RED IBEROAMERICANA DE PROTECCION DE DATOS

Red Iberoamericana
Rede Ibero-Americana

Normas ibero-americanas

sobre a utilização de dados pessoais em sistemas de inteligência artificial

BY NC SA

Publicado em
novembro de 2026

Preâmbulo

A inteligência artificial está a transformar profundamente a forma como os dados pessoais são recolhidos, utilizados e reutilizados. O seu desenvolvimento aumentou a capacidade de gerar inferências, automatizar decisões, reutilizar informação para novos fins e combinar grandes volumes de dados em contextos cada vez mais complexos. Estes avanços não alteram a vigência dos princípios de proteção de dados pessoais, mas exigem que se especifique a maneira como devem aplicar-se quando os tratamentos incorporam sistemas de inteligência artificial.

Com este propósito, e na sequência de um processo de elaboração, consulta e deliberação técnica em que participaram as suas autoridades-membros, a Rede Ibero-americana de Proteção de Dados aprova as presentes Normas Ibero-americanas sobre a utilização de dados pessoais em sistemas de inteligência artificial (IA) (doravante designadas como «a Norma»), concebidas como um instrumento orientador para promover uma interpretação comum do regime de proteção de dados no contexto da inteligência artificial no âmbito ibero-americano e contribuir para o desenvolvimento de uma inteligência artificial que respeite os direitos e as liberdades das pessoas.

A Norma constitui uma iniciativa pioneira, ao desenvolver de forma sistemática as especificidades introduzidas pela inteligência artificial na perspetiva da proteção de dados pessoais. Não cria um regime ético-jurídico paralelo para a inteligência artificial, nem pretende substituir as legislações nacionais ou as Normas de Proteção de Dados Pessoais dos Estados ibero-americanos. O seu objetivo é complementar esse quadro comum nos casos em que a utilização de sistemas de inteligência artificial suscita questões específicas, que exigem critérios adicionais para a aplicação dos princípios, direitos e obrigações próprios da proteção de dados, sem prejuízo dos requisitos adicionais estabelecidos pelas legislações nacionais. A Norma não reduz nem flexibiliza o nível de proteção reconhecido por esse quadro comum: as disposições específicas nela previstas funcionam assim como critérios adicionais para a sua aplicação e não como exceções ao mesmo.

A proteção dos dados pessoais constitui um direito fundamental das pessoas e assenta na autonomia informativa, entendida como a faculdade de decidir sobre a utilização dos próprios dados pessoais e de manter o controlo sobre o seu tratamento; o seu reconhecimento nos quadros legislativos da região responde à necessidade de preservar a dignidade humana, a autonomia pessoal, a igualdade e as demais liberdades que o tratamento da informação pode comprometer. A intensificação da capacidade de inferir, prever e decidir que caracteriza os sistemas de inteligência artificial torna especialmente imperativo preservar essa faculdade, uma vez que os tratamentos de dados que os incorporam podem produzir dados e decisões sobre a pessoa sem a sua intervenção direta e influenciar as decisões que a afetam. Essa condição de direito fundamental constitui o parâmetro a partir do qual as disposições da Norma devem ser lidas e interpretadas. A Norma não cria nem substitui os direitos reconhecidos pelo regime geral de proteção de dados e pelas legislações nacionais, mas especifica a forma como o seu exercício se concretiza quando o tratamento incorpora sistemas de inteligência artificial.

A Norma baseia-se num corpo normativo de referência já existente, ao qual faz referência através de expressões equivalentes, cujo âmbito é definido nas disposições gerais da Norma relativas ao seu objeto. A Norma não pretende substituir esse corpo nem antecipar as decisões que competem a cada ordenamento jurídico; a sua função é precisar como devem ser aplicadas as obrigações e garantias já existentes quando o tratamento incorpora sistemas de inteligência artificial. Entre os responsáveis

encontram-se os organismos do setor público, cuja atuação se rege, além disso, por regras próprias do ordenamento jurídico nacional em matéria de autorização do tratamento, comunicação de dados entre organismos ou a particulares, divulgação da informação e acesso à informação pública, bem como pelos deveres de transparência que esse ordenamento lhes imponha no que diz respeito à utilização de sistemas de inteligência artificial; de acordo com a sua natureza orientadora e complementar, a Norma é dirigida também a esses responsáveis, sem prejuízo dessas regras, sem as substituir nem condicionar e tendo em conta as particularidades que a ação pública confere aos tratamentos que incorporam sistemas de inteligência artificial.

A Norma parte de uma ideia essencial: o seu objeto não são os sistemas de inteligência artificial considerados de forma abstrata, mas sim os tratamentos de dados pessoais que os incorporam. Dessa premissa deriva a abordagem do ciclo de vida que estrutura o instrumento e que a Norma desenvolve ao abordar os tratamentos e o seu ciclo de vida, definindo as obrigações relativas a cada tratamento e às finalidades para as quais este é realizado. O princípio da lealdade assume, neste contexto, uma função de contraponto especialmente relevante, uma vez que a inteligência artificial pode acentuar a distância entre o momento em que as pessoas fornecem os seus dados pessoais e a forma como estes são posteriormente utilizados; o critério segundo o qual essa lealdade é avaliada é estabelecido na Norma ao regulamentar a lealdade, a finalidade e a compatibilidade.

A metodologia seguida responde a uma decisão deliberada de especialização normativa: a Norma aborda apenas as questões em que a inteligência artificial exige uma adaptação das regras gerais de proteção de dados e fornece critérios para resolver os problemas específicos que esta suscita, evitando duplicações desnecessárias.

Além disso, a Norma adota uma abordagem baseada no risco e na responsabilidade proativa. As medidas previstas devem ser aplicadas de forma proporcionada, tendo em conta a natureza do tratamento, os dados utilizados, as finalidades pretendidas, o contexto de utilização e o impacto que o tratamento possa ter sobre os direitos e liberdades das pessoas. Esta abordagem visa reforçar a proteção efetiva, sem impor encargos desnecessários nem entravar o desenvolvimento e a adoção responsável da inteligência artificial.

Esta abordagem aplica-se a operações de natureza e intensidade distintas: a determinação da base jurídica e, quando aplicável, a respetiva ponderação, a análise da necessidade e da proporcionalidade, a identificação e avaliação dos riscos para os direitos e liberdades das pessoas e a determinação das medidas adequadas para os gerir e, quando exigível, a avaliação de impacto. Estas operações respondem a finalidades próprias e são complementares entre si: nenhuma substitui as outras, embora os elementos documentados numa operação possam ser aproveitados noutra quando o seu objeto coincida, e a exigibilidade de cada uma obedeça à legislação aplicável ao tratamento, sem que a Norma altere o momento em que surge nem as condições a que está sujeita. O recurso ao interesse legítimo como base jurídica suscita, neste âmbito, dificuldades específicas: a escala em que os dados pessoais podem ser reutilizados, o intervalo de tempo entre o momento da sua recolha e o da sua posterior utilização, e o carácter pouco percetível que estes tratamentos costumam apresentar para as pessoas. Estas circunstâncias devem ser tidas em conta na avaliação, que deverá ser especialmente rigorosa quando, pela natureza dos dados, a escala do tratamento, os seus fins e os seus possíveis efeitos, possam surgir riscos acrescidos para os direitos e liberdades das pessoas. A graduação das medidas tem igualmente em conta os efeitos do tratamento dos dados sobre as pessoas, para o que a Norma emprega deliberadamente duas formulações distintas: quando exige efeitos jurídicos ou um impacto significativo,

delimita o caso de acordo com o significado que o regime geral de proteção de dados atribui a essas expressões, sem que o impacto significativo se limite a consequências de natureza jurídica, uma vez que abrange também as de ordem material, social ou económica que a utilização de sistemas de inteligência artificial é suscetível de produzir; quando se refere aos efeitos sem os qualificar, alude a qualquer consequência que o tratamento possa produzir sobre a pessoa, sem que isso implique uniformizar a intensidade das medidas exigíveis, que é determinada de acordo com o critério de proporcionalidade em relação aos riscos e não através de uma qualificação prévia dos efeitos.

Com esse mesmo objetivo, o texto utiliza formulações tecnologicamente neutras — ou seja, independentes de produtos, marcas ou fornecedores específicos — e evita impor soluções técnicas concretas quando basta definir o objetivo jurídico a atingir, sem que isso implique qualquer atenuação das garantias reconhecidas às pessoas. O seu objetivo é oferecer um quadro estável, capaz de acompanhar a evolução da inteligência artificial sem criar barreiras desnecessárias à inovação nem perder a sua utilidade como referência para as autoridades de proteção de dados, legisladores, responsáveis e encarregados do tratamento, fornecedores de sistemas de inteligência artificial e outras organizações dos setores público e privado.

A Norma será interpretada de forma coerente com o regime geral de proteção de dados, constituído pelas Normas de Proteção de Dados Pessoais para os Estados Ibero-americanos, com os demais documentos e critérios adotados pela Rede Ibero-americana de Proteção de Dados, com as legislações nacionais aplicáveis e com os instrumentos internacionais pertinentes, e tem como objetivo reforçar a convergência regulatória na região, facilitar a aplicação coerente da proteção de dados no contexto da inteligência artificial e promover um modelo de inovação responsável que coloque a confiança, a proteção das pessoas e o respeito pelos direitos fundamentais como condições essenciais para o desenvolvimento e a adoção da inteligência artificial.

Algumas manifestações da inteligência artificial suscitam uma preocupação específica e têm sido objeto de trabalhos específicos no seio da Rede Ibero-americana de Proteção de Dados e dos organismos internacionais especializados: a proteção dos dados pessoais de pessoas ou grupos em situação de vulnerabilidade, que ocupa um lugar próprio na tradição ibero-americana de proteção de dados, o tratamento de dados relativos à atividade neuronal e a geração de inferências sobre estados cognitivos, emocionais ou comportamentais, devido à sua capacidade de revelar aspetos particularmente íntimos da pessoa e ao seu impacto na autonomia individual, e o tratamento de dados biométricos e o reconhecimento ou a inferência de emoções. A Norma não substitui esse acervo nem o regime que as legislações nacionais atribuem a estas matérias, abordando apenas as particularidades que o seu tratamento apresenta, desde uma perspetiva de proteção dos dados pessoais, quando realizado através de sistemas de inteligência artificial. Os seus critérios sobre estas matérias serão interpretados em coerência com os referidos trabalhos e com a evolução do conhecimento científico disponível sobre a fiabilidade de ditos sistemas.

Capítulo I.
Disposições gerais, âmbito e critérios gerais de aplicação

1.1 Objeto

1.1.1. A Norma estabelece critérios orientadores para a proteção de dados pessoais nos tratamentos que incorporem sistemas de inteligência artificial ou que sejam necessários para o seu desenvolvimento, com o objetivo de reforçar a proteção das pessoas e promover uma aplicação harmonizada na região ibero-americana.

1.1.2. A Norma tem natureza orientadora e carácter complementar em relação ao regime geral de proteção de dados. As suas disposições aplicam-se sem prejuízo do estabelecido nas legislações aplicáveis e definem a forma como, de acordo com a Norma, devem ser aplicadas as obrigações e garantias de proteção de dados quando o tratamento envolve sistemas de inteligência artificial. As referências que a Norma faz ao regime geral de proteção de dados têm carácter esclarecedor, não condicionando nem delimitando a aplicação desse regime, que se aplica independentemente da Norma. Para efeitos da Norma, entende-se que as expressões «legislação em matéria de proteção de dados», «legislação aplicável» e «ordenamento jurídico aplicável» designam esse mesmo regime geral; as referências à legislação específica designam as disposições setoriais ou de âmbito específico que sejam adicionalmente aplicáveis, de acordo com cada ordenamento jurídico.

1.1.3 As referências da Norma ao regime geral de proteção de dados devem ser entendidas como referências ao ordenamento aplicável em cada caso e, como referência comum da região ibero-americana, às Normas de Proteção de Dados dos Estados Ibero-americanos.

1.2 Âmbito e condições de aplicação

1.2.1. A Norma aplica-se aos tratamentos de dados pessoais que incorporem sistemas de inteligência artificial ou que sejam necessários para o seu desenvolvimento, incluindo os dados pessoais inferidos ou derivados que estes gerem, independentemente de tais sistemas intervirem na totalidade ou em parte das operações que compõem o tratamento dos dados. A aplicação da Norma deverá ser proporcional aos riscos decorrentes do tratamento, de modo a não implicar obrigações desnecessárias quando esses riscos forem limitados, nem a atenuar as garantias exigíveis quando o tratamento dos dados implicar riscos elevados para os direitos e liberdades das pessoas.

1.2.2. Os âmbitos objetivo, subjetivo e territorial reger-se-ão pelo regime geral de proteção de dados, sem que a Norma altere a determinação da legislação aplicável que corresponda a cada ordenamento jurídico.

1.2.3. A Norma não será aplicável quando não forem tratados dados pessoais, nomeadamente nos casos de dados anonimizados nos termos exigidos pela Norma, dados sintéticos que não

permitam a identificação ou reidentificação das pessoas, e de modelos de inteligência artificial que não tratem nem permitam a obtenção de dados pessoais.

1.2.4. Quem invocar a inaplicabilidade da Norma deverá poder comprovar dita impossibilidade, independentemente do caso invocado, e dispor, para o efeito, da análise em que se baseia. Se, posteriormente, existir um risco razoável de identificação ou reidentificação, nos termos previstos na Norma, o tratamento ficará sujeito às disposições da mesma.

1.2.5. Quando, a partir de um modelo — incluindo os seus parâmetros e os resultados que produz —, for possível extrair, revelar ou atribuir razoavelmente os dados pessoais relativos a uma pessoa identificada ou identificável, o tratamento dos dados ficará sujeito à Norma.

1.3 Tratamentos e ciclo de vida

1.3.1. A aplicação da Norma abrangerá o tratamento de dados pessoais e as finalidades para as quais este é realizado, e não os sistemas ou modelos de inteligência artificial, nem as tecnologias em que se baseiam, considerados de forma abstrata.

1.3.2. A análise dos tratamentos que incorporem sistemas de inteligência artificial ou que sejam necessários para o seu desenvolvimento, independentemente da função que o sistema desempenhe nos mesmos, deverá ter em conta as diferentes fases do ciclo de vida do tratamento dos dados, com o fim de identificar as alterações que possam ocorrer nas finalidades, nos dados tratados, nos intervenientes ou nos riscos para as pessoas e determinar, em cada caso, as obrigações e garantias aplicáveis.

1.3.3. Para os efeitos previstos no número anterior, as referências da Norma ao desenvolvimento, treino, avaliação e melhoria designam fases distintas do ciclo de vida do tratamento dos dados. As obrigações e garantias aplicáveis, em particular as relativas à licitude, à minimização e à qualidade dos dados, devem determinar-se separadamente para cada uma delas.

1.4 Documentação do tratamento

1.4.1. Para comprovar o cumprimento da legislação em matéria de proteção de dados e da Norma, a documentação relativa ao tratamento de dados pessoais deve ser suficiente, tendo em conta a natureza, a complexidade e os riscos do tratamento.

1.4.2. Sempre que seja relevante para comprovar essa conformidade, a documentação poderá incluir as decisões tomadas sobre a conceção, a configuração ou a utilização do sistema de inteligência artificial.

1.4.3. Quando intervenham responsáveis pelo tratamento ou fornecedores de sistemas ou modelos de inteligência artificial, o responsável pelo tratamento dos dados deverá assegurar-se, através das relações jurídicas adequadas, de que dispõe da informação e da documentação necessárias sobre o sistema e, quando for relevante, sobre os tratamentos prévios realizados pelo

fornecedor, para cumprir as suas obrigações, incluindo as de transparência e explicabilidade, em conformidade com a legislação em matéria de proteção de dados e com a Norma. Esta informação deverá incluir, na medida do necessário, a relativa à proveniência, representatividade e condições de obtenção dos dados utilizados, às limitações conhecidas do sistema, aos enviesamentos identificados e às medidas de mitigação adotadas. Sempre que existam tratamentos de dados pessoais fornecidos pelo responsável pelo tratamento ou gerados ou inferidos durante a prestação do serviço, que excedam o objeto da prestação de serviços, deverá ser documentado, pelo menos, o cumprimento da legislação em matéria de proteção de dados no que diz respeito a estes tratamentos. As condições de utilização dos dados pelos fornecedores durante a relação regem-se pelo disposto na Norma relativa a intervenientes, a cadeia de valor e às transferências internacionais de dados.

1.5 Finalidades e reutilização de dados

1.5.1. Devem identificar-se, de forma diferenciada — sempre que impliquem tratamentos distintos ou uma reutilização dos dados para fins diferentes —, as finalidades operacionais do tratamento de dados pessoais e as de desenvolvimento, formação, avaliação ou melhoria e as finalidades instrumentais, como as de segurança ou prevenção da fraude.

1.5.2. Quando, no âmbito de um tratamento de dados que incorpore um sistema de inteligência artificial, os dados pessoais forem utilizados para uma finalidade diferente daquela para a qual foram obtidos, deverá verificar-se se essa utilização dispõe de uma base jurídica adequada e, quando aplicável, realizar a correspondente análise de compatibilidade, em conformidade com o regime geral de proteção de dados.

1.5.3. O treino, o ajuste ou o re-treino de modelos constituirão um tratamento diferenciado quando responderem a uma finalidade própria ou implicarem alterações relevantes na finalidade, nos dados utilizados, nos intervenientes ou nos riscos do tratamento.

1.6 Definições

1.6.1. Para efeitos da Norma no seu conjunto, e sem prejuízo do regime geral de proteção de dados, do qual se extraem os conceitos não definidos nesta secção — entre os quais os de responsável pelo tratamento, encarregado e corresponsável pelo tratamento dos dados, cuja determinação nos tratamentos que incorporem sistemas de inteligência artificial se rege pelo disposto na Norma sobre intervenientes, cadeia de valor e transferências internacionais —, entender-se-á por:

a) **Sistema de inteligência artificial:** conjunto integrado de componentes que, para objetivos explícitos ou implícitos e a partir de dados de entrada, gera previsões, inferências, recomendações, conteúdos ou decisões através da aprendizagem automática, do processamento estatístico ou de regras baseadas no conhecimento, com diferentes graus de autonomia.

b) **Modelo:** artefacto resultante do treino ou ajuste, que incorpora nos seus parâmetros padrões derivados dos dados utilizados e que, quando aplicado a novos dados, produz inferências ou previsões. O componente característico que define um sistema de inteligência artificial é a inclusão de um ou mais modelos.

c) **Inferência:** resultado que o sistema deduz, prevê ou estima a partir de dados de entrada, incluindo atributos, comportamentos, preferências ou categorias não fornecidos pelo titular dos dados.

d) **Treino e ajuste:** operações que constroem ou modificam um modelo para que este cumpra objetivos predefinidos com níveis adequados de qualidade; incluem o treino inicial e as operações posteriores de ajuste ou especialização.

e) **Desenvolvimento:** atividades preparatórias para o treino, incluindo a conceção do sistema, a seleção da arquitetura, a preparação e exploração dos conjuntos de dados e os testes experimentais, que não constituem, por si só, treino ou ajuste

f) **Dados inferidos e dados derivados:** dados pessoais produzidos pelo sistema. Os dados inferidos resultam de uma previsão, estimativa ou hipótese; os dados derivados, da transformação ou combinação de dados já existentes.

g) **Dados sintéticos:** dados gerados artificialmente para reproduzir as propriedades estatísticas de um conjunto de referência, sem corresponderem a pessoas concretas. O seu carácter sintético não implica, por si só, a anonimização dos dados de referência, caso existam.

h) **Fornecedor de inteligência artificial:** quem desenvolve, treina, fornece ou opera modelos ou serviços de inteligência artificial para que sejam incorporados por terceiros no tratamento de dados pessoais.

i) **Neurodados:** dados pessoais obtidos a partir de um tratamento técnico específico (de forma direta, indireta ou por inferência), relacionados com as características anatómicas, fisiológicas, funcionais ou comportamentais de uma pessoa singular relacionadas com a atividade cerebral e do seu sistema nervoso

j) **Pessoas ou grupos em situação de vulnerabilidade:** aqueles grupos ou pessoas que, de forma permanente ou circunstancial e devido à sua idade, deficiência ou a outras circunstâncias pessoais, sociais, económicas ou contextuais, incluindo as próprias do ambiente digital, apresentam um risco acrescido de sofrer danos ou maiores dificuldades em compreender, controlar ou exercer os seus direitos no que diz respeito ao tratamento de dados pessoais e à utilização de sistemas de inteligência artificial.

Capítulo II.
Princípios e obrigações gerais de proteção de dados no tratamento com inteligência artificial

2.1 Licitude e bases jurídicas

2.1.1. A licitude do tratamento de dados e os fundamentos jurídicos que o possam sustentar regem-se pelo regime geral de proteção de dados, que determina os fundamentos jurídicos admissíveis e as condições da sua utilização; este parágrafo não os enumera nem os hierarquiza, limitando-se a especificar a sua aplicação quando o tratamento envolve sistemas de inteligência artificial.

A necessidade de uma nova base jurídica ou de uma análise de compatibilidade dependerá de se verificar uma alteração na finalidade do tratamento ou nas condições que inicialmente justificaram a sua licitude. Consequentemente, as diferentes fases do ciclo de vida de um sistema de inteligência artificial não constituem, por si só, tratamentos independentes nem exigem necessariamente uma base jurídica distinta.

2.1.2. Quando a legislação aplicável o permitir e nos termos em que o fizer, o interesse legítimo poderá constituir uma base jurídica adequada para determinados tratamentos de dados que respondam às finalidades de desenvolvimento, treino, avaliação ou melhoria de sistemas de inteligência artificial, desde que seja efetuada a ponderação correspondente e sejam adotadas as medidas técnicas e organizativas necessárias para proteger os direitos e liberdades das pessoas. A adequação do interesse legítimo como base jurídica não pode ser presumida. Nessa ponderação, poderão revelar-se especialmente relevantes, entre outros fatores, a natureza dos dados tratados e o contexto do seu tratamento, a aplicação de medidas de minimização ou pseudonimização, as expetativas razoáveis das pessoas relativamente a essa utilização, o impacto sobre elas e a gravidade dos riscos para os seus direitos e liberdades, a inexistência de decisões com efeitos jurídicos ou que afetem significativamente as pessoas de forma semelhante durante essas fases e a possibilidade de exercer efetivamente o direito de oposição. A existência desta base jurídica não dispensa o cumprimento dos princípios da limitação da finalidade e da minimização, nem das técnicas de redução do risco de identificação previstas na Norma, aplicáveis a cada uma das finalidades enunciadas.

A ponderação deverá ser especialmente rigorosa quando o tratamento implicar a reutilização em massa de dados pessoais, categorias especiais de dados, dados de pessoas ou grupos em situação de vulnerabilidade ou atividades de definição de perfis que possam produzir efeitos jurídicos ou que afetem significativamente e de forma semelhante as pessoas. Essa ponderação não dispensa o regime especificamente aplicável às categorias especiais de dados, cujas condições de licitude e garantias reforçadas devem ser cumpridas de forma adicional, nem substitui a avaliação de impacto, nem é por esta substituída, uma vez que se trata de exigências distintas.

2.1.3. No que diz respeito ao tratamento de dados efetuado por entidades do setor público no exercício de funções públicas ou de poderes de autoridade, a admissibilidade do interesse legítimo e a determinação das bases jurídicas que possam fundamentar o tratamento regem-se pelas regras de habilitação estabelecidas pela legislação aplicável

2.2 Lealdade, finalidade e compatibilidade

2.2.1. O princípio da lealdade assume especial relevância no tratamento de dados pessoais destinados ao desenvolvimento, treino, avaliação ou melhoria de sistemas de inteligência artificial, bem como naqueles tratamentos que criem perfis, classificações ou priorizem pessoas ou tomem decisões sobre elas com base nessas operações, especialmente quando estas impliquem a reutilização de dados pessoais para fins distintos daqueles para os quais foram obtidos. Nestes casos, a avaliação da lealdade terá em conta a correspondência entre o tratamento efetivamente realizado e aquilo que as pessoas podem razoavelmente esperar quando fornecem os seus dados pessoais.

2.2.2. A utilização, por parte de prestadores de serviços ou subcontratantes, de dados pessoais tratados por conta do responsável pelo tratamento para fins próprios, tais como o desenvolvimento, treino, avaliação ou melhoria de modelos ou serviços de inteligência artificial, será considerada, de um modo geral, um fim distinto e não será entendida como abrangida pelo tratamento encomendado, salvo se existir uma autorização expressa e uma base jurídica que a sustente. Para estes efeitos, a anonimização ou transformação desses dados realizada para esses fins próprios constitui uma utilização sujeita ao disposto neste número, sem que o resultado anonimizado possa considerar-se abrangido pela delegação quando a operação que o produziu não o esteja.

2.2.3. O facto de os dados pessoais ou dados públicos serem acessíveis ao público não legitima, por si só, a sua utilização para o desenvolvimento, treino ou aperfeiçoamento de modelos ou sistemas de inteligência artificial.

2.2.4. São incompatíveis com os princípios de proteção de dados os tratamentos realizados através de sistemas de inteligência artificial destinados a manipular de forma enganosa o comportamento das pessoas, a explorar indevidamente situações de vulnerabilidade — entre outras, as decorrentes da idade, da deficiência ou da situação socioeconómica — ou a estabelecer mecanismos de pontuação social que produzam efeitos discriminatórios ou restrições injustificadas de direitos. O disposto neste número entende-se sem prejuízo das garantias reforçadas estabelecidas pela Norma para os tratamentos que incorporem técnicas biométricas e para a obtenção de dados pessoais acessíveis ao público, aplicáveis à constituição ou enriquecimento de bases de dados biométricas através da recolha massiva, sistemática e indiscriminada de imagens ou gravações, bem como as proibições, limitações ou requisitos adicionais estabelecidos pela legislação aplicável.

2.3 Minimização e proporcionalidade

2.3.1. Nos tratamentos de dados com inteligência artificial, o princípio da minimização aplica-se igualmente à capacidade do sistema para identificar, distinguir ou gerar inferências sobre as pessoas, evitando tais resultados quando os mesmos não forem necessários para a finalidade do tratamento.

2.3.2. A minimização deverá ter especialmente em conta a seleção dos dados e a geração de inferências durante o tratamento.

2.3.3. Nos tratamentos de dados que utilizem sistemas de inteligência artificial para identificar ou verificar a identidade das pessoas, deverá ser feita uma distinção clara entre a identificação e a verificação da identidade, tendo em conta os respetivos riscos e garantias. Esta distinção não prejudica a licitude desses tratamentos, que será determinada de acordo com o regime geral de proteção de dados e com a regulamentação específica aplicável, nem exclui a classificação dos dados utilizados como categorias especiais, quando tal for adequado de acordo com o referido regime, com as garantias reforçadas daí decorrentes.

2.4 Qualidade e exatidão

2.4.1. A qualidade e a exatidão dos dados tratados através de sistemas de inteligência artificial, bem como das inferências e dos resultados obtidos a partir desse tratamento, devem ser avaliadas em função da sua adequação à finalidade do tratamento de dados pessoais e ao contexto de utilização. A exatidão exige o grau de adequação à realidade necessário para cumprir essa finalidade e proteger os direitos das pessoas, sem que seja exigível, em todos os casos, uma correspondência absoluta. Quando se trate de fundamentar decisões que produzam efeitos jurídicos sobre uma pessoa ou que a afetem significativamente de forma semelhante, a exigência de exatidão e atualização será avaliada com especial rigor, sem prejuízo dos direitos de retificação, atualização e supressão reconhecidos pelo regime geral de proteção de dados e da sua aplicação às inferências, aos resultados e aos modelos previamente treinados, em conformidade com o previsto na Norma relativa aos direitos das pessoas.

2.4.2. Quando as inferências ou os resultados possam ter efeitos sobre uma pessoa, devem ser utilizados tendo em conta o seu carácter de hipótese, dedução ou proposta e o grau de incerteza associado, evitando tratá-los como se fossem factos certos quando não existam fundamentos suficientes para tal e abstendo-se de os apresentar como tal perante a pessoa ou perante terceiros. De acordo com a regra proporcional aos riscos prevista na Norma no que diz respeito ao âmbito e às condições de aplicação, o rigor exigido nessa avaliação será determinado em função da relevância dos efeitos que as inferências ou os resultados possam ter sobre a pessoa. Essa natureza da inferência ou do resultado não altera as garantias aplicáveis aos dados pessoais utilizados para gerar ditos resultados.

2.4.3. A qualidade e a exatidão exigíveis podem variar consoante a finalidade e a fase do tratamento dos dados. Nas atividades de desenvolvimento, treino, validação ou teste de sistemas de inteligência artificial, desde que tal seja adequado à finalidade dessas atividades e não se

verifiquem efeitos indesejáveis sobre as pessoas ou sobre os seus direitos, poderão ser utilizados dados que não cumpram as mesmas condições exigíveis na fase de utilização do sistema. Esta modulação diz respeito às condições de qualidade e exatidão exigíveis e não pressupõe nem autoriza, por si só, a utilização de dados pessoais nessas atividades, às quais se aplicam igualmente os princípios da licitude, da limitação da finalidade e da minimização, bem como as técnicas de redução do risco de identificação previstas na Norma.

2.5 Transparência e explicabilidade

2.5.1. Quando o tratamento de dados pessoais envolver um sistema de inteligência artificial, o responsável pelo tratamento deverá informar as pessoas, em termos compreensíveis nos termos do presente parágrafo, sobre a utilização do sistema, a finalidade para a qual dito tratamento é utilizado, o papel que desempenha no tratamento e as consequências que pode ter para elas. A mera indicação de que se utiliza inteligência artificial ou algoritmos não cumpre o dever de informação.

2.5.2. A informação deverá permitir compreender as categorias e as origens dos dados, se o sistema gera perfis, inferências, classificações, recomendações ou decisões, os destinatários e, quando for relevante, a intervenção de fornecedores ou terceiros, os critérios de conservação e, quando determinados, os prazos aplicáveis, o grau de intervenção humana, as consequências razoavelmente previsíveis e as vias para o exercício dos direitos e para a impugnação. A descrição da intervenção humana deve expressar a sua função efetiva e não apresentar como garantia uma supervisão meramente formal.

2.5.3. Sempre que for necessário para compreender o tratamento dos dados ou para exercer os direitos aplicáveis, será oferecida à pessoa uma explicação significativa e em linguagem compreensível. A explicação deverá incluir a lógica do sistema, os fatores que influenciam de forma relevante o resultado, as fontes de dados pertinentes, as limitações conhecidas e as medidas de deteção e correção de erros e enviesamentos. Não é obrigatório revelar o código-fonte, o modelo completo nem informação cuja divulgação comprometa a segurança, os segredos empresariais ou a propriedade intelectual, desde que a pessoa possa ter uma compreensão suficiente do tratamento. Esta limitação aplica-se apenas ao conteúdo da explicação exigível e não dispensa a prestação de informação adicional que se considere necessária para assegurar a compreensão suficiente, sem prejuízo do disposto neste parágrafo sobre o conteúdo essencial do direito à informação. Esta limitação também não afeta as competências de supervisão que a legislação aplicável atribua às autoridades de proteção de dados, nem os requisitos adicionais estabelecidos pela regulamentação específica aplicável em matéria de transparência e de acesso à informação pública. A explicação poderá, além disso, basear-se nos resultados de auditorias, certificações ou sistemas de selos que ofereçam garantias sobre o funcionamento do sistema, sem que tal substitua a explicação exigível nem reduza o seu conteúdo.

2.5.4. A extensão e o nível de pormenor da informação e da explicação serão determinados em função do impacto do tratamento de dados pessoais, do grau de automatização e da complexidade do sistema. No caso de uma decisão individual automatizada, as informações e a explicação deverão

proporcionar à pessoa o conhecimento das garantias e das vias disponíveis para solicitar a intervenção humana, contestar a decisão ou exercer os direitos que lhe assistem.

2.5.5. A informação poderá ser apresentada por camadas ou níveis de pormenor, desde que permita às pessoas compreender o tratamento dos dados e exercer efetivamente os seus direitos. A proteção da segurança, dos segredos empresariais ou da propriedade intelectual não poderá ser invocada para esvaziar o conteúdo essencial do direito à informação, nem para impedir o exercício efetivo dos direitos que o regime geral de proteção de dados reconhece às pessoas.

Capítulo III.
Categorias especiais, inferências sensíveis e grupos de proteção reforçada

3.1 Sensibilidade inferida

3.1.1. A saúde, a ideologia, a orientação sexual ou as crenças podem ser inferidas mesmo a partir de variáveis aparentemente neutras. Podem igualmente ser geradas outras inferências especialmente sensíveis, entre as quais as relativas à vulnerabilidade económica. Estas inferências, quando não constituírem, por si só, categorias especiais de dados, devem ser avaliadas tendo em conta os seus efeitos sobre as pessoas, de acordo com a regra de aplicação proporcional aos riscos e à avaliação de impacto previstas na Norma, nos termos e nas condições aí estabelecidos. O regime reforçado que o regime geral de proteção de dados prevê para as categorias especiais de dados será determinado pela natureza efetiva da informação inferida e não apenas pela natureza dos dados de entrada.

3.1.2. O regime reforçado previsto pelo regime geral de proteção de dados para as categorias especiais de dados será aplicável quando o sistema gerar ou utilizar inferências que permitam atribuir razoavelmente a uma pessoa uma categoria especial de dados. A finalidade, o contexto e o impacto do tratamento serão tidos em conta para avaliar o carácter razoável dessa atribuição. O grau de fiabilidade ou de exatidão da inferência não excluirá, por si só, a aplicação do regime reforçado quando essa inferência for utilizada para tomar ou justificar decisões relativas à pessoa em causa.

3.1.3. A presença acidental de categorias especiais de dados no desenvolvimento ou na formação de um sistema deve ser avaliada de forma diferenciada para cada uma dessas fases, de acordo com a abordagem do ciclo de vida prevista de forma geral na Norma, tendo em conta se esses dados são utilizados, se podem influenciar o modelo ou se podem ser revelados através das suas inferências ou resultados. O responsável adotará medidas razoáveis para limitar a sua utilização e evitar que sirvam de base para inferências ou decisões sobre as pessoas, quando tal não for necessário e lícito.

3.1.4. O tratamento de categorias especiais de dados ou de inferências que permitam atribuir razoavelmente tais categorias, incluindo a sua conservação e utilização, só poderá ser realizado quando se verifique alguma das exceções previstas pelo regime geral de proteção de dados para essas categorias. A Norma não constitui, por si só, uma autorização para esse tratamento. Quando o regime geral de proteção de dados o permitir com o objetivo de detetar, avaliar ou corrigir efeitos discriminatórios ou preconceitos, o tratamento ficará sujeito aos princípios da minimização e da proporcionalidade e às garantias reforçadas exigíveis nos termos da Norma e do referido regime.

3.2 Pessoas ou grupos em situação de vulnerabilidade

3.2.1. Nos tratamentos de dados com inteligência artificial que afetem pessoas ou grupos em situação de vulnerabilidade, o seu interesse superior deve ser tido em conta tanto na definição do tratamento como na avaliação e utilização das inferências e dos resultados gerados pelo sistema.

3.2.2. A utilização de dados pessoais de pessoas ou grupos em situação de vulnerabilidade para o desenvolvimento, treino, validação ou melhoria de sistemas de inteligência artificial exigirá, em cada uma dessas fases, uma justificação especialmente rigorosa e a adoção de garantias reforçadas, tendo em conta o seu interesse superior. O conteúdo destas garantias será determinado tendo em conta os riscos do tratamento para este grupo e os requisitos que o regime geral de proteção de dados estabeleça para os seus dados pessoais. Quando esse tratamento não for necessário para a finalidade pretendida, deverão ser adotadas medidas para evitar a utilização destes dados.

3.2.3. Nos sistemas dirigidos a pessoas ou grupos em situação de vulnerabilidade, ou que possam afetar-lhes de forma significativa, incluindo os casos de efeitos discriminatórios, deverão aplicar-se configurações especialmente protetoras e predefinidas, uma conceção adequada à sua idade e garantias reforçadas contra a criação de perfis, a publicidade comportamental e a recolha indevida dos seus dados pessoais, em conformidade com a proteção de dados desde a conceção e por predefinição prevista na Norma. Estas medidas não autorizam, por si só, o tratamento, cuja licitude se rege pelo regime geral de proteção de dados e pelas proibições e limitações por este estabelecidas. A criação de perfis, a publicidade comportamental e as inferências que exploram indevidamente a situação de vulnerabilidade destas pessoas ou grupos está abrangida pela incompatibilidade com os princípios de proteção de dados declarada com carácter geral na Norma. Quando, apesar das medidas adotadas, persistir um risco elevado para este grupo, aplicar-se-á o disposto de forma geral na Norma para os casos em que o risco elevado persista. A informação e a explicação exigíveis nos termos da Norma serão fornecidas em termos compreensíveis, tendo em conta a idade das pessoas ou do grupo.

3.3 Neurodados

3.3.1. O responsável submeterá os tratamentos de dados realizados através de sistemas de inteligência artificial que utilizem neurodados ou gerem inferências sobre estados cognitivos, emocionais ou comportamentais a uma avaliação especial de necessidade e proporcionalidade, tendo em conta a sua capacidade para revelar aspetos particularmente sensíveis da pessoa, o contexto em que são realizados — em particular quando envolvam relações caracterizadas por uma assimetria de poder — e os riscos que podem representar para a autonomia, a privacidade e os direitos fundamentais. Esta avaliação entende-se sem prejuízo da avaliação de impacto que possa ser exigida nos termos da regulamentação aplicável e da Norma.

3.3.2. São incompatíveis com os princípios de proteção de dados, nos termos estabelecidos com carácter geral pela Norma, os tratamentos de dados que utilizem neurodados ou inferências sobre estados cognitivos, emocionais ou comportamentais para manipular indevidamente a vontade ou o comportamento das pessoas ou para explorar situações de vulnerabilidade. Os

tratamentos destinados a inferir convicções íntimas ou a levar a cabo formas especialmente intrusivas de vigilância só poderão ser admitidos a título excecional quando exista uma base jurídica admissível, em conformidade com o regime geral de proteção de dados, quando respondam a uma finalidade legítima especialmente relevante — cuja especial relevância deverá ser justificada — ou quando sejam necessários e proporcionados e não existam alternativas menos intrusivas, sem prejuízo das proibições, limitações ou requisitos adicionais estabelecidos pela regulamentação específica aplicável. A concorrência de todas estas condições deverá poder comprovar-se, em conformidade com o dever de documentação do tratamento previsto na Norma. O consentimento não deve constituir uma base de legitimidade quando o responsável pelo tratamento não estiver em condições de determinar antecipadamente, com razoável precisão, quais as inferências que decorrerão do tratamento dos neurodados.

Capítulo IV.
Decisões automatizadas e criação de perfis

4.1 Identificação de decisões individuais automatizadas

4.1.1. O responsável identificará os casos em que exista uma decisão baseada exclusivamente no tratamento de dados automatizado, incluindo a definição de perfis, que produza efeitos jurídicos sobre a pessoa ou que a afete significativamente, independentemente da natureza — social, económica ou de outra ordem — desse impacto, distinguindo as decisões exclusivamente automatizadas, os sistemas de apoio à decisão e os casos de intervenção humana efetiva, de acordo com os critérios estabelecidos neste capítulo. A identificação destes casos determinará a aplicação dos deveres de transparência e de explicação, bem como das garantias previstas na Norma relativamente às decisões individuais automatizadas.

4.1.2. Esta identificação será revista sempre que se verifiquem alterações relevantes no tratamento dos dados ou no sistema de inteligência artificial, com a finalidade de determinar e adaptar as garantias aplicáveis, tendo em conta, entre outros aspetos, a natureza significativo dos efeitos do tratamento, a fase do ciclo de vida do tratamento e as características do sistema.

4.2 Intervenção humana efetiva

4.2.1. A natureza exclusivamente automatizada de uma decisão só será excluída quando exista uma intervenção humana prévia, real e efetiva, realizada por um pessoa com capacidade para avaliar e compreender o resultado do sistema e com autoridade suficiente para o confirmar, alterar ou afastar-se do mesmo. Não constituirá uma intervenção humana efetiva aquela que se limite a formalizar ou a endossar o resultado do sistema sem reunir essas condições; nesse caso, a decisão manterá o seu carácter exclusivamente automatizado e ser-lhe-ão aplicáveis as garantias relativas às decisões individuais previstas neste capítulo, bem como os deveres de informação e de explicação previstos na Norma em matéria de transparência e explicabilidade. As condições organizacionais necessárias para que essa intervenção seja efetiva, entre as quais a atribuição de responsabilidades, a formação e a supervisão por parte de quem a realiza serão adotadas de acordo com as medidas de governação algorítmica previstas na Norma.

4.2.2. A supervisão humana poderá recorrer a ferramentas automatizadas, tais como sistemas de alerta ou de deteção de discrepâncias, embora estas não substituam a intervenção humana quando esta resultar exigível, nem possam ser apresentadas como equivalentes a dita intervenção. A sua utilização não alterará as condições exigidas no presente capítulo para que a intervenção humana exclua o carácter exclusivamente automatizado da decisão.

4.3 Eficácia das garantias e não discriminação algorítmica

4.3.1. As garantias aplicáveis às decisões individuais incluem, como mínimo e nos termos previstos na Norma: a informação sobre a utilização do sistema de inteligência artificial, a finalidade para a qual é utilizado, o papel que desempenha no tratamento dos dados e as consequências que pode acarretar, bem como a explicação significativa do tratamento, em conformidade com o disposto na Norma em matéria de transparência e explicabilidade; o conhecimento das vias disponíveis para solicitar a intervenção humana, contestar a decisão e exercer os direitos que lhes assistem; e as medidas de prevenção, deteção e correção dos efeitos discriminatórios previstas neste capítulo. Essas garantias serão acessíveis, oportunas e com efeitos reais, e não meramente formais, permitindo que as pessoas compreendam a decisão e as suas consequências, solicitem a intervenção humana quando necessário e exerçam os direitos que lhes são reconhecidos pela legislação em matéria de proteção de dados.

4.3.2. O responsável avaliará se o sistema pode produzir efeitos discriminatórios, incluindo os decorrentes da utilização de variáveis aparentemente neutras, de diferenças relevantes no seu funcionamento em relação a diferentes grupos de pessoas ou das inferências geradas pelo sistema, e adotará as medidas necessárias para prevenir, detetar e corrigir quaisquer preconceitos que possam afetar injustificadamente as pessoas. A adequação e a suficiência destas medidas devem poder comprovar-se de acordo com o dever de documentação do tratamento previsto na Norma, sem prejuízo das competências que cabem às autoridades de proteção de dados, nos termos da legislação aplicável.

Capítulo V.
Direitos das pessoas em sistemas de inteligência artificial

5.1. Os direitos reconhecidos pela legislação em matéria de proteção de dados podem ser exercidos relativamente aos dados pessoais tratados através de sistemas de inteligência artificial, incluindo inferências, perfis e outros resultados que constituam dados pessoais. A natureza destes dados pode determinar o âmbito ou a forma de exercício de cada direito, sem prejuízo do disposto na referida legislação.

5.2. No exercício do direito de acesso, a pessoa deverá poder saber, quando tal for aplicável nos termos da legislação em matéria de proteção de dados, se os seus dados foram utilizados num sistema de inteligência artificial, se foram criados perfis ou inferências sobre si e se estes influenciaram ou foram utilizados para tomar ou apoiar decisões que a afetem.

5.3. Quando o direito de retificação se referir a inferências, perfis ou previsões geradas por um sistema de inteligência artificial, o seu exercício deverá adaptar-se à sua natureza. Quando estes não puderem ser retificados diretamente devido à sua própria natureza, a pessoa poderá solicitar a correção dos dados utilizados para as gerar, fornecer informação complementar, contestá-las ou solicitar a sua revisão, especialmente quando possam ter repercussões sobre a sua pessoa.

5.4. O exercício dos direitos de supressão, limitação e oposição reger-se-á pelo regime geral de proteção de dados. O responsável pelo tratamento dos dados procurará selecionar, configurar ou utilizar sistemas que incorporem, sempre que tal seja tecnicamente viável tendo em conta o estado da tecnologia e os meios razoavelmente disponíveis, mecanismos que facilitem o exercício efetivo destes direitos ao longo de todo o ciclo de vida do tratamento, nomeadamente através da eliminação, dissociação ou exclusão dos dados pessoais de futuros treinos. A viabilidade técnica desses mecanismos não condiciona a exigibilidade destes direitos e a sua avaliação deverá poder ser comprovada de acordo com o dever de documentação do tratamento previsto na Norma, sem prejuízo das competências que correspondem às autoridades de proteção de dados, em conformidade com a legislação aplicável.

5.5. Quando, devido ao estado da tecnologia, os direitos de supressão, limitação ou oposição não puderem ser plenamente exercidos relativamente a um modelo previamente treinado, o responsável pelo tratamento dos dados deverá justificar esta circunstância e registá-la em conformidade com o dever de documentação do tratamento previsto na Norma, informar a pessoa afetada e adotar as medidas razoavelmente disponíveis para limitar o tratamento e reduzir o seu impacto, incluindo, sempre que possível, a supressão dos dados pessoais dos ambientes em que se encontram — entre outros, os conjuntos de dados de treino, os índices, as bases de representações vetoriais e as memórias persistentes — e a sua exclusão de futuros treinos. Esta circunstância não terá carácter definitivo e será avaliada de acordo com o estado da tecnologia existente em cada momento. O disposto nesta secção deve interpretar-se sem prejuízo do dever do responsável, ao utilizar modelos ou serviços de inteligência artificial desenvolvidos por terceiros, de verificar as condições da sua utilização, em conformidade com o previsto na Norma relativa aos intervenientes e à cadeia de valor, e da responsabilidade que cabe a cada interveniente nos termos desse regime.

5.6. A portabilidade aplica-se aos dados fornecidos pelo titular e, se for o caso, aos dados observados que se encontrem estruturados. De acordo com o regime geral de proteção de dados, a portabilidade não abrangerá, como regra geral, os dados inferidos ou derivados, sem que isso afete a sua qualidade de dados pessoais nem o exercício, sobre os mesmos, dos restantes direitos reconhecidos ao titular dos dados. Poderão ser disponibilizados formatos estruturados que favoreçam a interoperabilidade e a mudança de fornecedor.

Capítulo VI.
Intervenientes, cadeia de valor e transferências internacionais

6.1. A qualidade de responsável ou encarregado do tratamento dos dados e, quando a legislação aplicável reconheça esta figura, a de corresponsável, será determinada em relação a cada tratamento de dados pessoais; considera-se como responsável quem decide as finalidades e os meios essenciais do tratamento concreto, mesmo que não desenvolva nem controle tecnicamente o modelo. Quando vários intervenientes partilharem essas decisões, as responsabilidades assumidas por cada um devem determinar-se desde a conceção do tratamento, definidas de acordo com o previsto na Norma relativa às relações entre os intervenientes no tratamento e documentadas de acordo com o dever de documentação do tratamento previsto na Norma.

6.2. Os fornecedores de modelos ou de serviços de inteligência artificial poderão atuar como responsáveis, encarregados ou corresponsáveis, consoante as funções que desempenhem em cada tratamento, avaliadas de acordo com o ciclo de vida do tratamento e tendo em conta as decisões tomadas em fases anteriores que o condicionem de forma relevante. Em particular, quando reutilizarem dados pessoais para fins próprios ou determinarem os fins ou os meios essenciais do tratamento, assumirão as responsabilidades que lhes correspondam, em conformidade com a legislação em matéria de proteção de dados. As condições de utilização dos dados para o desenvolvimento, treino ou melhoria de modelos devem ser determinadas expressamente entre as partes, sem que tal determinação substitua a base jurídica exigida pelo tratamento nem o previsto na Norma em matéria de lealdade, finalidade e compatibilidade relativamente à utilização de dados pessoais por fornecedores ou encarregados para fins próprios.

6.3. O responsável pelo tratamento dos dados identificará os intervenientes no desenvolvimento, fornecimento e utilização do sistema de inteligência artificial, incluindo os encarregados, subcontratantes e fornecedores sucessivos que intervenham no tratamento, bem como os tratamentos ou funções que cada um desempenha no que diz respeito aos dados pessoais e as transferências internacionais que possam ocorrer. Esta identificação deverá permitir determinar as responsabilidades de cada interveniente, formalizar as relações jurídicas correspondentes e dispor da informação necessária para o cumprimento da legislação em matéria de proteção de dados. O acima exposto entende-se sem prejuízo da informação que deva ser prestada às pessoas sobre os destinatários e sobre a intervenção de prestadores de serviços ou terceiros, que se regerá pelo disposto na Norma em matéria de transparência e explicabilidade.

6.4. A utilização de modelos ou serviços de inteligência artificial desenvolvidos por terceiros não isenta o responsável de verificar se a sua utilização é compatível com a legislação em matéria de proteção de dados, nem de avaliar as garantias oferecidas por esses fornecedores, especialmente quando as características do modelo ou as condições de prestação do serviço possam afetar o tratamento de dados pessoais. A seleção de fornecedores deverá ter em conta, entre outros aspetos, a natureza dos dados tratados e as finalidades do tratamento, as garantias oferecidas de cumprimento da legislação em matéria de proteção de dados e a informação colocada à disposição do responsável pelo tratamento para comprovar esse cumprimento,

incluindo a informação relativas aos intervenientes na prestação do serviço, as limitações que possam afetar o tratamento dos dados e os mecanismos previstos para comunicar ao responsável as alterações relevantes na prestação do serviço. O disposto neste parágrafo entende-se sem prejuízo da informação e da documentação de que o responsável deve dispor sobre o sistema e sobre os tratamentos prévios realizados pelo prestador, em conformidade com o dever de documentação do tratamento previsto na Norma.

6.5. As relações entre os diferentes intervenientes no tratamento dos dados, incluindo os subcontratantes e os prestadores de serviços sucessivos, devem estabelecer claramente as responsabilidades assumidas por cada um, em particular no que diz respeito à utilização dos dados pessoais, incluindo a aplicação de técnicas de anonimização aos mesmos, a sua utilização para o desenvolvimento, treino ou melhoria de modelos, em conformidade com o previsto na Norma em matéria de lealdade, finalidade e compatibilidade, o exercício dos direitos das pessoas, as transferências internacionais e as obrigações cujo cumprimento dependa da atuação, das capacidades ou dos meios de que o prestador disponha.

6.6. As transferências internacionais de dados pessoais realizadas no contexto do desenvolvimento, formação, implementação ou utilização de sistemas de inteligência artificial estarão sujeitas ao regime geral de proteção de dados. Sempre que o contexto do tratamento ou os riscos associados à utilização de sistemas de inteligência artificial assim o exijam, deverão adotar-se as medidas complementares adequadas relativamente aos dados objeto de transferência, tais como a sua minimização, a encriptação, a pseudonimização ou garantias contratuais adicionais sobre a sua utilização, conservação ou reutilização. A identificação das transferências que possam ocorrer quando intervenham prestadores de serviços ou subcontratantes reger-se-á pelo disposto no presente capítulo sobre a identificação dos intervenientes no tratamento.

Capítulo VII.
Governança algorítmica, medidas proativas e avaliação de impacto

7.1. A proteção de dados desde a conceção e por predefinição deverá aplicar-se e integrar-se na governação do tratamento dos dados ao longo de todo o ciclo de vida dos tratamentos que incorporem sistemas de inteligência artificial, tendo em conta os riscos específicos decorrentes do seu desenvolvimento, treino, implementação, utilização e evolução, e aplicando a cada uma dessas fases o princípio da minimização nos termos previstos na Norma.

7.2. A documentação e o registo das atividades de tratamento cumprirão, no que diz respeito aos tratamentos de dados que incorporem sistemas de inteligência artificial, a função comprovativa que corresponde ao dever de documentação do tratamento previsto na Norma, e identificarão, quando for relevante, as particularidades decorrentes da utilização desses sistemas, incluindo as categorias e a origem dos dados de entrada, os atributos, perfis, inferências ou classificações que o sistema gere ou possa razoavelmente gerar e as categorias de resultados que produza, bem como os fins e utilizações previstas desses resultados.

7.3. O responsável estabelecerá medidas de governação algorítmica adequadas, proporcionais ao risco e passíveis de verificação, para garantir o cumprimento da legislação em matéria de proteção de dados ao longo de todo o ciclo de vida do tratamento dos dados. Estas medidas incluirão, quando aplicável, a atribuição de responsabilidades, a gestão de riscos, a supervisão humana, a formação adequada das pessoas envolvidas no tratamento e, em especial, na configuração, utilização ou supervisão do sistema de inteligência artificial, a coordenação entre as funções relevantes da organização e a revisão periódica e a melhoria contínua das medidas adotadas. A adequação destas medidas será avaliada tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento, bem como os riscos que este possa acarretar para os direitos e liberdades das pessoas, sem prejuízo das competências que cabem às autoridades de proteção de dados nos termos da legislação aplicável.

7.4. Sempre que for necessário nomear um delegado ou responsável pela proteção de dados, em conformidade com a legislação aplicável, este participará desde as fases iniciais dos tratamentos de dados que envolvam sistemas de inteligência artificial, tendo acesso à informação necessária, à formação e aos recursos adequados para desempenhar as suas funções de forma eficaz e não meramente formal.

Quando a organização dispuser de funções ou órgãos específicos de governação da inteligência artificial, estes coordenarão a sua atuação com o delegado ou responsável pela proteção de dados, nas questões que afetem o tratamento de dados pessoais, respeitando a autonomia funcional que corresponda a cada um.

7.5. Sempre que tal seja exigido pela legislação aplicável, o responsável pelo tratamento dos dados deverá realizar a avaliação de impacto antes do início do tratamento dos dados e da sua implementação, e proceder à sua revisão sempre que se verifiquem alterações relevantes nos dados, finalidades, modelos e sistemas de inteligência artificial utilizados, nos fornecedores ou

nos riscos para as pessoas. Recomenda-se a sua realização, independentemente essa exigência, sempre que o tratamento dos dados possa implicar um risco elevado para os direitos e liberdades das pessoas. A avaliação prestará especial atenção aos riscos decorrentes da utilização de decisões automatizadas, da definição de perfis e dos possíveis efeitos discriminatórios ou adversos sobre as pessoas ou grupos afetados, quando forem relevantes para o tratamento. Quando o tratamento possa produzir tais efeitos ou afetar pessoas ou grupos que necessitem de proteção reforçada, procurar-se-á registar o ponto de vista das pessoas ou grupos potencialmente afetados ou dos seus representantes. O âmbito e o nível da documentação da avaliação devem ser proporcionais à natureza, ao contexto e aos riscos do tratamento.

7.6. Quando a avaliação identificar riscos elevados, o responsável pelo tratamento dos dados deverá adotar medidas adicionais para os mitigar. Se, apesar disso, persistir um risco elevado, deverá consultar a autoridade de proteção de dados competente antes do início do tratamento ou da implementação do sistema, ou abster-se de iniciar o tratamento dos dados. Quando a legislação aplicável preveja um procedimento específico para estes casos, deverá agir-se de acordo com o mesmo. Requerem uma atenção especialmente rigorosa na identificação, avaliação e gestão do risco, entre outros, os tratamentos que envolvam decisões automatizadas que produzam efeitos jurídicos sobre as pessoas ou que as afetem significativamente, a pontuação social ou a avaliação generalizada de pessoas, a identificação biométrica ou o reconhecimento ou inferência de emoções, a identificação biométrica à distância em espaços públicos, o tratamento de neurodados ou a geração de inferências sobre estados cognitivos, emocionais ou comportamentais, o tratamento de dados de pessoas ou grupos em situação de vulnerabilidade, e a reutilização em massa de dados pessoais para o desenvolvimento ou treino de sistemas de inteligência artificial, tudo isto em conformidade com o previsto na Norma no que diz respeito a grupos de proteção reforçada, neurodados e padrões tecnológicos e de utilização, sem prejuízo dos tratamentos de dados que a Norma considera incompatíveis com os princípios de proteção de dados.

7.7. A adesão a códigos de conduta, normas técnicas ou esquemas de certificação, bem como a avaliação, autorização, certificação ou supervisão de um sistema de inteligência artificial em conformidade com a regulamentação específica que lhe seja aplicável, podem facilitar a aplicação da Norma e comprovar a adoção de boas práticas, mas não substituem a responsabilidade que cabe ao responsável por garantir o cumprimento da legislação em matéria de proteção de dados, nem a gestão adequada dos riscos decorrentes da utilização de sistemas de inteligência artificial, e entendem-se sem prejuízo das competências que cabem às autoridades de proteção de dados, em conformidade com a legislação aplicável

7.8. Nos tratamentos de dados que apresentem riscos elevados, a revisão periódica e a melhoria contínua das medidas de governação algorítmica previstas neste capítulo serão intensificadas em função da gravidade desses riscos, sendo ainda recomendada a realização de revisões ou auditorias independentes, sempre que estas contribuam para verificar a eficácia das medidas adotadas, reforçar a governação algorítmica e melhorar a gestão dos riscos, com base em critérios de avaliação previamente definidos e proporcionais ao risco e sempre que seja possível comprovar a independência, a competência técnica e a ausência de conflitos de interesses de quem as realiza.

7.9. A documentação elaborada com base nestas Normas deverá estar à disposição da autoridade de proteção de dados competente no exercício das suas funções de supervisão, nos termos do n.º 42.4 das Normas de Proteção de Dados dos Estados Ibero-americanos.

Capítulo VIII.
Medidas técnicas e organizativas de proteção de dados e segurança na utilização de sistemas de inteligência artificial

8.1 Ameaças e riscos específicos

O responsável identificará e manterá atualizada uma lista de ameaças específicas da inteligência artificial aplicáveis ao seu sistema, que inclua, entre outras, a extração de dados de treino, a inversão de modelo, os ataques de pertença, as fugas através das instruções ao sistema, a exposição das representações vetoriais, a reidentificação, a memorização, a contaminação dos dados de treino, a recuperação indevida de informação em sistemas de geração aumentada por recuperação e a injeção de instruções.

A identificação destas ameaças e a avaliação do risco que representam para os direitos e liberdades das pessoas servirão de base para definir as medidas de segurança, os testes e a resposta a incidentes adequadas à proteção dos dados pessoais tratados. Quando o tratamento combinar diferentes fontes de informação, deverá avaliar-se o risco de agregação e de reidentificação.

8.2 Controlos técnicos e testes específicos

As medidas de segurança devem ser mantidas e revistas ao longo de todo o ciclo de vida do tratamento de dados pessoais. O responsável pelo tratamento deverá adotar as medidas legais, técnicas e organizacionais adequadas para fazer face às ameaças identificadas e aos riscos concretos que estas acarretam para o tratamento de dados pessoais. Estas medidas podem incluir, entre outras, controlos de acesso, segregação de ambientes, encriptação, monitorização, isolamento de ambientes ou componentes, mecanismos de filtragem e validação de entradas e saídas, medidas para limitar o armazenamento ou a divulgação de dados pessoais e outras medidas técnicas e organizacionais adaptadas ao estado da técnica, à evolução das ameaças e os riscos associados ao tratamento. Além disso, deverá realizar os testes adequados para verificar a eficácia destas medidas no âmbito da sua revisão e, em especial, quando se verificarem alterações relevantes no tratamento dos dados ou no sistema de inteligência artificial. Para este efeito, poderá basear-se em normas, metodologias ou padrões técnicos geralmente reconhecidas, desde que sejam adequadas aos riscos do tratamento e contribuam para a melhoria contínua dos controlos adotados, sem prejuízo do valor que a Norma atribui aos códigos de conduta, às normas técnicas e aos esquemas de certificação.

8.3 Técnicas de redução do risco de identificação

8.3.1. A pseudonimização reduz a exposição, mas não exclui o tratamento do regime geral de proteção de dados. A anonimização só poderá ser considerada eficaz quando se comprove que não existe um risco razoável de identificação ou reidentificação, tendo em conta os meios que possam razoavelmente ser utilizados, apreciação que exige especial prudência quando o tratamento dos

dados, o sistema ou os seus resultados possam facilitar a reidentificação ou revelar dados por memorização. Estas técnicas constituem medidas de proteção de dados desde a conceção e por predefinição, nos termos previstos na Norma.

8.3.2. Segundo o caso, poderão utilizar-se técnicas como a filtragem prévia de dados, a supressão de duplicados, a redução do nível de detalhe da informação, a pseudonimização, a privacidade diferencial, os dados sintéticos e outras medidas destinadas a reduzir o risco de identificação. A utilização destas técnicas não isenta os responsáveis e encarregados do cumprimento da legislação em matéria de proteção de dados nem da adoção das medidas de segurança adequadas.

8.4 Resposta a incidentes

8.4.1. O responsável deverá incluir nos seus procedimentos de gestão de incidentes as vulnerabilidades específicas decorrentes da utilização de sistemas de inteligência artificial, em particular aquelas que possam dar origem à divulgação, extração ou utilização indevida de dados pessoais ou à perda da sua disponibilidade, integrando estas vulnerabilidades nos procedimentos gerais de gestão de incidentes. Além disso, deverá prever as medidas adequadas para a sua deteção, contenção e mitigação, bem como para a avaliação do risco para os direitos e liberdades das pessoas. Quando for relevante, a resposta ao incidente deverá estar em conformidade com o regime Regulamento Geral sobre a Proteção de Dados aplicável às violações de segurança dos dados pessoais, incluindo a notificação que, nos termos desse regime, deva ser feita à autoridade de proteção de dados competente e, se for caso disso, aos titulares dos dados.

Capítulo IX.
Disposições específicas aplicáveis a determinados padrões tecnológicos e de utilização

Para além das disposições gerais contidas na Norma, quando um tratamento de dados incorporar algum dos seguintes padrões tecnológicos ou de utilização, deverão aplicar-se as disposições específicas previstas neste capítulo, na medida em que se considerem pertinentes.

9.1 Inteligência artificial generativa

Nos tratamentos de dados que incorporem sistemas de inteligência artificial generativa, deverão adotar-se medidas específicas para evitar a introdução desnecessária de dados pessoais, próprios ou de terceiros, nas instruções, definir as condições de conservação das instruções e dos resultados, bem como da sua eventual utilização para o treino ou o aperfeiçoamento dos modelos, prevenir a divulgação, recuperação ou armazenamento indevido de dados pessoais e verificar os resultados quando estes possam ser utilizados para tomar decisões sobre as pessoas. Esta verificação entende-se sem prejuízo da exatidão exigível às inferências e aos resultados, em conformidade com a Norma. Quando o tratamento incluir o desenvolvimento ou treino de modelos, deverá dispor-se da informação suficiente sobre a origem dos dados utilizados, em conformidade com o dever de documentação do tratamento previsto na Norma.

9.2 Inteligência artificial agêntica

Quando um sistema de inteligência artificial for capaz de aceder de forma autónoma a dados pessoais ou executar ações sobre os mesmos, o responsável pelo seu tratamento deverá determinar o nível de autonomia admissível, tendo em conta as ações que o sistema possa executar e os seus possíveis efeitos sobre as pessoas, de modo que, quanto maior for a gravidade desses efeitos, maior será o grau de autonomia e mais intensa será a supervisão; delimitar os dados, ferramentas, serviços ou recursos aos quais o sistema pode aceder; controlar a utilização de memórias persistentes quando estas impliquem a conservação ou reutilização de dados pessoais, que ficará sujeita aos princípios da finalidade e da limitação do prazo de conservação, em conformidade com a Norma e com a legislação em matéria de proteção de dados; garantir a rastreabilidade das ações, incluindo os acessos aos recursos autorizados e as interações com outros sistemas, serviços ou agentes e prever mecanismos de supervisão humana e de suspensão ou interrupção das ações, que possam ser ativados independentemente do próprio sistema, sempre que tal seja necessário para proteger os direitos das pessoas. As ações autónomas do sistema deverão manter-se dentro do âmbito do tratamento e das finalidades previamente determinadas pelo responsável pelo tratamento dos dados. Quando a ação autónoma do sistema implicar uma finalidade diferente da inicialmente prevista, deverá verificar-se se esta dispõe de uma base jurídica adequada e, quando aplicável, se é compatível com a finalidade original, em conformidade com o previsto na Norma em matéria de finalidades e reutilização de dados. A ação autónoma do sistema não isenta nem substitui as responsabilidades que correspondem às pessoas que intervêm no

tratamento dos dados, em conformidade com a Norma e com a legislação em matéria de proteção de dados.

9.3 Biometria e reconhecimento de emoções

Os tratamentos de dados que incorporem sistemas de inteligência artificial e técnicas biométricas, independentemente de estas serem utilizadas pelo próprio sistema, deverão distinguir, entre outros casos, a verificação, a identificação e outras utilizações de técnicas biométricas, de acordo com a distinção entre identificação e verificação da identidade estabelecida na Norma em matéria de minimização e proporcionalidade, aplicando, se for o caso, as garantias reforçadas exigíveis nos termos da legislação em matéria de proteção de dados, incluindo as decorrentes do regime reforçado aplicável às categorias especiais de dados previsto na Norma em matéria de sensibilidade inferida, quando aplicável, e do risco associado ao tratamento. Deverá prestar-se uma atenção especialmente rigorosa à identificação biométrica à distância e, quando implicarem o tratamento de dados pessoais, ao reconhecimento e inferência de emoções e outras utilizações que, pela sua natureza, contexto ou alcance, possam afetar significativamente os direitos das pessoas, sem prejuízo das proibições, limitações ou requisitos adicionais estabelecidos pela regulamentação específica aplicável e do disposto na Norma para os tratamentos que gerem inferências sobre estados cognitivos, emocionais ou comportamentais. Nestes casos, deverá ser possível comprovar, em conformidade com os deveres de qualidade, exatidão e documentação do tratamento previstos na Norma, a adequação e a fiabilidade do sistema para a finalidade e o contexto em que é utilizado. Estes tratamentos de dados estão, além disso, incluídos entre aqueles que requerem uma atenção especialmente rigorosa na identificação, avaliação e gestão do risco e entre os que determinam o reforço da revisão periódica e a melhoria contínua das medidas de governação algorítmica, nos termos e nas condições estabelecidos na Norma.

9.4 Pontuação, seleção e priorização

Os tratamentos de dados que incorporem sistemas de inteligência artificial destinados à avaliação, seleção, classificação ou priorização de pessoas deverão incorporar medidas específicas para prevenir resultados discriminatórios, em conformidade com o previsto na Norma em matéria de eficácia das garantias e de não discriminação algorítmica; garantir uma transparência adequada ao seu impacto, em conformidade com o previsto na Norma em matéria de transparência e explicabilidade; e assegurar o respeito pelas garantias aplicáveis às decisões individuais automatizadas, quando aplicável, sem prejuízo das proibições, limitações ou requisitos adicionais estabelecidos pela regulamentação específica aplicável e da incompatibilidade declarada de forma geral na Norma para os mecanismos de pontuação social que produzam efeitos discriminatórios ou restrições injustificadas de direitos.

9.5 Obtenção de dados acessíveis ao público

A utilização de dados pessoais acessíveis ao público para o desenvolvimento, treino ou aperfeiçoamento de modelos ou sistemas de inteligência artificial reger-se-á pela regra estabelecida na Norma em matéria de lealdade, finalidade e compatibilidade, segundo a qual a sua natureza, por si só, não legitima essa

utilização. Dita natureza dos dados também não exclui a aplicação do princípio da finalidade. A reutilização desses dados para fins distintos daqueles que justificaram a sua publicação ou recolha exigirá uma base jurídica adequada e, se for o caso, garantias reforçadas, sem prejuízo da análise de compatibilidade exigida nos termos da Norma em matéria de fins e reutilização de dados. Estas garantias serão especialmente exigíveis quando a reutilização se realizar através de compilações em massa ou se basear no interesse legítimo e no ordenamento jurídico que reconheça esta base jurídica, sem que a acessibilidade pública dos dados constitua, por si só, esse interesse legítimo ou dispense a ponderação exigida nos termos da Norma. Na determinação da base jurídica adequada e das garantias aplicáveis, ter-se-ão em conta a finalidade e o contexto que justificaram a disponibilização pública dos dados, bem como as expectativas razoáveis das pessoas relativamente a essa reutilização. Essas garantias podem compreender as técnicas de redução do risco de identificação previstas na Norma, aplicadas com especial atenção às categorias especiais de dados e aos dados de pessoas ou grupos em situação de vulnerabilidade. As condições estabelecidas neste número funcionam como garantias adicionais exigíveis para a reutilização e não como uma autorização da mesma. O disposto neste número entende-se sem prejuízo das garantias reforçadas e das medidas de prevenção exigíveis nos termos da Norma no que diz respeito aos dados pessoais de pessoas ou grupos em situação de vulnerabilidade.

RED IBEROAMERICANA DE PROTECCION DE DATOS

Red Iberoamericana
Rede Ibero-Americana

Financiado pela
União Europeia

Documento financiado pela União Europeia, em colaboração com a Fundação para a Internacionalização das Administrações Públicas (FIAP) no âmbito da Aliança Digital UE-ALC. As opiniões e os argumentos expressos neste documento não refletem necessariamente os pontos de vista oficiais da União Europeia, nem dos seus Estados-Membros.