE IA DE PROPÓSITO GERAL

SEÇÃO 1

Regras de classificação

Artigo 51

Regras para classificar modelos de IA de uso geral como modelos de IA de uso geral com risco sistêmico

1. Um modelo de IA de uso geral será classificado como um modelo de IA de uso geral com risco sistémico se cumprir qualquer uma das seguintes condições:

a) possui capacidades de alto impacto avaliadas por meio de ferramentas e metodologias técnicas adequadas, como indicadores e benchmarks;

(b) em conformidade com uma decisão da Comissão, tomada por sua própria iniciativa ou na sequência de um alerta qualificado do grupo de peritos científicos, tenha capacidades ou um impacto equivalentes aos definidos na alínea a), tendo em conta os critérios estabelecidos no anexo XIII.

2. Presume-se que um modelo de IA de uso geral tem capacidades de alto impacto, nos termos da alínea a) do n.º 1, quando a quantidade cumulativa de computação utilizada para o treinar, medida em operações de vírgula flutuante, for superior a 10^{25}.

3. A Comissão adota atos delegados, em conformidade com o artigo 97.º, para alterar os limiares referidos nos n.ºs 1 e 2 do presente artigo e para complementar os parâmetros de referência e os indicadores com base em desenvolvimentos tecnológicos, como melhorias algorítmicas ou maior eficiência do hardware, sempre que necessário para garantir que os limiares refletem o estado atual da técnica.

Artigo 52

Procedimento

1. Sempre que um modelo de IA para fins gerais cumprir a condição referida na alínea a) do artigo 51.º, n.º 1, o fornecedor relevante deve notificar a Comissão sem demora e, em qualquer caso, o mais tardar duas semanas após o cumprimento desse requisito ou quando se souber que será cumprido. Essa notificação deverá incluir as informações necessárias para demonstrar que o requisito relevante foi cumprido. Se a Comissão tiver conhecimento de um modelo de IA de uso geral que apresente riscos sistêmicos e que não tenha sido notificado, ela poderá decidir designá-lo como um modelo com risco sistêmico.

2. O fornecedor de um modelo de IA para fins gerais que cumpra a condição referida na alínea a) do artigo 51.º(1) pode apresentar, juntamente com a sua notificação, argumentos suficientemente fundamentados que demonstrem que, excepcionalmente, embora o modelo de IA para fins gerais cumpra esse requisito, não apresenta, devido às suas características específicas, riscos sistémicos e, por conseguinte, não deve ser classificado como um modelo de IA para fins gerais com risco sistémico.

3. Se a Comissão concluir que os argumentos apresentados nos termos do parágrafo 2 não estão suficientemente fundamentados e que o fornecedor relevante não conseguiu demonstrar que o modelo de IA de uso geral não apresenta, devido às suas características específicas, riscos sistémicos, rejeitará esses argumentos e o modelo de IA de uso geral será considerado um modelo de IA de uso geral com risco sistémico.

4. A Comissão pode determinar que um modelo de IA para fins gerais apresenta riscos sistémicos, ex officio ou na sequência de um alerta qualificado do grupo de peritos científicos 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, em conformidade com o artigo 97.º, para alterar o anexo XIII, especificando e atualizando os critérios estabelecidos nesse anexo.

5. Mediante solicitação fundamentada de um provedor cujo modelo tenha sido designado como um modelo de IA de uso geral com risco sistêmico, nos termos do parágrafo 4, a Comissão levará em consideração a solicitação e poderá decidir reavaliar se o modelo de IA de uso geral pode continuar a ser considerado como apresentando riscos sistêmicos, de acordo com os critérios estabelecidos no Anexo XIII. Tal solicitação deverá conter justificativas objetivas, detalhadas e novas que tenham surgido desde a decisão de nomeação. Os fornecedores não podem solicitar reavaliação antes de decorridos seis meses da decisão de designação. Se, após a reavaliação, a Comissão decidir manter a designação como um modelo de IA de uso geral com risco sistêmico, os provedores não poderão solicitar outra reavaliação até que seis meses tenham decorrido dessa decisão.

6. A Comissão deve assegurar que seja publicada e mantida atualizada uma lista de modelos de IA de uso geral com risco sistémico, sem prejuízo da necessidade de respeitar e proteger os direitos de propriedade intelectual e as informações comerciais confidenciais ou os segredos comerciais, em conformidade com o direito da União e nacional.

SEÇÃO 2

Obrigações dos provedores de modelos de IA de uso geral

Artigo 53

Obrigações dos provedores de modelos de IA de uso geral

1. Provedores de modelos de IA de uso geral:

(a) desenvolver e manter documentação técnica atualizada para o modelo, incluindo informações relativas ao processo de treinamento e teste e aos resultados de sua avaliação, que deve conter, no mínimo, as informações estabelecidas no Anexo XI, a fim de fornecê-las, mediante solicitação, ao Gabinete de IA e às autoridades nacionais competentes;

(b) desenvolver e manter informações e documentação atualizadas e disponibilizá-las aos fornecedores de sistemas de IA que pretendam integrar o modelo de IA de uso geral nos seus sistemas de IA. Sem prejuízo da necessidade de observar e proteger os direitos de propriedade intelectual e industrial e as informações comerciais confidenciais ou segredos comerciais, em conformidade com a legislação da União e nacional, tais informações e documentação:

(i) permitir que os fornecedores de sistemas de IA tenham uma boa compreensão das capacidades e limitações do modelo de IA para fins gerais e cumpram as suas obrigações ao abrigo do presente regulamento, e

(ii) conter, no mínimo, os elementos previstos no Anexo XII;

(c) estabelecer orientações para o cumprimento do direito da União em matéria de direitos de autor e direitos conexos e, em especial, para a deteção e o cumprimento, por exemplo através de tecnologias de ponta, de uma reserva de direitos expressa nos termos do artigo 4.º, n.º 3, da Diretiva (UE) 2019/790;

(d) elaborar e disponibilizar publicamente um resumo suficientemente detalhado do conteúdo utilizado para o treinamento do modelo de IA de uso geral, de acordo com o modelo fornecido pelo AI Office.

2. As obrigações estabelecidas no parágrafo 1(a) e (b) não se aplicam aos fornecedores de modelos de IA que são divulgados sob uma licença livre e de código aberto que permite o acesso, uso, modificação e distribuição do modelo e cujos parâmetros, incluindo pesos, informações sobre a arquitetura do modelo e informações sobre o uso do modelo, são disponibilizados publicamente. Esta exceção não se aplicará a modelos de IA de uso geral com risco sistêmico.

3. Os fornecedores de modelos de IA para fins gerais devem cooperar com a Comissão e as autoridades nacionais competentes, conforme necessário, no exercício dos seus poderes e autoridades ao abrigo do presente regulamento.

4. Os fornecedores de modelos de IA para fins gerais podem basear-se em códigos de boas práticas, na aceção do artigo 56.º, para demonstrar o cumprimento das obrigações estabelecidas no n.º 1 do presente artigo, até que seja publicada uma norma harmonizada. A conformidade com as normas europeias harmonizadas concede aos fornecedores uma presunção de conformidade na medida em que tais normas regulam tais obrigações. Os provedores de modelos de IA de uso geral que não aderirem a um código de práticas aprovado ou não cumprirem uma norma europeia harmonizada serão obrigados a demonstrar conformidade com suas obrigações por meios alternativos apropriados para avaliação pela Comissão.

5. A fim de facilitar o cumprimento das disposições do anexo XI, em especial dos pontos 2, alíneas d) e e), a Comissão fica habilitada a adotar atos delegados, em conformidade com o artigo 97.º, para especificar as metodologias de medição e cálculo, com vista a tornar a documentação comparável e verificável.

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

7. Qualquer informação ou documentação obtida ao abrigo deste artigo, incluindo segredos comerciais, será tratada de acordo com as obrigações de confidencialidade estabelecidas no artigo 78.º.

Artigo 54

Representantes autorizados de provedores de modelos de IA de uso geral

1. Antes de colocarem um modelo de IA para fins gerais no mercado da União, os prestadores estabelecidos em países terceiros devem nomear, por meio de um mandato escrito, um representante autorizado estabelecido na União.

2. Os fornecedores devem permitir que seu representante autorizado execute as tarefas especificadas no mandato recebido do fornecedor.

3. Os representantes autorizados executarão as tarefas especificadas no mandato recebido do fornecedor. Eles fornecerão ao Gabinete de IA, mediante solicitação, uma cópia do mandato em uma das línguas oficiais das instituições da União. Para efeitos do presente regulamento, o mandato deve permitir ao representante autorizado desempenhar as seguintes tarefas:

(a) verificar se a documentação técnica indicada no anexo XI foi elaborada e se o fornecedor cumpre todas as obrigações referidas no artigo 53.º e, se aplicável, no artigo 55.º;

(b) manter à disposição do Instituto de IA e das autoridades nacionais competentes uma cópia da documentação técnica constante do anexo XI, por um período de dez anos a contar da colocação no mercado do modelo de IA para fins gerais, bem como os dados de contacto do fornecedor que nomeou o representante autorizado;

(c) fornecer ao Gabinete de Auditoria Interna, mediante solicitação fundamentada, todas as informações e documentação, incluindo as informações e a documentação referidas na alínea b), que sejam necessárias para demonstrar o cumprimento das obrigações estabelecidas no presente Capítulo;

(d) cooperar com o Gabinete de IA e as autoridades competentes, mediante pedido fundamentado, em qualquer ação que tomem em relação ao modelo de IA de uso geral, incluindo quando o modelo estiver integrado num sistema de IA colocado no mercado ou em serviço na União.

4. O mandato deve permitir que o representante autorizado seja contactado pelo Gabinete de Auditoria Interna ou pelas autoridades competentes, em complemento ou em substituição do prestador, relativamente a todas as questões relacionadas com a garantia do cumprimento do presente regulamento.

5. O representante autorizado deve rescindir o mandato se considerar ou tiver motivos para considerar que o fornecedor está em violação das suas obrigações nos termos do presente regulamento. Nesse caso, deverá também informar imediatamente o Gabinete de Auditoria Interna sobre o fim do mandato e as razões para tal.

6. A obrigação estabelecida neste artigo não se aplica aos fornecedores de modelos de IA de uso geral que sejam divulgados sob uma licença livre e de código aberto que permita o acesso, o uso, a modificação e a distribuição do modelo e cujos parâmetros, incluindo pesos, informações sobre a arquitetura do modelo e informações sobre o uso do modelo, sejam disponibilizados publicamente, exceto quando tais modelos de IA de uso geral apresentem riscos sistêmicos.

SEÇÃO 3

Obrigações dos provedores de modelos de IA de uso geral com risco sistémico

Artigo 55

Obrigações dos provedores de modelos de IA de uso geral com risco sistémico

1. Além das obrigações enumeradas nos artigos 53.º e 54.º, os fornecedores de modelos de IA de uso geral com risco sistémico:

a) avaliar os modelos em relação a protocolos e ferramentas padronizados que reflitam o estado da arte, incluindo a realização e documentação de testes de simulação adversarial em relação ao modelo, com vistas a detectar e mitigar riscos sistêmicos;

(b) avaliar e atenuar potenciais riscos sistémicos a nível da União que possam surgir do desenvolvimento, da colocação no mercado ou da utilização de modelos de IA para fins gerais com risco sistémico, bem como a origem desses riscos;

(c) monitorizar, documentar e comunicar, sem demora injustificada, ao Gabinete de Auditoria Interna e, quando apropriado, às autoridades nacionais competentes, informações relevantes sobre incidentes graves e possíveis medidas corretivas para os resolver;

(d) garantir que existe um nível adequado de proteção da cibersegurança para o modelo de IA de uso geral com risco sistémico e para a infraestrutura física do modelo.

2. Os fornecedores de modelos de IA de uso geral com risco sistémico podem basear-se em códigos de boas práticas, na aceção do artigo 56.º, para demonstrar o cumprimento das obrigações estabelecidas no n.º 1 do presente artigo, até que seja publicada uma norma harmonizada. A conformidade com as normas europeias harmonizadas concede aos fornecedores uma presunção de conformidade na medida em que tais normas regulam tais obrigações. Os provedores de modelos de IA de uso geral que não aderirem a um código de práticas aprovado ou não cumprirem uma norma europeia harmonizada serão obrigados a demonstrar conformidade com suas obrigações por meios alternativos apropriados para avaliação pela Comissão.

3. Qualquer informação ou documentação obtida ao abrigo do presente artigo, incluindo segredos comerciais, será tratada de acordo com as obrigações de confidencialidade estabelecidas no artigo 78.º.

SEÇÃO 4

Códigos de boas práticas

Artigo 56

Códigos de boas práticas

1. O Gabinete de IA deve incentivar e facilitar o desenvolvimento de códigos de boas práticas à escala da União, a fim de contribuir para a correta aplicação do presente regulamento, tendo em conta as abordagens internacionais.

2. O Gabinete de IA e o Conselho de IA devem garantir que os códigos de prática abrangem pelo menos as obrigações estabelecidas nos artigos 53.º e 55.º, incluindo as seguintes questões:

(a) os meios para garantir que as informações referidas no artigo 53.º, n.º 1, alíneas a) e b), sejam mantidas atualizadas relativamente à evolução do mercado e ao progresso tecnológico;

b) o nível adequado de detalhamento quanto ao resumo do conteúdo utilizado no treinamento;

(c) a determinação do tipo e da natureza dos riscos sistémicos a nível da União, incluindo a sua origem, se for caso disso;

(d) medidas, procedimentos e modalidades para avaliar e gerir riscos sistémicos a nível da União, incluindo a sua documentação, que devem ser proporcionais aos riscos e ter em conta a sua gravidade e probabilidade, bem como os desafios específicos na sua abordagem, tendo em conta a forma como tais riscos podem surgir e materializar-se ao longo da cadeia de valor da IA.

3. O Gabinete de IA pode convidar todos os fornecedores de modelos de IA de uso geral, bem como as autoridades nacionais competentes relevantes, a participar no desenvolvimento de códigos de boas práticas. Organizações da sociedade civil, indústria, academia e outras partes interessadas relevantes, como fornecedores e especialistas independentes, poderão contribuir para o processo.

4. O Gabinete de IA e o Conselho de IA devem garantir que os códigos de prática estabeleçam claramente os seus objetivos específicos e contenham compromissos ou medidas, como indicadores-chave de desempenho, quando apropriado, para garantir a concretização 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 AI Office deve garantir que os participantes dos códigos de boas práticas informem regularmente o AI Office sobre a implementação dos compromissos e as ações tomadas e seus resultados, incluindo sua avaliação em relação aos principais indicadores de desempenho, se aplicável. Os principais indicadores de desempenho e os compromissos de relatórios refletirão as diferenças de tamanho e capacidade entre os participantes.

6. O Gabinete de IA e o Conselho de IA monitorizam e avaliam regularmente a concretização dos objetivos dos códigos de boas práticas pelos participantes e a sua contribuição para a correta aplicação do presente Regulamento. O Gabinete de IA e o Conselho de IA devem avaliar se os códigos de boas práticas incluem as obrigações estabelecidas nos artigos 53.º e 55.º e devem monitorizar e avaliar regularmente a concretização dos seus objetivos. Eles publicarão sua avaliação da adequação dos códigos de boas práticas.

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

7. O AI Office pode convidar todos os provedores de modelos de IA de uso geral a aderir aos códigos de boas práticas. Para os provedores de modelos de IA de uso geral que não apresentem riscos sistêmicos, essa adesão poderá ser limitada às obrigações previstas no Artigo 53, salvo se declararem expressamente seu interesse em aderir ao código integral.

8. O Gabinete de IA também incentivará e facilitará, conforme apropriado, a revisão e adaptação de códigos de boas práticas, em particular tendo em conta as normas emergentes. O AI Office auxiliará na avaliação dos padrões disponíveis.

9. Os códigos de prática deverão ser finalizados até 2 de maio de 2025. O AI Office tomará as medidas necessárias, incluindo convidar os provedores a aderir aos códigos de prática de acordo com o parágrafo 7.

Se um código de boas práticas não tiver sido finalizado até 2 de agosto de 2025, ou se for considerado inadequado pelo AI Office após sua avaliação nos termos do parágrafo 6 deste artigo, a Comissão pode, por meio de atos de execução, estabelecer regras comuns para o cumprimento das obrigações estabelecidas nos artigos 53 e 55, incluindo as questões estabelecidas no parágrafo 2 deste artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 98.º, n.º 2.

CAPÍTULO VI

MEDIDAS DE APOIO À INOVAÇÃO

Artigo 57

Espaços de teste controlados para IA

1. Os Estados-Membros devem assegurar que as suas autoridades competentes criem pelo menos uma sandbox nacional de IA, que deverá estar operacional até 2 de agosto de 2026. Essa sandbox também pode ser criada em conjunto com as autoridades competentes de outros Estados-Membros. A Comissão pode fornecer apoio técnico, aconselhamento e ferramentas para o estabelecimento e operação de sandboxes de IA.

A obrigação prevista no primeiro parágrafo também pode ser cumprida através da participação numa área de ensaio controlada existente, na medida em que essa participação proporcione um nível equivalente de cobertura nacional aos Estados-Membros participantes.

2. Podem também ser criadas áreas de teste de IA adicionais 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 também criar uma área de testes de IA para instituições, organismos, gabinetes e agências da União e pode exercer as funções e tarefas das autoridades nacionais competentes nos termos do presente capítulo.

4. Os Estados-Membros devem assegurar que as autoridades competentes referidas nos n.ºs 1 e 2 atribuam recursos suficientes para dar cumprimento ao presente artigo de forma eficaz e atempada. Quando apropriado, as autoridades nacionais competentes devem cooperar com outras autoridades relevantes e podem permitir a participação de outros intervenientes no ecossistema de IA. O presente artigo não afeta outras áreas de testes controlados estabelecidas pela legislação da União ou nacional. Os Estados-Membros devem assegurar um nível adequado de cooperação entre as autoridades que supervisionam essas outras áreas de teste controladas e as autoridades nacionais competentes.

5. Os sandboxes de IA estabelecidos de acordo com o parágrafo 1 devem fornecer um ambiente controlado que promova a inovação e facilite o desenvolvimento, o treinamento, os testes e a validação de sistemas de IA inovadores por um período limitado antes de sua introdução no mercado ou de seu comissionamento, de acordo com um plano de sandbox específico acordado entre os fornecedores ou potenciais fornecedores e a autoridade competente. Esses espaços de teste controlados podem incluir testes supervisionados na vida real.

6. As autoridades competentes devem, sempre que adequado, fornecer orientação, supervisão e apoio no âmbito do ambiente experimental de IA com vista a determinar os riscos, em especial para os direitos fundamentais, a saúde e a segurança, para os testes e medidas de mitigação e a sua eficácia em relação às obrigações e requisitos do presente regulamento e, se aplicável, outras disposições do direito da União e nacional cuja observância é monitorizada no ambiente experimental de IA.

7. As autoridades competentes devem fornecer aos provedores e potenciais provedores que participam do ambiente experimental de IA orientações sobre as expectativas regulatórias e como cumprir os requisitos e obrigações estabelecidos no presente regulamento.

A pedido do fornecedor ou potencial fornecedor do sistema de IA, a autoridade competente deverá fornecer provas escritas das atividades realizadas com sucesso na sandbox controlada. A autoridade competente também fornecerá um relatório de saída detalhando as atividades realizadas no espaço de testes controlado e os resultados e aprendizados correspondentes. Os fornecedores podem usar esta documentação para demonstrar sua conformidade com este Regulamento por meio do processo de avaliação de conformidade relevante ou atividades de vigilância de mercado. A este respeito, as autoridades de fiscalização do mercado e os organismos notificados devem ter em conta de forma positiva os relatórios de produção e as provas escritas fornecidas pela autoridade nacional competente, com vista a acelerar os procedimentos de avaliação da conformidade numa medida razoável.

8. Sujeito às disposições de confidencialidade do artigo 78.º e com o acordo do prestador ou potencial prestador, a Comissão e o Conselho de IA serão autorizados a aceder aos relatórios de resultados e tê-los-ão em conta, conforme adequado, no exercício das suas funções ao abrigo do presente regulamento. Se tanto o fornecedor ou potencial fornecedor como a autoridade nacional competente concordarem expressamente, o relatório de saída pode ser tornado público através da plataforma única de informação referida no presente artigo.

9. A criação de sandboxes de IA terá como objetivo contribuir para os seguintes objetivos:

(a) melhorar a segurança jurídica no que diz respeito ao cumprimento do presente regulamento ou, se for caso disso, de outras disposições do direito da União e nacional aplicáveis;

b) apoiar o intercâmbio de melhores práticas por meio da cooperação com as autoridades envolvidas no ambiente experimental controlado de IA;

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

d) contribuir para a aprendizagem normativa baseada em evidências comprovadas;

(e) facilitar e acelerar o acesso ao mercado da União para sistemas de IA, em especial quando fornecidos por PME, incluindo empresas em fase de arranque.

10. As autoridades nacionais competentes devem garantir que, na medida em que os sistemas inovadores de IA envolvam o processamento de dados pessoais ou estejam abrangidos pelo âmbito de supervisão de outras autoridades nacionais ou autoridades competentes que forneçam ou apoiem o acesso aos dados, as autoridades nacionais de proteção de dados e outras autoridades nacionais ou competentes estejam vinculadas à operação do ambiente de testes de IA e envolvidas na supervisão de tais aspetos, na medida permitida pelas suas respetivas funções e poderes.

11. As sandboxes de IA não afetarão os poderes de supervisão ou corretivos das autoridades competentes que supervisionam as sandboxes de IA, inclusive a nível regional ou local. Quaisquer riscos significativos à saúde, segurança e direitos fundamentais identificados durante o processo de desenvolvimento e teste desses sistemas de IA resultarão em uma redução apropriada. As autoridades nacionais competentes terão poderes para suspender temporária ou permanentemente o processo de testes, ou a participação no ambiente experimental controlado, se a redução efetiva não for possível, e informarão o Gabinete de IA dessa decisão. Para apoiar a inovação da IA na União, as autoridades nacionais competentes exercerão os seus poderes de supervisão dentro dos limites da legislação aplicável e utilizarão o seu poder discricionário ao aplicar disposições legais relativas a um projeto específico de ambiente experimental de IA.

12. Os fornecedores e potenciais fornecedores que participam no sandbox de IA serão responsáveis, de acordo com a legislação da União e nacional sobre responsabilidade, por quaisquer danos causados a terceiros como resultado da experimentação realizada no sandbox. Contudo, desde que os potenciais fornecedores respeitem o plano e as condições específicas da sua participação e sigam de boa-fé as orientações fornecidas pela autoridade nacional competente, as autoridades não imporão multas administrativas por infrações ao presente Regulamento. Quando outras autoridades competentes responsáveis por outras disposições do direito da União e nacional tiverem participado ativamente na supervisão do sistema de IA no ambiente de teste e tiverem fornecido orientações para o cumprimento, não serão impostas multas administrativas em relação a essas disposições.

13. Os sandboxes de IA devem ser concebidos e implementados de modo a facilitar, quando adequado, a cooperação transfronteiriça entre as autoridades nacionais competentes.

14. As autoridades nacionais competentes coordenarão as suas atividades e cooperarão no âmbito do Conselho da IA.

15. As autoridades nacionais competentes devem informar o AI Office e o AI Council sobre o estabelecimento de um sandbox e podem solicitar seu apoio e orientação. O AI Office disponibilizará publicamente uma lista de sandboxes planejadas e existentes e a manterá atualizada para incentivar maior interação em sandboxes de IA, bem como cooperação transfronteiriça.

16. As autoridades nacionais competentes devem apresentar relatórios anuais ao Gabinete de IA e ao Conselho de IA, pela primeira vez um ano após a criação do ambiente experimental de IA e, posteriormente, anualmente até à sua conclusão, bem como um relatório final. Esses relatórios devem fornecer informações sobre o progresso e os resultados da implementação dessas áreas de teste, incluindo melhores práticas, incidentes, lições aprendidas e recomendações sobre sua criação e, quando apropriado, sobre a aplicação e possível revisão do presente regulamento, incluindo seus atos delegados e de execução, e sobre a aplicação de outras disposições do direito da União, conforme monitoradas pelas autoridades competentes no âmbito da área de teste. As autoridades nacionais competentes devem disponibilizar publicamente esses relatórios anuais, ou os seus resumos, online. A Comissão deve, sempre que adequado, ter em conta os relatórios anuais no exercício das suas funções ao abrigo do presente regulamento.

17. A Comissão desenvolverá uma interface única e dedicada contendo todas as informações relevantes relacionadas com as sandboxes de IA para permitir que as partes interessadas interajam com as sandboxes de IA e levantem questões junto das autoridades competentes, bem como solicitem orientações não vinculativas sobre a conformidade de produtos, serviços e modelos de negócio inovadores que incorporem tecnologias de IA, em conformidade com o artigo 62.º, n.º 1, alínea c). A Comissão coordenará proativamente com as autoridades nacionais competentes, sempre que apropriado.

Artigo 58

Disposições detalhadas relativas aos espaços de teste de IA controlados e à operação desses espaços espaços

1. A fim de evitar a fragmentação na União, a Comissão adota atos de execução que especifiquem disposições pormenorizadas para o estabelecimento, desenvolvimento, implementação, operação e supervisão de ambientes de teste de IA. Os atos de execução devem incluir princípios comuns sobre as seguintes questões:

a) os critérios de elegibilidade e seleção para participação no banco de testes de IA;

b) os procedimentos para solicitar, participar, monitorar, sair e encerrar o sandbox de IA, incluindo o plano do sandbox e o relatório de saída;

c) as condições aplicáveis aos participantes.

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

2. Os atos de execução referidos no n.º 1 devem garantir:

(a) que as áreas de testes de IA estejam abertas a qualquer fornecedor ou potencial fornecedor de um sistema de IA que apresente uma candidatura e cumpra os critérios de elegibilidade e seleção, que devem ser transparentes e justos, e que as autoridades nacionais competentes informem os candidatos da sua decisão no prazo de três meses a contar da apresentação da candidatura;

b) que os espaços de testes controlados de IA permitam um acesso amplo e equitativo e se adaptem à procura de participação; Fornecedores e potenciais fornecedores também podem enviar solicitações em parceria com implantadores e outros terceiros relevantes;

(c) as disposições e condições detalhadas relativas às áreas de teste de IA devem, na medida do possível, permitir às autoridades nacionais competentes flexibilidade na criação e gestão das suas áreas de teste de IA;

(d) que o acesso às áreas de testes de IA controladas deve ser gratuito para as PME, incluindo as start-ups, sem prejuízo dos custos excecionais que podem ser recuperados pelas autoridades nacionais competentes de forma justa e proporcional;

(e) que os fornecedores e potenciais fornecedores sejam facilitados, através dos resultados de aprendizagem dos ambientes de teste de IA, no cumprimento das obrigações de avaliação da conformidade previstas no presente regulamento e na aplicação voluntária dos códigos de conduta referidos no artigo 95.º;

(f) que as sandboxes de IA facilitem a participação de outros intervenientes relevantes no ecossistema da IA, tais como organismos notificados e organismos de normalização, PME, incluindo start-ups, empresas, inovadores, instalações de ensaio e experimentação, laboratórios de investigação e experimentação e centros europeus de inovação digital, centros de excelência e investigadores, a fim de permitir e facilitar a cooperação com os setores público e privado;

(g) os procedimentos, processos e requisitos administrativos para a candidatura, seleção, participação e saída do ambiente experimental de IA sejam simples, facilmente inteligíveis e claramente comunicados, a fim de facilitar a participação de PME, incluindo start-ups, com capacidades jurídicas e administrativas limitadas, e sejam simplificados em toda a União, a fim de evitar a fragmentação, e que a participação num ambiente experimental de IA estabelecido por um Estado-Membro ou pela Autoridade Europeia para a Proteção de Dados seja mutuamente e uniformemente reconhecida e tenha os mesmos efeitos jurídicos em toda a União;

(h) que a participação no ambiente experimental de IA é limitada a um período adequado à complexidade e à escala do projeto, podendo ser prorrogada pela autoridade nacional competente;

(i) que as sandboxes de IA facilitem o desenvolvimento de ferramentas e infraestruturas para testar, comparar, avaliar e explicar as dimensões dos sistemas de IA relevantes para a aprendizagem normativa, tais como a precisão, a robustez e a cibersegurança, bem como medidas para mitigar os riscos para os direitos fundamentais e para a sociedade como um todo.

3. Os serviços de pré-implantação, como orientação sobre a aplicação do presente regulamento, outros serviços de valor acrescentado, como assistência com documentos de normalização e certificação, e acesso a instalações de teste e experimentação, a polos europeus de inovação digital e a centros de excelência, serão oferecidos aos potenciais fornecedores que participam em ambientes de teste de IA, em especial PME e start-ups, quando adequado.

4. Sempre que as autoridades nacionais competentes considerem autorizar a realização de testes supervisionados no mundo real dentro de uma área restrita de IA controlada, a ser estabelecida nos termos do presente artigo, elas devem acordar especificamente as condições de tais testes e, em particular, as salvaguardas adequadas, com os participantes, com vistas a proteger os direitos fundamentais, a saúde e a segurança. Sempre que adequado, cooperarão com outras autoridades nacionais competentes, a fim de assegurar a coerência das práticas em toda a União.

Artigo 59

Tratamento posterior de dados pessoais para o desenvolvimento de determinados sistemas de IA no interesse do público
público no espaço de testes controlados para IA

1. No Sandbox, os dados pessoais coletados legalmente para outros fins podem ser processados exclusivamente para fins de desenvolvimento, treinamento e teste de determinados sistemas de IA no Sandbox, onde todas as seguintes condições forem atendidas:

(a) Os sistemas de IA são desenvolvidos para os fins de uma autoridade pública ou outra pessoa singular ou coletiva para proteger um interesse público essencial numa ou mais das seguintes áreas:

(i) saúde e segurança públicas, incluindo a detecção, o diagnóstico, a prevenção, o controlo e o tratamento de doenças e a melhoria dos sistemas de saúde,

(ii) um elevado nível de protecção e melhoria da qualidade ambiental, protecção da biodiversidade, protecção contra a poluição, medidas de transição ecológica, medidas de atenuação e adaptação às alterações climáticas,

iii) sustentabilidade energética,

(iv) a segurança e a resiliência dos sistemas de transporte e da mobilidade, das infra-estruturas e redes críticas,

v) a eficiência e a qualidade da administração pública e dos serviços públicos;

(b) os dados tratados são necessários para cumprir um ou mais dos requisitos referidos no Capítulo III, Secção 2, quando esses requisitos não possam ser eficazmente cumpridos através do tratamento de dados anonimizados ou sintéticos ou de outros dados não pessoais;

(c) existam mecanismos de monitorização eficazes para detetar se podem surgir riscos elevados para os direitos e liberdades dos titulares dos dados, tal como referido no artigo 35.º do Regulamento (UE) 2016/679 e no artigo 39.º do Regulamento (UE) 2018/1725, durante a experimentação na sandbox controlada, bem como mecanismos de resposta para atenuar esses riscos sem demora e, se for caso disso, interromper o tratamento;

(d) que os dados pessoais processados no contexto do sandbox estejam localizados num ambiente de processamento de dados funcionalmente separado, isolado e protegido, sob o controlo do potencial fornecedor, e que apenas pessoas autorizadas tenham acesso a esses dados;

(e) que os prestadores só podem partilhar dados originalmente recolhidos em conformidade com a legislação da União em matéria de proteção de dados; Dados pessoais criados na sandbox não podem sair da sandbox;

(f) o tratamento de dados pessoais no contexto do ambiente de teste não dá origem a medidas ou decisões que afetem os titulares dos dados ou que afetem a execução dos seus direitos ao abrigo do direito da União em matéria de proteção de dados pessoais;

(g) que os dados pessoais processados no contexto do sandbox sejam protegidos por medidas técnicas e organizacionais adequadas e sejam eliminados após o fim da participação no sandbox ou quando os dados pessoais atinjam o fim do seu período de retenção;

(h) os ficheiros de registo do tratamento de dados pessoais no contexto da sandbox são conservados durante o período de participação na sandbox, salvo disposição em contrário da legislação da União ou nacional;

(i) uma descrição completa e detalhada do processo e da lógica subjacentes ao treino, aos testes e à validação do sistema de IA, juntamente com os resultados do processo de teste, é mantida como parte da documentação técnica referida no anexo IV;

(j) um breve resumo do projeto de IA desenvolvido no ambiente experimental, juntamente com os seus objetivos e resultados esperados, é publicado no sítio Web das autoridades competentes; Esta obrigação não abrangerá dados operacionais sensíveis relacionados às atividades das autoridades responsáveis pela aplicação da lei, ao controlo de fronteiras, à imigração ou ao asilo.

2. Quando realizado para fins de prevenção, investigação, detecção ou repressão de infrações penais ou execução de sanções penais, incluindo a proteção contra ameaças à segurança pública e a prevenção delas, e sob o controle e a responsabilidade das autoridades responsáveis pela aplicação da lei, o tratamento de dados pessoais em sandboxes de IA controladas deve basear-se na legislação específica da União ou nacional e deve cumprir as condições cumulativas estabelecidas no parágrafo 1.

3. O parágrafo 1 não prejudica a legislação da União ou nacional que proíbe o tratamento de dados pessoais para fins diferentes dos expressamente mencionados nesses atos, e não prejudica a legislação da União ou nacional que estabelece a base para o tratamento de dados pessoais necessários para desenvolver, testar ou treinar sistemas inovadores de IA ou qualquer outra base jurídica em conformidade com a legislação da União sobre a proteção de dados pessoais.

Artigo 60

Testar sistemas de IA de alto risco em condições reais fora de espaços de teste controlados para IA

1. Os fornecedores ou potenciais fornecedores de sistemas de IA de alto risco listados no Anexo III podem realizar testes em condições reais de sistemas de IA de alto risco fora das áreas de teste de IA controladas, em conformidade com o presente artigo e com o plano de testes em condições reais a que se refere o presente artigo, sem prejuízo das proibições estabelecidas no artigo 5.º.

A Comissão adotará, por meio de um ato de execução, os elementos detalhados do plano de testes em condições reais. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 98.º, n.º 2.

O presente parágrafo não prejudica a legislação da União ou nacional relativa a testes em condições reais de sistemas de IA de alto risco associados a produtos abrangidos pelos atos legislativos de harmonização da União enumerados no Anexo I.

2. Os fornecedores ou potenciais fornecedores podem realizar testes de sistemas de IA de alto risco referidos no Anexo III em condições reais a qualquer momento antes da colocação no mercado ou da entrada em serviço do sistema de IA, por conta própria ou em parceria com um ou mais implantadores ou potenciais implantadores.

3. Os testes de sistemas de IA de alto risco em condições reais, nos termos do presente artigo, não prejudicam qualquer revisão ética exigida pela legislação da União ou nacional.

4. Os fornecedores ou potenciais fornecedores podem realizar testes em condições reais somente quando todas as seguintes condições forem atendidas:

(a) o fornecedor ou potencial fornecedor elaborou um plano de testes em condições reais e apresentou-o à autoridade de fiscalização do mercado do Estado-Membro em que os testes em condições reais serão realizados;

(b) a autoridade de fiscalização do mercado do Estado-Membro onde os testes em condições reais serão realizados tenha aprovado os testes em condições reais e o plano de testes em condições reais; Se a autoridade de fiscalização do mercado não responder no prazo de trinta dias, os testes em condições reais e o plano de testes em condições reais serão considerados aprovados; Quando a legislação nacional não preveja aprovação tácita, os ensaios em condições reais também estarão sujeitos a autorização neste caso;

(c) o fornecedor ou potencial fornecedor, com exceção dos fornecedores ou potenciais fornecedores de sistemas de IA de alto risco referidos nos pontos 1, 6 e 7 do anexo III nas áreas da aplicação da lei, da migração, do asilo e da gestão do controlo de fronteiras, bem como dos sistemas de IA de alto risco referidos no ponto 2 do anexo III, registou os testes em condições reais, em conformidade com o artigo 71.º, n.º 4, com um número de identificação único em toda a União e com as informações estabelecidas no anexo IX; o fornecedor ou potencial fornecedor de sistemas de IA de alto risco referidos nos pontos 1, 6 e 7 do anexo III nas áreas da aplicação da lei, da migração, do asilo e da gestão do controlo de fronteiras registou os testes em condições reais na parte não pública da base de dados da UE, em conformidade com o artigo 49.º, n.º 4, alínea d), com um número de identificação único a nível da União e as informações nele indicadas; o fornecedor ou potencial fornecedor de sistemas de IA de alto risco referidos no ponto 2 do anexo III registou testes em condições reais, em conformidade com o artigo 49.º, n.º 5;

(d) o fornecedor ou potencial fornecedor que realiza os ensaios em condições reais está estabelecido na União ou nomeou um representante legal estabelecido na União;

(e) os dados recolhidos e tratados para efeitos de testes em condições reais só serão transferidos para países terceiros se existirem salvaguardas adequadas e aplicáveis ao abrigo do direito da União;

(f) os ensaios em condições reais não durem mais do que o necessário para atingir os seus objectivos e, em qualquer caso, não excedam os seis meses, podendo ser prorrogados por um período adicional de seis meses, mediante notificação prévia do fornecedor ou potencial fornecedor à autoridade de fiscalização do mercado, acompanhada de uma explicação da necessidade dessa prorrogação;

g) os sujeitos de testes da vida real que sejam membros de grupos vulneráveis devido à sua idade ou deficiência tenham proteção adequada;

(h) quando um fornecedor ou potencial fornecedor organiza testes no mundo real em cooperação com um ou mais implantadores ou potenciais implantadores, estes últimos devem ter sido informados de todos os aspetos dos testes relevantes para a sua decisão de participar e devem ter recebido instruções relevantes para a utilização do sistema de IA referido no artigo 13.º; O fornecedor ou potencial fornecedor e o implantador ou potencial implantador devem chegar a um acordo detalhando suas funções e responsabilidades com vistas a garantir a conformidade com as disposições relativas aos testes em condições reais, nos termos do presente regulamento e de outras disposições da legislação aplicável da União e nacional;

(i) os sujeitos dos testes no mundo real deram consentimento informado, em conformidade com o artigo 61.º ou, na área da execução em que a tentativa de obter consentimento informado impediria que o sistema de IA fosse testado, os testes em si e os resultados dos testes no mundo real não terão qualquer impacto negativo nos sujeitos, cujos dados pessoais serão apagados após a realização do teste;

(j) os testes no mundo real são supervisionados de forma eficaz pelo fornecedor ou potencial fornecedor e pelos implementadores ou potenciais implementadores, recorrendo a pessoas devidamente qualificadas no domínio relevante e com as competências, a formação e a autoridade necessárias para desempenhar as suas tarefas;

k) as previsões, recomendações ou decisões do sistema de IA podem ser efetivamente revertidas e descartadas.

5. Qualquer sujeito de teste na vida real ou seu representante legalmente designado, conforme o caso, pode, sem sofrer qualquer desvantagem e sem ter que fornecer qualquer justificativa, retirar-se do teste a qualquer momento, retirando seu consentimento informado e solicitando a exclusão imediata e permanente de seus dados pessoais. A retirada do consentimento informado não afetará as atividades já concluídas.

6. Em conformidade com o artigo 75.º, os Estados-Membros devem conferir às suas autoridades de fiscalização do mercado o poder de exigir que os fornecedores e potenciais fornecedores forneçam informações, realizem inspecções remotas sem aviso prévio ouno locale controlar o desempenho de testes no mundo real e sistemas de IA de alto risco relacionados. As autoridades de fiscalização do mercado usarão esses poderes para garantir que os testes no mundo real sejam realizados com segurança.

7. Qualquer incidente grave detectado durante o curso de testes em condições reais deve ser relatado à autoridade nacional de fiscalização do mercado, de acordo com o Artigo 73. O fornecedor ou potencial fornecedor deve tomar medidas de redução imediatas ou, na sua falta, suspender os testes em condições reais até que tal redução ocorra ou encerrar os testes. O fornecedor ou potencial fornecedor deverá estabelecer um procedimento para recuperação rápida do sistema de IA no caso de os testes no mundo real serem encerrados.

8. O fornecedor ou potencial fornecedor deve notificar a autoridade nacional de fiscalização do mercado do Estado-Membro em que os testes em condições reais serão realizados sobre a suspensão ou o término dos testes em condições reais e os resultados finais.

9. O fornecedor ou potencial fornecedor será responsável, de acordo com a legislação aplicável da União e nacional em matéria de responsabilidade, por quaisquer danos causados no decurso dos seus testes em condições reais.

Artigo 61

Consentimento informado para participar em testes em condições reais fora dos espaços controlados Testando para IA

1. Para efeitos de testes em condições reais, nos termos do artigo 60.º, o consentimento informado e livremente dado deverá ser obtido dos sujeitos dos testes antes da participação em tais testes e após lhes terem sido fornecidas informações concisas, claras, relevantes e compreensíveis relativamente a:

a) a natureza e os objetivos dos testes em condições reais e os possíveis inconvenientes associados à sua participação;

b) as condições em que os testes no mundo real serão conduzidos, incluindo a duração esperada da participação do(s) sujeito(s);

(c) os seus direitos e garantias relativos à sua participação, nomeadamente o direito de recusar a participação e o direito de desistir dos testes em condições reais em qualquer momento, sem sofrer qualquer desvantagem e sem ter de apresentar qualquer justificação;

(d) disposições para solicitar a reversão ou o descarte de previsões, recomendações ou decisões do sistema de IA;

(e) o número de identificação único da União do teste em condições reais, em conformidade com o artigo 60.º, n.º 4, alínea c), e os dados de contacto do fornecedor ou do seu representante legal, junto dos quais podem ser obtidas informações adicionais.

2. O consentimento informado será datado e documentado, e uma cópia será entregue aos sujeitos do teste ou seus representantes legais.

Artigo 62

Medidas dirigidas aos fornecedores e aos responsáveis pela implementação, em particular às PME, incluindo as empresas emergente

1. Os Estados-Membros tomarão as seguintes medidas:

(a) proporcionar às PME, incluindo as start-ups, com sede ou sucursal registada na União, acesso prioritário a ambientes de teste de IA controlados, desde que cumpram as condições de elegibilidade e os critérios de seleção; O acesso prioritário não impede que outras PME, incluindo start-ups, que não as referidas no presente número, acedam à Sandbox de IA, desde que também cumpram as condições de elegibilidade e os critérios de seleção;

(b) organizar atividades de sensibilização e formação específicas sobre a aplicação do presente regulamento, adaptadas às necessidades das PME, incluindo as empresas em fase de arranque, os mobilizadores e, se for caso disso, as autoridades públicas locais;

(c) utilizar os canais existentes e, quando adequado, estabelecer novos canais específicos para a comunicação com as PME, incluindo as start-ups, os implementadores e outros intervenientes inovadores, bem como, quando adequado, as autoridades públicas locais, a fim de prestar aconselhamento e responder a questões levantadas relativamente à aplicação do presente regulamento, nomeadamente em relação à participação em ambientes de teste de IA;

d) incentivar a participação de PMEs e outras partes interessadas relevantes no processo de desenvolvimento da normalização.

2. Os interesses e necessidades específicos dos fornecedores de PME, incluindo as start-ups, devem ser tidos em conta na fixação de taxas para avaliação da conformidade nos termos do artigo 43.º, e essas taxas devem ser reduzidas proporcionalmente à sua dimensão, à dimensão do mercado e a outros indicadores relevantes.

3. O Gabinete de IA tomará as seguintes medidas:

(a) fornecer modelos padronizados para as áreas abrangidas pelo presente regulamento, conforme especificado pelo Conselho da IA no seu pedido;

(b) desenvolver e manter uma plataforma de informação única que forneça informações de fácil utilização relacionadas com o presente regulamento para todos os operadores da União;

(c) organizar campanhas de comunicação adequadas para aumentar a sensibilização para as obrigações decorrentes do presente regulamento;

d) avaliar e promover a convergência de boas práticas em procedimentos de contratação pública em relação aos sistemas de IA.

Artigo 63

Exceções para operadores específicos

1. As microempresas, na acepção da Recomendação 2003/361/CE, podem cumprir determinados elementos do sistema de gestão da qualidade exigidos pelo artigo 17.º do presente regulamento de forma simplificada, desde que não tenham empresas associadas ou empresas ligadas, na acepção dessa Recomendação. Para esse fim, a Comissão desenvolverá diretrizes sobre os elementos do sistema de gestão da qualidade que podem ser cumpridos de forma simplificada, levando em consideração as necessidades das microempresas, sem afetar o nível de proteção ou a necessidade de cumprir os requisitos relativos aos sistemas de IA de alto risco.

2. O parágrafo 1 do presente artigo não deve ser interpretado como isentando tais 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

GOVERNANÇA

SEÇÃO 1

Governação a nível da União

Artigo 64

Escritório de IA

1. A Comissão desenvolverá a experiência e as capacidades da União no domínio da IA através do Gabinete de IA.

2. Os Estados-Membros devem facilitar as tarefas confiadas ao Gabinete de IA, tal como refletido no presente regulamento.

Artigo 65

Criação e estrutura do Conselho Europeu de Inteligência Artificial

1. É criado um Conselho Europeu de Inteligência Artificial (a seguir designado por «Conselho da IA»).

2. O Conselho da IA será composto por um representante por Estado-Membro. A Autoridade Europeia para a Proteção de Dados participará como observadora. O AI Office também participará das reuniões do Conselho de IA sem participar da votação. O Conselho da IA pode convidar outras autoridades, organismos ou especialistas nacionais e da União para as reuniões, caso a caso, sempre que os tópicos discutidos sejam relevantes para eles.

3. Cada representante será nomeado pelo seu Estado-Membro por um período de três anos, renovável uma vez.

4. Os Estados-Membros devem assegurar que os seus representantes no Conselho da IA:

(a) Dispor, no seu Estado-Membro, dos poderes e competências relevantes para poderem contribuir activamente para o cumprimento das tarefas do Conselho de Administração da IA referidas no artigo 66.º;

(b) ser designado como um ponto de contacto único para o Conselho da IA e, quando adequado, tendo em conta as necessidades dos Estados-Membros, como um ponto de contacto único para as partes interessadas;

(c) ter poderes para facilitar a coerência e a coordenação entre as autoridades nacionais competentes no seu Estado-Membro em relação à aplicação do presente regulamento, nomeadamente através da recolha de dados e informações relevantes para o cumprimento das suas funções no Conselho da AI.

5. Os representantes designados dos Estados-Membros adoptarão o Regulamento Interno do Conselho da AI por maioria de dois terços. O Regulamento Interno estabelecerá, em particular, os procedimentos para o processo de seleção, a duração do mandato e as especificações das funções do Presidente, as modalidades detalhadas de votação e a organização das atividades do Conselho da AI e dos seus subgrupos.

6. O Conselho da IA estabelecerá dois subgrupos permanentes para fornecer uma plataforma para 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 de fiscalização do mercado deve atuar como um grupo de cooperação administrativa (ADCO) para o presente regulamento, na aceção do artigo 30.º do Regulamento (UE) 2019/1020.

O Conselho da IA pode estabelecer outros subgrupos permanentes ou temporários, conforme apropriado, para examinar questões específicas. Quando apropriado, representantes do fórum consultivo referido no Artigo 67 podem ser convidados para esses subgrupos ou para reuniões específicas desses subgrupos como observadores.

7. O Conselho da IA será organizado e gerido de forma a preservar a objetividade e a imparcialidade das suas atividades.

8. O Conselho da IA será presidido por um dos representantes dos Estados-Membros. O Gabinete da IA atuará como secretaria do Conselho da IA, convocará reuniões a pedido do Presidente e elaborará a pauta de acordo com as funções do Conselho da IA de acordo com estas Regras e seu Regulamento Interno.

Artigo 66

Funções do Conselho de IA

O Conselho de Administração da IA prestará aconselhamento e assistência à Comissão e aos Estados-Membros para facilitar a aplicação coerente e eficaz do presente regulamento. Para este efeito, o Conselho da IA pode, em particular:

(a) contribuir para a coordenação entre as autoridades nacionais competentes responsáveis pela aplicação do presente regulamento e, em cooperação e mediante acordo entre as autoridades de fiscalização do mercado em causa, apoiar as atividades conjuntas das autoridades de fiscalização do mercado referidas no artigo 74.º, n.º 11;

b) recolher e partilhar conhecimentos técnicos e regulamentares e melhores práticas entre os Estados-Membros;

(c) prestar aconselhamento sobre a aplicação do presente regulamento, em especial no que diz respeito ao cumprimento das regras relativas aos modelos de IA para fins gerais;

(d) contribuir para a harmonização das práticas administrativas nos Estados-Membros, nomeadamente no que se refere à isenção dos procedimentos de avaliação da conformidade referidos no artigo 46.º, à operação de ambientes de testes controlados para a IA e aos ensaios em condições reais referidos nos artigos 57.º, 59.º e 60.º;

(e) a pedido da Comissão ou por sua própria iniciativa, emitir recomendações e pareceres escritos sobre qualquer matéria relevante relacionada com a implementação do presente regulamento e a sua aplicação coerente e eficaz, por exemplo:

(i) sobre o desenvolvimento e a aplicação de códigos de conduta e de boas práticas, em conformidade com o presente regulamento e as orientações da Comissão,

(ii) sobre a avaliação e revisão do presente regulamento nos termos do artigo 112.º, incluindo no que diz respeito aos relatórios de incidentes graves referidos no artigo 73.º e ao funcionamento da base de dados da UE referida no artigo 71.º, à preparação de atos delegados ou de execução e no que diz respeito a possíveis adaptações do presente regulamento aos atos legislativos de harmonização da União enumerados no anexo I,

(iii) nas especificações técnicas ou normas existentes relativas aos requisitos estabelecidos no Capítulo III, Secção 2,

(iv) sobre a utilização de normas harmonizadas ou especificações comuns referidas nos artigos 40.º e 41.º,

(v) sobre tendências, como a competitividade global da Europa no domínio da IA, a adopção da IA na União e o desenvolvimento de capacidades digitais,

(vi) sobre as tendências na tipologia em mudança das cadeias de valor da IA, em particular sobre as implicações resultantes em termos de responsabilização,

(vii) sobre a possível necessidade de alterar o Anexo III, em conformidade com o artigo 7.º, e sobre a possível necessidade de rever o artigo 5.º, em conformidade com o artigo 112.º, tendo em conta as provas relevantes disponíveis e os desenvolvimentos tecnológicos recentes;

(f) apoiar a Comissão na promoção da literacia em matéria de IA, da sensibilização do público e da compreensão dos benefícios, riscos, salvaguardas e direitos e obrigações relacionados com a utilização de sistemas de IA;

(g) facilitar o desenvolvimento de critérios comuns e de um entendimento partilhado entre os operadores de mercado e as autoridades competentes dos conceitos relevantes previstos no presente regulamento, por exemplo, contribuindo para o desenvolvimento de índices de referência;

(h) cooperar, sempre que adequado, com outras instituições, organismos, gabinetes e agências da União, bem como com os grupos e redes de peritos relevantes 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 proteção dos consumidores e da proteção de dados e dos direitos fundamentais;

(i) contribuir para uma cooperação eficaz com as autoridades competentes de países terceiros e com organizações internacionais;

(j) auxiliar as autoridades nacionais competentes e a Comissão no desenvolvimento das competências técnicas e organizacionais necessárias à execução do presente regulamento, por exemplo, contribuindo para a avaliação das necessidades de formação do pessoal dos Estados-Membros envolvido na sua execução;

(k) auxiliar o Gabinete de IA a apoiar as autoridades nacionais competentes na criação e desenvolvimento de sandboxes de IA e facilitar a cooperação e a troca de informações entre sandboxes de IA;

l) contribuir para o desenvolvimento de documentos de orientação e fornecer aconselhamento relevante sobre os mesmos;

(m) prestar aconselhamento à Comissão sobre questões internacionais de IA;

(n) emitir pareceres à Comissão sobre alertas qualificados relativos a modelos de IA de uso geral;

(o) receber pareceres dos Estados-Membros sobre alertas qualificados relativos a modelos de IA para fins gerais e sobre experiências e práticas nacionais na supervisão e aplicação de sistemas de IA, em particular sistemas que integram modelos de IA para fins gerais.

Artigo 67

Fórum consultivo

1. Será criado um fórum consultivo para fornecer conhecimentos especializados e aconselhamento ao Conselho da IA e à Comissão, bem como para contribuir para as suas tarefas ao abrigo do presente regulamento.

2. A composição do fórum consultivo representará uma seleção equilibrada de partes interessadas, incluindo indústria, start-ups, PMEs, sociedade civil e academia. A composição do fórum consultivo será equilibrada no que diz respeito aos interesses comerciais e não comerciais e, dentro da categoria de interesses comerciais, no que diz respeito às PMEs e outras empresas.

3. A Comissão nomeará os membros do fórum consultivo, de acordo com os critérios estabelecidos no n.º 2, de entre as partes interessadas com reconhecida competência no domínio da IA.

4. O mandato dos membros do fórum consultivo será de dois anos, podendo ser prorrogado por um máximo de quatro anos.

5. A Agência dos Direitos Fundamentais da União Europeia, a Agência da União Europeia para a Cibersegurança, o Comité Europeu de Normalização (CEN), o Comité Europeu de Normalização Eletrotécnica (Cenelec) e o Instituto Europeu de Normas de Telecomunicações (ETSI) serão membros permanentes do fórum consultivo.

6. O fórum consultivo estabelecerá seu próprio regulamento interno. Elegerá entre os seus membros dois copresidentes, de acordo com os critérios previstos no n.º 2. O mandato dos copresidentes será de dois anos, renovável uma vez.

7. O fórum consultivo realizará reuniões pelo menos duas vezes por ano. Você poderá convidar especialistas e outras partes interessadas para suas reuniões.

8. O fórum consultivo pode elaborar pareceres, recomendações e contribuições escritas a pedido do Conselho da IA ou da Comissão.

9. O fórum consultivo poderá estabelecer subgrupos permanentes ou temporários, conforme apropriado, para examinar questões específicas relacionadas aos objetivos deste Regulamento.

10. O fórum consultivo elaborará um relatório anual sobre as suas atividades. Este relatório será disponibilizado ao público.

Artigo 68

Grupo de especialistas científicos independentes

1. A Comissão, por meio de um ato de execução, adota disposições relativas à criação de um grupo de peritos científicos independentes (a seguir designado por «grupo de peritos científicos») para apoiar as atividades de execução previstas no presente regulamento. O referido ato de execução é adotado pelo procedimento de exame a que se refere o artigo 98.º, n.º 2.

2. O grupo de peritos científicos será composto por peritos selecionados pela Comissão com base em conhecimentos científicos ou técnicos atualizados no domínio da IA, necessários para as tarefas definidas no n.º 3, e deverá ser capaz de demonstrar que preenche todas as seguintes condições:

a) conhecimentos especializados e competências específicas, e conhecimentos científicos ou técnicos no domínio da IA;

b) independência de qualquer fornecedor de sistemas de IA ou modelos de IA de uso geral;

c) capacidade de executar atividades com diligência, precisão e objetividade.

A Comissão, em consulta com o Conselho da IA, determinará o número de especialistas no grupo de acordo com as necessidades exigidas e garantirá uma representação geográfica e de gênero justa.

3. O Grupo de Peritos Científicos aconselhará e apoiará o Gabinete de IA, em particular no que diz respeito às seguintes funções:

(a) apoiar a implementação e a execução do presente regulamento no que diz respeito aos sistemas e modelos de IA para fins gerais, em particular:

(i) alertar o Gabinete de IA para potenciais riscos sistémicos a nível da União decorrentes de modelos de IA para fins gerais, em conformidade com o artigo 90.º,

(ii) contribuir para o desenvolvimento de ferramentas e metodologias para avaliar as capacidades dos sistemas e modelos de IA de uso geral, nomeadamente através de avaliações comparativas,

iii) aconselhar sobre a classificação de modelos de IA de uso geral com risco sistémico,

(iv) aconselhar sobre a classificação de vários sistemas e modelos de IA de uso geral,

v) contribuir para o desenvolvimento de ferramentas e modelos;

b) apoiar o trabalho das autoridades de fiscalização do mercado, a pedido destas;

(c) apoiar as atividades de fiscalização do mercado transfronteiriça referidas no artigo 74.º(11), sem prejuízo dos poderes das autoridades de fiscalização do mercado;

(d) apoiar o Gabinete de Auditoria Interna no exercício das suas funções no contexto do procedimento de salvaguarda da União, nos termos do artigo 81.º.

4. Os peritos do grupo desempenharão as suas funções de forma imparcial e objectiva e garantirão a confidencialidade das informações e dados obtidos no exercício das suas funções e actividades. Eles não devem procurar ou aceitar instruções de ninguém no exercício de suas funções nos termos do parágrafo 3. Cada especialista deve preencher uma declaração de interesses que será tornada pública. O Escritório de IA estabelecerá sistemas e procedimentos para gerenciar e prevenir ativamente potenciais conflitos de interesse.

5. O ato de execução a que se refere o n.º 1 deve incluir disposições sobre as condições, os procedimentos e os acordos detalhados para que o grupo de peritos científicos e os seus membros emitam alertas e solicitem a assistência do Gabinete de IA no exercício das funções do grupo de peritos científicos.

Artigo 69

Acesso a peritos pelos Estados-Membros

1. Os Estados-Membros podem recorrer a peritos do grupo de peritos científicos para apoiar as suas atividades de execução ao abrigo do presente regulamento.

2. Os Estados-Membros podem ser obrigados a pagar taxas pelo aconselhamento e apoio prestados por peritos. A estrutura e o montante das taxas, bem como a escala e a estrutura dos custos recuperáveis, serão definidos no ato de execução a que se refere o artigo 68.º, n.º 1, tendo em conta os objetivos da aplicação adequada do presente regulamento, a relação custo-eficácia e a necessidade de assegurar que todos os Estados-Membros tenham acesso efetivo a peritos.

3. A Comissão deve facilitar o acesso oportuno dos Estados-Membros aos peritos, conforme necessário, e deve assegurar que a combinação de atividades de apoio realizadas pelas estruturas de apoio aos testes de IA da União, nos termos do artigo 84.º, e pelos peritos, nos termos do presente artigo, seja organizada de forma eficiente e ofereça o maior valor acrescentado possível.

SEÇÃO 2

Autoridades nacionais competentes

Artigo 70

Designação de autoridades nacionais competentes e pontos de contacto únicos

1. Cada Estado-Membro deve criar ou designar pelo menos uma autoridade notificadora e pelo menos uma autoridade de fiscalização do mercado como autoridades nacionais competentes para efeitos do presente regulamento. Essas autoridades nacionais competentes exercerão os seus poderes de forma independente, imparcial e imparcial, a fim de preservar a objetividade das suas atividades e funções e de assegurar a aplicação e o cumprimento do presente regulamento. Os membros destas autoridades abster-se-ão de qualquer ato incompatível com as suas funções. Desde que esses princípios sejam respeitados, tais atividades e funções podem ser realizadas por uma ou mais autoridades designadas, de acordo com as necessidades organizacionais do Estado-Membro.

2. Os Estados-Membros devem informar a Comissão sobre a identidade das autoridades notificadoras e das autoridades de fiscalização do mercado e as funções dessas autoridades, bem como quaisquer alterações subsequentes às mesmas. Os Estados-Membros devem disponibilizar ao público, por meios eletrónicos, informações sobre como contactar as autoridades competentes e os pontos de contacto únicos até 2 de agosto de 2025. Os Estados-Membros devem designar uma autoridade de fiscalização do mercado para atuar como ponto de contacto único para o presente regulamento e devem notificar a Comissão da identidade desse ponto. A Comissão disponibilizará publicamente a lista de pontos de contacto únicos.

3. Os Estados-Membros devem assegurar que as suas autoridades nacionais competentes dispõem de recursos técnicos, financeiros e humanos e de infraestruturas adequados para desempenhar eficazmente as suas tarefas ao abrigo do presente regulamento. Em particular, as autoridades nacionais competentes devem dispor permanentemente de pessoal suficiente cujas competências e conhecimentos especializados devem incluir um profundo conhecimento da IA, dos dados e das tecnologias de computação de dados; proteção de dados pessoais, segurança cibernética, riscos aos direitos fundamentais, saúde e segurança, e conhecimento das normas e requisitos legais atuais. Os Estados-Membros devem avaliar anualmente e, sempre que necessário, atualizar as competências e os requisitos de recursos referidos no presente parágrafo.

4. As autoridades nacionais competentes tomarão as medidas adequadas para garantir um nível adequado de segurança cibernética.

5. No exercício das suas funções, as autoridades nacionais competentes agirão em conformidade com as obrigações de confidencialidade estabelecidas no artigo 78.º.

6. Até 2 de agosto de 2025 e, posteriormente, de dois em dois anos, os Estados-Membros devem apresentar à Comissão um relatório sobre o estado dos recursos financeiros e humanos das autoridades nacionais competentes, incluindo uma avaliação da sua adequação. A Comissão encaminhará essas informações ao Conselho de Administração da IA para discussão e, quando apropriado, para recomendações.

7. A Comissão facilitará o intercâmbio de experiências entre as autoridades nacionais competentes.

8. As autoridades nacionais competentes podem fornecer orientação e aconselhamento sobre a aplicação do presente regulamento, em particular às PME, incluindo as start-ups, tendo em conta a orientação e o aconselhamento do Conselho da IA e da Comissão, conforme adequado. Sempre que uma autoridade nacional competente pretenda fornecer orientação e aconselhamento em relação a um sistema de IA em áreas regulamentadas por outros atos do direito da União, as autoridades nacionais competentes devem ser consultadas em conformidade com esses atos, conforme adequado.

9. Sempre que as instituições, órgãos, gabinetes e agências da União sejam abrangidos pelo âmbito de aplicação do presente regulamento, a Autoridade Europeia para a Proteção de Dados atua como autoridade competente para a sua supervisão.

CAPÍTULO VIII

BASE DE DADOS DA UE PARA SISTEMAS DE IA DE ALTO RISCO

Artigo 71

Base de dados da UE para sistemas de IA de alto risco listada no ANEXO III

1. A Comissão, em colaboração com os Estados-Membros, deve criar e manter uma base de dados da UE que contenha as informações referidas nos n.ºs 2 e 3 do presente artigo relativas aos sistemas de IA de alto risco referidos no artigo 6.º, n.º 2, que estejam registados nos termos dos artigos 49.º e 60.º e aos sistemas de IA que não sejam considerados de alto risco nos termos do artigo 6.º, n.º 3, e que estejam registados nos termos do artigo 6.º, n.º 4, e do artigo 49.º. A Comissão deve consultar os peritos relevantes ao estabelecer as especificações funcionais dessa base de dados e o Conselho de IA ao atualizá-la.

2. Os dados enumerados no Anexo VIII, Secções A e B, devem ser introduzidos na base de dados da UE pelo fornecedor ou, quando aplicável, pelo representante autorizado.

3. Os dados enumerados na secção C do anexo VIII devem ser introduzidos na base de dados da UE pela pessoa responsável pela implantação, ou agindo em seu nome, que seja uma autoridade, organismo, serviço ou agência pública, em conformidade com o artigo 49.º, n.os 3 e 4.

4. Com exceção da secção referida no artigo 49.º, n.º 4, e no artigo 60.º, n.º 4, alínea c), as informações conservadas na base de dados da UE e registadas em conformidade com o artigo 49.º devem ser acessíveis e facilmente disponibilizadas ao público. As informações devem ser fáceis de navegar e legíveis por máquinas. As informações registradas de acordo com o Artigo 60 só podem ser acessadas pelas autoridades de fiscalização do mercado e pela Comissão, a menos que o fornecedor potencial ou o fornecedor tenha dado seu consentimento para que as informações também sejam acessíveis ao público.

5. A base de dados da UE só deve conter dados pessoais na medida necessária para a recolha e o tratamento de informações em conformidade com o presente regulamento. Essas informações devem incluir os nomes e detalhes de contato das pessoas físicas responsáveis pelo registro do sistema e que tenham autoridade legal para representar o provedor ou a pessoa responsável pela implantação, conforme aplicável.

6. A Comissão será a controladora da base de dados da UE e fornecerá apoio técnico e administrativo adequado aos fornecedores, potenciais fornecedores e implantadores. A base de dados da UE deve cumprir os requisitos de acessibilidade aplicáveis.

CAPÍTULO IX

VIGILÂNCIA PÓS-COMERCIALIZAÇÃO, TROCA DE INFORMAÇÕES E VIGILÂNCIA DE MERCADO

SEÇÃO 1

Vigilância pós-comercialização

Artigo 72

Vigilância pós-comercialização por fornecedores e plano de vigilância pós-comercialização para sistemas de IA de alto risco

1. Os fornecedores devem estabelecer e documentar um sistema de vigilância pós-comercialização de maneira proporcional à natureza das tecnologias de IA e aos riscos dos sistemas de IA de alto risco.

2. O sistema de vigilância pós-comercialização deve coletar, documentar e analisar de forma ativa e sistemática dados relevantes que podem ser fornecidos pelos implantadores ou coletados por outras fontes sobre o desempenho dos sistemas de IA de alto risco ao longo de sua vida útil, e que permitem ao fornecedor avaliar a conformidade contínua dos sistemas de IA com os requisitos estabelecidos no Capítulo III, Seção 2. Quando apropriado, a vigilância pós-comercialização incluirá análise da interação com outros sistemas de IA. Esta obrigação não abrangerá dados operacionais sensíveis dos responsáveis pela implantação, que são autoridades responsáveis por garantir o cumprimento da lei.

3. O sistema de vigilância pós-comercialização deve ser baseado num plano de vigilância pós-comercialização. O plano de vigilância pós-comercialização deve fazer parte da documentação técnica referida no anexo IV. A Comissão deve adotar um ato de execução que estabeleça disposições detalhadas que constituam um modelo para o plano de vigilância pós-comercialização e a lista de elementos a incluir no mesmo até 2 de fevereiro de 2026. Esse ato de execução deve ser adotado em conformidade com o procedimento de exame referido no artigo 98.º, n.º 2.

4. Para sistemas de IA de alto risco regulamentados pelos atos legislativos de harmonização da União listados na Seção A do Anexo I, onde um sistema e um plano de vigilância pós-comercialização já tenham sido estabelecidos de acordo com esses atos, a fim de garantir a consistência, evitar duplicações e minimizar encargos adicionais, os provedores podem optar por integrar, conforme apropriado, os elementos necessários descritos nos parágrafos 1, 2 e 3, usando o modelo referido no parágrafo 3, em sistemas e planos já em vigor ao abrigo dessa legislação, desde que atinja um nível equivalente de proteção.

O primeiro parágrafo do presente parágrafo aplica-se também aos sistemas de IA de alto risco referidos no ponto 5 do anexo III colocados no mercado ou em serviço por instituições financeiras sujeitas a requisitos relativos à sua governação, sistemas ou processos internos ao abrigo da legislação da União em matéria de serviços financeiros.

SEÇÃO 2

Troca de informações sobre incidentes graves

Artigo 73

Relatar incidentes graves

1. Os fornecedores de sistemas de IA de alto risco colocados no mercado da União devem notificar qualquer incidente grave às autoridades de fiscalização do mercado dos Estados-Membros em que o incidente ocorreu.

2. A notificação referida no n.º 1 deve ser efetuada imediatamente após o prestador ter estabelecido um nexo de causalidade entre o sistema de IA e o incidente grave ou a probabilidade razoável de que tal nexo exista e, em qualquer caso, o mais tardar 15 dias após o prestador ou, se for caso disso, o responsável pela implementação, tomar conhecimento do incidente grave.

O prazo de notificação referido no primeiro parágrafo deverá ter em conta a magnitude do incidente grave.

3. Não obstante o disposto no n.º 2 do presente artigo, no caso de uma infração generalizada ou de um incidente grave, tal como definido na alínea b) do artigo 3.º, ponto 49, a notificação referida no n.º 1 do presente artigo deve ser efetuada imediatamente e, o mais tardar, dois dias após o prestador ou, se for caso disso, a pessoa responsável pela implementação tomar conhecimento do incidente.

4. Não obstante o disposto no parágrafo 2, em caso de morte de uma pessoa, a notificação deverá ser feita imediatamente após o fornecedor ou o mobilizador ter estabelecido — ou assim que o fornecedor ou o mobilizador suspeitar — de uma relação causal entre o sistema de IA de alto risco e o incidente grave, mas o mais tardar dez dias a contar da data em que o fornecedor ou, quando aplicável, o mobilizador tiver conhecimento do incidente grave.

5. Quando necessário para garantir a notificação oportuna, o provedor ou, quando aplicável, o implantador pode inicialmente enviar uma notificação incompleta, seguida de uma notificação completa.

6. Após notificar um incidente grave nos termos do parágrafo 1, o Provedor deverá realizar sem demora as investigações necessárias em relação ao incidente grave e ao sistema de IA afetado. Isso incluirá uma avaliação de risco do incidente e medidas corretivas.

O fornecedor deve cooperar com as autoridades competentes e, se aplicável, com o organismo notificado em causa durante as investigações referidas no primeiro parágrafo e não deve tomar qualquer medida que possa modificar o sistema de IA afetado de uma forma que possa ter impacto em qualquer avaliação subsequente das causas do incidente sem primeiro informar as autoridades competentes dessa medida.

7. Após o recebimento de uma notificação relativa a um incidente grave referido na alínea c) do artigo 3.º, ponto 49, a autoridade de fiscalização do mercado relevante deve informar as autoridades ou organismos públicos nacionais referidos no artigo 77.º(1). A Comissão deve desenvolver orientações específicas para facilitar o cumprimento das obrigações estabelecidas no n.º 1 do presente artigo. Essas diretrizes serão publicadas até 2 de agosto de 2025 e serão avaliadas periodicamente.

8. A autoridade de fiscalização do mercado deve tomar as medidas adequadas previstas no artigo 19.º do Regulamento (UE) 2019/1020 no prazo de sete dias a contar da data em que receber a notificação referida no n.º 1 do presente artigo e deve seguir os procedimentos de notificação previstos nesse regulamento.

9. No caso de sistemas de IA de alto risco referidos no anexo III colocados no mercado ou em serviço por prestadores sujeitos a instrumentos legislativos da União que estabeleçam obrigações de comunicação equivalentes às estabelecidas no presente regulamento, a comunicação de incidentes graves deve limitar-se aos referidos no artigo 3.º, ponto 49, alínea c).

10. No caso de sistemas de IA de alto risco que sejam componentes de segurança de dispositivos, ou que sejam eles próprios dispositivos, regulados pelos Regulamentos (UE) 2017/745 e (UE) 2017/746, a notificação de incidentes graves deve limitar-se aos referidos na alínea c) do artigo 3.º, ponto 49, do presente regulamento, e deve ser efetuada à autoridade nacional competente escolhida para o efeito pelos Estados-Membros em que o incidente ocorreu.

11. As autoridades nacionais competentes devem informar imediatamente a Comissão de qualquer incidente grave, independentemente de terem tomado alguma medida a esse respeito, em conformidade com o artigo 20.º do Regulamento (UE) 2019/1020.

SEÇÃO 3

Garantia de conformidade

Artigo 74

Vigilância do mercado e controlo dos sistemas de IA no mercado da UE

1. O Regulamento (UE) 2019/1020 aplica-se aos sistemas de IA regulados pelo presente regulamento. Para efeitos de garantir o cumprimento efetivo do presente regulamento:

(a) qualquer referência a um operador económico nos termos do Regulamento (UE) 2019/1020 deve ser considerada como incluindo todos os operadores referidos no artigo 2.º, n.º 1, do presente regulamento;

(b) qualquer referência a um produto ao abrigo do Regulamento (UE) 2019/1020 deve ser considerada como incluindo todos os sistemas de IA abrangidos pelo âmbito de aplicação do presente regulamento.

2. Como parte das suas obrigações de comunicação de informações nos termos do artigo 34.º, n.º 4, do Regulamento (UE) 2019/1020, as autoridades de fiscalização do mercado devem comunicar anualmente à Comissão e às autoridades nacionais da concorrência relevantes quaisquer informações recolhidas no decurso das atividades de fiscalização do mercado que possam ser de potencial interesse para a aplicação do direito da concorrência da União. Deverão também apresentar anualmente um relatório à Comissão sobre qualquer utilização de práticas proibidas que tenha ocorrido durante esse ano e sobre as medidas tomadas.

3. Para sistemas de IA de alto risco associados a produtos regulamentados pelos atos legislativos de harmonização da União enumerados na secção A do anexo I, a autoridade de fiscalização do mercado para efeitos do presente regulamento será a autoridade responsável pelas atividades de fiscalização do mercado designada nos termos desses atos legislativos.

Em derrogação do primeiro parágrafo, em circunstâncias adequadas, os Estados-Membros podem designar outra autoridade relevante como autoridade de fiscalização do mercado, desde que seja assegurada a coordenação com as autoridades setoriais de fiscalização do mercado relevantes, responsáveis pela aplicação dos atos legislativos de harmonização da União enumerados no anexo I.

4. Os procedimentos referidos nos artigos 79.º a 83.º do presente regulamento não se aplicam aos sistemas de IA associados a produtos regulamentados pelos atos legislativos de harmonização da União enumerados na secção A do anexo I, sempre que esses atos legislativos já prevejam procedimentos que garantam um nível equivalente de proteção e que tenham o mesmo objetivo. Nesses casos, serão aplicados 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, para efeitos de assegurar a aplicação efetiva do presente regulamento, as autoridades de fiscalização do mercado podem exercer remotamente os poderes referidos nas alíneas d) e j) do artigo 14.º, n.º 4, desse regulamento, conforme adequado.

6. No caso de sistemas de IA de alto risco colocados no mercado, colocados em serviço ou utilizados por instituições financeiras regulamentadas pela legislação da União em matéria de serviços financeiros, a autoridade de fiscalização do mercado para efeitos do presente regulamento será a autoridade nacional relevante responsável pela supervisão financeira dessas instituições ao abrigo dessa 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, em circunstâncias adequadas e desde que seja assegurada a coordenação, o Estado-Membro pode designar outra autoridade relevante como autoridade de fiscalização do mercado para efeitos do presente regulamento.

Autoridades nacionais de fiscalização do mercado que supervisionam instituições de crédito regulamentadas pela Diretiva 2013/36/UE e participam no Mecanismo Único de Supervisão estabelecido pelo Regulamento (UE) n.º$_{\text{qualquer}}$1024/2013 comunicarão sem demora ao Banco Central Europeu quaisquer informações obtidas no decurso das suas atividades de vigilância do mercado que possam ser relevantes para as tarefas de supervisão prudencial do Banco Central Europeu especificadas nesse regulamento.

8. Para os sistemas de IA de alto risco enumerados no ponto 1 do anexo III do presente regulamento, na medida em que os sistemas sejam utilizados para efeitos de aplicação da lei, gestão de fronteiras, justiça e democracia, e para os sistemas de IA de alto risco enumerados nos pontos 6, 7 e 8 do anexo III do presente regulamento, os Estados-Membros devem designar como autoridades de fiscalização do mercado para efeitos do presente regulamento as autoridades de supervisão da proteção de dados competentes 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 não devem de forma alguma afetar a independência das autoridades judiciais nem interferir de outra forma nas suas atividades no exercício da sua função judicial.

9. Sempre que as instituições, órgãos, gabinetes e agências da União sejam abrangidos pelo âmbito de aplicação do presente regulamento, a Autoridade Europeia para a Proteção de Dados atua como respetiva autoridade de fiscalização do mercado, exceto em relação ao Tribunal de Justiça da União Europeia quando atua no exercício da sua função jurisdicional.

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 relevantes responsáveis pela supervisão da aplicação da legislação de harmonização da União referida no anexo I ou de outras disposições do direito da União que possam ser relevantes para os sistemas de IA de alto risco referidos no anexo III.

11. As autoridades de fiscalização do mercado e a Comissão podem propor atividades conjuntas, incluindo investigações conjuntas, a serem realizadas pelas autoridades de fiscalização do mercado ou pelas autoridades de fiscalização do mercado em conjunto com a Comissão, com o objetivo de promover a conformidade, detetar a não conformidade, aumentar a sensibilização ou fornecer orientações em relação ao presente regulamento no que diz respeito a categorias específicas de sistemas de IA de alto risco que representam um risco grave em dois ou mais Estados-Membros, em conformidade com o artigo 9.º do Regulamento (UE) 2019/1020. O Gabinete de Inteligência Artificial fornecerá suporte de coordenação para investigações conjuntas.

12. Sem prejuízo dos poderes previstos no Regulamento (UE) 2019/1020, e quando apropriado e limitado ao necessário para o desempenho das suas tarefas, os prestadores devem conceder às autoridades de fiscalização do mercado acesso total à documentação, bem como aos conjuntos de dados de formação, validação e teste utilizados para o desenvolvimento de sistemas de IA de alto risco, incluindo, quando apropriado e sujeito a salvaguardas de segurança, através de interfaces de programação de aplicações (API) ou outras ferramentas e meios técnicos relevantes que permitam o acesso remoto.

13. As autoridades de fiscalização do mercado terão acesso ao código-fonte do sistema de IA de alto risco mediante pedido fundamentado e apenas se estiverem reunidas as duas condições seguintes:

a) o acesso ao código-fonte é necessário para avaliar a conformidade de um sistema de IA de alto risco com os requisitos estabelecidos no Capítulo III, Secção 2, e

b) todos os procedimentos de teste ou auditoria e verificações baseados em dados e documentação fornecidos pelo fornecedor foram esgotados ou se mostraram insuficientes.

14. Qualquer informação ou documentação obtida pelas autoridades de fiscalização do mercado será tratada de acordo com as obrigações de confidencialidade estabelecidas no artigo 78.º.

Artigo 75

Assistência mútua, vigilância de mercado e controlo de sistemas de IA de uso geral

1. Quando um sistema de IA for baseado num modelo de IA de uso geral e tanto o modelo como o sistema forem desenvolvidos por um único fornecedor, o Gabinete de IA terá poderes para monitorizar e supervisionar a conformidade desse sistema de IA com as obrigações previstas no presente regulamento. Para executar estas tarefas de supervisão e fiscalização, o Gabinete de IA dispõe de todos os poderes de uma autoridade previstos na presente secção e no Regulamento (UE) 2019/1020.

2. Sempre que as autoridades de fiscalização do mercado relevantes tenham motivos suficientes para considerar que os sistemas de IA de uso geral que podem ser diretamente utilizados pelos implantadores para pelo menos uma das finalidades classificadas como de alto risco nos termos do presente regulamento não cumprem os requisitos estabelecidos no presente regulamento, devem cooperar com o Gabinete de IA para realizar avaliações de conformidade e comunicar as mesmas ao Conselho de IA e às outras autoridades de fiscalização do mercado.

3. Quando uma autoridade de fiscalização do mercado não conseguir concluir a sua investigação sobre o sistema de IA de alto risco devido à sua incapacidade de aceder a determinadas informações relativas ao modelo de IA de uso geral, apesar de ter envidado todos os esforços adequados para obter essas informações, pode apresentar um pedido fundamentado ao Gabinete de IA para impor o acesso a essas informações. Nesse caso, o AI Office deverá fornecer à autoridade requerente, sem demora e, em qualquer caso, no prazo de trinta dias, todas as informações que o AI Office considerar relevantes para determinar se um sistema de IA de alto risco não está em conformidade. As autoridades de fiscalização do mercado devem manter a confidencialidade das informações obtidas em conformidade com o artigo 78.º do presente regulamento. Será aplicadomutatis mutandiso procedimento previsto no Capítulo VI do Regulamento (UE) 2019/1020.

Artigo 76

Supervisão de testes em condições reais por autoridades de vigilância de mercado

1. As autoridades de fiscalização do mercado devem ter os poderes e as competências necessários para garantir que os testes em condições reais estejam em conformidade com o presente regulamento.

2. Quando forem realizados testes reais de sistemas de IA supervisionados dentro de uma área restrita de IA, nos termos do artigo 58.º, as autoridades de fiscalização do mercado devem verificar o cumprimento do artigo 60.º como parte da sua função de supervisão na área restrita de IA. Essas autoridades podem, conforme apropriado, permitir que o fornecedor ou potencial fornecedor realize testes em condições reais, como uma exceção às condições estabelecidas no Artigo 60(4)(f) e (g).

3. Sempre que uma autoridade de fiscalização do mercado tenha sido informada pelo potencial fornecedor, pelo fornecedor ou por um terceiro de um incidente grave ou tenha outras razões para crer que as condições estabelecidas nos artigos 60.º e 61.º não estão reunidas, pode tomar uma das seguintes decisões no seu território, conforme adequado:

a) suspender ou encerrar os testes em condições reais;

b) exigir que o fornecedor ou potencial fornecedor e a pessoa responsável pela implantação ou a pessoa responsável pela implantação potencial modifiquem qualquer aspecto do teste no mundo real.

4. Sempre que uma autoridade de fiscalização do mercado tiver tomado uma decisão referida no n.º 3 do presente artigo ou tiver levantado uma objeção na aceção do artigo 60.º, n.º 4, alínea b), a decisão ou objeção deve indicar os motivos da decisão e os meios disponíveis para o fornecedor ou potencial fornecedor contestar a decisão ou objeção.

5. Se for caso disso, quando uma autoridade de fiscalização do mercado tiver tomado uma decisão referida no n.º 3, deve comunicar os motivos dessa decisão às autoridades de fiscalização do mercado dos outros Estados-Membros em que o sistema de IA foi testado em conformidade com o plano de testes.

Artigo 77

Poderes das autoridades responsáveis pela protecção dos direitos fundamentais

1. As autoridades ou organismos públicos nacionais responsáveis pela monitorização ou execução de obrigações ao abrigo do direito da União relativas à proteção dos direitos fundamentais, incluindo o direito à não discriminação, no que diz respeito à utilização de sistemas de IA de alto risco referidos no anexo III têm o direito de solicitar e aceder a qualquer documentação criada ou mantida nos termos do presente regulamento, numa língua e num formato acessíveis, sempre que o acesso a essa documentação seja necessário para o desempenho eficaz dos seus mandatos, dentro dos limites da sua jurisdição. A autoridade ou organismo público relevante deve informar a autoridade de fiscalização do mercado do Estado-Membro relevante de qualquer pedido desse tipo.

2. Até 2 de novembro de 2024, cada Estado-Membro deve designar as autoridades ou organismos públicos referidos no n.º 1 e incluí-los numa lista que deve tornar pública. Os Estados-Membros devem notificar esta lista à Comissão e aos outros Estados-Membros e mantê-la atualizada.

3. Quando a documentação referida no n.º 1 não for suficiente para estabelecer se houve uma violação das obrigações decorrentes do direito da União relativas à proteção dos direitos fundamentais, a autoridade ou organismo público referido no n.º 1 pode apresentar um pedido fundamentado à autoridade de fiscalização do mercado para organizar testes do sistema de IA de alto risco por meios técnicos. A autoridade de fiscalização do mercado deve organizar os testes em estreita cooperação com a autoridade ou organismo público requerente dentro de um prazo razoável após a apresentação do pedido.

4. Qualquer informação ou documentação obtida pelas autoridades ou organismos públicos nacionais referidos no parágrafo 1 deste artigo, nos termos do presente artigo, será tratada de acordo com as obrigações de confidencialidade previstas no artigo 78.º.

Artigo 78

Confidencialidade

1. A Comissão, as autoridades de fiscalização do mercado, os organismos notificados e qualquer outra pessoa singular ou coletiva envolvida na aplicação do presente regulamento, em conformidade com o direito da União ou nacional, devem respeitar a confidencialidade das informações e dos dados obtidos no exercício das suas funções e atividades, de modo a proteger, em especial:

a) direitos de propriedade intelectual e industrial e informações comerciais confidenciais ou segredos comerciais de uma pessoa singular ou coletiva, incluindo o código-fonte, exceto nos casos referidos no artigo 5.º da Diretiva (UE) 2016/943 do Parlamento Europeu e do Conselho ([57]);

(b) a aplicação efectiva do presente regulamento, em especial para efeitos de investigações, inspecções ou auditorias;

c) os interesses da segurança pública e nacional;

d) o desenvolvimento de processos criminais ou de procedimentos administrativos;

(e) informações classificadas ao abrigo do direito da União ou do direito nacional.

2. As autoridades envolvidas na aplicação do presente regulamento nos termos do n.º 1 só devem solicitar os dados estritamente necessários para a avaliação do risco colocado pelos sistemas de IA e para o exercício dos seus poderes ao abrigo do presente regulamento e do Regulamento (UE) 2019/1020. Devem implementar medidas de segurança cibernética adequadas e eficazes para proteger a segurança e a confidencialidade das informações e dos dados obtidos e eliminar os dados recolhidos assim que deixarem de ser necessários para os fins para os quais foram obtidos, em conformidade com a legislação aplicável da União e nacional.

3. Sem prejuízo dos parágrafos 1 e 2, as informações trocadas de forma confidencial entre autoridades nacionais competentes ou entre autoridades nacionais competentes e a Comissão não serão divulgadas sem consulta prévia à autoridade nacional competente de origem e ao mobilizador, quando as autoridades responsáveis pela aplicação da lei, pelo controlo de fronteiras, pela imigração ou pelo asilo utilizarem sistemas de IA de alto risco referidos nos pontos 1, 6 ou 7 do Anexo III e tal divulgação comprometer os interesses públicos e de segurança nacional. Esta troca de informações não incluirá dados operacionais sensíveis relacionados às atividades das autoridades responsáveis pela aplicação da lei, controle de fronteiras, imigração ou asilo.

Quando as autoridades responsáveis pela aplicação da lei, pela imigração ou pelo asilo forem fornecedoras de sistemas de IA de alto risco referidos no Anexo III, pontos 1, 6 ou 7, a documentação técnica referida no Anexo IV permanecerá nas instalações dessas autoridades. Essas autoridades devem assegurar que as autoridades de fiscalização do mercado referidas no artigo 74.º, n.os 8 e 9, conforme o caso, possam, mediante pedido, aceder ou obter imediatamente uma cópia da documentação. O acesso a tal documentação ou a qualquer cópia dela somente será permitido ao pessoal da autoridade de vigilância do mercado que possua um nível adequado de autorização de segurança.

4. Os n.os 1, 2 e 3 não afetam os direitos ou obrigações da Comissão, dos Estados-Membros e das suas autoridades competentes, nem os direitos ou obrigações dos organismos notificados no que diz respeito ao intercâmbio de informações e à divulgação de alertas, incluindo no contexto da cooperação transfronteiriça, nem as obrigações de prestação de informações ao abrigo do direito penal dos Estados-Membros que incumbem às partes interessadas.

5. Sempre que necessário e em conformidade com as disposições pertinentes dos acordos internacionais e comerciais, a Comissão e os Estados-Membros podem trocar informações confidenciais com autoridades reguladoras de países terceiros com os quais tenham celebrado acordos de confidencialidade bilaterais ou multilaterais que garantam um nível adequado de confidencialidade.

Artigo 79

Procedimento aplicável a nível nacional aos sistemas de IA que apresentam um risco

1. Os sistemas de IA que apresentam um risco devem ser entendidos como «produtos que apresentam um risco», tal como definido no artigo 3.º, ponto 19, do Regulamento (UE) 2019/1020, na medida em que apresentem riscos que afetem a saúde, a segurança ou os direitos fundamentais das pessoas.

2. Sempre que a autoridade de fiscalização do mercado de um Estado-Membro tiver motivos suficientes para considerar que um sistema de IA apresenta um risco referido no n.º 1 do presente artigo, deve efetuar uma avaliação do sistema de IA em causa para verificar a sua conformidade com todos os requisitos e obrigações estabelecidos no presente regulamento. Deve-se dar atenção especial aos sistemas de IA que representam um risco para grupos vulneráveis. Sempre que forem identificados riscos para os direitos fundamentais, a autoridade de fiscalização do mercado deve também informar as autoridades nacionais ou os organismos públicos relevantes referidos no artigo 77.º, n.º 1, e cooperar plenamente com eles. Os operadores relevantes devem cooperar, conforme necessário, com a autoridade de fiscalização do mercado e outras autoridades nacionais ou organismos públicos referidos no artigo 77.º(1).

([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).

Sempre que, no decurso dessa avaliação, a autoridade de fiscalização do mercado ou, se aplicável, a autoridade de fiscalização do mercado em cooperação com a autoridade pública nacional referida no artigo 77.º, n.º 1, verificar que o sistema de IA não cumpre os requisitos e obrigações estabelecidos no presente regulamento, deve, sem demora injustificada, exigir que o operador relevante tome todas as medidas corretivas adequadas para tornar o sistema de IA conforme com esses requisitos e obrigações, para retirar o sistema de IA do mercado ou para o recolher, num prazo que essa autoridade possa determinar e, em qualquer caso, no prazo máximo de 15 dias úteis ou no prazo que possa ser previsto nos atos de harmonização legislativa da União pertinentes, conforme adequado.

A autoridade de fiscalização do mercado deve informar o organismo notificado relevante em conformidade. O artigo 18.º do Regulamento (UE) 2019/1020 aplica-se às medidas referidas no segundo parágrafo da presente secção.

3. Sempre que a autoridade de fiscalização do mercado considerar que a não conformidade não se limita ao seu território nacional, deve informar a Comissão e os outros Estados-Membros, sem demora injustificada, dos resultados da avaliação e das medidas que solicitou que o operador tomasse.

4. O operador deve garantir que sejam tomadas todas as medidas corretivas adequadas em relação a todos os sistemas de IA afetados que tenha colocado no mercado na União.

5. Caso o operador de um sistema de IA não tome as medidas corretivas adequadas dentro do prazo referido no n.º 2, a autoridade de fiscalização do mercado deve tomar todas as medidas provisórias adequadas para proibir ou restringir a colocação no mercado do sistema de IA no seu mercado nacional ou a sua entrada em serviço, para retirar o produto ou o sistema de IA autónomo desse mercado ou para o recolher. A referida autoridade notificará estas medidas sem demora injustificada à Comissão e aos outros Estados-Membros.

6. A notificação referida no n.º 5 deve incluir todos os detalhes disponíveis, em especial as informações necessárias para a identificação do sistema de IA não conforme, a origem do sistema de IA e da cadeia de abastecimento, a natureza da alegada não conformidade e o risco representado, a natureza e a duração das medidas nacionais adotadas e os argumentos apresentados pelo operador relevante. Especificamente, as autoridades de fiscalização do mercado devem indicar se a não conformidade se deve a uma ou mais das seguintes razões:

(a) o incumprimento da proibição de práticas de IA referida no artigo 5.º;

(b) falha de um sistema de IA de alto risco em cumprir os requisitos estabelecidos no Capítulo III, Secção 2;

(c) deficiências nas normas harmonizadas ou nas especificações comuns referidas nos artigos 40.º e 41.º que conferem a presunção de conformidade;

d) o incumprimento do disposto no artigo 50.º.

7. As autoridades de fiscalização do mercado que não sejam a autoridade de fiscalização do mercado do Estado-Membro que iniciou o procedimento devem, sem demora injustificada, comunicar à Comissão e aos outros Estados-Membros quaisquer medidas que tomem e quaisquer informações adicionais à sua disposição relativas à não conformidade do sistema de IA em causa e, em caso de desacordo com a medida nacional notificada, as suas objeções à mesma.

8. Se, no prazo de três meses a contar da receção da notificação referida no n.º 5 do presente artigo, nenhuma autoridade de fiscalização do mercado de um Estado-Membro ou a Comissão levantarem objeções a uma medida provisória tomada por uma autoridade de fiscalização do mercado de outro Estado-Membro, a medida será considerada justificada. Isto não prejudica os direitos processuais do operador relevante nos termos do artigo 18.º do Regulamento (UE) 2019/1020. O prazo de três meses a que se refere o presente número será reduzido para trinta dias em caso de incumprimento da proibição de práticas de IA referida no artigo 5.º do presente regulamento.

9. As autoridades de fiscalização do mercado devem assegurar que sejam tomadas sem demora injustificada medidas restritivas adequadas relativamente ao produto ou sistema de IA em causa, tais como a retirada do produto ou sistema de IA do seu mercado.

Artigo 80

Procedimento aplicável aos sistemas de IA classificados pelo fornecedor como não de alto risco na aplicação do Anexo III

1. Sempre que uma autoridade de fiscalização do mercado tiver motivos suficientes para considerar que um sistema de IA que o fornecedor classificou como não sendo de alto risco nos termos do artigo 6.º, n.º 3, é de alto risco, essa autoridade deve efetuar uma avaliação do sistema de IA em causa no que diz respeito à sua classificação como um sistema de IA de alto risco com base nas condições estabelecidas no artigo 6.º, n.º 3, e nas orientações da Comissão.

2. Sempre que, ao efetuar essa avaliação, a autoridade de fiscalização do mercado verificar que o sistema de IA em causa apresenta um risco elevado, deve, sem demora injustificada, exigir que o fornecedor relevante tome todas as medidas necessárias para garantir que o sistema de IA cumpre os requisitos e obrigações estabelecidos no presente regulamento e tome as medidas corretivas adequadas num prazo que a autoridade de fiscalização do mercado possa determinar.

3. Sempre que a autoridade de fiscalização do mercado considerar que a utilização do sistema de IA em causa não se limita ao seu território nacional, deve informar a Comissão e os outros Estados-Membros, sem demora injustificada, dos resultados da avaliação e das medidas que exigiu que o fornecedor tomasse.

4. O prestador deve garantir que sejam tomadas todas as medidas necessárias para garantir que o sistema de IA cumpre os requisitos e obrigações estabelecidos no presente regulamento. Caso o fornecedor de um sistema de IA afetado não tome as medidas necessárias para garantir o cumprimento desses requisitos e obrigações dentro do prazo referido no parágrafo 2 do presente artigo, serão-lhe impostas multas em conformidade com o artigo 99.º.

5. O fornecedor deve garantir que todas as medidas corretivas adequadas sejam tomadas para todos os sistemas de IA afetados que tenha colocado no mercado em toda a União.

6. Caso o fornecedor do sistema de IA em causa não tome as medidas corretivas adequadas no prazo referido no n.º 2 do presente artigo, aplica-se o artigo 79.º, n.ºs 5 a 9.

7. Sempre que, ao efetuar a avaliação nos termos do n.º 1 do presente artigo, a autoridade de fiscalização do mercado determinar que o fornecedor classificou incorretamente o sistema de IA como não sendo de alto risco, a fim de contornar a aplicação dos requisitos estabelecidos no Capítulo III, Secção 2, serão impostas coimas ao fornecedor nos termos do artigo 99.º.

8. No exercício dos seus poderes de supervisão 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 referida no artigo 71.º do presente regulamento.

Artigo 81

Procedimento de salvaguarda da União

1. Sempre que, no prazo de três meses a contar da receção da notificação referida no artigo 79.º, n.º 5, ou no prazo de 30 dias em caso de incumprimento da proibição de práticas de IA referida no artigo 5.º, a autoridade de fiscalização do mercado de um Estado-Membro levantar objeções a uma medida tomada por outra autoridade de fiscalização do mercado, ou sempre que a Comissão considerar que a medida é contrária ao direito da União, a Comissão deve iniciar consultas sem demora injustificada com a autoridade de fiscalização do mercado do Estado-Membro em causa e com o(s) operador(es) e deve avaliar a medida nacional. Com base nos resultados dessa avaliação, a Comissão deve, no prazo de seis meses a contar da notificação referida no artigo 79.º, n.º 5, ou de sessenta dias em caso de incumprimento da proibição de práticas de IA referida no artigo 5.º, decidir se a medida nacional é justificada e notificar a sua decisão à autoridade de fiscalização do mercado do Estado-Membro em causa. A Comissão também informará as outras autoridades de fiscalização do mercado sobre sua decisão.

2. Sempre que a Comissão considerar que a medida tomada pelo Estado-Membro relevante é justificada, todos os Estados-Membros devem assegurar que sejam tomadas medidas restritivas adequadas relativamente ao sistema de IA em causa, tais como exigir a retirada do sistema de IA do seu mercado sem demora injustificada, e devem informar a Comissão desse facto. Caso a Comissão considere que a medida nacional não é justificada, o Estado-Membro em causa deve retirá-la e informar a Comissão desse facto.

3. Sempre que a medida nacional for considerada justificada e a não conformidade do sistema de IA for atribuída a deficiências nas normas harmonizadas ou nas especificações comuns referidas nos artigos 40.º e 41.º do presente regulamento, a Comissão aplicará o procedimento previsto no artigo 11.º do Regulamento (UE) n.º 1079/2008.qualquer1025/2012.

Artigo 82

Sistemas de IA compatíveis que apresentam um risco

1. Sempre que, após efetuar uma avaliação em conformidade com o artigo 79.º e consultar a autoridade pública nacional referida no artigo 77.º, n.º 1, a autoridade de fiscalização do mercado de um Estado-Membro concluir que um sistema de IA de risco elevado, apesar de cumprir o presente regulamento, apresenta, no entanto, um risco para a saúde ou a segurança das pessoas, para os direitos fundamentais ou para outros aspetos do interesse público, deve exigir que o operador em causa tome todas as medidas adequadas para garantir que o sistema de IA em causa deixe de apresentar esse risco quando for colocado no mercado ou em serviço, sem demora injustificada, num prazo que essa autoridade pode determinar.

2. O fornecedor ou outro operador relevante deve garantir que sejam tomadas medidas corretivas em relação a todos os sistemas de IA afetados que tenha colocado no mercado da União dentro do período determinado pela autoridade de fiscalização do mercado do Estado-Membro referido no n.º 1.

3. Os Estados-Membros devem informar imediatamente a Comissão e os outros Estados-Membros quando chegarem a uma conclusão nos termos do n.º 1. As informações fornecidas devem incluir todos os detalhes disponíveis, em especial os dados necessários para detetar o sistema de IA em causa e determinar a sua origem e cadeia de fornecimento, a natureza do risco colocado e a natureza e duração das medidas nacionais adotadas.

4. A Comissão deve, sem demora injustificada, iniciar consultas com os Estados-Membros em causa e os operadores relevantes e avaliar as medidas nacionais tomadas. Com base nos resultados desta avaliação, a Comissão decidirá se a medida é justificada e, se necessário, proporá outras medidas adequadas.

5. A Comissão comunicará imediatamente a sua decisão aos Estados-Membros em causa e aos operadores relevantes. Deverá também informar os outros Estados-Membros.

Artigo 83

Não conformidade formal

1. Sempre que a autoridade de fiscalização do mercado de um Estado-Membro detetar uma das seguintes situações, deve exigir que o fornecedor em causa corrija a não conformidade em questão num prazo que a autoridade de fiscalização do mercado pode determinar:

a) a marcação CE foi aposta em violação do artigo 48.º;

b) a marcação CE não foi aposta;

(c) a declaração da UE não foi elaborada em conformidade com o artigo 47.º;

(d) a declaração da UE não foi elaborada corretamente, em conformidade com o artigo 47.º;

(e) o registo na base de dados da UE, em conformidade com o artigo 71.º, não foi efectuado;

f) quando aplicável, não tenha sido nomeado um representante autorizado;

g) não há documentação técnica disponível.

2. Se a não conformidade referida no n.º 1 persistir, a autoridade de fiscalização do mercado do Estado-Membro em causa deve tomar medidas adequadas e proporcionais para restringir ou proibir a colocação no mercado do sistema de IA de alto risco ou para garantir que este seja recolhido ou retirado do mercado sem demora.

Artigo 84

Estruturas de apoio para testes de IA da UE

1. A Comissão designa uma ou mais estruturas de apoio aos testes de IA da União para realizar as atividades enumeradas no artigo 21.º, n.º 6, do Regulamento (UE) 2019/1020 no domínio da IA.

2. Sem prejuízo das atividades referidas no n.º 1, as estruturas de apoio aos testes de IA da União devem também prestar aconselhamento técnico ou científico independente, a pedido do Conselho de IA, da Comissão ou das autoridades de fiscalização do mercado.

SEÇÃO 4

Formas de apelação

Artigo 85

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 crer que houve uma violação do presente regulamento pode apresentar queixa à autoridade de fiscalização do mercado competente.

De acordo com o Regulamento (UE) 2019/1020, tais reclamações serão levadas em consideração ao realizar atividades de fiscalização do mercado e serão tratadas de acordo com procedimentos específicos estabelecidos para essa finalidade pelas autoridades de fiscalização do mercado.

Artigo 86

Direito à explicação das decisões tomadas individualmente

1. Qualquer pessoa que seja afetada por uma decisão tomada pelo responsável pela implantação com base nos resultados de saída de um sistema de IA de alto risco enumerado no Anexo III, com exceção dos sistemas enumerados no ponto 2 do mesmo, e que produza efeitos jurídicos ou o afete substancialmente, de modo que considere que tem um efeito prejudicial na sua saúde, segurança ou direitos fundamentais, terá o direito de obter do responsável pela implantação explicações claras e significativas sobre o papel que o sistema de IA desempenhou no processo de tomada de decisão e os principais elementos da decisão tomada.

2. O n.º 1 não se aplica à utilização de sistemas de IA para os quais existam exceções ou restrições à obrigação prevista nesse número decorrentes do direito da União ou do direito nacional, em conformidade com o direito da União.

3. O presente artigo aplica-se apenas na medida em que o direito referido no n.º 1 não esteja previsto de outro modo no direito da União.

Artigo 87

Denúncia de infrações e proteção de denunciantes

A Diretiva (UE) 2019/1937 aplica-se à comunicação de infrações ao presente regulamento e à proteção das pessoas que comunicam tais infrações.

SEÇÃO 5

Supervisão, investigação, conformidade e monitoramento de provedores de modelos de IA de uso geral

Artigo 88

Conformidade com as obrigações dos provedores de modelos de IA de uso geral

1. A Comissão terá poderes exclusivos para monitorizar e fazer cumprir o Capítulo V, tendo em conta as garantias processuais previstas no artigo 94.º. A Comissão deverá confiar a execução destas tarefas ao Gabinete de Auditoria Interna, sem prejuízo dos poderes organizacionais da Comissão e da repartição de poderes entre os Estados-Membros e a União ao abrigo dos Tratados.

2. Sem prejuízo do 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 necessário e proporcionado para auxiliar a execução das atividades abrangidas pela sua competência ao abrigo do presente regulamento.

Artigo 89

Medidas de acompanhamento

1. Para executar as tarefas que lhe são conferidas pela presente Secção, o Gabinete de IA pode tomar as medidas necessárias para monitorizar a implementação e execução efetivas do presente Regulamento pelos fornecedores de modelos de IA de uso geral, incluindo a sua conformidade com códigos de boas práticas aprovados.

2. Os fornecedores subsequentes terão o direito de apresentar queixas alegando violações do presente regulamento. As reclamações devem ser devidamente justificadas e indicar, no mínimo:

a) o ponto de contacto do fornecedor do modelo de IA de uso geral em questão;

(b) uma descrição dos factos, das disposições do presente regulamento afetadas e das razões pelas quais o fornecedor a jusante considera que o fornecedor do modelo de IA para fins gerais em causa violou o presente regulamento;

c) quaisquer outras informações que o prestador subsequente que apresentar a reclamação considere relevantes, tais como, quando aplicável, informações que tenha recolhido por sua própria iniciativa.

Artigo 90

Alertas do grupo de peritos científicos sobre riscos sistémicos

1. O grupo de peritos científicos pode fornecer alertas qualificados ao Gabinete de IA quando tiver motivos para suspeitar que:

(a) um modelo de IA para fins gerais representa um risco específico reconhecível a nível da União, ou

(b) um modelo de IA para fins gerais satisfaz as condições referidas no artigo 51.º.

2. Após a recepção de tal alerta qualificado, a Comissão pode, através do Gabinete de Auditoria Interna e após ter informado o Conselho de Administração da Auditoria Interna, exercer os poderes previstos na presente secção para avaliar a questão. O Gabinete de IA informará o Conselho de IA sobre quaisquer medidas tomadas nos termos dos artigos 91 a 94.

3. Os alertas qualificados devem ser devidamente justificados e indicar, no mínimo:

a) o ponto de contacto do fornecedor do modelo de IA de uso geral com o risco sistémico em questão;

b) uma descrição dos factos e das razões pelas quais o grupo de peritos científicos está a emitir o alerta;

(c) quaisquer outras informações que o grupo de peritos científicos considere relevantes, tais como, quando apropriado, informações que tenha recolhido por sua própria iniciativa.

Artigo 91

Poderes para solicitar documentação e informações

1. A Comissão pode solicitar ao fornecedor do modelo de IA para fins gerais em causa que forneça a documentação preparada pelo fornecedor em conformidade com os artigos 53.º e 55.º, ou qualquer outra informação necessária para avaliar a conformidade do fornecedor com o presente regulamento.

2. Antes de enviar a solicitação de informações, o AI Office pode iniciar um diálogo estruturado com o fornecedor do modelo de IA de uso geral.

3. Quando o grupo de peritos científicos apresentar um pedido devidamente fundamentado, a Comissão pode dirigir um pedido de informações ao fornecedor de um modelo de IA para fins gerais, se o acesso a essas informações for necessário e proporcional para que o grupo de peritos científicos desempenhe as suas tarefas nos termos do artigo 68.º(2).

4. O pedido de informação deve indicar o fundamento jurídico e a finalidade do pedido, especificar quais as informações pretendidas, fixar o prazo em que as informações devem ser prestadas e indicar as multas previstas no artigo 101.º por prestação de informação incorrecta, incompleta ou enganosa.

5. O fornecedor do modelo de IA de uso geral interessado, ou seu representante, deverá fornecer as informações solicitadas. No caso de pessoas jurídicas, corporações ou empresas, ou quando o provedor não tiver personalidade jurídica, as pessoas autorizadas por lei ou por seus estatutos a representá-las fornecerão as informações solicitadas em nome do provedor do modelo de IA de uso geral em questão. Advogados devidamente autorizados podem fornecer informações em nome de seus clientes. As partes representadas, no entanto, permanecerão totalmente responsáveis se as informações fornecidas estiverem incompletas, incorretas ou enganosas.

Artigo 92

Poderes para realizar avaliações

1. O Gabinete de IA, após consulta ao Conselho de IA, pode realizar avaliações do modelo de IA de uso geral em questão, a fim de:

(a) avaliar se o fornecedor cumpre as suas obrigações ao abrigo do presente regulamento, quando as informações recolhidas nos termos do artigo 91.º forem insuficientes, ou

(b) investigar os riscos sistémicos à escala da União dos modelos de IA para fins gerais com risco sistémico, em especial na sequência de um alerta qualificado do grupo de peritos científicos, em conformidade com o artigo 90.º, n.º 1, alínea a).

2. A Comissão pode decidir nomear peritos independentes para realizar as avaliações em seu nome, incluindo peritos científicos do grupo criado em conformidade com o artigo 68.º. Os peritos independentes nomeados para realizar estas tarefas devem cumprir os critérios estabelecidos no artigo 68.º, n.º 2.

3. Para efeitos do n.º 1, a Comissão pode solicitar acesso ao modelo de IA de uso geral em questão através de APIs ou outros meios e ferramentas técnicas adequados, como o código-fonte.

4. O pedido de acesso deverá indicar o fundamento jurídico, a finalidade e os motivos do pedido, bem como fixar o prazo durante o qual o acesso deve ser facultado e as multas previstas no artigo 101.º pela sua não prestação.

5. Os fornecedores de modelos de IA de uso geral interessados ou seus representantes devem fornecer as informações solicitadas. No caso de pessoas jurídicas, corporações ou empresas, ou quando o provedor não tiver personalidade jurídica, as pessoas autorizadas por lei ou por seus estatutos a representá-las facilitarão o acesso solicitado em nome do provedor do modelo de IA de uso geral em questão.

6. A Comissão adota atos de execução que estabeleçam as modalidades e condições detalhadas das avaliações, incluindo disposições pormenorizadas para o envolvimento de peritos independentes e o procedimento para a sua seleção. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 98.º, n.º 2.

7. Antes de solicitar acesso ao modelo de IA de uso geral relevante, o AI Office pode iniciar um diálogo estruturado com o fornecedor do modelo de IA de uso geral para coletar mais informações sobre os testes internos do modelo, salvaguardas internas para evitar riscos sistêmicos e outros procedimentos e medidas internas que o fornecedor tenha tomado para mitigar tais riscos.

Artigo 93

Poderes para solicitar a adoção de medidas

1. Sempre que necessário e apropriado, a Comissão pode exigir que os fornecedores:

(a) tomar as medidas adequadas para cumprir as obrigações estabelecidas nos artigos 53.º e 54.º;

(b) implementar medidas de redução dos riscos sempre que a avaliação efetuada em conformidade com o artigo 92.º indique que existem razões sérias e fundamentadas para preocupação quanto à existência de um risco sistémico a nível da União;

c) restringir a comercialização do modelo, retirá-lo ou recuperá-lo.

2. Antes de solicitar uma ação, o AI Office pode iniciar um diálogo estruturado com o fornecedor do modelo de IA de uso geral.

3. Se, durante o diálogo estruturado referido no n.º 2, o fornecedor do modelo de IA de uso geral com risco sistémico se comprometer a tomar medidas de atenuação para fazer face a um risco sistémico a nível da União, a Comissão pode, por meio de uma decisão, tornar esses compromissos vinculativos e declarar que já não existem motivos para agir.

Artigo 94

Garantias processuais para operadores económicos do modelo de IA de uso geral

O artigo 18.º do Regulamento (UE) 2019/1020 é aplicávelmutatis mutandisaos fornecedores do modelo de IA de uso geral, sem prejuízo das salvaguardas processuais mais específicas previstas no presente regulamento.

CAPÍTULO X

CÓDIGOS DE CONDUTA E DIRETRIZES

Artigo 95

Códigos de conduta para a aplicação voluntária de requisitos específicos

1. O Gabinete de IA e os Estados-Membros devem incentivar e facilitar o desenvolvimento de códigos de conduta, com mecanismos de governação adequados, 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 de alto risco, tendo em conta as soluções técnicas disponíveis e as melhores práticas da indústria que permitam a implementação desses requisitos.

2. O Gabinete de IA e os Estados-Membros devem facilitar o desenvolvimento de códigos de conduta relativos à implementação voluntária, incluindo pelos implementadores, de requisitos específicos para todos os sistemas de IA, com base em objetivos claros e indicadores-chave de desempenho para medir a concretização desses objetivos, incluindo, mas não se limitando a, elementos como:

(a) os elementos aplicáveis estabelecidos nas Diretrizes Éticas da União para uma IA Fiável;

(b) avaliar e minimizar os impactos dos sistemas de IA na sustentabilidade ambiental, nomeadamente no que diz respeito à programação energeticamente eficiente e às técnicas para conceber, treinar e utilizar a IA de forma eficiente;

(c) promover a literacia em IA, em particular para aqueles envolvidos no desenvolvimento, operação e utilização da IA;

(d) facilitar a conceção inclusiva e diversificada de sistemas de IA, por exemplo, através da criação de equipas de desenvolvimento inclusivas e diversificadas e da promoção da participação das partes interessadas nesse processo;

(e) a avaliação e a prevenção de danos causados pelos sistemas de IA a pessoas vulneráveis ou a grupos de pessoas vulneráveis, nomeadamente no que diz respeito à acessibilidade para pessoas com deficiência, bem como à igualdade de género.

3. Os códigos de conduta podem ser desenvolvidos por provedores ou implantadores de sistemas de IA específicos, suas organizações representativas ou ambos, inclusive com o envolvimento de quaisquer partes interessadas e suas organizações representativas, como organizações da sociedade civil e academia. Os códigos de conduta podem abranger um ou mais sistemas de IA, dependendo da similaridade da finalidade pretendida dos diferentes sistemas.

4. O Gabinete de IA e os Estados-Membros devem ter em conta os interesses e as necessidades específicas das PME, incluindo as start-ups, ao incentivar e facilitar o desenvolvimento de códigos de conduta.

Artigo 96

Orientações da Comissão sobre a aplicação do presente regulamento

1. A Comissão elaborará orientações sobre a aplicação prática do presente regulamento e, em especial, sobre:

(a) a aplicação dos requisitos e obrigações referidos nos artigos 8.º a 15.º e no artigo 25.º;

b) as práticas proibidas referidas no artigo 5.º;

c) a aplicação prática das disposições relativas às modificações substanciais;

(d) a aplicação prática das obrigações de transparência estabelecidas no artigo 50.º;

(e) informações pormenorizadas sobre a relação entre o presente regulamento e a lista de atos legislativos de harmonização da União enumerados no anexo I, bem como outras disposições pertinentes do direito da União, nomeadamente no que diz respeito à coerência na sua aplicação;

(f) a aplicação da definição de sistema de IA estabelecida no artigo 3.º, ponto 1.

Ao publicar estas diretrizes, a Comissão prestará especial atenção às necessidades das PME, incluindo start-ups, autoridades públicas locais e setores mais suscetíveis de serem afetados por este regulamento.

As orientações referidas no primeiro parágrafo do presente número devem ter em devida conta o estado da arte geralmente reconhecido no domínio da IA, bem como as normas harmonizadas e as especificações comuns relevantes referidas nos artigos 40.º e 41.º, ou as normas harmonizadas ou as especificações técnicas estabelecidas nos termos da legislação de harmonização da União.

2. A pedido dos Estados-Membros ou do Gabinete de Inteligência Artificial, ou por sua própria iniciativa, a Comissão atualizará as orientações previamente adotadas, sempre que o considere necessário.

CAPÍTULO XI

DELEGAÇÃO DE PODERES E PROCEDIMENTO DO COMITÊ

Artigo 97

Exercício de delegação

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

2. O poder de adotar atos delegados referido no artigo 6.º(6), artigo 6.º(7), artigo 7.º(1) e (3), artigo 11.º(3), artigo 43.º(5) e (6), artigo 47.º(5), artigo 51.º(3), artigo 52.º(4) e artigo 53.º(5) e (6) será conferido à Comissão por um período de cinco anos a partir de 1 de agosto de 2024. A Comissão elaborará um relatório relativo à delegação de poderes o mais tardar nove meses antes do final do período de cinco anos. A delegação de poderes será 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 período.

3. A delegação de poderes referida no artigo 6.º, n.os 6 e 7, no artigo 7.º, n.os 1 e 3, no artigo 11.º, n.os 3, no artigo 43.º, n.os 5 e 6, no artigo 47.º, n.º 5, no artigo 51.º, n.º 3, no artigo 52.º, n.º 4, e no artigo 53.º, n.os 5 e 6, pode ser revogada a qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação dos poderes nela especificados. A decisão entrará em vigor no dia seguinte ao da sua publicação no Diário Oficial da União.Jornal Oficial da União Europeiaou em uma data posterior indicada nele. Não afetará a validade dos atos delegados já em vigor.

4. Antes de adotar um ato delegado, a Comissão consulta os peritos designados por cada Estado-Membro, em conformidade 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. Um ato delegado adotado nos termos do artigo 6.º, n.º 6 ou (7), do artigo 7.º, n.º 1 ou (3), do artigo 11.º, n.º 3, do artigo 43.º, n.º 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.º 5 ou (6), só entrará em vigor se nem o Parlamento Europeu nem o Conselho tiverem formulado objeções no prazo de três meses a contar da notificação desse ato ao Parlamento Europeu e ao Conselho ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não formularão objeções. O prazo será prorrogado por três meses por iniciativa do Parlamento Europeu ou do Conselho.

Artigo 98

Procedimento de comissão

1. A Comissão será assistida por um comité. Este comité será um comité na acepção do Regulamento (UE) n.qualquer182/2011.

2. Sempre que se faça referência ao presente número, aplica-se o artigo 5.º do Regulamento (UE). n.qualquer182/2011.

CAPÍTULO XII

SANÇÕES

Artigo 99

Sanções

1. Sem prejuízo das condições estabelecidas no presente regulamento, os Estados-Membros devem estabelecer o sistema de sanções e outras medidas de execução, tais como advertências ou medidas não pecuniárias, aplicáveis às infrações ao presente regulamento cometidas pelos operadores e devem tomar todas as medidas necessárias para garantir que são aplicadas de forma adequada e eficaz, tendo em conta as orientações emitidas pela Comissão nos termos do artigo 96.º. Essas sanções devem ser efetivas, proporcionais e dissuasivas. Eles levarão em consideração os interesses das PMEs, incluindo startups, bem como sua viabilidade econômica.

2. Os Estados-Membros devem comunicar à Comissão, sem demora e, o mais tardar, na data de aplicação, as regras relativas às sanções e outras medidas de execução referidas no n.º 1 e informá-la, sem demora, de qualquer alteração dessas regras.

3. O incumprimento da proibição de práticas de IA referida no artigo 5.º estará sujeito a coimas administrativas até 35 000 000 EUR ou, se o infrator for uma empresa, até 7 % do seu volume de negócios mundial total do exercício financeiro anterior, consoante o valor mais elevado.

4. O incumprimento de qualquer das seguintes disposições relativamente a operadores ou organismos notificados que não os referidos no artigo 5.º será sujeito a coimas administrativas até 15 000 000 EUR ou, se o infrator for uma empresa, até 3 % do seu volume de negócios mundial total do exercício financeiro anterior, consoante o valor mais elevado:

(a) as obrigações dos fornecedores nos termos do artigo 16.º;

(b) as obrigações dos representantes autorizados 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 mobilização nos termos do artigo 26.º;

(f) os requisitos e obrigações dos organismos notificados nos termos do artigo 31.º, do artigo 33.º(1), (3) e (4) ou do artigo 34.º;

(g) as obrigações de transparência dos prestadores e dos distribuidores, nos termos do artigo 50.º.

5. A apresentação de informações inexatas, incompletas ou enganosas aos organismos notificados ou às autoridades nacionais competentes em resposta a um pedido estará sujeita a multas administrativas até 7 500 000 EUR ou, se o infrator for uma empresa, até 1 % do volume de negócios mundial total do exercício financeiro anterior, consoante o valor mais elevado.

6. No caso das PME, incluindo as start-ups, cada uma das multas referidas neste artigo poderá ser na percentagem ou no montante referidos nos n.ºs 3, 4 e 5, consoante o que for menor.

7. Na decisão sobre a aplicação de uma coima administrativa e o seu montante em cada caso específico, serão tidas em conta todas as circunstâncias relevantes da situação em questão e, quando for caso disso, serão tidos em conta os seguintes aspetos:

(a) a natureza, a gravidade e a duração da infração e as suas consequências, tendo em conta a finalidade do sistema de IA e, se for caso disso, o número de pessoas afetadas e o nível de danos sofridos;

(b) se outras autoridades de fiscalização do mercado já impuseram coimas administrativas ao mesmo operador pela mesma infração;

(c) se outras autoridades já tiverem imposto coimas administrativas ao mesmo operador por infrações a outros atos legislativos nacionais ou da União, sempre que tais infrações decorram da mesma atividade ou omissão, constituindo uma infração relevante ao presente regulamento;

(d) a dimensão, o volume de negócios anual e a quota de mercado do operador que comete a infração;

(e) qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, tais como benefícios financeiros obtidos ou perdas evitadas, direta ou indiretamente, através da infração;

(f) o grau de cooperação com as autoridades nacionais competentes para remediar a infração e atenuar os seus potenciais efeitos adversos;

g) o grau de responsabilidade do operador, tendo em conta as medidas técnicas e organizacionais aplicadas pelo operador;

(h) a forma como as autoridades nacionais competentes tomaram conhecimento da infração, em especial se o operador notificou a infração e, em caso afirmativo, em que medida;

i) a intencionalidade ou negligência da infração;

j) as ações adotadas pelo operador para mitigar os danos sofridos pelas pessoas afetadas.

8. Cada Estado-Membro estabelecerá regras que determinem a medida em que as multas administrativas podem ser impostas às autoridades e organismos públicos estabelecidos nesse Estado-Membro.

9. Dependendo do sistema jurídico dos Estados-Membros, as regras relativas às multas administrativas podem ser aplicadas de modo que as multas sejam impostas pelos tribunais nacionais competentes ou outros organismos, conforme apropriado nesses Estados-Membros. A aplicação destas regras nestes Estados-Membros terá um efeito equivalente.

10. O exercício dos poderes previstos no presente artigo está sujeito a garantias processuais adequadas, em conformidade com o direito da União e o direito nacional, incluindo a proteção judicial efetiva e o devido processo legal.

11. Os Estados-Membros devem apresentar anualmente à Comissão um relatório sobre as multas administrativas impostas durante esse ano, em conformidade com o presente artigo, bem como sobre quaisquer litígios ou processos judiciais conexos.

Artigo 100

Multas administrativas impostas a instituições, organismos e agências da União Europeia

1. A Autoridade Europeia para a Proteção de Dados pode impor coimas administrativas às instituições, órgãos, gabinetes e agências da União abrangidos pelo âmbito de aplicação do presente regulamento. Ao decidir se deve impor uma multa administrativa e seu valor em cada caso específico, todas as circunstâncias relevantes da situação em questão devem ser levadas em consideração e deve-se levar em conta o seguinte:

(a) a natureza, a gravidade e a duração da infração e as suas consequências, tendo em conta a finalidade do sistema de IA em causa, bem como, se for caso disso, o número de pessoas afetadas e o nível de danos por elas sofridos;

(b) o grau de responsabilidade da instituição, órgão, serviço ou agência da União, tendo em conta as medidas técnicas e organizacionais aplicadas;

(c) as medidas tomadas pela instituição, órgão, serviço ou agência da União para atenuar os danos sofridos pelas pessoas em causa;

(d) o grau de cooperação com a Autoridade Europeia para a Proteção de Dados, a fim de remediar a violação e atenuar os seus potenciais efeitos adversos, incluindo o cumprimento de quaisquer medidas que a Autoridade Europeia para a Proteção de Dados tenha previamente ordenado contra a instituição, órgão, serviço ou agência da União em causa relativamente à mesma matéria;

(e) qualquer infração semelhante anterior cometida pela instituição, órgão, serviço ou agência da União;

(f) a forma como a Autoridade Europeia para a Proteção de Dados tomou conhecimento da violação, em especial se a instituição, órgão, organismo ou agência da União notificou a Autoridade Europeia para a Proteção de Dados da violação e, em caso afirmativo, em que medida;

(g) o orçamento anual da instituição, órgão, serviço ou agência da União.

2. O incumprimento da proibição de práticas de IA referida no artigo 5.º é punível com coimas administrativas até 1 500 000 EUR.

3. O incumprimento pelo sistema de IA de qualquer dos requisitos ou obrigações previstos no presente regulamento, para além dos previstos no artigo 5.º, é passível de coimas administrativas até 750 000 EUR.

4. Antes de tomar qualquer decisão nos termos do presente artigo, a Autoridade Europeia para a Proteção de Dados dará à instituição, órgão, organismo ou agência da União sujeito ao procedimento conduzido pela Autoridade Europeia para a Proteção de Dados a oportunidade de ser ouvida relativamente à potencial violação. O Supervisor Europeu de Proteção de Dados baseará suas decisões exclusivamente nos elementos e circunstâncias sobre os quais as partes afetadas tiveram a oportunidade de expressar suas opiniões. Os reclamantes, se houver, serão envolvidos de perto nos procedimentos.

5. O direito de defesa das partes será plenamente garantido durante todo o processo. Eles terão o direito de acessar o arquivo da Autoridade Europeia para a Proteção de Dados, sem prejuízo do interesse legítimo de indivíduos e empresas na proteção de seus dados pessoais ou segredos comerciais.

6. A receita proveniente da aplicação de multas nos termos deste artigo contribuirá para o orçamento geral da União. As multas não afetarão o funcionamento efetivo da instituição, órgão, repartição ou agência da União sancionada.

7. A Autoridade Europeia para a Proteção de Dados deve apresentar anualmente à Comissão um relatório sobre quaisquer coimas administrativas impostas nos termos do presente artigo e sobre quaisquer litígios ou procedimentos legais por si iniciados.

Artigo 101

Multas para provedores de modelos de IA de uso geral

1. A Comissão pode impor multas aos fornecedores de modelos de IA para fins gerais não superiores a 3 % do seu volume de negócios global anual total do exercício financeiro anterior ou 15 000 000 EUR, consoante o valor mais elevado, sempre que a Comissão considere que, intencionalmente ou por negligência:

a) violou as disposições pertinentes do presente Regulamento;

(b) não responderam a um pedido de informações ou documentos nos termos do artigo 91.º, ou forneceram informações inexactas, incompletas ou enganosas;

c) não cumpriu medida solicitada nos termos do artigo 93.º;

(d) não forneceu à Comissão acesso ao modelo de IA para fins gerais ou ao modelo de IA para fins gerais com risco sistémico para uma avaliação a ser realizada nos termos do artigo 92.º.

Na fixação do montante da multa ou da sanção pecuniária compulsória, serão tidas em consideração a natureza, a gravidade e a duração da infração, tendo em conta os princípios da proporcionalidade e da adequação. A Comissão também terá em conta os compromissos assumidos nos termos do artigo 93.º, n.º 3, e os códigos de práticas relevantes previstos no artigo 56.º.

2. Antes de adotar uma decisão nos termos do parágrafo 1, a Comissão deve comunicar suas conclusões preliminares ao fornecedor do modelo de IA de uso geral ou do modelo de IA e dar-lhe a oportunidade de ser ouvido.

3. As multas impostas nos termos do presente artigo serão eficazes, proporcionais e dissuasivas.

4. As informações sobre multas impostas nos termos deste artigo também serão comunicadas ao Conselho da IA, conforme apropriado.

5. O Tribunal de Justiça da União Europeia tem plena jurisdição para rever as decisões que impõem uma multa adotadas pela Comissão nos termos do presente artigo. Poderá cancelar, reduzir ou aumentar o valor da multa aplicada.

6. A Comissão adota atos de execução que contenham disposições detalhadas e salvaguardas processuais para os procedimentos com vista à possível adoção de decisões nos termos do n.º 1 do presente artigo. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 98.º, n.º 2.

CAPÍTULO XIII

DISPOSIÇÕES FINAIS

Artigo 102

Emenda ao Regulamento (CE) n.ºqualquer300/2008

No artigo 4(3) do Regulamento (CE) n.ºqualquer300/2008, é aditado o seguinte parágrafo:

"Ao adotar medidas detalhadas relativas às especificações técnicas e aos procedimentos de aprovação e utilização de equipamentos de segurança em relação aos sistemas de inteligência artificial, na aceção do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho (*), devem ser tidos em conta os requisitos estabelecidos no Capítulo III, Secção 2, do referido regulamento.

(*) Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial e altera os Regulamentos (CE) n.º 1689/2008 e (CE) n.º 1689/2009.qualquer 300/2008, (UE) n.ºqualquer167/2013, (UE) n.ºqualquer168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento sobre Inteligência Artificial) (JO L 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artigo 103

Emenda ao Regulamento (UE) n.ºqualquer167/2013

No artigo 17(5) do Regulamento (UE) n.ºqualquer167/2013, é aditado o seguinte parágrafo:

«Ao adotar atos delegados nos termos do primeiro parágrafo relativos a sistemas de inteligência artificial que sejam componentes de segurança na aceção do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho (*), devem ser tidos em conta os requisitos estabelecidos no Capítulo III, Secção 2, desse regulamento.

(*) Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial e altera os Regulamentos (CE) n.º 1689/2008 e (CE) n.º 1689/2009.qualquer 300/2008, (UE) n.ºqualquer167/2013, (UE) n.ºqualquer168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento sobre Inteligência Artificial) (JO L 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artigo 104

Emenda ao Regulamento (UE) n.º$_{qualquer}$168/2013

No artigo 22(5) do Regulamento (UE) n.º$_{qualquer}$168/2013, é aditado o seguinte parágrafo:

«Ao adotar atos delegados nos termos do primeiro parágrafo relativos a sistemas de inteligência artificial que sejam componentes de segurança na aceção do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho (*), devem ser tidos em conta os requisitos estabelecidos no Capítulo III, Secção 2, desse regulamento.

(*) Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial e altera os Regulamentos (CE) n.º 1689/2008 e (CE) n.º 1689/2009.$_{qualquer}$ 300/2008, (UE) n.º$_{qualquer}$167/2013, (UE) n.º$_{qualquer}$168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento sobre Inteligência Artificial) (JO L 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artigo 105

Emenda à Diretiva 2014/90/UE

No artigo 8.º da Diretiva 2014/90/UE, é aditado o seguinte parágrafo:

«5. No caso de sistemas de inteligência artificial que sejam componentes de segurança na acepção do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho (*), a Comissão deve ter em conta os requisitos estabelecidos no Capítulo III, Secção 2, desse regulamento 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.

(*) Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial e altera os Regulamentos (CE) n.º 1689/2008 e (CE) n.º 1689/2009.$_{qualquer}$ 300/2008, (UE) n.º$_{qualquer}$167/2013, (UE) n.º$_{qualquer}$168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento sobre Inteligência Artificial) (JO L 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artigo 106

Emenda à Diretiva (UE) 2016/797

No artigo 5.º da Diretiva (UE) 2016/797, é aditado o seguinte parágrafo:

«12. Ao adoptar actos delegados nos termos do n.º 1 e actos de execução nos termos do n.º 11 relativos Para os sistemas de inteligência artificial que sejam componentes de segurança na aceção do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho (*), devem ser tidos em conta os requisitos estabelecidos no Capítulo III, Secção 2, desse regulamento.

(*) Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial e altera os Regulamentos (CE) n.º 1689/2008 e (CE) n.º 1689/2009.$_{qualquer}$ 300/2008, (UE) n.º$_{qualquer}$167/2013, (UE) n.º$_{qualquer}$168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento sobre Inteligência Artificial) (JO L 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artigo 107

Emenda ao Regulamento (UE) 2018/858

No artigo 5.º do Regulamento (UE) 2018/858, é aditado o seguinte parágrafo:

«4. Ao adotar atos delegados nos termos do parágrafo 3 relativos a sistemas de inteligência artificial que sejam componentes de segurança na acepção 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) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial e altera os Regulamentos (CE) n.º 1689/2008 e (CE) n.º 1689/2009.qualquer 300/2008, (UE) n.ºqualquer167/2013, (UE) n.ºqualquer168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento sobre Inteligência Artificial) (JO L 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artigo 108

Emenda ao Regulamento (UE) 2018/1139

O Regulamento (UE) 2018/1139 é alterado do seguinte modo:

1) No artigo 17, é acrescentado o seguinte parágrafo:

«3. Sem prejuízo do disposto no n.º 2, ao adoptar actos de execução nos termos do n.º 1 relativos a Para os sistemas de inteligência artificial que sejam componentes de segurança na aceção do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho (*), devem ser tidos em conta os requisitos estabelecidos no Capítulo III, Secção 2, desse regulamento.

(*) Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial e altera os Regulamentos (CE) n.º 1689/2008 e (CE) n.º 1689/2009. qualquer300/2008, (UE) n.ºqualquer167/2013, (UE) n.ºqualquer168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento sobre Inteligência Artificial) (JO L 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

2) No artigo 19, é acrescentado o seguinte parágrafo:

«4. Ao adoptar actos delegados nos termos dos n.ºs 1 e 2 relativos aos sistemas de inteligência artificial que são componentes de segurança na acepção do Regulamento (UE) 2024/1689, devem ser tidos em conta os requisitos estabelecidos no Capítulo III, Secção 2, do referido regulamento.».

3) No artigo 43, é acrescentado o seguinte parágrafo:

«4. Ao adotar atos de execução nos termos do n.º 1 relativos aos sistemas de inteligência artificial que são componentes de segurança na acepção do Regulamento (UE) 2024/1689, devem ser tidos em conta os requisitos estabelecidos no Capítulo III, Secção 2, do referido regulamento.».

4) No artigo 47, é acrescentado o seguinte parágrafo:

«3. Ao adoptar actos delegados nos termos dos n.ºs 1 e 2 relativos aos sistemas de inteligência artificial que são componentes de segurança na acepção do Regulamento (UE) 2024/1689, devem ser tidos em conta os requisitos estabelecidos no Capítulo III, Secção 2, do referido regulamento.».

5) No artigo 57, é acrescentado o seguinte parágrafo:

"Ao adotar os atos de execução relativos aos sistemas de inteligência artificial que são componentes de segurança na aceção do Regulamento (UE) 2024/1689, devem ser tidos em conta os requisitos estabelecidos no Capítulo III, Secção 2, do referido regulamento."

6) No artigo 58, é acrescentado o seguinte parágrafo:

«3. Ao adoptar actos delegados nos termos dos n.ºs 1 e 2 relativos aos sistemas de inteligência artificial que são componentes de segurança na acepção do Regulamento (UE) 2024/1689, devem ser tidos em conta os requisitos estabelecidos no Capítulo III, Secção 2, do referido regulamento.».

Artigo 109

Emenda ao Regulamento (UE) 2019/2144

No artigo 11.º do Regulamento (UE) 2019/2144, é aditado o seguinte parágrafo:

«3. Ao adotar atos de execução nos termos do n.º 2 relativos aos sistemas de inteligência artificial que são componentes de segurança na acepção do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho (*), devem ser tidos em conta os requisitos estabelecidos no Capítulo III, Secção 2, do referido regulamento.

(*) Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas sobre inteligência artificial e altera os Regulamentos (CE) n.º 1689/2008 e (CE) n.º 1689/2009.qualquer 300/2008, (UE) n.ºqualquer167/2013, (UE) n.ºqualquer168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento sobre Inteligência Artificial) (JO L 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artigo 110

Emenda à Diretiva (UE) 2020/1828

No Anexo I da Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho (58) é acrescentado o seguinte ponto:

"68) Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 1689 que estabelece regras medidas harmonizadas no domínio da inteligência artificial e que altera o Regulamento (CE) n.ºqualquer300/2008, (UE) n.ºqualquer167/2013, (UE) n.ºqualquer168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento sobre Inteligência Artificial) (JO L 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).».

Artigo 111

Sistemas de IA já introduzidos no mercado ou colocados em serviço e modelos de IA de uso geral já introduzido no mercado

1. Sem prejuízo da aplicação do artigo 5.º, nos termos do artigo 113.º, n.º 3, alínea a), os sistemas de IA que sejam componentes de sistemas de computação em larga escala estabelecidos nos termos dos atos legislativos enumerados no anexo X que sejam colocados no mercado ou em serviço antes de 2 de agosto de 2027 devem cumprir o presente regulamento até 31 de dezembro de 2030.

Os requisitos estabelecidos no presente regulamento devem ser tidos em conta na avaliação de cada sistema informático de grande escala estabelecido nos termos dos atos jurídicos enumerados no anexo X, efetuada em conformidade com esses atos jurídicos e sempre que esses atos jurídicos tenham sido substituídos ou alterados.

2. Sem prejuízo da aplicação do artigo 5.º nos termos do artigo 113.º, n.º 3, alínea a), o presente regulamento aplica-se aos operadores de sistemas de IA de alto risco, que não os referidos no n.º 1 do presente artigo, que tenham sido colocados no mercado ou em serviço antes de 2 de agosto de 2026, apenas se, a partir dessa data, esses sistemas sofrerem alterações significativas na sua conceção. Em qualquer caso, os prestadores e os responsáveis pela implementação de sistemas de IA de alto risco destinados à utilização por autoridades públicas devem tomar as medidas necessárias para cumprir os requisitos e obrigações do presente regulamento até 2 de agosto de 2030.

3. Os fornecedores de modelos de IA de uso geral que tenham sido colocados no mercado antes de 2 de agosto de 2025 devem tomar as medidas necessárias para cumprir as obrigações estabelecidas no presente regulamento até 2 de agosto de 2027.

(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).

Artigo 112

Avaliação e revisão

1. A Comissão avalia a necessidade de alterar a lista do anexo III e a lista de práticas de IA proibidas previstas no artigo 5.º uma vez por ano, a partir da entrada em vigor do presente regulamento até ao final do período de delegação de poderes previsto no artigo 97.º. A Comissão apresenta as conclusões dessa avaliação ao Parlamento Europeu e ao Conselho.

2. Até 2 de agosto de 2028 e, posteriormente, de quatro em quatro anos, a Comissão deve avaliar os seguintes pontos e apresentar um relatório ao Parlamento Europeu e ao Conselho:

(a) a necessidade de expandir as áreas enumeradas no Anexo III ou de acrescentar novas áreas;

(b) a necessidade de alterar a lista de sistemas de IA que exigem medidas de transparência adicionais, nos termos do artigo 50.º;

c) a necessidade de melhorar a eficácia do sistema de supervisão e governação.

3. Até 2 de agosto de 2029 e, posteriormente, de quatro em quatro anos, a Comissão deve apresentar ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e revisão do presente regulamento. O relatório deve incluir uma avaliação da estrutura de execução e da possível necessidade de uma agência da União para resolver as deficiências identificadas. Com base nas suas conclusões, este relatório será acompanhado, quando adequado, de uma proposta de alteração do presente regulamento. Os relatórios serão tornados públicos.

4. Nos relatórios referidos no n.º 2, será dada especial atenção ao seguinte:

(a) o estado dos recursos financeiros, técnicos e humanos das autoridades nacionais competentes para desempenhar eficazmente as tarefas que lhes são atribuídas pelo presente regulamento;

(b) o estado das sanções, em especial as multas administrativas referidas no artigo 99.º, n.º 1, aplicadas pelos Estados-Membros às infrações às disposições do presente regulamento;

(c) as normas harmonizadas adoptadas e as especificações comuns desenvolvidas em apoio ao presente regulamento;

(d) o número de empresas que entraram no mercado após o início da aplicação do presente regulamento, incluindo o número de PME.

5. Até 2 de agosto de 2028, a Comissão avaliará o funcionamento do Gabinete de IA, se lhe foram atribuídos poderes e competências suficientes para desempenhar as suas tarefas e se seria relevante e necessário para a aplicação e execução adequadas do presente Regulamento reforçar o Gabinete de IA e os seus poderes de execução, bem como aumentar os seus recursos. A Comissão apresentará um relatório sobre a sua avaliação ao Parlamento Europeu e ao Conselho.

6. Até 2 de agosto de 2028 e a cada quatro anos a partir de então, a Comissão apresentará um relatório sobre a revisão do progresso no desenvolvimento de documentos de normalização sobre o desenvolvimento energeticamente eficiente de modelos de IA de uso geral e avaliará a necessidade de medidas ou ações adicionais, incluindo medidas ou ações vinculativas. Este relatório será submetido ao Parlamento Europeu e ao Conselho e tornado público.

7. Até 2 de agosto de 2028 e a cada três anos a partir de então, a Comissão avaliará o impacto e a eficácia dos códigos de conduta voluntários na promoção da aplicação dos requisitos estabelecidos no Capítulo III, Seção 2, aos sistemas de IA que não sejam de alto risco e, quando apropriado, de outros requisitos adicionais aplicáveis aos sistemas de IA que não sejam de alto risco, como requisitos relacionados à sustentabilidade ambiental.

8. Para efeitos dos n.os 1 a 7, o Conselho de Administração da IA, os Estados-Membros e as autoridades nacionais competentes devem fornecer informações à Comissão, mediante pedido e sem demora injustificada.

9. Ao realizar as avaliações e revisões referidas nos n.ºs 1 a 7, a Comissão terá em conta as posições e conclusões do Conselho de Administração, do Parlamento Europeu, do Conselho e de outros organismos ou fontes relevantes.

10. A Comissão deve, sempre que necessário, apresentar propostas adequadas para alterar o presente regulamento, tendo em conta, nomeadamente, os desenvolvimentos tecnológicos e o impacto dos sistemas de IA na saúde, na segurança e nos direitos fundamentais, e à luz dos desenvolvimentos na sociedade da informação.

11. Para orientar as avaliações e revisões referidas nos parágrafos 1 a 7 deste artigo, o Gabinete de IA será responsável por desenvolver uma metodologia objetiva e participativa para a avaliação dos níveis de risco com base nos critérios estabelecidos nos artigos relevantes e a inclusão de novos sistemas em:

(a) a lista estabelecida no Anexo III, incluindo a extensão de áreas existentes ou a inclusão de novas áreas nesse Anexo;

b) a lista de práticas proibidas estabelecida no artigo 5.º, e

(c) a lista de sistemas de IA que exigem medidas de transparência adicionais nos termos do artigo 50.º.

12. As alterações ao presente regulamento nos termos do n.º 10, ou dos atos delegados ou de execução relevantes, que afetem os atos legislativos de harmonização setoriais da União enumerados na secção B do anexo I devem ter em conta as especificidades regulamentares de cada setor e os mecanismos de governação, avaliação da conformidade e execução em vigor, bem como as autoridades neles estabelecidas.

13. Até 2 de agosto de 2031, a Comissão deve avaliar a aplicação do presente regulamento e apresentar um relatório 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 suas conclusões, esse relatório será acompanhado, se for caso disso, de uma proposta de alteração do presente regulamento no que diz respeito à estrutura de execução e à necessidade de uma agência da União para corrigir as deficiências identificadas.

Artigo 113

Entrada em vigor e aplicação

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação noJornal Oficial da União Europeia.

Será aplicável a partir de 2 de agosto de 2026. No entanto:

(a) Os Capítulos I e II serão aplicáveis a partir de 2 de fevereiro de 2025;

(b) O Capítulo III, Seção 4, Capítulo V, Capítulo VII, Capítulo XII e Artigo 78 serão aplicáveis a partir de 2 de agosto de 2025, com exceção do Artigo 101;

(c) O artigo 6.º(1) e as obrigações correspondentes do presente regulamento são aplicáveis a partir de 2 de agosto de 2027.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, 13 de junho de 2024.

Pelo Parlamento Europeu	Pelo Conselho
O Presidente	O Presidente
R. METSOLA	Senhor MICHEL

ANEXO I

Lista de atos legislativos de harmonização da União

Secção A — Lista de actos legislativos de harmonização da União com base no novo quadro legislativo

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

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 motos 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 das legislações dos Estados-Membros respeitantes aos ascensores e aos 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 das legislações dos Estados-Membros respeitantes aos 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 das legislações dos Estados-Membros respeitantes à comercialização de equipamentos de rádio 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 das legislações dos Estados-Membros respeitantes à comercialização de equipamentos sob pressão (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 1018/2009 e o Regulamento (CE) n.º 1018/2009.qualquer178/2002 e Regulamento (CE) n.º qualquer1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho (JO L 117 de 5.5.2017, pág. 1)

12. Regulamento (UE) 2017/746 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos de diagnósticoem vitroe 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 outros actos legislativos de harmonização da União

13. Regulamento (CE) n.ºqualquer300/2008 do Parlamento Europeu e do Conselho, de 11 de março de 2008, relativa a regras comuns para a segurança da aviação civil e que revoga o Regulamento (CE) n.º 300/2008.qualquer2320/2002 (JO L 97 de 9.4.2008, p. 72)

14. Regulamento (UE) n.ºqualquer168/2013 do Parlamento Europeu e do Conselho, de 15 de janeiro de 2013, relativo à homologação de veículos de duas ou três rodas e de quadriciclos e à fiscalização do mercado desses veículos (JO L 60 de 2.3.2013, p. 52)

15. Regulamento (UE) n.ºqualquer167/2013 do Parlamento Europeu e do Conselho, de 5 de fevereiro de 2013, relativo à homologação de veículos agrícolas ou florestais e à fiscalização do mercado desses veículos (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 de veículos a motor e seus reboques, e de sistemas, componentes e unidades técnicas destinados a esses veículos, que altera os Regulamentos (CE) n.º 189/2018 e (CE) n.º 189/201 ... e (CE) n.º 189/2018 ... n.qualquer715/2007 e (CE) n.º.qualquer595/2009 e que 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 para veículos a motor e seus reboques, e sistemas, componentes e unidades técnicas separadas destinados a esses veículos, no que diz respeito à sua segurança geral e à proteção dos ocupantes dos veículos e dos utilizadores vulneráveis da estrada, que altera o Regulamento (UE) 2018/858 do Parlamento Europeu e do Conselho e revoga o Regulamento (CE) n.º 1018/2009 do Parlamento Europeu e do Conselho. n.qualquer78/2009, (CE) n.ºqualquer79/2009 e (CE) n.º.qualquer661/2009 do Parlamento Europeu e do Conselho e Regulamentos (CE) n.qualquer631/2009, (UE) n.ºqualquer406/2010, (UE) n.ºqualquer672/2010, (UE) n.ºqualquer1003/2010, (UE) n.ºqualquer1005/2010, (UE) n.ºqualquer 1008/2010, (UE) n.ºqualquer1009/2010, (UE) n.ºqualquer19/2011, (UE) n.qualquer109/2011, (UE) n.ºqualquer458/2011, (UE) n.ºqualquer65/2012, (UE) n.º qualquer130/2012, (UE) n.ºqualquer347/2012, (UE) n.ºqualquer351/2012, (UE) n.ºqualquer1230/2012 e (UE) 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 e que altera os Regulamentos (CE) n.º 1139/2018 e (CE) n.º 1139/2018.qualquer2111/2005, (CE) n.º.qualquer1008/2008, (UE) n.ºqualquer 996/2010 e (UE) n.qualquer376/2014 e Diretivas 2014/30/UE e 2014/53/UE do Parlamento Europeu e do Conselho e Regulamentos (CE) n.ºqualquer552/2004 e (CE) n.º.qualquer216/2008 do Parlamento Europeu e do Conselho e Regulamento (CEE) n.ºqualquer3922/91 do Conselho (JO L 212 de 22.8.2018, p. 1), na medida em que afeta a conceção, a produção e a colocação no mercado das aeronaves referidas no artigo 2.º, n.º 1, alíneas a) e b), no que diz respeito às aeronaves não tripuladas e aos seus motores, hélices, componentes e equipamentos para o seu controlo remoto

ANEXO II

Lista das infracções referidas no artigo 5.º, n.º 1, primeiro parágrafo, alínea h), ponto iii)

Infracções referidas no artigo 5.º, n.º 1, primeiro parágrafo, alínea h), subalínea iii):

— terrorismo,

— tráfico de pessoas,

— exploração sexual de menores e pornografia infantil,

— tráfico ilícito de estupefacientes ou de substâncias psicotrópicas,

— tráfico ilícito de armas, munições e explosivos,

— homicídio culposo voluntário, agressão com lesão grave,

— tráfico ilícito de órgãos ou tecidos humanos,

— tráfico ilícito de materiais nucleares ou radioativos,

— sequestro, detenção ilegal ou tomada de reféns,

— crimes que sejam da competência do Tribunal Penal Internacional,

— sequestro de aeronaves ou navios,

— estupro,

— crimes contra o meio ambiente,

— assalto organizado ou à mão armada,

— sabotagem,

— participação em organização criminosa envolvida em um ou mais dos crimes listados nesta lista.

ANEXO III

Sistemas de IA de alto risco referidos no artigo 6.º(2)

Os sistemas de IA de alto risco, na aceção do artigo 6.º(2), são sistemas de IA que se enquadram em qualquer uma das seguintes áreas:

1. Dados biométricos, na medida em que a sua utilização seja permitida pela legislação aplicável da União ou nacional:

   a) Sistemas de identificação biométrica remota

      Estão excluídos os sistemas de IA destinados a serem usados para fins de verificação biométrica, cujo único propósito é confirmar que uma pessoa física específica é quem ela afirma ser.

   b) Sistemas de IA destinados a serem utilizados para categorização biométrica com base em atributos ou características sensíveis ou protegidas com base na inferência de tais atributos ou características

   c) Sistemas de IA destinados a serem usados para reconhecimento de emoções

2. Infraestruturas críticas: sistemas de IA destinados a serem utilizados como componentes de segurança na gestão e operação de infraestruturas digitais críticas, tráfego rodoviário ou fornecimento de água, gás, aquecimento ou eletricidade

3. Educação e formação profissional:

   a) Sistemas de IA destinados a serem utilizados para determinar o acesso ou a admissão de pessoas singulares a estabelecimentos de ensino e de formação profissional de todos os níveis ou para distribuir pessoas singulares entre esses estabelecimentos

   b) Sistemas de IA destinados a serem utilizados para avaliar resultados de aprendizagem, incluindo quando tais resultados são utilizados para orientar o processo de aprendizagem de pessoas singulares em estabelecimentos de ensino e de formação profissional a todos os níveis

   c) Sistemas de IA destinados a serem utilizados para avaliar o nível adequado de educação que uma pessoa receberá ou poderá aceder, no contexto de centros de educação e formação profissional ou dentro destes, a todos os níveis

   d) Sistemas de IA destinados a serem utilizados para monitorizar e detetar comportamentos proibidos por parte de estudantes durante exames no contexto de instituições de ensino e formação profissional ou dentro destas, a todos os níveis

4. Emprego, gestão de funcionários e acesso ao trabalho autônomo:

   a) Sistemas de IA destinados a serem utilizados no recrutamento ou seleção de pessoas singulares, em especial para a publicação de anúncios de emprego específicos, a análise e filtragem de candidaturas e a avaliação de candidatos

   b) Sistemas de IA destinados a serem utilizados para tomar decisões que afetem as condições de relações de trabalho ou a promoção ou rescisão de relações contratuais de trabalho, para a atribuição de tarefas com base no comportamento individual ou em traços ou características pessoais ou para monitorar e avaliar o desempenho e o comportamento de indivíduos no âmbito de tais relações.

5. Acesso e usufruto de serviços privados essenciais e serviços e benefícios públicos essenciais:

   (a) Sistemas de IA destinados a serem utilizados por ou em nome de autoridades públicas para avaliar a elegibilidade de pessoas singulares para serviços e benefícios essenciais de assistência pública, incluindo serviços de saúde, e para conceder, reduzir, retirar ou reclamar o seu reembolso;

   b) Sistemas de IA destinados a serem utilizados para avaliar a solvabilidade de pessoas singulares ou estabelecer a sua notação de crédito, exceto os sistemas de IA utilizados para efeitos de deteção de fraudes financeiras.

   c) Sistemas de IA destinados a serem utilizados para avaliação e fixação de preços de risco em relação a pessoas singulares no caso de seguros de vida e de saúde

(d) Sistemas de IA destinados a serem utilizados para a avaliação e classificação de chamadas de emergência efetuadas por pessoas singulares ou para o envio ou priorização do envio de socorristas em situações de emergência, por exemplo, polícia, bombeiros e serviços médicos, e em sistemas de triagem de pacientes no contexto de cuidados de saúde de emergência

6. Garantir o cumprimento da lei, na medida em que a sua utilização seja permitida pela legislação aplicável da União ou nacional:

(a) Sistemas de IA destinados a serem utilizados por ou em nome de autoridades responsáveis pela aplicação da lei ou por instituições, organismos, gabinetes e agências da União em apoio ou em nome de autoridades responsáveis pela aplicação da lei para avaliar o risco de uma pessoa singular se tornar vítima de infrações penais

(b) Sistemas de IA destinados a serem utilizados por ou em nome de autoridades responsáveis pela aplicação da lei ou por instituições, organismos, gabinetes e agências da União em apoio às autoridades responsáveis pela aplicação da lei, como polígrafos ou ferramentas semelhantes

(c) Sistemas de IA destinados a serem utilizados por ou em nome de autoridades responsáveis pela aplicação da lei ou por instituições, organismos, gabinetes e agências da União em apoio às autoridades responsáveis pela aplicação da lei para avaliar a fiabilidade das provas durante a investigação ou a acusação de infrações penais

(d) Sistemas de IA destinados a serem utilizados por ou em nome de autoridades responsáveis pela aplicação da lei ou por instituições, organismos, gabinetes e agências da União que apoiem as autoridades responsáveis pela aplicação da lei para avaliar o risco de uma pessoa singular cometer uma infração penal ou reincidir, tendo em conta não só a definição de perfis de pessoas singulares referida no ponto (4) do artigo 3.º da Diretiva (UE) 2016/680, ou para avaliar traços e características de personalidade ou comportamento criminoso passado de pessoas singulares ou coletivas;

(e) Sistemas de IA destinados a serem utilizados por ou em nome de autoridades responsáveis pela aplicação da lei ou por instituições, organismos, serviços e agências da União em apoio às autoridades responsáveis pela aplicação da lei para a definição de perfis de pessoas singulares, tal como referido no ponto (4) do artigo 3.º da Diretiva (UE) 2016/680, durante a deteção, investigação ou repressão de infrações penais

7. Gestão da migração, do asilo e do controlo de fronteiras, na medida em que a sua utilização seja permitida pela legislação aplicável da União ou nacional:

(a) Sistemas de IA destinados a serem utilizados pelas autoridades públicas competentes ou em seu nome, ou pelas instituições, organismos, gabinetes e agências da União, tais como polígrafos ou instrumentos semelhantes

(b) Sistemas de IA destinados a serem utilizados por ou em nome de autoridades públicas competentes ou por instituições, organismos, gabinetes e agências da União para avaliar um risco, como um risco para a segurança, a saúde ou a migração irregular, colocado por uma pessoa singular que pretenda entrar ou tenha entrado no território de um Estado-Membro

(c) Sistemas de IA destinados a serem utilizados por ou em nome de autoridades públicas competentes ou por instituições, organismos, gabinetes e agências da União para auxiliar as autoridades públicas competentes na análise de pedidos de asilo, vistos ou autorizações de residência e pedidos conexos, com vista a determinar se as pessoas singulares requerentes preenchem os requisitos para que o seu pedido seja deferido, incluindo a avaliação conexa da fiabilidade das provas;

(d) Sistemas de IA destinados a serem utilizados por ou em nome de autoridades públicas competentes ou por instituições, organismos, gabinetes e agências da União no contexto da gestão da migração, do asilo ou do controlo de 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 destinados a serem utilizados por ou em nome de uma autoridade judicial para auxiliar uma autoridade judicial na investigação e interpretação de factos e da lei, bem como para garantir o cumprimento da lei relativamente a um conjunto específico de factos, ou para serem utilizados de forma semelhante na resolução alternativa de litígios;

b) Sistemas de IA destinados a serem utilizados para influenciar o resultado de uma eleição ou referendo ou o comportamento eleitoral de pessoas singulares que exerçam o seu direito de voto em eleições ou referendos. Estão excluídos os sistemas de IA cujos resultados não são diretamente expostos a pessoas físicas, como ferramentas usadas para organizar, otimizar ou estruturar campanhas políticas de um ponto de vista administrativo ou logístico.

ANEXO IV

Documentação técnica referida no artigo 11.º, n.º 1

A documentação técnica referida no artigo 11.º, n.º 1, deve incluir, pelo menos, as seguintes informações, aplicáveis ao sistema de IA relevante:

1. Uma visão geral do sistema de IA, incluindo:

   a) sua finalidade, o nome do fornecedor e a versão do sistema de modo a refletir sua relação com versões anteriores;

   b) a maneira como o sistema de IA interage ou pode ser usado para interagir comferragensqualquersoftware,também com outros sistemas de IA, que não fazem parte do próprio sistema de IA, quando aplicável;

   c) as versões dePrograsqualquerfirmwarerelevantes e quaisquer requisitos relacionados a atualizações de versão;

   (d) uma descrição de todas as formas pelas quais o sistema de IA é introduzido no mercado ou colocado em serviço, como pacotes de software integrados no sistema de IA;ferragens,downloads ou API;

   e) a descrição doferragensno qual o sistema de IA deve ser executado;

   f) no caso em que o sistema de IA seja um componente de um produto, fotografias ou ilustrações das características externas, marcação e configuração interna do referido produto;

   g) uma descrição básica da interface do usuário fornecida ao implantador;

   h) instruções de uso para o implantador e uma descrição básica da interface do usuário fornecida ao implantador, quando aplicável.

2. Uma descrição detalhada dos elementos do sistema de IA e seu processo de desenvolvimento, incluindo:

   (a) os métodos e medidas adotados para o desenvolvimento do sistema de IA, incluindo, quando aplicável, a utilização de sistemas ou ferramentas pré-treinados fornecidos por terceiros e a forma como foram utilizados, integrados ou modificados pelo fornecedor;

   b) as especificações de projeto do sistema, nomeadamente a lógica geral do sistema de IA e algoritmos; principais decisões de projeto, incluindo a lógica e as suposições feitas, inclusive com relação às pessoas ou grupos de pessoas em relação às quais o sistema se destina a ser usado; principais decisões de classificação; o que o sistema foi projetado para otimizar e a relevância dos vários parâmetros; a descrição dos resultados esperados do sistema e a qualidade desses resultados; decisões tomadas sobre quaisquer possíveis concessões no que diz respeito às soluções técnicas adotadas para cumprir os requisitos estabelecidos no Capítulo III, Seção 2;

   c) a arquitetura do sistema, com uma explicação de como os componentes do sistema funcionam juntos.Programaseles são usados ou enriquecem uns aos outros e a maneira como são integrados no processamento geral; os recursos computacionais utilizados para desenvolver, treinar, testar e validar o sistema de IA;

   (d) quando aplicável, requisitos de dados, sob a forma de fichas técnicas que descrevam as metodologias e técnicas de formação, bem como os conjuntos de dados de formação utilizados, incluindo uma descrição geral desses conjuntos de dados e informações sobre a sua origem, âmbito e principais características; a forma como os dados foram obtidos e selecionados; procedimentos de rotulagem (por exemplo, para aprendizagem supervisionada) e metodologias de limpeza de dados (por exemplo, detecção de anomalias);

   (e) uma avaliação das medidas de supervisão humana necessárias, em conformidade com o artigo 14.º, incluindo uma avaliação das medidas técnicas necessárias para facilitar a interpretação dos resultados dos sistemas de IA pelos responsáveis pela sua implementação, em conformidade com o artigo 13.º, n.º 3, alínea d);

   (f) quando aplicável, uma descrição detalhada das alterações pré-determinadas ao sistema de IA e ao seu funcionamento, juntamente com todas as informações relevantes relativas às soluções técnicas adotadas com o objetivo de garantir a conformidade contínua do sistema de IA com os requisitos relevantes estabelecidos no Capítulo III, Secção 2;

   g) os procedimentos de validação e teste utilizados, incluindo informações sobre os dados de validação e teste utilizados e suas principais características; os parâmetros utilizados para medir a precisão, a robustez e a conformidade com outros requisitos relevantes estabelecidos no Capítulo III, Seção 2, bem como os efeitos potencialmente discriminatórios; os arquivos de registro de testes e todos os relatórios de testes datados e assinados pelas pessoas responsáveis, também no que diz respeito às alterações pré-determinadas referidas na alínea f);

h) as medidas de segurança cibernética adotadas.

3. Informações detalhadas sobre o monitoramento, a operação e o controle do sistema de IA, em particular no que diz respeito às suas capacidades e limitações operacionais, incluindo os níveis de precisão para as pessoas ou grupos de pessoas específicos em relação aos quais o sistema se destina a ser usado e o nível geral de precisão esperado em relação à sua finalidade pretendida; os resultados não intencionais previsíveis e as fontes de risco para a saúde e a segurança, os direitos fundamentais e a discriminação, tendo em conta a finalidade pretendida do sistema de IA; as medidas de supervisão humana necessárias, em conformidade com o artigo 14.º, incluindo medidas técnicas postas em prática para facilitar a interpretação dos resultados dos sistemas de IA pelos responsáveis pela sua implementação; especificações de dados de entrada, conforme aplicável.

4. Uma descrição da adequação dos parâmetros de desempenho para o sistema de IA específico. Uma

5. descrição detalhada do sistema de gestão de riscos de acordo com o Artigo 9.

6. Uma descrição das alterações relevantes feitas pelo fornecedor no sistema ao longo de seu ciclo de vida.

7. Uma lista de normas harmonizadas, aplicadas no todo ou em parte, cujas referências foram publicadas no Jornal Oficial da União Europeia;Quando não tiverem sido aplicadas normas harmonizadas, uma descrição detalhada das soluções adotadas para atender aos requisitos estabelecidos no Capítulo III, Seção 2, incluindo uma lista de outras normas e especificações técnicas relevantes que foram aplicadas.

8. Uma cópia da declaração de conformidade da UE em conformidade com o artigo 47.º.

9. Uma descrição detalhada do sistema estabelecido para avaliar o desempenho do sistema de IA na fase pós-comercialização, de acordo com o artigo 72.º, incluindo o plano de vigilância pós-comercialização referido no artigo 72.º(3).

ANEXO V

Declaração de conformidade da UE

A declaração UE de conformidade referida no artigo 47.º deve conter todas as seguintes informações:

1. O nome e o tipo do sistema de IA, e quaisquer referências adicionais inequívocas que permitam a identificação e rastreabilidade do sistema de IA.

2. O nome e endereço do fornecedor ou, quando aplicável, do seu representante autorizado.

3. A declaração de que a declaração de conformidade da UE nos termos do artigo 47 é emitida sob a exclusiva responsabilidade do fornecedor.

4. A declaração de que o sistema de IA está em conformidade com o presente regulamento e, se aplicável, com quaisquer outras disposições relevantes do direito da União que prevejam a emissão da declaração da UE nos termos do artigo 47.º.

5. Quando um sistema de IA envolve o processamento de dados pessoais, uma declaração de que o sistema de IA está em conformidade com o Regulamento (UE) 2016/679, o Regulamento (UE) 2018/1725 e a Diretiva (UE) 2016/680.

6. Referências a quaisquer normas harmonizadas relevantes que tenham sido aplicadas ou a qualquer outra especificação comum à qual seja declarada conformidade.

7. Quando aplicável, o nome e o número de identificação do organismo notificado, uma descrição do procedimento de avaliação da conformidade seguido e a identificação do certificado emitido.

8. O local e a data de emissão da declaração, o nome e o cargo da pessoa que a assina, a indicação da pessoa em cujo nome ou por conta de quem a declaração é assinada e a assinatura.

ANEXO VI

Procedimento de avaliação da conformidade baseado no controlo interno

1. O procedimento de avaliação da conformidade baseado no controle interno é o procedimento de avaliação da conformidade baseado nos pontos 2, 3 e 4.

2. O fornecedor verifica se o sistema de gestão da qualidade estabelecido está em conformidade com os requisitos estabelecidos no Artigo 17.

3. O fornecedor examina as informações na documentação técnica para avaliar a conformidade do sistema de IA com os requisitos essenciais relevantes estabelecidos no Capítulo III, Seção 2.

4. O fornecedor deve também verificar se o processo de concepção e desenvolvimento do sistema de IA e a sua vigilância pós-comercialização referidos no artigo 72.º são consistentes com a documentação técnica.

ANEXO VII

Conformidade baseada na avaliação do sistema de gestão da qualidade e na avaliação do documentação técnica

1. Introdução

A conformidade baseada na avaliação do sistema de gestão da qualidade e na avaliação da documentação técnica é o procedimento de avaliação da conformidade baseado nos pontos 2 a 5.

2. Apresentação geral

O sistema de gestão da qualidade aprovado relativo à concepção, desenvolvimento e teste de sistemas de IA nos termos do artigo 17.º será examinado em conformidade com o ponto 3 e estará sujeito a vigilância em conformidade com o ponto 5. A documentação técnica do sistema de IA será examinada em conformidade com o ponto 4.

3. Sistema de gestão da qualidade

3.1. A solicitação do fornecedor deverá incluir:

(a) o nome e endereço do fornecedor e, se o pedido for apresentado pelo representante autorizado, também o seu nome e endereço;

b) a lista de sistemas de IA aos quais se aplica o mesmo sistema de gestão da qualidade;

c) a documentação técnica de cada sistema de IA ao qual o mesmo sistema de gestão da qualidade é aplicado;

(d) documentação relativa ao sistema de gestão da qualidade, que deverá abranger todos os aspectos enumerados no artigo 17.º;

e) uma descrição dos procedimentos estabelecidos para garantir que o sistema de gestão da qualidade permaneça adequado e eficaz;

(f) uma declaração escrita de que o mesmo pedido não foi apresentado a nenhum outro organismo notificado.

3.2. O sistema de gestão da qualidade deve ser avaliado pelo organismo notificado, que deve determinar se cumpre os requisitos especificados no artigo 17.º.

A decisão será notificada ao fornecedor ou seu representante autorizado.

A notificação deve incluir as conclusões da avaliação do sistema de gestão da qualidade e uma decisão fundamentada sobre a avaliação.

3.3. O Fornecedor deverá continuar a implementar e manter o sistema de gestão da qualidade aprovado para que ele permaneça adequado e eficaz.

3.4. O fornecedor deve informar o organismo notificado sobre quaisquer alterações pretendidas ao sistema de gestão da qualidade aprovado ou à lista de sistemas de IA aos quais se aplica.

O organismo notificado deve examinar as alterações propostas e decidir se o sistema de gestão da qualidade modificado continua a cumprir os requisitos referidos no ponto 3.2 ou se é necessária uma nova avaliação.

O organismo notificado deve notificar o fornecedor da sua decisão. A notificação deve incluir as conclusões da revisão das alterações e uma decisão fundamentada sobre a avaliação.

4. Controle de documentação técnica

4.1. Além do pedido referido no ponto 3, o fornecedor deve apresentar um pedido ao organismo notificado da sua escolha para a avaliação da documentação técnica relativa ao sistema de IA que o fornecedor pretende colocar no mercado ou colocar em serviço e ao qual se aplica o sistema de gestão da qualidade referido no ponto 3.

4.2. O pedido deverá incluir:

a) o nome e endereço do fornecedor;

b) uma declaração escrita de que o mesmo pedido não foi submetido a nenhum outro organismo notificado;

c) a documentação técnica prevista no Anexo IV.

4.3. O organismo notificado deve examinar a documentação técnica. Sempre que adequado e na medida necessária ao desempenho das suas tarefas, o organismo notificado deverá ter pleno acesso aos conjuntos de dados de formação, validação e ensaio utilizados, incluindo, sempre que adequado e sujeito a salvaguardas de segurança, por meio de API ou outras ferramentas e meios técnicos relevantes que permitam acesso remoto.

4.4. Ao examinar a documentação técnica, o organismo notificado pode exigir que o fornecedor forneça mais evidências. documentos de suporte ou realizar testes adicionais para permitir que a conformidade do sistema de IA com os requisitos estabelecidos no Capítulo III, Seção 2 seja adequadamente avaliada. Quando o organismo notificado não estiver satisfeito com os testes realizados pelo fornecedor, ele próprio realizará os testes apropriados diretamente, conforme apropriado.

4.5. O organismo notificado também terá acesso ao modelo de formação e ao modelo treinado do Sistema de IA, com os seus parâmetros correspondentes, para, se necessário, uma vez esgotados todos os outros meios razoáveis de verificação da conformidade e se tenham revelado insuficientes, e mediante pedido fundamentado, avaliar a conformidade do sistema de IA de alto risco com os requisitos estabelecidos no Capítulo III, Secção 2. Esse acesso estará sujeito à legislação da União aplicável à proteção da propriedade intelectual e dos segredos comerciais.

4.6. O fornecedor ou seu representante autorizado deve ser notificado da decisão do organismo notificado. A notificação deve incluir as conclusões da avaliação da documentação técnica e uma decisão fundamentada sobre a avaliação.

Quando o sistema de IA cumprir os requisitos estabelecidos no Capítulo III, Secção 2, o organismo notificado emitirá um certificado da União de avaliação da documentação técnica. Este certificado deverá indicar o nome e endereço do fornecedor, as conclusões do exame, as condições de validade (se aplicável) e os dados necessários para identificar o sistema de IA.

O certificado e seus anexos devem conter todas as informações relevantes para permitir a avaliação da conformidade do sistema de IA e para permitir o controle do sistema de IA durante o uso, quando aplicável.

Caso o sistema de IA não cumpra os requisitos estabelecidos no Capítulo III, Secção 2, o organismo notificado deve recusar a emissão do certificado da União de avaliação da documentação técnica e informar o requerente, fundamentando detalhadamente a sua decisão.

Quando o sistema de IA não atender aos requisitos relativos aos dados utilizados para seu treinamento, será necessário um novo treinamento do sistema antes de solicitar uma nova avaliação de conformidade. Neste caso, a decisão fundamentada sobre a avaliação do organismo notificado que recusa emitir o certificado da União de avaliação da documentação técnica deve conter considerações específicas relativas à qualidade dos dados utilizados para treinar o sistema de IA, em especial no que diz respeito aos motivos da não conformidade.

4.7. Qualquer alteração no sistema de IA que possa afetar sua conformidade com os requisitos ou sua finalidade pretendida deve ser avaliada pelo organismo notificado que emitiu o certificado da União para avaliação da documentação técnica. O fornecedor deve informar o organismo notificado da sua intenção de introduzir qualquer uma das alterações acima mencionadas ou se tem conhecimento de que tais alterações ocorreram. O organismo notificado deve avaliar as alterações pretendidas e decidir se estas requerem uma nova avaliação da conformidade, em conformidade com o artigo 43.º, n.º 4, ou se podem estar sujeitas a um suplemento ao certificado da União de avaliação da documentação técnica. Neste último caso, o organismo notificado deve avaliar as alterações, notificar a sua decisão ao fornecedor e, se aprovar as alterações, emitir um suplemento ao certificado da União de avaliação da documentação técnica.

5. Monitoramento do sistema de gestão da qualidade aprovado

5.1. O objetivo da vigilância pelo organismo notificado referido no ponto 3 é garantir que o fornecedor cumpre devidamente as condições do sistema de gestão da qualidade aprovado.

5.2. Para efeitos da avaliação, o fornecedor deve conceder ao organismo notificado acesso às instalações onde os sistemas de IA estão a ser concebidos, desenvolvidos ou testados. Além disso, o fornecedor deve fornecer ao organismo notificado todas as informações necessárias.

5.3. O organismo notificado deve realizar auditorias periódicas para garantir que o fornecedor mantém e aplica as sistema de gestão da qualidade e lhe fornecerá um relatório de auditoria. No âmbito dessas auditorias, o organismo notificado pode realizar novos testes de sistemas de IA para os quais foram emitidos certificados da União para a avaliação da documentação técnica.

ANEXO VIII

Informações a serem enviadas para registro no registro de sistemas de IA de alto risco de acordo com o artigo 49

Secção A — Informações a apresentar pelos fornecedores de sistemas de IA de alto risco, de acordo com o Artigo 49, parágrafo 1

Para que os sistemas de IA de alto risco sejam registados nos termos do artigo 49.º, n.º 1, devem ser fornecidas e devidamente atualizadas as seguintes informações:

1. O nome, endereço e detalhes de contato do fornecedor.

2. Quando outra pessoa envia as informações em nome do fornecedor, o nome, endereço e detalhes de contato dessa pessoa.

3. O nome, endereço e detalhes de contato do representante autorizado, se aplicável.

4. O nome comercial do sistema de IA e qualquer referência inequívoca adicional que permita sua identificação e rastreabilidade.

5. A descrição da finalidade pretendida do sistema de IA e dos componentes e funções suportados por ele.

6. Uma descrição simples e concisa das informações que o sistema utiliza (dados, entradas) e sua lógica operacional.

7. O status do sistema de IA (comercializado ou colocado em serviço, não mais comercializado ou em serviço, recuperado).

8. O tipo, número e data de validade do certificado emitido pelo organismo notificado e o nome ou número de identificação do organismo notificado, quando aplicável.

9. Uma cópia digitalizada do certificado referido no ponto 8, quando aplicável.

10. Qualquer Estado-Membro em que o sistema de IA tenha sido colocado no mercado, colocado em serviço ou disponibilizado no mercado da União.

11. Uma cópia da declaração UE de conformidade referida no artigo 47.º.

12. Instruções eletrônicas de uso. Essas informações não serão fornecidas para sistemas de IA de alto risco nas áreas de aplicação da lei ou migração, asilo e gerenciamento de controle de fronteiras. referido no Anexo III, pontos 1, 6 e 7.

13. Um URL para informações adicionais (opcional).

Secção B — Informações a apresentar pelos fornecedores de sistemas de IA de alto risco, de acordo com o Artigo 49, parágrafo 2

No que diz respeito aos sistemas de IA a registar nos termos do artigo 49.º, n.º 2, devem ser fornecidas e devidamente atualizadas as seguintes informações:

1. O nome, endereço e detalhes de contato do fornecedor.

2. Quando outra pessoa envia as informações em nome do fornecedor, o nome, endereço e detalhes de contato dessa pessoa.

3. O nome, endereço e detalhes de contato do representante autorizado, se aplicável.

4. O nome comercial do sistema de IA e qualquer referência inequívoca adicional que permita sua identificação e rastreabilidade.

5. A descrição da finalidade pretendida do sistema de IA.

6. A condição ou condições referidas no artigo 6.º(3) em que o sistema de IA é considerado não de alto risco.

7. Um breve resumo das razões pelas quais o sistema de IA não é considerado de alto risco na aplicação do procedimento estabelecido no artigo 6.º(3).

8. O status do sistema de IA (comercializado ou colocado em serviço, não mais comercializado ou em serviço, recuperado).

9. Qualquer Estado-Membro em que o sistema de IA tenha sido colocado no mercado, colocado em serviço ou comercializado na União.

Secção C — Informações a apresentar pelos responsáveis pela implementação de sistemas de IA de alto risco de acordo com o artigo 49, parágrafo 3

Para que os sistemas de IA de alto risco sejam registados nos termos do artigo 49.º, n.º 3, devem ser fornecidas e devidamente atualizadas as seguintes informações:

1. O nome, endereço e detalhes de contato da pessoa responsável pela implantação.

2. O nome, endereço e detalhes de contato da pessoa que envia as informações em nome da pessoa responsável pela implantação.

3. URL de entrada do sistema de IA no banco de dados da UE pelo seu provedor.

4. Um resumo das conclusões da avaliação de impacto sobre os direitos fundamentais realizada de acordo com o Artigo 27.

5. Um resumo da avaliação de impacto da proteção de dados realizada em conformidade com o artigo 35.º do Regulamento (UE) 2016/679 ou o artigo 27.º da Diretiva (UE) 2016/680, conforme especificado no artigo 26.º, n.º 8, do presente regulamento, quando aplicável.

ANEXO IX

Informações a serem apresentadas para registo de sistemas de IA de alto risco listados no Anexo III em relação a testes de conformidade no mundo real com artigo 60

No que se refere aos ensaios em situação real a inscrever no registo nos termos do artigo 60.º, devem ser fornecidas e devidamente atualizadas as seguintes informações:

1. O número de identificação único para toda a União do teste em condições reais.

2. O nome e os detalhes de contato do fornecedor ou potencial fornecedor e dos responsáveis pela implantação envolvidos no teste real.

3. Uma breve descrição do sistema de IA, sua finalidade pretendida e outras informações necessárias para identificar o sistema.

4. Um resumo das principais características do plano de teste do mundo real.

5. Informações sobre a suspensão ou término do teste em condições reais.

ANEXO X

Atos legislativos da União relativos a sistemas de tecnologia da informação em larga escala no domínio da liberdade, da segurança e da justiça

1. Sistema de Informação 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 de 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, que altera a Convenção de Aplicação do Acordo de Schengen e que altera e revoga o Regulamento (CE) n.º 1861/2009.qualquer1987/2006 (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, que altera e revoga a Decisão 2007/533/JAI do Conselho e revoga o Regulamento (CE) n.º 1862/2009 do Parlamento Europeu e do Conselho.qualquer1986/2006 do Parlamento Europeu e do Conselho e Decisão 2010/261/UE da Comissão (JO L 312 de 7.12.2018, p. 56).

2. Sistema de Informação de Vistos

a) Regulamento (UE) 2021/1133 do Parlamento Europeu e do Conselho, de 7 de julho de 2021, que altera o Regulamento (UE) n.ºqualquer603/2013, (UE) 2016/794, (UE) 2018/1862, (UE) 2019/816 e (UE) 2019/818 no que diz respeito 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 1134/2009 e (CE) n.º 1134/2009.qualquer767/2008, (CE) n.ºqualquer810/2009, (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, a fim de reformar o Sistema de Informação sobre Vistos (JO L 248 de 13.7.2021, p. 11).

3. Eurodac

(a) Regulamento (UE) 2024/1358 do Parlamento Europeu e do Conselho, de 14 de maio de 2024, relativo à criação do sistema «Eurodac» para a comparação de dados biométricos para efeitos da aplicação efetiva dos Regulamentos (UE) 2024/1315 e (UE) 2024/1350 do Parlamento Europeu e do Conselho e da Diretiva 2001/55/CE do Conselho e da identificação de nacionais de países terceiros em situação irregular e de apátridas, bem como a pedidos das autoridades responsáveis pela aplicação da lei dos Estados-Membros e da Europol para efeitos 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 1389/2008.qualquer603/2013 do Parlamento Europeu e do Conselho (JO L 2024/1358, 22.5.2024, ELI: http://data.europa.eu/eli/reg/2024/1358/oj).

4. Sistema de entrada e saída

(a) Regulamento (UE) 2017/2226 do Parlamento Europeu e do Conselho, de 30 de novembro de 2017, que estabelece um Sistema de Entrada/Saída (EES) para registo de dados de entrada e saída e de dados de recusa de entrada relativos a nacionais de países terceiros que atravessam as fronteiras externas dos Estados-Membros, que determina as condições de acesso ao EES para efeitos de aplicação da lei e que altera a Convenção de Aplicação do Acordo de Schengen e os Regulamentos (CE) n.º 1789/2008 e (CE) n.º 1789/2008.qualquer767/2008 e (UE) n.qualquer1077/2011 (JO L 327 de 9.12.2017, p. 20).

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 o Regulamento (UE) n.º 1240/2018.qualquer1077/2011, (UE) n.ºqualquer515/2014, (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 com o objetivo de estabelecer o 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 em relação a nacionais de países terceiros e apátridas

Regulamento (UE) 2019/816 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, que estabelece um sistema centralizado para a identificação dos Estados-Membros que detêm informações sobre condenações relativas a nacionais de países terceiros e apátridas (ECRIS-TCN), para complementar 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, que estabelece um quadro de interoperabilidade entre os sistemas de informação da UE no domínio das fronteiras e vistos e que altera os Regulamentos (CE) n.º 1189/2008 e (CE) n.º 1189/2008.qualquer767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 e (UE) 2018/1861 do Parlamento Europeu e do Conselho e 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 ao estabelecimento de um quadro 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 referida no artigo 53.º, n.º 1, alínea a) — documentação técnica para provedores de modelos de IA de uso geral

Seção 1

Informações a serem enviadas por provedores de modelos de IA de uso geral

A documentação técnica referida no artigo 53.º, n.º 1, alínea a), deve incluir, pelo menos, as seguintes informações, em função da dimensão e do perfil de risco do modelo:

1. Uma visão geral do modelo de IA de uso geral, incluindo:

a) as tarefas que o modelo deve executar e o tipo e a natureza dos sistemas de IA nos quais ele pode ser integrado;

b) as políticas de uso aceitável aplicáveis;

c) a data de lançamento e os métodos de distribuição;

d) a arquitetura e o número de parâmetros;

e) a modalidade (por exemplo, texto, imagem) e o formato das entradas e saídas;

f) a licença.

2. Uma descrição detalhada dos elementos do modelo referidos no ponto 1 e informações relevantes sobre o processo de desenvolvimento, incluindo os seguintes elementos:

a) os meios técnicos (por exemplo, instruções de utilização, infraestruturas, ferramentas) necessários para integrar o modelo de IA de uso geral nos sistemas de IA;

b) as especificações de projeto do modelo e do processo de treinamento, incluindo métodos e técnicas de treinamento, principais decisões de projeto, incluindo a justificativa e as suposições feitas; o que o modelo foi projetado para otimizar e a relevância dos vários parâmetros, conforme apropriado;

c) informações sobre os dados utilizados para treinamento, teste e validação, quando aplicável, incluindo o tipo e a procedência dos dados e os métodos de gestão (por exemplo, limpeza, filtragem, etc.), o número de pontos de dados, seu escopo e suas principais características; como os dados foram obtidos e selecionados, incluindo quaisquer outras medidas para detectar fontes de dados inadequadas e métodos para detectar vieses identificáveis, quando apropriado;

d) os recursos computacionais usados para treinar o modelo (por exemplo, número de operações de ponto flutuante, tempo de treinamento e outros detalhes relevantes relacionados ao modelo;

e) o consumo de energia conhecido ou estimado do modelo.

Em relação à letra e), quando o consumo energético do modelo é desconhecido, uma estimativa do consumo energético pode ser feita a partir de informações relativas aos recursos computacionais utilizados.

Seção 2

Informações adicionais a serem enviadas por provedores de modelos de IA de uso geral com risco sistêmico

1. Uma descrição detalhada das estratégias de avaliação, com seus resultados, com base em protocolos e ferramentas de avaliação disponíveis publicamente ou outros métodos de avaliação. As estratégias de avaliação incluirão critérios de avaliação, parâmetros e método de detecção de limitações.

2. Quando aplicável, uma descrição detalhada das medidas tomadas para realizar testes adversários internos ou externos (por exemplo, uso de "equipes vermelhas") e adaptações de modelos, incluindo seu alinhamento e ajuste.

3. Quando aplicável, uma descrição detalhada da arquitetura do sistema, com uma explicação de como os componentes de software incorporam ou enriquecem uns aos outros e como eles são integrados ao processamento geral.

ANEXO XII

Informações sobre transparência referidas no artigo 53.º, n.º 1, alínea b) — documentação técnica dos fornecedores de modelos de IA para fins gerais para fornecedores a jusante integre o modelo ao seu sistema de IA

As informações referidas no artigo 53.º, n.º 1, alínea b), devem incluir, pelo menos, as seguintes informações:

1. Uma descrição geral do modelo de IA para fins gerais, incluindo:

a) as tarefas que o modelo deve executar e o tipo e a natureza dos sistemas de IA nos quais ele pode ser integrado;

b) as políticas de uso aceitável aplicáveis;

c) a data de lançamento e os métodos de distribuição;

d) a maneira como o modelo interage ou pode ser usado para interagir com oferragensou software que não faça parte do modelo em si, quando aplicável;

(e) as versões do software relevante relacionadas com a utilização do modelo de IA de uso geral, quando aplicável;

f) a arquitetura e o número de parâmetros;

g) a modalidade (por exemplo, texto, imagem) e o formato das entradas e saídas;

h) a licença modelo.

2. Uma descrição dos elementos do modelo e seu processo de desenvolvimento, incluindo:

a) os meios técnicos (por exemplo, instruções de utilização, infraestruturas, ferramentas) necessários para integrar o modelo de IA de uso geral nos sistemas de IA;

b) a modalidade (por exemplo, texto, imagem, etc.) e o formato das entradas e saídas e seu tamanho máximo (por exemplo, comprimento da janela de contexto, etc.);

c) informações sobre os dados utilizados para treinamento, teste e validação, quando aplicável, incluindo o tipo e a fonte dos dados e métodos de gestão.

ANEXO XIII

Critérios para a classificação de modelos de IA de uso geral com risco sistémico a que estão sujeitos
O artigo 51 refere-se

A fim de determinar se um modelo de IA para fins gerais tem capacidades ou efeitos equivalentes aos referidos 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 o tamanho do conjunto de dados, por exemplo medido através de criptomoedas;

c) a quantidade de computação usada para treinar o modelo, medida em operações de ponto flutuante ou indicada por uma combinação de outras variáveis, como o custo estimado do treinamento, o tempo estimado necessário ou o consumo estimado de energia para o treinamento;

e) as modalidades de entrada e saída do modelo, como texto para texto (modelos de linguagem grande), texto para imagem, multimodalidade e limites de ponta para determinar as capacidades de alto impacto de cada modalidade e o tipo específico de entradas e saídas (por exemplo, sequências biológicas);

e) os benchmarks e avaliações das capacidades do modelo, tendo também em conta o número de tarefas sem formação adicional, a sua adaptabilidade para aprender diferentes novas tarefas, o seu nível de autonomia e expansibilidade, e as ferramentas a que tem acesso;

E) se as suas implicações para o mercado interno forem significativas devido ao seu âmbito, o que será o caso quando tiver sido disponibilizado a pelo menos 10 000 utilizadores profissionais registados estabelecidos na União;

e) o número de usuários finais registrados.