Parecer conjunto 5/2021

do CEPD e da AEPD

sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial)

18 de junho de 2021

Síntese

Em 21 de abril de 2021, a Comissão Europeia apresentou a sua proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (doravante, a «proposta»). O CEPD e a AEPD saúdam a preocupação do legislador em abordar a utilização da inteligência artificial (IA) na União Europeia (UE) e salientam que a proposta tem **implicações no domínio da proteção de dados** que são manifestamente significativas.

O CEPD e a AEPD constatam que a **base jurídica** da proposta é, em primeiro lugar, o artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE). Além disso, a proposta tem igualmente por base o artigo 16.º do TFUE, na medida em que contém regras específicas aplicáveis à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, nomeadamente restrições à utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública. O CEPD e a AEPD recordam que, em conformidade com a jurisprudência do Tribunal de Justiça da União Europeia (TJUE), o artigo 16.º do TFUE proporciona uma base jurídica adequada nos casos em que a proteção de dados pessoais consiste num dos objetivos ou elementos essenciais das regras adotadas pela legislatura da UE. A aplicação do artigo 16.º do TFUE implica igualmente a **necessidade de garantir uma supervisão independente da conformidade** com os requisitos em matéria de tratamento de dados pessoais, tal como igualmente exigido no artigo 8.º da Carta dos Direitos Fundamentais da União Europeia.

No que diz respeito ao **âmbito de aplicação da proposta,** o CEPD e a AEPD congratulam-se vivamente com o facto de que abrange o fornecimento e a utilização de sistemas de IA por parte das instituições, órgãos e organismos da UE. Contudo, o CEPD e a AEPD consideram que a **exclusão da cooperação internacional para a aplicação da lei do âmbito de aplicação** estabelecido da proposta suscita sérias preocupações, uma vez que tal exclusão cria um risco significativo de evasão (por exemplo, países terceiros ou organizações internacionais que operam aplicações de risco elevado nas quais as autoridades públicas da UE se baseiam).

O CEPD e a AEPD **congratulam-se com a abordagem baseada no risco** que sustenta a proposta. No entanto, esta abordagem deve ser esclarecida e o conceito de «risco para os direitos fundamentais» deve ser alinhado com o RGPD e o Regulamento (UE) 2018/1725 (RPDUE), dado que estão em causa aspetos relacionados com a proteção de dados pessoais.

O CEPD e a AEPD concordam com a proposta de que a classificação de um **sistema de IA como sendo de risco elevado não significa necessariamente que tal sistema seja legal** *per se* e possa ser implantado pelo utilizador como tal. O responsável pelo tratamento **poderá ter de cumprir outros requisitos decorrentes da legislação da UE em matéria de proteção de dados**. Do mesmo modo, o cumprimento das obrigações legais decorrentes da legislação da União (incluindo em matéria de proteção de dados pessoais) deve ser uma condição prévia para permitir a entrada no mercado europeu enquanto produto com a marcação CE. Neste sentido, o CEPD e a AEPD consideram que **o requisito de assegurar o cumprimento do RGPD e do RPDUE deve ser incluído no título III, capítulo 2**. Além disso, o CEPD e a AEPD consideram necessário adaptar o procedimento de avaliação da conformidade previsto na proposta,

de modo que terceiros efetuem sempre avaliações da conformidade *ex ante* dos sistemas de IA de risco elevado.

Dado o elevado risco de discriminação, a proposta proíbe a «classificação social» quando efetuada «durante um certo período» ou «por autoridades públicas ou em seu nome». Contudo, as empresas privadas, tais como prestadores de serviços de redes sociais e serviços de computação em nuvem, podem também tratar grandes quantidades de dados pessoais e proceder à classificação social. Por conseguinte, **o futuro regulamento relativo à IA deve proibir qualquer tipo de classificação social**.

A identificação biométrica à distância de pessoas singulares em espaços acessíveis ao público representa um elevado risco de intromissão na vida privada das pessoas, com graves efeitos sobre as expetativas da população de permanecer anónima em espaços públicos. Por estes motivos, o CEPD e a AEPD **apelam à proibição geral de qualquer utilização de IA para o reconhecimento automatizado de características humanas em espaços acessíveis ao público** (tal como de rostos, mas também do andar, de impressões digitais, do ADN, da voz, da digitação e de outros sinais comportamentais ou biométricos) em qualquer contexto. Recomenda-se igualmente a **proibição** de **sistemas de IA que categorizem, com base na biometria, as pessoas singulares em grupos** de acordo com a origem étnica, o género, bem como a orientação sexual ou política, ou outras razões de discriminação nos termos do artigo 21.º da Carta. Além disso, o CEPD e a AEPD consideram que a utilização de IA para **inferir as emoções de uma pessoa singular é extremamente indesejável e deve ser proibida.**

O CEPD e a AEPD congratulam-se com a **designação da AEPD como autoridade competente e autoridade de fiscalização do mercado para a supervisão das instituições, órgãos e organismos da União**. O papel e as funções da AEPD devem, contudo, ser clarificados, especificamente no que se refere ao seu papel de autoridade de fiscalização do mercado. Do mesmo modo, o futuro regulamento relativo à IA deve estabelecer claramente a **independência das autoridades de controlo** no desempenho das suas funções de supervisão e aplicação.

A designação das autoridades de proteção de dados como autoridades nacionais de controlo asseguraria uma abordagem regulamentar mais harmonizada, bem como contribuiria para a interpretação coerente das disposições relativas ao tratamento de dados e evitaria contradições na sua aplicação entre os Estados-Membros. Por conseguinte, o CEPD e a AEPD consideram que **as autoridades de proteção de dados devem ser designadas como autoridades nacionais de controlo nos termos do artigo 59.º da proposta.**

A proposta atribui à Comissão um papel predominante no Comité Europeu para a Inteligência Artificial (EAIB, «European Artificial Intelligence Board»). O papel em causa entra em conflito com a necessidade de que um organismo europeu de IA seja independente de qualquer influência política. Para garantir a sua independência, o futuro regulamento relativo à IA deve conferir **mais autonomia ao EAIB** e garantir que este possa agir por sua própria iniciativa.

Tendo em conta a disseminação dos sistemas de IA em todo o mercado único e a probabilidade de casos transfronteiriços, é absolutamente necessária uma aplicação harmonizada e uma repartição adequada de competências entre as autoridades nacionais de controlo. O CEPD e a AEPD propõem a previsão de **um mecanismo que garanta um ponto de contacto único para as pessoas singulares visadas pela legislação, bem como para as empresas, por cada sistema de IA.**

No que diz respeito aos **ambientes de testagem,** o CEPD e a AEPD **recomendam clarificar o seu âmbito de aplicação e objetivos**. A proposta deve também estipular claramente que a base jurídica de tais ambientes de testagem deve cumprir os requisitos estabelecidos no atual quadro de proteção de dados.

O **sistema de certificação** descrito na proposta **carece de uma relação clara com a legislação da UE em matéria de proteção de dados**, bem como com outras legislações da UE e dos Estados-Membros aplicáveis a cada «domínio» do sistema de IA de risco elevado, e não tem em consideração os **princípios de minimização de dados e de proteção de dados desde a conceção** enquanto um dos aspetos a ter em conta **antes de obter a marcação CE**. Assim, o CEPD e a AEPD recomendam alterar a proposta por forma a clarificar a relação entre os certificados emitidos ao abrigo do referido regulamento e os procedimentos de certificação, selos e marcas de proteção de dados. Por fim, as autoridades de proteção de dados devem participar na preparação e no estabelecimento de normas harmonizadas e especificações comuns.

No que diz respeito aos **códigos de conduta**, o CEPD e a AEPD consideram **necessário clarificar** se a proteção de dados pessoais deve ser considerada como parte dos «requisitos adicionais» que podem ser abordados pelos códigos de conduta em causa, bem como garantir que as «especificações técnicas e soluções» não entram em conflito com as regras e os princípios do atual quadro de proteção de dados.

ÍNDICE

O Comité Europeu para a Proteção de Dados e a Autoridade Europeia para a Proteção de Dados

Tendo em conta o artigo 42.º, n.º 2, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE[1],

Tendo em conta o Acordo EEE e, nomeadamente, o anexo XI e o respetivo Protocolo 37, com a redação que lhe foi dada pela Decisão n.º 154/2018 do Comité Misto do EEE, de 6 de julho de 2018[2],

Tendo em conta o pedido de parecer conjunto da Autoridade Europeia para a Proteção de Dados e do Comité Europeu para a Proteção de Dados, de 22 de abril de 2021, sobre a proposta de regulamento que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial),

ADOTARAM O PRESENTE PARECER CONJUNTO

1 INTRODUÇÃO

1. O advento dos sistemas de inteligência artificial («IA») é um passo extremamente importante na evolução das tecnologias e na forma como os seres humanos interagem com as mesmas. A IA é um conjunto de tecnologias essenciais que alterarão profundamente as nossas vidas quotidianas, seja de uma perspetiva societal ou económica. Nos próximos anos, esperam-se decisões determinantes no âmbito da IA, uma vez que nos ajuda a superar alguns dos maiores desafios que enfrentamos atualmente em muitos domínios, desde a saúde à mobilidade ou da administração pública à educação.

2. Contudo, estes avanços anunciados não estão isentos de riscos. Na verdade, os riscos são de grande pertinência, tendo em conta que os efeitos individuais e societais dos sistemas de IA são, em larga medida, uma experiência nova. A criação de conteúdos, a realização de previsões ou a tomada de uma decisão de forma automatizada, tal como os sistemas de IA fazem, por meio de lógica ou técnicas de aprendizagem automática e regras de inferência probabilística, não é o mesmo que os seres humanos levarem a cabo tais atividades, por meio de raciocínio criativo ou teórico, assumindo plena responsabilidade pelas consequências.

3. A IA irá aumentar a quantidade de previsões que podem ser feitas em vários domínios a partir de correlações mensuráveis entre dados (invisíveis para os olhos humanos, mas visíveis para as máquinas), facilitando as nossas vidas e resolvendo inúmeros problemas; contudo, ao

[1] JO L 295 de 21.11.2018, p. 39–98.
[2] As referências a «Estados-Membros» no presente documento devem ser entendidas como referências a «Estados-Membros do EEE».

mesmo tempo, irá desgastar a nossa capacidade de dar uma interpretação causal aos resultados, de tal forma que os conceitos de transparência, controlo humano e responsabilidade sobre os resultados serão seriamente questionados.

4. Os dados (pessoais e não pessoais) no âmbito da IA são, em muitos caos, a premissa fundamental para as decisões autónomas, o que irá afetar inevitavelmente as vidas dos cidadãos a vários níveis. É por este motivo que o CEPD e a AEPD defendem firmemente desde já que a proposta de regulamento que estabelece regras harmonizadas em matéria de inteligência artificial (Regulamento Inteligência Artificial) (doravante, a «proposta»)[3] tem **implicações significativas no domínio da proteção de dados**.

5. A atribuição da função de decidir às máquinas, com base nos dados, criará riscos para os direitos e liberdades das pessoas singulares, afetará as suas vidas privadas e poderá prejudicar grupos ou até mesmo sociedades no seu conjunto. O CEPD e a AEPD destacam que os direitos à privacidade e à proteção dos dados pessoais – em conflito com o pressuposto da autonomia de decisão das máquinas subjacente ao conceito de IA – são um pilar dos valores da UE conforme consagrados na Declaração Universal dos Direitos Humanos (artigo 12.º), na Convenção Europeia dos Direitos Humanos (artigo 8.º) e na Carta dos Direitos Fundamentais da União Europeia (doravante, a «Carta») (artigos 7.º e 8.º). A conciliação da perspetiva de crescimento oferecida pelas aplicações de IA e a centralidade e primazia dos seres humanos em relação às máquinas é um objetivo muito ambicioso, mas necessário.

6. O CEPD e a AEPD acolhem favoravelmente a participação no regulamento de todas as partes interessadas da cadeia de valor da IA e a introdução de requisitos específicos para os fornecedores de soluções, dado que estes desempenham um papel significativo nos produtos que utilizam os seus sistemas. No entanto, é necessário delimitar e atribuir claramente as responsabilidades das várias partes – utilizador, fornecedor, importador ou distribuidor de um sistema de IA. Em particular, ao efetuar o tratamento de dados pessoais, deve ser dada especial atenção à coerência entre estas funções e responsabilidades e as definições de responsável pelo tratamento e subcontratante previstas no quadro de proteção de dados, uma vez que ambas as normas não são coerentes.

7. A proposta confere um lugar de destaque ao conceito de supervisão humana (artigo 14.º), que o CEPD e a AEPD acolhem positivamente. Contudo, tal como referido anteriormente, devido à forte possibilidade de determinados sistemas de IA terem impacto sobre os cidadãos ou grupos de cidadãos, a verdadeira centralidade humana deve apoiar-se numa supervisão humana altamente qualificada e num tratamento lícito – na medida em que tais sistemas têm por base o tratamento de dados pessoais ou efetuam o tratamento de dados pessoais para cumprir a sua função – por forma a garantir que o direito de não ser objeto de decisões baseadas unicamente no tratamento automatizado é respeitado.

8. Além disso, devido à natureza de utilização intensiva de dados de muitas aplicações de IA, a proposta deve promover a adoção de uma abordagem de proteção de dados desde a conceção e por defeito em todos os níveis, incentivando a aplicação efetiva de princípios de proteção de

[3] COM(2021) 206 final.

dados (conforme previsto no artigo 25.º do RGPD e no artigo 27.º do RPDUE) através de tecnologias de ponta.

9. Por fim, o CEPD e a AEPD salientam que o presente parecer conjunto é apresentado apenas como uma análise preliminar da proposta, sem prejuízo de outras avaliações ou pareceres posteriores sobre os efeitos da proposta e a sua compatibilidade com a legislação da UE em matéria de proteção de dados.

2 ANÁLISE DOS PRINCÍPIOS FUNDAMENTAIS DA PROPOSTA

2.1 Âmbito de aplicação da proposta e relação com o atual quadro jurídico

10. De acordo com a exposição de motivos, a **base jurídica** da proposta é, em primeiro lugar, o artigo 114.º do TFUE, que prevê a adoção de medidas para garantir o estabelecimento e o funcionamento do mercado interno[4]. A proposta tem ainda por base o artigo 16.º do TFUE, *na medida em que contém regras específicas aplicáveis à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais*, nomeadamente restrições à utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública[5].

11. O CEPD e a AEPD recordam que, em conformidade com a jurisprudência do TJUE, o artigo 16.º do TFUE proporciona uma base jurídica adequada nos casos em que a proteção de dados pessoais consiste num dos objetivos ou elementos essenciais das regras adotadas pela legislatura da UE[6]. A aplicação do artigo 16.º do TFUE implica igualmente a necessidade de garantir uma supervisão independente da conformidade com os requisitos em matéria de tratamento de dados pessoais, tal como igualmente exigido no artigo 8.º da Carta.

12. O CEPD e a AEPD relembram que já existe um quadro abrangente de proteção de dados adotado com base no artigo 16.º do TFUE, que consiste no Regulamento Geral sobre a Proteção de Dados (RGPD)[7], no Regulamento sobre a Proteção de Dados para instituições, órgãos e organismos da União Europeia (RPDUE)[8] e na Diretiva sobre a Proteção de Dados na

[4] Exposição de motivos, p. 5.
[5] Exposição de motivos, p. 6. Consultar igualmente o considerando 2 da proposta.
[6] Parecer de 26 de julho de 2017, *PNR Canada*, processo de parecer 1/15, ECLI:EU:C:2017:592, n.º 96.
[7] 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. 1–88).
[8] Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39–98).

Aplicação da Lei (PDAL)[9]. De acordo com a proposta, apenas as restrições adicionais relativas ao tratamento de dados biométricos constantes da proposta podem considerar-se que têm por base o artigo 16.º do TFUE e, por conseguinte, que têm a mesma base jurídica que o RGPD, o RPDUE ou a PDAL. O que precede tem importantes implicações para a relação da proposta com o RGPD, o RPDUE e a PDAL de uma forma geral, conforme estabelecido infra.

13. No que diz respeito ao **âmbito de aplicação da proposta**, o CEPD e a AEPD congratulam-se vivamente com o facto de que a proposta abrange a utilização de sistemas de IA por parte das instituições, órgãos e organismos da UE. Uma vez que a utilização de sistemas de IA por parte das entidades em questão pode ter igualmente um impacto significativo nos direitos fundamentais das pessoas singulares, semelhante à utilização nos Estados-Membros da UE, é imprescindível que o novo quadro regulamentar para a IA seja aplicável tanto aos Estados-Membros da UE como a instituições, órgãos e organismos da UE, a fim de garantir uma abordagem coerente em toda a União. Dado que as instituições, órgãos e organismos da UE podem atuar como fornecedores e utilizadores de sistemas de IA, o CEPD e a AEPD consideram inteiramente adequado incluir tais entidades no âmbito de aplicação da proposta com base no artigo 114.º do TFUE.

14. Contudo, o CEPD e a AEPD manifestam grande apreensão quanto à exclusão da cooperação internacional para a aplicação da lei do âmbito de aplicação estabelecido no artigo 2.º, n.º 4, da proposta. Tal exclusão cria um risco significativo de evasão (por exemplo, países terceiros ou organizações internacionais que operam aplicações de risco elevado nas quais as autoridades públicas da UE se baseiam).

15. O desenvolvimento e a utilização de sistemas de IA implicarão, em muitos casos, o tratamento de dados pessoais. Assegurar a clareza da relação entre a presente proposta e a atual legislação da UE em matéria de proteção de dados assume uma importância primordial. A proposta complementa e não prejudica o RGPD, o RPDUE e a PDAL. Embora os considerandos da proposta clarifiquem que a utilização de sistemas de IA deve continuar a cumprir a legislação em matéria de proteção de dados, **o CEPD e a AEPD recomendam veementemente clarificar no artigo 1.º da proposta que a legislação da União em matéria de proteção de dados pessoais** (nomeadamente o RGPD, o RPDUE, a Diretiva Privacidade Eletrónica[10] e a PDAL) é aplicável a qualquer tratamento de dados pessoais abrangido pelo âmbito de aplicação da proposta. Um considerando correspondente deve clarificar igualmente que a proposta não pretende afetar a aplicação da legislação da UE em vigor que rege o tratamento de dados pessoais, incluindo as funções e competências das autoridades de controlo independentes competentes para controlar o cumprimento desses instrumentos.

[9] 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. 89–131).

[10] 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), com a redação que lhe foi dada pela Diretiva 2006/24/CE e a Diretiva 2009/136/CE.

2.2 Abordagem baseada no risco

16. O CEPD e a AEPD **congratulam-se com a abordagem baseada no risco** que sustenta a proposta. A proposta seria aplicável a todos os sistemas de IA, incluindo aos que não implicam o tratamento de dados pessoais, mas que ainda assim podem afetar os interesses ou os direitos fundamentais e as liberdades.

17. O CEPD e a AEPD constatam que algumas disposições da proposta não incluem os riscos para grupos de pessoas singulares ou para a sociedade em geral (por exemplo, efeitos coletivos com uma pertinência específica, como discriminação de grupo ou expressão de opiniões políticas em espaços públicos). O CEPD e a AEPD recomendam que os riscos societais/de grupo decorrentes dos sistemas de IA também sejam avaliados e mitigados.

18. O CEPD e a AEPD consideram que a abordagem baseada no risco prevista na proposta deve ser esclarecida e o conceito de «risco para os direitos fundamentais» **deve ser alinhado com o RGPD**, na medida em que estão em causa aspetos relacionados com a proteção de dados pessoais. Quer sejam utilizadores finais, apenas titulares dos dados ou outras pessoas visadas pelo sistema de IA, a ausência de qualquer referência no texto à pessoa singular afetada pelo sistema de IA apresenta-se como um ângulo morto na proposta. De facto, as obrigações impostas aos intervenientes face às pessoas afetadas devem decorrer de forma mais concreta da proteção da pessoa singular e dos seus direitos. Assim, o CEPD e a AEPD exortam os legisladores a abordar expressamente na proposta os **direitos e vias de recursos à disposição das pessoas singulares** sujeitas aos sistemas de IA.

19. O CEPD e a AEPD tomam nota da opção de fornecer uma lista exaustiva de **sistemas de IA de risco elevado**. Esta opção poderá criar um efeito a preto e branco, com fracas capacidades de atração de situações de elevado risco, comprometendo a abordagem global baseada no risco subjacente à proposta. Do mesmo modo, esta lista de sistemas de IA de risco elevado especificada nos anexos II e III da proposta carece de alguns tipos de casos de utilização que implicam riscos significativos, tais como a utilização de IA para determinar o prémio de seguro, para avaliar tratamentos médicos ou para efeitos de investigação no domínio da saúde. O CEPD e a AEPD salientam igualmente que os referidos anexos terão de ser atualizados regularmente, a fim de garantir que o seu âmbito de aplicação é adequado.

20. A proposta exige que os **fornecedores** do sistema de IA efetuem uma avaliação de riscos; contudo, na maioria dos casos, os responsáveis pelo tratamento (de dados) serão os **utilizadores** ao invés dos fornecedores dos sistemas de IA (por exemplo, um utilizador de um sistema de reconhecimento do rosto é um «responsável pelo tratamento» e, por conseguinte, não está vinculado pelos requisitos aplicáveis a fornecedores de IA de risco elevado nos termos da proposta).

21. Além disso, **um fornecedor nem sempre conseguirá avaliar todas as utilizações** de um sistema de IA. Assim, a avaliação inicial de riscos terá um caráter mais geral do que a efetuada pelo utilizador do sistema de IA. Mesmo que a avaliação inicial de riscos efetuada pelo fornecedor não indique que o sistema de IA é de «risco elevado» nos termos da proposta, tal não deve excluir **uma avaliação posterior (mais granular)** (avaliação de impacto sobre a

proteção de dados nos termos do artigo 35.º do RGPD, do artigo 39.º do RPDUE ou do artigo 27.º da PDAL) **que deve ser realizada pelo utilizador do sistema**, tendo em conta o contexto da utilização e os casos de utilização específicos. A interpretação sobre a questão de saber se um tipo de tratamento ao abrigo do RGPD, do RPDUE e da PDAL é suscetível de resultar num risco elevado deve ser feita de forma independente da proposta. Contudo, a classificação de um sistema de IA como sendo de «risco elevado» devido ao seu impacto nos direitos fundamentais[11] **desencadeia uma presunção de «risco elevado» nos termos do RGPD, do RPDUE e da PDAL, na medida em que os dados pessoais são objeto de tratamento.**

22. **O CEPD e a AEPD concordam com a proposta de que a classificação de um sistema de IA como sendo de risco elevado não significa necessariamente que tal sistema seja legal *per se* e possa ser implantado pelo utilizador como tal. O responsável pelo tratamento poderá ter de cumprir outros requisitos decorrentes da legislação da UE em matéria de proteção de dados.** Além disso, o raciocínio subjacente ao artigo 5.º da proposta – segundo o qual, ao contrário dos sistemas proibidos, os sistemas de risco elevado podem ser admissíveis em princípio – deve ser abordado e dissipado na proposta, especialmente porque a marcação CE proposta não implica que o tratamento conexo de dados pessoais seja lícito.

23. No entanto, o cumprimento das obrigações legais decorrentes da legislação da União (incluindo em matéria de proteção de dados pessoais) deve ser uma condição prévia para permitir a entrada no mercado europeu enquanto produto com a marcação CE. Neste sentido, o CEPD e a AEPD **recomendam incluir no título III, capítulo 2, da proposta o requisito de assegurar o cumprimento do RGPD e do RPDUE**. Este requisito deve ser objeto de auditoria (auditoria por parte de terceiros) antes da marcação CE, em conformidade com o princípio de responsabilidade. No contexto da referida auditoria por parte de terceiros, a avaliação inicial de impacto a ser realizada pelo fornecedor será especialmente pertinente.

24. Tendo em conta as complexidades decorrentes do desenvolvimento de sistemas de IA, importa destacar que as características técnicas dos sistemas de IA (por exemplo, o tipo de abordagem no domínio da IA) poderiam resultar em maiores riscos. Por conseguinte, qualquer avaliação de riscos sobre um sistema de IA deve ter em consideração **as características técnicas** juntamente **com os respetivos casos de utilização específicos e o contexto** no qual o sistema opera.

25. À luz do que precede, o CEPD e a AEPD recomendam especificar na proposta que **o fornecedor** deve realizar uma avaliação inicial de riscos sobre o sistema de IA em causa, **tendo em conta os casos de utilização** [a especificar na proposta – como complemento, por exemplo, do anexo III, ponto 1, alínea a), onde os casos de utilização dos sistemas biométricos de IA não

[11] A Agência dos Direitos Fundamentais da União Europeia (FRA) já abordou a necessidade de realizar avaliações de impacto sobre os direitos fundamentais ao utilizar IA ou tecnologias conexas. No seu relatório de 2020, «Getting the future right – Artificial intelligence and fundamental rights» (Construir o futuro certo – Inteligência artificial e direitos fundamentais), a FRA identificou obstáculos na utilização da IA (por exemplo, no policiamento preditivo, nos diagnósticos médicos, nos serviços sociais e na publicidade direcionada) e salientou que as organizações privadas e públicas devem efetuar avaliações sobre o modo como a IA poderia ser prejudicial para os direitos fundamentais, a fim de reduzir os impactos negativos sobre os cidadãos.

são referidos], e que o **utilizador** do sistema de IA, na qualidade de responsável pelo tratamento nos termos da legislação da UE em matéria de proteção de dados (se aplicável), deve realizar a avaliação de impacto sobre a proteção de dados conforme previsto no artigo 35.º do RGPD, no artigo 39.º do RPDUE e no artigo 27.º da PDAL, tendo em consideração não só a característica técnica e **o caso de utilização**, como **também o contexto específico** no qual a IA irá operar.

26. É ainda necessário clarificar alguns dos termos mencionados no anexo III da proposta (como, por exemplo, «serviços privados essenciais» ou «fornecedor de pequena dimensão que utiliza IA de avaliação da capacidade de endividamento para utilização própria»).

2.3 Utilizações de IA proibidas

27. O CEPD e a AEPD são de opinião que as **formas intrusivas de IA** – nomeadamente as que possam afetar a dignidade humana – devem ser consideradas sistemas de IA proibidos ao abrigo do artigo 5.º da proposta ao invés de serem simplesmente classificadas como sendo de «risco elevado» no anexo III da proposta, tal como os sistemas ao abrigo do artigo 6.º. Tal é aplicável, em especial, a comparações de dados que, em larga escala, afetam igualmente pessoas que deram muito poucos ou nenhuns motivos para vigilância policial, bem como a tratamentos que prejudicam o princípio de limitação das finalidades ao abrigo da legislação em matéria de proteção de dados. A utilização de IA no domínio da polícia e da aplicação da lei requer regras específicas, precisas, previsíveis e proporcionais que devem considerar os interesses das pessoas em causa e os efeitos no funcionamento de uma sociedade democrática.

28. O artigo 5.º da proposta corre o risco de adular os «valores» e a proibição dos sistemas de IA em contraste com tais valores. De facto, os critérios referidos no artigo 5.º para «classificar» os sistemas de IA como proibidos **limitam o âmbito de aplicação da proibição** de tal forma que esta poderia deixar de ter sentido na prática (por exemplo, «cause ou seja suscetível de causar danos físicos ou psicológicos» no artigo 5.º, n.º 1, alíneas a) e b); limitação das autoridades públicas no artigo 5.º, n.º 1, alínea c); formulação vaga no artigo 5.º, n.º 1, alínea c), subalíneas i) e ii); limitação apenas da identificação biométrica à distância «em tempo real» sem qualquer definição clara, entre outros).

29. Em particular, a utilização de IA para efeitos de «classificação social», tal como prevista no artigo 5.º, n.º 1, alínea c), da proposta, pode conduzir a discriminação e é contrária aos valores fundamentais da UE. A proposta apenas proíbe estas práticas quando efetuadas «durante um certo período» ou «por autoridades públicas ou em seu nome». As empresas privadas, nomeadamente prestadores de serviços de redes sociais e serviços de computação em nuvem, podem tratar grandes quantidades de dados pessoais e proceder à classificação social. Por conseguinte, **a proposta deve proibir qualquer tipo de classificação social**. Importa salientar que, no contexto da aplicação da lei, o artigo 4.º da PDAL já limita significativamente – se não o proibir na prática – este tipo de atividades.

30. A **identificação biométrica à distância** de pessoas singulares em espaços acessíveis ao público representa um elevado risco de intromissão na vida privada das pessoas. Por conseguinte, o CEPD e a AEPD **consideram necessária uma abordagem mais rigorosa**. A

utilização de sistemas de IA pode colocar graves problemas de proporcionalidade, uma vez que pode implicar o tratamento de dados de um número indiscriminado e desproporcionado de titulares dos dados para a identificação de apenas algumas pessoas (por exemplo, passageiros em aeroportos e estações ferroviárias). A natureza **sem fricção** dos sistemas de identificação biométrica à distância levanta igualmente problemas de transparência e questões relacionadas com a base jurídica para o tratamento nos termos da legislação da UE (PDAL, RGPD, RPDUE e outra legislação aplicável). O problema no que diz respeito ao modo de informar devidamente as pessoas singulares sobre o tratamento em questão, bem como ao exercício efetivo e atempado dos seus direitos, permanece por resolver. O mesmo se aplica aos **efeitos graves e irreversíveis sobre as expetativas** (razoáveis) **da população de permanecer anónima em espaços públicos**, que resultam num efeito adverso direto sobre o exercício da liberdade de expressão, de reunião, de associação e de circulação.

31. O artigo 5.º, n.º 1, alínea d), da proposta prevê uma extensa **lista de casos excecionais** em que a identificação biométrica à distância «em tempo real» em espaços acessíveis ao público é permitida para efeitos de manutenção da ordem pública. O CEPD e a AEPD consideram **esta abordagem deficiente** em vários aspetos: Em primeiro lugar, não é claro o que deve ser entendido como «atraso significativo» e a forma como tal atraso deve ser considerado um fator atenuante, tendo em conta que um sistema de identificação em massa pode identificar milhares de pessoas em apenas algumas horas. Além disso, o caráter intrusivo do tratamento nem sempre depende de a identificação ser ou não efetuada em tempo real. A identificação biométrica à distância posterior no contexto de um protesto político poderá ter um significativo efeito inibidor no exercício dos direitos fundamentais e liberdades (tais como a liberdade de reunião e de associação) e, de um modo mais geral, nos princípios de base da democracia. Em segundo lugar, o caráter intrusivo do tratamento não depende necessariamente da sua finalidade. A utilização do sistema em causa para outras finalidades como a segurança privada constitui a mesma ameaça aos direitos fundamentais de respeito pela vida privada e familiar e de proteção dos dados pessoais. Por último, mesmo com as limitações previstas, o potencial número de suspeitos ou autores de crimes será quase sempre «suficientemente elevado» para justificar a utilização contínua dos sistemas de IA para a deteção de suspeitos, apesar das condições adicionais previstas no artigo 5.º, n.ºs 2 a 4, da proposta. O raciocínio subjacente à proposta parece omitir que, ao vigiar áreas abertas, as obrigações ao abrigo da legislação da UE em matéria de proteção de dados têm de ser cumpridas não só para os suspeitos, mas também para todos aqueles que são objeto de vigilância na prática.

32. Por todos estes motivos, o CEPD e a AEPD **apelam à proibição geral de qualquer utilização de IA para o reconhecimento automatizado de características humanas em espaços acessíveis ao público (tal como de rostos, mas também do andar, de impressões digitais, do ADN, da voz, da digitação e de outros sinais comportamentais ou biométricos) em qualquer contexto**. A abordagem atual da proposta consiste em identificar e enumerar todos os sistemas de IA que devem ser proibidos. Assim, por uma questão de coerência, os **sistemas de IA para a identificação à distância em grande escala em espaços em linha** devem ser proibidos nos termos do artigo 5.º da proposta. Tendo em conta a PDAL, o RPDUE e o RGPD, o CEPD e a AEPD não conseguem discernir de que forma este tipo de prática poderia cumprir os requisitos de necessidade e proporcionalidade, sendo que tal decorre, em última análise, do

que são consideradas interferências aceitáveis dos direitos fundamentais pelo TJUE e pelo TEDH.

33. Além disso, o CEPD e a AEPD **recomendam a proibição**, aplicável tanto a autoridades públicas como a entidades privadas, dos **sistemas de IA que categorizem, com base na biometria (por exemplo, reconhecimento do rosto), as pessoas singulares em grupos de acordo com a origem étnica, o género, bem como a orientação sexual ou política, ou outras razões de discriminação proibidas nos termos do artigo 21.º da Carta ou** dos sistemas de IA cuja validade científica não esteja demonstrada ou que estejam em conflito direto com os valores fundamentais da UE [por exemplo, polígrafo, anexo III, ponto 6, alínea b), e ponto 7, alínea a)]. Em conformidade, a «**categorização biométrica**» deve ser **proibida ao abrigo do artigo 5.º**.

34. Do mesmo modo, **a dignidade humana é afetada ao ser determinada ou classificada por um computador quanto ao comportamento futuro independente da livre vontade de uma pessoa**. Os sistemas de IA concebidos para serem utilizados por autoridades policiais em avaliações individuais de riscos relativamente a pessoas singulares, a fim de determinar o risco de uma pessoa singular cometer ou voltar a cometer infrações penais [cf. anexo III, ponto 6, alínea a)], ou para prever a ocorrência ou a recorrência de uma infração penal real ou potencial com base na definição de perfis de pessoas singulares, ou para avaliar os traços de personalidade e as características ou o comportamento criminal passado [cf. anexo III, ponto 6, alínea e)], utilizados de acordo com a finalidade prevista, conduzirão a uma subordinação crucial das decisões policiais e judiciais, objetificando assim o ser humano afetado. Tais sistemas de IA que se aproximam da essência do direito à dignidade humana devem ser proibidos ao abrigo do artigo 5.º.

35. O CEPD e a AEPD consideram ainda que a utilização de IA para **inferir as emoções de uma pessoa singular é extremamente indesejável e deve ser proibida,** salvo em determinados casos de utilização bem especificados, nomeadamente para efeitos de investigação ou no domínio da saúde (por exemplo, doentes em relação aos quais o reconhecimento de emoções é importante), sempre com salvaguardas adequadas em vigor e, claro, sujeita a todas as outras condições e limites em matéria de proteção de dados, incluindo limitação das finalidades.

2.4 Sistemas de IA de risco elevado

2.4.1 Necessidade de uma avaliação da conformidade *ex ante* por terceiros externos

36. O CEPD e a AEPD congratulam-se com o facto de que os sistemas de IA que representam um risco elevado devem ser sujeitos a uma avaliação prévia da conformidade antes de poderem ser colocados no mercado ou de outro modo colocados em serviço na UE. Em princípio, este modelo regulamentar é acolhido com agrado, uma vez que oferece um bom equilíbrio entre inovação e facilidade de utilização, bem como um elevado nível de proteção proativa dos direitos fundamentais. Para a sua colocação em funcionamento em ambientes específicos, tais como processos de decisão de instituições de serviço público ou infraestruturas críticas, é necessário definir formas para investigar o código-fonte completo.

37. Contudo, o CEPD e a AEPD defendem a adaptação do procedimento de avaliação da conformidade nos termos do artigo 43.º da proposta no sentido de que uma **avaliação da conformidade *ex ante* por terceiros deve ser geralmente efetuada em relação a IA de elevado risco**. Embora uma avaliação da conformidade por terceiros relativamente ao tratamento de dados pessoais de elevado risco não seja uma exigência do RGPD ou RPDUE, os riscos decorrentes dos sistemas de IA não são ainda totalmente compreendidos. A inclusão geral de uma obrigação de avaliação da conformidade por terceiros reforçaria assim ainda mais a segurança jurídica e a confiança em todos os sistemas de IA de risco elevado.

2.4.2 O âmbito de aplicação do regulamento deve abranger igualmente os sistemas de IA já em utilização

38. Segundo o artigo 43.º, n.º 4, da proposta, os sistemas de IA de risco elevado devem ser sujeitos a um novo procedimento de avaliação da conformidade sempre que seja efetuada uma alteração significativa. É correto garantir que os sistemas de IA cumprem os requisitos do regulamento relativo à IA ao longo de todo o ciclo de vida. Os sistemas de IA que sejam colocados no mercado ou em serviço antes da aplicação da proposta de regulamento (ou 12 meses após essa data no que diz respeito aos sistemas informáticos de grande escala enumerados no anexo IX) não são abrangidos pelo seu âmbito de aplicação, salvo se os referidos sistemas forem sujeitos a «alterações significativas» em termos de conceção ou finalidade prevista (artigo 83.º).

39. Porém, o limiar das «alterações significativas» não é claro. O considerando 66 da proposta especifica um limiar inferior para a reavaliação da conformidade sempre que seja efetuada uma alteração de maneira que possa afetar o cumprimento. Um limiar semelhante seria adequado para o artigo 83.º, pelo menos relativamente aos sistemas de IA de risco elevado. Além disso, a fim de colmatar lacunas no domínio da proteção, é necessário que os sistemas de IA já criados e em funcionamento – após uma fase de execução determinada – cumpram igualmente todos os requisitos do regulamento relativo à IA.

40. As diversas possibilidades de tratamento de dados pessoais e riscos externos também afetam a segurança dos sistemas de IA. A ênfase do artigo 83.º nas «alterações significativas em termos de conceção ou finalidade prevista» não inclui nenhuma referência às alterações em termos de riscos externos. Por conseguinte, deve ser incluída no artigo 83.º da proposta uma referência às alterações no contexto das ameaças, decorrentes dos riscos externos (por exemplo, ciberataques, ataques antagónicos e queixas fundamentadas de consumidores).

41. Além disso, uma vez que a entrada em aplicação está prevista para 24 meses após a entrada em vigor do futuro regulamento, o CEPD e a AEPD não consideram adequado isentar os sistemas de IA já colocados no mercado por um período ainda mais longo. Embora a proposta preveja igualmente que os requisitos do regulamento devem ser tidos em conta na avaliação de cada sistema informático de grande escala, conforme previsto nos atos jurídicos enumerados no anexo IX, o CEPD e a AEPD consideram que os requisitos relativos à colocação em serviço e utilização de sistemas de IA devem ser aplicáveis a partir da data de aplicação do futuro regulamento.

2.5 Governação e Comité Europeu para a Inteligência Artificial

2.5.1 Governação

42. O CEPD e a AEPD congratulam-se com a designação da AEPD como autoridade competente e autoridade de fiscalização do mercado para a supervisão das instituições, órgãos e organismos da União sempre que estes estejam abrangidos pelo âmbito de aplicação da presente proposta. A AEPD está disposta a preencher o seu novo papel de regulador da IA para a administração pública da UE. Além disso, o papel e as funções da AEPD não são suficientemente pormenorizados e devem ser clarificados na proposta, especificamente no que se refere ao seu papel de autoridade de fiscalização do mercado.

43. O CEPD e a AEPD reconhecem na proposta a atribuição de recursos financeiros, que está prevista para o Comité e a AEPD na qualidade de organismo notificador. No entanto, o exercício das novas funções previstas para a AEPD, na qualidade de organismo notificador, exigiria recursos financeiros e humanos significativamente mais elevados.

44. Em primeiro lugar, a redação do artigo 63.º, n.º 6, estabelece que a AEPD «deve atuar como a autoridade de fiscalização do mercado» relativamente às instituições, órgãos e organismos da União que se insiram no âmbito da proposta, o que não clarifica se a AEPD deve ser considerada uma «autoridade de fiscalização do mercado» plenamente incorporada, tal como previsto no Regulamento (UE) 2019/1020. O que precede levanta questões sobre as funções e competências da AEPD na prática. Em segundo lugar, e desde que a resposta à questão anterior seja afirmativa, é pouco claro o modo como o papel da AEPD, conforme previsto no RPDUE, pode conciliar as funções estipuladas no artigo 11.º do Regulamento (UE) 2019/1020, que incluem «a fiscalização eficaz do mercado no seu território dos produtos disponibilizados em linha» ou «controlos físicos e laboratoriais baseados em amostras adequadas». Ao aceitar o novo conjunto de funções sem incluir uma melhor clarificação na proposta, existe o risco de poder comprometer o cumprimento das suas obrigações como autoridade para a proteção de dados.

45. Contudo, o CEPD e a AEPD salientam que determinadas disposições da proposta que definem as funções e competências das diferentes autoridades competentes nos termos do regulamento relativo à IA, as suas relações, a sua natureza e a garantia da sua independência parecem, nesta fase, pouco claras. Embora o Regulamento (UE) 2019/1020 estabeleça que a autoridade de fiscalização do mercado deve ser independente, a proposta de regulamento não requer que as autoridades de controlo sejam independentes, exigindo mesmo que informem a Comissão sobre determinadas funções executadas pelas autoridades de fiscalização do mercado, que podem ser diferentes instituições. Dado que a proposta determina ainda que as autoridades de proteção de dados atuarão como as autoridades de fiscalização do mercado para os sistemas de IA utilizados para efeitos de manutenção da ordem pública (artigo 63.º, n.º 5), tal significa igualmente que estarão, possivelmente através da respetiva autoridade nacional de controlo, sujeitas às obrigações de comunicação à Comissão (artigo 63.º, n.º 2), o que se afigura incompatível com a sua independência.

46. Por conseguinte, o CEPD e a AEPD consideram que as disposições em causa devem ser clarificadas, a fim de serem coerentes com o Regulamento (UE) 2019/1020, o RPDUE e o RGPD, sendo que a proposta deve estabelecer claramente que as autoridades de controlo ao abrigo do regulamento relativo à IA devem ser completamente independentes no exercício das suas funções, uma vez que tal seria uma garantia essencial para a adequada supervisão e execução do futuro regulamento.

47. O CEPD e a AEPD gostariam também de recordar que as autoridades de proteção de dados já aplicam o RGPD, o RPDUE e a PDAL aos sistemas de IA que envolvem dados pessoais, a fim de garantir a proteção dos direitos fundamentais e, mais especificamente, o direito à proteção de dados. Assim, conforme exigido na proposta para as autoridades nacionais de controlo, as autoridades de proteção de dados já dispõem, até certo ponto, de conhecimentos relativos às tecnologias de IA, aos dados e à computação de dados e aos direitos fundamentais, bem como de experiência na avaliação dos riscos para os direitos fundamentais decorrentes das novas tecnologias. Além disso, sempre que os sistemas de IA tenham por base o tratamento de dados pessoais ou efetuem o tratamento de dados pessoais, as disposições da proposta estão diretamente ligadas ao quadro jurídico em matéria de proteção de dados, que será o caso na maior parte dos sistemas de IA abrangidos pelo âmbito de aplicação do regulamento. Em resultado, existirão interligações de competências entre as autoridades de controlo ao abrigo da proposta e as autoridades de proteção de dados.

48. Por conseguinte, a designação das autoridades de proteção de dados como autoridades nacionais de controlo asseguraria uma abordagem regulamentar mais harmonizada, bem como contribuiria para a interpretação coerente das disposições relativas ao tratamento de dados e evitaria contradições na sua aplicação nos Estados-Membros. Seria igualmente vantajoso para todas as partes interessadas da cadeia de valor da IA dispor de um ponto de contacto único para todas as operações de tratamento de dados pessoais que se enquadrem no âmbito de aplicação da proposta, bem como limitar as interações entre dois organismos de regulação diferentes para o tratamento visados pela proposta e pelo RGPD. Consequentemente, o CEPD e a AEPD consideram que **as autoridades de proteção de dados devem ser designadas como autoridades nacionais de controlo nos termos do artigo 59.º da proposta.**

49. Em todo o caso, na medida em que a proposta contém regras específicas aplicáveis à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais adotadas com base no artigo 16.º do TFUE, o cumprimento das referidas regras – nomeadamente restrições à utilização de sistemas de IA para a identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de manutenção da ordem pública – **deve ficar sujeito ao controlo de autoridades independentes**.

50. Contudo, não existe uma disposição explícita na proposta que atribua competências para assegurar o cumprimento das regras em causa ao controlo de autoridades independentes. A única referência às autoridades de controlo no domínio da proteção de dados, designadas nos termos do RGPD ou da PDAL, encontra-se no artigo 63.º, n.º 5, da proposta, mas apenas como organismos «de fiscalização do mercado» e, em alternativa, com algumas outras autoridades. O CEPD e a AEPD consideram que este quadro não assegura o cumprimento dos requisitos de controlo independente estabelecidos no artigo 16.º, n.º 2, do TFUE e no artigo 8.º da Carta.

2.5.2 Comité Europeu para a Inteligência Artificial

51. A proposta cria um Comité Europeu para a Inteligência Artificial (EAIB, «European Artificial Intelligence Board»). O CEPD e a AEPD reconhecem a necessidade de uma aplicação coerente e harmonizada do quadro proposto, bem como da participação de peritos independentes no desenvolvimento da política da UE em matéria de IA. Ao mesmo tempo, a proposta prevê a atribuição de um papel predominante à Comissão. De facto, a Comissão não só faria parte do EAIB como também o presidiria, tendo direito de veto na adoção do regulamento interno do EAIB. O que precede entra em conflito com a necessidade de um organismo europeu de IA independente de qualquer influência política. Por este motivo, o CEPD e a AEPD consideram que o futuro regulamento relativo à IA deve conferir **mais autonomia ao EAIB**, a fim de permitir que o mesmo assegure efetivamente a aplicação coerente do regulamento em todo o mercado único.

52. O CEPD e a AEPD constatam igualmente que não são conferidos poderes ao EAIB relativamente à execução da proposta de regulamento. Porém, tendo em conta a disseminação dos sistemas de IA em todo o mercado único e a probabilidade de casos transfronteiriços, é absolutamente necessária uma aplicação harmonizada e uma repartição adequada de competências entre as autoridades nacionais de controlo. O CEPD e a AEPD recomendam, portanto, que os mecanismos de cooperação entre as autoridades nacionais de controlo sejam especificados no futuro regulamento relativo à IA. O CEPD e a AEPD propõem impor um mecanismo que garanta um ponto de contacto único para as pessoas singulares visadas pela legislação, bem como para as empresas, por cada sistema de IA, sendo que, no que diz respeito a organizações cuja atividade abranja mais de metade dos Estados-Membros da UE, o EAIB pode designar a autoridade nacional que ficará responsável pela execução do regulamento relativo à IA quanto ao sistema de IA em causa.

53. Tendo ainda em conta a natureza independente das autoridades que constituem o Comité, este último deverá poder agir por sua própria iniciativa e não apenas prestar aconselhamento e assistência à Comissão. O CEPD e a AEPD salientam, portanto, a necessidade de prorrogar a missão confiada ao Comité, que, além disso, não corresponde às funções constantes da proposta.

54. A fim de satisfazer tais objetivos, o **EAIB deve dispor de competências suficientes e adequadas**, devendo o seu estatuto jurídico ser clarificado. De modo que, em particular, o âmbito material do futuro regulamento se mantenha pertinente, parece necessário envolver as autoridades responsáveis pela sua aplicação na respetiva evolução. Assim, o CEPD e a AEPD recomendam que o EAIB fique habilitado a propor à Comissão alterações ao anexo I, que define as técnicas e abordagens no domínio da IA, e ao anexo III, que enumera os sistemas de IA de risco elevado a que se refere o artigo 6.º, n.º 2. O EAIB deve ser igualmente consultado pela Comissão antes de qualquer alteração dos referidos anexos.

55. O artigo 57.º, n.º 4, da proposta prevê intercâmbios entre o Comité e outras instituições, órgãos, organismos e grupos consultivos da União. Tendo em conta o seu trabalho anterior na área da IA e os seus conhecimentos no domínio dos direitos humanos, o CEPD e a AEPD recomendam que a Agência dos Direitos Fundamentais seja considerada um dos observadores do Comité.

3 INTERAÇÃO COM O QUADRO DE PROTEÇÃO DE DADOS

3.1 Relação entre a proposta e a atual legislação da UE em matéria de proteção de dados

56. Uma relação claramente definida entre a proposta e a atual legislação em matéria de proteção de dados é uma condição prévia essencial para garantir e apoiar o respeito e a aplicação do acervo da União no domínio da proteção de dados pessoais. A legislação da UE em causa (nomeadamente o RGPD, o RPDUE e a PDAL) deve ser considerada uma condição prévia que poderá servir de base para novas propostas legislativas sem influenciar ou interferir com as disposições em vigor, incluindo no que diz respeito às competências das autoridades de controlo e à governação.

57. Como tal, na perspetiva do CEPD e da AEPD, importa evitar claramente incoerências na proposta, bem como eventuais conflitos com o RGPD, o RPDUE e a PDAL. Tal é importante não só por motivos de segurança jurídica, como também para evitar que a proposta prejudique, direta ou indiretamente, o direito fundamental à proteção de dados pessoais, conforme estabelecido no artigo 16.º do TFUE e no artigo 8.º da Carta.

58. Em particular, as máquinas com autoaprendizagem apenas poderiam proteger os dados pessoais das pessoas singulares se tal fosse incorporado desde a conceção. É igualmente essencial que as pessoas singulares disponham da possibilidade imediata de exercer os direitos nos termos do artigo 22.º (decisões individuais automatizadas, incluindo definição de perfis) do RGPD ou do artigo 23.º do RPDUE, independentemente das finalidades do tratamento. Neste sentido, é necessário incluir nos sistemas de IA, logo de início, outros direitos dos titulares dos dados relacionados com o direito de retificação e apagamento de acordo com a legislação em matéria de proteção de dados, independentemente da abordagem selecionada no domínio da IA ou da arquitetura técnica.

59. A utilização de dados pessoais para a aprendizagem de sistemas de IA pode conduzir à criação de padrões de decisões enviesadas no núcleo do sistema de IA. Como tal, estes processos devem contar com várias salvaguardas e, nomeadamente, uma supervisão humana qualificada, a fim de garantir que os direitos dos titulares dos dados são respeitados e assegurados, bem como para evitar quaisquer efeitos adversos para as pessoas singulares. As autoridades competentes devem também poder propor orientações para avaliar o enviesamento dos sistemas de IA e auxiliar no exercício da supervisão humana.

60. Sempre que os seus dados sejam utilizados no treino de IA e/ou em previsões, os titulares dos dados devem ser informados da base jurídica para o tratamento em causa, da explicação geral da lógica (procedimento) e do âmbito do sistema de IA. Neste contexto, os direitos das pessoas singulares à limitação do tratamento (artigo 18.º do RGPD e artigo 20.º do RPDUE) e ao apagamento dos dados (artigo 16.º do RGPD e artigo 19.º do RPDUE) devem ser sempre assegurados. Além disso, o responsável pelo tratamento deve ser expressamente obrigado a informar o titular dos dados sobre os prazos aplicáveis à objeção, à limitação, ao apagamento

dos dados, entre outros. O sistema de IA deve cumprir todos os requisitos em matéria de proteção de dados através de medidas técnicas e organizacionais adequadas. O direito a uma explicação deve proporcionar uma transparência suplementar.

3.2 Ambiente de testagem e tratamento adicional (artigos 53.º e 54.º da proposta)

61. Dentro dos limites legais e morais existentes, é importante promover a inovação europeia através de ferramentas como os ambientes de testagem. Um ambiente de testagem oferece a oportunidade de introduzir as salvaguardas necessárias para desenvolver a confiança nos sistemas de IA. Em ambientes complexos, os profissionais da IA poderão ter dificuldade em ponderar todos os interesses de forma adequada. Especialmente no que diz respeito às pequenas e médias empresas com recursos limitados, o funcionamento dos ambientes de testagem da regulamentação podem produzir ideias mais rapidamente e, assim, promover a inovação.

62. O artigo 53.º, n.º 3, da proposta determina que os ambientes de testagem não afetam os poderes de supervisão e de correção. Caso esta clarificação seja útil, é igualmente necessário elaborar diretrizes ou orientações sobre como alcançar um bom equilíbrio entre ser uma autoridade de controlo, por um lado, e dar orientações pormenorizadas através de um ambiente de testagem, por outro lado.

63. O artigo 53.º, n.º 6, especifica que as modalidades e condições de funcionamento dos ambientes de testagem devem ser estabelecidas em atos de execução. É importante elaborar orientações específicas com vista a assegurar a coerência e o apoio no âmbito do estabelecimento e funcionamento dos ambientes de testagem. Contudo, os atos de execução vinculativos poderiam limitar a capacidade de cada Estado-Membro para personalizar o ambiente de testagem de acordo com as suas necessidades e práticas locais. Deste modo, o CEPD e a AEPD recomendam que o EAIB forneça, em vez disso, orientações para os ambientes de testagem.

64. O artigo 54.º da proposta visa proporcionar uma base jurídica para o tratamento adicional de dados pessoais para efeitos de desenvolvimento de certos sistemas de inteligência artificial de interesse público no ambiente de testagem da regulamentação da inteligência artificial. A relação do artigo 54.º, n.º 1, da proposta com o artigo 54.º, n.º 2, e o considerando 41 da proposta e, por conseguinte, também com a atual legislação da UE em matéria de proteção de dados continua a ser pouco clara. Contudo, o RGPD e o RPDUE já têm uma base estabelecida para «tratamento posterior». Nomeadamente no que diz respeito a casos em que seja do interesse público permitir um tratamento adicional, a consecução de um equilíbrio entre os interesses do responsável pelo tratamento e os interesses do titular dos dados não tem de prejudicar a inovação. Atualmente, o artigo 54.º da proposta não aborda duas importantes questões: i) os interesses dos titulares dos dados são ponderados em que circunstâncias, utilizando que critérios (adicionais), e ii) se os sistemas de IA apenas serão utilizados no ambiente de testagem. O CEPD e a AEPD congratulam-se com a exigência de um direito da União ou do Estado-Membro ao efetuar o tratamento de dados pessoais recolhidos nos termos da PDAL num ambiente de testagem; contudo, recomendam especificar o que se pretende, em conformidade com o RGPD e o RPDUE, clarificando sobretudo que a base jurídica dos ambientes de testagem em causa deve cumprir os requisitos estabelecidos no artigo 23.º, n.º 2,

do RGPD e no artigo 25.º do RPDUE. Do mesmo modo, recomendam explicitar que todas as utilizações do ambiente de testagem devem ser sujeitas a uma avaliação aprofundada. Tal é igualmente aplicável à lista completa de condições constante do artigo 54.º, n.º 1, alíneas b) a j).

65. Algumas considerações suplementares relativas à reutilização de dados nos termos do artigo 54.º da proposta indicam que o funcionamento de um ambiente de testagem tem um consumo intensivo de recursos e que, por conseguinte, é realista estimar que apenas um pequeno número de empresas teria oportunidade de participar. A participação no ambiente de testagem pode ser uma vantagem competitiva. Para permitir a reutilização de dados, seria necessária uma consideração cuidadosa sobre a forma como os participantes são selecionados, a fim de garantir que estes se enquadram no âmbito de aplicação e evitar a desigualdades de tratamento. O CEPD e a AEPD receiam que permitir a reutilização de dados no quadro do ambiente de testagem seja um desvio da abordagem de responsabilidade ao abrigo do RGPD, em que a responsabilidade cabe ao responsável pelo tratamento, não à autoridade competente.

66. Tendo em conta os objetivos do ambiente de testagem, que consistem em desenvolver, testar e validar os sistemas de IA, o CEPD e a AEPD consideram ainda que os ambientes de testagem não podem ser abrangidos pelo âmbito da PDAL. Embora a PDAL preveja a reutilização de dados para efeitos de investigação científica, os dados tratados para essa finalidade secundária estarão sujeitos ao RGPD ou RPDUE, deixando de estar sujeitos à PDAL.

67. Não é claro o que um ambiente de testagem da regulamentação irá englobar. Coloca-se a questão de saber se o ambiente de testagem da regulamentação proposto inclui uma infraestrutura informática em cada Estado-Membro com determinados fundamentos jurídicos suplementares para o tratamento adicional ou se apenas organiza o acesso a orientações e conhecimentos especializados no domínio da regulamentação. O CEPD e a AEPD exortam o legislador a clarificar este conceito na proposta e a indicar expressamente na mesma que o ambiente de testagem não obriga as autoridades competentes a fornecerem as suas infraestruturas técnicas. Em todos os casos, devem ser fornecidos recursos humanos e financeiros às autoridades competentes em conformidade com a clarificação referida.

68. Por fim, o CEPD e a AEPD gostariam de destacar o desenvolvimento de sistemas de IA transfronteiras que estarão disponíveis no mercado único digital europeu no seu conjunto. No caso de tais sistemas de IA, o ambiente de testagem da regulamentação enquanto ferramenta para a inovação não deve tornar-se um obstáculo para o desenvolvimento transfronteiras. Consequentemente, o CEPD e a AEPD recomendam uma abordagem transfronteiras coordenada que ainda esteja suficientemente disponível a nível nacional para todas as PME, proporcionando um quadro comum em toda a Europa sem ser demasiado restritivo. É necessário alcançar um equilíbrio entre a coordenação europeia e os procedimentos nacionais, a fim de evitar uma execução contraditória do futuro regulamento relativo à IA que prejudicaria a inovação à escala da UE.

3.3 Transparência

69. O CEPD e a AEPD congratulam-se com o facto de que os sistemas de IA de risco elevado devem ser registados numa base de dados pública (mencionada nos artigos 51.º e 60.º da proposta). A referida base de dados deve ser encarada como uma oportunidade para fornecer informações ao público em geral sobre o âmbito de aplicação dos sistemas de IA e sobre falhas conhecidas e incidentes que possam comprometer o seu funcionamento, incluindo os recursos adotados pelos fornecedores para dar resposta e resolver os mesmos.

70. Um princípio democrático fundamental consiste em recorrer à verificação e comprovação. Assim, o facto de a obrigação de transparência não ser aplicável aos sistemas de IA utilizados para detetar, prevenir, investigar e reprimir infrações penais constitui uma exceção demasiado ampla. É necessário estabelecer uma distinção entre os sistemas de IA que são utilizados para deteção ou prevenção e os sistemas de IA concebidos para investigar ou auxiliar na repressão de infrações penais. As salvaguardas da prevenção e deteção devem ser mais rigorosas devido à presunção de inocência. Além disso, o CEPD e a AEPD lamentam a ausência de medidas de coação na proposta, o que pode ser interpretado como uma luz verde para a utilização até mesmo de sistemas ou aplicações de IA de risco elevado que não tenham sido comprovados.

71. Nos casos em que pouca ou nenhuma transparência pode ser dada ao público por motivos de sigilo, mesmo numa democracia efetiva, devem ser estabelecidas salvaguardas e os sistemas de IA em causa devem ser registados com transparência, bem como devem proporcionar transparência à autoridade de controlo competente.

72. A garantia da transparência nos sistemas de IA é um objetivo extremamente exigente. A abordagem de decisões totalmente quantitativa de vários sistemas de IA, inerentemente diferente da abordagem humana que se baseia principalmente no raciocínio causal e teórico, pode entrar em conflito com a necessidade de obter uma explicação prévia compreensível dos resultados automáticos. O regulamento deve promover novas formas mais proativas e oportunas de informar os utilizadores de sistemas de IA sobre o estatuto (das decisões) em que o sistema se encontra em qualquer momento, fornecendo um alerta precoce de potenciais resultados prejudiciais, de modo que as pessoas singulares cujos direitos e liberdades possam ser prejudicados pelas decisões autónomas da máquina possam reagir ou recorrer da decisão.

3.4 Tratamento de categorias especiais de dados e dados relativos às infrações penais

73. O tratamento de categorias especiais de dados no domínio da manutenção da ordem pública é regido pelas disposições do quadro de proteção de dados da UE, incluindo a PDAL, bem como pela respetiva aplicação nacional. A proposta argumenta que não fornece um fundamento jurídico geral para o tratamento de dados pessoais, incluindo de categorias especiais de dados pessoais (cf. considerando 41). Simultaneamente, o artigo 10.º, n.º 5, da proposta afirma que «os fornecedores desses sistemas podem tratar categorias especiais de dados pessoais». Além disso, a mesma disposição exige salvaguardas adicionais, apresentando também exemplos. Assim, a proposta parece interferir com a aplicação do RGPD, da PDAL e do RPDUE. Embora o CEPD e a AEPD se congratulem com a tentativa de providenciar salvaguardas adequadas, é necessária uma abordagem regulamentar mais coerente, uma vez que as disposições atuais não parecem

suficientemente claras para criar uma base jurídica para o tratamento de categorias especiais de dados, devendo ser complementadas com medidas de proteção adicionais que ainda têm de ser avaliadas. Além disso, sempre que os dados pessoais tenham sido recolhidos através do tratamento no âmbito da PDAL, é necessário ter em conta as eventuais salvaguardas e limitações adicionais decorrentes das transposições nacionais da PDAL.

3.5 Mecanismos de conformidade

3.5.1 Certificação

74. Um dos principais pilares da proposta é a certificação. O sistema de certificação descrito na proposta assenta numa estrutura de entidades (autoridades notificadoras/organismos notificados/Comissão) e numa avaliação da conformidade/procedimento de certificação que abrange os requisitos obrigatórios aplicáveis aos sistemas de IA de risco elevado, bem como tem por base normas harmonizadas europeias ao abrigo do Regulamento (UE) n.º 1025/2012 e especificações comuns a serem estabelecidas pela Comissão. Este mecanismo é diferente do sistema de certificação destinado a assegurar a conformidade com as regras e os princípios em matéria de proteção de dados, previstos nos artigos 42.º e 43.º do RGPD. Contudo, é pouco clara a forma como os certificados emitidos pelos organismos notificados em conformidade com a proposta podem interagir com procedimentos de certificação, selos e marcas de proteção de dados previstos no RGPD, ao contrário do que está previsto para outros tipos de certificações [consultar o artigo 42.º, n.º 2, no que se refere às certificações emitidas ao abrigo do Regulamento (UE) 2019/881].

75. Na medida em que os sistemas de IA de risco elevado têm por base o tratamento de dados pessoais ou efetuam o tratamento de dados pessoais para cumprir a sua função, estes desvios podem criar insegurança jurídica relativamente a todos os organismos envolvidos, uma vez que podem conduzir a situações em que os sistemas de IA, certificados ao abrigo da proposta e marcados com uma marcação de conformidade CE, após colocados no mercado ou em serviço, podem ser utilizados de uma forma não conforme com as regras e os princípios de proteção de dados.

76. A proposta carece de uma relação clara com a legislação em matéria de proteção de dados, bem como com outras legislações da UE e dos Estados-Membros aplicáveis a cada «domínio» do sistema de IA de risco elevado constante do anexo III. Nomeadamente, a proposta deve incluir os princípios de minimização de dados e de proteção de dados desde a conceção enquanto um dos aspetos a ter em conta antes de obter a marcação CE, dado o possível nível elevado de interferência dos sistemas de IA de risco elevado com os direitos fundamentais à privacidade e à proteção dos dados pessoais, bem como a necessidade de garantir um elevado nível de confiança no sistema de IA. Assim, o CEPD e a AEPD recomendam alterar a proposta por forma a clarificar a relação entre os certificados emitidos ao abrigo do referido regulamento e os procedimentos de certificação, selos e marcas de proteção de dados. Por fim, as autoridades de proteção de dados devem participar na preparação e no estabelecimento de normas harmonizadas e especificações comuns.

77. Em articulação com o artigo 43.º da proposta, no que diz respeito à avaliação da conformidade, a derrogação do procedimento de avaliação da conformidade estabelecida no artigo 47.º parece ser muito abrangente, incluindo demasiadas exceções, tal como por motivos excecionais de segurança pública ou de proteção da vida e da saúde das pessoas, de proteção do ambiente e de proteção de ativos industriais e infraestruturas essenciais. Propomos que os legisladores reduzam as exceções.

3.5.2 Códigos de conduta

78. De acordo com o artigo 69.º da proposta, a Comissão e os Estados-Membros devem incentivar e facilitar a elaboração de códigos de conduta destinados a fomentar a aplicação voluntária dos requisitos aplicáveis a sistemas de IA de risco elevado, bem como de requisitos adicionais, por parte dos fornecedores de sistemas de IA que não são de risco elevado. Em conformidade com o considerando 78 do RGPD, o CEPD e a AEPD recomendam identificar e definir sinergias entre estes instrumentos e os códigos de conduta previstos no RGPD, que apoiam o cumprimento em matéria de proteção de dados. Neste contexto, importa clarificar se a proteção de dados pessoais deve ser considerada como parte dos «requisitos adicionais» que podem ser abordados pelos códigos de conduta a que se refere o artigo 69.º, n.º 2. Importa igualmente garantir que as «especificações técnicas e soluções», abordadas nos códigos de conduta a que se refere o artigo 69.º, n.º 1, conforme elaboradas para fomentar o cumprimento dos requisitos da proposta de regulamento relativo à IA, não entram em conflito com as regras e os princípios do RGPD e do RPDUE. Deste modo, a adesão às ferramentas em questão por parte dos fornecedores de sistemas de IA que não são de risco elevado – na medida em que tais sistemas têm por base o tratamento de dados pessoais ou efetuam o tratamento de dados pessoais para cumprir a sua função – representaria um valor acrescentado, uma vez que tal garantirá que o responsável pelo tratamento e os subcontratantes cumprirão as suas obrigações em matéria de proteção de dados na utilização desses sistemas.

79. Ao mesmo tempo, o quadro jurídico para uma inteligência artificial de confiança seria complementado pela incorporação dos códigos de conduta, por forma a promover a confiança na utilização desta tecnologia de um modo seguro e em conformidade com a lei, incluindo o respeito pelos direitos fundamentais. No entanto, a conceção de tais instrumentos deve ser reforçada, prevendo mecanismos que visem comprovar se os códigos em causa disponibilizam «especificações técnicas e soluções» efetivas e estabelecem «objetivos claros e indicadores-chave de desempenho que permitam medir a consecução desses objetivos» como parte integrante dos referidos códigos. Além disso, a ausência de qualquer referência aos mecanismos de controlo (obrigatórios) dos códigos de conduta destinados a verificar se os fornecedores de sistemas de IA que não são de risco elevado cumprem as suas disposições, bem como a possibilidade de os fornecedores a título individual criarem (e aplicarem autonomamente) os referidos códigos (consultar o ponto 5.2.7 da exposição de motivos), podem enfraquecer ainda mais a eficácia e a executoriedade destes instrumentos.

80. Por fim, o CEPD e a AEPD solicitam esclarecimentos relativamente aos tipos de iniciativas que a Comissão pode desenvolver, de acordo com o considerando 81 da proposta, «para facilitar a redução de obstáculos técnicos que impeçam o intercâmbio transfronteiras de dados para o desenvolvimento da inteligência artificial».

4 CONCLUSÃO

81. Embora o CEPD e a AEPD acolham positivamente a proposta da Comissão e sejam de opinião que tal regulamentação é necessária para assegurar os direitos fundamentais dos cidadãos e residentes da UE, consideram que a proposta carece de adaptação em diversas questões, a fim de garantir a sua aplicabilidade e eficiência.

82. Dada a complexidade da proposta e as questões que esta se propõe resolver, há ainda muito trabalho a fazer até que a proposta possa dar origem a um quadro jurídico efetivo, que complete de forma eficiente o RGPD na proteção dos direitos humanos fundamentais, promovendo simultaneamente a inovação. O CEPD e a AEPD continuarão a estar disponíveis para oferecer o seu apoio neste percurso.

Bruxelas, 18 de junho de 2021

Pelo Comité Europeu para a Proteção de Dados	Pela Autoridade Europeia para a Proteção de Dados
A Presidente	A Autoridade
Andrea JELINEK	Wojciech Rafał WIEWIÓROWSKI