

METODOLOGIA EUROPEIA DE AVALIAÇÃO DA DISCRIMINAÇÃO ALGORÍTMICA



Em colaboração com
o Centro Interfederal para a Igualdade de Oportunidades (Unia), Bélgica,
a Provedoria de Justiça para a Não Discriminação (YVV), Finlândia,
e a Comissão para a Cidadania e a Igualdade de Género (CIG), Portugal

Louise Hooper
Ylja Remmits
Ioanna Papageorgiou

Co-funded
by the European Union



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Co-funded and implemented
by the Council of Europe

METODOLOGIA EUROPEIA DE AVALIAÇÃO DA DISCRIMINAÇÃO ALGORÍTMICA

**Louise Hooper
Ylja Remmits
Ioanna Papageorgiou**

Em colaboração com
o Centro Interfederal para a Igualdade
de Oportunidades (Unia), Bélgica,
a Provedoria de Justiça para a Não
Discriminação (YVV), Finlândia,
e a Comissão para a Cidadania e a
Igualdade de Género (CIG), Portugal

Esta publicação foi elaborada com o apoio financeiro da União Europeia e do Conselho da Europa. O conteúdo é da exclusiva responsabilidade das autoras e autores. As opiniões aqui expressas não podem, de forma alguma, ser consideradas como refletindo a posição oficial da União Europeia ou do Conselho da Europa.

É autorizada a reprodução de excertos (até 500 palavras), exceto para fins comerciais, desde que seja preservada a integridade do texto, o excerto não seja utilizado fora do contexto, não forneça informações incompletas nem induza a/o leitora/leitor em erro quanto à natureza, âmbito ou conteúdo do texto. A fonte do texto deve ser sempre indicada da seguinte forma: “© Conselho da Europa, ano de publicação”.

Todos os outros pedidos relativos à reprodução ou tradução, na totalidade ou em parte, do documento devem ser dirigidos à Divisão de Publicações e Identidade Visual do Conselho da Europa (F-67075 Estrasburgo Cedex ou publishing@coe.int).

Qualquer outra correspondência relativa a este documento deve ser dirigida à Coordenação de IA da Divisão de Programas de Inclusão e Antidiscriminação do Conselho da Europa, F-67075 Estrasburgo Cedex, e-mail: anti-discrimination@coe.int

Design da capa: Divisão de Publicações e Identidade Visual (DPIV), Conselho da Europa Diagramação da versão em inglês: Luminess Diagramação da versão em português: Formato Verde, Lda. Tradução: Multilingual Europe Trads Unip. Lda Revisão jurídica da tradução: Rute Silva Gomes Fotografias: Shutterstock, Unsplash and Better Images of AI

© Conselho da Europa, setembro de 2026

Índice

ABREVIATURAS	5
TERMINOLOGIA	6
AGRADECIMENTOS	9
RESUMO EXECUTIVO	10
INTRODUÇÃO	12
Elementos-chave do novo quadro jurídico	13
Categorias de risco ao abrigo do Regulamento sobre a IA	18
De que forma é que a metodologia aplica as categorias de risco?	20
Características protegidas	21
COMO UTILIZAR A METODOLOGIA	23
Passo 1	23
Passo 2	24
Passo 3	24
Passo 4	24
PASSO 1 - IDENTIFICAÇÃO DE SISTEMAS DE IA OU ALGORÍTMICOS	27
Como reconhecer sistemas algorítmicos e IA	28
1.1. Recolha inicial de informações	29
1.2. Pesquisa documental complementar	36
1.3. Identificação de sistemas algorítmicos ou de IA de risco elevado	40
1.4. Continuação do caso	43
PASSO 2 - RECOLHA DE INFORMAÇÕES SOBRE O SISTEMA ALGORÍTMICO OU DE IA PARA IDENTIFICAR DISCRIMINAÇÃO	47
2.1. Sistemas algorítmicos	50
2.2. Informações adicionais disponíveis para sistemas de IA de risco elevado	64
PASSO 3 - METODOLOGIA PARA AVALIAR A INFORMAÇÃO RECEBIDA	83
Introdução aos conceitos	85
Como utilizar o passo 3	93
3.1. Quais são os riscos conhecidos ou suspeitos de discriminação?	94
3.2. Existem características protegidas ou proxies conhecidos nos dados de entrada ou nos conjuntos de dados?	99
3.3. Avaliação dos riscos para os direitos fundamentais (avaliações de risco, AIDH, AIDF e AIPD)	102
3.4. Qual é a finalidade do sistema algorítmico e como é que ele funciona?	108
3.5. Dados de treino, teste e validação	114
3.6. Testes e avaliação	121

3.7. Avaliar se as provas são suficientes para fundamentar um caso <i>prima facie</i> de discriminação envolvendo um sistema de IA ou algorítmico	136
3.8. A parte inquirida pode demonstrar que a diferença de tratamento não é discriminatória?	140
PASSO 4 - VIAS DE RECURSO	149
4.1. Vias de recurso para todos os sistemas algorítmicos	151
4.2. Vias de recurso adicionais para sistemas de IA de risco elevado	157
4.3. O que fazer quando um sistema ou caso de utilização representa um risco para os direitos fundamentais, mas não é classificado como “de risco elevado” ou “proibido”	160
REFERÊNCIAS	164
Bibliografia	164
Legislação	171
Jurisprudência	173
ANEXO A - MODELO DE PEDIDO DE ACESSO DA PESSOA TITULAR DOS DADOS (PAPTD)	179
ANEXO B - MODELO PARA SOLICITAR EXPLICAÇÕES NOS TERMOS DO ARTIGO 86.º DO REGULAMENTO SOBRE A IA	182
ANEXO C - EXEMPLOS DA UTILIZAÇÃO DE ALGORITMOS E IA	184
ANEXO D - EXEMPLOS DE DISCRIMINAÇÃO ALGORÍTMICA OU DE RISCO DE DISCRIMINAÇÃO	186
ANEXO E - PROXIES	189
ANEXO F - LISTA DE REGISTOS DE IA E ALGORITMOS NA EUROPA	192
ANEXO G - DIRETIVAS EM MATÉRIA DE NÃO DISCRIMINAÇÃO, MOTIVOS PROTEGIDOS E ÂMBITO	194
ANEXO H - OUTROS REGULAMENTOS E ORIENTAÇÕES POTENCIALMENTE RELEVANTES	195
ANEXO I - PRÁTICAS DE IA DE RISCO ELEVADO	198
ANEXO J - PRÁTICAS PROIBIDAS EM MATÉRIA DE IA	200
ANEXO K - FICHA DE REGISTO PARA O PASSO 3	212

Abreviaturas

AFM	Autoridade de fiscalização do mercado
AIDF	Avaliação de impacto sobre os direitos fundamentais
AIDH	Avaliação de impacto sobre os direitos humanos
AIPD	Avaliação de impacto sobre a proteção de dados
APD	Autoridade de proteção de dados
CEPD	Comité Européu para a Proteção de Dados
DAL	Diretiva relativa à aplicação da lei
IA	Inteligência artificial
OI	Organismo para a igualdade
OSC	Organização da sociedade civil
PAPTD	Pedido de acesso da pessoa titular dos dados
RAL	Resolução alternativa de litígios
RGPD	Regulamento Geral sobre a Proteção de Dados
TDA	Tomada de decisão automatizada
TJUE	Tribunal de Justiça da União Europeia

Terminologia

Para efeitos da presente metodologia, foram feitas as seguintes escolhas terminológicas relevantes; caso contrário, os termos terão os significados a seguir indicados.

Sistema de IA: “um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais” (Regulamento sobre a IA, artigo 3.º, n.º 1).

Sistema algorítmico: termo utilizado nesta metodologia para abranger tanto os sistemas de IA como os sistemas que não são de IA, incluindo os sistemas de TDA. Inclui também sistemas de IA que não são utilizados em processos de tomada de decisão.

Sistema de tomada de decisão automatizada (TDA): este termo abrange uma vasta gama de sistemas automatizados, que são utilizados no contexto da tomada de decisões ou com esse objetivo. Podem basear-se em IA, mas também podem basear-se noutras tecnologias, mesmo que sejam tão simples como regras básicas do tipo “se... então...”. Estes sistemas vão desde sistemas totalmente automatizados, que não envolvem qualquer intervenção humana, até sistemas semiautomatizados ou de apoio à tomada de decisões, que incluem tanto a intervenção de máquinas como a intervenção humana e são amplamente utilizados na prática.

Pessoa responsável: uma pessoa pertencente a um organismo para a igualdade que realiza a avaliação em qualquer etapa desta metodologia, no âmbito do seu trabalho de investigação de casos de discriminação.¹

Pessoa(s) queixosa(s): a pessoa ou grupo de pessoas que alega ou é vítima de discriminação (ilegal). Por uma questão de coerência com a redação do RGPD e do Regulamento sobre a IA, os termos “pessoas titular(es) de dados” e “pessoa(s) afetada(s)” correspondem a “pessoa(s) queixosa(s)” quando se fazem referência às disposições relevantes desses regulamentos, respetivamente.

Matriz de confusão: uma tabela utilizada para avaliar o desempenho de um sistema algorítmico, comparando as suas previsões com os resultados reais observados no mundo real. As linhas da tabela da matriz de confusão representam os resultados reais, enquanto as colunas representam as previsões do sistema. A tabela mostra quantas das previsões estavam corretas ou incorretas.

Especialista: uma pessoa com conhecimentos especializados ou competências técnicas, consultada ou envolvida pelo organismo para a igualdade para apoiar a

1. Embora esta metodologia se destine principalmente aos OI, pode também ser relevante para as estruturas nacionais de direitos humanos (ENDH), as instituições de provedoria ou outras partes interessadas. Nos casos em que esta metodologia é aplicada pelas ENDH e pelas provedorias de justiça, o termo “pessoa responsável” também pode referir-se às pessoas responsáveis desses organismos.

pessoa responsável em qualquer etapa desta metodologia. A/O especialista presta aconselhamento especializado, mas não é a pessoa responsável principal.

Sistema de IA de risco elevado: ou “IA de risco elevado”, esta expressão é utilizada para se referir a um sistema de IA, tal como definido de forma exaustiva no artigo 6.º do Regulamento sobre a IA.

Dados de entrada: quaisquer informações, sinais ou dados brutos fornecidos ao sistema algorítmico, com base nos quais o sistema chega ao seu resultado. Por exemplo, uma aplicação de rastreio do cancro baseada em IA, destinada a detetar sinais suspeitos, pode utilizar a idade, o sexo e uma fotografia do sinal como dados de entrada. Num sistema LLM (modelo de linguagem de grande escala) como o ChatGPT, os dados de entrada são o texto da interação de chat e, potencialmente, também o texto de interações de chat anteriores.

Autoridade de fiscalização do mercado: a autoridade ou autoridades nacionais que realizam atividades e tomam medidas ao abrigo do Regulamento (UE) n.º 2019/1020 (fiscalização do mercado e conformidade dos produtos).

Não discriminação: o termo “não discriminação” é utilizado em vez de “igualdade” ou de termos relacionados.

Diretivas em matéria de não discriminação: o termo refere-se às diretivas da UE enumeradas no Anexo G.

Organismo notificado: trata-se de um organismo de avaliação da conformidade que realiza avaliações de conformidade por terceiros, incluindo testes, certificação e inspeção. Por exemplo, o organismo notificado avalia a conformidade dos sistemas de IA de risco elevado, em conformidade com os procedimentos de avaliação da conformidade estabelecidos no Regulamento sobre a IA da UE.

Sistema de IA de risco não elevado: um sistema de IA que não está incluído na definição exaustiva de IA de risco elevado prevista no Regulamento sobre a IA. Note-se que isto significa apenas que estes sistemas não são classificados como de risco elevado ao abrigo do Regulamento sobre a IA, e não que estes sistemas de IA são isentos de riscos.

Dados de saída: o resultado do sistema algorítmico após o processamento dos dados de entrada. Por exemplo, uma característica prevista sobre uma pessoa, uma pontuação, uma recomendação, uma decisão ou conteúdos como imagens, vídeos ou texto.

Entidade prestadora/responsável pela implantação: estes termos são utilizados na aceção que lhes é atribuída no artigo 3.º do Regulamento sobre a IA. Embora definidos com referência aos sistemas de IA, os respetivos papéis podem também aplicar-se, por analogia, a sistemas que não sejam de IA.

TDA elegível: para efeitos da presente metodologia, entende-se por “TDA elegível” uma subcategoria de sistemas de TDA que cumpre os critérios definidos no artigo 22.º do RGPD, relativos à tomada de decisões “exclusivamente” automatizada (Regulamento (UE) n.º 2016/679). Estes sistemas implicam maiores obrigações em matéria de transparência e informação ao abrigo do RGPD.

Parte inquirida: a organização ou entidade alvo de investigação por parte do organismo para a igualdade por discriminação ilegal, na sequência de uma queixa, de um procedimento *ex officio* ou de uma notificação da autoridade de fiscalização do mercado (AFM). No contexto do RGPD e do Regulamento sobre a IA, as partes inquiridas podem ser designadas por “responsáveis pelo tratamento de dados” e “entidades prestadoras de IA” ou “responsáveis pela implantação”, respetivamente, tal como definido nesses regulamentos.

No que diz respeito à terminologia relacionada com o Regulamento sobre a IA da UE, consulte [o artigo 3.º do Regulamento sobre a IA da UE](#).

Agradecimentos

O presente relatório foi elaborado no âmbito do projeto “Promoção da Igualdade e da Não Discriminação pelos Organismos para a Igualdade no que diz respeito à Utilização da Inteligência Artificial nas Administrações Públicas”, cofinanciado pela União Europeia através do Instrumento de Apoio Técnico e pelo Conselho da Europa. O projeto é implementado pelo Conselho da Europa em cooperação com a Comissão Europeia, o Centro Interfederal para a Igualdade de Oportunidades (Unia, Bélgica), a Provedoria de Justiça para a Não Discriminação (YVV, Finlândia) e a Comissão para a Cidadania e a Igualdade de Género (CIG, Portugal).

O relatório foi elaborado por Louise Hooper (consultora internacional, Conselho da Europa), Ylja Remmits e Ioanna Papageorgiou (auditoras de algoritmos/consultoras internacionais, Conselho da Europa). O Conselho da Europa deseja expressar a sua gratidão às instituições beneficiárias do projeto e à Comissão Europeia pelo seu empenho constante ao longo de todo o processo de elaboração, e, em particular, a: Nele Roekens, Sophie Vincent, Thelma Raes e Laetitia Parmentier (Unia, Bélgica); Tiina Valonen e Ville Rantala (YVV, Finlândia); Carla Peixe, Lúcia Pestana e Alexandra Andrade (CIG, Portugal); Massimiliano Santini (Grupo de Trabalho para a Reforma e o Investimento, Secretariado-Geral, Comissão Europeia); e Menno Ettema, Sara Haapalainen, Ayca Dibekoğlu e Delfine Gaillard (Divisão de Programas de Inclusão e Antidiscriminação, Conselho da Europa).

Um agradecimento especial a Raphaële Xenidis, Kris Shrishak, Brent Mittelstadt, Chris Russell, Ydo Bergstra e Jurriaan Parie pelas suas contribuições na revisão, e a Laurens Naudts e Plixavra Vogiatzoglou pelos seus contributos especializados. O relatório contou também com as discussões e contribuições de especialistas nacionais de organismos para a igualdade e de organizações da sociedade civil que participaram num seminário e num workshop multinacionais, realizados em Bruxelas, a 15 de abril de 2026. Todas estas perspetivas enriqueceram as secções analíticas e operacionais destas orientações.



YHDENVERTAISUUSVALTUUTETTU
NON-DISCRIMINATION OMBUDSMAN



CIG

COMISSÃO PARA A CIDADANIA
E A IGUALDADE DE GÉNERO

Resumo executivo

Os sistemas algorítmicos podem reforçar e criar discriminação, uma vez que são frequentemente concebidos para diferenciar as pessoas singulares: classificando-as, ordenando-as por importância ou selecionando-as como alvo. Em combinação com as desigualdades históricas e os preconceitos humanos incorporados nos dados, nas regras e nas escolhas de conceção dos sistemas algorítmicos, os padrões discriminatórios podem ser reproduzidos e ampliados, a menos que sejam identificados e mitigados de forma proativa.

Esta metodologia fornece orientações passo a passo aos organismos para a igualdade (OI) e a outras estruturas de direitos humanos na Europa para avaliarem casos de discriminação relacionados com a inteligência artificial (IA) ou com sistemas algorítmicos. Destina-se às pessoas responsáveis, consultores e advogadas/os destas entidades que investigam denúncias de discriminação que envolvam ou se suspeite que envolvam IA ou tomada de decisão automatizada (TDA). O seu objetivo é servir de lista de referência de questões e fontes a ter em conta em cada etapa de uma avaliação. A metodologia divide-se em quatro etapas iterativas:

Passo 1: identificação de casos relacionados com IA ou algoritmos

Passo 2: recolha de informações sobre a IA ou o sistema algorítmico para identificar situações de discriminação

Passo 3: metodologia para avaliar a informação recebida

Passo 4: vias de recurso

Estas etapas baseiam-se no quadro regulamentar europeu em matéria de IA, nomeadamente no Regulamento sobre a IA da UE, e na legislação relativa à não discriminação, e fazem referência a outra legislação, como a relativa à proteção de dados, casos exemplificativos e jurisprudência, sempre que relevante. As etapas estabelecem distinções entre os sistemas de IA de risco elevado e outros sistemas, em conformidade com o Regulamento sobre a IA da UE, prevendo meios para aceder à documentação técnica, aos dados e aos resultados dos testes dos sistemas de risco elevado, especialmente por parte dos organismos designados como “autoridades responsáveis pela proteção dos direitos fundamentais” nos termos do artigo 77.º do Regulamento sobre a IA da UE.

A metodologia não se centra na legislação nacional e, em alguns países, a legislação nacional pode prever meios mais eficazes para garantir o acesso à informação ou poderes de investigação em matéria de discriminação algorítmica. As pessoas responsáveis devem ter estas considerações em conta ao utilizarem esta ferramenta.

Para apoiar a aplicação das quatro etapas, a metodologia inclui uma extensa lista de anexos que fornecem modelos de cartas para solicitar informações, ajudam a compreender os riscos de discriminação algorítmica - por exemplo, por tipo de sistema de IA ou pelo setor em que o sistema é utilizado - e auxiliam na avaliação das informações, nomeadamente através de uma lista de verificação/ficha de registo para o passo 3.

Para facilitar a utilização desta metodologia, é útil ter um conhecimento básico sobre IA, enviesamento e discriminação algorítmicos e sobre a terminologia relacionada, embora a ferramenta também forneça uma lista de terminologia. Outras publicações elaboradas no âmbito do projeto “Promoção da Igualdade e da Não Discriminação pelos Organismos para a Igualdade no que diz respeito à Utilização da Inteligência Artificial nas Administrações Públicas” complementam esta metodologia e podem contribuir para a construção desse conhecimento básico.

- ▶ [Proteção jurídica contra a discriminação algorítmica na Europa: quadros jurídicos atuais e lacunas remanescentes](#), dezembro de 2025 (também disponível em francês, holandês, português, finlandês, sueco).
- ▶ [Orientações políticas europeias sobre IA e discriminação baseada em algoritmos para organismos para a igualdade e outras estruturas nacionais de direitos humanos](#), dezembro de 2025 (também disponível em francês, holandês, português, finlandês, sueco).

Introdução

Os novos quadros regulamentares em matéria de IA, tais como o Regulamento sobre a IA da UE², as diretivas da UE relativas às normas para os organismos para a igualdade (doravante designadas “as diretivas relativas às normas”)³ e a Convenção-Quadro do Conselho da Europa sobre Inteligência Artificial, Direitos Humanos, Democracia e Estado de Direito (doravante designada “Convenção-Quadro do Conselho da Europa sobre IA”), proporcionam novas ferramentas e competências aos organismos para a igualdade e às estruturas de direitos humanos para investigarem a discriminação algorítmica.

Estas ferramentas apresentam algumas limitações e desafios. Por exemplo, alguns sistemas algorítmicos discriminatórios podem não ser classificados como IA ao abrigo do Regulamento sobre a IA da UE.⁴ Além disso, muitos aspetos jurídicos relacionados com a IA e a discriminação ainda não se encontram bem definidos. Por fim, para muitas leitoras e leitores e pessoas responsáveis, esta será uma área do direito nova e relativamente complexa.

Apesar destes desafios, esta metodologia em quatro etapas visa apoiar e fornecer uma estrutura para analisar sistematicamente o impacto discriminatório de uma decisão ou tratamento que possa ter sido tomado por um sistema algorítmico ou com a sua ajuda. As leitoras e leitores não devem considerar cada passo da metodologia como algo que tenha de ser concluído. Pelo contrário, estes passos constituem um manual de referência que contém uma variedade de ferramentas para identificar sistemas, recolher e avaliar provas e decidir quais as medidas a tomar. Ao seguir os passos previstos na metodologia e ao recorrer à assistência de especialistas (técnicos) sempre que necessário, deverá ser possível reunir os elementos necessários para estabelecer a presunção de discriminação e solicitar vias de recurso em casos de discriminação algorítmica.

2 Regulamento (UE) n.º 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial).

3 Diretiva (UE) 2024/1499 do Conselho, de 7 de maio de 2024, que estabelece as normas aplicáveis aos organismos para a igualdade em questões de igualdade de tratamento entre pessoas independentemente da sua origem racial ou étnica, de igualdade de tratamento no emprego e na atividade profissional entre as pessoas, independentemente da sua religião ou crença, deficiência, idade ou orientação sexual, e de igualdade de tratamento entre homens e mulheres em matéria de segurança social e no acesso a bens e serviços e seu fornecimento, e que altera as Diretivas 2000/43/CE e 2004/113/CE e a Diretiva (UE) 2024/1500 do Parlamento Europeu e do Conselho, de 14 de maio de 2024, que estabelece normas aplicáveis aos organismos para a igualdade em questões de igualdade de tratamento e igualdade de oportunidades entre mulheres e homens em domínios ligados ao emprego e à atividade profissional, e que altera as Diretivas 2006/54/CE e 2010/41/UE.

4 Alguns exemplos de discriminação algorítmica baseiam-se em sistemas simples, assentes em regras, que não se enquadram na definição de IA, tais como os exemplos holandeses de algoritmos discriminatórios no escândalo dos subsídios de acolhimento de crianças (Amnistia Internacional 2021) e na avaliação do risco de fraude pela Agência Executiva da Educação dos Países Baixos (Rechtbank Overijssel 2024).

Os OI devem abordar as queixas de discriminação relacionadas com a IA e a TDA tal como qualquer outro caso de discriminação, mas devem também reconhecer que a falta de transparência ou a incerteza quanto ao funcionamento de um sistema algorítmico podem ser tidas em conta ao decidir se existe um risco de discriminação ou se foi estabelecido um caso *prima facie*. Isto deve-se ao reconhecimento crescente de que existe um desequilíbrio de poder e de informação entre as empresas que criam sistemas de IA, as responsáveis pela sua implementação e aquelas em relação às quais os sistemas são implementados.⁵ Nessas circunstâncias, o ónus da prova pode recair sobre a parte inquirida, que deverá demonstrar que o sistema algorítmico não discriminou nem contribuiu para a discriminação de forma ilegal. Para que as pessoas afetadas tenham acesso efetivo à justiça, será necessário um maior grau de transparência.

O *Omnibus Digital* em matéria de IA,⁶ um pacote legislativo que altera e simplifica o Regulamento sobre a IA e outras leis, foi aprovado pelo Parlamento Europeu. Sempre que pertinente, são feitas referências a estas alterações.

Elementos-chave do novo quadro jurídico

As diretivas relativas às normas

As diretivas relativas às normas, que devem ser transpostas até 19 de junho de 2026 (artigo 24.º das diretivas relativas às normas), estabelecem requisitos mínimos para o funcionamento dos organismos para a igualdade, com vista a melhorar a sua eficácia e garantir a sua independência. Estas competências devem ser interpretadas em conjunto com as competências já previstas nas diretivas da UE em matéria de não discriminação.

A Diretiva 2024/1500, no Considerando 21, e a Diretiva 2024/1499, no Considerando 22, estabelecem, no que diz respeito à afetação de recursos financeiros, que:

É fundamental prestar atenção às oportunidades e aos riscos decorrentes da utilização de sistemas automatizados, incluindo a inteligência artificial. Em especial, os organismos para a igualdade deverão estar dotados de recursos humanos e técnicos adequados. Esses recursos deverão, nomeadamente, permitir aos organismos para a igualdade que utilizem, por um lado, sistemas automatizados no seu trabalho, e por outro, avaliem a sua conformidade com as regras de não discriminação. Quando o organismo para a igualdade faça parte de um organismo com vários mandatos, deverão ser assegurados os recursos necessários ao desempenho do seu mandato.⁷

⁵ Este assunto é abordado em pormenor na subsecção 3.8.

⁶ Regulamento (UE) 2026/1744 do Parlamento Europeu e do Conselho, de 8 de julho de 2026, que altera os Regulamentos (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 no que diz respeito à simplificação da aplicação das regras harmonizadas em matéria de inteligência artificial (Regulamento *Omnibus Digital* em matéria de IA). Disponível em: <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>, consultado a 24 de julho de 2026.

⁷ O artigo 26.º da Convenção-Quadro sobre IA exige igualmente que os OIs sejam eficazes, imparciais e independentes, disponham de recursos suficientes e possuam poderes e conhecimentos especializados adequados.

Regulamento sobre a IA da UE, artigo 77.º: poderes das autoridades responsáveis pela proteção dos direitos fundamentais e cooperação com as autoridades de fiscalização do mercado

São atribuídos novos poderes aos organismos para a igualdade e às estruturas nacionais de direitos humanos (ENDH) que cumpram os requisitos do artigo 77.º do Regulamento sobre a IA⁸ no que diz respeito aos sistemas de IA de risco elevado, a fim de garantir que possam cumprir o seu mandato.⁹ As atuais propostas no *Omnibus* Digital em matéria IA visam esclarecer que estes poderes não prejudicam os poderes existentes nem a independência destes organismos.¹⁰

A lista das autoridades responsáveis pela proteção dos direitos fundamentais deveria ter sido notificada à Comissão Europeia até 2 de novembro de 2024 e os Estados-Membros “devem [manter a lista das autoridades] atualizada”.¹¹ A Comissão reconhece que a lista dos organismos abrangidos pelo “artigo 77.º” é atualizada continuamente, à luz da implementação em curso do Regulamento sobre a IA.¹² Os Ols que não tenham sido indicados pelos Estados-Membros até ao primeiro prazo de notificação ainda podem ser adicionados. Os Ols também poderiam ser retirados da lista.

As autoridades competentes estão habilitadas, nos termos do n.º 1 do artigo 77.º, a solicitar e a aceder a qualquer documento criado ou mantido ao abrigo do Regulamento sobre a IA, em linguagem e formato acessíveis, caso tal seja necessário para o cumprimento eficaz do seu mandato, dentro dos limites da sua competência. Isto deverá significar que podem ser apresentados pedidos relativos à documentação criada ou mantida por outras autoridades nacionais competentes, incluindo as autoridades de fiscalização do mercado e os organismos notificados, bem como por prestadores, responsáveis pela implantação ou outros intervenientes no ciclo de vida de um sistema de IA. O *Omnibus* Digital esclarece que os pedidos de acesso a informações e documentação devem ser dirigidos às autoridades de fiscalização

8 N.º 1 do artigo 77.º do Regulamento sobre a IA, incluindo as alterações Omnibus: “As autoridades ou organismos públicos nacionais que supervisionam ou asseguram o respeito das obrigações previstas na legislação da União que protege os direitos fundamentais, incluindo o direito à não discriminação, têm poderes para solicitar e aceder a quaisquer informações ou documentação criadas ou mantidas, da autoridade de fiscalização do mercado competente, nos termos do presente regulamento numa língua acessível e num formato legível por máquina, por via eletrónica, sempre que o acesso a essas informações ou documentação for necessário para o exercício dos seus mandatos dentro dos limites das respetivas jurisdições. O presente artigo aplica-se sem prejuízo das competências, das atribuições, dos poderes e da independência das autoridades ou dos organismos públicos nacionais competentes no âmbito dos respetivos mandatos.”

9 Nem todos os organismos para a igualdade se enquadram na definição prevista no artigo 77.º, embora muitos o façam. O termo “autoridade nos termos do artigo 77.º” é utilizado ao longo do presente documento para designar qualquer OI ou ENDH que corresponda à definição prevista no artigo 77.º do Regulamento sobre a IA.

10 Regulamento (UE) 2026/1744 do Parlamento Europeu e do Conselho, de 8 de julho de 2026, que altera os Regulamentos (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 no que diz respeito à simplificação da aplicação das regras harmonizadas em matéria de inteligência artificial (Regulamento Omnibus Digital em matéria de IA). Disponível em: <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>, consultado a 24 de julho de 2026.

11 Regulamento sobre a IA, artigo 77.º, n.º 2.

12 <https://digital-strategy.ec.europa.eu/en/policies/fundamental-rights-protection-authorities-ai-act>, consultada a 5 de junho de 2026.

do mercado, as quais devem conceder “acesso a essas informações ou documentação, nomeadamente solicitando, quando necessário e sem demora injustificada, essas informações ou documentação a quem presta ou é responsável pela implantação”¹³ e que as autoridades ou organismos envolvidos “cooperam estreitamente e prestam-se a assistência mútua necessária ao exercício dos respetivos mandatos”.¹⁴ Esta cooperação e assistência incluirão o intercâmbio de informações, sempre que necessário para a supervisão ou aplicação eficaz do Regulamento sobre a IA e de outra legislação da União, o que incluiria as diretivas em matéria de não discriminação (ver [Anexo G](#)).

Se a documentação for insuficiente para determinar se ocorreu uma violação das obrigações decorrentes do direito da União em matéria de proteção dos direitos fundamentais, o organismo para a igualdade pode apresentar um pedido fundamentado à autoridade de fiscalização do mercado, no sentido de esta organizar a realização de testes ao sistema de IA de risco elevado através de meios técnicos (Regulamento sobre a IA da UE, artigo 77.º, n.º 3; ver [Passo 4](#)).

Qualquer informação ou documentação obtida deve ser tratada em conformidade com os requisitos de confidencialidade previstos no artigo 78.º. O n.º 2 do artigo 78.º esclarece que a autoridade a que se refere o artigo 77.º deve solicitar apenas os dados estritamente necessários para a avaliação do risco representado pelos sistemas de IA e para o exercício dos seus poderes, em conformidade com o regulamento e com o direito da União. Qualquer solicitação ao abrigo do Regulamento sobre a IA deve, por conseguinte, ser claro e específico, para evitar que seja recusado.

Sempre que forem solicitados e obtidos dados, o organismo para a igualdade deve assegurar a existência de medidas de cibersegurança adequadas e eficazes para proteger a segurança e a confidencialidade das informações e dos dados obtidos, e deve apagar esses dados assim que deixem de ser necessários para a finalidade para a qual foram obtidos, em conformidade com a legislação aplicável da União ou nacional.

Da mesma forma, as normas do Conselho da Europa, tais como a Convenção-Quadro sobre a IA e a [Recomendação CM/Rec\(2026\)1 sobre igualdade e inteligência artificial](#), definem as medidas a tomar pelos Estados-Membros e outras partes interessadas para promover a igualdade e prevenir e combater a discriminação em todas as atividades ao longo do ciclo de vida dos sistemas de IA.

Confidencialidade

Os requisitos de confidencialidade estão estabelecidos no n.º 1 do artigo 78.º do Regulamento sobre a IA, segundo os quais a Comissão Europeia, as autoridades

¹³ Regulamento (UE) 2026/1744 do Parlamento Europeu e do Conselho, de 8 de julho de 2026, que altera os Regulamentos (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 no que diz respeito à simplificação da aplicação das regras harmonizadas em matéria de inteligência artificial (Regulamento Omnibus Digital em matéria de IA). Disponível em: <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>, consultado a 24 de julho de 2026.

¹⁴ Ibid.

de fiscalização do mercado e os organismos notificados (artigo 70.º), bem como qualquer outra pessoa singular ou coletiva envolvida na aplicação do Regulamento sobre a IA, devem respeitar a confidencialidade das informações e dos dados obtidos, de forma a proteger:

- ▶ os direitos de propriedade intelectual e as informações comerciais confidenciais ou segredos comerciais de uma pessoa singular ou coletiva, incluindo o código-fonte (Diretiva (UE) 2016/943, artigo 5.º). No que diz respeito aos organismos para a igualdade, o artigo 5.º da Diretiva 2016/943 prevê uma exceção com o objetivo de revelar condutas indevidas, irregularidades ou atividades ilegais, desde que a parte inquirida (o OI ou, potencialmente, a AFM) tenha agido com o objetivo de proteger o interesse público geral (artigo 5.º, alínea b)) ou de proteger um interesse legítimo reconhecido pelo direito da União ou pelo direito nacional (artigo 5.º, alínea d)). A proteção dos direitos fundamentais e a prevenção ou combate à discriminação estão, pelo menos em certa medida, abrangidos por esta exceção;
- ▶ a aplicação efetiva do regulamento, nomeadamente para efeitos de inspeções, inquéritos ou auditorias;
- ▶ interesses de segurança pública e nacional;
- ▶ a condução de processos penais ou administrativos;
- ▶ informações classificadas nos termos da legislação da União ou nacional.

De momento, não é claro de que forma estes fatores poderão afetar a capacidade do OI de obter informações junto das partes relevantes; no entanto, nos casos em que a divulgação seja recusada invocando a confidencialidade, o OI poderá recorrer a uma autoridade competente ao abrigo do Regulamento sobre a IA da UE ou à APD ao abrigo do RGPD. É provável que, nos casos em que os segredos comerciais sejam invocados como motivo para a não divulgação, a autoridade de supervisão competente ou o tribunal possa ter de ponderar os direitos e interesses em causa, com vista a determinar o que deve ser divulgado (ver CK contra Dun & Bradstreet Austria GmbH e Magistrat der Stadt Wien (2025), analisado no passo 2.1).

Cooperação intersetorial

Para que o novo quadro jurídico seja plenamente eficaz, será também necessário procurar estabelecer, desenvolver, reforçar e formalizar a cooperação com as autoridades de fiscalização do mercado competentes, as autoridades de proteção de dados e quaisquer outras autoridades previstas no artigo 77.º, caso tal ainda não exista. Esta obrigação de cooperação é formalizada no *Omnibus* Digital através de uma alteração que insere o n.º 1-B do artigo 77.º.¹⁵ Para o efeito, poderá

15 Regulamento (UE) 2026/1744 do Parlamento Europeu e do Conselho, de 8 de julho de 2026, que altera os Regulamentos (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 no que diz respeito à simplificação da aplicação das regras harmonizadas em matéria de inteligência artificial (Regulamento Omnibus Digital em matéria de IA). Disponível em: <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>, consultado a 24 de julho de 2026.

ser necessário ou útil elaborar protocolos de trabalho interinstitucionais.¹⁶ Para ver exemplos e boas práticas, consulte o quadro abaixo. As novas diretivas relativas às normas preveem a criação de quadros nacionais para a realização de inquéritos que permitam aos organismos para a igualdade proceder à apuração dos factos, incluindo mecanismos adequados de cooperação entre organismos para a igualdade e outras autoridades públicas relevantes para esse efeito (artigo 8.º das diretivas relativas às normas).

As negociações entre os OIs e os governos dos seus Estados-Membros, com vista a garantir uma base jurídica clara para a partilha de informações entre os organismos abrangidos pelo artigo 77.º, incluindo os organismos para a igualdade e as autoridades de proteção de dados, bem como entre as AFM e os organismos abrangidos pelo artigo 77.º - tal como previsto na sua cooperação nos termos dos artigos 73.º, n.º 7, e do artigo 79.º, n.º 2, do Regulamento sobre a IA - desempenharão um papel fundamental a este respeito (Autoriteit Persoonsgegevens 2024, n.º 37). A existência dessas bases jurídicas é um pré-requisito para a celebração de acordos de cooperação bilaterais e multilaterais com vista à partilha de informações. Esses acordos devem ser redigidos em termos amplos, de modo a abranger o âmbito de competências das entidades abrangidas pelo artigo 77.º e das AFM, e a permitir a celebração de acordos bilaterais adicionais específicos para cada caso, sempre que necessário (Autoriteit Persoonsgegevens 2024, n.º 37).

Exemplos e práticas promissoras

No Reino Unido, a Comissão para a Igualdade e os Direitos Humanos colaborou com o Gabinete de Informação, no âmbito do desafio da equidade e da inovação, em casos-piloto nos domínios do ensino superior, finanças, cuidados de saúde e recrutamento, com o objetivo de encontrar novas formas de combater os enviesamentos e a discriminação de natureza estatística, humana e estrutural nos sistemas de IA. O desafio foi financiado pelo Ministério da Ciência do Reino Unido (Departamento de Ciência, Tecnologia e Inovação, 2024).

Na Noruega, o organismo para a igualdade tem colaborado com a autoridade de proteção de dados no âmbito de um ambiente de teste regulatório sobre inteligência artificial (Autoridade Norueguesa de Proteção de Dados, 2023).

Em França, a cooperação entre o Defensor dos Direitos e a autoridade de proteção de dados, a Commission Nationale de l'Informatique et des Libertés (CNIL), é facilitada por vários mecanismos: ambas as instituições têm um memorando de entendimento e o Defensor dos Direitos desempenha também um papel consultivo junto do conselho de administração da CNIL. Devido a esta ligação estrutural, o Defensor dos Direitos é informado de todos os projetos apresentados nas reuniões plenárias do conselho de administração da CNIL (Conselho da Europa, 2025b).

16 Ver também o artigo 26.º da Convenção-Quadro do Conselho da Europa sobre IA (2024), “Deve ser facilitada uma cooperação eficaz entre as instituições”, e o artigo 14.º das diretivas relativas às normas, que exigem mecanismos de cooperação adequados.

No Reino Unido, um memorando de entendimento entre o Information Commissioner's Office (a APD) e a Comissão para a Igualdade e os Direitos Humanos (o organismo para a igualdade) estabelece os princípios relativos à partilha de informações e à cooperação, as bases jurídicas em que a partilha de informações pode ocorrer, os aspetos práticos relacionados com o controlo e o tratamento de dados e os respetivos papéis, funções e poderes de cada organismo. Ver: Memorando de Entendimento

Categorias de risco ao abrigo do Regulamento sobre a IA

O Regulamento sobre a IA da UE adota um quadro regulamentar que classifica os sistemas de IA de acordo com um nível presumido de risco que representam para os direitos fundamentais, a saúde e a segurança (Regulamento sobre a IA da UE, Artigo 1.º). Esta abordagem reflete a ideia de que nem todos os sistemas de IA suscitam o mesmo nível de preocupação: alguns representam riscos inaceitáveis e devem ser totalmente proibidos, outros apresentam riscos significativos que exigem uma supervisão rigorosa, enquanto outros são considerados como não necessitando de qualquer regulamentação específica em matéria de IA.

A categoria de risco determina as obrigações aplicáveis - que vão desde a proibição absoluta até requisitos técnicos abrangentes e deveres básicos de transparência. Para os organismos para a igualdade, esta estrutura baseada no risco é diretamente relevante: determina quais as informações e a documentação que devem existir e influencia as vias de recurso disponíveis ao abrigo do Regulamento sobre a IA.

IA proibida

O Regulamento sobre a IA da UE proíbe determinadas práticas de IA que representem riscos inaceitáveis para os direitos fundamentais, a segurança ou os valores democráticos (artigo 5.º do Regulamento sobre a IA). Estas incluem:

- ▶ técnicas manipuladoras que distorcem substancialmente o comportamento, incluindo a produção de conteúdos sexuais e íntimos sem consentimento ou de material de abuso sexual de menores (CSAM);
- ▶ exploração de vulnerabilidades;
- ▶ sistemas de pontuação social;
- ▶ avaliações de risco de pessoas singulares com o objetivo de prever a prática de crimes com base na definição de perfis;
- ▶ Identificação biométrica remota em tempo real em espaços públicos (com exceções limitadas);
- ▶ reconhecimento de emoções em contextos laborais e educativos;
- ▶ categorização biométrica que deduza características protegidas;
- ▶ recolha indiscriminada de imagens faciais.

Ver também o [Anexo J - Práticas proibidas em matéria de IA](#).

IA de risco elevado

Os sistemas de IA de risco elevado incluem casos de utilização que se considera representarem riscos significativos para a saúde, a segurança ou os direitos fundamentais e que são utilizados em domínios específicos enumerados no Anexo III do Regulamento sobre a IA (artigo 6.º). Estes incluem sistemas utilizados em:

- ▶ biometria
- ▶ gestão de infraestruturas críticas
- ▶ educação e formação profissional
- ▶ emprego e gestão de trabalhadores
- ▶ acesso a serviços e prestações essenciais
- ▶ aplicação da lei
- ▶ migração, asilo e controlo de fronteiras
- ▶ administração da justiça.

Nota: um sistema de IA referido no Anexo III deve ser sempre considerado de risco elevado se esse sistema de IA efetuar a definição de perfis de uma pessoa singular.

Ver também o [Anexo I - Práticas de IA de risco elevado](#)

Se o sistema de IA se destinar a realizar qualquer uma das seguintes funções, o sistema não será considerado de risco elevado (artigo 6.º, n.º 3):

- ▶ uma tarefa processual restrita;
- ▶ melhorar os resultados de uma atividade humana previamente concluída;
- ▶ detetar padrões de tomada de decisões ou desvios em relação a padrões de tomada de decisões anteriores;
- ▶ uma tarefa preparatória para uma avaliação.

Os sistemas de IA de risco elevado estão sujeitos a requisitos de documentação exaustivos, obrigações de transparência e procedimentos de gestão de riscos ao abrigo do Regulamento sobre a IA.

IA de finalidade geral (IAFG)

As categorias de risco elevado e proibidas abrangem casos de utilização específicos, e a categorização baseia-se na finalidade explícita dos sistemas. Em contrapartida, os modelos de IA de finalidade geral, por exemplo, os modelos de linguagem de grande escala (LLM), são modelos capazes de realizar uma vasta gama de tarefas distintas e que podem ser integrados numa variedade de sistemas ou aplicações a jusante (Regulamento sobre a IA, artigo 3.º, n.º 63). A IAFG, por definição, não tem um objetivo específico. Um modelo de IAFG pode, no entanto, constituir a base de aplicações específicas com finalidades específicas que poderiam ser classificadas na categoria de risco elevado.

É improvável que a documentação elaborada em resultado das obrigações impostas à IAFG esteja disponível para as OI ao abrigo do Regulamento sobre a IA, uma vez que os direitos de acesso se limitam às aplicações de sistemas de IA de risco elevado (Regulamento sobre a IA, artigo 77.º). Os OIs teriam o direito de

recorrer aos seus poderes atuais e à legislação nacional, mas, na maioria dos casos, é altamente provável que seja necessária uma decisão judicial. Para efeitos desta metodologia, os modelos de IAFG são, em termos gerais, incluídos na categoria dos sistemas algorítmicos.

De que forma é que a metodologia aplica as categorias de risco?

No Regulamento sobre a IA da UE, tal como explicado acima, estão previstas novos poderes para a obtenção de informações relativas a sistemas de risco elevado. A metodologia está, portanto, estruturada principalmente em torno da distinção entre sistemas de IA de risco elevado e outros sistemas algorítmicos. No caso da IA de risco não elevado, espera-se que os OIs funcionem ao abrigo do mesmo quadro informativo que se aplica aos restantes sistemas algorítmicos. O passo 1 da metodologia ajuda as pessoas responsáveis a compreender que tipo de sistema estão a analisar.

O Regulamento sobre a IA impõe requisitos regulamentares adicionais às diversas partes intervenientes envolvidas no desenvolvimento, distribuição e implementação de sistemas de IA de risco elevado. No que diz respeito a esses sistemas, isto proporcionará informações significativas e relevantes sobre as medidas de gestão de riscos, os dados utilizados e as medidas de governação de dados em vigor, a documentação técnica que explica as principais escolhas de conceção e de dados e a finalidade pretendida do sistema, bem como informações sobre os testes e a monitorização e os riscos de discriminação identificados. Esta documentação constituirá um recurso essencial para os organismos para a igualdade que pretendam identificar ou avaliar potenciais casos de discriminação algorítmica.

Essas informações não estarão disponíveis em todos os casos, nem mesmo na maioria deles. No entanto, estes requisitos também ajudam os OIs a identificar e interpretar as provas relativas à IA e a outros sistemas algorítmicos, nos casos em que não existam tais requisitos formais. Isto deve-se ao facto de servirem como passos de referência para identificar, reduzir ou eliminar o risco de discriminação, sendo que a documentação faz frequentemente parte do desenvolvimento padrão técnico e de software.

A metodologia procura distinguir, ao longo do texto, entre as circunstâncias em que é conferida a um OI, nos termos do artigo 77.º do Regulamento sobre a IA da UE, o poder para solicitar e aceder à documentação criada ou mantida ao abrigo desse Regulamento sobre a IA no que diz respeito a sistemas de risco elevado e os casos em que tal poder não existe.

É importante ter em conta que os quadros jurídicos nacionais conferem frequentemente aos organismos para a igualdade poderes de recolha de informações ou de investigação. Os organismos para a igualdade que não sejam autoridades nos termos do artigo 77.º não dispõem de uma base jurídica direta ao abrigo do Regulamento sobre a IA para aceder à documentação relevante relativa a sistemas de IA de risco elevado, mas poderão, ainda assim, recorrer a estes poderes previstos na legislação nacional e noutros atos legislativos da União.

Características protegidas

Ao longo desta metodologia, são referidas características protegidas. Estas são características protegidas pela Convenção Europeia dos Direitos Humanos (a Convenção) e pelas diretivas da UE.

O Tribunal Europeu dos Direitos Humanos elaborou um [guia sobre o artigo 14.º da Convenção Europeia dos Direitos Humanos e sobre o artigo 1.º do Protocolo n.º 12 à Convenção](#).

Tabela 1. Características protegidas abrangidas pela legislação europeia

O “X” na tabela significa que a característica está abrangida pela regulamentação. Uma célula vazia significa que não está coberta.

	Artigo 14.º da Convenção Europeia dos Direitos Humanos	Carta dos Direitos Fundamentais da UE	Diretivas da UE em matéria de não discriminação
Sexo	X	X	X (2004/113/ CE, 2000/78/ CE, 2006/54/CE, 2023/970/UE, 2010/41/UE)
Raça¹⁷	X	X	X (2000/43/CE)
Cor	X	X	
Língua	X	X	
Religião	X	X (ou crença)	X (2000/78/CE)
Opinião política ou de outra natureza	X	X	X (2000/78/CE)
Origem nacional ou social	X	X (origem étnica ou social)	
Associação com uma minoria nacional	X	X (adesão)	
Propriedade	X	X	
Nascimento	X	X	
Outro estatuto	X		

17 Uma vez que todos os seres humanos pertencem à mesma espécie, o Comité de Ministros do Conselho da Europa rejeita as teorias baseadas na existência de diferentes “raças”. No entanto, no presente documento, o termo “raça” é utilizado para garantir que as pessoas que são, de forma generalizada e errada, consideradas como “pertencentes a outra raça” não sejam excluídas da proteção prevista pela legislação e pela aplicação de políticas.

	Artigo 14.º da Convenção Europeia dos Direitos Humanos	Carta dos Direitos Fundamentais da UE	Diretivas da UE em matéria de não discriminação
Deficiência	Outro estatuto	X	X (2000/78/CE)
Idade	Outro estatuto	X	X (2000/78/CE)
Orientação sexual	Outro estatuto	X	X (2000/78/CE)
Nacionalidade	Outro estatuto	X (qualificada)	
Características genéticas	Outro estatuto	X	
Estado civil	Outro estatuto		
Estatuto de migrante ou pessoa refugiada	Outro estatuto		



Como utilizar a metodologia

A metodologia adota uma abordagem em quatro etapas (ver também a Figura 1 abaixo).

Passo 1: identificação de casos relacionados com IA ou algoritmos

Passo 2: recolha de informações sobre a IA ou o sistema algorítmico para identificar situações de discriminação

Passo 3: metodologia para avaliar a informação recebida

Passo 4: vias de recurso

Sempre que pertinente, a metodologia distingue as diferentes fontes dos casos:

- A. uma queixa (apresentada por uma pessoa singular ou por um grupo)
- B. uma investigação *ex officio*
- C. informações fornecidas por uma AFM

Nota: os passos são apresentados como passos consecutivos para maior clareza estrutural desta metodologia. Não são estritamente consecutivos, mas, na prática, são frequentemente circulares e iterativos.

Passo 1

A comunicação inicial ou as informações relativas a um caso de discriminação em que se possa reconhecer o envolvimento de sistemas algorítmicos.

Questões-chave:

- ▶ Trata-se de um caso que envolve um sistema de IA de risco elevado ao abrigo do Regulamento sobre a IA?
- ▶ Trata-se de um caso que envolve um sistema algorítmico?

Passo 2

O próximo passo consiste em procurar informações sobre o sistema identificado, o que poderá contribuir para a identificação posterior de discriminação. O Passo 2 define os tipos de informação relevante, documentação e outros tipos de provas que possam estar disponíveis ou acessíveis aos OI e as suas fontes potenciais.

Nota: a informação identificada neste passo é analisada em pormenor no passo 3. Por conseguinte, os passos 2 e 3 devem ser considerados em conjunto. Da mesma forma, nos casos em que faltam informações e existe poder legal para as obter, a via de recurso é abordada no passo 4.

Questão-chave:

- ▶ Que informações estão disponíveis e como se pode aceder a elas?

Passo 3

É realizada uma análise exaustiva das provas relevantes, utilizando como orientação um conjunto de questões sugeridas. Estas questões não são exaustivas.

O quadro jurídico em matéria de não discriminação é então aplicado a esses elementos de prova.

Questões-chave:

- ▶ É possível estabelecer um caso *prima facie* de discriminação?
- ▶ É provável que a parte inquirida consiga cumprir o ónus da prova?
- ▶ Tendo em conta todas as provas, ficou comprovada a existência de discriminação ilegal?

Passo 4

Analisar e aplicar as vias de recurso disponíveis.

Questão-chave:

- ▶ Que vias de recurso devem ser tomadas ou aplicadas?

Em todas as etapas, a pessoa responsável terá de ter em conta o seguinte:

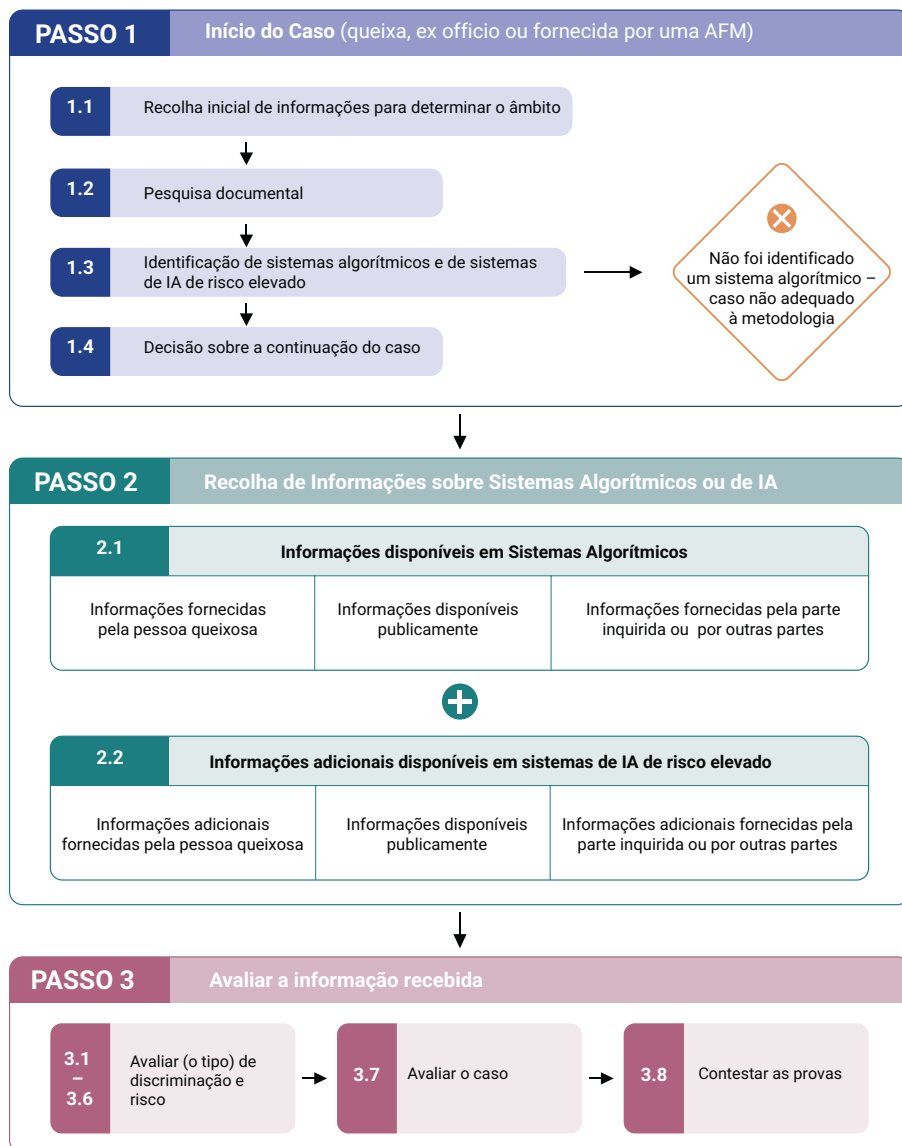
- ▶ Se não houver qualquer alegação de discriminação passível de contestação, o caso deve ser arquivado.
- ▶ Se não estiver envolvido qualquer sistema algorítmico, o caso deve ser arquivado ao abrigo desta metodologia e analisado no âmbito do processo ordinário de discriminação do OI.

Recurso a especialistas

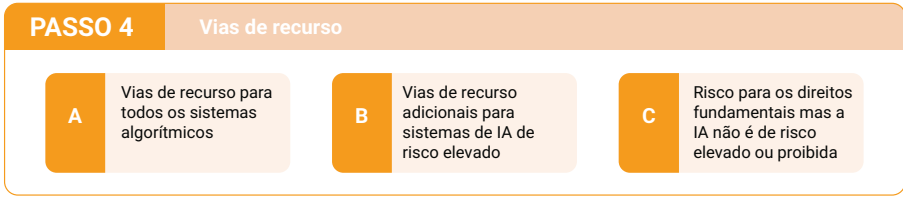
Pode ser necessário recorrer à assistência de especialistas no que diz respeito a alguns elementos desta metodologia, nos casos em que, por exemplo, sejam necessários conhecimentos especializados em matéria de dados ou de ciências da computação para a avaliação técnica do modelo ou dos dados. A metodologia

indica os tipos de questões que podem ser feitas a uma pessoa especialista e em que circunstâncias tal deve ser considerado. Uma vez que foram adotadas as alterações ao artigo 77.º do *Omnibus Digital*,¹⁸ os organismos para a igualdade poderão solicitar assistência à AFM, a outras autoridades públicas ou a organismos com competências na matéria, com base na disposição relativa à assistência mútua prevista no n.º 1-B do artigo 77.º proposto.

Figura 1. Passos 1 a 4 da metodologia



18 Ver acima, na secção “Regulamento sobre a IA da UE, artigo 77.º: Poderes das autoridades responsáveis pela proteção dos direitos fundamentais”.





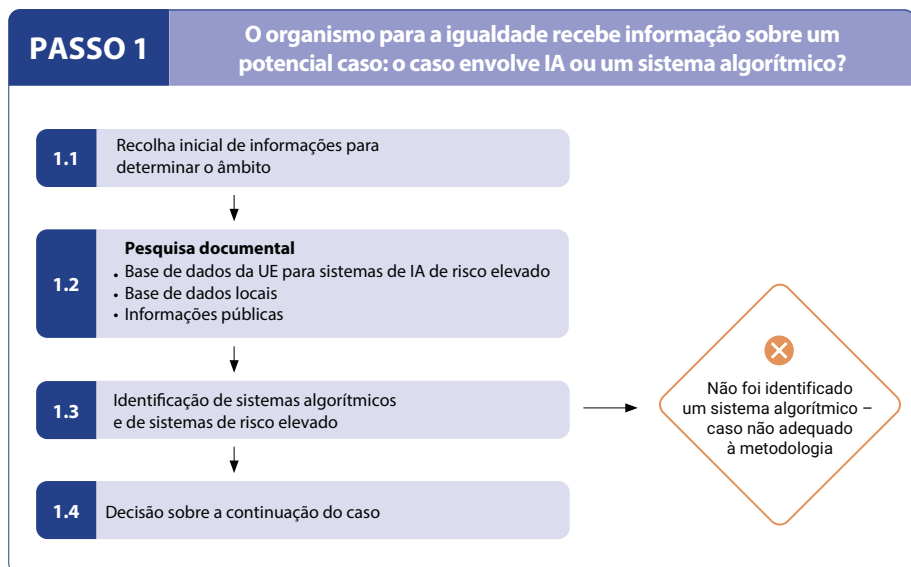
Passo 1

Identificação de sistemas de IA ou algorítmicos

O objetivo deste primeiro passo é apenas perceber se está envolvido uma TDA ou um sistema de IA (de risco elevado) e determinar se há informação suficiente para avançar para o passo 2. Neste passo, não é realizada qualquer investigação detalhada.

O passo 1 é composto pelos seguintes sub-passos.

Figura 2. Passo 1 – O caso envolve IA ou um sistema algorítmico?



Nota: os passos são apresentados como passos consecutivos para maior clareza estrutural deste protocolo. Estes sub-passos não são estritamente consecutivos, mas, na prática, são frequentemente circulares e iterativos.

A identificação dos casos de IA e TDA varia consoante a origem do caso:

- A. de uma queixa (apresentada por uma pessoa singular ou por um grupo)
- B. em resultado de uma investigação *ex officio*
- C. através de informações fornecidas por uma AFM

Como reconhecer sistemas algorítmicos e IA

Os sistemas algorítmicos podem ser tão simples quanto a automatização de um conjunto limitado de regras definidas pelo ser humano. Em geral, os sistemas algorítmicos (incluindo a IA) são difíceis de reconhecer. As definições têm vindo a mudar ao longo dos anos ou são interpretadas de forma diferente.

No Regulamento sobre a IA da UE, a definição técnica prevista no n.º 1 do artigo 3.º estabelece que:

Sistema de IA significa um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais¹⁹

Mesmo quando há consenso quanto às definições, os sistemas algorítmicos muitas vezes não são reconhecidos pelas organizações ou são designados por termos diferentes.

Uma avaliação destinada a determinar se é utilizado um sistema algorítmico deve abranger uma variedade de termos.

Todos os termos a seguir podem indicar a utilização de sistemas algorítmicos.

- ▶ Automatização, baseado em máquinas, informatizado, baseado em algoritmos
- ▶ Perfilagem ou criação de perfis
- ▶ Tomada de decisão automatizada ou sistemas de apoio à decisão
- ▶ Um sistema ou computador decide/analisa/compara/recomenda/trata os dados de uma pessoa
- ▶ Um sistema, computador ou câmara vê/ouve/compreende
- ▶ Qualquer referência ao cálculo de pontuações, probabilidade, verosimilhança ou estimativa de comportamentos futuros
- ▶ Avaliação automatizada de riscos, reconhecimento automatizado
- ▶ Qualquer referência a estatísticas
- ▶ Qualquer referência à aprendizagem automática

¹⁹ A isto acrescem as Orientações da Comissão C(2025) 5053 relativas à definição de um sistema de inteligência artificial estabelecida pelo Regulamento (UE) n.º 2024/1689 (Regulamento sobre a IA).

As seguintes palavras podem indicar a utilização de IA.

- ▶ Aprendizagem automática, aprendizagem profunda
- ▶ Um modelo/máquina/computador foi treinado
- ▶ Foram identificados padrões a partir dos dados
- ▶ Baseado em modelos de linguagem de grande escala (LLMs)
- ▶ Modelos preditivos

Exemplo: “Com base nestes dados, a entidade prestadora de serviços calcula valores de probabilidade utilizando métodos matemático-estatísticos para avaliar o risco de incumprimento de pagamento e para verificar a sua morada.”

1.1. Recolha inicial de informações

A. Queixa

Quando a origem do caso é uma queixa, existe um momento inicial em que a queixa é apresentada. Nesta etapa, é possível recolher informações iniciais sobre se poderá estar envolvido um sistema algorítmico ou um sistema de IA. Esta recolha inicial de informações é simples, de modo a alinhar-se, tanto quanto possível, com os processos existentes de receção de queixas nos organismos para a igualdade.

1.1.1. Determinação inicial do âmbito e das competências

- ▶ Forma de apresentação da queixa: telefone, formulário online, correio, outro
- ▶ Nome e dados de contacto da pessoa queixosa
- ▶ Breve descrição do problema
- ▶ Qual é a organização visada (a organização que é objeto da queixa)?
 - Entidade pública ou privada?
- ▶ Avaliação de competências
 - Motivos protegidos?
 - Setor?
- ▶ Via de recurso solicitada/objetivo pretendido com o caso
 - Aconselhar?
 - Intentar uma ação judicial?
 - Recomendar uma ação?

Este caso é da competência do organismo para a igualdade? A queixa já foi apresentada a outro organismo/entidade ou existe alguma outra entidade já envolvida no caso?

1.1.2. Recolha de informações adicionais com base na queixa

É possível que a pessoa queixosa tenha mais informações à sua disposição. Esta secção define exemplos de perguntas a colocar à pessoa queixosa, quer através de um formulário online, quer numa conversa (telefónica), para determinar se esteve envolvido um sistema algorítmico ou de IA.

Tanto o Regulamento sobre a IA como o RGPD impõem obrigações de transparência para com as pessoas singulares - titulares dos dados ou pessoas afetadas - relativamente à utilização de sistemas algorítmicos ou de IA. Consulte os quadros que contêm as disposições relevantes abaixo. As informações relevantes podem ser fornecidas às pessoas singulares através de correspondência pessoal ou de acordos contratuais, normalmente incluídas em avisos de privacidade ou termos e condições, ou comunicadas publicamente através do sítio Web ou das plataformas da organização (ver [1.2.3. Sítio Web e comunicações externas da parte inquirida](#))

Por conseguinte, o simples facto de lhes pedir que forneçam quaisquer documentos relevantes de que possam dispor, juntamente com uma análise sumária da informação pública, poderá contribuir para o passo seguinte (ver [1.2 Pesquisa documental complementar](#))

Nota: essas disposições não abrangem todos os casos em que se recorre à IA ou a sistemas algorítmicos e, por conseguinte, a ausência de informação pode simplesmente significar que são necessários mais esclarecimentos.

Existem várias disposições no Regulamento sobre a IA que exigem que as pessoas sejam notificadas sobre a utilização da IA.

Quando um sistema de IA de risco elevado é utilizado no local de trabalho, os representantes das trabalhadoras e trabalhadores e as trabalhadoras e trabalhadores afetados devem ter sido informados de que estão sujeitos à utilização de um sistema de IA de risco elevado (Regulamento sobre a IA, artigo 26.º, n.º 7).

- ▶ Quando os sistemas de IA de risco elevado tomam decisões ou prestam assistência na tomada de decisões relacionadas com pessoas singulares, estas devem ter sido informadas pela entidade criadora de que estão sujeitas à utilização do sistema de IA de risco elevado (Regulamento sobre a IA, artigo 26.º, n.º 11). Essas informações devem incluir a finalidade pretendida e os tipos de decisões que toma. A entidade responsável pela implantação deve também informar as pessoas singulares sobre o seu direito a explicações, previsto neste regulamento (Considerando 93 do Regulamento sobre a IA).
- ▶ Quando as pessoas singulares interagem diretamente com a IA (através de *chatbots* ou assistentes de voz, por exemplo), devem ser informadas desse facto (Regulamento sobre a IA, artigo 50.º, n.º 1). Isto pode ser feito através de notificações claras ou janelas pop-up como: "Olá, sou um *chatbot*."/"Olá, está agora a conversar com um assistente de IA."/"Chamo-me X, sou um assistente de IA e estou aqui para a/o ajudar."
- ▶ Da mesma forma, as pessoas devem ser informadas sobre o funcionamento dos sistemas de reconhecimento de emoções (um sistema de IA que identifica a raiva ou a satisfação de clientes através de características faciais ou vocais, por exemplo) ou dos sistemas de categorização biométrica (um sistema de IA que realiza a identificação do género com base no cabelo ou na forma do rosto de uma pessoa, por exemplo) (Regulamento sobre a IA, artigo 50.º, n.º 3).

- Existem também requisitos de transparência previstos no RGPD (RGPD, artigo 5.º, n.º 1, alínea a), 13.º e 14.º), que exigem que a pessoa titular dos dados seja notificada sobre a utilização de sistemas algorítmicos, incluindo informações sobre a identidade de quem é responsável pelo tratamento, as finalidades do tratamento e a existência de tomada de decisões automatizada e de definição de perfis (ver passo [2.1.1. Informações fornecidas pela pessoa queixosa](#)).

Esta informação pode constar nos termos e condições ou na política ou declaração de privacidade. No que diz respeito ao Regulamento sobre a IA, o Gabinete da IA publicou, em julho de 2026, as orientações sobre as obrigações de transparência previstas na referida lei.²⁰

Questões a colocar à pessoa queixosa e/ou a ter em conta na pesquisa documental

Nota: uma pessoa queixosa pode não saber de que informações dispõe ou se estas são relevantes. Por isso, um bom ponto de partida é simplesmente perguntar: “Que sítios Web/aplicações estava a utilizar?” e “Recebeu alguma documentação?”.

A documentação relevante pode incluir, entre outros, um pedido apresentado pela pessoa queixosa, cartas, e-mails, faturas ou formulários de consentimento e avisos de privacidade enviados pela organização inquirida, bem como contratos entre a pessoa queixosa e a organização, incluindo anexos e atualizações contratuais entregues em papel, por email ou através de notificações em aplicações ou portais. Se disponível, a documentação relevante deve ser recolhida e consultada durante a etapa [1.2 Pesquisa documental complementar](#) para responder a algumas ou a todas as seguintes questões.

- Foi informado à pessoa queixosa que estava a ser utilizado um sistema de IA?
 - Quando o caso diz respeito ao local de trabalho: a pessoa queixosa consultou os seus representantes de trabalhadores ou o sindicato?
 - Se sim: o que lhes foi dito?
- Foi informado à pessoa queixosa que estava a ser utilizado o tratamento automatizado de dados?²¹
- Foi pedida à pessoa queixosa autorização para o tratamento específico de dados ou foi-lhe pedido que confirmasse ter lido uma declaração ou aviso de privacidade?
 - Se sim: é possível partilhar o texto do pedido de autorização, a declaração de privacidade ou o aviso?

20 Saiba mais aqui: [Código de conduta sobre a identificação e rotulagem de conteúdos gerados por IA – Moldar o futuro digital da Europa](#).

21 Quando são utilizados dados pessoais para a tomada de decisões totalmente automatizada, as pessoas utilizadoras devem ter sido informadas de que estão sujeitas a uma tomada de decisões totalmente automatizada (RGPD, artigo 13.º, n.º 2, alínea f)).

- Se não: houve alguma outra referência do tipo “é assim que tratamos os seus dados” ou “é assim que os seus dados podem ser utilizados”?
- Foi feita alguma referência à automatização, a um sistema informático que execute tarefas autónomas ou a um sistema informático que contribua para a tomada de uma decisão? Preste atenção a expressões e formas de dizer como as que se seguem.
 - Um sistema ou computador decide/analisa/compara/recomenda/trata os dados de uma pessoa.
 - Um sistema, computador ou câmara “vê”/“ouve”/“compreende”.
 - Qualquer referência ao cálculo de pontuações, probabilidade, verosimilhança ou estimativa de comportamentos futuros.
 - A utilização de um sistema informático para apoiar um processo, eventualmente com uma marca específica. Por exemplo: “Utilizamos o Clippy/Frank/Maya para tratar os seus dados e para apoiar o nosso trabalho”.
- O contrato entre a pessoa queixosa e a parte inquirida contém alguma referência à automatização, a processos algorítmicos, a sistemas especificamente identificados, a estatísticas, os parâmetros de desempenho, a classificações ou pontuações (tais como a desativação automática ou pontuações de fiabilidade)?
 - Se sim: é possível partilhar o contrato ou as cláusulas contratuais relevantes?
- Onde ocorreu a interação ou a comunicação com a organização (inquirida)?
- Nos casos de interação presencial ou por telefone:
 - Se pessoalmente, a outra pessoa consultou um computador para tomar decisões ou chegar a conclusões?
- Nos casos de interação através de um computador ou de um smartphone:
 - foi preenchido algum formulário online?
 - quanto tempo depois da interação houve um resultado ou uma decisão (imediatamente, entre alguns minutos e uma hora, alguns dias, ou mais tempo)?
 - foi solicitada autorização para o tratamento de dados pessoais, por exemplo, através de uma caixa de seleção relativa a dados pessoais ou à privacidade?
 - foi solicitada alguma informação sobre algum atributo protegido (ver [Características protegidas](#)) durante a interação com o sistema?

1.1.3. Breve análise da informação pública

Base de dados da UE para sistemas de IA de risco elevado

A partir de 2 de agosto de 2026, prevê-se que esteja disponível uma base de dados da UE para sistemas de risco elevado²², antes de estes serem colocados no merca-

²² Embora esta base de dados ainda não exista e não se saiba ao certo como será a sua estrutura e a sua interface, foi aqui incluída porque se prevê que venha a tornar-se uma fonte de informação de grande relevância no futuro.

do ou colocados em serviço. De acordo com o *Omnibus Digital* em matéria de IA, os sistemas colocados em serviço antes de 2 de dezembro de 2027, no caso dos sistemas de IA de risco elevado autónomos, e antes de 2 de agosto de 2028, no caso dos sistemas de IA de risco elevado incorporados em produtos, só terão de ser registados se forem objeto de uma “alteração significativa”.²³ As partes públicas da base de dados estarão disponíveis para todos.

Nos casos de queixas relacionadas com sistemas utilizados na educação, no emprego, na administração pública, na banca, nos seguros, na administração da justiça e nas eleições, bem como relacionadas com ações/atividades como a automatização da identificação de pessoas singulares, o reconhecimento facial ou de voz, o reconhecimento de emoções, a previsão de intenções ou riscos, uma pesquisa rápida na base de dados - utilizando palavras-chave relevantes que podem ser, por exemplo, o nome da organização inquirida, o nome do sistema ou o setor relevante - pode constituir um ponto de partida útil.

- Se a parte inquirida constar da base de dados como desempenhando qualquer função num caso de utilização relevante para a queixa, existe uma certeza relativa de que está envolvida IA (de risco elevado).²⁴ Passe ao passo 1.3. **Identificação de sistemas algorítmicos ou de IA de risco elevado.**

Nota: existem algumas exceções aos requisitos de registo, ou pode ser que quem presta ou é responsável pela implantação não tenha cumprido as suas obrigações regulamentares. No passo 2.2.2. **Informação disponível ao público.**

Comparar com a lista de casos de utilização

- O **Anexo C** contém uma lista de utilizações comuns de sistemas algorítmicos e de IA em diferentes setores. Algum destes exemplos parece ser relevante para a situação, o caso ou o processo da queixa? Ver também o **Anexo F** sobre bases de dados de IA e casos de utilização.

Pesquisa geral na Internet

- Faça uma pesquisa na Internet sobre inovação/automatização na situação, caso ou processo descritos na queixa ou por parte da organização inquirida.
 - Por exemplo: “A polícia de [país] está a utilizar IA?”. A título de exemplo, no caso da Finlândia, isto resulta numa lista de resultados de pesquisa que inclui: **A Finlândia planeia uma grande expansão dos poderes da polícia em matéria de recolha de dados biométricos – ID Tech.**
 - Por exemplo: “A IA é utilizada no recrutamento em [país]?”. No caso da Bélgica, isto dá o seguinte resultado, sugerindo que um terço das empresas belgas utiliza IA nos processos de recrutamento: www.anews.com.tr/

23 Regulamento (UE) 2026/1744 do Parlamento Europeu e do Conselho, de 8 de julho de 2026, que altera os Regulamentos (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 no que diz respeito à simplificação da aplicação das regras harmonizadas em matéria de inteligência artificial (Regulamento Omnibus Digital em matéria de IA). Disponível em: <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>, consultado a 24 de julho de 2026.

24 Note-se que o facto de um sistema não constar desta base de dados não significa que não esteja envolvido nenhum sistema de IA (de risco elevado); há exceções.

europe/2023/07/19/in-belgium-one-third-of-companies-use-artificial-intelligence-in-their-recruitment-processes.

- Certifique-se de que os resultados são resultados de pesquisa e não gerados por IA.

Nota: certas práticas são proibidas nos termos do artigo 5.º do Regulamento sobre a IA. Consulte o [Anexo J - Práticas proibidas em matéria de IA](#) para obter uma lista.

Estes passos têm carácter meramente indicativo. Se as respostas a estas perguntas indicarem que é provável que tenha sido utilizado um sistema de IA ou um sistema algorítmico, avance para o passo [1.3. Identificação de sistemas algorítmicos ou de IA de risco elevado](#).

Se a informação não for conclusiva, considere recolher mais informação (pública) durante a pesquisa documental, tal como descrito no passo [1.2 Pesquisa documental complementar](#).

B. Ex officio

Alguns organismos para a igualdade têm o mandato de iniciar investigações *ex officio* ou por via de *actio popularis* (ao abrigo da legislação nacional).

Nesta etapa, partimos do princípio de que não está envolvida qualquer queixa apresentada por uma pessoa singular ou por um grupo de pessoas singulares. Nas etapas finais da investigação, o organismo para a igualdade pode optar por envolver as pessoas diretamente afetadas. Para efeitos desta metodologia de avaliação, parte-se do princípio de que existe um domínio de interesse específico (um setor, uma área operacional dentro desse setor e, potencialmente, organizações específicas) já definido; por exemplo, algoritmos de fixação de preços utilizados pelas seguradoras ou a avaliação do risco de fraude no âmbito da segurança social/prestações sociais.

Informações a recolher

- Situação, caso ou processo de interesse e informação pública disponível.
- Queixas relevantes (ainda por resolver) apresentadas pelo organismo para a igualdade ou por outra entidade competente. Poderão tratar-se de queixas que, consideradas isoladamente, não constituíam casos suficientemente sólidos ou em que a pessoa queixosa retirou a sua queixa.
- Indicação do envolvimento de IA ou de sistemas algorítmicos, se disponível; ver [“Como reconhecer sistemas algorítmicos e IA”](#) acima.
- Informações sobre a organização que seria objeto desta investigação *ex officio*, caso esta fosse formalmente iniciada (doravante designada “parte inquirida”), ou, no caso de uma análise setorial, uma lista das organizações representativas do setor em análise.²⁵

²⁵ Por exemplo, se um OI abrir um inquérito *ex officio* sobre os algoritmos de fixação de preços utilizados pelas seguradoras, poderá ser utilizada, nesta etapa do protocolo, uma lista representativa de seguradoras, em vez de uma parte inquirida específica.

Comparar com uma lista de casos existentes

- ▶ O **Anexo C** contém uma lista de utilizações comuns de sistemas algorítmicos e de IA em diferentes setores. Algum destes exemplos parece ser relevante para a situação, o caso ou o processo da eventual investigação?

Quando um caso é instaurado *ex officio*, pode já ser evidente que está envolvido um sistema de IA. Os passos 1.2 e 1.3 não são relevantes neste caso: passe ao passo 1.4. [Continuação do caso.](#)

C. Informado pela AFM

Espera-se que o organismo para a igualdade receba informações da autoridade de fiscalização do mercado (AFM) relativas a sistemas de IA que representem um risco de discriminação, nomeadamente nos seguintes casos.

- ▶ Incidentes graves (Regulamento sobre a IA, artigo 73.º, n.º 7)
 - Caso uma entidade prestadora notifique a AFM de um incidente grave,²⁶ a AFM deve informar as autoridades previstas no artigo 77.º, incluindo o organismo para a igualdade, se for caso disso. A consulta sobre as orientações específicas relativas aos procedimentos de comunicação e sobre um projeto de modelo de relatório de incidente, realizada pela Comissão, concluiu-se a 7 de novembro de 2025.²⁷
- ▶ **Produtos que apresentam um risco (Regulamento sobre a IA, artigo 79.º, em conjugação com o artigo 3.º, n.º 19, do Regulamento (UE) 2019/1020)**
 - Sempre que a AFM tiver motivos suficientes para considerar que um sistema de IA se enquadra na categoria de produto que representa um risco para o direito à não discriminação, tem o dever de informar e cooperar plenamente com as autoridades competentes previstas no artigo 77.º, incluindo o organismo para a igualdade.

Estas informações podem incluir o seguinte.

- ▶ Organização: entidade pública ou privada.
- ▶ Sistema de IA: identificação do sistema e da área de classificação de risco elevado (Anexo I ou Anexo III do Regulamento sobre a IA, incluindo o domínio e o caso de utilização).
- ▶ Função da organização (responsável pela implantação, entidade prestadora, outra).

26 Por “incidente grave” entende-se qualquer incidente ou anomalia num sistema de IA que, direta ou indiretamente, tenha alguma das seguintes consequências:

(a) a morte de uma pessoa ou danos graves para a saúde de uma pessoa;
(b) uma perturbação grave e irreversível da gestão ou do funcionamento de uma infraestrutura crítica;
(c) a infração das obrigações decorrentes do direito da União destinadas a proteger os direitos fundamentais;
(d) danos graves a bens ou ao ambiente (Regulamento sobre a IA, artigo 3.º, n.º 49).

27 Saiba mais em: [Regulamento sobre a IA: A Comissão emite um projeto de orientações e um modelo de comunicação de incidentes graves relacionados com a IA e solicita o parecer das partes interessadas.](#)

- ▶ Quando a notificação se baseia no artigo 73.º do Regulamento sobre a IA (incidente grave):
 - as circunstâncias do incidente ou da anomalia;
 - o tipo de dano que ocorreu ou que se suspeitava ter ocorrido;
 - a relação entre o sistema de IA e o incidente (como a IA causou ou contribuiu para o incidente);
 - qualquer informação disponível sobre a avaliação de risco realizada pela entidade prestadora relativamente ao incidente e as medidas corretivas propostas ou implementadas.
- ▶ Quando a notificação se baseia no artigo 79.º do Regulamento sobre a IA (risco):
 - a razão pela qual se considera que o sistema de IA representa um risco para os direitos fundamentais;
 - (opcional, se disponível) informações relevantes sobre avaliações já realizadas;
 - (opcional, se disponível) ações corretivas propostas ou implementadas.
- ▶ Nos casos que envolvam um sistema de IA de risco elevado nos domínios da aplicação da lei, migração, asilo e gestão do controlo de fronteiras (pontos 1, 6 e 7 do Anexo III), a AFM poderá aceder às informações relativas ao sistema de IA, tal como registadas na base de dados da UE para sistemas de IA de risco elevado.

Quando um organismo para a igualdade é informado por uma AFM, há a certeza de que está envolvido um sistema de IA de risco elevado. Os passos 1.2 e 1.3 não são relevantes neste caso: passe ao passo 1.4.

1.2 Pesquisa documental complementar

Se houver capacidade disponível para a pesquisa documental, existem várias fontes que podem ser consultadas para determinar se se prevê a utilização de TDA ou IA no caso. Esta secção descreve em pormenor as fontes e o que se deve procurar.

Os passos referidos nesta secção variam em termos de profundidade e do tempo necessário para realizar esta pesquisa documental:

- ▲ passos que poderiam ser considerados prioritários;
- ▼ passos adicionais para uma pesquisa documental mais aprofundada.

Por exemplo, deverá ser relativamente fácil efetuar uma pesquisa na base de dados da UE (abaixo) assim que esta estiver operacional e desde que a parte inquirida esteja registada na mesma. Isto permitirá obter uma resposta rápida à pergunta “está a ser utilizado um sistema de IA?”. Se quem é responsável pela implantação não estiver registado, será necessário realizar uma pesquisa mais aprofundada.

Esta secção não se aplica aos casos em que a fonte seja “C. Com base na AFM”. Neste caso, a AFM já terá determinado que se trata de um sistema de IA de risco elevado e, por conseguinte, a pesquisa documental descrita nesta secção seria redundante.

1.2.1. Base de dados da UE para sistemas de IA de risco elevado

Procure a parte inquirida ou qualquer responsável pela implantação ou entidade prestadora conhecida na base de dados.

A parte inquirida consta como responsável pela implantação na parte C da base de dados?²⁸

- ▲ A parte inquirida é a responsável pela implantação de um caso de utilização relevante para a queixa?
- ▲ Que organização é a entidade prestadora?

Informações relevantes disponíveis na base de dados para identificação inicial:

- ▶ dados de contacto da entidade prestadora e da/o representante autorizada/o;
- ▶ nome e dados de contacto de quem é responsável pela implantação (apenas autoridades públicas, instituições, órgãos e agências da UE, ou pessoas que atuem em seu nome);
- ▶ o URL do registo do sistema de IA na base de dados da UE, efetuado pela entidade prestadora.

A parte inquirida consta da base de dados como entidade prestadora na parte A ou B da mesma?

- ▲ A parte inquirida é a entidade prestadora num caso de utilização de risco elevado que seja relevante para a queixa?
- ▲ A parte inquirida é a entidade prestadora de um caso de utilização destinado a ser utilizado num domínio de risco elevado, mas que, segundo a sua própria avaliação, se enquadra na exceção prevista no n.º 3 do artigo 6.º do Regulamento sobre a IA? Esta avaliação pode ser solicitada pelas autoridades nacionais competentes.

Informações relevantes disponíveis na base de dados para identificação inicial:

- ▶ dados de contacto da entidade prestadora e da/o representante autorizada/o;
- ▶ nome comercial ou outra referência que permita a identificação e o rastreio do sistema de IA (isto pode ser útil, por exemplo, nos casos em que um sistema de risco elevado seja utilizado como parte de outro sistema);
- ▶ finalidade pretendida.

28 Note-se que apenas as autoridades públicas são obrigadas a registar-se como responsáveis pela implantação. Outras organizações não têm essa obrigação.

Se for encontrado nesta base de dados, significa que está a ser utilizado um sistema de IA. Passe para o passo [1.3. Identificação de sistemas algorítmicos ou de IA de risco elevado](#) e/ou [1.4. Continuação do caso](#).

Caso contrário, procure na base de dados organizações semelhantes à da parte inquirida:

- ▼ Existem organizações semelhantes na base de dados, registadas como entidades prestadoras ou responsáveis pela implantação de um caso de utilização relevante para a queixa? Por exemplo, outras seguradoras semelhantes indicam o uso de sistemas de IA para a fixação de preços quando o caso diz respeito à (in)equidade dos preços, ou outras administrações públicas semelhantes no mesmo país indicaram o uso de sistemas de IA para a avaliação de prestações sociais quando o caso diz respeito à recusa de prestações.

Nos termos do n.º 4 do artigo 49.º, o registo de sistemas de IA de risco elevado nos domínios da aplicação da lei, da migração, do asilo e da gestão do controlo de fronteiras deve ser efetuado numa secção segura e não pública da base de dados da UE referida no artigo 71.º e deve incluir apenas um conjunto específico de informações, tal como definido no n.º 4 do artigo 49.º. O acesso a estas secções da base de dados será limitado.

Para mais informações sobre a secção não pública da base de dados e os aspetos relacionados com a transparência no domínio da aplicação da lei, consulte as [restrições ao acesso à informação](#) no passo 2.2.2 e o quadro Domínio da aplicação da lei no passo 2.2.4, respetivamente.

1.2.2. Outras bases de dados e inventários relativos a sistemas de IA (de risco elevado) e sistemas algorítmicos

Algumas organizações e autarquias mantêm uma base de dados, um registo ou um inventário local dos sistemas de IA utilizados. No [Anexo F](#) encontra-se uma lista destas bases de dados. Nem todas estas bases de dados são relevantes. Assinale apenas as opções que sejam relevantes para o seu contexto nacional.

Procure a parte inquirida na base de dados:

- ▲ Existe algum sistema algorítmico ou de IA indicado como sendo utilizado ou desenvolvido pela parte inquirida que seja relevante para a situação, o caso ou o processo abrangido pela queixa?

Pesquise organizações semelhantes à da parte inquirida:

- ▼ Existe algum sistema algorítmico ou de IA indicado como sendo utilizado ou desenvolvido por uma organização comparável, o qual teria sido relevante para a situação, o caso ou o processo abrangido pela queixa, caso esta se referisse a essa organização comparável?

Compare com a lista de casos de utilização existentes:

- ▼ Consulte o [Anexo C](#) para uma lista de utilizações comuns de sistemas algorítmicos e IA em diferentes setores.

Alguns destes casos de utilização parece ser relevante para a situação, o caso ou o processo da queixa?

1.2.3. Sítio Web e comunicações externas da parte inquirida

Aviso/Declaração de Privacidade

Procure expressões que indiquem a utilização de sistemas algorítmicos, por exemplo, qualquer uma das seguintes.

- ▲ Finalidades que sugerem a automatização, criação de perfis ou métodos estatísticos. Consulte [“Como reconhecer sistemas algorítmicos e IA”](#) e as perguntas incluídas no passo 1.2.2. [Outras bases de dados e inventários relativos a sistemas de IA \(de risco elevado\) e sistemas algorítmicos”](#).
- ▲ Entidades terceiras que recebem dados pessoais (destinatárias/os ou categorias de destinatárias/os). Verifique se existem indícios de envolvimento de entidades terceiras, tais como empresas de pontuação de crédito ou agências de informação de crédito, o que pode implicar a definição de perfis ou decisões automatizadas.
- ▼ Dados de contacto de quem é responsável pelo tratamento de dados: sabe-se se a entidade responsável pelo tratamento de dados implementa soluções de IA ou automação no setor em questão? Se existir um sistema de IA ou algorítmico, a entidade responsável pelo tratamento de dados será, normalmente, responsável pela implantação do sistema e a parte inquirida, na aceção desta metodologia.

Outros tipos de comunicação

Existe alguma referência a um sistema algorítmico que possa ser relevante para o caso?

- ▼ Pesquise no sítio Web da parte inquirida artigos sobre a sua implementação de IA, inovação e automatização ou as perguntas frequentes (FAQ) no sítio Web/plataforma da parte inquirida. A forma mais fácil de procurar um sítio Web específico é adicionar “sítio Web: [sítio Web da parte inquirida]” à consulta de pesquisa. Por exemplo, o sítio Web sobre inovação em IA: [bi-bank.com](#).
- ▼ Consulte as ofertas de emprego na área técnica para cientistas de dados, IA ou aprendizagem automática. Existe alguma referência a um sistema algorítmico que possa ser relevante para o caso? A descrição de funções para “cientista de dados sénior” elaborada por um banco inclui o seguinte: “A prevenção do branqueamento de capitais e do financiamento do terrorismo é um dos aspetos fundamentais para a nossa sociedade e para a nossa organização... será responsável por otimizar o nosso atual sistema de monitorização de transações (MT) baseado em regras e, a longo prazo, por introduzir metodologias analíticas mais avançadas, como a aprendizagem automática, nos nossos modelos de MT.” Consulte [a oferta de emprego para cientista de dados sénior na área de monitorização de transações – Rabobank](#).

Se aplicável: analise o sítio Web e as comunicações das entidades responsáveis pela implantação de casos de utilização de IA de risco elevado relevantes.

Se houver casos de utilização relevantes para o caso em questão listados por responsáveis pela implantação terceiros/os na base de dados da UE relativa a sistemas de IA de risco elevado, consulte o sítio Web da entidade prestadora.

- ▼ A parte inquirida consta no sítio Web como uma “organização com a qual trabalhamos” ou “que conta com a confiança destes clientes”?
- ▼ A parte inquirida é mencionada de alguma outra forma no sítio Web da entidade prestadora? A forma mais fácil de encontrar isso seria através de um motor de busca na Internet. Por exemplo, pesquise [parte inquirida] sítio Web: [entidade prestadora].com.

1.2.4. Análise adicional da informação pública

Alguns dos passos aqui referidos já foram mencionados no passo 1.1. Para garantir a exaustividade da informação, repetimo-los aqui.

Pesquisa geral na Internet

- ▼ Ver pesquisa na Internet no passo 1.1.3.
- ▼ Aperfeiçoar a pesquisa realizada no passo 1.1.3, verificando especificamente se organizações não governamentais (ONG), organismos ou organizações nacionais ou internacionais relataram a utilização de IA ou de sistemas algorítmicos numa situação, caso ou processo semelhante ao da queixa, quer por parte da parte inquirida, quer por parte de organizações semelhantes. Entre as ONG relevantes contam-se a Amnistia, a AlgorithmWatch e organizações nacionais da sociedade civil. Por exemplo, nos Países Baixos, a APD elabora um relatório sobre os riscos da IA e dos algoritmos duas vezes por ano. A pesquisa no contexto nacional neerlandês poderia ser “[setor da queixa] Relatório sobre os riscos da IA e dos algoritmos da Autoriteit Persoonsgegevens”.
- ▼ Opcional: refinar a pesquisa e incluir estratégias nacionais e internacionais em matéria de IA.
- ▼ Outros recursos relevantes podem incluir o [monitor de incidentes e riscos relacionados com a IA da OCDE](#) e a [base de dados de incidentes de inteligência artificial](#), ou relatórios elaborados pelo Conselho da Europa, tais como “Discriminação, inteligência artificial e tomada de decisões algorítmica” (Zuiderveen Borgesius, 2018).

1.3. Identificação de sistemas algorítmicos ou de IA de risco elevado

Com base nas informações recolhidas nos passos 1.1 e 1.2, é possível determinar de forma razoável se está a ser utilizado um sistema algorítmico ou um sistema de IA de risco elevado e qual o grau de certeza dessa determinação.

Lembrete: esta metodologia distingue apenas entre sistemas de IA de risco elevado e sistemas algorítmicos. Os sistemas algorítmicos incluem sistemas de IA de

risco não elevado e sistemas de TDA. No que diz respeito aos sistemas de IA de risco elevado, o Regulamento sobre a IA impõe requisitos de transparência abrangentes e obrigações de documentação, o que significa que se espera que esteja disponível documentação adicional. Se um sistema de IA não for considerado de risco elevado, a informação disponível e os passos a seguir são os mesmos que para os sistemas algorítmicos mais simples e, por conseguinte, são agrupados numa única categoria.

Tipo de sistema

- **Sistema de IA de risco elevado**
- **Sistema algorítmico**

Certeza

- **Relativamente certo**
- **Potencialmente**

Nota: determinar se são utilizados sistemas de IA ou algorítmicos é uma avaliação difícil e complexa nesta etapa, uma vez que a informação disponível é muito limitada. As conclusões a seguir apresentadas são sugestões, destinadas apenas a servir de orientação.

Base de dados da UE para sistemas de IA de risco elevado

O sistema está registado na base de dados da UE?

- SIM na secção A ou C: foi identificado um sistema de IA de risco elevado para este caso. É **relativamente certo** que, neste caso, está a ser utilizado um **sistema de IA de risco elevado**.
- SIM, na secção B:²⁹ existe um sistema de IA envolvido, mas não se prevê que esteja disponível qualquer documentação exigida para sistemas de risco elevado. É **relativamente certo** que, neste caso, está a ser utilizado um **sistema algorítmico**.
- NÃO, mas existem organizações semelhantes (como outro banco) que indicaram sistemas relevantes para o caso (tais como sistemas de pontuação de crédito) nas secções A ou C. Por conseguinte, pode ser razoável supor que a parte inquirida esteja a utilizar um sistema semelhante de risco elevado. Nesta etapa da metodologia, parte-se do princípio de que é **relativamente certo** que, neste caso, seja utilizado um **sistema algorítmico**. Neste caso, é **potencialmente** utilizado um **sistema de IA de risco elevado**.

Informações fornecidas pela parte inquirida (seja à pessoa queixosa, em documentos públicos ou mediante pedido)

- A parte inquirida indicou a utilização de automação, algoritmos ou IA para fins relevantes para o caso, quer diretamente à pessoa queixosa, quer no aviso/política de privacidade. É **relativamente certo** que, neste caso, está a ser utilizado um **sistema algorítmico**.

29 Nos termos do n.º 3 do artigo 6.º do Regulamento sobre a IA, o sistema de IA é considerado como não sendo de risco elevado.

- ▶ A parte inquirida indicou a utilização de automação, algoritmos ou IA para fins relevantes para as categorias de IA de risco elevado (ver Anexo I), quer diretamente à pessoa queixosa, quer no aviso/política de privacidade. É **relativamente certo** que, neste caso, é utilizado um **sistema algorítmico**; **potencialmente**, neste caso, é utilizado um **sistema de IA de risco elevado**.
- ▶ A parte inquirida incluiu um sistema algorítmico ou de IA numa base de dados pública (ver Anexo F) para fins relevantes para o caso. É **relativamente certo** que, neste caso, está a ser utilizado um **sistema algorítmico**.
- ▶ A parte inquirida declarou publicamente, em publicações de blogues, comunicados de imprensa ou outras fontes, que utiliza sistemas algorítmicos ou IA para fins relevantes para o caso. Note-se que as referências à utilização de sistemas algorítmicos podem ser vagas ou evasivas (ver o **passo 1.1** para conhecer as possíveis expressões utilizadas). É **relativamente certo** que, neste caso, está a ser utilizado um **sistema algorítmico**.

Outras informações

- ▶ Entidades conceituadas, tais como ONGs e órgãos de comunicação social de confiança, relataram a utilização de sistemas algorítmicos ou de IA pela parte inquirida para fins relevantes para o caso. Não foi possível encontrar qualquer confirmação por parte da organização. É **relativamente certo** que, neste caso, está a ser utilizado um **sistema algorítmico**.
- ▶ Outras partes relataram a utilização de sistemas algorítmicos ou de IA pela parte inquirida para fins relevantes para o caso. Não foi possível encontrar qualquer confirmação por parte da parte inquirida. **Potencialmente** neste caso, é utilizado um **sistema algorítmico**.
- ▶ A IA e os sistemas algorítmicos são frequentemente utilizados para fins relevantes para o caso, tal como enumerados no Anexo C. **Potencialmente** neste caso, é utilizado um **sistema algorítmico**.
- ▶ Segundo informações, organizações semelhantes utilizam sistemas algorítmicos para fins relevantes para o caso. **Potencialmente** neste caso, é utilizado um **sistema algorítmico**.
- ▶ Existem pistas contextuais que indicam que podem estar envolvidos sistemas algorítmicos neste caso. Por exemplo, devido à rapidez na tomada de decisões, quando processos complexos ou decisões que exigem discrição são tratados instantaneamente ou em poucos minutos. **Potencialmente** neste caso, é utilizado um **sistema algorítmico**.
- ▶ Existem pistas contextuais que indicam que podem estar envolvidos sistemas algorítmicos neste caso. Por exemplo, devido à rapidez na tomada de decisões, quando processos complexos ou decisões que exigem discrição são tratados instantaneamente ou em poucos minutos e tanto a IA como os sistemas algorítmicos são frequentemente utilizados para fins relevantes para o caso, tal como enumerado no Anexo C, ou quando se verifica que organizações semelhantes utilizam sistemas algorítmicos para fins relevantes para o caso. É **relativamente certo** que, neste caso, está a ser utilizado um **sistema algorítmico**.

1.4. Continuação do caso

Os passos 1.1. a 1.3. abrangem a avaliação da probabilidade de um sistema algorítmico estar envolvido. Para decidir se o processo deve prosseguir, é necessário proceder a uma avaliação mais aprofundada da probabilidade de se tratar de um caso de discriminação fundamentado. Isto deve ser avaliado com base nos critérios estabelecidos pelo organismo para a igualdade. Quando existe a possibilidade de um sistema algorítmico estar envolvido, tal pode exigir a imposição de um limiar de certeza mais baixo antes de se decidir dar seguimento ao pedido.

Manjang contra Uber Eats UK Ltd e outros (2021)

Este caso por discriminação racial foi instaurado com base em alegações de assédio, vitimização e discriminação indireta, na sequência da introdução de tecnologia de reconhecimento facial. A pessoa queixosa, um motorista de entregas, recebeu um e-mail da Uber Eats (a parte inquirida) a notificá-lo da sua suspensão definitiva da plataforma, com o fundamento de que estava a “partilhar a sua conta de parceiro de entregas da Uber Eats” e de que não tinha sido aprovado numa verificação por reconhecimento facial. Respondeu afirmando: “Pelo que parece, o vosso algoritmo é racista e isto tem de ser resolvido, uma vez que não consegue reconhecer nem verificar as minhas fotos, o que provavelmente explica porque é que me pedem para tirar fotos minhas várias vezes por dia”. A Uber Eats contestou a alegação de discriminação e solicitou a sua rejeição numa etapa inicial, alegando que esta se baseava em “erros factuais”. Em seguida, apresentaram informações sobre os fundamentos da sua contestação à alegação relativa ao funcionamento da tecnologia e, em resposta, a pessoa queixosa alterou a sua alegação. O tribunal recusou-se a indeferir a petição alterada, reconhecendo que, no momento em que a pessoa queixosa apresentou os seus argumentos, não havia clareza quanto ao motivo pelo qual a sua conta tinha sido desativada. Alguns meses mais tarde, durante o processo judicial, a parte inquirida afirmou que as razões apresentadas à pessoa queixosa - segundo as quais a decisão tinha sido tomada de forma automatizada - estavam erradas e que tinha sido efetuada uma revisão por parte de um ser humano. A pessoa queixosa sustentou, e o tribunal concordou, que havia falta de transparência quanto ao motivo pelo qual as fotografias da pessoa queixosa foram rejeitadas e a sua conta desativada. Por fim, chegou-se a um acordo financeiro extrajudicial.

Este é um exemplo de um caso financiado e apoiado por um OI, neste caso, a Comissão para a Igualdade e os Direitos Humanos (Reino Unido).

Tabela 2. Certeza sobre um sistema de risco elevado ou algorítmico e probabilidade de discriminação

	Baixa probabilidade de discriminação	Probabilidade média de discriminação	Elevada probabilidade de discriminação
Relativamente certo IA de risco elevado	Caso de elevada prioridade; considerar o envolvimento de especialista (interna/o) em sistemas algorítmicos	Caso de elevada prioridade; considerar o envolvimento de especialista (interna/o) em sistemas algorítmicos	Caso de elevada prioridade; considerar o envolvimento de especialista (interna/o) em sistemas algorítmicos
Relativamente certo sistema algorítmico, potencialmente IA de risco elevado	Caso de prioridade média; considerar o envolvimento de especialista (interna/o) em sistemas algorítmicos	Caso de elevada prioridade; considerar o envolvimento de especialista (interna/o) em sistemas algorítmicos	Caso de elevada prioridade; considerar o envolvimento de especialista (interna/o) em sistemas algorítmicos
Relativamente certo sistema algorítmico	Caso de baixa prioridade; caso se decida dar continuidade, considerar o envolvimento de especialista (interna/o) em sistemas algorítmicos	Caso de prioridade média; considerar o envolvimento de especialista (interna/o) em sistemas algorítmicos	Caso de elevada prioridade; considerar o envolvimento de especialista (interna/o) em sistemas algorítmicos
Potencialmente sistema algorítmico	Consulte as metodologias existentes, em vez desta metodologia	Caso de baixa prioridade ao abrigo desta metodologia, em que a probabilidade de discriminação é média, mas a probabilidade de o sistema de IA estar envolvido é baixa; consulte as metodologias existentes, em vez desta metodologia	Caso de prioridade média; considerar o envolvimento de especialista (interna/o) em sistemas algorítmicos

Suspeita de classificação incorreta ao abrigo do Regulamento sobre a IA

Classificação errada como “risco não elevado”

Existe a possibilidade de as entidades prestadoras de sistemas de IA nas áreas do Anexo III evitarem o regime aplicável a IA de risco elevado, procedendo a uma autoavaliação de qualquer uma das seguintes formas.

- ▶ Não é um sistema de IA. Neste caso, o Regulamento sobre a IA não se aplicaria.
- ▶ Não se trata de um sistema de risco elevado devido às exceções (Regulamento sobre a IA, artigo 6.º, n.º 3). Neste caso, o sistema deve continuar a estar registado na base de dados da UE na secção B. Nessa situação, a entidade prestadora é obrigada a documentar a sua avaliação para a exclusão antes de colocar no mercado ou de colocar em serviço o sistema de IA, e a registar o sistema na base de dados da UE na secção B (Regulamento sobre a IA, artigo 49.º, n.º 2). Não é obrigatório publicar a avaliação, mas a entidade prestadora é obrigada a apresentar a documentação relativa à avaliação, mediante pedido das autoridades nacionais competentes (AFM ou organismo notificador).
- ▶ Não se trata de um sistema de risco elevado, uma vez que a finalidade não está abrangida pela formulação dos casos de utilização enumerados no Anexo III do Regulamento sobre a IA (Regulamento sobre a IA, artigo 6.º, n.º 3).

Se um organismo para a igualdade suspeitar que um sistema foi indevidamente considerado fora do âmbito de aplicação do regime aplicável a IA de risco elevado, deve informar a AFM competente, independentemente de se poder ou não comprovar a existência de um caso de discriminação (ver o passo 4, procedimento da AFM para lidar com sistemas de IA classificados pela entidade prestadora como de risco não elevado, e o passo 4.3).

Para efeitos desta metodologia, o sistema deve ser considerado como um sistema algorítmico, uma vez que a informação que se espera que esteja disponível para sistemas de IA de risco elevado muito provavelmente não estará disponível neste caso.

Questões a colocar

- ▶ O sistema está abrangido pelos casos de utilização do Anexo III?
- ▶ É provável que o sistema seja um sistema de IA? Veja [“Como reconhecer sistemas algorítmicos e IA”](#).
- ▶ Faz parte da lista de exemplos práticos? (Ver o [Anexo C](#) e/ou a lista elaborada pela Comissão, quando disponível, n.º 4 do artigo 6.º).
- ▶ Consulte a secção B da base de dados. A entidade prestadora do sistema tem a obrigação de se registar, bem como de registar o sistema, nos termos do artigo 49.º.

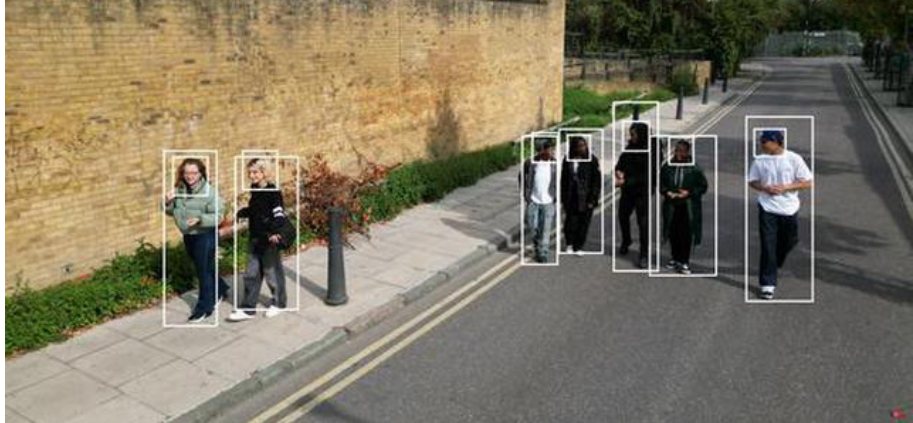
Sistema suspeito de ser proibido

Certas práticas são proibidas ao abrigo do Regulamento sobre a IA (ver [Anexo J - Práticas proibidas em matéria de IA](#))

Se o OI se deparar com um sistema ou prática proibida:

- ▶ uma vez que estas práticas são proibidas, a sua própria utilização viola a legislação da UE. Devem ser tomadas medidas imediatas para notificar a AFM competente, independentemente de se poder comprovar a existência de um caso de discriminação;
- ▶ além disso, quando um OI concluir que uma prática que não consta atualmente desta lista viola os direitos fundamentais, deve reunir as provas e apresentar relatórios às autoridades competentes do Estado-Membro em causa e à Comissão (ver passo 4.3. [O que fazer quando um sistema ou caso de utilização representa um risco para os direitos fundamentais, mas não é classificado como “de risco elevado” ou “proibido”](#)).

Os casos que envolvam práticas proibidas podem também ser sistemas de risco elevado e/ou ter dado origem a discriminação, sendo necessário que o OI decida se são necessárias medidas adicionais relacionadas com a discriminação.



Passo 2

Recolha de informações sobre o sistema algorítmico ou de IA para identificar discriminação

O passo 2 identifica os tipos de informação que podem estar disponíveis ou acessíveis, tanto relativamente ao sistema como à probabilidade de se comprovar a existência de discriminação. Fornece orientações sobre possíveis fontes e sobre como recolher a informação.

O passo 2 é composto pelos seguintes sub-passos.

Figura 3. Passo 2 – Recolha de informações para identificar discriminação

PASSO 2		Recolha de informações sobre o sistema algorítmico ou de IA	
2.1		Informações disponíveis em sistemas algorítmicos	
2.1.1 Informações da pessoa queixosa ▶ Entrevistas ▶ Documentos da pessoa queixosa ▶ Pedido de acesso da pessoa titular dos dados (PAPTD)	2.1.2 Informações públicas ▶ Comunicações externas da parte inquirida ▶ Jurisprudência existente ▶ Outras fontes	2.1.3 Informações do requerido ou de outras partes ▶ Informações solicitadas à parte inquirida – Avaliação de impacto sobre a proteção de dados (AIPD) – Avaliação de impacto sobre os direitos humanos ou direitos fundamentais (AIDH/AIDF) – Avaliação do impacto sobre a igualdade ou género – AI Act documentation ▶ Informações estatísticas ou de inquéritos ▶ Outra documentação relativa à segurança dos produtos	

2.2 Informações adicionais em sistemas de IA de risco elevado			
2.2.1 Informações da pessoa queixosa ► Pedido baseado no artigo 86.º: direito a explicações	2.2.2 Informações públicas ► Base de dados de IA de risco elevado do Regulamento sobre a IA	2.2.3 Informações fornecidas pela parte inquirida ou outras partes ► Documentação do Regulamento sobre a IA ► AIDF ► AIPD	2.2.4 Notificação da AFM ou investigação <i>ex officio</i>

Se um OI não for uma autoridade nos termos do artigo 77.º e/ou o sistema não for identificado como de risco elevado, o passo 2.2 (por exemplo, avaliação de impacto na igualdade e informações estatísticas ou de inquéritos) pode, ainda assim, ser utilizada como orientação-quadro para permitir que qualquer OI solicite informações comparáveis à entidade responsável pela implantação ou à entidade prestadora, recorrendo aos seus poderes de investigação ou de recolha de informações, e para avaliar qualquer resposta ou falta de resposta ao abrigo do [passo 3](#). No entanto, é importante ter em conta que, nos termos do Regulamento sobre a IA, as partes inquiridas não têm a obrigação legal de apresentar essa documentação nestas circunstâncias (embora possam ter essa obrigação ao abrigo de outra legislação, por exemplo, a relativa à segurança dos produtos ou ao direito das/os consumidoras/es).

A análise destas provas recolhidas no passo 2 é realizada no passo 3. Na prática, estes passos são normalmente realizados em conjunto.

No passo 2, já se identificou, com um certo grau de certeza, que um sistema algorítmico ou um sistema de IA está envolvido no caso em análise e, potencialmente, a sua classificação como sistema de IA de risco elevado.³⁰ O próximo passo consiste em procurar informações sobre este sistema, o que poderá ajudar a identificar casos de discriminação no [passo 3](#).

Existem três categorias de fontes.

1. Informações que podem ser fornecidas ao OI pela pessoa queixosa. Essas informações podem estar disponíveis ou ser acessíveis às pessoas queixosas através da sua experiência pessoal com o processo contestado, da sua correspondência com a parte inquirida e do exercício dos seus direitos de acesso à informação, principalmente ao abrigo do RGPD e do Regulamento sobre a IA.
2. Outras informações disponíveis ao público.
3. Informações que o OI pode solicitar à parte inquirida no âmbito do exercício dos seus poderes de investigação e recolha de informações decorrentes da legislação nacional ou da União, incluindo os conferidos ao abrigo do Regulamento sobre a IA da UE.

30 Caso não tenha sido possível identificar um sistema de IA ou algorítmico, interrompa este protocolo e recorra aos seus procedimentos habituais.

Lembre-se de que as informações também podem ser divulgadas ou solicitadas durante a correspondência pré-processual ou no decurso do litígio.

Nota: o passo 2 não pretende ser exaustivo; poderão também estar disponíveis outros tipos de informação ou fontes de informação. Os quadros jurídicos nacionais, incluindo a legislação em matéria de liberdade de informação ou as normas relativas à transparência dos documentos, podem conferir aos OI poderes de recolha de informações ou de investigação que vão além dos referidos na metodologia. O acesso à informação pode também ser facilitado por novos poderes de investigação previstos nas diretivas relativas às normas (ver Introdução e passo 4).

Obstáculos conhecidos à obtenção de informação

As estratégias utilizadas para obter informação, tais como os pedidos ao abrigo da lei de acesso à informação, podem deparar-se com desafios e limitações, nomeadamente no que diz respeito a questões relacionadas com a confidencialidade e os requisitos operacionais. Em França, por exemplo, um pedido de acesso à informação apresentado por uma OSC para obter esclarecimentos sobre um sistema de pontuação de risco utilizado pela administração da segurança social responsável pela gestão dos subsídios familiares resultou apenas na divulgação do código-fonte de modelos anteriores (em oposição ao modelo atual) e de listas censuradas das variáveis utilizadas (Conselho da Europa 2025a; *La Quadrature du Net e outros contra Premier ministre and Ministère de la Culture* 2024; ver também Big Brother Watch 2025).

No processo *Kelly contra National University of Ireland* (C-104/10), em que a parte requerente alegou discriminação com base no sexo após lhe ter sido recusado o acesso a um programa de desenvolvimento profissional e solicitou à instituição de ensino informações sobre as qualificações de outras candidatas e candidatos da mesma instituição, o TJUE esclareceu que a legislação derivada da União não confere esse direito individual de acesso a tais dados. No entanto, o TJUE considerou que cabe aos tribunais nacionais determinar se, nas circunstâncias do caso, a divulgação pública desses dados é necessária para dar cumprimento aos objetivos da legislação aplicável, nomeadamente a Diretiva 97/80/CE.

O TJUE poderá, de igual modo, no futuro, continuar a interpretar as disposições relevantes das diretivas em matéria de não discriminação, a fim de garantir uma proteção judicial eficaz contra a discriminação, de forma a facilitar o acesso das partes requerentes à informação já na etapa que antecede a constituição do caso *prima facie* (Farkas e O'Farrell 2015).

Pode ser útil manter um registo prático e pesquisável das fontes consultadas. Isto pode ajudar a identificar padrões de discriminação e poupar tempo valioso às pessoas responsáveis. Os títulos sugeridos para as revisões da literatura poderiam incluir:

- ▶ fonte (incluindo um link)
- ▶ palavras-chave (discriminação por proxy, mitigação de enviesamentos, por exemplo)
- ▶ resumo
- ▶ relevância (por exemplo, a existência de discriminação detetada num sistema de reconhecimento facial).

2.1. Sistemas algorítmicos

2.1.1. Informações fornecidas pela pessoa queixosa

A pessoa queixosa dispõe frequentemente de informações muito relevantes para a identificação de uma eventual discriminação. Essas informações podem estar à sua disposição ou ser-lhes acessíveis através da sua experiência pessoal no processo de contestação ou da sua correspondência com a parte inquirida, e podem basear-se nos seus direitos de acesso à informação, nomeadamente os previstos no RGPD (ver o quadro abaixo).

Quando o caso é tratado no âmbito de uma investigação *ex officio* ou é identificado por uma AFM, não há qualquer pessoa queixosa direta envolvida. Para efeitos de recolha de informações, tenha em conta o seguinte.

Envolver as pessoas queixosas de queixas anteriores, mais antigas ou não concluídas, ou verificar se já foi apresentada uma queixa junto de outro órgão ou entidade.

Se for o caso, sugerir o exercício coletivo do direito de acesso previsto no RGPD em casos de grande importância.³¹

31 Embora o RGPD, o Regulamento sobre a IA e a DAL ofereçam oportunidades limitadas de representação coletiva, as académicas e académicos têm defendido que o exercício coletivo dos direitos individuais pode, ainda assim, ser proveitoso (Mahieu, Asghari e van Eeten 2018). Por exemplo, várias pessoas poderiam apresentar pedidos de acesso, e as informações resultantes poderiam ser partilhadas com uma pessoa intermediária de confiança através de doações de dados. Esses esforços coletivos, através de ações individualizadas, poderiam criar um conjunto de conhecimentos mais vasto sobre a utilização de dados por parte de determinadas/os intervenientes ou setores. Da mesma forma, o exercício coletivo - mas individual - do direito de acesso previsto nos artigos 15.º e 22.º do RGPD, ou do direito a explicações previsto no artigo 86.º do Regulamento sobre a IA, por parte das pessoas titulares dos dados ou das pessoas afetadas, poderia constituir uma via para obter um conhecimento mais abrangente do funcionamento dos sistemas de IA. No entanto, ao abrigo das alterações propostas ao direito de acesso previsto no RGPD, incluídas na proposta de regulamento do *Omnibus* Digital, a eficácia dos pedidos de acesso, enquanto instrumentos de transparência tanto individuais como coletivos, poderá ser significativamente reduzida. Veja mais abaixo [sobre como elaborar e dar resposta a um pedido de acesso da pessoa titular dos dados \(PAPTD\) nos termos do artigo 15.º do RGPD](#).

Obrigações de transparência e direitos relativos aos dados ao abrigo do RGPD

O RGPD inclui obrigações de transparência *ex ante* e direitos de acesso *ex post*, que permitem que as pessoas titulares dos dados sejam informadas sobre a utilização justa dos seus dados pessoais.

Ex ante

- ▶ Nos termos do n.º 1 do artigo 5.º e do Considerando 60 do RGPD, os dados pessoais devem ser tratados de forma leal e transparente em relação às pessoas titulares dos dados, que devem ser informadas da existência da operação de tratamento e das suas finalidades. Quem é responsável pelo tratamento deve fornecer à pessoa titular dos dados quaisquer informações adicionais necessárias para garantir um tratamento justo e transparente, tendo em conta as circunstâncias e o contexto específicos em que os dados pessoais são tratados.
- ▶ Nos termos dos artigos 13.º e 14.º do RGPD, quando são tratados dados pessoais, deve ser prestada às pessoas titulares dos dados informação sobre a identidade e os contactos de quem é responsável pelo tratamento, a finalidade do tratamento, a base jurídica do tratamento, as categorias de dados pessoais caso estes sejam obtidos junto de terceiros ou de fontes publicamente disponíveis, e a existência de tomadas de decisão automatizadas, incluindo a definição de perfis.³²

Estas informações *ex ante* são, normalmente, de carácter mais geral e são frequentemente incluídas em avisos ou declarações de privacidade.

TDA elegível

- ▶ Nos termos do artigo 13.º, n.º 2, alínea f), e do artigo 14.º, n.º 2, alínea g), do RGPD, as pessoas titulares dos dados devem ser explicitamente informadas da existência de processos de tomada de decisão e de definição de perfis exclusivamente automatizados, a que se refere o artigo 22.º do RGPD, e devem receber informações significativas sobre a lógica envolvida, bem como sobre o significado e as consequências previstas desse tratamento para a pessoa titular dos dados.

Uma vez que a tomada de decisões exclusivamente automatizada só é permitida nos termos do n.º 2 do artigo 22.º do RGPD se a decisão for

- ▶ necessária para a celebração ou a execução de um contrato;
- ▶ autorizada pelo direito da União ou de um Estado-Membro;

32 Parece existir um consenso crescente de que isto se aplica também às TDA não abrangidas, uma vez que ambos os artigos exigem que quem é responsável pelo tratamento revele quais são as finalidades do tratamento, em conjugação com o Regulamento (UE) 2016/679, do Considerando 60 (Barros Vale e Zanfir-Fortuna 2022: 16).

- baseada no consentimento explícito da pessoa titular dos dados, os OIs deveriam também poder identificar as disposições relevantes do contrato, a lei que autoriza o tratamento ou o consentimento, bem como o que foi exatamente consentido, por exemplo, numa declaração escrita assinada, num formulário eletrónico ou num e-mail.

Ex post

- Nos termos do artigo 15.º do RGPD, as pessoas titulares dos dados têm o direito de solicitar o acesso aos seus dados pessoais, incluindo informações sobre as categorias dos dados pessoais, as finalidades do tratamento efetuado, as/os destinatárias/os ou categorias de destinatárias/os dos dados pessoais e a existência de tomadas de decisão automatizadas, incluindo a definição de perfis.

TDA elegível

- Nos termos da alínea h) do artigo 15.º do RGPD, nos casos de tomada de decisões e de definição de perfis exclusivamente automatizadas a que se refere o artigo 22.º, as pessoas titulares dos dados têm o direito de solicitar também informações significativas sobre a lógica envolvida, bem como sobre o significado e as consequências previstas desse tratamento para a pessoa titular dos dados.

O CEPD incentiva quem é responsável pelo tratamento, como “boa prática”, a fornecer informações significativas sobre a lógica envolvida e a explicar o significado e as consequências previstas da TDA e da definição de perfis, mesmo no caso de TDA que não seja elegível (Barros Vale e Zanfir-Fortuna 2022: 16).

Nota: as jurisdições nacionais podem prever direitos adicionais no que diz respeito à divulgação de documentos. Por exemplo, na Suécia, uma pessoa que se candidate a um emprego, a uma promoção ou a uma oportunidade de formação, mas que não seja selecionada, tem o direito de solicitar e receber da entidade patronal informações por escrito sobre a formação, a experiência profissional e outras qualificações da pessoa que foi selecionada, a fim de poder comparar as qualificações (Lei sueca contra a discriminação, artigo 4.º).

No caso dos países não abrangidos pelo RGPD, devem ser tidas em conta as disposições da legislação nacional.

Casos importantes: SCHUFA Holding (2023) e CK contra Dun & Bradstreet Austria GmbH e Magistrat der Stadt Wien (2025)

(Os números entre parênteses retos referem-se aos parágrafos da decisão.)

A questão de saber se estava a ser utilizado um sistema automatizado e quais as informações que devem ser fornecidas à pessoa titular dos dados tem sido objeto de debate no contexto do RGPD, onde se aplicam disposições específicas no que diz respeito ao “tratamento automatizado, incluindo a definição de perfis” (artigo 22.º). Para que o artigo 22.º seja aplicável, é necessário que sejam preenchidas três condições.

- ▶ Tem de haver uma “decisão” (ver Considerando 71, que confirma que se trata de um âmbito alargado e apresenta exemplos específicos de recusa automática de um pedido de crédito online ou de práticas de recrutamento eletrónico sem intervenção humana).
- ▶ A decisão deve basear-se “exclusivamente no tratamento automatizado (incluindo a definição de perfis)”.
- ▶ Esta decisão, baseada exclusivamente no tratamento automatizado, deve produzir um “efeito na esfera jurídica ou de importância semelhante” para a pessoa em causa.

Quando estas condições forem cumpridas, as organizações que utilizam um sistema de tomada de decisão automatizado devem poder fornecer à pessoa titular dos dados uma “explicação significativa sobre a forma como a decisão foi tomada”. Esta formulação é muito semelhante à utilizada no artigo 86.º do Regulamento sobre a IA, “direito a explicações”.

SCHUFA Holding

No processo C-634/21, SCHUFA Holding (Pontuação), o TJUE analisou um caso em que uma empresa privada fornecia avaliações de crédito às suas entidades parceiras, tais como bancos. Para chegar a uma decisão sobre a solvabilidade, as características de uma pessoa singular foram comparadas com dados sobre o comportamento de outras pessoas com características semelhantes. Em seguida, foi atribuída uma pontuação através de procedimentos matemáticos e estatísticos para indicar, por exemplo, qual a probabilidade de uma pessoa reembolsar um empréstimo [14].

À pessoa queixosa, OQ, foi recusado um empréstimo por um banco (uma entidade terceira) na sequência de informações negativas transmitidas ao banco pela SCHUFA. OQ solicitou informações sobre os dados pessoais em causa e pediu a eliminação de alguns dados que alegadamente estavam incorretos [15].

- ▶ A SCHUFA respondeu, informando OQ da sua pontuação e descrevendo, em linhas gerais, os métodos utilizados para calcular as pontuações. No entanto, invocando o sigilo comercial, recusou-se a divulgar os vários elementos tidos em conta para efeitos desse cálculo, bem como a respetiva ponderação. Por

último, a SCHUFA afirmou que se limitou a enviar informações ao banco e que foi o banco que tomou a decisão efetiva. Com efeito, argumentaram que a pontuação não constituía uma “decisão” [16].

Em resposta às três questões colocadas, o tribunal decidiu o seguinte.

- ▶ Decisão: o conceito de decisão era suficientemente abrangente para incluir o resultado do cálculo da solvabilidade de uma pessoa, sob a forma de um valor de probabilidade relativo à capacidade dessa pessoa para cumprir os seus compromissos de pagamento no futuro [47].
- ▶ “Baseada exclusivamente na tomada de decisões automatizada, incluindo a definição de perfis”: foi consensual que a atividade da SCHUFA correspondia à definição de perfis e que a condição estava preenchida.
- ▶ “efeito na esfera jurídica ou de importância semelhante”: Um valor de probabilidade insuficiente leva, em quase todos os casos, à recusa do banco em conceder o empréstimo solicitado. Uma vez que a entidade terceira se baseia “fortemente” no valor da probabilidade, esta condição também foi cumprida [48].

Consequentemente, o tribunal considerou que, nos casos em que “o valor de probabilidade estabelecido por uma sociedade que fornece informações comerciais e comunicado a um banco desempenha um papel determinante na concessão de um crédito, a determinação desse valor deve ser qualificada, em si mesma, de decisão que produz, em relação ao titular dos dados, «efeitos na sua esfera jurídica ou que o afet[a] significativamente de forma similar», na aceção do artigo 22.º, n.º 1, do RGPD”.

O tribunal reiterou ainda a necessidade de:

- ▶ prevenir riscos de discriminação decorrentes da definição de perfis;
- ▶ recorrer a procedimentos matemáticos ou estatísticos adequados na definição de perfis;
- ▶ serem adotadas medidas técnicas e organizacionais, nomeadamente para garantir que as imprecisões nos dados pessoais sejam corrigidas e que o risco de erros seja minimizado;
- ▶ os dados serem protegidos.

É importante referir que, o tribunal considerou também que os Estados-Membros não podem adotar regulamentos que autorizem a definição de perfis sem respeitar os requisitos estabelecidos nos artigos 5.º (princípios relativos ao tratamento de dados) e 6.º (licitude do tratamento) do RGPD, nem podem prescrever de forma definitiva os resultados da ponderação dos direitos e interesses em causa na legislação [70].

Dun & Bradstreet

As explicações devem permitir que a pessoa titular dos dados compreenda e, se necessário, conteste a decisão e exerça os seus direitos em matéria de dados. A mera comunicação de uma fórmula matemática complexa, como um algoritmo ou uma descrição pormenorizada de todos os passos de um processo automatizado

de tomada de decisão, não satisfaz este requisito, uma vez que não seria suficientemente concisa e inteligível [58-59].

“Informações úteis relativas à lógica subjacente” devem descrever o procedimento e os princípios concretamente aplicados, de forma a que a pessoa titular dos dados possa compreender quais dos seus dados pessoais foram utilizados e de que forma no processo de tomada de decisão automatizada em causa. A complexidade das operações não é considerada suficiente para isentar quem é responsável pelo tratamento do dever de prestar explicações [61].

No contexto da definição de perfis de crédito, o TJUE considerou que um tribunal pode considerar suficientemente transparente e compreensível informar a pessoa titular dos dados em que medida uma variação nos dados pessoais tidos em conta teria conduzido a um resultado diferente [62]. Isto pode não ser o caso para todos os sistemas algorítmicos.

Caso quem é responsável pelo tratamento considere que estas informações não podem ser fornecidas sem revelar dados de entidades terceiras ou segredos comerciais, quem é responsável pelo tratamento é obrigada/o a fornecer as informações alegadamente protegidas à autoridade de controlo competente ou ao tribunal, que deve ponderar os direitos e interesses em causa, com vista a determinar o âmbito do direito de acesso da pessoa titular dos dados previsto no artigo 15.º desse regulamento.

Estes dois casos servem de orientação quanto à abordagem que o TJUE poderá adotar ao analisar em que medida a informação deve ser disponibilizada e sob que forma, ao abrigo do RGPD e, por analogia, das explicações exigidas pelo Regulamento sobre a IA.

Entrevista com a pessoa afetada

As pessoas queixosas que apresentam uma queixa por discriminação com base num ou mais motivos protegidos dispõem, frequentemente, de informações relevantes sobre as características que comunicaram à parte inquirida, quer recentemente, quer no passado. Também pode ser útil recolher outras informações sobre as suas características protegidas e sobre as ocasiões em que essas características possam ter sido reveladas. Tenha em atenção as suas próprias obrigações em matéria de proteção de dados. Considere questões como as que se seguem.

- ▶ Quando foi o seu primeiro contacto com esta organização/departamento governamental e quaisquer contactos subsequentes? Se tiver havido contacto prévio com a organização/departamento governamental antes do evento que está na origem da queixa, é possível que, nessa altura, tenham sido fornecidas informações sobre características protegidas.
- ▶ Pediram-lhe para preencher formulários?
- ▶ Se for esse o caso, que formulários lhe pediram para preencher?
- ▶ Considere a lista de [Características protegidas](#). Foi-lhe pedido que fornecesse informações ou que assinalasse as opções correspondentes a algum destes pontos?

- Consulte a lista de proxies conhecidos no [Anexo E](#). Foi-lhe pedido que fornecesse informações sobre algum deles?

Documentos apresentados pela pessoa queixosa

A documentação disponível ou acessível à pessoa queixosa pode conter informações relevantes. Isto pode incluir:

- documentos apresentados pela pessoa queixosa (formulários de pedido, correspondência, pedidos de acesso a dados ou outros pedidos);
- documentos fornecidos pela parte inquirida à pessoa queixosa (quaisquer contratos entre a parte inquirida e a pessoa queixosa, juntamente com os respetivos anexos, informações relativas ao tratamento de dados ou avisos de privacidade e comunicações internas, incluindo atualizações contratuais).

Elaboração e resposta a um pedido de acesso da pessoa titular dos dados (PAPTD) nos termos do artigo 15.º do RGPD

As pessoas titulares dos dados têm o direito de solicitar a quem é responsável pelo tratamento (normalmente quem é responsável pela implantação do sistema) o acesso aos seus dados pessoais, nos termos do artigo 15.º do RGPD. As respostas aos PAPTD, quando devidamente tratadas, podem conter informações altamente relevantes (ver o [passo 3](#) para mais pormenores), adaptadas ao caso específico da pessoa, incluindo:

- as categorias de dados pessoais tratados e uma cópia digital desses dados;
- as finalidades do tratamento efetuado;
- As entidades destinatárias ou as categorias de entidades destinatárias dos dados pessoais;
- a existência de tomadas de decisão automatizadas e/ou de definição de perfis, juntamente com informações significativas sobre a lógica envolvida e as consequências previstas desse tratamento para a pessoa titular dos dados.

Se uma pessoa queixosa ainda não tiver apresentado um PAPTD, recomenda-se que se incentive a pessoa a fazê-lo antes de se avançar com qualquer queixa ou investigação. Embora não existam requisitos formais sobre como apresentar um PAPTD, é aconselhável apresentar o pedido por escrito e guardá-lo (guarde uma cópia de qualquer e-mail ou carta, guarde qualquer comprovativo de envio postal ou de entrega, faça uma captura de ecrã se utilizar um formulário online, um portal ou um canal de atendimento a clientes). Para ver um modelo, consulte o [Anexo A](#).

O incumprimento das obrigações previstas no RGPD no que diz respeito ao PAPTD é generalizado. Por conseguinte, é comum deparar-se com a ausência de resposta, atrasos na resposta ou o fornecimento de informações inadequadas ou incompletas após a apresentação de um pedido. As pessoas queixosas que exerçam os seus direitos enquanto titulares dos dados devem estar preparadas para eventuais comunicações de acompanhamento, incluindo lembretes e pedidos de esclarecimentos adicionais dirigidos à organização. Em casos de grande importância, considere a possibilidade de colaborar com a APD nacional competente (ver “[Cooperação intersetorial](#)”).

A proposta de regulamento *Omnibus* Digital introduz alterações ao direito de acesso da pessoa titular dos dados ao abrigo do RGPD. A alteração proposta ao n.º 5 do artigo 12.º do RGPD³³ tem sido alvo de críticas (Skiotytė e Sadauskaitė 2026). Se for aprovada, esta medida permitiria a quem é responsável pelo tratamento recusar ou cobrar uma taxa pelos PAPTD que sejam considerados excessivos ou que visem fins “não relacionados com a proteção de dados”. Tal não deverá afetar os pedidos válidos apresentados com vista a fazer valer os direitos das pessoas titulares dos dados.

2.1.2. Informação disponível ao público

Comunicações externas da parte inquirida

A informação relevante pode ser comunicada pela parte inquirida no seu sítio Web ou plataforma, nomeadamente nas páginas de perguntas frequentes, nos termos e condições ou nos avisos de privacidade, em conformidade com as obrigações de transparência aplicáveis ao abrigo do RGPD (ver o quadro sobre as obrigações de transparência do RGPD e os direitos relativos aos dados, acima).

Preste especial atenção às referências ao objetivo do sistema, às finalidades do tratamento de dados, aos tipos de dados tratados, incluindo qualquer referência a dados sensíveis - também designados por “categorias especiais de dados” - e a qualquer referência à existência de TDA com impacto significativo (elegível) ou de definição de perfis, bem como à respetiva lógica e consequências. Estes elementos podem indicar a utilização de algoritmos ou de características protegidas (para mais pormenores, ver os passos 3.2. e 3.3.).

Em alguns países (como a Finlândia), as administrações públicas estão sujeitas a obrigações de informação e devem publicar no seu sítio Web informações relativas à utilização de sistemas de TDA e informar as pessoas titulares de dados sobre essa utilização aquando da tomada de decisões. No entanto, na maioria dos casos, não existe um registo sistemático a nível nacional ou transnacional, apesar das iniciativas locais para criar bases de dados sobre aplicações de IA e TDA (como na Bélgica e na Finlândia). Assim, os OIs enfrentam dificuldades no exercício do seu mandato de investigar, monitorizar, identificar e contestar casos de discriminação algorítmica, bem como de apoiar as vítimas (Conselho da Europa 2025a).

Jurisprudência existente

Pesquise a jurisprudência relativa a sistemas de IA ou algorítmicos semelhantes, ou a processos de tomada de decisão automatizados. Isto pode incluir a jurisprudência nacional, a jurisprudência europeia (incluindo a do Tribunal Europeu dos Direi-

33 Considerando 35, artigo 3.º, da proposta de regulamento do Parlamento Europeu e do Conselho que altera os Regulamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 e (UE) 2023/2854 e as Diretivas 2002/58/CE, (UE) 2022/2555 e (UE) 2022/2557 no respeitante à simplificação do quadro legislativo digital e que revoga os Regulamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 e a Diretiva (UE) 2019/1024 (Omnibus Digital). Disponível em: [EUR-Lex - 52025PC0837](#).

tos Humanos e do TJUE) e a jurisprudência nacional de outros países, uma vez que os sistemas algorítmicos e as plataformas funcionam frequentemente de acordo com lógicas semelhantes e padrões recorrentes em diferentes países.

Uma vez que a jurisprudência da UE em matéria de IA e regulamentação algorítmica ainda se encontra numa etapa inicial, considere também analisar a jurisprudência relacionada com o RGPD, em particular as decisões que abordam a tomada de decisões automatizada, uma vez que estas podem fornecer orientações úteis. Considere consultar o seguinte.

- ▶ Bases de dados como a [Jurisprudência – EUR-Lex](#) ou a [Base de Dados de Jurisprudência da Agência dos Direitos Fundamentais da União Europeia](#), relativas a processos do TJUE ou a processos judiciais, utilizando palavras-chave como “inteligência artificial”, “tomada de decisão automatizada”, “perfilagem” e “pontuação de crédito”, para analisar acórdãos existentes ou acompanhar os pedidos pendentes dos tribunais nacionais ao TJUE para decisões prejudiciais relevantes para aspetos pertinentes do Regulamento sobre a IA ou do RGPD.
- ▶ No que diz respeito a bases de dados específicas para IA ou sistemas algorítmicos, considere também a [Base de Dados de Jurisprudência – Tech Litigation](#), que reúne processos judiciais contra sistemas automatizados, incluindo sentenças, decisões e pareceres de tribunais nacionais e internacionais, bem como de autoridades de proteção de dados. Além disso, a [DAIL – a Base de Dados de Litígios sobre IA – Ethical Tech Initiative](#), que compila dados sobre litígios nos EUA envolvendo IA e sistemas algorítmicos, pode fornecer informações valiosas sobre tendências emergentes em matéria de litígios relacionados com a discriminação algorítmica, falhas sistémicas e riscos de discriminação, associados a tipos específicos de tecnologias, incluindo informações relevantes sobre empresas sediadas nos EUA que operam na União Europeia, quer como entidades prestadoras de sistemas de IA semelhantes, quer como responsáveis pelo tratamento de dados (como a Clearview AI).

Algumas organizações da sociedade civil estão a começar a compilar bases de dados especificamente dedicadas a casos de discriminação algorítmica ([formulário de denúncia da Algorithm Watch](#)). Estas bases de dados serão mais úteis se os OIs contribuírem para as mesmas, comunicando os resultados dos seus próprios processos judiciais ou investigações. Isto deve ser feito em conformidade com os princípios da proteção de dados e do privilégio processual.

- ▶ [Rastreador de Aplicação do RGPD – lista de coimas ao abrigo do RGPD e Coimas – Comité Europeu para a Proteção de Dados](#): para uma visão geral das coimas e sanções que as autoridades de proteção de dados na UE aplicaram ao abrigo do RGPD, com uma lista das coimas que inclui o país, a autoridade, a data, o montante da coima, a entidade responsável pelo tratamento/subcontratante, o setor e o tipo.
- ▶ [Tomada de decisões automatizada ao abrigo do RGPD](#): relatório do Future of Privacy Forum: para uma compilação de jurisprudência sobre TDA ao abrigo do RGPD, com data de abril de 2022.
- ▶ Bases de dados nacionais de jurisprudência.

Outras fontes

Existe uma vasta gama de fontes de dados que podem revelar-se úteis no contexto da identificação, investigação ou comprovação de um caso de discriminação algorítmica.

- ▶ Relatórios por país do 7.º ciclo de monitorização da Comissão Europeia contra o Racismo e a Intolerância (ECRI) terão em conta a IA.
- ▶ Relatórios de organizações da sociedade civil (OSC), que abrangam quer sistemas de IA ou algorítmicos semelhantes, quer processos de tomada de decisão semelhantes.
- ▶ Conclusões dos órgãos de monitorização da ONU, incluindo o Comité para a Eliminação da Discriminação contra as Mulheres (CEDAW), o Comité para a Eliminação da Discriminação Racial (CERD), o Comité dos Direitos da Criança, o Comité contra a Tortura (CAT), relatores especiais, a Organização Mundial da Saúde (OMS) e o Comité dos Direitos Económicos, Sociais e Culturais.
- ▶ Conclusões de outros organismos internacionais, tais como o Escritório para as Instituições Democráticas e os Direitos Humanos da Organização para a Segurança e Cooperação na Europa (OSCE/ODIHR) e a Organização para a Cooperação e Desenvolvimento Económico (OCDE). Neste contexto, o registo da OCDE sobre incidentes e riscos relacionados com a IA ([OECD AI Incident Monitor, uma base de dados para uma IA fiável – OECD.AI](#)) pode revelar-se particularmente relevante.
- ▶ Conclusões de organismos especializados nacionais, incluindo provedorias de justiça, organismos para a igualdade e ONGs.
- ▶ Registos administrativos, tais como os registos de população a nível central e local.
- ▶ Dados relativos a queixas, tais como estatísticas provenientes da polícia, do Ministério Público e dos processos e registos judiciais.
- ▶ Investigação académica e pontual, incluindo conclusões de instituições de investigação da UE, tais como a Agência dos Direitos Fundamentais da União Europeia (FRA) e o Instituto Europeu para a Igualdade de Género (EIGE). Uma pesquisa por área temática no [Repositório de Riscos da IA do MIT](#) também pode revelar informações úteis.
- ▶ Informações comparativas sobre jurisprudência, políticas e práticas nos diferentes Estados-Membros (dados relativos ao “consenso europeu”).

2.1.3. Informações fornecidas pela parte inquirida ou por outras partes

Informações solicitadas à parte inquirida ao abrigo de poderes previstos na legislação nacional ou noutra legislação da União

Os organismos para a igualdade podem solicitar informações às partes inquiridas e a outras partes, por exemplo, a quem é responsável pela implantação ou presta o sistema (caso se trate de uma organização diferente da parte inquirida), exercendo os seus poderes de investigação e recolha de informações ao abrigo da legislação

aplicável, incluindo as leis nacionais que transpõem as diretivas relativas às normas,³⁴ legislação relativa à liberdade de informação e instrumentos internacionais, tais como a Convenção-Quadro do Conselho da Europa sobre Inteligência Artificial,³⁵ ou recorrendo a canais de colaboração com as autoridades nacionais de proteção de dados.

A informação pode ser divulgada durante investigações, negociações e correspondência pré-processual, ou no decurso de um processo judicial.

Investigações: diretivas relativas às normas (artigo 8.º)

O artigo 8.º das Diretivas 2024/1499 e 2024/1500 poderia reforçar os direitos de acesso à informação dos organismos para a igualdade, nomeadamente:

- ▶ nos termos do n.º 1 do artigo 8.º das diretivas relativas às normas, os Estados-Membros devem conferir aos organismos para a igualdade poderes para investigar se ocorreu uma violação do princípio da igualdade de tratamento;
- ▶ nos termos do n.º 2 do artigo 8.º das diretivas relativas às normas, os Estados-Membros devem estabelecer um quadro para a realização de investigações que permita aos organismos para a igualdade proceder ao apuramento dos factos, incluindo:
 - direitos efetivos de acesso à informação e aos documentos necessários para determinar se ocorreu discriminação;
 - mecanismos adequados para que os organismos para a igualdade cooperem com as entidades públicas relevantes para esse efeito.

É importante referir que o n.º 3 do artigo 8.º prevê que os Estados-Membros possam delegar estes poderes noutro órgão competente. Poderia ser, por exemplo, a AFM. Nesse caso, seria a AFM a exercer os poderes previstos nos números 1 e 2 do artigo 8.º. Quando esse organismo competente tiver concluído a sua investigação, deverá fornecer ao organismo para a igualdade, mediante pedido deste, informações sobre os resultados da investigação.

34 Nos termos do artigo 16.º das diretivas relativas às normas, os organismos para a igualdade dispõem de diversos poderes em matéria de recolha de dados, incluindo a recolha de dados para a elaboração de relatórios e a realização de inquéritos independentes (artigo 16.º, n.º 2), bem como o direito de aceder a dados estatísticos, sempre que necessário, para efetuar uma avaliação global da situação em matéria de discriminação no Estado-Membro e para a elaboração de relatórios (artigo 16.º, n.º 3).

35 A Convenção-Quadro do Conselho da Europa sobre IA (2024) estabelece que as partes devem adotar ou manter medidas destinadas a garantir requisitos adequados de transparência e supervisão (artigo 8.º) e a assegurar a prestação de contas e a responsabilização por impactos negativos sobre os direitos humanos (artigo 9.º). Em particular, o artigo 14.º exige que as partes garantam vias de recurso acessíveis e eficazes, incluindo a documentação e o fornecimento de informações sobre sistemas de IA com impacto significativo sobre os direitos humanos aos organismos autorizados e, quando adequado, às pessoas afetadas, para que as pessoas possam contestar decisões tomadas com base na IA e apresentar queixas junto das autoridades competentes.

Se fossem atribuídos estes poderes à AFM, é importante referir que, nos termos do Regulamento sobre a IA, tal exige a cooperação com o OI (artigo 79.º, n.º 2).

- As investigações podem revelar-se particularmente relevantes num caso que envolva sistemas classificados como de risco não elevado, nos quais se tenha revelado difícil obter provas documentais ou em que exista uma suspeita de discriminação coletiva, mas não haja provas suficientes nos casos individuais.

Nota: não é possível dar início a quaisquer investigações nem dar-lhes continuidade enquanto estiverem pendentes processos judiciais relativos ao mesmo caso. É provável que as investigações sejam regidas pelas disposições da legislação nacional.

Avaliação de impacto sobre a proteção de dados (AIPD)

Qualquer tratamento de dados pessoais que possa implicar um risco elevado para os direitos das pessoas titulares dos dados, devido à sua natureza, âmbito, contexto ou finalidades, exige que quem é responsável pelo tratamento realize uma AIPD, em conformidade com o n.º 1 do artigo 35.º do RGPD. Por conseguinte, as AIPD são extremamente relevantes em casos que envolvam a tomada de decisões automatizada e a definição de perfis através de sistemas algorítmicos (artigo 35.º, n.º 3, do RGPD). No entanto, para além de um conjunto restrito de responsáveis pela implantação de sistemas de IA de risco elevado que têm obrigações de publicação ao abrigo do Regulamento sobre a IA (ver também a AIPD no passo 2.2.3 abaixo), não existe qualquer requisito legal, nem ao abrigo do RGPD nem do Regulamento sobre a IA, que obrigue quem é responsável pela implantação a publicar ou a fornecer a AIPD a um organismo para a igualdade. Qualquer controlo sobre a avaliação de impacto é deixado à iniciativa das APD – os canais de colaboração com essas APD podem revelar-se relevantes nesse sentido. Isto não deve dissuadir o organismo para a igualdade de apresentar tal pedido. Algumas organizações podem concordar em disponibilizar a AIPD, caso esta esteja disponível - quer ao abrigo do n.º 3 do artigo 35.º do RGPD, quer de forma voluntária - ou podem até optar por publicar um resumo da mesma. A AIPD pode ser solicitada durante a correspondência pré-processual ou caso seja instaurado um processo judicial.

Avaliações de impacto sobre os direitos humanos ou sobre os direitos fundamentais (AIDH/AIDF)

O Regulamento sobre a IA prevê uma obrigação explícita de realizar qualquer tipo de AIDF apenas para determinadas entidades responsáveis pela implantação e prestadoras de sistemas de IA de risco elevado (ver também a avaliação de impacto sobre os direitos fundamentais no passo 2.2.3 abaixo). No que diz respeito a outros sistemas algorítmicos ou de IA, não existe tal obrigação ao abrigo do Regulamento sobre a IA. No entanto, isto não impede que as entidades prestadoras adotem voluntariamente esses instrumentos (Centro Europeu para o Direito das Organizações Sem Fins Lucrativos e Instituto Dinamarquês dos Direitos Humanos

2025; FRA, 2025), com base na sua obrigação geral de respeitar e proteger os direitos fundamentais estabelecidos a nível da UE e a nível nacional, e como forma de reforçar a responsabilização das entidades operadoras de IA a este respeito (Mantelero 2024).

Mais concretamente, uma AIDH é um termo genérico que designa o processo e a ferramenta destinados a identificar, avaliar e abordar os impactos adversos, potenciais e reais, de produtos ou atividades sobre os direitos humanos, podendo ser realizada de várias formas. A metodologia e o modelo HUDERIA, desenvolvidos pelo Conselho da Europa, constituem um tipo de avaliação de riscos em matéria de direitos humanos (Conselho da Europa 2025c, 2026).

Da mesma forma, pode ter sido realizada uma AIDH ou AIDF pelas entidades criadoras, a título voluntário, para sistemas de IA de risco não elevado - nomeadamente no âmbito da sua própria diligência devida ou dos seus compromissos em matéria de direitos humanos, ou em conformidade com quadros normativos como os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos. A legislação, as políticas ou as práticas nacionais ou regionais podem também exigir que sejam realizadas e publicadas avaliações de impacto sobre os direitos humanos ou sobre os direitos fundamentais.

Em todos estes casos, os organismos para a igualdade podem solicitar a divulgação dessas avaliações no âmbito dos seus poderes de recolha de informações.

Avaliação de impacto em matéria de igualdade ou de género

Sempre que essas avaliações sejam exigidas pela legislação nacional, os organismos para a igualdade podem solicitá-las. Pode não existir qualquer obrigação legal de as realizar ou disponibilizar.

Documentação no âmbito do Regulamento sobre a IA

Mesmo que um sistema não seja classificado como de risco elevado, os organismos para a igualdade podem, ainda assim, solicitar informações comparáveis a quem é responsável pela implantação ou prestador(a), recorrendo aos seus poderes de investigação ou de recolha de informações. Embora as partes inquiridas não estejam legalmente obrigadas a elaborar e/ou fornecer essa documentação no caso de sistemas de IA de risco não elevado ou que não envolvam IA, os organismos para a igualdade podem orientar-se pelo quadro do Regulamento sobre a IA na formulação dos seus pedidos e avaliar a reação - ou a inação - da parte inquirida em conformidade, nos passos 3 e 4.

Inquéritos e informações estatísticas

Os organismos para a igualdade podem realizar ou aceder a inquéritos, incluindo inquéritos por amostragem que registem as experiências de grupos expostos à discriminação e inquéritos de opinião que avaliem a prevalência de preconceitos (diretivas relativas às normas, artigo 16.º). Podem também aceder a fontes estatísticas oficiais relevantes, tais como as compiladas pelos institutos nacionais de estatística no âmbito das diretivas da UE em matéria de não discriminação, bem

como a dados recolhidos através de recenseamentos da população e de outras fontes importantes, como o Inquérito às Forças de Trabalho (LFS) e o Inquérito sobre Rendimentos e Condições de Vida (SILC).

Diretivas relativas às normas

- ▶ Nos termos do n.º 2 do artigo 16.º das Diretivas 2024/1499 e 2024/1500, os organismos para a igualdade podem realizar inquéritos independentes sobre a discriminação.
- ▶ Nos termos do n.º 3 do artigo 16.º das Diretivas 2024/1499 e 2024/1500, os organismos para a igualdade devem poder aceder a estatísticas relacionadas com os direitos e obrigações decorrentes das diretivas da UE em matéria de combate à discriminação, sempre que tal seja necessário para efetuar uma avaliação global da situação em matéria de discriminação no Estado-Membro e para elaborar relatórios periódicos sobre o estado da igualdade no seu Estado-Membro.

Documentação ao abrigo de outra legislação em matéria de segurança dos produtos

No caso de produtos de risco não elevado vendidos por uma empresa a consumidores, podem existir requisitos ao abrigo do Regulamento relativo à Segurança Geral dos Produtos³⁶ (RSGP) e do Regulamento AFM,³⁷ que incluem obrigações e requisitos de documentação semelhantes aos previstos no Regulamento sobre a IA. Tal encontra-se fora do âmbito desta metodologia, uma vez que as competências pertencem à AFM; no entanto, isto é mencionado porque o RSGP é considerado uma rede de segurança para a IA de risco não elevado (Considerando 166 do Regulamento sobre a IA) e os seus requisitos podem levar a que a documentação relevante esteja disponível quer diretamente para a pessoa singular, quer através do organismo para a igualdade, agindo em cooperação com a AFM. Por exemplo, as entidades fabricantes abrangidas pelo regulamento são obrigadas a garantir que os seus produtos sejam acompanhados de instruções claras e de instruções de segurança destinadas a consumidores (artigo 9.º, n.º 7), bem como a elaborar documentação técnica e a realizar avaliações de risco que devem ser disponibilizadas à AFM (artigos 9.º, n.º 2 e 3, e 15.º).

³⁶ Regulamento (UE) 2023/988.

³⁷ Regulamento (UE) 2019/1020.

2.2. Informações adicionais disponíveis para sistemas de IA de risco elevado

2.2.1. Informações adicionais à disposição da pessoa queixosa

Elaboração e resposta a um pedido de esclarecimento nos termos do artigo 86.º do Regulamento sobre a IA

Este direito pode ser invocado para além do pedido de PAPTD (ver “[Elaboração e resposta a um pedido de acesso da pessoa titular dos dados \(PAPTD\) nos termos do artigo 15.º do RGPD](#)”). Qualquer pessoa sujeita a uma decisão que a afete de forma significativa e negativa, tomada com base nos resultados de um sistema de IA de risco elevado, tem o direito de obter informações sobre o papel do sistema de IA no processo de tomada de decisão e sobre os principais elementos da decisão. Estes esclarecimentos devem ser claros e significativos. As respostas devidamente tratadas podem conter informações altamente relevantes, incluindo os dados de entrada e os critérios que influenciaram a decisão (ver o [passo 3](#) para mais pormenores), para a posterior identificação de discriminação *prima facie*. Se uma pessoa queixosa ainda não tiver apresentado tal pedido, recomenda-se que se incentive a pessoa a fazê-lo antes de se avançar com qualquer queixa ou investigação. Para ver um modelo, consulte o [Anexo B](#).

Este direito só se aplica na medida em que não esteja previsto de outra forma no direito da União. Por exemplo, se o sistema algorítmico for um sistema totalmente automatizado que trata os dados pessoais da pessoa afetada, é possível que o direito a uma explicação esteja previsto no RGPD, nos artigos 13.º a 15.º (Regulamento (UE) 2016/679). Quando a parte inquirida indeferir o pedido de explicação com esta justificação, o passo seguinte seria apresentar um pedido de acompanhamento ao abrigo do RGPD (ou de outra legislação da União relevante) (a menos que tal já tenha sido feito). Para ver um modelo, consulte o [Anexo A](#).

2.2.2. Informação disponível ao público

Base de dados da UE

Ver também [1.2.1.Base de dados da UE para sistemas de IA de risco elevado](#).

No passo 1, realizou uma verificação preliminar da base de dados da UE. Se a parte inquirida constar da lista, já deverá ter verificado se está registada na base de dados como:

- ▶ entidade prestadora, constante da secção A ou B da base de dados:
 - para um caso de utilização de risco elevado que seja relevante na situação da pessoa queixosa;
 - para um caso de utilização destinado a ser utilizado num domínio de risco elevado, mas que se enquadra na exceção prevista no n.º 3 do artigo 6.º do Regulamento sobre a IA;

- ▶ uma entidade responsável pela implantação, constante da parte C da base de dados:
 - responsável pela implantação para um caso de utilização que seja relevante no contexto da queixa; qual é a entidade prestadora?

A seguir apresentam-se os principais pontos de interesse da base de dados (Regulamento sobre a IA, Anexo VIII).

Secção A: sistemas de IA de risco elevado

- ▶ Dados de contacto da entidade prestadora e da/o representante autorizada/o.
- ▶ Nome comercial ou outra referência que permita a identificação e o rastreio do sistema de IA (isto pode ser útil, por exemplo, nos casos em que um sistema de risco elevado seja utilizado como parte de outro sistema).
- ▶ Finalidade pretendida.
- ▶ Informações utilizadas pelo sistema (dados, entradas) e a sua lógica de funcionamento (não aplicável a sistemas nos domínios da aplicação da lei, migração, asilo e controlo de fronteiras).
- ▶ Estado do sistema de IA (por exemplo, ainda se encontra no mercado?).
- ▶ Tipo, número e data de validade do certificado emitido pelo organismo notificado, bem como o nome ou número de identificação desse organismo e uma cópia digitalizada do certificado (não aplicável a sistemas nos domínios da aplicação da lei, migração, asilo e controlo de fronteiras).
- ▶ Estados-Membros onde o sistema é ou foi comercializado (informação útil para a cooperação com outras autoridades).
- ▶ Uma cópia da declaração de conformidade da UE (Regulamento sobre a IA, artigo 47.º).
- ▶ Instruções de utilização em formato eletrónico (não aplicável a sistemas nos domínios da aplicação da lei, migração, asilo e controlo de fronteiras).

Secção B: Sistema de IA em relação ao qual a entidade prestadora concluiu que não apresenta um risco elevado

- ▶ Dados de contacto da entidade prestadora e da/o representante autorizada/o.
- ▶ Nome comercial ou outra referência que permita a identificação e o rastreio do sistema de IA.
- ▶ Finalidade pretendida.
- ▶ Condição prevista no n.º 3 do artigo 6.º e justificação pela qual o sistema não é considerado de risco elevado (não aplicável aos domínios da aplicação da lei, migração, asilo e controlo de fronteiras).
- ▶ Estado do sistema de IA (ainda se encontra no mercado?).
- ▶ Estados-Membros onde o sistema é ou foi comercializado.

Secção C: responsáveis pela implantação de sistemas de risco elevado (Regulamento sobre a IA, artigo 49.º, n.º 3)

- ▶ Nome e dados de contacto de quem é responsável pela implantação (apenas autoridades públicas, instituições, órgãos e agências da UE, ou pessoas que atuem em seu nome).
- ▶ URL do registo do sistema de IA na base de dados da UE (conforme efetuado pela entidade prestadora).
- ▶ Resumo da avaliação de impacto sobre os direitos fundamentais (AIDF) (não aplicável aos domínios da aplicação da lei, migração, asilo e controlo de fronteiras).
- ▶ Resumo da avaliação de impacto na proteção de dados (AIPD).

Nem todos os sistemas de IA de risco elevado constam da secção pública da base de dados da UE.

A tabela abaixo indica em que casos de utilização a informação deve ser fornecida na base de dados.

Tabela 3. Informações disponíveis na base de dados de risco elevado ao nível da UE e a nível nacional

Secção pública (artigo 49.º, n.º 1 a 3), (exceto responsáveis pela implantação privados, a menos que atue, em nome de um organismo público)	Secção não pública (artigo 49.º, n.º 4)	Aplicação a nível nacional/registo (artigo 49.º, n.º 5)
Todas as informações acima descritas são obrigatórias e estão incluídas na secção pública da base de dados.	É necessária uma quantidade limitada de informação, que se encontra apenas numa secção segura e não pública da base de dados.	Os requisitos de registo aplicam-se apenas a nível nacional.
Educação e formação profissional	Aplicação da lei	Infraestruturas críticas
Emprego, gestão de trabalhadoras e trabalhadores e acesso ao emprego por conta própria	Migração, asilo e controlo de fronteiras	
Serviços e benefícios essenciais	Sistemas de IA de risco elevado em fase de teste	
Administração da justiça e processos democráticos	Biometria utilizada nos domínios de aplicação da lei, migração, asilo e controlo de fronteiras	

Restrições ao acesso à informação

De acordo com o artigo 49.º, n.º 4, alínea d), do Regulamento sobre a IA, no que diz respeito aos sistemas de IA de risco elevado utilizados na aplicação da lei, na migração, no asilo e na gestão do controlo de fronteiras (pontos 1, 6 e 7 do Anexo III), as informações sobre o sistema de IA, tal como registadas na base de dados da UE, são arquivadas numa secção não pública e acessíveis apenas à Comissão Europeia e às AFM relevantes. Para estes efeitos, apenas a autoridade responsável pela proteção de dados ou a Autoridade Europeia para a Proteção de Dados (AEPD, no que diz respeito à Comissão) serão as AFM competentes (artigo 74.º, n.º 8 e 9) e terão acesso às informações contidas na base de dados.

Isso não significa que o material em que esses registos se baseiam também não esteja disponível. No entanto, isso significa que são necessários mais elementos para justificar o acesso aos documentos e que esse acesso pode ser recusado. Os OIs que são autoridades nos termos do artigo 77.º têm poderes para solicitar e aceder a qualquer informação ou documentação criada ou mantida ao abrigo do regulamento (ver abaixo, passo 2.2.3). Qualquer pedido deste tipo deve ser devidamente justificado, de modo a demonstrar que é necessário para o cumprimento eficaz do seu mandato, dentro dos limites da sua competência.

O regulamento deixa também claro que as atividades de fiscalização do mercado “em nada afetam a independência das autoridades judiciais nem se ingerem nas atividades destas últimas no exercício das suas funções judiciais” (artigo 74.º, n.º 8). Isto significa que, no que diz respeito a qualquer informação relevante que deva ser disponibilizada ao OI ou a uma pessoa singular no âmbito de procedimentos judiciais, as restrições previstas no n.º 8 do artigo 74.º não se aplicam. A disponibilização de material sensível, mesmo através destes procedimentos, deverá ser regida por outros requisitos de confidencialidade e por interesses de segurança pública e nacional (ver “[Confidencialidade](#)”).

Se forem estabelecidas bases jurídicas para a partilha de informações entre os organismos para a igualdade, as autoridades de fiscalização do mercado e outras autoridades nos termos do artigo 77.º (ver “[Cooperação intersetorial](#)”), será então possível que os organismos para a igualdade tenham acesso às informações obtidas pelas autoridades de fiscalização do mercado nos termos do artigo 71.º, n.º 4, e do artigo 49.º, n.º 4 (Conselho da Europa 2025b).

2.2.3. Informações adicionais fornecidas pela parte inquirida ou por outras partes

Documentação e obrigações de comunicação de informações ao abrigo do Regulamento sobre a IA

Ver também o [Regulamento sobre a IA da UE, artigo 77.º: Poderes das autoridades responsáveis pela proteção dos direitos fundamentais](#).

O Regulamento sobre a IA impõe às entidades prestadoras e responsáveis pela implantação de sistemas de IA de risco elevado a obrigação de elaborar e manter

vários tipos de documentação ao longo de todo o ciclo de vida do sistema. Os organismos para a igualdade que sejam autoridades nos termos do artigo 77.º têm o poder de solicitar e aceder a qualquer documentação criada ou mantida ao abrigo do Regulamento sobre a IA, em linguagem e formato acessíveis, necessária para o cumprimento eficaz dos seus mandatos, dentro dos limites dos seus poderes.³⁸ (Regulamento sobre a IA da UE, artigo 77.º)

Esta documentação consta da tabela de diferentes tipos de documentação técnica que se segue.

Recomenda-se que se solicitem todas estas informações, uma vez que, em conjunto, todos estes documentos proporcionam uma visão clara da utilização, da conceção, dos dados e dos riscos do sistema.

O passo 3 apresenta explicações detalhadas sobre o que estas informações revelam e como as pode utilizar.

É provável que a documentação seja organizada com base em normas de documentação universais e específicas do setor, desenvolvidas pela indústria nos últimos anos, incluindo referências a “folhas de dados” e “fichas de modelo” no Anexo IV. Para os organismos para a igualdade, seria útil conhecer estes dois tipos de documentação (Mittelstadt 2024). A estrutura e o conteúdo exigidos para este tipo de documentação estarão sujeitos às normas do Comité Técnico Conjunto n.º 21 (JTC-21) (ver abaixo, “[Normas harmonizadas](#)”).

Ver também “[Cooperação intersetorial](#)”.

De seguida apresenta-se uma lista de requisitos que devem ser cumpridos no que diz respeito aos sistemas de IA de risco elevado, nos termos do Regulamento sobre a IA. Embora nem todos os requisitos exijam explicitamente documentação, é seguro partir do princípio de que existirá, pelo menos, documentação interna sobre cada um desses requisitos.

38 Os organismos para a igualdade que não se enquadram nos termos do artigo 77.º não dispõem de uma base jurídica direta adicional ao abrigo do Regulamento sobre a IA para aceder à documentação relevante relativa a sistemas de IA de risco elevado, tendo de recorrer aos seus poderes já existentes. Continua a ser questionável se serão capazes de adquirir conhecimentos suficientes sobre o funcionamento dos sistemas de IA de risco elevado para cumprir eficazmente as suas atribuições.

Tabela 4. Requisitos para sistemas de IA de risco elevado ao abrigo do Regulamento sobre a IA da UE

Requisito (artigo)	Descrição da obrigação	Função
Sistema de gestão de riscos (artigo 9.º)	Sistema de gestão de riscos que identifica e analisa os riscos razoavelmente previsíveis para a saúde, a segurança ou os direitos fundamentais, de acordo com as medidas de gestão de riscos.	Entidade prestadora
Dados e governação de dados (artigo 10.º)	Os conjuntos de dados de treino, validação e teste devem estar sujeitos à governação de dados. As práticas incluem escolhas de conceção, recolha e origem dos dados, preparação adequada, pressupostos formulados, análise de enviesamentos e medidas adequadas para prevenir o enviesamento.	Entidade prestadora
Documentação técnica para sistemas de IA de risco elevado (Artigo 11.º, Anexo IV)	Descrição geral do sistema de IA e descrição pormenorizada de determinados elementos e processos. A tabela abaixo apresenta uma descrição mais pormenorizada.	Entidade prestadora
Manutenção de registos (artigo 12.º)	Os sistemas devem registar eventos relevantes para a identificação de riscos para a saúde, a segurança ou os direitos fundamentais e facilitar a monitorização pós-comercialização. Isto inclui o registo do período de utilização, a base de dados de referência, os dados introduzidos e a identificação das pessoas singulares envolvidas na verificação dos resultados.	Entidade prestadora
Instruções de utilização (artigo 13.º) e supervisão humana (artigo 14.º)	O funcionamento dos sistemas deve ser suficientemente transparente. Isto inclui as características, capacidades e limitações do sistema, bem como a sua finalidade e os parâmetros de desempenho. Além disso, devem ser tidos em conta a supervisão humana e os recursos necessários para o funcionamento do sistema.	Entidade prestadora a quem é responsável pela implantação
Sistema de gestão da qualidade (artigo 17.º)	Documentação de políticas, procedimentos e instruções, incluindo a estratégia de conformidade, técnicas de conceção e controlo de qualidade, bem como a análise antes, durante e após o desenvolvimento. Inclui ainda especificações técnicas e sistemas de gestão de dados. Por fim, a documentação relativa à resposta a incidentes graves, à comunicação com as autoridades, à manutenção de registos, à gestão de recursos e à repartição de responsabilidades.	Entidade prestadora

Requisito (artigo)	Descrição da obrigação	Função
Registos gerados automaticamente (artigo 19.º)	Os prestadores de serviços devem conservar os registos gerados automaticamente durante, pelo menos, seis meses. As instituições financeiras mantêm os registos em conformidade com a legislação aplicável em matéria de serviços financeiros.	Entidade prestadora
Registos gerados automaticamente (artigo 26.º)	Quem é responsável pela implantação deve conservar os registos gerados automaticamente durante, pelo menos, seis meses. As instituições financeiras mantêm os registos em conformidade com a legislação aplicável em matéria de serviços financeiros.	Responsável pela implantação
Avaliação de impacto sobre os direitos fundamentais (artigo 27.º)	Embora haja exceções, quem é responsável pela implantação devem realizar uma avaliação do impacto que a utilização do sistema possa ter sobre os direitos fundamentais. Isto inclui os processos de acordo com a finalidade pretendida, a descrição do período de tempo e da frequência, as categorias de pessoas afetadas, os riscos específicos de danos, as medidas de supervisão humana e as medidas adotadas caso o risco se concretize.	Responsável pela implantação
Declaração de conformidade da UE (artigo 47.º, anexo V)	A entidade prestadora deve elaborar uma declaração de conformidade da UE (legível por máquina), por escrito e assinada, para cada sistema de IA de risco elevado, que deve permanecer à disposição das autoridades nacionais durante 10 anos após a sua colocação no mercado, na qual se ateste que o sistema cumpre os requisitos estabelecidos na secção 2 do Regulamento sobre a IA.	Entidade prestadora
Marcação CE (artigo 48.º)	Os sistemas estão sujeitos aos princípios gerais estabelecidos no artigo 30.º do Regulamento (CE) n.º 765/2008 e devem ostentar a marcação CE.	Entidade prestadora
Dados de monitorização pós-comercialização (artigo 72.º)	As entidades prestadoras devem estabelecer um sistema de monitorização pós-comercialização, que recolha, documente e analise dados relevantes sobre o desempenho do sistema, de modo a permitir a avaliação da conformidade.	Entidade prestadora
Comunicação de incidentes (artigo 73.º)	As entidades prestadoras são obrigadas a comunicar incidentes graves às autoridades de fiscalização do mercado do respetivo Estado-Membro.	Entidade prestadora à AFM. A AFM deverá envolver os OI.

A documentação técnica exigida às entidades prestadoras nos termos do artigo 11.º do Regulamento sobre a IA, em conjugação com o Anexo IV do mesmo regulamento, constituirá um recurso particularmente útil para os OI.

A tabela que se segue aprofunda esta documentação técnica e indica aos organismos para a igualdade os elementos obrigatórios que podem ser relevantes para efeitos da aplicação desta metodologia.

Tabela 5. Diferentes tipos de documentação técnica nos termos do artigo 11.º e do anexo IV

(adaptado com autorização de Mittelstadt 2024)

Tipo de documentação	Explicação
1. Descrição geral do sistema de IA	Isto inclui: ▶ finalidade pretendida ▶ interações com o sistema ▶ gestão de versões e reflexão ▶ presença em software e hardware, ou nos produtos de que faz parte ▶ hardware no qual se destina a ser utilizado ▶ interface de utilizador e instruções para quem é responsável pela implantação.
2. Especificações de conceção	Isto inclui: ▶ métodos e passos para o desenvolvimento do sistema ▶ especificações de conceção; lógica, algoritmo e escolhas fundamentais, incluindo pressupostos e opções de otimização ▶ relevância dos parâmetros escolhidos ▶ resultado esperado e a sua qualidade ▶ possíveis compromissos no que diz respeito ao cumprimento das normas.
3. Arquitetura do sistema	Explicação da estrutura dos componentes de software, da sua interação e integração, bem como dos recursos computacionais utilizados para o desenvolvimento, formação, testes e validação.
4. Requisitos relativos aos dados	Os requisitos em matéria de dados incluem folhas de dados que descrevam os métodos de treino, as técnicas e os conjuntos de dados utilizados, com informações sobre a sua origem, âmbito e características, a forma como foram obtidos, os procedimentos de rotulagem e os métodos de limpeza.
5. Supervisão humana	Avaliação das medidas de supervisão humana implementadas em conformidade com o artigo 14.º, juntamente com as medidas técnicas necessárias para facilitar a interpretação do sistema de IA por quem é responsável pela implantação.

Tipo de documentação	Explicação
6. Indicadores de desempenho	Procedimentos de validação e teste utilizados, juntamente com informações sobre as principais características dos dados de teste, parâmetros utilizados para medir a exatidão, a robustez e a conformidade, bem como os impactos potencialmente discriminatórios. Contém também todos os registos e relatórios de testes, incluindo as alterações previamente definidas.
7. Capacidades	São necessárias informações detalhadas sobre a monitorização, o funcionamento e o controlo do sistema de IA, nomeadamente as suas capacidades e limitações. Isto inclui os níveis de exatidão para grupos específicos.
8. Gestão de riscos	Sistema de gestão de riscos, tal como descrito no artigo 9.º.
9. Monitorização pós-comercialização	Uma descrição pormenorizada do sistema em vigor para avaliar o desempenho do sistema após a comercialização, em conformidade com o artigo 72.º.
10. Outra legislação da UE	Normas harmonizadas aplicadas, cópia da declaração de conformidade da UE (artigo 47.º).

Normas harmonizadas

As normas harmonizadas são normas técnicas atualmente em fase de desenvolvimento pelas organizações europeias de normalização (CEN/CENELEC) que, se forem cumpridas, conferirão às entidades prestadoras de sistemas de IA de risco elevado uma “presunção de conformidade” com o Regulamento sobre a IA. Na prática, isto abrangerá provavelmente um vasto leque de elementos de informação, incluindo aqueles necessários para facilitar a compreensão do funcionamento do sistema de IA, das suas características, capacidades, pontos fortes, limitações e desempenho, em conformidade com o texto legal (Soler Garrido et al. 2024)

As seguintes normas, atualmente em fase de elaboração, foram consideradas particularmente importantes para definir os requisitos da documentação técnica à disposição dos organismos para a igualdade.³⁹

- **JT021036** “Inteligência artificial – Conceitos, medidas e requisitos para a gestão do enviesamento em sistemas de IA”: o objetivo desta norma é definir “conceitos, medidas e requisitos para a avaliação e o tratamento do enviesamento em sistemas de IA. Isto inclui enviesamentos indesejados pela entidade prestadora e por quem é responsável pela implantação da IA, de acordo

³⁹ Para uma lista e a descrição de todas as normas atualmente em fase de elaboração, consulte o documento do CEN/CENELEC intitulado “Programa de Trabalho do CEN/CLC/JTC 21”, disponível em: [CEN - CEN/CLC/JTC 21](#), consultado a 25 de junho de 2026. Outras normas, incluindo trabalhos de normalização internacional já existentes (tais como as normas ISO/IEC), podem também ser relevantes quando se trata de abordar o enviesamento e a transparência nos sistemas de IA. As normas internacionais não são, normalmente, gratuitas e estão sujeitas a proteções de propriedade intelectual, o que dificulta o acesso dos organismos para a igualdade às mesmas.

com as respetivas especificações do sistema de IA, no contexto do Regulamento sobre a IA”.

- ▶ **JT021008** “Quadro de fiabilidade da IA”, partes 1 (registo), 2 (exatidão e robustez) e 3 (transparência e supervisão humana): o objetivo desta norma é definir terminologia, conceitos, requisitos e orientações sobre registo, precisão, robustez, transparência e supervisão humana.
- ▶ **JT021024** “Gestão de riscos da IA”: o objetivo desta norma é definir requisitos e fornecer orientações para a gestão de riscos dos sistemas de IA ao longo de todo o seu ciclo de vida. Este documento exige que as entidades prestadoras estabeleçam critérios objetivos para a aceitabilidade do risco, mas não especifica os níveis de risco aceitáveis.

É improvável que estas normas definam limiares ou expliquem de que forma um tratamento diferenciado entre pessoas ou grupos de pessoas constituiria discriminação ilegal. De acordo com Mittelstadt (2024), os OIs devem estar cientes de que as normas definirão expectativas sobre a forma como o enviesamento pode ser medido e mitigado nos sistemas de IA, mas não determinarão se esses enviesamentos são ilegais ou antiéticos.

Normas, avaliações de conformidade e certificados

Presume-se que os sistemas de risco elevado em conformidade com as normas harmonizadas cumprem os requisitos da secção 2 do Regulamento sobre a IA (requisitos para sistemas de IA de risco elevado). No entanto, é importante notar que o cumprimento das obrigações de transparência ou de outras obrigações não indica que a utilização do sistema de IA ou os seus resultados sejam lícitos ao abrigo do regulamento ou de outra legislação, tal não devendo prejudicar outras obrigações de transparência aplicáveis a quem é responsável pela implantação de sistemas de IA previstas na legislação da União ou na legislação nacional (Considerando 137). As entidades prestadoras devem indicar as normas harmonizadas aplicadas ao sistema de IA. Nos casos em que não tenham sido utilizadas normas harmonizadas, as entidades prestadoras devem explicar de que forma os requisitos do Regulamento sobre a IA (Capítulo III, secção 2, do Regulamento sobre a IA) foram cumpridos de outra forma, por exemplo, através da utilização de outras normas e especificações técnicas relevantes. Isto deverá permitir que os organismos para a igualdade determinem quando foi cumprida uma norma relevante em matéria de enviesamento, fiabilidade ou gestão harmonizada de riscos.

Impacto de uma presunção de conformidade

A eventual presunção de conformidade não impede a investigação ou a tomada de medidas relativamente a casos de discriminação ou outros riscos para os direitos humanos. Em primeiro lugar, o próprio Regulamento sobre a IA reconhece que um sistema de IA que cumpra o regulamento pode, ainda assim, apresentar riscos e, no artigo 82.º, prevê um procedimento para lidar com esta situação. Da mesma forma, o n.º 3 do artigo 7.º do Regulamento (UE) n.º 2023/988 relativo à segurança geral dos produtos (que pode aplicar-se a sistemas de IA de risco não elevado) prevê que a presunção de conformidade com o requisito geral de segurança previsto no regu-

lamento não impede a AFM de tomar todas as medidas adequadas ao abrigo do regulamento, caso existam provas de que, apesar da presunção, o produto é perigoso.

Nota: nos termos do Regulamento AFM (UE) 2019/1020, sempre que qualquer operador(a) económico(a) apresente relatórios de teste ou certificados que atestem a conformidade do seu produto com a legislação de harmonização da União, a AFM deve ter “devidamente em conta” o relatório ou certificado.

Avaliação de impacto sobre os direitos fundamentais

A obrigação de realizar uma avaliação de impacto sobre os direitos fundamentais (AIDF) aplica-se apenas a determinadas entidades responsáveis pela implantação de sistemas de IA de risco elevado, tal como previsto no artigo 27.º do Regulamento sobre a IA e nas alíneas b) e c) do n.º 5 do Anexo III do Regulamento sobre a IA. Isto inclui:

- a. responsáveis pela implantação de sistemas de IA de risco elevado que sejam organismos públicos ou entidades privadas prestadoras de serviços públicos;
- b. responsáveis pela implantação de sistemas de IA de risco elevado utilizados para avaliar a solvabilidade de pessoas singulares ou para determinar a sua pontuação de crédito (com exceção dos sistemas de IA utilizados para a deteção de fraude financeira), bem como os utilizados para avaliar riscos ou determinar os preços nos seguros de vida e de saúde.

No âmbito do *Omnibus* Digital sobre a IA, reconhece-se que existe uma sobreposição entre a AIDF e a AIPD. Assim, poderá ser necessário solicitar a AIPD caso esta seja apenas referenciada, em vez de estar incorporada na AIDF.⁴⁰

Após a conclusão da AIDF, a entidade responsável pela implantação, nos termos dos números 3 e 5 do artigo 27.º do Regulamento sobre a IA, é obrigado a notificar a AFM competente dos resultados da AIDF, mediante a apresentação de um modelo (padronizado) devidamente preenchido. Além disso, quem é responsável pela implantação deve apresentar um resumo das conclusões da AIDF no âmbito do seu processo de registo na base de dados da UE, no caso dos que têm obrigações de registo nos termos do n.º 3 do artigo 49.º do Regulamento sobre a IA. As entidades responsáveis pela implantação da segunda categoria (do setor do crédito e dos seguros) não estão sujeitas a esta obrigação. Espera-se, portanto, que os organismos para a igualdade encontrem um resumo na secção C da base de dados da UE, tal como previsto no Anexo VIII, apenas relativamente às AIDFs obrigatórias realizadas por organismos públicos ou por entidades privadas que se enquadram na primeira categoria.

Nota: a aplicação de ambas as obrigações é limitada no caso das autoridades públicas que implantam sistemas de IA de risco elevado nos domínios da aplicação da lei, da migração, do asilo e do controlo de fronteiras. Nos termos do n.º 4 do artigo

⁴⁰ Regulamento (UE) 2026/1744 do Parlamento Europeu e do Conselho, de 8 de julho de 2026, que altera os Regulamentos (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 no que diz respeito à simplificação da aplicação das regras harmonizadas em matéria de inteligência artificial (Regulamento Omnibus Digital em matéria de IA). Disponível em: <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>, consultado a 24 de julho de 2026.

49.º do Regulamento sobre a IA, não deve ser apresentado à base de dados da UE qualquer resumo das conclusões da AIDF - nem mesmo na sua secção segura e não pública. Além disso, nos termos do n.º 3 do artigo 27.º do Regulamento sobre a IA, essas entidades responsáveis pela implantação, em casos excepcionais - incluindo por razões de segurança pública - podem ser isentas da obrigação de notificar as autoridades de fiscalização do mercado (AFM) dos resultados da AIDF, ao abrigo da derrogação ao procedimento de avaliação da conformidade descrita no n.º 1 do artigo 46.º do Regulamento sobre a IA (ver também o quadro abaixo sobre o domínio da aplicação da lei). As possibilidades de os organismos para a igualdade acederem a informações nestes casos são, por conseguinte, limitadas nos termos do Regulamento sobre a IA.

As entidades responsáveis pela implantação de outras categorias de sistemas de IA de risco elevado - por exemplo, uma empresa de recrutamento que utilize IA para filtrar ou selecionar candidatas e candidatos - não são legalmente obrigadas a realizar uma AIDF. No entanto, isso não significa necessariamente que, nesses casos, não seja realizada uma AIDF. Algumas organizações podem fazê-lo ao abrigo da legislação nacional, em conformidade com quadros como os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos, ou para se alinharem com os seus próprios compromissos em matéria de diligência devida ou de direitos humanos. Nestes casos, os organismos para a igualdade podem solicitar a divulgação de informações no âmbito dos seus poderes de recolha de informações.

As entidades prestadoras de sistemas de IA de risco elevado não estão sujeitas à obrigação de realizar uma avaliação de impacto sobre os direitos fundamentais do tipo específico referido no artigo 27.º do Regulamento sobre a IA. No entanto, a realização de uma AIDF como ferramenta geral para identificar, avaliar e abordar impactos adversos potenciais ou efetivos sobre os direitos fundamentais, com base no quadro da avaliação de impacto sobre os direitos humanos (AIDH), faz parte da avaliação da conformidade e da obrigação da entidade prestadora de dispor de um sistema de gestão de riscos e de gestão da qualidade, tal como previsto no n.º 2 do artigo 9.º, alínea g), n.º 1, do artigo 17.º e no artigo 43.º do Regulamento sobre a IA (Mantelero 2024). Este tipo de avaliação de impacto seguiria, normalmente, uma abordagem baseada em normas e pode, da mesma forma, ser solicitada, juntamente com o resto da documentação mantida ao abrigo do Regulamento sobre a IA, pelos organismos para a igualdade que exerçam os seus poderes nos termos do artigo 77.º do Regulamento sobre a IA (ver acima, no passo 2.1.3).

Para além dos requisitos legais previstos no Regulamento sobre a IA da UE, as leis, políticas ou práticas nacionais ou regionais podem exigir a realização de avaliações de impacto sobre os direitos humanos ou os direitos fundamentais e, em alguns casos, a sua divulgação pública. Nestes casos, os organismos para a igualdade podem solicitar a divulgação de informações no âmbito das suas competências de recolha de informações.

Avaliação de impacto sobre a proteção de dados (AIPD)

Qualquer tratamento de dados pessoais que possa implicar um risco elevado para os direitos das pessoas titulares dos dados, devido à sua natureza, âmbito, contexto ou finalidades, exige que quem é responsável pelo tratamento realize uma avalia-

ção de impacto sobre a proteção de dados (AIPD), em conformidade com o n.º 1 do artigo 35.º do RGPD. Por conseguinte, as AIPD são, por definição, extremamente relevantes nos casos de sistemas de IA de risco elevado que envolvam o tratamento de dados pessoais, a tomada de decisões automatizada e a definição de perfis (ver n.º 3 do artigo 35.º do RGPD).

No entanto, a apresentação de resumos das AIPD na base de dados da UE (secção C) é exigida apenas a determinados grupos restritos de responsáveis pela implantação de sistemas de IA de risco elevado, que são obrigadas/os a registar a sua utilização de IA na base de dados da UE, nos termos do n.º 3 do artigo 49.º. Isto inclui as autoridades públicas, as instituições, os órgãos, os serviços e as agências da União - ou as pessoas que atuam em seu nome e que utilizam sistemas de IA de risco elevado. No que diz respeito às restantes entidades responsáveis pela implantação de sistemas de IA de risco elevado, não existe qualquer requisito legal direto, nem ao abrigo do RGPD nem do Regulamento sobre a IA, para publicar ou disponibilizar a AIPD a um organismo para a igualdade. Qualquer controlo sobre a avaliação de impacto é deixado à iniciativa das APD - os canais de colaboração com essas APD podem revelar-se relevantes nesse sentido. Isto não deve dissuadir o organismo para a igualdade de apresentar tal pedido, no âmbito dos seus poderes de recolha de informações previstos na legislação nacional. Algumas organizações podem concordar em disponibilizar a AIPD, caso esta esteja disponível, ou podem até optar por publicar um resumo da mesma. A AIPD pode ser solicitada durante a correspondência pré-processual ou caso seja instaurado um processo judicial.

A proposta de regulamento *Omnibus Digital*⁴¹ exige que o CEPD elabore listas únicas, válidas em toda a UE, das atividades de tratamento que exigem ou não uma AIPD, juntamente com uma metodologia e um modelo comuns,⁴² que se prevê que substituam o atual sistema fragmentado de listas nacionais e harmonizem essas listas ao nível da UE.

2.2.4. Notificação da AFM ou investigação *ex officio*

O organismo para a igualdade pode esperar receber informações da AFM sobre sistemas de IA que representem um risco para os direitos à não discriminação ou que estejam envolvidos em incidentes graves que violem esses direitos. Para mais informações sobre o tipo de informação a esperar, consulte o ponto 1.1. [Recolha inicial de informações](#).

Os OI poderiam obter a documentação relativa ao Regulamento sobre a IA junto das AFM, caso uma AFM já a tivesse obtido junto da entidade prestadora. Isto poderá acelerar o processo de acesso dos OI. As partes inquiridas não podem impedir

41 Artigo 3.º da Proposta de Regulamento do Parlamento Europeu e do Conselho que altera os Regulamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 e (UE) 2023/2854 e as Diretivas 2002/58/CE, (UE) 2022/2555 e (UE) 2022/2557 no respeitante à simplificação do quadro legislativo digital e que revoga os Regulamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 e a Diretiva (UE) 2019/1024 (Omnibus Digital), [EUR-Lex - 52025PC0837 - EN - EUR-Lex](#), consultada a 25 de junho de 2026.

42 Em maio de 2026, o Comité Europeu para a Proteção de Dados realizou uma consulta sobre um modelo de AIPD, que está disponível aqui: www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en.

que as AFM partilhem a documentação com os OIs a pretexto da proteção do segredo comercial, especialmente quando os OIs solicitam a documentação através da AFM (Conselho da Europa 2025b). Para um exemplo análogo da aplicação desta questão na prática, consulte o processo CK contra Dun & Bradstreet Austria GmbH e Magistrat der Stadt Wien, parágrafo 76.

Quando o caso é tratado no âmbito de uma investigação *ex officio* ou de uma notificação por uma AFM, considere:

- ▶ solicitar a divulgação de documentos da AFM que sejam necessários para a investigação do OI;
- ▶ organizar uma mesa-redonda ou um workshop com ONGs relevantes ou outras organizações interessadas e aproveitar o debate para recolher informações relevantes;
- ▶ sensibilizar e realizar consultas para identificar as pessoas ou grupos afetados, nomeadamente através de inquéritos ou de outros processos participativos de recolha de informação.

Domínio da aplicação da lei

As possibilidades de recolha de informação serão mais limitadas no contexto da aplicação da lei, tornando mais difícil identificar a utilização de IA ou de sistemas algorítmicos e qualquer discriminação daí resultante.⁴³

Regulamento sobre a IA

- ▶ Nos termos do n.º 4 do artigo 49.º do Regulamento sobre a IA, o registo de sistemas de IA de risco elevado nos domínios da aplicação da lei, da migração, do asilo e da gestão do controlo de fronteiras deve ser efetuado numa secção segura e não pública da base de dados da UE referida no artigo 71.º e deve incluir apenas um conjunto específico de informações, excluindo, por exemplo, informações sobre os dados de entrada e a sua lógica de funcionamento. Esta base de dados não pública é ainda acessível às AFM designadas para os sistemas de IA destinados à aplicação da lei e ao controlo de fronteiras, em conformidade com o n.º 8 do artigo 74.º, e, em princípio, não é acessível aos OI. Para mais informações, consulte a secção 2.2.2 “Restrições ao acesso à informação”.
- ▶ Em conformidade com o n.º 1 do artigo 27.º do Regulamento sobre a IA, as autoridades responsáveis pela aplicação da lei, na sua qualidade de autoridades públicas, são obrigadas a realizar uma avaliação de impacto sobre os direitos fundamentais (AIDF) antes da implementação de um sistema de IA de risco elevado. No entanto, há duas exceções a este respeito. Em primeiro lugar, nos termos do artigo 49.º, n.º 4, alínea c), do Regulamento sobre a IA, tais responsáveis pela implantação não devem submeter um resumo das conclusões da AIDF ou da AIPD à base de dados da UE - nem mesmo na sua secção segura e não pública. Em segundo lugar, podem, em casos excecio-

43 Para uma comparação entre os direitos relativos aos dados algorítmicos no RGPD e na DAL, ver González Fuster (2020).

nais, nomeadamente por razões de segurança pública, ser autorizadas pela AFM a colocar no mercado ou a colocar em serviço um sistema de IA de risco elevado sem cumprir os procedimentos de avaliação da conformidade ou, em casos “urgentes”, sem qualquer autorização (artigo 46.º, n.º 1 e 2, do Regulamento sobre a IA). Nos termos do n.º 3 do artigo 27.º do Regulamento sobre a IA, tal incluiria também a isenção da obrigação de notificar a AFM dos resultados da AIDF.

Nota: Os artigos 27.º e 46.º do Regulamento sobre a IA não preveem qualquer isenção da obrigação de realizar a AIDF, e a condição prevista no n.º 1 do artigo 46.º limita-se especificamente ao “período limitado enquanto estiverem em curso os procedimentos de avaliação da conformidade necessários”. O n.º 2 do artigo 46.º exige ainda que, em casos urgentes, a autorização seja solicitada “durante ou após a utilização, sem demora injustificada”.

É importante referir que, caso a autorização venha a ser recusada posteriormente:

- ▶ a utilização do sistema de risco elevado deve ser suspensa com efeito imediato;
- ▶ todos os resultados e produtos decorrentes dessa utilização devem ser imediatamente eliminados.

As possíveis vias através das quais os organismos para a igualdade podem aceder a informações relacionadas tanto com a AIPD como com a AIDF são analisadas de seguida.

Diretiva relativa à aplicação da lei

Além disso, a diretiva relativa à aplicação da lei (DAL)⁴⁴ prevê várias exceções e possíveis restrições aos direitos de informação das pessoas singulares através das transposições nacionais, caso tal seja necessário para evitar prejudicar a prevenção, deteção, investigação ou repressão de infrações penais ou a execução de sanções penais e para proteger a segurança pública e nacional (artigo 13.º, n.º 3, e artigo 15.º da DAL).

Consequentemente, as práticas variam entre os Estados-Membros no que diz respeito ao tipo de informação a fornecer e à forma como esta pode ser consultada; por isso, a remissão para a legislação nacional é fundamental nesta matéria.

Tomada de decisão automatizada

- ▶ O artigo 11.º da DAL proíbe certas formas de tratamento automatizado, incluindo a definição de perfis, e exige que esse tratamento seja explicitamente autorizado pelo direito da União ou dos Estados-Membros, sob reserva de garantias adequadas para os direitos e liberdades das pessoas titulares dos

44 A referência à DAL no que diz respeito às fontes de informação não deve ser considerada exaustiva; outros instrumentos no âmbito mais vasto da liberdade, segurança e justiça, tais como a Decisão do Conselho relativa ao SIS II, o VIS e o EURODAC, podem igualmente conter normas substantivas e processuais relativas aos direitos das pessoas titulares dos dados, incluindo os direitos à informação e ao acesso.

dados. O nível mínimo de proteção exigido consiste no direito de obter intervenção humana por parte de quem é responsável pelo tratamento. Será necessário analisar os quadros jurídicos nacionais que regulam o tratamento automatizado por parte das autoridades responsáveis pela aplicação da lei, a fim de determinar que informações sobre o tratamento automatizado devem estar disponíveis. Para conhecer as diferentes formas de transposição nos vários Estados-Membros, consultar Vogiatzoglou e Marquiene 2022; ver também o Considerando 38.

- Os artigos 13.º e 14.º da DAL não estabelecem explicitamente obrigações de informação relativas à utilização da tomada de decisões automatizada, incluindo a definição de perfis.

Divulgação de informações

- Nos termos do n.º 1 do artigo 13.º da DAL, as entidades responsáveis pelo tratamento de dados encontram-se obrigadas a fornecer determinadas informações mínimas, incluindo a sua identidade e os dados de contacto da entidade responsável pelo tratamento, o direito das pessoas titulares dos dados de aceder aos seus dados pessoais e as finalidades previstas para o tratamento dos dados.

Essa informação não diz respeito a uma determinada pessoa titular dos dados, mas sim a um determinado procedimento de tratamento e a todas as pessoas titulares dos dados potencialmente afetadas por esse procedimento. Normalmente, está disponível no sítio Web específico da autoridade competente. Foi referido que nem sempre é fácil ou possível encontrar as informações relevantes no sítio Web da entidade centralizada que supervisiona as autoridades responsáveis pela aplicação da lei, da autoridade policial nacional ou do ministério competente (Vogiatzoglou e Marquiene 2022).

- O n.º 2 do artigo 13.º da DAL alarga o âmbito das informações a partilhar com as pessoas titulares dos dados, incluindo a base jurídica para o tratamento e, quando aplicável, as categorias de destinatárias/os com quem os dados pessoais serão partilhados e, se necessário, informações adicionais, em especial quando os dados pessoais forem recolhidos sem o conhecimento da pessoa titular dos dados. Nos termos do n.º 3 do artigo 13.º, tal pode ser adiado, restringido ou mesmo omitido ao abrigo da legislação nacional, desde que essa medida cumpra os critérios de necessidade e proporcionalidade numa sociedade democrática.

Essas informações, se forem suficientemente específicas, podem ser disponibilizadas no sítio Web, juntamente com as informações mínimas.

Direito de acesso

- Nos termos do artigo 14.º da DAL, é concedido às pessoas titulares dos dados o direito de aceder a mais informações sobre as atividades de tratamento de dados para além das informações gerais disponibilizadas ao público, incluindo as finalidades da operação de tratamento, as categorias de dados em causa e as destinatárias e destinatários ou categorias de destinatárias e

destinatários a quem os dados são divulgados, bem como a comunicação dos dados objeto de tratamento e da sua origem.

Ao contrário do RGPD, o artigo não prevê explicitamente o direito de ser informado sobre a existência e a lógica da tomada de decisões automatizada, nem sobre as potenciais consequências para a pessoa titular dos dados. No entanto, as autoridades responsáveis pela aplicação da lei podem ser obrigadas, ao abrigo da legislação nacional, a divulgar informações sobre a forma como foi estabelecido o perfil de uma pessoa singular.

- ▶ Nos termos do Considerando 43 da DAL, as informações fornecidas não têm de incluir uma cópia efetiva dos dados tratados, como acontece, por exemplo, no RGPD; em vez disso, basta um resumo completo.
- ▶ O conteúdo da resposta - quando o acesso não é recusado por motivos de forma - resume-se frequentemente a respostas padronizadas, breves e desprovidas de informação substancial, mas que, ainda assim, são consideradas formalmente conformes (Erdogan 2024).

Nos termos do artigo 15.º da DAL, o direito de acesso pode ser adiado, restringido ou mesmo suprimido ao abrigo da legislação nacional, caso tal medida seja necessária e proporcionada numa sociedade democrática para a proteção, nomeadamente, da segurança pública ou nacional, ou para o bom desenrolar de inquéritos, investigações ou processos oficiais ou judiciais.

Pedido de acesso

- ▶ Os artigos 14.º e 17.º, n.º 3, da DAL preveem dois tipos de procedimento para o exercício do direito de acesso. Em primeiro lugar, o procedimento de “acesso direto” previsto no artigo 14.º da DAL, ao abrigo do qual as pessoas singulares podem dirigir-se diretamente à autoridade responsável pela aplicação da lei, ou seja, a quem é responsável pelo tratamento, com questões relativas aos seus dados pessoais. Em segundo lugar, um procedimento excecional, o acesso “indireto”, em que o direito de acesso é exercido pela autoridade nacional de proteção de dados (APD), na qualidade de intermediária.

As leis nacionais que implementam o sistema de acesso indireto, como é o caso da Bélgica, onde o acesso indireto é a regra por defeito, têm sido alvo de críticas devido às suas deficiências estruturais e processuais (Dimitrova e De Hert 2024), que limitam a supervisão eficaz das atividades de tratamento de dados e a comunicação de informações relevantes às pessoas titulares dos dados em causa.

Nota: quando as informações são recolhidas por uma autoridade competente para fins de aplicação da lei, estas enquadram-se no âmbito de aplicação da DAL - por exemplo, dados relativos aos antecedentes criminais de uma pessoa. Quando as informações são extraídas de outra fonte pública ou recolhidas para fins que não sejam a aplicação da lei (tais como a situação civil, laboral ou educativa), estas enquadram-se no âmbito de aplicação do RGPD. Em determinados sistemas de IA utilizados pelas forças de segurança, podem ser utilizados ambos os tipos de dados de entrada, pelo que é necessário ter cuidado ao determinar

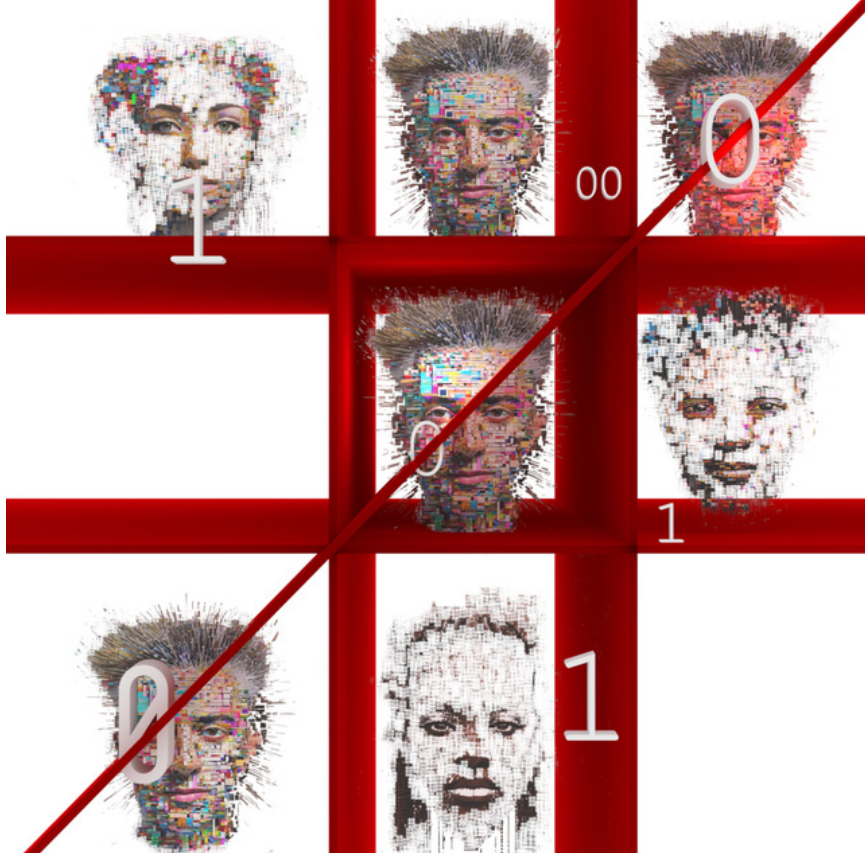
se os direitos de informação aplicáveis são regidos pelo RGPD ou pela DAL. Esta situação torna-se ainda mais complexa quando há empresas privadas envolvidas no desenvolvimento de software ou no tratamento ou controlo de dados relevantes (ver Erdogan 2023). Em caso de dúvida, deve procurar-se aconselhamento jurídico especializado.

Registos das atividades de tratamento

- ▶ Nos termos do artigo 24.º da DAL, as entidades responsáveis pelo tratamento são obrigadas a manter um registo das operações de tratamento, incluindo informações sobre as finalidades do tratamento; as categorias de destinatárias/os a quem os dados pessoais foram ou serão divulgados; e, quando aplicável, a utilização de perfis. Essas informações devem ser disponibilizadas às autoridades de proteção de dados, mediante pedido (para conhecer as possibilidades de colaboração com as APD, consulte [“Cooperação intersetorial”](#)).

Avaliação de impacto sobre a proteção de dados (AIPD)

- ▶ No contexto da aplicação da lei, o artigo 27.º da DAL exige a realização de uma avaliação de impacto sobre a proteção de dados sempre que um tipo de tratamento que recorra a novas tecnologias seja suscetível de implicar um risco elevado para os direitos e liberdades das pessoas singulares. As obrigações relativas à AIPD variarão de Estado-Membro para Estado-Membro, consoante as transposições nacionais. O Grupo de Trabalho sobre Proteção de Dados do Artigo 29.º recomendou que os legisladores nacionais imponham a quem é responsável pelo tratamento a obrigação de realizar uma AIPD no âmbito das decisões automatizadas. No entanto, tal como acontece com as AIDFs, as autoridades responsáveis pela aplicação da lei não são obrigadas a enviar um resumo das mesmas para a base de dados da UE (artigo 49.º, n.º 4, alínea c), do Regulamento sobre a IA).
-



Passo 3

Metodologia para avaliar a informação recebida

O passo 3 apresenta os tipos de discriminação causados pelos sistemas de IA, quer sejam utilizados para a tomada de decisões automatizadas, quer para apoiar os decisores.

A introdução aos conceitos apresenta os tipos de discriminação e aplica-os ao contexto da IA. Os novos conceitos para os organismos para a igualdade podem incluir a discriminação indireta e outras variáveis. Introduce ainda a identificação e o estabelecimento de uma presunção ou de um caso *prima facie* de discriminação.

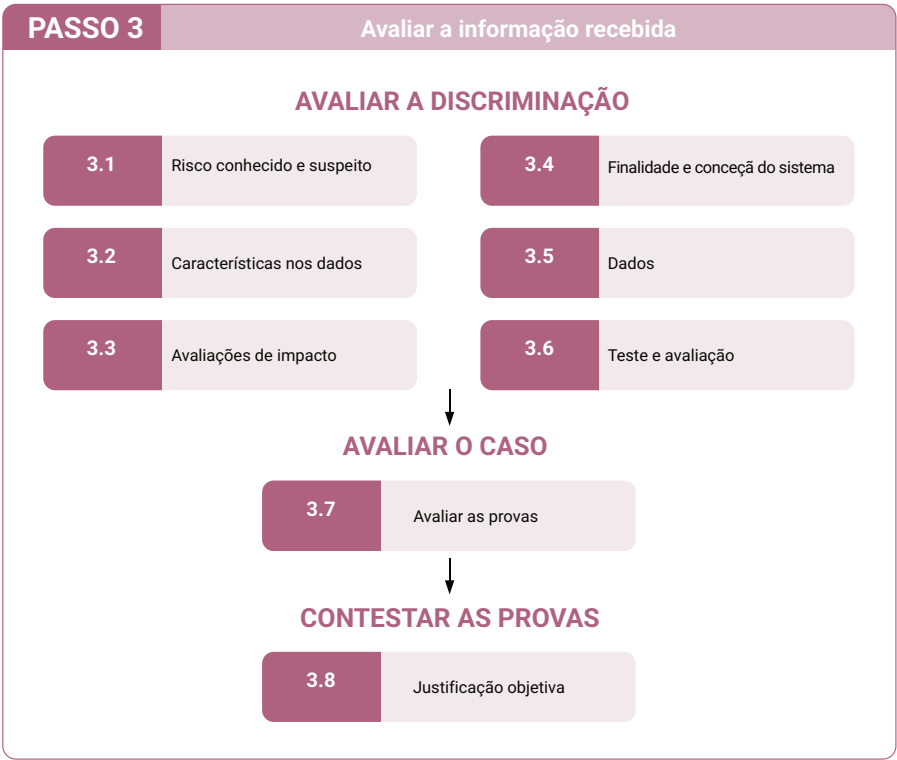
A parte operativa do passo 3 destina-se a ajudar as pessoas responsáveis a avaliar as informações recebidas no passo 2, podendo a ficha de registo de amostra constante do Anexo K ser utilizada em paralelo para registar essas informações. Nos passos 3.2 a 3.6, é fornecida à pessoa responsável uma breve explicação, um conjunto de questões a considerar, possíveis fontes de informação que possam ajudar a responder a essas questões e exemplos de indicadores de discriminação ou de práticas discriminatórias.

O passo 3.7 reúne todas essas conclusões e fornece um guia para avaliar se existe uma presunção de discriminação e, mais importante ainda, o que fazer quando as provas disponíveis são insuficientes ou quando há falta de transparência.

O passo 3.8 fornece orientações sobre como avaliar a probabilidade de a parte inquirida poder refutar ou apresentar uma justificação para qualquer discriminação.

Não se espera que as pessoas responsáveis consigam responder a todas as perguntas ou tenham acesso a todos os documentos ou provas. Em vez disso, esperamos que isso permita às pessoas responsáveis tirar o máximo partido da informação disponível e compreender a sua relevância.

Figura 4. Passo 3 - Avaliar a informação recebida



No passo 2, já deve ter dado início ao processo de recolha da documentação relevante e de outras provas. No passo 3, irá utilizar esses elementos de prova para avaliar se é possível estabelecer uma presunção ou um caso *prima facie* de discriminação e também se existe a probabilidade de a parte inquirida conseguir refutar qualquer presunção de discriminação ou apresentar uma justificação.

Em muitos dos sub-passos do passo 3, os conhecimentos técnicos podem revelar-se úteis. Deve tratar-se de um(a) especialista com bons conhecimentos de estatística, ciência de dados e IA. Os conceitos essenciais ao desenvolvimento de sistemas algorítmicos, tais como dados de treino, rótulos de referência, resultados e entradas, não são explicados em pormenor nesta metodologia; parte-se do princípio de que se tratam de conhecimentos básicos nas áreas da estatística, da ciência de dados e

da IA. Ao contratar um(a) especialista técnica/o, certifique-se de que esta/este compreende tanto a ciência de dados como os princípios da não discriminação.

Em alguns casos, as AFM ou outras agências do Estado-Membro disporão dos conhecimentos técnicos necessários, que poderão ser utilizados pelos organismos para a igualdade (ver “[Cooperação intersetorial](#)”).

Além disso, por vezes, os conhecimentos especializados setoriais podem ser úteis para compreender os padrões das desigualdades históricas e atuais no setor em que o sistema é aplicado. Ao recorrer a conhecimentos especializados setoriais, pode ser útil contar com especialistas com formação em ciências sociais e investigação empírica, uma vez que essa formação ajuda a colmatar a lacuna entre os conhecimentos especializados setoriais e os conhecimentos técnicos. Caso tal não seja possível, poderá ser necessário que o OI realize uma investigação mais aprofundada sobre as desigualdades históricas e de outra natureza, a fim de poder avaliar se estas afetaram o sistema. Por exemplo, a conhecida repressão policial excessiva em determinadas comunidades ou as disparidades de rendimento entre os géneros.

Em cada sub-passo, é feita uma recomendação no sentido de se recorrer a especialistas, sempre que aplicável.

Nota: tal como indicado na metodologia, o novo artigo 77.º, n.º 1, alínea b), relativo ao requisito de cooperação e assistência mútua, pode implicar que a AFM ou outra autoridade ou organismo público abrangido pelo regulamento possa disponibilizar os conhecimentos especializados necessários.

Nota: caso não haja informação suficiente disponível, terá de considerar uma das seguintes opções:

- ▶ o impacto da falta de transparência sobre o ónus da prova (ver “transparência” no passo 3.7; ou
- ▶ solicitar uma avaliação do sistema e a realização de testes pela AFM (ver passo 4.2.1).

Espera-se que possua um nível razoável de conhecimento sobre a legislação em matéria de discriminação para utilizar esta metodologia, mas os conceitos básicos são reiterados no início deste passo, a fim de demonstrar melhor a forma como se relacionam com os sistemas algorítmicos.

Introdução aos conceitos

Tipos de discriminação

Discriminação direta

Uma pessoa é tratada de forma menos favorável em comparação com a forma como outras pessoas numa situação semelhante são ou seriam tratadas, e a razão

para tal reside numa característica específica que possui e que se enquadra num motivo protegido (e, apenas nos casos da UE relativos à idade/deficiência e nos casos de requisitos profissionais genuínos, não há justificação).

Exemplo de discriminação algorítmica direta

Na Finlândia, uma instituição financeira recusou conceder um empréstimo a um homem, tendo recorrido a um sistema de pontuação baseado em dados como o local de residência, o género, a idade e a língua materna para avaliar o risco de incumprimento do empréstimo. Constatou-se que o homem teria obtido aprovação para o empréstimo se fosse mulher ou se o sueco fosse a sua língua materna. Além disso, não foi realizada qualquer avaliação individualizada do risco no que diz respeito à sua probabilidade de incumprimento; o empréstimo foi-lhe simplesmente recusado com base em pressupostos estatísticos relacionados com o seu género e a sua língua materna. O Tribunal Nacional Finlandês para a Não Discriminação e a Igualdade concluiu, em 2018, na sequência de um pedido de investigação apresentado pela Provedoria de Justiça para a Não Discriminação, que se tratava de um caso de discriminação direta.

Leitura complementar

- ▶ Avaliação da solvabilidade, autoridade, discriminação múltipla direta, género, língua, idade, local de residência, motivos financeiros, coima condicional, Tribunal da Finlândia (2018)
-

Discriminação indireta

Uma disposição, critério ou prática (DCP) aparentemente neutra que coloque os membros de um grupo protegido numa situação de desvantagem específica em comparação com outras pessoas numa situação semelhante, a menos que:

- ▶ a DCP seja objetivamente justificada por um objetivo legítimo; e
- ▶ os meios para atingir esse objetivo sejam adequados e necessários.

Ainda não existe uma decisão definitiva sobre se alguns ou todos os processos de tomada de decisão automatizada constituem uma disposição, um critério ou uma prática, mas existe uma opinião firmemente defendida por profissionais de que, quase certamente, assim é: “Na nossa opinião, os processos automatizados de tomada de decisão que utilizam algoritmos constituem, quase certamente, DCP para efeitos de uma queixa por discriminação indireta” (Allen e Masters 2019).

Exemplo de discriminação algorítmica indireta (caso Deliveroo)

Verificou-se que o sistema algorítmico de “reserva self-service” da Deliveroo, utilizado para a atribuição de turnos de trabalho, era indiretamente discriminatório, nomeadamente com base nas convicções (participação em ações coletivas, como greves) e na deficiência. Ao basear-se em estatísticas de participação e fiabilidade - critérios aparentemente neutros -, o sistema, na prática, prejudicava as condutoras e condutores que se ausentavam do trabalho por motivos legítimos, tais como greves, doença ou responsabilidades de prestação de cuida-

dos, reduzindo as suas pontuações e, consequentemente, o seu acesso a futuras oportunidades de trabalho.

A “cegueira” das estatísticas utilizadas, ou seja, o facto de o sistema não ter em conta os motivos de indisponibilidade relacionados com motivos protegidos, fez com que situações diferentes fossem tratadas de forma semelhante, o que resultou num impacto desproporcionado nos grupos protegidos.

Leitura complementar

- *Filcams Cgil Bologna e outros contra Deliveroo Italia S.R.* (2020)
 - *Purificato* (2021)
-

Discriminação múltipla

A discriminação pode ocorrer com base em mais do que um motivo. Por exemplo, uma pessoa pode ser vítima de discriminação com base na raça e também com base no género ou na deficiência. Existem vários termos diferentes utilizados para descrever a discriminação que ocorre com base em mais do que um motivo. Alguns exemplos de termos utilizados são “discriminação múltipla”, “discriminação cumulativa”, “discriminação composta”, “discriminação combinada” e “discriminação interseccional” (Fredman 2016). Todas estas expressões têm significados ligeiramente diferentes. No âmbito desta metodologia, é importante reconhecer que a base da discriminação pode ser multifacetada (Xenidis 2021).

Discriminação interseccional

“Em essência... a interseccionalidade é uma forma de pensar a identidade e a sua relação com o poder” (Crenshaw 2015).

A discriminação interseccional difere de outras formas de discriminação múltipla, na medida em que não se trata simplesmente da soma de discriminações baseadas em motivos isolados, mas sim de características pessoais diferentes que se sobrepõem e não podem ser separadas. As estruturas sociais, económicas, culturais e institucionais interligam-se e formam um sistema complexo que cria (e perpetua) a desigualdade (Crenshaw 1991). Por exemplo, categorias sociais como a idade e o género podem sobrepor-se, criando vantagens ou desvantagens, dependendo das circunstâncias. A desigualdade pode variar consoante as circunstâncias e os factos e, por vezes, depende do momento e do local. Por exemplo, uma mulher não migrante pode ser “menos” igual do que um homem, mas mais igual do que uma mulher migrante. As desigualdades sociais também podem moldar as relações de poder. Estas estruturas de desigualdade interligadas refletem-se nos dados do mundo real utilizados para conceber, construir e testar sistemas algorítmicos. Além disso, as abordagens de aprendizagem automática utilizadas para criar sistemas de IA são capazes de identificar padrões de interação que não são conhecidos ou que não são evidentes a partir de análises básicas dos dados. Dessa forma, os sistemas algorítmicos podem conduzir à discriminação interseccional (Xenidis 2021). Embora a discriminação interseccional tenha sido rejeitada pelo TJUE no processo Parris (C-443/17), algumas comentadoras e comentadores sugerem que esta ques-

tão deve ser reexaminada, nomeadamente à luz do crescente reconhecimento do fenómeno no direito da União, como a Diretiva relativa à transparência remuneratória 2023/970/CE e a Diretiva (UE) 2024/1385 relativa ao combate à violência contra as mulheres e à violência doméstica (Howard 2024).

Discriminação por proxy

A discriminação baseada na utilização de características, conhecidas como “proxies”, que não estão, por si só, associadas a nenhum dos motivos de discriminação explicitamente proibidos (ver “[Características protegidas](#)”), mas que estão correlacionadas com um motivo protegido, é designada por “discriminação por proxy”. Embora a legislação da UE não reconheça nem faça referência explícita à discriminação por proxy, trata-se de um conceito teórico que ajuda a compreender como a discriminação algorítmica pode surgir.

- ▶ A discriminação por proxy pode constituir discriminação direta se existir uma ligação indissociável entre as características escolhidas - neutras - e as características explicitamente protegidas (gravidez e género, por exemplo: *Dekker contra Stichting Vormingscentrum voor Jong Volwassenen (VJV-Centrum) Plus*, 1990; *Dita Danosa contra LKB Līzings SIA*, 2010; *Andersen contra Region Syd-danmark*, 2010; *VL contra Szpital Kliniczny im. dra J. Babińskiego SPZOZ contra Krakowie*, 2021).
- ▶ Em alternativa, a discriminação por proxy pode constituir discriminação indireta se a disposição, o critério ou a prática, incluindo os proxies, afetarem de forma desproporcionada as pessoas com características protegidas (para uma explicação prática deste aspeto, ver o processo *Jyske Finans contra Lige-behandlingsnævnet*, 2017 (C-668/15)).

Caso importante: *Dekker contra Stichting Vormingscentrum* (1990)

Uma entidade empregadora violou diretamente o princípio da igualdade de tratamento (Diretiva 76/207/CE do Conselho) relativo à concretização do princípio da igualdade de tratamento entre homens e mulheres no que se refere ao acesso ao emprego, à formação e promoção profissionais e às condições de trabalho, ao recusar-se a celebrar um contrato de trabalho com uma candidata adequada para o cargo, quando essa recusa se baseou nas possíveis consequências negativas decorrentes da contratação de uma mulher grávida, uma vez que o regime nacional de doença equiparava a gravidez a uma doença. O tribunal reconheceu que apenas às mulheres pode ser recusado o emprego com base na gravidez, o que constitui discriminação direta com base no sexo.

Variáveis proxy

No contexto da legislação em matéria de não discriminação, os termos “proxies” ou “variáveis proxy” referem-se a características ou combinações destas que, por si só, não constam da lista dos motivos de discriminação explicitamente proibidos ao abrigo do quadro jurídico relevante, mas que estão correlacionadas com

esses motivos de tal forma que a sua utilização pode conduzir a uma discriminação ilegal. Um exemplo disso é o código postal: um código postal não é, por si só, discriminatório; no entanto, se numa determinada zona viverem muitas pessoas migrantes ou pessoas de uma determinada origem étnica, esse código pode funcionar como um proxy de um motivo de discriminação proibido, nomeadamente a origem étnica.

Os proxies podem ser identificados através da sobre-representação: se as pessoas com um determinado atributo protegido estiverem sobre-representadas num grupo, é provável que os identificadores desse grupo sejam proxies. Assim, no exemplo acima, uma vez que pessoas de diferentes origens estão sobre-representadas em determinados bairros, um código postal pode ser considerado um proxy.

Quando um proxy é utilizado como dado de entrada num sistema algorítmico, tal pode indicar uma potencial discriminação. Note-se que, dependendo do tipo de proxy, a utilização de proxies pode indicar tanto discriminação direta como indireta (Weerts et al. 2024). Sabe-se, através da investigação sobre o tema e da jurisprudência relevante, que certas características constituem proxies de características protegidas. Os proxies podem também ser identificados através da compreensão e análise do contexto específico em que um sistema algorítmico é aplicado, tendo em conta as desigualdades históricas existentes e os dados demográficos.

Para obter mais informações e exemplos dos diferentes tipos de proxies, consulte o [Anexo E](#).

No caso *Chez* (C-83/14), foi imposta uma medida coletiva (a instalação de contadores de eletricidade num bairro “Roma” a uma altura compreendida entre seis e sete metros, em vez de a menos de dois metros, como noutros bairros) a um bairro habitado principalmente, mas não exclusivamente, por pessoas de origem Roma. Se se comprovasse que essa medida foi introduzida e/ou mantida por motivos relacionados com a origem étnica comum à maioria das pessoas habitantes do distrito em causa, tal seria considerado discriminação direta ou indireta, nomeadamente contra as pessoas habitantes desse distrito de origem não Roma. Cabia ao tribunal nacional decidir esta questão, tendo em conta todas as circunstâncias relevantes do caso e as regras relativas à inversão do ónus da prova previstas no n.º 1 do artigo 8.º da Diretiva 2000/43.

Exemplo de algoritmo: verificação de bolsa de estudos universitária

Este exemplo deverá ajudar a explicar como funcionam os proxies. Neste caso, “viver perto dos pais” e “frequentar o ensino profissional” serviram como proxies de “origem migrante não europeia”.

A Agência Executiva para a Educação dos Países Baixos (DUO) realiza verificações para garantir que as bolsas de estudo atribuídas são concedidas de forma adequada. Este processo é conhecido como “verificação de bolsa universitária” (abreviado em neerlandês para CUB). Surgiram suspeitas de que o processo CUB, agora extinto, fosse discriminatório em relação a estudantes de origem migrante. Esta

suspeita baseava-se nos processos de recurso interpostos por estudantes que se verificou terem recebido bolsas indevidamente, nos quais as advogadas e advogados constataram que as/os respetivas/os clientes eram, na sua esmagadora maioria, de origem migrante. A investigação revelou que, neste processo, foi utilizado um sistema de pontuação do risco de fraude para dar prioridade às investigações sobre a utilização (i)legítima das bolsas.

A Algorithm Audit realizou uma análise do sistema algorítmico, das diferenças de tratamento nos diferentes passos do processo CUB e investigou se os dados introduzidos no sistema poderiam ser considerados proxies.⁴⁵ Verificou-se que o sistema utilizava três dados: a idade das/dos estudantes, o nível de escolaridade e a distância entre a sua morada e a dos pais. A nacionalidade, o contexto migratório ou qualquer outra informação relativa à raça ou etnia não foram utilizados no sistema de avaliação de risco de fraude.

As principais conclusões da Algorithm Audit foram as seguintes:

- ▶ o processo CUB, no seu conjunto, conduziu a um tratamento desigual de estudantes de origem migrante não europeia;
- ▶ o perfil de risco atribuiu pontuações de risco mais elevadas a estudantes com antecedentes migratórios; estudantes com antecedentes migratórios não europeus tinham duas vezes mais probabilidades de serem classificadas/os numa categoria de risco elevado do que estudantes de origem neerlandesa;
- ▶ a seleção manual posterior de estudantes para o grupo de controlo reforçou a sobrerrepresentação, em vez de a reduzir. As/Os estudantes de origem não europeia tinham 6,2 vezes mais probabilidades de serem selecionadas/os para uma verificação, que envolvia uma visita domiciliar invasiva, do que as/os estudantes de origem neerlandesa.

Um tribunal holandês concluiu que esta prática não se justificava objetivamente e constituía discriminação indireta (Rechtbank Overijssel 2024).

Análises detalhadas revelaram que o sistema de pontuação de risco atribuía pontuações de risco mais elevadas a estudantes dos níveis de ensino mais baixos (ensino profissional) e a estudantes que viviam mais perto dos pais. Verificou-se que ambas as variáveis apresentam uma correlação (forte) com o contexto migratório, sendo, por isso, proxies desse contexto (ver os gráficos abaixo).

45 A Algorithm Audit obteve acesso total tanto ao algoritmo como aos dados internos da DUO. Devido ao Regulamento Geral sobre a Proteção de Dados (RGPD), a DUO não recolhe nem trata informações sobre a origem de estudantes para efeitos do processo CUB. Para realizar estas análises, a DUO e a Algorithm Audit colaboraram com o instituto nacional de estatística dos Países Baixos (Estatísticas dos Países Baixos ou CBS). O CBS forneceu estatísticas agregadas sobre o país de nascimento e o país de origem, com base nas populações definidas pela Algorithm Audit para cada um dos passos do processo (categoria de risco, seleção para controlo, controlo do resultado, procedimento de recurso, recurso do resultado) e variáveis de entrada (nível de escolaridade, idade, distância em relação aos pais).

Gráfico 1: Distribuição de estudantes com antecedentes migratórios (não) europeus e de estudantes de origem neerlandesa, por tipo de ensino, na população beneficiária de bolsas de estudo universitárias

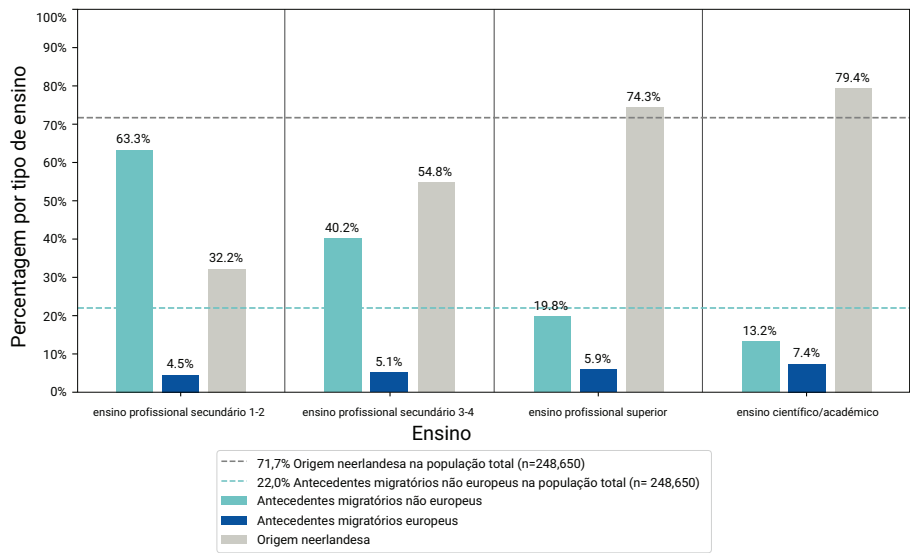
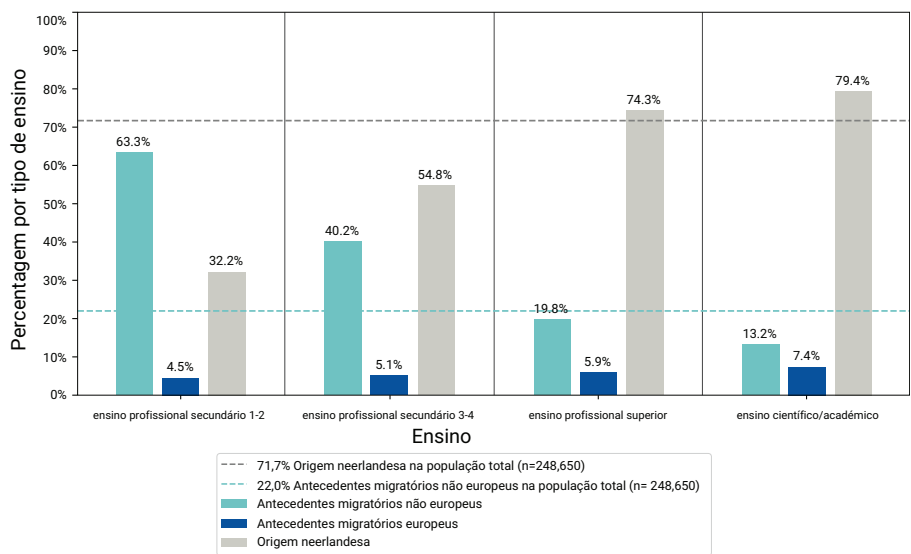


Gráfico 2: Distribuição de estudantes com antecedentes migratórios (não) europeus e de estudantes de origem neerlandesa, por categoria de distância, na população beneficiária de bolsas de estudo universitárias



Fonte do gráfico: Algorithm Audit

Para uma explicação completa, consulte a Algorithm Audit 2024a e 2024b.

Comparadores

Um comparador é uma pessoa que se encontra numa situação semelhante à da pessoa queixosa, mas que não partilha a característica protegida que se presume ser o motivo da discriminação.

Nota: é possível que dois grupos de pessoas sejam considerados numa situação análoga para efeitos de uma queixa, mas não para efeitos de outra. Por conseguinte, é sempre importante avaliar o elemento de comparação à luz do objetivo da medida contestada (Conselho da Europa e Agência dos Direitos Fundamentais da União Europeia 2018: 44-49).

A escolha do comparador adequado será importante na avaliação das evidências em sistemas algorítmicos, em particular ao analisar o objetivo do sistema, as medidas de treino, teste e validação, bem como os próprios testes e avaliações. Em particular, poderá ser necessário avaliar se foram utilizados dados relativos a características protegidas para treinar o sistema algorítmico e que opções foram adotadas durante os testes do sistema. Este assunto é abordado com mais pormenor nas secções 3.3, 3.5 e 3.6.

Estabelecimento de uma presunção de discriminação

De acordo com as diretivas em matéria de não discriminação, quando as pessoas que se consideram lesadas pelo facto de o princípio da igualdade de tratamento não lhes ter sido aplicado apresentarem perante um tribunal ou outra autoridade competente factos a partir dos quais se possa presumir que houve discriminação direta ou indireta, cabe à parte inquirida provar que não houve violação do princípio da igualdade de tratamento.⁴⁶ Ver também o passo 3.8.

Isto significa que a pessoa queixosa deve apresentar provas suficientes para dar origem a uma presunção de discriminação.

Depois disso, o ónus da prova recai sobre a parte inquirida. Na prática, os tribunais nacionais dispõem de uma margem de apreciação para determinar quando as provas apresentadas pela pessoa queixosa são suficientes para transferir o ónus da prova para a parte inquirida.⁴⁷

As provas podem incluir dados estatísticos,⁴⁸ documentos escritos - desde que o seu conteúdo esteja relacionado com a discriminação ou se refira ao caso específico da parte requerente - e relatórios e análises provenientes de fontes relevantes (ver dados recolhidos no [passo 2](#)), testes de situação (ver no [passo 3.6](#)), avaliações baseadas no senso comum, depoimentos de testemunhas e inferências extraídas de provas circunstanciais. O TJUE salienta a importância de ter em conta “todas as circunstâncias que envolvem a prática controvertida ” (C-83/14 CHEZ, parágrafos 80-84). Assim, tanto os dados estatísticos como os qualitativos podem ser utiliza-

46 Diretiva 2000/78/CE, artigo 10.º; Diretiva 2006/54/CE, artigo 19.º; Diretiva 2000/43/CE, artigo 8.º.

47 Na prática, isto será frequentemente diferente no caso da discriminação direta e da discriminação indireta. Para leitura adicional, consulte Farkas e O'Farrell (2015).

48 Para mais informações sobre as estatísticas enquanto elementos de prova, consulte abaixo a secção “[Abordagem aos dados estatísticos](#)”.

dos para estabelecer uma presunção de discriminação, e há quem defenda que, na verdade, ambos devem ser utilizados.

O que são os “dados relativos à igualdade”?

No contexto da metodologia, referimo-nos tanto aos dados quantitativos (incluindo os estatísticos) como aos qualitativos como “dados relativos à igualdade”, com base na seguinte definição apresentada nas “Orientações sobre a melhoria da recolha e utilização de dados relativos à igualdade” (Comissão Europeia, 2021):

qualquer elemento de informação útil para efeitos de descrição e análise do estado da igualdade. As informações podem ser de natureza quantitativa ou qualitativa. Podem incluir dados agregados que reflitam desigualdades ou as suas causas ou efeitos na sociedade. Por vezes, os dados recolhidos principalmente por outros motivos que não para efeitos relacionados com a igualdade podem ser utilizados para a produção de dados relativos à igualdade. (Comissão Europeia 2021: 8)

Os dados relativos à igualdade são utilizados, entre outras coisas, para “fornecer dados concretos fiáveis no âmbito de processos administrativos ou judiciais relativamente a discriminação, através de dados que apontam para discriminação direta ou indireta; e para apoiar a argumentação e a sensibilização no domínio da igualdade e da não discriminação” (Comissão Europeia 2021: 9).

Leitura complementar

- ▶ “Manual sobre a identificação e utilização de dados relativos à igualdade no tratamento de processos judiciais” (Illeva 2024);
- ▶ “Manual de litígio estratégico” (Equinet 2017);
- ▶ “Manual: inteligência artificial, tomada de decisões judiciais e direitos fundamentais” (Projeto JuLIA 2024).

Como utilizar o passo 3

As secções que se seguem apresentam as questões orientadoras que podem ajudar os organismos para a igualdade a determinar se existe um caso *prima facie* de discriminação. O objetivo é mostrar em que parte da informação recolhida no passo 2 é possível encontrar os elementos de prova relevantes, o que procurar nesses elementos e como utilizá-los para provar a discriminação.

Cada secção desta parte segue a seguinte estrutura básica.

- ▶ Uma explicação sobre o que deve ser avaliado pelo OI.
- ▶ Questões a ter em conta ao avaliar a informação.
- ▶ Possíveis fontes de informação.
- ▶ Indicadores de discriminação.

As secções 3.7 e 3.8 fornecem, em seguida, um quadro para avaliar se as provas recolhidas são suficientes para sustentar um caso *prima facie* de discriminação envolvendo um sistema de IA ou algorítmico (3.7. [Avaliar se as provas são suficientes](#)

para fundamentar um caso *prima facie* de discriminação envolvendo um sistema de IA ou algorítmico) e para avaliar a probabilidade de a parte inquirida poder refutá-las ou apresentar uma justificação para qualquer discriminação (3.8. A parte inquirida pode demonstrar que a diferença?). Isto ajudará a determinar se devem ser tomadas medidas contra a parte inquirida. Haverá, inevitavelmente, alguma sobreposição no processo e na análise das provas entre estas tarefas.

É extremamente improvável que um OI consiga aceder a toda a informação ou responder a todas as perguntas nesta etapa. Pelo contrário, estas destinam-se a servir de orientação quanto aos tipos de informação que poderão estar disponíveis e à forma como estes podem ser avaliados, tanto a nível individual como, posteriormente, a nível coletivo.

No Anexo K é apresentado um modelo de ficha de registo, que se destina a servir de apoio e pode ser adaptado às necessidades específicas de cada OI.

Leitura complementar

Alguns dos conceitos do passo 3 serão novos ou desconhecidos. Os recursos abaixo explicam estes temas com mais pormenor.

- Wachter, Mittelstadt, and Russell, 2020, Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, Volume 41, julho 2021.
- Mittelstadt, 2024, How to use the Artificial Intelligence Act to investigate bias and discrimination: A guide for equality bodies, *Equinet*.

3.1. Quais são os riscos conhecidos ou suspeitos de discriminação?

A utilização de sistemas algorítmicos em determinados contextos pode acarretar um risco inerente de práticas discriminatórias. Quando já se tenha demonstrado a existência de discriminação algorítmica num caso de utilização semelhante num setor semelhante, tal poderá indicar um risco mais alargado de discriminação que também se aplica ao caso em análise. Por exemplo, quando se comprova que o reconhecimento facial utilizado no âmbito policial é discriminatório, é provável que o reconhecimento facial utilizado para outros fins também o seja.

3.1.1. O tipo de sistema algorítmico ou o domínio em que é aplicado são explicitamente referidos no Regulamento sobre a IA no que diz respeito aos seus riscos de discriminação?

O Regulamento sobre a IA refere-se tanto a “setores” como a “casos de utilização” no âmbito desses setores.

Quando os sistemas algorítmicos são utilizados em setores onde existem desigualdades históricas e/ou onde se verificou que a discriminação ocorre com frequência, tal deve suscitar uma maior suspeita de discriminação. Os sistemas algorítmicos baseiam-se em dados do mundo real. As desigualdades existentes e os enviesamentos humanos refletem-se nos dados e, por isso, surgem frequentemente e podem ser exacerbados no sistema algorítmico.

Enviesamentos nos dados históricos: exemplo de algoritmo, ferramenta de recrutamento da Amazon

A Amazon desenvolveu uma ferramenta de recrutamento baseada em IA, treinada com currículos históricos que refletiam um conjunto de candidatos predominantemente masculino. Como resultado, o sistema “aprendeu por si próprio que os candidatos do sexo masculino eram preferíveis”. Embora o sistema não utilizasse explicitamente o género como critério de seleção, baseava-se em dados proxy correlacionados com o facto de se ser mulher - tais como a palavra “feminino” (“capitã do clube de xadrez feminino”, por exemplo) ou diplomas de faculdades femininas - e rebaixava sistematicamente as candidaturas de mulheres (Dastin 2018).

Muitos dos casos de utilização de risco elevado previstos no Regulamento sobre a IA foram classificados pela UE como pertencentes à categoria de risco elevado precisamente devido ao risco de discriminação. Os Considerandos 54 e 56 a 60 do Regulamento sobre a IA referem explicitamente o risco de discriminação, a perpetuação de desigualdades históricas e vulnerabilidades específicas. Mesmo que um sistema não seja tecnologicamente complexo e/ou não se trate de IA, a utilização de sistemas algorítmicos (baseados em regras) para estes casos de utilização acarreta um risco semelhante de discriminação. O [Anexo I](#) descreve domínios e casos de utilização de IA de risco elevado.

Um caso de utilização explicitamente referido no Regulamento sobre a IA justifica um nível adicional de análise. Além disso, podem estar disponíveis dados relativos à igualdade, tanto qualitativos como quantitativos, para estes casos, os quais podem frequentemente ser encontrados na jurisprudência, em trabalhos académicos, em OSC ou em relatórios governamentais. Ver também a secção [2.1.2. Informação disponível ao público](#), “Jurisprudência existente”, e “Outras fontes”.

Nota: se o sistema for um sistema de IA de risco elevado e estiver registado na base de dados da UE, incluindo na secção B,⁴⁹ então, por definição, é explicitamente referido no Regulamento sobre a IA e, por conseguinte, representa potencialmente um risco elevado de discriminação.

⁴⁹ Quando um sistema consta da secção B da base de dados da UE, isso significa que foi autoavaliado por uma entidade prestadora como sendo utilizado num setor de risco elevado, mas que não representa um risco com base num conjunto restrito de exceções (ver Regulamento sobre a IA, artigo 6.º, n.º 3). Embora seja muito provável que a documentação exigida pelo Regulamento sobre a IA não esteja disponível, este sistema é aplicado num domínio explicitamente referido no Regulamento sobre a IA devido aos seus riscos de discriminação.

Questões a ter em conta

- ▶ O sistema algorítmico constitui um “tipo” de tecnologia conhecido por criar um risco de discriminação, como a definição de perfis (artigo 6.º, n.º 3, e Considerando 53), a análise preditiva de riscos (Considerando 42) ou a biometria e o reconhecimento de emoções (Anexo III, n.º 1, Considerandos 44 e 54)?
- ▶ A decisão ou o tratamento a que foi submetido estava relacionado com algum dos seguintes setores?
 - Educação e formação profissional (Anexo III, n.º 3, Considerando 56).
 - Emprego, gestão de trabalhadoras e trabalhadores e acesso ao emprego por conta própria (Anexo III, n.º 4, Considerando 57).
 - Acesso a serviços e prestações públicos essenciais, bem como o usufruto dos mesmos (segurança social) (Anexo III, n.º 5, alínea a)).
 - Classificação de crédito (Anexo III, n.º 5, alínea b), Considerando 58).
 - Seguros de vida e de saúde (Anexo III, n.º 5, alínea c), Considerando 58).
 - Acesso aos serviços de saúde e condições de elegibilidade para os mesmos (Anexo III, n.º 5, alínea a), Considerando 58).
 - Aplicação da lei (Anexo III, n.º 6, Considerando 59).
 - Migração, asilo e controlo de fronteiras (Anexo III, n.º 7, Considerando 60).
 - Administração da justiça (Anexo III, n.º 8, alínea a), Considerando 61).
 - Gestão dos processos democráticos (Anexo III, n.º 8, alínea b), Considerando 61).
- ▶ Se o caso estiver relacionado com um dos setores acima referidos, esse caso abrange um caso de utilização enumerado na secção pertinente do Anexo III (incluindo no considerando relevante)?

Possíveis fontes de informação para avaliar um risco de discriminação geralmente reconhecido

Regulamento sobre a IA da UE

- ▶ Artigo 6.º, Anexo III e considerandos – estes descrevem os tipos de IA de risco elevado.
- ▶ Artigo 5.º – este artigo descreve as práticas proibidas em matéria de IA e os considerandos 28 a 45.

Outros

- ▶ Orientações da Comissão sobre práticas proibidas no domínio da inteligência artificial (IA), tal como definidas no Regulamento sobre a IA.
- ▶ Em breve: Orientações da Comissão sobre a classificação de sistemas de IA de risco elevado e os requisitos conexos.⁵⁰

50 À data da elaboração desta metodologia, a Comissão publicou um projeto de orientações para consulta: [A Comissão solicita comentários sobre o projeto de orientações para a classificação de sistemas de inteligência artificial de risco elevado](#).

Indicadores de risco de discriminação

Se algum destes indicadores se verificar, tal, por si só, não constitui prova de discriminação. No entanto, estes indicadores podem apontar para um sistema com risco de discriminação:

- ▶ se o sistema for um sistema de IA de risco elevado abrangido pelas secções A ou C;
- ▶ para sistemas de risco não elevado:
 - se o sistema se destinar a ser utilizado num setor em que exista um risco identificado de discriminação (Anexo III ou considerandos); e/ou
 - se se tratar de um tipo de tecnologia em que exista um risco conhecido de discriminação.

Registe se o sistema é ou não um sistema de risco elevado ou se se destina a ser utilizado em algum dos setores ou domínios identificados como apresentando um risco de discriminação no Regulamento sobre a IA.

Suspeita de classificação incorreta ao abrigo do Regulamento sobre a IA

Se um organismo para a igualdade suspeitar que um sistema tenha sido indevidamente autoavaliado como não sendo um sistema de IA de risco elevado ou não tenha sido reconhecido como uma prática de IA proibida (ver “sistemas de IA suspeitos de serem proibidos” no passo 1.4), deve informar a AFM competente, independentemente de se poder comprovar a existência de um caso de discriminação (ver também o passo 4).

3.1.2. Foi identificado algum risco conhecido de discriminação neste setor ou nesta tecnologia pelas autoridades nacionais ou regionais, pelas OSC nacionais ou internacionais ou pelas estruturas de direitos humanos?

Os relatórios elaborados por instituições de provedoria, pela sociedade civil e pelo meio académico, bem como a jurisprudência existente, podem revelar um padrão de resultados desiguais relativamente a um motivo de proteção específico.

Utilize as informações recolhidas no passo 2 para avaliar se este sistema, ou este tipo de sistema, já é conhecido ou se há suspeitas de que produza um resultado discriminatório. Qualquer informação relevante poderá também ajudá-lo a realizar os próximos passos.

Neste passo, seria útil contar com conhecimentos especializados no setor.

Possíveis fontes de informação para avaliar um risco de discriminação geralmente reconhecido

- ▶ Monitorização, investigação ou estudos do OI

- ▶ Relatórios de OSC nacionais e internacionais
- ▶ Jurisprudência existente
- ▶ Pesquisas na Internet
- ▶ Especialistas

Indicadores de discriminação

- ▶ Foi identificada, ou existe a suspeita por parte de entidades terceiras, de discriminação na utilização específica dos sistemas algorítmicos por parte da parte inquirida, abrangida pelo presente caso.
- ▶ Foi identificada, ou existe a suspeita por parte de entidades terceiras, de discriminação em utilizações de sistemas algorítmicos muito semelhantes às abrangidas pelo presente caso, o que indica um potencial padrão de discriminação.

Registe o domínio em que existe um risco conhecido, a tecnologia utilizada e quaisquer outras informações e provas relevantes. Por exemplo:

Setor: aplicação da lei

Tecnologia: reconhecimento facial, biometria

Fontes de informação: Investigação realizada por uma ONG/instituição académica, artigo 5.º do Regulamento sobre a IA (sistemas proibidos), artigo 6.º (risco elevado) e Anexo III.

Casos de utilização que devem ser considerados de risco elevado ou proibidos ao abrigo do Regulamento sobre a IA

Se o padrão identificado de resultados discriminatórios para um caso de utilização algorítmica específico for evidente e consistente, mas não constar das listas do Anexo III, os OIs devem considerar a possibilidade de comunicar esse caso de utilização à Comissão Europeia, para que seja adicionado à lista nos termos do artigo 7.º (ver passo 4.3.2. [Sistema utilizado num setor de risco elevado cujo caso de utilização não está registado no Anexo III do Regulamento sobre a IA](#)).

Se o OI considerar que uma prática de IA contradiz fundamentalmente os valores da União em matéria de respeito pela dignidade humana, liberdade, igualdade, democracia e Estado de direito, bem como os direitos fundamentais consagrados na Carta, mas essa prática não for proibida nem considerada de risco elevado ao abrigo do Regulamento sobre a IA (ver passo 4.3.2.).

3.2. Existem características protegidas ou proxies conhecidos nos dados de entrada ou nos conjuntos de dados?

Os dados de entrada de um sistema algorítmico definem a saída e, consequentemente, o resultado. Por conseguinte, se uma característica protegida (ver “[Características protegidas](#)”) ou um proxy (ver “[discriminação por proxy](#)”) for utilizado como dado de entrada no sistema algorítmico, deve suspeitar-se da existência de discriminação.

Neste passo, os conhecimentos especializados setoriais revelam-se úteis.

Questões a ter em conta

- ▶ São tratados dados pessoais que revelem características protegidas ou proxies de características protegidas?
- ▶ É feita referência a características protegidas ou a proxies conhecidos (ver [Anexo E](#)) em algum dos documentos relevantes?
- ▶ As características protegidas ou os proxies conhecidos são mencionados diretamente como dados de entrada do sistema (seja na fase de treino, de teste ou durante a utilização)? Isto poderia ser formulado da seguinte forma: “X, Y e Z são utilizados para prever/calcular”.
- ▶ Um dos dados de entrada do sistema - ou uma combinação destes - poderá constituir um proxy provável de um atributo protegido, com base no conhecimento setorial? Para responder a esta questão, poderá ser necessário consultar estatísticas nacionais ou especialistas setoriais com conhecimentos sobre a forma como as desigualdades se manifestam e se relacionam num determinado setor. Por exemplo:
 - nos países onde existe uma dedução fiscal para despesas relacionadas com cuidados de saúde, é provável que as pessoas com deficiência estejam sobrerrepresentadas entre aquelas que recorrem a essa dedução. Assim, o recurso a esta dedução constitui um proxy provável de incapacidade;
 - em muitos países, as pessoas de origem migrante estão sub-representadas entre as pessoas titulares de diplomas universitários; por isso, o nível de escolaridade é um proxy provável da origem racial ou étnica.
- ▶ Algum dos proxies mencionados está indissociavelmente ligado a uma característica protegida? Ver [Anexo E - Proxies](#).
- ▶ A suspeita de que uma (seleção de) entrada(s) seja(m) um proxy pode ser comprovada por provas? Por exemplo, existem estatísticas disponibilizadas por um instituto nacional de estatística ou por investigação académica que demonstrem uma sobrerrepresentação ou sub-representação de um grupo com uma característica protegida num subgrupo específico dos dados de entrada? Por exemplo:
 - se o nível de escolaridade for um dos fatores que se suspeita servir de proxy da origem étnica, existem estatísticas que demonstrem que as pessoas com antecedentes migratórios estão sobrerrepresentadas no grupo com diplomas de formação profissional?

Nota: a recolha destas provas poderá exigir a colaboração de especialistas com experiência em análise de dados.

- ▶ O sistema foi treinado, testado ou validado com base em informações que contenham características protegidas? (Ver passo 3.5.)

Possíveis fontes de informação para compreender os dados de entrada do sistema

Pessoa queixosa

- ▶ Lista das informações fornecidas pela pessoa queixosa à parte inquirida.
- ▶ Explicações, justificações e fundamentação fornecidas à pessoa queixosa relativamente ao tratamento.

RGPD, artigos 13.º e 14.º: informações prestadas à pessoa titular dos dados

- ▶ Informações prestadas à pessoa titular dos dados (pessoa queixosa) no momento em que forneceu os dados (artigo 13.º do RGPD).
- ▶ Informações fornecidas por quem é responsável pelo tratamento, nos casos em que os dados pessoais não tenham sido obtidos diretamente junto da pessoa titular dos dados (artigo 14.º do RGPD).
- ▶ A lógica subjacente aos casos de tomada de decisão automatizada (artigo 13.º, n.º 2, alínea f), e artigo 14.º, n.º 2, alínea g)).

RGPD, resposta ao PAPTD

- ▶ As categorias de dados pessoais em causa (artigo 15.º, n.º 1, alínea b)): quem é responsável pelo tratamento deve fornecer uma cópia dos dados pessoais objeto de tratamento. Isto pode incluir dados fornecidos por entidades terceiras (artigo 14.º do RGPD).
- ▶ Potencialmente: variáveis ou parâmetros de entrada utilizados na tomada de decisões e a forma como foram obtidos (por exemplo, através de informação estatística), bem como o respetivo peso a nível agregado (parecer do AG Pikamäe no processo SCHUFA Holding, 2023, parágrafo 58).

Regulamento sobre a IA da UE, artigo 86.º: pedido de explicações

- ▶ Dados de entrada e elementos principais da decisão.

Disponível ao público

- ▶ Base de dados da UE para sistemas de IA de risco elevado: secção A – sistemas de IA de risco elevado – uma descrição da informação utilizada pelo sistema (dados, entradas) e da sua lógica de funcionamento.
- ▶ Perguntas frequentes na plataforma.
- ▶ Comunicações das empresas cotadas em bolsa.

Parte inquirida

Da entidade prestadora:

Regulamento sobre a IA da UE, artigo 11.º e Anexo IV: documentação técnica

- ▶ Anexo IV, n.º 2, alínea b): a lógica geral do sistema de IA e dos algoritmos, a fundamentação e os pressupostos utilizados, nomeadamente no que diz respeito às pessoas ou grupos de pessoas a quem o sistema se destina; as principais opções de classificação; o objetivo para o qual o sistema foi concebido e a relevância dos diferentes parâmetros; a descrição do resultado esperado e da qualidade do resultado do sistema.
- ▶ Anexo IV, n.º 2, alínea d): uma descrição geral dos conjuntos de dados, informações sobre a sua proveniência, âmbito e principais características.

De quem é responsável pela implantação:

Regulamento sobre a IA da UE, artigo 27.º: avaliação de impacto sobre os direitos fundamentais

- ▶ As categorias de pessoas singulares e grupos suscetíveis de serem afetados pelo sistema algorítmico (artigo 27.º, n.º 1, alínea c), do Regulamento sobre a IA da UE).

Outros

- ▶ Cláusulas contratuais.
- ▶ Pesquisa documental, jurisprudência existente e estatísticas sobre a sobre-representação e a sub-representação no domínio em questão.

Indicadores de discriminação

- ▶ Utilização direta de características protegidas no sistema.
- ▶ Utilização de proxies que estão indissociavelmente ligados a um atributo protegido no sistema.
- ▶ Utilização de proxies conhecidos no sistema.
- ▶ Utilização de características protegidas ou proxies para treinar, testar ou validar o sistema.

Tudo o que foi referido acima requer provas de que esses fatores conduzem a um tratamento desigual. Os indicadores *a* e *b* são indicativos de discriminação direta. Os indicadores *c* e *d* são indicativos de discriminação indireta.

- ▶ Registe a utilização direta das características protegidas. Onde é que são utilizadas e como?
- ▶ Registe qualquer utilização de características protegidas ou proxies que tenham, ou se presuma que tenham, impacto no resultado do sistema. Analisar a conceção técnica do sistema e a influência dos proxies (presumíveis)

nos resultados do sistema. O facto de se utilizar um proxy como dado de entrada não é, por si só, prova suficiente de discriminação. O próximo passo consiste em avaliar os dados para compreender se a utilização destes fatores conduz a um tratamento desigual.⁵¹

- Para cada proxy, inclua provas ou argumentos que justifiquem a razão pela qual o OI o considera um proxy.

3.3. Avaliação dos riscos para os direitos fundamentais (avaliações de risco, AIDH, AIDF e AIPD)

As entidades prestadoras e as responsáveis pela implantação de sistemas de IA de risco elevado têm obrigações diversas e variadas no que diz respeito à identificação e documentação dos riscos de discriminação. No caso de sistemas algorítmicos que não sejam de risco elevado, as entidades prestadoras e/ou responsáveis pela implantação de IA podem muito bem ter identificado e documentado os riscos de discriminação no âmbito da sua conformidade com o RGPD (nomeadamente numa AIPD) ou da sua própria diligência devida em matéria de empresas e direitos humanos (Nações Unidas, 2011). Podem também ser introduzidas novas obrigações em virtude da Convenção-Quadro do Conselho da Europa sobre IA.

Os riscos de discriminação são normalmente identificados numa avaliação de impacto sobre os direitos fundamentais (AIDF), numa avaliação de impacto sobre a proteção de dados (AIPD) e/ou noutros procedimentos de gestão de riscos. Se forem realizados de forma adequada, estes processos devem identificar e registar quaisquer riscos de discriminação decorrentes de um sistema de IA ou do tratamento de dados através de um sistema de IA, bem como quaisquer medidas de mitigação adotadas e o respetivo impacto.

Nos documentos técnicos e nas avaliações de risco, podem ser referidos termos como “enviesamento” ou “equidade”, em vez de “desigualdade” ou “discriminação”.

Neste passo, seria útil contar com conhecimentos especializados, tanto técnicos como setoriais.

Avaliação de impacto sobre os direitos fundamentais: Regulamento sobre a IA

A obrigação de realizar uma AIDF aplica-se apenas a determinadas entidades responsáveis pela implantação de sistemas de IA de risco elevado (ver passo 2.2. para mais pormenores).

⁵¹ Uma informação introduzida no sistema que indique um motivo protegido, ou um proxy conhecido, e que não se sobreponha a um motivo protegido pode, por si só, não ser suficiente para fundamentar uma alegação de discriminação. Veja-se, por exemplo, o caso STAR na Dinamarca. Nesse caso, a ferramenta de previsão utilizou a “ascendência” ou a “origem” como característica preditiva. O comité determinou que o termo “ascendência”, quando utilizado na ferramenta de perfil, “não indica nada sobre a origem étnica”. www.retsinformation.dk/eli/accn/W20220951825. Para mais informações, consulte Equinet 2022: 23-24.

A AIDF (e outras avaliações) devem incluir uma série de informações que destaquem possíveis lacunas e violações de direitos, incluindo o princípio da não discriminação. Isto inclui:

- ▶ informações sobre a forma como quem é responsável pela implantação irá utilizar o sistema de IA de risco elevado, tal como previsto pela entidade prestadora;
- ▶ durante quanto tempo e com que frequência o sistema será utilizado;
- ▶ como foram implementadas as medidas de supervisão humana;
- ▶ as categorias de pessoas singulares e grupos suscetíveis de serem afetados;
- ▶ os riscos específicos de violação dos direitos fundamentais, incluindo a não discriminação, tendo em conta as informações fornecidas pela entidade prestadora;
- ▶ as disposições relativas à governação interna e aos mecanismos de queixa que quem é responsável pela implantação utilizará caso o risco se concretize.

Se quem é responsável pela implantação devesse ter realizado uma AIDF, mas não o fez ou não incluiu informações relevantes nesta, consulte o [Passo 4](#).

AIPD

Uma AIPD ⁵² deve ter em conta todos os riscos para os direitos e liberdades das pessoas singulares decorrentes do tratamento de dados pessoais, e não apenas os riscos para a privacidade. Isto inclui também os riscos de discriminação (Grupo de Trabalho sobre Proteção de Dados do artigo 29.º, 2017a). O OI poderá ter de cooperar com as autoridades responsáveis pela proteção de dados.

Questões a ter em conta

As informações relativas às várias avaliações de risco realizadas pela entidade prestadora e por quem é responsável pela implantação devem ser cruzadas entre si, devendo ser assinaladas quaisquer discrepâncias.

- ▶ A entidade prestadora ou quem é responsável pela implantação identificou riscos relevantes em matéria de direitos fundamentais que a outra não identificou?
- ▶ Quando uma das partes realizou mais do que uma avaliação de riscos ou mais do que um tipo de avaliação de riscos, existe consistência no que diz respeito aos riscos identificados? Há algum risco identificado numa avaliação que não conste noutra (a menos que haja uma boa explicação; por exemplo, o risco só se coloca no que diz respeito a uma criança e é especificamente considerado na avaliação de risco da criança)?

Para todos os sistemas algorítmicos, incluindo a IA de risco elevado:

- ▶ A entidade prestadora ou quem é responsável pela implantação identificou alguma discriminação (ou outro risco para os direitos fundamentais)?
- ▶ A entidade prestadora implementou um processo de gestão de riscos?
- ▶ De que forma foram utilizados os procedimentos de gestão de riscos e as

52 Em maio de 2026, o Comité Europeu para a Proteção de Dados realizou uma consulta sobre um modelo de AIPD, disponível aqui: www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en.

avaliações de impacto para identificar enviesamentos ou desigualdades nos dados ou no sistema? Como é que o enviesamento é definido ou delimitado?

- Existem riscos não mitigados? Sempre que possível, verifique os riscos referidos na documentação técnica em relação ao sistema de gestão de riscos.

Nota: nos casos em que tenha sido identificada discriminação e tenham sido implementadas as medidas de gestão alegadas, será necessária uma investigação mais aprofundada (ver passo 3.6. [testes e avaliação](#)). Se o sistema for de risco elevado e o OI for uma autoridade nos termos do artigo 77.º, esta pode solicitar acesso à documentação de avaliação de riscos prevista no artigo 9.º.

Nos casos que envolvam um sistema de IA de risco elevado:

- existe algum processo de gestão de riscos que esteja em conformidade com os requisitos do artigo 9.º?

Nos casos que envolvam um sistema de IA de risco elevado, em que é exigida uma AIDF por parte de quem é responsável pela implantação:

- a AIDF foi realizada corretamente? Não deve ser um exercício de preenchimento de formulários;
- A entidade responsável pela implantação envolveu alguma das partes interessadas relevantes ao realizar a avaliação de riscos? (O considerando 96 prevê essa possibilidade);
- deviam as partes interessadas ter sido consultadas, por exemplo, as pessoas suscetíveis de serem afetadas pelo sistema? (ver o caso Bridges abaixo);
- se tiver havido um processo de consulta, considere contactar as pessoas que foram consultadas, mas tenha em conta que estas podem estar sujeitas a um dever de confidencialidade ou a um acordo de não divulgação;
- verifique se todos os riscos de discriminação identificados na documentação técnica (artigo 11.º) estão todos referidos na documentação do sistema de gestão de riscos (artigo 9.º). Caso tal não suceda, poderá surgir uma presunção de discriminação.

Possíveis fontes de informação sobre riscos e avaliações de risco

Pessoa queixosa

RGPD, artigos 13.º a 15.º, Informações prestadas à pessoa titular dos dados

- A existência de processos de tomada de decisão automatizada e/ou de definição de perfis (artigos 13.º a 15.º, 21.º e 22.º do RGPD).
- A lógica subjacente à TDA utilizada (artigo 13.º, n.º 2, alínea f), artigo 14.º, n.º 2, alínea g), e artigo 15.º, n.º 1, alínea h), do RGPD).

Disponível ao público

- Base de dados da UE para sistemas de IA de risco elevado: secção C - responsável pela implantação: resumo da AIPD e da AIDF (exceto no caso de aplicação da lei ou controlo da migração).

Parte inquirida

Da entidade prestadora:

Regulamento sobre a IA da UE, artigo 9.º, sistema de gestão de riscos

- ▶ As entidades prestadoras são obrigadas a estabelecer um sistema de gestão de riscos no que diz respeito aos sistemas de IA de risco elevado. Trata-se de um processo iterativo contínuo que requer:
 - identificação de riscos: a identificação e análise dos riscos conhecidos e razoavelmente previsíveis para os direitos fundamentais (artigo 9.º, n.º 2, alínea a));
 - gestão de riscos: a adoção de medidas de gestão de riscos adequadas e específicas (artigo 9.º, n.º 2, alínea d)), incluindo a prestação de informação e formação a entidades responsáveis pela implantação, com vista a eliminar ou reduzir os riscos (artigo 9.º, n.º 5, alínea c), e artigo 13.º);
 - testes: garantir que o sistema foi testado com o objetivo de identificar as medidas de gestão de riscos mais adequadas e específicas (artigo 9.º, n.º 6);
 - grupos específicos: aquando da implementação do sistema, deve ter-se em conta se este é suscetível de ter um impacto negativo em pessoas com menos de 18 anos e, se for caso disso, noutros grupos vulneráveis (artigo 9.º, n.º 9).

No entanto, a gestão de riscos só é exigida no que diz respeito aos riscos que “possam ser razoavelmente atenuados ou eliminados aquando do desenvolvimento ou da conceção do sistema de IA de risco elevado ou por meio da prestação de informações técnicas adequadas”.

Regulamento sobre a IA da UE, artigo 10.º, dados e governação de dados (ver passo 3.6. [Testes e avaliação](#))

Regulamento sobre a IA da UE, artigo 11.º e Anexo IV, documentação técnica

- ▶ A alínea g) do n.º 2 do Anexo IV exige que a documentação técnica inclua informações sobre quaisquer impactos potencialmente discriminatórios.
- ▶ Anexo IV, n.º 3: informações pormenorizadas sobre a monitorização, o funcionamento e o controlo do sistema de IA, em particular no que diz respeito às suas capacidades e limitações em termos de desempenho, incluindo os graus de exatidão para pessoas específicas ou grupos de pessoas aos quais o sistema se destina a ser aplicado e o nível global de exatidão esperado em relação à finalidade a que se destina; os resultados indesejados previsíveis e as fontes de risco para a saúde e a segurança, os direitos fundamentais e a discriminação, tendo em conta a finalidade prevista do sistema de IA; as medidas de supervisão humana necessárias, em conformidade com o artigo 14.º, incluindo as medidas técnicas implementadas para facilitar a interpretação dos resultados dos sistemas de IA por quem é responsável pela implantação; especificações relativas aos dados de entrada, conforme adequado.

De quem é responsável pela implantação:

Regulamento sobre a IA da UE, artigo 13.º, transparência e prestação de informações a responsáveis pela implantação

- ▶ Instruções de utilização fornecidas a quem é responsável pela implantação por parte da entidade prestadora (artigo 13.º, n.º 3):
 - circunstâncias conhecidas ou previsíveis de utilização pretendida ou indevida que possam pôr em risco os direitos fundamentais;
 - quando for o caso, o seu desempenho em relação a pessoas específicas ou grupos de pessoas a quem o sistema se destina;
 - quando for o caso, as especificações relativas aos dados de entrada ou quaisquer outras informações relevantes no que diz respeito aos conjuntos de dados de treino, validação e teste utilizados, tendo em conta a finalidade prevista do sistema de IA de risco elevado.

Regulamento sobre a IA da UE, artigo 26.º, n.º 9, avaliação de impacto sobre a proteção de dados: realizada com base nas informações fornecidas pela entidade prestadora/RGPD, artigo 35.º, avaliação de impacto sobre a proteção de dados (AIPD)

Regulamento sobre a IA da UE, artigo 27.º, n.º 1, alínea d), avaliação de impacto sobre os direitos fundamentais

- ▶ Os riscos específicos de violação dos direitos fundamentais, incluindo a não discriminação, tendo em conta as informações fornecidas pela entidade prestadora.

Outros

- ▶ Avaliação realizada com base na avaliação de riscos e impactos dos sistemas de IA do Conselho da Europa, do ponto de vista dos direitos humanos, da democracia e do Estado de direito (metodologia HUDERIA).
 - ▶ Algumas organizações irão realizar e publicar, de forma voluntária, uma AIDH ou AIDF, uma AIPD ou uma avaliação de impacto nos direitos da criança. Pode haver uma avaliação “ética”.
 - ▶ Quaisquer outras avaliações (de risco) partilhadas pela parte inquirida.
 - ▶ Pedidos de acesso à informação, quando disponíveis.
-

Caso importante: *R (Bridges) contra Chief Constable of South Wales Police*, 2020

(Os números entre parênteses retos correspondem aos números dos parágrafos do acórdão.)

O caso Bridges foi decidido pelo Tribunal de Recurso do Reino Unido, que analisou se uma autoridade pública tinha violado os direitos humanos ou não tinha cumprido os deveres de avaliar os impactos em matéria de igualdade, nos termos da Lei da Igualdade de 2010, antes de implementar o reconhecimento facial em tempo real. O dever de igualdade no setor público exige que uma autoridade pública tenha “devida consideração” pela necessidade de eliminar a discriminação, o assédio, a vitimização e outras condutas relevantes, promover a igualdade de oportunidades e fomentar boas relações entre pessoas que partilham uma característica relevante e pessoas que não a partilham.

O tribunal considerou que o dever:

- ▶ deve ser cumprido antes e no momento em que se está a ponderar a adoção de uma política (relativa à utilização do reconhecimento facial);
- ▶ deve ser exercido na prática, com rigor e espírito aberto – não se trata de um exercício de preenchimento de formulários;
- ▶ é indelegável, o que pode criar dificuldades muito concretas para as entidades públicas responsáveis pela implantação que recorrem a entidades prestadoras terceiras, especialmente se não tiverem sido fornecidas informações suficientes sobre o desempenho de um sistema ou se a entidade não dispuser de conhecimentos especializados ou experiência suficientes para compreender as informações ou o sistema [199].

Além disso, caso não estejam disponíveis dados relevantes para a avaliação, existe a obrigação de os obter - o que poderá exigir uma consulta adicional aos grupos relevantes. Por fim, desde que haja uma análise rigorosa desse dever, de modo a que se avalie devidamente o impacto potencial da decisão nos objetivos de igualdade e a desejabilidade de os promover, cabe a quem decide determinar o peso que deve ser atribuído aos fatores que informam a decisão.

Em termos gerais, o tribunal considerou que o cumprimento deste dever “exige a adoção de medidas razoáveis para obter informações sobre o que ainda possa não ser do conhecimento de uma autoridade pública relativamente ao impacto potencial de uma decisão ou política proposta sobre as pessoas com as características relevantes, em particular, para os fins que nos ocupam, a raça e o sexo” [181].

Considerou-se que o simples facto de haver uma intervenção humana não era, por si só, suficiente para cumprir o dever legal, uma vez que esse dever regula o processo e não o conteúdo de uma decisão.

E o tribunal reconheceu que os seres humanos cometem erros [185].

É provável que observações semelhantes se apliquem às avaliações de risco ao abrigo do Regulamento sobre a IA.

Indicadores de discriminação

Um risco de discriminação que tenha sido identificado, mas que não tenha sido mitigado, monitorizado ou justificado, deve ser considerado um indicador sólido.

- ▶ Referência direta à discriminação, enviesamento ou desigualdade na AIDF.
- ▶ Referência direta à discriminação, enviesamento ou desigualdade na AIPD.
- ▶ Caso o enviesamento seja referido como um risco, o significado e os tipos de enviesamento não estão definidos, ou estão definidos de forma inadequada, na documentação.
- ▶ Não existem procedimentos de gestão de riscos, ou estes são inadequados, para os riscos identificados de discriminação, enviesamento ou desigualdade.
- ▶ O risco inquestionável de discriminação é evidente na documentação.
- ▶ Testes insuficientes.
- ▶ Referência direta ao risco de violação dos direitos fundamentais, quer na AIDF, quer na AIPD:
 - sempre que exista o risco de violação dos direitos fundamentais, tal deve constituir um indício da necessidade de uma investigação mais aprofundada, a fim de garantir que o sistema não é discriminatório.
- ▶ Uma AIDF ou AIPD incompleta, superficial ou imprecisa justificaria uma investigação mais aprofundada.
- ▶ A falta de consulta às partes interessadas relevantes para identificar riscos, nos casos em que estas deveriam claramente ter sido incluídas (por exemplo, um sistema concebido para tomar decisões sobre pessoas com deficiência que não tenha consultado nenhuma pessoa com deficiência nem organizações representativas antes da sua implantação pode não ter realizado a AIDF com o cuidado necessário).

- ▶ Registe quaisquer riscos de discriminação identificados pela entidade prestadora ou por quem é responsável pela implantação, bem como quaisquer medidas identificadas para mitigar esses riscos.
- ▶ Analise e registe se existem falhas claras e evidentes na avaliação de riscos, na AIPD ou na AIDF.

3.4. Qual é a finalidade do sistema algorítmico e como é que ele funciona?

Para perceber se ocorreu discriminação algorítmica, os OIs devem compreender o próprio sistema, pelo menos em termos gerais. Compreender o objetivo e a conceção do sistema, bem como o seu funcionamento, ajuda a avaliar os seguintes aspetos.

- ▶ Qual é a finalidade do sistema?
 - a finalidade está relacionada com um domínio em que se tem verificado discriminação histórica no que diz respeito à(s) característica(s) protegida(s)?

- os dados utilizados são adequados para o fim a que se destinam (ver passo 3.5)?
- ▶ De que forma as entradas contribuem para os resultados?
 - uma entrada identificada no passo 3.2 influencia o resultado e conduz a uma eventual diferença no tratamento?
- ▶ Quer o sistema algorítmico tenha impacto no processo de tomada de decisão no seu conjunto, quer tenha impacto no resultado final para o grupo afetado:
 - qual é a importância do sistema? Por exemplo, é o único responsável pelas decisões ou apoia quem é responsável pelas decisões?
 - o sistema algorítmico é o sistema na sua totalidade ou apenas uma parte de um sistema muito maior que pode envolver outros sistemas algorítmicos?

No que diz respeito às informações sobre a utilização prevista e a conceção, deve analisar, de um modo geral, se as escolhas de conceção parecem adequadas à finalidade prevista e à utilização efetiva. Neste passo, tanto os conhecimentos técnicos como os conhecimentos especializados setoriais são úteis.

A informação disponibilizada aos Ols deverá, em última análise, permitir que estes compreendam o que o sistema de IA faz, como o faz - através de informação significativa sobre a lógica envolvida, o significado do tratamento e as consequências previstas para a pessoa singular - e por que razão foram feitas as várias escolhas em relação à conceção e aos dados. Quando se considera que o sistema algorítmico se enquadra na categoria de TDA ou de sistema de IA de risco elevado utilizado para a tomada de decisões com impacto significativo, é obrigatória a disponibilização desta informação. No entanto, se a documentação não permitir essa compreensão, poderão surgir problemas relacionados com a falta de transparência (ver abaixo, “Transparência”, no passo 3.7).

A conceção do sistema pode também revelar-se particularmente importante mais tarde, quando se analisarem as formas como a parte inquirida poderá procurar refutar qualquer presunção de discriminação ou justificar as decisões tomadas.

Questões a ter em conta

Finalidade e utilização

- ▶ Como é que o sistema algorítmico deve ser utilizado?
 - Qual é a finalidade pretendida?
 - Como é utilizado na prática?
 - Nos casos em que o sistema é fornecido por uma entidade fornecedora: é utilizado por quem é responsável pela implantação da forma pretendida pela entidade prestadora?
- ▶ A quem se destina o sistema?
 - Quais foram as escolhas de conceção (ver o quadro abaixo) adotadas no que diz respeito às pessoas ou grupos de pessoas a quem o sistema se destina?
- ▶ Existem pressupostos relativos a pessoas ou grupos de pessoas a quem o sistema se destina? Por exemplo, prevê-se que este sistema seja utilizado ape-

nas por pessoas adultas, ou parte-se do princípio de que este sistema será utilizado num setor específico ou por uma população específica. Será que estes pressupostos são racionais e justificados?

- ▶ De que forma é que o sistema influencia o tratamento das pessoas?
- ▶ Nos casos em que existe um decisor humano responsável por tomar decisões que influenciam o tratamento das pessoas (interveniente humano):
 - existem orientações ou protocolos dirigidos às partes decisoras para as ajudar a compreender como utilizar o sistema de IA ou a interpretar os resultados?
 - a pessoa responsável possui a competência, a formação e a autoridade necessárias para anular uma decisão tomada por um sistema de IA?
 - a pessoa responsável recebeu formação para compreender e interpretar os resultados do sistema e para reconhecer em que situações podem surgir enviesamentos e ser necessária uma intervenção?

Nota: a mera existência de um interveniente humano não significa que o sistema não influencie o tratamento das pessoas, uma vez que esse interveniente humano é influenciado pelos resultados do sistema, em maior ou menor grau.

Como funciona o sistema

- ▶ O sistema foi concebido para otimizar o quê?
 - Foi concebido para otimizar algo (ligeiramente) diferente do seu caso de utilização previsto? Por exemplo, foi otimizado para prever erros, mas agora é utilizado para prever fraudes?
- ▶ O sistema utiliza características de grupo para gerar resultados a nível individual (definição de perfis)?
- ▶ Como é que o sistema lida com desvios?
 - Como é que o sistema lida com desvios em relação ao comportamento esperado (por exemplo, erros ou atividades invulgares)?
- ▶ Todos os desvios são tratados da mesma forma, independentemente do motivo subjacente?
 - O sistema foi concebido para garantir justiça e equidade?
 - A equidade ou a não discriminação fizeram parte da conceção?
 - A noção de equidade, específica ao contexto, está explicitamente definida?
 - Que medidas foram tomadas para garantir a equidade e a igualdade na conceção?

Influência das entradas

- ▶ Como foi feita a escolha de qualquer modelo ou algoritmo (pré-treinado)?
 - Este procedimento está documentado e à disposição de quem é responsável pela implantação do sistema?

- ▶ Que critérios influenciam o resultado do sistema?
 - Os atributos protegidos relevantes e/ou as variáveis proxy presentes nos dados são processados ou utilizados como base para uma TDA ou para a definição de perfis (por exemplo, dados utilizados para criar um perfil, informações sobre o perfil)?
 - Existem parâmetros disponíveis sobre o peso/influência de um fator específico no resultado?
- ▶ Que critérios têm maior peso no sistema ou na decisão?
 - A parte inquirida poderia alegar que os atributos protegidos e/ou os proxies têm um impacto insignificante no resultado?
- ▶ Qual é o impacto cumulativo da combinação de várias variáveis proxy, tais como fatores como o código postal e o nível de escolaridade?
- ▶ Os dados utilizados ou aos quais é atribuído maior peso são arbitrários ou irrelevantes para o fim a que se destinam?

Possíveis fontes de informação para compreender o objetivo, a conceção e o funcionamento do sistema

Pessoa queixosa

RGPD, artigos 13.º a 15.º, informações prestadas à pessoa titular dos dados

- ▶ A existência de processos de tomada de decisão automatizada e/ou de definição de perfis (artigos 13.º a 15.º, 21.º e 22.º do RGPD).
- ▶ A lógica subjacente à TDA utilizada (artigo 13.º, n.º 2, alínea f), artigo 14.º, n.º 2, alínea g), e artigo 15.º, n.º 1, alínea h), do RGPD).

RGPD, artigo 15.º, n.º 3: PAPTD

- ▶ O âmbito, a natureza e o nível de pormenor das informações que serão fornecidas em resposta a um PAPTD podem variar. No caso das TDA elegíveis, é necessário incluir os seguintes elementos; no entanto, no que diz respeito a outros sistemas algorítmicos (ou partes destes), esta informação também pode ser incluída:
 - variáveis ou parâmetros de entrada utilizados na tomada de decisões e a forma como foram obtidos (por exemplo, através de informação estatística), bem como o respetivo peso (parecer do AG Pikamäe SCHUFA Holding, 2023, n.º 58);
 - o efeito de uma variável de entrada na pontuação; explicação do motivo pelo qual foi atribuída uma determinada pontuação à pessoa titular dos dados; lista das possíveis categorias de perfil e cenários contrafactuais;
 - o princípio de cálculo subjacente: explicações detalhadas sobre o método de cálculo do valor da pontuação; atribuição da pessoa titular dos dados a um resultado de avaliação; lista de categorias de perfil (Barros Vale e Zanfir-Fortuna 2022);

-
- a existência de tomadas de decisão automatizadas e/ou de definição de perfis, bem como informações significativas sobre a lógica subjacente, o significado e as consequências previstas desse tratamento para a pessoa titular dos dados (artigo 15.º, n.º 1, alínea h)).

Regulamento sobre a IA da UE, artigo 86.º, Regulamento sobre a IA: direito a explicações

- ▶ O papel do sistema de IA no processo de tomada de decisões. Por exemplo: “O sistema de IA [nome/designação do sistema de IA] foi utilizado para [descrição da função específica do sistema de IA, como a análise de dados, a avaliação de critérios, a realização de análises de voz para o reconhecimento de emoções, etc.]. O sistema de IA contribuiu para o processo de tomada de decisão ao [analisar os dados e apresentar uma avaliação dos parâmetros relevantes, por exemplo]”.
- ▶ A lógica de processamento: “O sistema analisou os dados introduzidos utilizando [descrição de algoritmos ou modelos, como árvores de decisão] para realizar [descrição do objetivo, como a avaliação de riscos]”.
- ▶ Resultado: “Com base nesta análise, o sistema de IA gerou o seguinte resultado, que foi incorporado na decisão final: [Descrição do resultado, uma pontuação, uma classificação, por exemplo]”.
- ▶ Impacto da decisão tomada na pessoa afetada: “A decisão tem o seguinte impacto potencial para si: [impacto na solvabilidade, acesso a determinados serviços, impacto financeiro, etc.]. Estes impactos são relevantes, uma vez que podem afetar significativamente a sua capacidade de [explicar as consequências, tais como a participação em programas ou a receção de ofertas de financiamento]”.
- ▶ Ponderação dos critérios: “Os principais critérios determinantes foram ponderados da seguinte forma: [breve explicação da importância de cada critério]”.

Parte inquirida

Da entidade prestadora

Regulamento sobre a IA da UE, Secção A, n.º 5 e 6 do Anexo VIII, relativa aos sistemas de IA de risco elevado

- ▶ Descrição da finalidade pretendida do sistema de IA, descrição básica e concisa da informação utilizada pelo sistema (dados, entradas) e da sua lógica de funcionamento.
 - No que diz respeito à aplicação da lei e ao controlo da migração, poderá haver informações adicionais na base de dados à disposição da AFM competente.

Regulamento sobre a IA da UE, artigo 11.º e Anexo IV, documentação técnica

- ▶ N.º 1, alínea a) A finalidade prevista.

- ▶ N.º 1, alínea d) A descrição de todas as formas sob as quais o sistema de IA é colocado no mercado ou colocado em serviço (tais como pacotes de *software* integrados em *hardware*, descarregamentos ou APIs).
- ▶ N.º 1, alínea h) Uma descrição básica da interface de utilizador facultada a quem é responsável pela implantação.
- ▶ N.º 2, alínea b) Especificações de conceção e lógica geral. Ver acima, passo 3.2. [Existem características protegidas ou proxies conhecidos nos dados de entrada ou nos conjuntos de dados?](#)

De quem é responsável pela implantação

- ▶ Artigo 13.º, Transparência e prestação de informações a responsáveis pela implantação
- ▶ A entidade prestadora deve disponibilizar (artigo 13.º, n.º 2) instruções de utilização destinadas a quem é responsável pela implantação.
- ▶ Artigo 13.º, n.º 3, alínea b), subalínea iv), quando aplicável, as capacidades e características técnicas do sistema de IA de risco elevado para fornecer informações relevantes para explicar os seus resultados, e n.º 3, alínea b), subalínea v), o seu desempenho no que diz respeito a pessoas específicas ou grupos de pessoas aos quais o sistema se destina a ser utilizado.
- ▶ Artigo 13.º, n.º 3, alínea c), as alterações ao sistema de IA de risco elevado e ao seu desempenho que tenham sido predeterminadas pela entidade prestadora no momento da avaliação inicial da conformidade, se for caso disso.

Outros

- ▶ Pesquisa documental
- ▶ Cláusulas contratuais
- ▶ Perguntas frequentes na plataforma
- ▶ Comunicações das empresas cotadas em bolsa

Indicadores de discriminação

Indicadores fortes

Estes indicadores, *em conjunto*, poderiam constituir um caso *prima facie*.

- ▶ Os critérios suspeitos (conforme identificados no [passo 3.2](#)) têm uma influência não negligenciável no resultado do sistema.
 - Quando uma característica protegida ou um proxy que esteja indissociavelmente ligado a uma característica protegida tem uma influência não negligenciável no resultado do sistema, isso constitui uma indicação clara de discriminação direta.

- Quando um proxy (suspeito) tem uma influência não negligenciável nos resultados do sistema, isso constitui um indício de discriminação indireta.
- O resultado do sistema (pelo menos em parte) determina o tratamento dado às pessoas singulares.

Outros indicadores

- Suspeita-se que a utilização prevista, os pressupostos e/ou as escolhas de conceção reflitam ou ampliem as desigualdades históricas, conduzindo a um tratamento desigual.
- As escolhas de conceção favorecem um grupo de pessoas em detrimento de outro.
- O sistema é otimizado para grupos historicamente favorecidos.
- O sistema não está a ser utilizado para o fim a que se destinava quando foi desenvolvido/fornecido.

- Registe a finalidade do sistema e o que este visa otimizar.
- Registe os proxies e as características protegidas que influenciam os resultados do sistema e, quando disponíveis, os parâmetros relativos ao seu peso/influência nos resultados.

3.5. Dados de treino, teste e validação

Os dados são utilizados para desenvolver e testar sistemas algorítmicos. Mesmo os sistemas algorítmicos baseados em regras que são concebidos manualmente são validados com base em dados. Os dados são sempre uma representação imperfeita da realidade. Os enviesamentos e as desigualdades existentes refletem-se nos dados. A avaliação dos enviesamentos e das desigualdades nos dados pode ser utilizada para argumentar que o sistema resultante conduz a resultados discriminatórios. Note-se que a compreensão dos enviesamentos nos dados, por si só, não demonstra um tratamento desigual. No entanto, em conjunto com outras fontes de análise complementares, contribui para a constituição de um caso *prima facie* e pode ser utilizado para fundamentar pedidos de testes adicionais.

Quando existem dados estatísticos relativos à igualdade, esta secção reveste-se de especial importância para avaliar a validade e a fiabilidade dos dados utilizados no cálculo dessas estatísticas. Nesse caso, esta secção deve ser lida em conjunto com a secção 3.6.

Ao analisar os dados, deve procurar, de um modo geral, verificar que informações a parte inquirida forneceu sobre a forma como treinou e testou o seu sistema. A partir disto, poderá identificar quaisquer questões-chave relacionadas com a discriminação; por exemplo, não foram incluídas mulheres no conjunto de dados, os dados de treino eram de uma cidade, mas o sistema é utilizado numa zona rural, etc.

Noutros casos, poderá ser necessário recorrer a conhecimentos especializados técnicos e setoriais para determinar se o sistema foi treinado e testado com conjuntos

de dados representativos, relevantes, medidos com exatidão e de forma adequada e generalizáveis.

Algumas questões fundamentais a ter em conta incluem uma variedade de enviesamentos. Estes enviesamentos não são independentes uns dos outros: um enviesamento influencia outro.

- ▶ Se é provável que exista um enviesamento histórico nos dados. Em todos os domínios em que existe uma desigualdade histórica ou atual, essa desigualdade reflete-se nos dados, a menos que seja cuidadosamente corrigida. Exemplos disso são a repressão policial excessiva de que as comunidades negras foram alvo no passado e os períodos de desemprego decorrentes de responsabilidades parentais ou de outros cuidados, que afetam a igualdade de género.
- ▶ Se existe algum enviesamento de representatividade nos dados. Por exemplo, a população-alvo reflete a população utilizadora? Por exemplo, os dados que são representativos de Lisboa podem não ser representativos do Porto. Os dados relativos a Helsínquia há 30 anos podem não refletir a população atual. Podem surgir questões adicionais relacionadas com quem está representado nos dados e em que medida. Por exemplo, nos dados relativos à saúde, poderá haver uma sub-representação das mulheres e/ou uma sobre-representação de mulheres grávidas. Qualquer um destes fatores pode distorcer os dados e afetar os resultados. Além disso, preste atenção à forma como as minorias estão representadas nos dados. Por exemplo, quando determinados sotaques não foram incluídos num sistema de reconhecimento de voz, esse sistema funcionará menos bem com esses sotaques. Se as pessoas que usam hijab não tiverem sido incluídas nos dados para o reconhecimento facial, existe a possibilidade de que as pessoas com hijab não sejam bem reconhecidas.
- ▶ Se existe um enviesamento de seleção nos dados. É o que acontece quando só existem dados relativos a um subgrupo específico do conjunto de dados. Por exemplo, no que diz respeito à concessão de empréstimos, só existem informações sobre quem não cumpre as suas obrigações de pagamento relativamente ao grupo que recebeu o empréstimo no passado. Os dados relativos às patrulhas policiais incluem apenas informações sobre as áreas onde a polícia efetivamente realizou patrulhas. Os dados relativos à fraude só podem incluir o grupo que foi alvo de investigação por fraude no passado. Os dados de recrutamento contêm menos informações sobre pessoas candidatas cujos currículos nunca foram selecionados para as fases seguintes. Isto poderia distorcer os dados, especialmente se as pessoas com uma característica protegida específica tivessem sido, historicamente, sobre-representadas ou sub-representadas neste contexto.
- ▶ Se existe algum enviesamento de medição nos dados. É o que acontece quando os rótulos (a medição) não refletem o conceito que se pretendem medir. Por exemplo, se quiser avaliar a fraude nos subsídios sociais, mas decidir que todas as concessões incorretas de subsídios devem ser tidas em conta, o resultado será que incluirá tanto erros inocentes como fraudes. Por sua vez, isto pode ter um impacto desigual em determinados grupos, por exemplo, aqueles com baixos níveis de literacia, um baixo nível de escolaridade e aqueles cuja língua

materna não é uma das línguas nacionais. Outra forma de enviesamento de medição ocorre quando os enviesamentos humanos (ou a discriminação humana) influenciam os rótulos registados que são agora considerados a verdade de referência. Em qualquer situação em que os rótulos de referência sejam o resultado de uma avaliação humana com algum grau de discricionabilidade individual, existe o risco de que os enviesamentos humanos tenham dado origem a um enviesamento de medição. Exemplos disso são as avaliações de professoras/es, os dados relativos ao recrutamento ou as investigações de fraude.

Questões a ter em conta

Refleta sobre as questões que se seguem, tendo em conta o enviesamento e a desigualdade. Todas as questões abaixo são subjetivas, apresentam nuances e dependem do contexto. Para responder a estas questões, será necessário um bom conhecimento do setor e das desigualdades que nele existem, bem como dos sistemas e da tecnologia utilizados. O resultado desta avaliação servirá, sobretudo, para orientar novas avaliações ou poderá ser utilizado para constituir um caso *prima facie*.

Note-se que, no caso de sistemas algorítmicos concebidos manualmente, não haverá quaisquer dados de treino. Em alguns sistemas de IA, os dados de treino não incluem rótulos. Nesse caso, continua a haver a expectativa de existência de dados de teste, que incluem algum tipo de rótulos para verificar se o modelo fornece resultados corretos ou aceitáveis.

Dados de treino, teste e validação

- ▶ Como foram escolhidos os conjuntos de dados de treino, teste e validação?
- ▶ Que dados de treino/teste/validação foram recolhidos?
- ▶ Quais são as fontes desses dados?
- ▶ Com que finalidade foram os dados recolhidos inicialmente? A sua utilização num contexto diferente suscita algum problema? Por exemplo, se os dados tiverem sido recolhidos com o objetivo de avaliar a saúde, a sua reutilização para fins de seguros suscita alguma questão relacionada com potenciais enviesamentos de medição?
- ▶ Que métodos foram utilizados para recolher os dados?
 - Estes métodos parecem razoáveis, no sentido de que conduzem, de forma razoável, a dados fiáveis e relevantes para a tarefa a que o sistema algorítmico se destina?
 - Certificaram-se de que os dados eram representativos e tinham sido medidos de forma adequada? Será razoável esperar que os dados sejam aplicáveis ao domínio e ao contexto em que os sistemas algorítmicos são atualmente utilizados?
 - Foram recolhidos (ou rotulados) dados adicionais para serem utilizados como dados de treino/teste/validação? Foi utilizada uma amostra aleatória para recolher os dados?
- ▶ Caso o conjunto de dados seja proveniente de uma entidade terceira, como foi obtido? Os dados fornecidos por entidades terceiras foram verificados?

- ▶ Existem desigualdades históricas que possam vir a refletir-se nos dados (ver a secção sobre enviesamentos acima)? Tenha também em conta, neste contexto, a discriminação múltipla/interseccional.
- ▶ As minorias estão suficientemente representadas nos dados? Isto é particularmente relevante no caso dos sistemas algorítmicos aplicados em setores em que a cultura, o contexto e a aparência física podem influenciar os resultados.

Rótulos

- ▶ Quão fiáveis são os rótulos?
- ▶ Os rótulos correspondem à finalidade dos sistemas? Por outras palavras, os rótulos medem aquilo que o sistema deve prever?
- ▶ A correção pode ser determinada de forma objetiva? Já foi determinada?
- ▶ Nos casos em que a rotulagem envolve o julgamento humano, os enviesamentos humanos poderão ter distorcido os rótulos? Existem motivos para suspeitar de discriminação?

Medidas de mitigação existentes

- ▶ Como foi avaliada a qualidade dos dados?
 - Que medidas foram tomadas para resolver eventuais problemas de qualidade detetados, tais como o preenchimento ou a remoção de dados?
- ▶ Que medidas foram tomadas para garantir que os dados fossem representativos, relevantes, medidos com exatidão e generalizáveis?
- ▶ De que forma foram mitigados eventuais enviesamentos e desigualdades no conjunto de dados?
 - Foram implementadas medidas⁵³ para mitigar o enviesamento?
 - Para que tipos de enviesamentos foram estas medidas implementadas? Existem alguns enviesamentos reconhecidos para os quais não tenham sido implementadas medidas de mitigação?
 - Que técnicas foram utilizadas?
 - Existem dados disponíveis sobre a eficácia destas medidas de mitigação do enviesamento?

Possíveis fontes de informação para avaliar os dados utilizados

Pessoa queixosa

Regulamento sobre a IA da UE, artigo 86.º, direito a explicações

RGPD, artigos 13.º a 15.º, informações prestadas à pessoa titular dos dados

53 As medidas de mitigação do enviesamento podem ser quaisquer medidas tomadas para evitar o enviesamento nos dados ou num sistema. Estas podem incluir a amostragem aleatória, a recolha de dados adicionais para aumentar a representatividade dos dados, protocolos rigorosos para a avaliação dos casos, a revisão por duas pessoas na avaliação dos casos, a reavaliação dos dados e muitas outras medidas.

Disponível ao público

Base de dados da UE para sistemas de IA de risco elevado

- ▶ Secção A, sistemas de IA de risco elevado – informação utilizada pelo sistema, incluindo dados e entradas.
- ▶ Secção C, responsável pela implantação – resumo da AIPD e da AIDF (a menos que seja utilizada para fins de aplicação da lei ou de controlo da migração).

Parte inquirida

Da entidade prestadora:

Regulamento sobre a IA da UE, Anexo IV, n.º 2, alínea d), documentação técnica

- ▶ “Se for caso disso, os requisitos de dados em termos de folhas de dados que descrevam as metodologias e técnicas de treino e os conjuntos de dados de treino utilizados, incluindo uma descrição geral desses conjuntos de dados, informações sobre a sua proveniência, o seu âmbito e as suas principais características; a forma como os dados foram obtidos e selecionados; procedimentos de rotulagem (por exemplo, para aprendizagem supervisionada), metodologias de limpeza de dados (por exemplo, deteção de valores atípicos).”

Regulamento sobre a IA da UE, artigo 10.º, práticas de governação e gestão de dados

- ▶ As entidades prestadoras devem ter implementado práticas adequadas, de modo a garantir que os conjuntos de dados sejam “pertinentes, suficientemente representativos e, tanto quanto possível, isentos de erros e completos, tendo em conta a finalidade prevista. Devem ter as propriedades estatísticas adequadas, nomeadamente, quando aplicável, no tocante às pessoas ou grupos de pessoas em relação às quais se destina a utilização do sistema de IA de risco elevado. Essas características dos conjuntos de dados podem ser satisfeitas a nível de conjuntos de dados individuais ou de uma combinação dos mesmos.”

Isto abrange, pelo menos:

- ▶ escolhas de conceção relevantes;
- ▶ recolha e utilização de dados (artigo 10.º, n.º 2, alíneas b), e) e g));
- ▶ operações de tratamento para a preparação de dados, incluindo a anotação e a rotulagem (artigo 10.º, n.º 2, alínea c));
- ▶ formulação de pressupostos, nomeadamente no que diz respeito à mensuração e à representação (artigo 10.º, n.º 2, alínea d));
- ▶ explicitamente tendo em conta o enviesamento, são obrigadas a analisar e a tomar as “medidas adequadas para detetar, prevenir e atenuar eventuais enviesamentos” (artigo 10.º, n.º 2, alínea g)) nos conjuntos de dados que sejam suscetíveis de “ter repercussões negativas nos direitos fundamentais

ou de resultar em discriminações proibidas pelo direito da União” (artigo 10.º, n.º 2, alínea f)).

Regulamento sobre a IA da UE, artigo 17.º, n.º 1, alínea f), gestão da qualidade

- ▶ As políticas, procedimentos e instruções por escrito devem incluir: “sistemas e procedimentos de gestão de dados, incluindo aquisição de dados, recolha de dados, análise de dados, rotulagem de dados, armazenamento de dados, filtragem de dados, prospeção de dados, agregação de dados, conservação de dados e qualquer outra operação relativa aos dados que seja realizada antes e para efeitos da colocação no mercado ou colocação em serviço de sistemas de IA de risco elevado”.

De quem é responsável pela implantação:

Regulamento sobre a IA da UE, artigo 13.º, alínea b), subalínea vi), instruções de utilização

- ▶ A entidade prestadora deve disponibilizar “quando oportuno, especificações para os dados de entrada, ou quaisquer outras informações importantes em termos dos conjuntos de dados de treino, validação e teste utilizados, tendo em conta a finalidade prevista do sistema de IA de risco elevado” (na informação fornecida a quem é responsável pela implantação por parte da entidade prestadora).

Regulamento sobre a IA da UE, artigo 26.º, n.º 4

Na medida em que quem é responsável pela implantação exerça controlo sobre os dados de entrada, tal responsável pela implantação deverá assegurar que os dados de entrada sejam relevantes e suficientemente representativos, tendo em conta a finalidade pretendida do sistema de IA de risco elevado.

Outros

- ▶ Documentação sobre iniciativas
- ▶ Folhas de dados para conjuntos de dados
- ▶ Fichas de modelo para relatórios sobre modelos
- ▶ Governança de dados aplicada e normas de qualidade – quando a parte inquirida referiu a utilização de normas, estas podem ser utilizadas para compreender o compromisso assumido pela parte inquirida.
- ▶ No que diz respeito à aplicação da lei e ao controlo da migração, poderá haver informações adicionais na base de dados à disposição da AFM competente.

Indicadores de discriminação

Os indicadores abaixo revelam problemas nos dados, o que pode contribuir para a constituição de um caso *prima facie*, ao indicar, de um modo geral, que estão a

ser utilizados dados não fiáveis ou enviesados, e pode servir de base para solicitar testes adicionais. É provável que esta lista esteja incompleta. Poderão existir outras considerações decorrentes do exposto acima que não estejam aqui enumeradas.

- ▶ Questões gerais relacionadas com os dados:
 - não representativos (área geográfica, setor);
 - de origem inadequada (reutilizados);
 - não atualizados;
 - existe um enviesamento de seleção;
 - existe um enviesamento de medição, no sentido de que o rótulo reflete um conceito diferente do que é previsto, ou de que os rótulos são, em geral, pouco fiáveis.
- ▶ Indicadores de problemas de qualidade dos dados relacionados com a discriminação:
 - os dados não são representativos de todas as pessoas afetadas;
 - elevada probabilidade de refletir desigualdades históricas ou persistentes;
 - é provável que o enviesamento de seleção conduza a uma sobrerrepresentação ou sub-representação de grupos com atributos protegidos;
 - é provável que o enviesamento de medição afete grupos com atributos protegidos;
 - há indícios de discriminação na recolha, na elaboração ou na rotulagem dos dados.
- ▶ As decisões relativas aos dados não estão devidamente documentadas.
- ▶ Não existem medidas de mitigação ou não é possível demonstrar que as medidas de mitigação sejam eficazes.

Indicadores de incumprimento no que diz respeito aos sistemas de risco elevado previstos no Regulamento sobre a IA

Embora o incumprimento do Regulamento sobre a IA não seja o foco desta metodologia de avaliação, qualquer indício de que os requisitos do Regulamento sobre a IA não estejam a ser cumpridos pode servir de base para a adoção de medidas corretivas (ver [Passo 4](#)).

- ▶ A entidade prestadora não consegue demonstrar que implementou práticas que garantam que os conjuntos de dados sejam “pertinentes, suficientemente representativos e, tanto quanto possível, isentos de erros e completos, tendo em conta a finalidade prevista. Devem ter as propriedades estatísticas adequadas, nomeadamente, quando aplicável, no tocante às pessoas ou grupos de pessoas em relação às quais se destina a utilização do sistema de IA de risco elevado. Essas características dos conjuntos de dados podem ser satisfeitas a nível de conjuntos de dados individuais ou de uma combinação dos mesmos.” Ou não conseguem apresentar documentação que comprove isso.
- ▶ A entidade prestadora não realizou testes de enviesamento, ou não testou todos os enviesamentos relevantes.

- ▶ A entidade prestadora não implementou medidas eficazes para prevenir e mitigar os enviesamentos que detetou ou suspeita que existam.

- ▶ Registe quaisquer problemas gerais relacionados com os dados, quaisquer problemas relacionados com a qualidade dos dados, problemas decorrentes de documentação insuficiente e quaisquer preocupações relativas às medidas de mitigação.
- ▶ Registe quaisquer problemas relacionados com dados sobre desigualdade e discriminação, quaisquer preocupações relativas às medidas de mitigação e - quando disponível - uma argumentação sobre a forma como estas medidas conduziriam a um tratamento desigual no caso em apreço.
- ▶ Registe quaisquer indicadores de incumprimento das disposições do Regulamento sobre a IA relevantes em matéria de dados.

3.6. Testes e avaliação

Os resultados dos testes e da avaliação podem fornecer informações valiosas para determinar se ocorreu discriminação. A questão central aqui é saber se o sistema algorítmico produz resultados desiguais para diferentes grupos de pessoas. Uma forma de demonstrar isto é através de estatísticas sobre os resultados do sistema.

Quando estiverem disponíveis dados estatísticos relativos à igualdade, esses dados devem ser avaliados quanto à sua validade e fiabilidade (ver abaixo). Por conseguinte, é importante analisar a validade e a fiabilidade dos dados utilizados para calcular estas estatísticas. Por conseguinte, esta secção deve ser lida em conjunto com a secção 3.5. [Dados de treino, teste e validação](#).

Neste passo, conhecimentos especializados técnicos e setoriais podem revelar-se úteis.

Para analisar os resultados de diferentes grupos com características protegidas distintas, é necessário que existam dados disponíveis sobre essas características protegidas. Por exemplo, para verificar se um sistema produz resultados diferentes para homens e mulheres, é necessário saber, para cada uma das pessoas titulares dos dados de teste, quem é homem e quem é mulher. Estes dados podem nem sempre estar disponíveis. Neste caso, os testes devem centrar-se nas características que estão disponíveis, incluindo aquelas que estão ou podem estar relacionadas com atributos protegidos. Por exemplo, pode não haver dados disponíveis sobre a origem étnica, mas sim sobre a nacionalidade; ou, no caso das imagens faciais, pode não haver dados disponíveis sobre pessoas sujeitas a discriminação racial, mas o valor da cor dessas imagens faciais poderia ser utilizado.

Obtenção de dados estatísticos (adicionais)

Quando não existem dados estatísticos disponíveis ou estes são insuficientes para avaliar a discriminação algorítmica, existem algumas opções que podem ajudar a obter dados estatísticos (adicionais).

Avaliação e testes realizados pela AFM

Caso um OI não consiga determinar se ocorreu uma violação de direitos ao abrigo do direito da União, o n.º 3 do artigo 77.º do Regulamento sobre a IA permite que o OI apresente um “pedido fundamentado à autoridade de fiscalização do mercado para organizar a testagem do sistema com recurso a meios técnicos”. O OI deve estar estreitamente envolvido nos testes.

O Considerando 157 deixa claro que o procedimento previsto no artigo 77.º deve ser aplicado aos sistemas de IA de risco elevado que representem um risco para os direitos fundamentais, aos sistemas proibidos colocados no mercado (artigo 6.º), colocados em serviço ou utilizados em violação das práticas proibidas previstas no regulamento (artigo 5.º) e aos sistemas de IA, quer sejam de risco elevado ou não, que tenham sido disponibilizados em violação dos requisitos de transparência do regulamento e que representem um risco (artigo 6.º, n.º 4, e artigo 50.º).

Testes realizados pelo OI ou em colaboração com entidades terceiras

Os organismos para a igualdade podem recolher os seus próprios dados relativos à igualdade no âmbito do exercício das suas funções de monitorização e de outras atribuições previstas nas diretivas e regulamentos relativos à discriminação e/ou aos organismos para a igualdade, ou de outra forma. No entanto, poderá ser necessário ter cuidado ao utilizar estes dados, uma vez que existe o risco de que não sejam considerados independentes no exercício de uma função contenciosa. De momento, não é claro de que forma as obrigações de confidencialidade previstas no artigo 78.º do Regulamento sobre a IA afetariam a utilização de informações obtidas para um determinado fim em processos judiciais civis (ver os processos penais e administrativos explicitamente referidos).

Analise se as provas em que pretende basear-se foram obtidas:

1. em resultado do exercício, por parte do organismo para a igualdade, das suas funções de decisão independente e imparcial ou das suas funções de monitorização e tratamento de dados; ou
2. para efeitos de litígio.

Se os dados tivessem sido criados para o ponto 1., a independência desses dados poderia ser posta em causa. Conforme referido pela Equinet:

Quando um organismo para a igualdade intenta uma ação judicial com base nos seus próprios dados, o tribunal poderia, em teoria, ter dificuldade em considerar esses dados como externos e independentes. Mais ainda, quando um organismo para a igualdade decide sobre casos, baseando-se (em parte) nos seus próprios dados relativos à igualdade, as partes envolvidas num processo e outras observadoras e observadores poderiam questionar tal prática com base em, pelo menos, dois fundamentos: será que o organismo é um árbitro imparcial se identificar e utilizar proativamente provas que favoreçam a alegada vítima; e essas provas são credíveis se tiverem sido produzidas pelo próprio organismo, que, por definição, é a favor da igualdade e das vítimas. Essas potenciais questões (percebidas) relacionadas com o direito a um julgamento justo e

a igualdade de armas poderiam afetar a credibilidade global de um organismo para a igualdade na sociedade, incluindo a sua função de apresentação de relatórios. (Ilieva 2024)

Análises estatísticas do sistema algorítmico

Nos casos em que o sistema algorítmico e os dados relevantes estejam à disposição do OI, este poderá realizar a sua própria avaliação estatística. Tanto os parâmetros de equidade como os métodos de aplicação foram implementados numa série de conjuntos de ferramentas de código aberto dedicadas à equidade. Estes conjuntos de ferramentas podem ser utilizados para avaliar as lacunas de desempenho em sistemas algorítmicos ou nos conjuntos de dados que lhes são disponibilizados. Entre os exemplos mais utilizados contam-se o IBM AI Fairness 360 e o Microsoft Fairlearn, mas existem muitos outros disponíveis. Não existe um conjunto de ferramentas específico recomendado, uma vez que cada um tem as suas próprias vantagens e desvantagens (Mittelstadt 2024).

Testes de simulação

Os testes de “simulação” também podem ser utilizados para obter provas de discriminação. O teste de simulação é um método experimental em que se formam pares de participantes que diferem apenas numa característica protegida, com o objetivo de testar as diferenças no tratamento.

Em alguns contextos, como o recrutamento algorítmico, uma opção viável consiste em recolher dados estatísticos sobre um sistema algorítmico específico através de testes de simulação (de discriminação). Em vários países, incluindo o Reino Unido, os Países Baixos, a França, a Dinamarca, a Finlândia e a Suécia, os testes de simulação foram reconhecidos como uma forma válida de prova (Comissão Europeia 2019). Os testes de simulação em grande escala também podem fornecer dados estatísticos e têm sido aplicados em muitos contextos diferentes, tais como o acesso ao emprego, à habitação e a outros tipos de bens e serviços. Os resultados dos testes são considerados provas admissíveis em vários países da UE. Para garantir resultados fiáveis, o OI poderá ter de colaborar com entidades especializadas na realização dos testes (Makkonen 2016).

Colaboração com institutos de estatística/utilização de estatísticas gerais

As estatísticas gerais podem ser utilizadas para argumentar que a utilização de proxies conduz a uma diferença de tratamento. Por exemplo, no caso neerlandês das verificações de bolsa de estudos universitária:

- ▶ o algoritmo diferenciou consoante o nível de escolaridade;
- ▶ de acordo com as estatísticas gerais do Instituto Nacional de Estatística dos Países Baixos, estudantes com origem migratória não ocidental estão sobrerrepresentados nos níveis de ensino mais baixos: o número de estudantes com origem migratória não ocidental é cerca do dobro do que seria de esperar, em comparação com o total de estudantes ([StatLine – Mbo; studenten, niveau, leerweg, migratie 2005/'06-2021/'22](#));

- consequentemente, sem aceder a dados específicos sobre o percurso educativo de cada estudante, a utilização do percurso educativo nos sistemas algorítmicos conduz a um tratamento desigual.

Abordagem dos tribunais aos dados estatísticos

Sobre a necessidade de dados estatísticos

As estatísticas, por si só, não revelam necessariamente a existência de discriminação ou de uma prática discriminatória (*Hugh Jordan contra o Reino Unido*, Recurso n.º 24746/94, Tribunal Europeu dos Direitos Humanos).⁵⁴ Estas constituem algumas das formas de prova relevantes que podem ser utilizadas para estabelecer ou refutar um caso *prima facie* de discriminação direta ou indireta. De um modo geral, os tribunais podem estar mais inclinados a aceitar provas estatísticas apresentadas pelas pessoas queixosas para estabelecer um caso *prima facie* de discriminação direta do que a basear-se em tais provas apresentadas pelas partes inquiridas para o refutar, o que reflete o desequilíbrio de informação entre as partes e as dificuldades reconhecidas que as pessoas queixosas enfrentam ao fundamentar as alegações de discriminação (Makkonen 2007). Caberá ao tribunal nacional avaliar se as estatísticas disponíveis são “válidas” e podem ser tidas em conta (ver Enderby, Caso C-127/92, parágrafo 16).

Dados estatísticos e discriminação direta

Num caso de discriminação direta, as estatísticas podem revelar a existência de um padrão discriminatório e, por conseguinte, constituir prova de discriminação direta no âmbito de uma queixa individual. No entanto, o recurso a provas estatísticas não é, normalmente, necessário para efeitos de apresentação de um caso *prima facie* de discriminação direta.

Dados estatísticos e discriminação indireta

Os dados estatísticos são particularmente úteis no caso de discriminação indireta, em que a pessoa queixosa pode recorrer às estatísticas para demonstrar que a aplicação de uma prática ou regra aparentemente neutra tem um efeito ou impacto desproporcional num grupo específico de pessoas, em comparação com outras que se encontram numa situação semelhante (FRA 2018: 242).

Em particular, “sempre que uma pessoa requerente consiga demonstrar, com base em estatísticas oficiais incontestáveis, a existência de uma indicação *prima facie* de que uma regra específica - embora formulada de forma neutra - afeta, de facto, uma percentagem claramente superior de mulheres do que de homens, cabe ao Governo requerido demonstrar que tal se deve a fatores objetivos não relacionados com qualquer discriminação com base no sexo” (*Hoogendijk contra os Países Baixos*, 2005).

54 As estatísticas revelaram uma diferença entre o número de pessoas mortas de diferentes religiões, mas não indicaram se essas mortes foram ilegais ou resultaram do uso excessivo da força por parte de membros das forças de segurança (parágrafo 154).

Não foi definido um limiar rigoroso, mas normalmente é necessário atingir um valor substancial para demonstrar um impacto diferencial, ou seja, um “número muito superior” (Ingrid Rinner-Kühn, 1989) ou “uma percentagem consideravelmente mais baixa” (Helga Nimz, 1991, e Maria Kowalska, 1990) ou “muito mais” (M. A. De Weerd, 1994), embora a apresentação de dados estatísticos para provar a discriminação indireta não seja um requisito formal (ver *D.H. e outros contra a República Checa*, 2007, parágrafo 188).

No entanto, não são necessários dados estatísticos precisos, especialmente se a parte que alega ter sido vítima de discriminação não tiver acesso a essas estatísticas ou tiver dificuldade em aceder às mesmas (*Minoo Schuch-Ghannadan*, 2019).

Recurso a outros dados e provas

Pode ser suficiente apresentar provas das práticas ou crenças de entidades terceiras em relação às pessoas que pertencem à mesma categoria protegida. Por exemplo, a prática de colocar crianças em turmas separadas com base no seu domínio insuficiente do croata só era aplicada a estudantes de origem Roma, o que deu origem a uma presunção de tratamento diferenciado, apesar de as estatísticas não terem conseguido comprovar a existência de discriminação. O Tribunal Europeu dos Direitos Humanos deixou claro que “a discriminação indireta pode ser provada sem recurso a dados estatísticos” (*Oršuš e outros contra a Croácia*, 2010).

Nos casos que envolvem sistemas algorítmicos, outras informações factuais e provas podem também ser suficientes para estabelecer a existência de discriminação *prima facie*. Por exemplo, no caso da Deliveroo, o tribunal não exigiu testes estatísticos exaustivos nem análises complexas de dados. Em vez disso, a conceção do sistema em si - tal como reconstruída a um nível básico a partir da informação disponível, nomeadamente cláusulas contratuais, perguntas frequentes da plataforma, comunicações externas e internas da parte inquirida e testemunhos de pessoas singulares afetadas -, combinada com uma avaliação dos seus efeitos previsíveis, foi suficiente para demonstrar uma desvantagem desproporcionada e para estabelecer uma discriminação *prima facie*.

Avaliação dos dados estatísticos relativos à igualdade por parte da parte inquirida

Para efeitos da legislação em matéria de igualdade, os dados estatísticos devem ser válidos e fiáveis.

Os testes de validade e fiabilidade devem ser aplicados ao longo de todo o processo. O seguinte processo em três passos poderá ser útil.

- ▶ A abordagem adotada pela entidade prestadora ou por quem é responsável pela implantação nos testes e na avaliação baseou-se ou produziu dados estatísticos válidos e fiáveis?
- ▶ As suas evidências estatísticas, que visam contestar a parte inquirida, são válidas e fiáveis?
- ▶ Alguma prova estatística apresentada em refutação é válida e fiável?

Para que os dados estatísticos sejam considerados “válidos”, devem ser cumpridos os seguintes critérios.

- ▶ Parecerem ser, em geral, significativos.
- ▶ Abrangerem um número suficiente de pessoas.
- ▶ Identificarem fenómenos que não sejam fortuitos nem de curta duração.
- ▶ No seu conjunto, serem “relevantes e suficientes”.

A fiabilidade dos dados estatísticos implica a estabilidade ou a consistência da medição ou do teste aplicado. Uma medida de discriminação, por exemplo, é fiável na medida em que o procedimento de medição produza os mesmos resultados em testes repetidos. Por exemplo, se se medir o número de incidentes relacionados com a igualdade comunicados por ano, mas o número de organismos competentes (para a igualdade) for variando ao longo do tempo, tal terá um efeito negativo na fiabilidade deste indicador e afetará também a sua comparabilidade ao longo do tempo. Nenhuma medida é fiável; a fiabilidade é, portanto, sempre uma questão de grau.⁵⁵

Escolha dos parâmetros de igualdade

Na ciência de dados, foram identificados vários parâmetros para avaliar diferentes conceitos do que é justo. Estes parâmetros não foram definidos com base na legislação de não discriminação e a sobreposição entre os indicadores de equidade no domínio da ciência de dados e da IA e os conceitos de igualdade nem sempre é clara (Weerts et al. 2023). Infelizmente, é matematicamente impossível criar um sistema que seja justo de acordo com todos os parâmetros técnicos.

Por conseguinte, é fundamental determinar o que significa uma diferença de tratamento e uma desvantagem específica (como parte integrante da discriminação) no contexto do caso em apreço e escolher os parâmetros que melhor correspondam a esta definição. Note-se que o simples facto de apresentar qualquer parâmetro de equidade que demonstre que o sistema é “justo” segundo esse parâmetro não significa, por si só, que o sistema resulte num tratamento igualitário. Nos casos em que houver injustiça, será importante analisar por que razão se optou por utilizar esse conjunto de parâmetros de igualdade e que medidas foram tomadas para resolver a desigualdade daí resultante.

A paridade demográfica mede se a probabilidade de uma determinada previsão é a mesma para dois grupos. Este parâmetro é mais relevante quando um resultado é menos vantajoso do que outros resultados para as pessoas envolvidas. Isto reflete melhor o conceito de tratamento desigual em exemplos como a previsão de fraude (quando um grupo é suspeito de fraude com mais frequência do que o outro) ou o recrutamento (quando um grupo é selecionado para uma entrevista com mais frequência do que o outro). Em muitos casos, a paridade demográfica é o parâmetro relevante, a menos que existam razões convincentes para recorrer a outro parâmetro. Note-se que a paridade demográfica também é, por vezes, designada por independência, equidade de grupo, paridade estatística, impacto desigual, taxa de seleção igual ou taxa de aceitação igual.

55 Ver Comissão Europeia 2021: 20; Enderby, 1993, n.º 17; Seymour-Smith, 1999, parágrafo 62. Quanto aos requisitos gerais relativos às estatísticas em processos de não discriminação, ver *Enderby contra Frenchay Health Authority e Secretary of State for Health*, parágrafo 17.

Outros parâmetros relevantes baseiam-se nos erros do sistema e verificam se os sistemas geram mais erros num grupo do que no outro. Este tipo de parâmetro é mais relevante quando os danos resultam, na sua grande maioria, de erros nos sistemas e não do próprio resultado. Os exemplos em que os parâmetros baseados no erro são mais relevantes são o reconhecimento facial e os exames de diagnóstico na medicina. Consulte a tabela 6 abaixo para obter uma visão geral dos parâmetros potencialmente relevantes.

É improvável que uma abordagem única para os testes seja suficiente. Em vez disso, será importante ter em conta tanto os modelos estatísticos utilizados e as suas limitações, como as circunstâncias que os rodeiam, tais como a organização responsável pela tomada de decisões e os processos por ela adotados (Barocas et al. 2023). Como tal, os “números” sem contexto terão um significado insuficiente para serem válidos ou fiáveis.

Mesmo quando a paridade demográfica é escolhida como parâmetro principal, é aconselhável ter também em conta um parâmetro que tenha em consideração os erros. As entidades prestadoras são obrigadas a definir um “nível geral esperado de exatidão” para grupos específicos de pessoas (Regulamento sobre a IA, Anexo IV, n.º 3).

As estatísticas sobre a igualdade podem ser apresentadas sob a forma de uma razão ou de parâmetros distintos entre grupos. Seguem-se alguns exemplos.

- ▶ As estatísticas de paridade demográfica num contexto de recrutamento podem ser expressas da seguinte forma: Após a seleção automática dos currículos, 25% das pessoas que se candidatam do sexo masculino são convidadas para uma entrevista e 15% das pessoas que se candidatam do sexo feminino são convidadas. Isto também pode ser expresso como uma razão: $0,15/0,25 = 0,6$.
- ▶ A igualdade de oportunidades no rastreio do cancro pode ser expressa da seguinte forma: 75% dos homens com cancro são detetados pela ferramenta de rastreio e 65% das mulheres com cancro são detetadas pela ferramenta de rastreio. Isto também pode ser expresso como uma razão: $0,15/0,25 = 0,87$.

Tabela 6. Descrição dos parâmetros de equidade

(adaptado com autorização de Mittelstadt 2023)

Parâmetro	Descrição	Aplicável quando	Exemplo
Paridade demográfica	Os diferentes grupos devem apresentar a mesma taxa de resultados positivos.	▶ Situações em que um determinado resultado em si (e não os erros) é desfavorável. ▶ Situações em que se prevê que os dados históricos sejam prejudiciais.	Recrutamento, aprovação de empréstimos, deteção de fraudes, acesso à educação.

Parâmetro	Descrição	Aplicável quando	Exemplo
Paridade demográfica	A paridade demográfica pode ser designada por independência, equidade de grupo, paridade estatística, impacto desigual, taxa de seleção igual ou taxa de aceitação igual.	► Situação em que não existem rótulos fiáveis (não existe um padrão de referência consensual).	
Igualdade de oportunidades	Os diferentes grupos devem apresentar a mesma taxa de falsos negativos. Também poderia ser designada por equilíbrio da taxa de erros de falso negativo.	► Situações em que o dano predominante resulta de falsos negativos. ► Existem rótulos fiáveis (padrão de referência consensual).	Rastreo de doenças.
Paridade preditiva	A percentagem de falsos positivos, entre todos os resultados positivos, deve ser a mesma para os diferentes grupos. Também pode ser designada por teste de resultados ou paridade do valor preditivo positivo.	► Situações em que o dano predominante resulta de falsos positivos. ► Existem rótulos fiáveis (padrão de referência consensual).	Reconhecimento facial pela polícia para identificar uma pessoa procurada.
Equilíbrio da taxa de falsos positivos	Os diferentes grupos devem apresentar a mesma taxa de falsos positivos. Também pode ser designada por equidade preditiva.	► Situações em que o dano predominante resulta de falsos positivos. ► Existem rótulos fiáveis (padrão de referência consensual).	Reconhecimento facial pela polícia para identificar uma pessoa procurada.

Parâmetro	Descrição	Aplicável quando	Exemplo
Probabilidades equilibradas	As taxas de verdadeiros positivos e falsos positivos devem ser iguais para os diferentes grupos. Também poderia ser designada por igualdade na exatidão dos procedimentos condicionais e tratamento desigual.	► Situações em que se deve ter em conta tanto o dano resultante de falsos positivos como o resultante de falsos negativos. ► Existem rótulos fiáveis (padrão de referência consensual).	Tratamento de uma doença através da realização de uma cirurgia de risco.

Avaliação das estatísticas fornecidas pela parte inquirida

Para avaliar a validade dos parâmetros estatísticos de igualdade, os Ols devem ter em conta, pelo menos, três aspetos.

1. De um modo geral, a qualidade e os enviesamentos dos dados utilizados para calcular o parâmetro (ver passo 3.5).
2. A conceção do parâmetro e a escolha dos grupos de comparação.

Ao analisar a forma como a entidade prestadora de um sistema identificou e avaliou eventuais lacunas de desempenho, os Ols devem prestar especial atenção à forma como foi tomada a decisão de proceder à avaliação e aos grupos de pessoas que estão a ser comparados. Esta é uma decisão importante no contexto da legislação em matéria de não discriminação, em que a definição de grupos “desfavorecidos” e “de comparação” adequados é, muitas vezes, fundamental. (Mittelstadt 2024). A escolha dos grupos pode (deliberadamente) ocultar resultados desiguais no mundo real.

Recomenda-se aos Ols que:

- analisem quais seriam os grupos “desfavorecidos” e “de comparação” adequados, antes de analisar as estatísticas da parte inquirida;
- avaliem se a parte inquirida escolheu e definiu os mesmos grupos e, caso contrário, o Ol deverá analisar que informações são acrescentadas ou perdidas nas escolhas da parte inquirida;
- considerem os grupos interseccionais, uma vez que centrar-se exclusivamente em grupos definidos por uma única característica oculta as desigualdades interseccionais;
- para compreender os grupos de comparação escolhidos pela parte inquirida, analisem as explicações por ela fornecidas, em especial qualquer informação sobre até que ponto uma variação nos dados pessoais tidos em conta teria conduzido a um resultado diferente;

- nos casos em que a parte inquirida não tenha prestado informações sobre parâmetros de equidade relevantes ou tenha definido de forma restrita os grupos afetados, considerem a possibilidade de obter dados estatísticos adicionais (ver o quadro sobre a obtenção de dados estatísticos (adicionais) acima) (Mittelstadt 2024).

Os parâmetros estatísticos de igualdade fazem frequentemente parte de relatórios de desempenho mais abrangentes que incluem uma variedade de resultados de testes que medem vários aspetos do desempenho de um sistema, tais como a exatidão (a frequência com que o sistema faz a previsão correta) e a robustez (resiliência face a erros, comportamentos imprevistos e alterações do mundo real (desvio)). É importante que os OIs compreendam o desempenho em geral, uma vez que o desempenho do sistema é extremamente relevante na avaliação da discriminação algorítmica, nomeadamente quando se considera uma potencial justificação objetiva (ver [passo 3.8](#)), em que as questões centrais envolverão determinar se o sistema é adequado, apropriado e necessário.

1. Relevância dos parâmetros para o sistema atual, tal como é aplicado na prática.

Os parâmetros devem refletir o sistema algorítmico atual. Os testes realizados podem ter ficado desatualizados ou o processo relacionado com o sistema pode ter sofrido alterações (por exemplo, o sistema aplica uma política governamental e essa política foi alterada).

É importante ter em conta que os parâmetros apresentados devem refletir o estado do sistema após a aplicação de quaisquer medidas de mitigação destinadas a “eliminar enviesamentos” ou a prevenir a discriminação. Se estas medidas forem realizadas manualmente, os OIs devem assegurar que as estatísticas refletem o resultado após essa intervenção manual.

Sempre que um sistema de IA de risco elevado tenha obtido um certificado de conformidade na sequência de uma avaliação, presume-se que cumpre os requisitos em matéria de dados previstos no n.º 4 do artigo 10.º do Regulamento sobre a IA, nomeadamente “devem ter em conta, na medida do necessário para a finalidade prevista, as características ou os elementos que são idiossincráticos do enquadramento geográfico, contextual, comportamental ou funcional específico no qual o sistema de IA de risco elevado se destina a ser utilizado”.

É provável que estas considerações orientem a aplicação do teste de “validade” (ver mais informações sobre dados estatísticos no passo 3.6), mas é importante referir que esta presunção pode ser refutada. Os organismos para a igualdade poderão querer analisar, em particular, se os dados utilizados cumprem, de facto, estes requisitos para a utilização específica do sistema de IA. Se o sistema estiver a ser utilizado para fins diferentes daqueles a que se destina, esta presunção não se aplicará.

Questões a ter em conta

Sobre os testes de desempenho geral

- Que aspetos do desempenho foram testados?
- Como e onde foi registado o desempenho do sistema junto de pessoas e grupos de pessoas?

- Estes valores serão atualizados ao longo do ciclo de vida do sistema? Se sim, como?
- ▶ Que potenciais impactos sobre pessoas e grupos de pessoas foram tidos em conta na realização dos testes de desempenho?
- ▶ Foi escolhida alguma forma de erro como ponto central dos testes (como falsos positivos ou falsos negativos)?
- ▶ Que métricas foram utilizadas nos testes de desempenho?
- ▶ Foram elaboradas matrizes de confusão no âmbito dos testes de desempenho?
- ▶ Como foram validados os resultados dos testes?
- ▶ Os dados utilizados para realizar os testes de desempenho são suficientemente representativos, relevantes e medidos de forma precisa e adequada (ver passo 3.5. [Dados de treino, teste e validação](#))?
- ▶ Os testes de desempenho realizados pela parte inquirida cumprem os testes de validade e fiabilidade?

Dados estatísticos relativos à igualdade

- ▶ Que (tipos de) dados estatísticos relativos à igualdade, parâmetros de equidade ou testes de enviesamento foram utilizados?
 - Os parâmetros escolhidos pela parte inquirida refletem a igualdade de tratamento no contexto específico? (Normalmente, paridade demográfica, a menos que existam justificações claras para a utilização de outros parâmetros; ver a tabela 6 acima).
 - Nos casos em que existem parâmetros baseados em erros, foram consideradas as mesmas formas de erro que nos testes de desempenho normais? (Por exemplo, quando os testes de desempenho regulares utilizavam um parâmetro centrado nos falsos positivos, os testes de igualdade faziam o mesmo?) Ao verificar a igualdade com base no desempenho, é lógico que o parâmetro de desempenho mais relevante deva também ser utilizado para essa verificação de igualdade. A escolha, sem justificação, de um parâmetro diferente poderá indicar uma omissão no teste da igualdade.
 - Qual é a justificação ou o fundamento com base no qual estes foram escolhidos?
 - Foram consideradas e/ou rejeitadas outras opções? Se sim, porquê/por que não?
 - A variedade de testes utilizados, que abrangiam diferentes características protegidas, foi suficientemente ampla para identificar diferentes tipos de potencial discriminação ou impactos que afetam diferentes grupos (interseccionais)?
 - Foram escolhidos grupos de “comparação” relevantes para cada teste? Estas considerações estão incluídas na documentação técnica do sistema?
- ▶ Foram utilizados quaisquer (tipos de) métodos de garantia da equidade ou de eliminação de enviesamento?
 - Qual é a justificação ou o fundamento com base no qual estes foram escolhidos?

- Foram consideradas e/ou rejeitadas outras opções? Se sim, porquê/por que não?
- Estas considerações estão incluídas na documentação técnica do sistema?
- Que benefícios e prejuízos resultaram da aplicação da equidade ou da eliminação de enviesamento?
 - Que grupos de pessoas é que isto afetou ou irá afetar?
 - Foram investigados os efeitos secundários no que diz respeito à igualdade de tratamento de outros grupos?
- Como foram validados os resultados dos testes?
- Os dados utilizados para calcular as estatísticas são suficientemente representativos e relevantes, e foram medidos de forma precisa e adequada (ver passo 3.5. [Dados de treino, teste e validação](#))?
- Os dados estatísticos fornecidos pela parte inquirida cumprem os testes de validade e fiabilidade?

Possíveis fontes de informação para avaliar os dados estatísticos relativos à igualdade

Pessoa queixosa

RGPD, artigo 15.º, n.º 1, alínea h), informações significativas sobre a lógica envolvida

Parte inquirida

Da entidade prestadora

Regulamento sobre a IA da UE, artigo 10.º, dados e governação dos dados

Regulamento sobre a IA da UE, artigo 11.º, documentação técnica (Anexo IV, n.º 2, alínea g)):

- “os procedimentos de validação e testagem aplicados, incluindo informações sobre os dados de validação e de teste utilizados e as principais características desses dados; os parâmetros utilizados para aferir a exatidão, a solidez e a conformidade com outros requisitos aplicáveis estabelecidos no capítulo III, secção 2, bem como potenciais impactos discriminatórios; registos dos testes e todos os relatórios de teste datados e assinados pelas pessoas responsáveis, inclusive no respeitante às alterações predeterminadas a que se refere a alínea f)”.

Regulamento sobre a IA da UE, artigo 11.º, registos

Outras informações que possam ser solicitadas à parte inquirida:

- acesso ao sistema
- conjuntos de dados de exemplo (sintéticos)
- algum relatório sobre o desempenho ou a fiabilidade do sistema, incluindo matrizes de erros

- ▶ informações sobre o tipo de testes e a metodologia utilizada, incluindo as eventuais normas (harmonizadas) aplicadas
 - ▶ quaisquer relatórios sobre testes de enviesamento e equidade realizados
 - ▶ informações sobre o tipo de testes e a metodologia utilizada, incluindo as eventuais normas (harmonizadas) aplicadas
 - ▶ AIDH ou AIDF, AIPD, avaliação de impacto em matéria de ética ou dos direitos da criança voluntárias
 - ▶ quaisquer outras avaliações (de risco) partilhadas pela parte inquirida
 - ▶ pedidos ao abrigo da lei da liberdade de informação.
-

Indicadores de discriminação

- ▶ Existem discrepâncias nos resultados ou erros entre grupos de pessoas com características protegidas, com base nos parâmetros mais relevantes que refletem a igualdade de tratamento no caso específico.
- ▶ Os parâmetros mais relevantes que refletem a igualdade de tratamento neste caso específico não estão disponíveis ou são aplicados parâmetros irrelevantes.
- ▶ Existem discrepâncias nos resultados ou erros entre grupos de pessoas com características protegidas, com base noutros parâmetros (que não o parâmetro que melhor reflete a igualdade de tratamento no caso específico).
- ▶ Nem todos os grupos afetados foram incluídos, ou os grupos afetados foram definidos de forma demasiado restrita, sem ter em conta a discriminação interseccional.
- ▶ Foram identificados os grupos corretos e aplicados os parâmetros relevantes, mas as conclusões não resistem a uma análise mais aprofundada, por exemplo, devido a problemas com os dados.
- ▶ Apresenta apenas um parâmetro testado, em vez dos resultados de vários parâmetros de equidade (tais como precisão, revogação e taxas de erro⁵⁶). Pode ser necessário realizar testes com vários parâmetros para identificar diferentes tipos de lacunas de desempenho.

Indicadores cumulativos de discriminação

Todos os indicadores acima referidos podem atuar de forma cumulativa; eis alguns exemplos.

- ▶ Risco de discriminação identificado pela entidade prestadora/responsável pela implantação (ver passo 3.3.), mas os testes não abrangeram o conjunto

56 Na análise de dados, podem ser utilizados diferentes parâmetros para refletir diferentes aspetos do desempenho de um sistema. Por exemplo, a precisão centra-se na exatidão das previsões positivas (evitando falsos alarmes), enquanto a revogação mede a capacidade de detetar todos os casos positivos reais (evitando eventos perdidos).

completo de pessoas singulares e/ou grupos em risco de sofrer danos – ter em conta, em particular, os proxies, a discriminação múltipla e a discriminação interseccional. Por exemplo, o teste incidiu sobre a discriminação com base no sexo, mas não sobre a discriminação com base na raça ou na etnia, embora tenha sido identificado o risco de discriminação racial.

- ▶ (Risco de) discriminação identificado por entidades terceiras (ver passo 3.1), mas os testes não abrangeram o conjunto completo de pessoas singulares e/ou grupos em risco de sofrerem danos - ter em conta, em particular, os proxies, a discriminação múltipla e a discriminação interseccional. Por exemplo, o teste incidiu sobre a discriminação com base no sexo, mas não sobre a discriminação com base na raça ou na etnia, ao passo que, em casos semelhantes já ocorridos, as pessoas foram prejudicadas com base na raça e na gravidez.
- ▶ Os critérios de entrada estão intimamente relacionados com atributos protegidos ou são utilizados proxies nos algoritmos (ver passo 3.3) e não são realizados testes para verificar se os requisitos de igualdade de tratamento são cumpridos em relação ao grupo protegido.

- ▶ Registe quaisquer lacunas ao nível dos resultados ou do tratamento, tal como reveladas nas estatísticas.
- ▶ Registe quaisquer problemas relacionados com as estatísticas apresentadas (tais como parâmetro incorreto ou problemas com os dados).
- ▶ Registe quaisquer lacunas nos testes.
- ▶ Combine os resultados deste passo com os do passo anterior para determinar se, em conjunto, é possível argumentar a existência de um caso *prima facie* de discriminação e/ou se a parte inquirida conseguiu refutar a presunção ou justificar a discriminação (se estiver a analisar a justificação, consulte também o passo 3.4. para ter em conta o objetivo do sistema).
- ▶ Registe a conclusão.

Exemplo: Smart Check de Amesterdão

Este modelo foi concebido para analisar os pedidos de prestações sociais e identificar aqueles que apresentam maior probabilidade de conter erros graves, assinalá-los e encaminhar os casos para um departamento de investigação para uma análise mais aprofundada. O objetivo era reduzir o número de pessoas identificadas para investigação.

Foram consideradas quinze características, incluindo uma variedade de fatores, tais como se a pessoa requerente já tinha solicitado ou recebido prestações sociais anteriormente, o número de moradas que possuía e o valor total dos seus bens, para determinar uma pontuação de risco. Este evitou deliberadamente recorrer a motivos protegidos e tentou evitar “proxies”.

Segundo os autores, “este foi treinado com base num conjunto de dados que abrange 3.400 investigações anteriores. Isto levou ao risco de incorporar enviesamentos históricos; por exemplo, se as pessoas responsáveis tivessem, historicamente, cometido taxas mais elevadas de erros com um determinado grupo étnico, o modelo poderia aprender, de forma errada, a prever que esse grupo comete fraude com maior frequência”.

As autoridades de Amesterdão adotaram uma definição de equidade baseada na distribuição equitativa do peso das investigações indevidas entre os diferentes grupos demográficos. Além disso, realizou um amplo processo de consulta. Todos os grupos de partes interessadas, desde a Autoridade de Proteção de Dados de Amesterdão até às empresas de consultoria externas, aprovaram o projeto, com exceção do grupo que representa as pessoas diretamente afetadas (beneficiárias/os).

Apesar disso, o sistema foi submetido a testes. O modelo inicial tinha duas vezes mais probabilidades de sinalizar erroneamente pessoas que se candidatam não neerlandesas e quase duas vezes mais probabilidades de sinalizar uma pessoa que se candidata com nacionalidade não ocidental do que uma com nacionalidade ocidental. Era também 14% mais provável que indicasse indevidamente homens para investigação.

A cidade de Amesterdão também analisou os dados recolhidos pelas pessoas responsáveis. Nesse processo, descobriram que os humanos tinham mais tendência a assinalar erroneamente as cidadãs e cidadãos neerlandeses e mulheres.

Devido à existência de um enviesamento, a equipa tentou recorrer à reponderação dos dados de treino para resolver o problema. Isto significava que as pessoas que se candidatavam com nacionalidade não ocidental, em relação às quais se considerava que tinham cometido erros significativos nas suas candidaturas, era atribuído menos peso nos dados, enquanto às pessoas que se candidatavam com nacionalidade ocidental era atribuído mais peso. Após a reponderação do modelo, as cidadãs e cidadãos neerlandeses e as cidadãs e cidadãos não neerlandeses passaram a ter a mesma probabilidade de serem erroneamente identificados.

O problema com a reponderação dos dados era que, embora pudesse reduzir a equidade em relação às pessoas de origem migrante, não garantiria a equidade entre identidades que se cruzam.

No entanto, o sistema foi implementado de forma limitada para ser utilizado com pessoas candidatas reais. O seu desempenho deveria ser avaliado com base em dois critérios fundamentais: i) seria capaz de analisar as pessoas que se candidatam sem enviesamento?; ii) seria capaz de detetar fraudes na prestação social de forma mais eficaz e justa do que as pessoas responsáveis humanas?

Em vez de identificar menos pessoas que se candidatam para investigação, identificou mais. E não era melhor do que um ser humano a identificar aquelas que exigiam uma análise mais aprofundada. Além disso, apesar da reponderação, o sistema passou a assinalar erroneamente as pessoas que se candidatam com nacionalidade neerlandesa e as mulheres. Além disso, as pessoas requerentes de prestações sociais com filhas/filhos também eram mais propensas a serem alvo de investigação.

No final, o projeto não teve continuidade.

O texto acima é um resumo do artigo “Por dentro da experiência de alto risco de Amesterdão para criar uma IA social justa”, de 11 de junho de 2025, publicado na MIT Technology Review, Lighthouse Reports and Trouw, E. G., Geiger G. and Braun J-C. Para informações mais detalhadas, consulte a Lighthouse Reports 2025.

3.7. Avaliar se as provas são suficientes para fundamentar um caso *prima facie* de discriminação envolvendo um sistema de IA ou algorítmico

- ▶ Analise toda a informação e as respostas às perguntas do passo 3 para avaliar se foi demonstrada a existência de um caso *prima facie* de discriminação. Utilize os indicadores de discriminação como orientação.
- ▶ Nesta etapa, parte-se do princípio de que não existe uma explicação adequada para os factos que demonstrem um caso *prima facie* (pode haver; no entanto, tal seria relevante para a avaliação da defesa da parte inquirida (ver 3.8 abaixo)).
- ▶ Da mesma forma, a falta de provas ou a falta de transparência relativamente a um sistema não deve impedir que um processo seja instaurado ou prosseguido nesta etapa. Recorde-se que, no [Passo 1](#), concluiu-se que a rejeição precoce de reivindicações em que existe um desequilíbrio de informação era provavelmente inadequada: ver [1.4. Continuação do caso](#)

Poderá ter de considerar todos ou alguns dos seguintes aspetos.

- ▶ Quem é a vítima e quais são os motivos de proteção em causa?
- ▶ Qual é o comparador adequado? Por que razão foi escolhido este comparador?
- ▶ Houve discriminação direta ou indireta?
- ▶ Existem formas múltiplas ou sobrepostas de discriminação?
- ▶ Identificou algum caso de discriminação por proxy?
- ▶ Por que razão ocorreu a discriminação (causalidade)? Considere, por exemplo, se a discriminação ocorreu devido ao objetivo do sistema, ao seu desenvolvimento, à utilização de dados no âmbito do sistema ou porque o sistema não está a ser utilizado para o fim a que se destina ou está a ser utilizado de forma incorreta por quem é responsável pela implantação.

No que diz respeito à discriminação indireta, considere também o seguinte.

- ▶ Qual é a disposição, critério ou prática neutra?

- ▶ De que forma é que os efeitos da disposição, do critério ou da prática têm um impacto significativamente mais negativo sobre um grupo protegido?
- ▶ A pessoa queixosa provou factos a partir dos quais se possa concluir que foi tratada de forma menos favorável devido a motivos protegidos?
- ▶ Se a diferença de tratamento não estiver “diretamente” relacionada com uma característica protegida, estará suficientemente ligada a ela? Tal será particularmente importante quando se analisar a discriminação por proxy.
- ▶ Qual foi o contexto da discriminação? A parte inquirida poderia argumentar com sucesso que a decisão foi tomada por um motivo diferente da discriminação proibida?

Tendo em conta todas as circunstâncias, será que foi estabelecido um caso *prima facie* de discriminação?

Se sim, avance para a secção 3.8. [A parte inquirida pode demonstrar que a diferença.](#)

Se não, considere o seguinte.

- ▶ Houve algum incumprimento das obrigações em matéria de documentação, testes, monitorização ou apresentação de relatórios que possa explicar a discriminação ou resultar em lacunas nas provas?
- ▶ Existem medidas pré-processuais que possam ser tomadas para colmatar eventuais lacunas nas provas?
 - Considere apresentar pedidos de divulgação de provas com base em considerações de transparência e acesso à justiça, ao abrigo do artigo 13.º da Convenção Europeia dos Direitos Humanos (direito a um recurso efetivo perante uma autoridade nacional) e do artigo 47.º da Carta dos Direitos Fundamentais da União Europeia (direito à ação e a um tribunal imparcial).
 - Note-se que, em algumas circunstâncias em que a parte inquirida pretenda invocar a confidencialidade comercial ou os direitos de entidades terceiras, poderão estar disponíveis procedimentos confidenciais ao abrigo da AFM, da APD ou dos tribunais. A jurisprudência atual sugere que existe uma tendência crescente para exigir que estas informações sejam disponibilizadas; ver [Dun & Bradstreet](#) (no contexto do RGPD):

Se quem é responsável pelo tratamento considerar que estas informações não podem ser fornecidas sem revelar dados de entidades terceiras ou segredos comerciais, quem é responsável pelo tratamento é obrigada/o a comunicar as informações alegadamente protegidas à autoridade de controlo ou ao órgão jurisdicional competentes, aos quais incumbe ponderar os direitos e interesses em causa para determinar o alcance do direito de acesso da pessoa titular dos dados previsto no artigo 15.º deste regulamento. (consulte também “[Confidencialidade](#)”).

Quanto à importância de apresentar informações estatísticas para estabelecer um caso *prima facie* de discriminação, consulte o ponto 3.6. [Testes e avaliação.](#)

Transparência

Um tribunal pode tirar conclusões da falta de apresentação de dados estatísticos ou outros dados relevantes. Também é possível deduzir a existência de discriminação a partir de factos e circunstâncias conexos, tais como as respostas de uma parte inquirida às perguntas ou o incumprimento de um código de conduta relevante. Ao não fornecer informações, a parte inquirida pode, na prática, não cumprir o ónus da prova, levando o tribunal a presumir a existência de discriminação (ver o ponto 3.8. para conhecer as circunstâncias em que surge o ónus legal de fornecer informações).

- ▶ Muitas vezes, é possível tirar conclusões a partir de uma resposta ambígua, inadequada ou evasiva a um questionário ou de uma declaração prestada durante a fase pré-processual ou no decurso do processo.
- ▶ Também é possível tirar conclusões da recusa em confirmar ou negar a existência de uma informação.

Questões a ter em conta

- ▶ Houve alguma omissão relevante na divulgação de informações por parte da parte inquirida que tenha conduzido a uma falta de transparência? Por exemplo, houve uma resposta adequada a quaisquer pedidos ao abrigo do RGPD, a quaisquer pedidos de acesso à informação, a correspondência pré-processual, a pedidos apresentados ao abrigo do Regulamento sobre a IA da UE ou a outros pedidos?
- ▶ Será possível tirar alguma conclusão a partir das provas disponíveis? Por exemplo, estatísticas, factos relacionados, casos conhecidos de discriminação?
- ▶ Será possível tirar alguma conclusão a partir da falta de provas? Por exemplo, a não resposta a perguntas, o incumprimento de orientações ou de códigos de conduta?
- ▶ Em todas as circunstâncias, será que os factos e circunstâncias conexos, incluindo a eventual falta de resposta a perguntas ou pedidos de informação - tais como um pedido PAPTD - ou a não prestação de explicações nos termos do artigo 86.º do Regulamento sobre a IA da UE, permitem inferir a existência de discriminação?

Exemplos do TJUE

- ▶ C-109/88, Handels- og Kontorfunktionærernes Forbund I Danmark contra Danfoss: o sindicato intentou uma ação em nome das trabalhadoras de uma empresa, uma vez que estas auferiam, em média, 7% menos do que os seus colegas do sexo masculino em cargos iguais ou semelhantes. Neste caso, o TJUE decidiu que, uma vez que o sistema salarial utilizado carecia totalmente de transparência, deve presumir-se a existência de discriminação, e o ónus da prova deve recair sobre a parte inquirida/entidade empregadora, que deve demonstrar que existem razões objetivas e não discriminatórias para a diferença nos salários pagos.

- C-415/10 Galina Meister contra Speech Design Carrier Systems GmbH: a autora alegou discriminação com base no género, na idade e na origem étnica no processo de seleção para o emprego e solicitou ao tribunal que ordenasse à entidade empregadora que tornasse pública a informação sobre se outra candidata ou candidato tinha sido contratada/o no final do processo. O TJUE considerou que, embora as diretivas em matéria de não discriminação não prevejam o direito de acesso a este tipo de informação, a recusa da parte inquirida em conceder qualquer acesso à informação à autora pode constituir um dos fatores que podem ser tidos em conta no âmbito da apuração dos factos a partir dos quais se possa presumir a ocorrência de discriminação direta ou indireta.

Exemplos das consequências da falta de transparência extraídos da jurisprudência nacional

► **Processo NL24.38560 (2025) dos Países Baixos (sentença interlocutória)**

O tribunal decidiu, por iniciativa própria, investigar a existência de um algoritmo de concessão de vistos e instruiu o(a) ministro(a) competente a:

- fornecer informações relevantes para a tomada de decisões;
- realizar uma AIDH;

com base na transparência no processo de tomada de decisões e no direito a uma proteção jurídica efetiva, nos termos tanto do artigo 13.º da Convenção Europeia dos Direitos Humanos como do artigo 47.º da Carta dos Direitos Fundamentais da União Europeia.

► **Processo no Tribunal Fiscal do Reino Unido (primeira instância): Elsbury contra The Information Commissioner (2025) UKFTT 915 (GRC) (2 de agosto de 2025)**

“O facto de a HMRC não ter confirmado nem negado que detém a informação solicitada reforça a convicção, baseada em indicadores presentes na correspondência da HMRC relativa aos pedidos de R&D, de que a IA está a ser utilizada por pessoal da HMRC - talvez de forma não autorizada -, minando assim a confiança das pessoas contribuintes na forma como a HMRC trata os pedidos de reembolso, o que, por sua vez, desencoraja as pessoas requerentes legítimas de apresentarem pedidos, prejudicando assim os objetivos políticos do próprio regime de benefícios fiscais R&D.”

► **Filcams Cgil Bologna e outros contra Deliveroo Italia S.R. (2020)**

O Tribunal de Bolonha considerou que a empresa não tinha cumprido o ónus da prova, uma vez que não demonstrou nem explicou o funcionamento concreto do algoritmo e não apresentou quaisquer provas do seu funcionamento efetivo. Não foi esclarecido quais os critérios específicos utilizados para determinar as estatísticas de motoristas, e estes não foram divulgados na plataforma, que se limitou a referir-se genericamente à “fiabilidade” e à “participação”

como indicadores para a atribuição de futuras oportunidades de trabalho. Para mais informações sobre este caso, consulte [Purificato \(2021\)](#).

3.8. A parte inquirida pode demonstrar que a diferença de tratamento não é discriminatória?

Na prática, provavelmente terá de ter em conta os mesmos elementos de prova e colocar as mesmas questões que as acima referidas (3.1-3.8). No entanto, é possível que, nesta fase, surjam agora novos elementos de prova a analisar ou que a explicação da parte inquirida sobre os elementos de prova ou o sistema seja mais pormenorizada. Para tal, será necessário rever o material original e as análises anteriormente realizadas, a fim de garantir que continuam a ser válidas à luz das novas informações.

Assim que a pessoa que alega discriminação tiver estabelecido um caso *prima facie* de discriminação, o ónus da prova passa então para a parte inquirida, que deve demonstrar que a diferença de tratamento não é discriminatória. Isto pode ser feito da seguinte forma.

- ▶ Demonstrar que, na realidade, não existe qualquer diferença de tratamento, porque, por exemplo, o comparador foi mal escolhido, ou a base da decisão não foi o motivo protegido, ou ainda porque os factos e as circunstâncias do caso são diferentes dos do comparador.
- ▶ Demonstrar que não existia qualquer nexo de causalidade entre o motivo proibido e o tratamento diferenciado.
- ▶ Demonstrar que, embora o tratamento diferenciado esteja relacionado com o motivo proibido, pode ser justificado ao abrigo de uma das exceções previstas no direito da UE (tais como requisitos profissionais genuínos e determinantes).
- ▶ Demonstrar que a medida, lei ou prática adotada é adequada e necessária para alcançar o objetivo legítimo em causa e que quaisquer desvantagens causadas não foram desproporcionadas em relação aos objetivos perseguidos (justificação razoável e objetiva), nos termos da Convenção Europeia dos Direitos Humanos no que se refere à discriminação direta e indireta e do direito da UE nos casos de discriminação indireta.

Se a parte inquirida não conseguir provar qualquer uma destas circunstâncias, será considerada responsável por discriminação.

Assim, no contexto dos sistemas algorítmicos ou de IA, uma vez demonstrado o caso *prima facie*, tal exigiria que a parte inquirida divulgasse informações relevantes sobre o sistema. Estas informações poderão ter como objetivo demonstrar que quaisquer decisões tomadas foram tomadas de acordo com critérios objetivos e não discriminatórios. Quanto à importância da apresentação de informação estatística para refutar o ónus da prova, ver o passo 3.6 sobre a abordagem aos dados estatísticos.

Tabela 7. As diretivas em matéria de não discriminação e a inversão do ónus da prova, com exemplos da abordagem adotada pelo TJUE para tirar conclusões da não apresentação de provas

Diretiva	Considerandos/ artigo	Motivos protegidos	Âmbito	Exemplo de caso que ilustra a abordagem do TJUE quanto à formulação de conclusões decorrentes da omissão, por parte da parte inquirida, de divulgar informações relevantes ou necessárias e/ ou de quaisquer outros requisitos de transparência
2000/43/CE (Diretiva relativa à igualdade racial)	Considerandos 15 e 21 Artigo 8.º	Raça e origem étnica – e não nacionalidade, e sem prejuízo do tratamento decorrente do estatuto jurídico de nacionais de países terceiros e de apátridas	Emprego, formação profissional, proteção social, educação, bens e serviços, incluindo a habitação	Meister C-415/10: a recusa em fornecer informações (sobre os critérios de recrutamento, por exemplo) pode dar origem a uma presunção de discriminação
Diretiva 2000/78/CE	Considerando 31 Artigo 10.º	Religião ou crença, deficiência, idade, orientação sexual	Emprego e profissão	Kelly C-104/10: não existe direito ao acesso aos dados, mas a não divulgação pode permitir que os tribunais tirem conclusões

Diretiva	Considerandos/ artigo	Motivos protegidos	Âmbito	Exemplo de caso que ilustra a abordagem do TJUE quanto à formulação de conclusões decorrentes da omissão, por parte da parte inquirida, de divulgar informações relevantes ou necessárias e/ ou de quaisquer outros requisitos de transparência
Diretiva 2006/54/CE (Diretiva relativa à igualdade de género, na sua versão reformulada)	Considerando 30 Artigo 19.º	Sexo (incluindo gravidez e maternidade)	Emprego e profissão (incluindo regimes de segurança social)	Danfoss C109/88: quando o sistema salarial é opaco, o ónus recai sobre a entidade empregadora Enderby C-127/92: as justificações para as diferenças salariais podem ser obrigadas a satisfazer o teste da justificação objetiva Kenny C-427/11: os dados salariais de comparação podem ser exigidos para refutar o caso <i>prima facie</i>
Diretiva 2004/113/CE (Diretiva relativa à igualdade de tratamento entre homens e mulheres no acesso a bens e serviços)	Considerando 22 Artigo 9.º	Sexo	Bens e serviços	Test-Achats C-236/09 Ver também a proibição específica da utilização do sexo como fator no cálculo dos prémios de seguros e de serviços financeiros conexos, bem como a consideração de fatores atuariais previstos no artigo 5.º

Diretiva	Considerandos/ artigo	Motivos protegidos	Âmbito	Exemplo de caso que ilustra a abordagem do TJUE quanto à formulação de conclusões decorrentes da omissão, por parte da parte inquirida, de divulgar informações relevantes ou necessárias e/ ou de quaisquer outros requisitos de transparência
2010/41/UE (Diretiva relativa à igualdade de tratamento entre homens e mulheres que exerçam uma atividade independente)		Sexo	Trabalhadoras/es independentes, cônjuges ou companheiras/os de trabalhadoras/es independentes	(Processo pendente) Loredas C-531/23: relativo à legalidade das isenções da obrigação de manter registos do tempo de trabalho
2023/970/UE Diretiva relativa à igualdade de remuneração (transposição até junho de 2026)	Artigos 5.º, 6.º e 8.º a 9.º		Emprego	Confere um direito direto à transparência. O Capítulo II prevê o direito à transparência remuneratória (artigo 5.º), a política de fixação da remuneração e de progressão da remuneração (artigo 6.º), o direito à informação, que deve ser acessível (artigos 8.º e 9.º), e a apresentação de relatórios sobre as disparidades remuneratórias (artigos 9.º e 10.º)

Existe alguma justificação objetiva?

Para demonstrar que uma diferença de tratamento não é discriminatória, num caso de discriminação indireta,⁵⁷ a parte inquirida poderia alegar que existe uma justificação objetiva para essa prática. Esta secção destaca os aspetos a ter em conta na avaliação de uma justificação objetiva apresentada por uma parte inquirida.

Para justificar um tratamento diferenciado, é necessário demonstrar que:

- ▶ o sistema algorítmico tem um objetivo legítimo;
- ▶ o sistema algorítmico é adequado ou apropriado para atingir esse objetivo;
- ▶ o sistema algorítmico é necessário para atingir esse objetivo;
- ▶ o sistema algorítmico é proporcionado, ou seja, o sistema algorítmico é eficaz na consecução do objetivo, não existem outros meios de alcançar o objetivo legítimo que conduzam a uma diferença de tratamento menor e o objetivo legítimo é suficientemente importante para justificar a diferença de tratamento.

Exemplo de processo no TJUE: C-167/97 Seymour-Smith

Em circunstâncias em que as ações por despedimento sem justa causa só eram possíveis após dois anos de emprego e em que as estatísticas demonstravam que tal constituía uma discriminação indireta contra as mulheres, o Estado-Membro responsável pela disposição, critério ou prática discriminatória indireta era obrigado a demonstrar que a regra refletia um objetivo legítimo da sua política social, que esse objetivo não estava relacionado com qualquer discriminação com base no sexo e que podia razoavelmente considerar que os meios escolhidos eram adequados para atingir esse objetivo. Nesse processo, o tribunal considerou que “simples generalizações a respeito da aptidão de uma determinada medida para a promoção do emprego não bastam para demonstrar que o objetivo da regra controvertida é alheio a qualquer discriminação em razão do sexo nem a dar elementos que permitam razoavelmente concluir que essa medida é adequada à realização desse objetivo” (parágrafos 76-77). O tribunal observou ainda que as estatísticas posteriores à adoção da medida poderiam ser tidas em conta para fornecer um indicador do impacto da medida nas mulheres e nos homens (parágrafo 49).

Objetivo do sistema

Para defender uma justificação razoável e objetiva, é necessário partir de um objetivo legítimo. Neste contexto, pode ser útil verificar se a parte inquirida mencionou objetivos diferentes ao longo dos vários documentos; ver: [3.4. Qual é a finalidade do sistema algorítmico e como é que ele funciona?](#)

Tome nota dos diferentes tipos de objetivos:

- ▶ objetivos de nível inferior (prever fraudes, determinar se estudantes estão em frente ao computador, prever a probabilidade de uma pessoa singular entrar em incumprimento num empréstimo);

⁵⁷ Nos termos do direito da UE, normalmente não é possível invocar uma justificação em casos de discriminação direta, exceto nos casos relacionados com a idade ou a deficiência e nos casos de profissões genuínas.

- objetivos de nível superior (minimizar a despesa pública com prestações sociais destinadas a pessoas singulares que não preenchem os requisitos para as receber, supervisão dos exames online, minimizar a taxa global de incumprimento).

Pode também ser necessário ter em conta o quadro jurídico nacional ao abrigo do qual o sistema algorítmico foi implementado. Ver *Glukhin contra a Rússia*, Recurso n.º 11519/20 (4 de julho de 2023) (abaixo).⁵⁸

Idoneidade ou adequação

A parte inquirida deve demonstrar que o sistema algorítmico é capaz de atingir o objetivo. Isto significa que, quando o objetivo é melhorar a eficiência de um processo de tomada de decisão, a parte inquirida deve demonstrar que o algoritmo reduziu o tempo de processamento, diminuiu a capacidade necessária ou aumentou a eficiência de outra forma. No caso de um sistema preditivo, demonstrar adequação pode significar demonstrar a precisão preditiva do sistema. Note-se que as alegações de adequação devem corresponder ao objetivo do sistema. Isto deve ter em conta objetivos tanto mais abrangentes como de nível superior. Um sistema pode ser inadequado por não cumprir um dos objetivos:

- objetivos de nível inferior, por exemplo, se o sistema for concebido para otimizar algo diferente do seu caso de utilização previsto. Por exemplo, foi otimizado para prever erros, mas agora é utilizado para prever fraudes;
- objetivos de nível superior, por exemplo, se o objetivo for reduzir as despesas com prestações sociais fraudulentas, mas as inspeções realizadas com base no algoritmo forem mais dispendiosas do que a redução das despesas, então este sistema algorítmico não é adequado para esse objetivo específico.

Necessidade

- O objetivo não pode ser alcançado (de forma tão eficaz) sem o algoritmo:
 - em comparação com a situação anterior à aplicação do algoritmo;
 - em comparação com abordagens não algorítmicas.
- O objetivo não pode ser alcançado (de forma tão eficaz) com outro sistema algorítmico:
 - em comparação com algoritmos que utilizam outros dados de entrada (por exemplo, excluindo os proxies mais fortes);
 - em comparação com outros conjuntos de dados sobre desenvolvimento (que incluem menos desigualdades históricas ou enviesamentos humanos).

⁵⁸ Ver também *Beghal contra o Reino Unido* para uma análise mais aprofundada dos requisitos impostos às leis nacionais para que uma medida contestada seja considerada “em conformidade com a lei”.

Exemplo de um processo do Tribunal Europeu dos Direitos Humanos: *Glukhin contra a Rússia*, Recurso n.º 11519/20 (4 de julho de 2023)

O Tribunal Europeu dos Direitos Humanos analisou a utilização da tecnologia de reconhecimento facial em tempo real (RFTR) para identificar e localizar um manifestante no metro russo à luz do artigo 8.º (vida privada) e do artigo 10.º (liberdade de expressão). Embora reconhecendo a importância das técnicas científicas modernas de investigação e identificação (parágrafo 85) e tendo constatado a ausência de fundamento jurídico para as medidas adotadas, devido à falta de delimitação legal da utilização de RFTR, o Tribunal avaliou igualmente a “necessidade numa sociedade democrática” das medidas adotadas, nomeadamente à luz do seu potencial “efeito dissuasor” sobre o direito à liberdade de expressão e de reunião (artigo 10.º). O Tribunal concluiu:

90. À luz de todas as considerações acima expostas, o Tribunal conclui que a utilização de tecnologia de reconhecimento facial altamente intrusiva no contexto do exercício, por parte do autor, do seu direito à liberdade de expressão consagrado na Convenção é incompatível com os ideais e valores de uma sociedade democrática regida pelo Estado de direito, que a Convenção se propõe a preservar e promover. O tratamento dos dados pessoais do autor através da tecnologia de reconhecimento facial no âmbito de um processo por infração administrativa - em primeiro lugar, para o identificar a partir das fotografias e do vídeo publicados no Telegram e, em segundo lugar, para o localizar e deter enquanto se deslocava no metro de Moscovo - não pode ser considerado “necessário numa sociedade democrática”.

Proporcionalidade

Em todos os casos, a discriminação resultante da utilização do sistema que a parte inquirida procura justificar deve ser proporcional ao objetivo a alcançar. Em termos gerais, isto exige que o tribunal pondere a gravidade do dano em relação aos outros fatores considerados nesta secção.

Questões a ter em conta

- ▶ A parte inquirida pode provar que não discriminou?
- ▶ A parte inquirida pode provar que não deve ser considerada como tendo sido vítima de discriminação?
 - A intervenção humana resolve de forma suficiente qualquer discriminação residual?
 - Note-se que a discriminação pode ser resultado de um erro humano e não do sistema algorítmico.
- ▶ A parte inquirida poderia alegar que foi escolhido um comparador errado?
- ▶ A parte inquirida pode demonstrar que a pessoa queixosa não se encontra numa situação semelhante ou comparável à do seu comparador?
- ▶ Existe alguma explicação alternativa sustentável para a diferença de tratamento, para além da discriminação?
- ▶ Que medidas foram tomadas para evitar a discriminação (ajustes razoáveis)?

- Sempre que for o caso, a parte inquirida pode demonstrar que o tratamento diferenciado não se baseia no motivo protegido, mas sim noutras diferenças objetivas?
- Essas diferenças objetivas estão explicitamente abrangidas pelas diretivas em matéria de não discriminação?
- A disposição ou prática em questão visa um objetivo legítimo?
- Analise a secção 3.4 sobre o que o sistema de IA pretende fazer e como o faz – os meios escolhidos foram adequados?
- Os meios utilizados para atingir o objetivo são adequados, necessários e proporcionais ao objetivo que se pretende alcançar?



Passo 4

Vias de recurso

O passo 4 descreve em pormenor as várias vias de recurso e medidas que estão ao dispor dos organismos para a igualdade. É provável que os poderes e os mandatos variem significativamente de Estado-Membro para Estado-Membro; por conseguinte, este passo foi elaborado especificamente para analisar a inter-relação entre as diretivas relativas às normas, que devem ser transpostas até 19 de junho de 2026, o Regulamento sobre a IA, o RGPD e qualquer outra legislação da União relevante.

Normalmente, será necessário considerar mais do que uma via de recurso, dependendo da questão ou do caso.

A secção 4.1 aborda as vias de recurso aplicáveis a todos os sistemas algorítmicos.

A secção 4.2 prevê vias de recurso adicionais para sistemas de risco elevado.

A secção 4.3 descreve o que um OI deve fazer nos casos em que um sistema ou caso de utilização represente um risco para os direitos fundamentais, mas não seja classificado como de risco elevado ao abrigo do Regulamento sobre a IA, incluindo as medidas que uma AFM possa tomar e que exijam ou possam exigir o envolvimento do OI.

Figura 5. Passo 4 - Vias de recurso

PASSO 4		Vias de recurso
4.1	Vias de recurso para todos os sistemas algorítmicos	POSSÍVEIS MEDIDAS • Poderes corretivos dos organismos para a igualdade • Assistência inicial • Submeter uma queixa a uma AFM • Vias de recurso do RGPD • Resolução alternativa de litígios • Contencioso • Recolha e reporte de dados relativos à igualdade
4.2	Vias de recurso adicionais para sistemas de IA de risco elevado	POSSÍVEIS MEDIDAS • Resposta da AFM a incidentes graves • Investigação da AFM de qualquer risco grave para os direitos fundamentais • Classificações de IA erradas • Sistemas de IA conformes que representam um risco para os direitos fundamentais
4.3	Risco grave para os direitos fundamentais mas a IA não é um sistema de risco elevado ou proibido	POSSÍVEIS MEDIDAS • Propor alterações ao Regulamento sobre a IA • Propor adendas ao Anexo III do Regulamento sobre a IA

Ao abrigo das diretivas relativas à não discriminação e das diretivas relativas às normas, os OIs dispõem de amplos poderes para levar a cabo atividades destinadas a prevenir a discriminação e a promover a igualdade de tratamento. Esses poderes incluem a sensibilização (artigo 5.º), a prestação de assistência às vítimas (artigo 6.º), a resolução alternativa de litígios (artigo 7.º), a realização de inquéritos sobre violações do princípio da igualdade de tratamento (artigo 8.º), a emissão de pareceres e decisões, incluindo o direito de apurar factos (artigo 9.º), e a intervenção em processos judiciais, incluindo o direito de apresentar observações (artigo 10.º).

Sempre que se identifique discriminação num sistema algorítmico, deve ponderar-se o exercício destes poderes para garantir:

- ▶ que a parte inquirida deixa de utilizar o sistema de IA de forma discriminatória ou, caso tal não seja possível, deixa de utilizar o sistema de IA por completo;
- ▶ que a sensibilização para a discriminação algorítmica é devidamente comunicada aos grupos e organismos afetados;
- ▶ que é prestado aconselhamento e assistência às vítimas individuais, nomeadamente no que diz respeito à resolução alternativa de litígios (RAL) e ao contencioso;
- ▶ que são tomadas medidas corretivas, nomeadamente através da prestação de formação, aconselhamento e apoio;
- ▶ que é realizado um debate público sobre a questão da discriminação nos sistemas algorítmicos e se promovam medidas de ação positiva e a integração da perspetiva de igualdade junto das entidades públicas e privadas;
- ▶ que há comunicação com as partes interessadas relevantes, incluindo os parceiros sociais, e promoção do intercâmbio de boas práticas.

Ao levar a cabo essas atividades, os organismos para a igualdade podem ter em consideração situações específicas de desvantagem resultantes da discriminação interseccional, entendida como a discriminação baseada numa combinação de motivos protegidos pelas diretivas em matéria de não discriminação.

Os OIs devem ter em consideração as ferramentas e os formatos de comunicação adequados para cada grupo-alvo. Devem centrar-se, em particular, nos grupos cujo acesso à informação possa ser dificultado, por exemplo, devido à sua situação económica precária, idade, deficiência, nível de alfabetização, nacionalidade ou estatuto de residência, ou devido à falta de acesso a ferramentas online.

Recursos essenciais

- ▶ “Manual de litígio estratégico” (Equinet 2017)
- ▶ “Como utilizar o Regulamento sobre a Inteligência Artificial para investigar o enviesamento e a discriminação na IA: um guia para os organismos para a igualdade” (Mittelstadt 2024)

4.1. Vias de recurso para todos os sistemas algorítmicos

Seguir o processo descrito nos passos 2 e 3 deveria ter ajudado a identificar se existe discriminação e qual poderá ter sido a causa dessa discriminação. Os OIs devem utilizar as informações recolhidas durante essas etapas para sugerir medidas corretivas e adotar um plano para a eliminação ou alteração das práticas, algoritmos ou sistemas contestados. Por exemplo, o OI pode ter concluído que a escolha dos parâmetros de equidade era inadequada para o caso de utilização ou que os dados não eram suficientemente representativos.

Caso o OI decida que o risco de discriminação ou a discriminação identificada é ilegal, mas pode ser corrigido(a), considere a adoção de medidas para alcançar:

- ▶ a proibição da utilização do sistema até que a discriminação tenha sido corrigida;
- ▶ quaisquer medidas corretivas que devam ser tomadas.

Caso o OI decida que o risco de discriminação é ilícito e não pode ser corrigido, devem ser consideradas medidas destinadas a alcançar um dos seguintes resultados:

- ▶ a proibição total da utilização do sistema algorítmico;
- ▶ a proibição da utilização do sistema algorítmico num determinado setor;
- ▶ a proibição da utilização do sistema algorítmico para um fim específico.

Tal ação poderia ser concretizada através do exercício, por parte dos organismos para a igualdade, dos seus próprios poderes no que diz respeito à emissão de pareceres, à formulação de recomendações e à realização de consultas, em conjunto com a AFM, quer ao abrigo do RSGP ou do Regulamento sobre a IA, quer através dos tribunais.

4.1.1. Poderes de correção dos organismos para a igualdade

Os organismos para a igualdade devem, em primeiro lugar, ter em conta os seus poderes de correção previstos na legislação nacional, tal como referido acima. Estas medidas podem incluir qualquer uma ou todas as vias de recurso que venham a ser formalizadas pelas diretivas relativas às normas, tais como a emissão de um parecer ou de uma recomendação, ou a exigência de uma consulta ou de testes.

Se as diretivas relativas às normas forem transpostas para a legislação nacional, os Ols deverão dispor de poderes de correção. Entre estes contam-se o artigo 9.º (emissão de um parecer vinculativo ou não vinculativo, consoante o contexto nacional) e o artigo 15.º, relativo aos poderes de consulta e de recomendação.

Os organismos para a igualdade devem também ter poderes para apresentar e documentar a sua avaliação do caso, incluindo a apuração dos factos e uma conclusão fundamentada sobre a existência de discriminação. No caso da discriminação algorítmica, tal poderia incluir a cooperação com a AFM.

Sempre que adequado, tanto os pareceres não vinculativos como as decisões vinculativas devem incluir medidas específicas destinadas a corrigir qualquer violação do princípio da igualdade de tratamento que tenha sido constatada e a prevenir a repetição de tais situações. Os Ols podem necessitar de assistência especializada para implementar medidas específicas e, caso não disponham dos conhecimentos necessários, poderão querer consultar a AFM. Devem ser estabelecidos mecanismos adequados para o acompanhamento dos pareceres não vinculativos, tais como obrigações de resposta, e para a execução das decisões vinculativas.

As consultas podem ser utilizadas para identificar a existência de problemas, para avaliar o impacto social e discriminatório dos sistemas nas comunidades afetadas ou potencialmente afetadas e para recolher dados.

De um modo mais geral, as recomendações e consultas poderiam ter como objetivo garantir que esses problemas não surjam no futuro, por exemplo, recomendando:

- ▶ avaliações de impacto sobre a proteção de dados e a igualdade;
- ▶ consulta à comunidade e uma AIDF liderada pela comunidade;
- ▶ utilização de ambientes de teste isolados e testes em condições reais.

Leitura complementar

- ▶ Crowley (2023), “Informing the policy agenda: equality bodies making recommendations”.

4.1.2. Prestar assistência inicial a uma vítima

O artigo 6.º das diretivas relativas às normas prevê que os organismos para a igualdade prestem assistência inicial, informando as vítimas sobre o seguinte:

- ▶ o quadro jurídico relativo à discriminação e aos sistemas algorítmicos, incluindo aconselhamento adaptado à sua situação específica;

- ▶ os serviços prestados pelo organismo para a igualdade e os aspetos processuais conexos;
- ▶ vias de recurso disponíveis, incluindo a possibilidade de levar o caso a tribunal, nomeadamente:
 - ao abrigo da legislação em matéria de não discriminação;
 - ao abrigo do Regulamento sobre a IA – ver, por exemplo, o direito de apresentar uma queixa junto da AFM (artigo 85.º do Regulamento sobre a IA) e o [direito a explicações](#) (artigo 86.º do Regulamento sobre a IA);
 - ao abrigo da legislação em matéria de proteção de dados – por exemplo, apresentar uma queixa junto da APD (artigo 77.º do RGPD) e o direito de apresentar um [pedido de acesso aos dados](#) (artigo 15.º do RGPD);⁵⁹
- ▶ as regras de confidencialidade aplicáveis e a proteção de dados pessoais (por exemplo, as políticas de proteção de dados dos OIs e, quando relevante, qualquer conflito entre a obtenção de provas por parte do OI no exercício de uma parte do seu mandato e a possibilidade de disponibilizar essas provas para utilização em tribunal por parte de uma pessoa singular);
- ▶ a possibilidade de obter apoio psicológico ou outro tipo de apoio relevante por parte de outras entidades ou organizações.

Os organismos para a igualdade devem informar a pessoa queixosa, num prazo razoável, se a queixa será arquivada ou se existem motivos para lhe dar seguimento.

Após a prestação de assistência inicial, as vias de recurso à disposição de uma pessoa singular queixosa podem incluir:

- ▶ [apresentar uma queixa junto da AFM](#) (artigo 85.º do Regulamento sobre a IA);
- ▶ [considerar a resolução alternativa de litígios](#);
- ▶ [recorrer à justiça nos tribunais nacionais para contestar a discriminação](#).

Qualquer decisão sobre a melhor forma de agir deve ser tomada em conjunto com a pessoa ou o grupo afetado. Se o OI não tiver capacidade, competência (por exemplo, em matéria de proteção de dados) ou recursos para dar seguimento à ação pretendida pela pessoa afetada, o caso deve ser encaminhado para outra entidade prestadora de serviços jurídicos competente.

4.1.3. Prestar assistência a uma pessoa coletiva ou singular na apresentação de uma queixa junto da AFM

Caso a investigação realizada no passo 3 tenha identificado problemas de conformidade ao abrigo do Regulamento sobre a IA, qualquer pessoa singular ou coletiva tem o direito de apresentar uma queixa junto da AFM (artigo 85.º do Regulamento sobre a IA da UE). Isto significa que esse direito se estende a uma entidade dotada

⁵⁹ O direito a explicações está previsto tanto no RGPD (artigos 15.º e 22.º) como no Regulamento sobre a IA (artigo 86.º). No [passo 2](#) e nos Anexos [A](#) e [B](#), são fornecidas explicações adicionais e modelos para a apresentação do pedido.

de personalidade jurídica, como uma sociedade ou uma organização. O OI pode ajudar a pessoa que apresenta a queixa com as provas identificadas no passo 3.

Este direito não prejudica nem se subtrai aos direitos e vias de recurso existentes ao abrigo do direito da UE e do direito nacional (Considerando 170). Não se limita aos sistemas de IA de risco elevado.

Qualquer queixa deste tipo é “tida em conta” para efeitos da realização de atividades de fiscalização do mercado ao abrigo do Regulamento (UE) 2019/1020 relativo à fiscalização do mercado e à conformidade dos produtos. É muito provável que prazos sejam estabelecidos na legislação nacional (ver artigo 11.º do Regulamento (UE) n.º 2019/1020).

Qualquer sistema de IA que não seja de risco elevado estaria abrangido pelo Regulamento relativo à Segurança Geral dos Produtos (UE) 2023/988, pelo Regulamento (UE) 2023/988 e pelo Regulamento AFM (UE) 2019/1020.

É importante que os sistemas de IA relacionados com produtos que não são de risco elevado, nos termos do presente regulamento e que, como tal, não são obrigados a cumprir os requisitos aplicáveis a sistemas de IA de risco elevado, sejam seguros quando são colocados no mercado ou colocados em serviço. A fim de contribuir para alcançar esse objetivo, o Regulamento (UE) 2023/988 do Parlamento Europeu e do Conselho (53) deverá ser aplicado como uma rede de segurança. (Considerando 166 do Regulamento sobre a IA)

O direito de apresentar uma queixa não prejudica quaisquer outros recursos administrativos ou judiciais, pelo que constitui uma medida que deve ser tomada em conjunto com quaisquer outros recursos aplicáveis. Por si só, é improvável que esta seja a melhor solução para uma pessoa singular, sobretudo porque não há qualquer disposição relativa a indemnizações. No entanto, trata-se de uma medida de acompanhamento importante e, uma vez que a AFM dispõe de poderes e vias de recurso muito abrangentes ao abrigo do Regulamento (UE) 2019/1020, valerá a pena considerá-la num caso adequado. Uma queixa apresentada à AFM deverá dar origem a uma investigação mais estrutural por parte da AFM e a uma medida corretiva de maior alcance, com impacto num grupo mais vasto de pessoas singulares afetadas do que uma queixa individual por discriminação. A AFM dispõe de amplos poderes, tanto ao abrigo do Regulamento sobre a IA como do Regulamento (UE) 2019/1020, e pode realizar controlos documentais, físicos e laboratoriais (ver secção 4.2).

Se a queixa for deferida, a AFM pode exigir que um(a) operador(a) económico/a tome medidas corretivas, desde que essas medidas sejam adequadas e proporcionadas. Se a medida corretiva não for tomada ou não for bem-sucedida, a AFM pode proibir ou restringir a colocação de um produto no mercado ou ordenar que o produto seja retirado do mercado ou recolhido. No caso de produtos que apresentem um risco com repercussões para além do próprio Estado-Membro da MSA, esta é obrigada a notificar imediatamente a Comissão Europeia e os restantes Estados-Membros da UE das medidas tomadas. O Regulamento (UE) 2019/1020 prevê disposições abrangentes em matéria de cooperação transfronteiriça entre os diferentes Estados-Membros.

4.1.4. Vias de recurso ao dispor da pessoa titular dos dados ao abrigo do RGPD ou dos regimes nacionais de proteção de dados

Nos termos do RGPD, uma pessoa titular de dados (uma pessoa singular) tem os seguintes direitos em matéria de dados, para além do direito a explicações.

- ▶ O direito a opor-se ao tratamento automatizado dos seus dados pessoais (artigo 21.º).
- ▶ O direito à retificação de dados pessoais inexatos que lhe digam respeito e à integração de dados pessoais incompletos mediante a apresentação de uma declaração complementar (artigo 16.º).
- ▶ O direito ao apagamento dos seus dados pessoais sem demora injustificada, sempre que se verifique uma das seguintes situações:
 - o consentimento for retirado e não se aplicar qualquer outro fundamento jurídico;
 - exerceram o seu direito de oposição nos termos do n.º 1 do artigo 21.º;
 - os dados pessoais foram tratados ilicitamente.

Estes podem ser relevantes nos casos em que um sistema algorítmico tenha dado origem a discriminação. Qualquer medida tomada poderá exigir o envolvimento de uma pessoa especialista em proteção de dados ou da autoridade responsável pela proteção de dados.

Nos casos em que os Estados tenham adotado regimes de proteção de dados para além do RGPD, ou nos Estados que não estejam sujeitos ao RGPD, será importante ter em conta quaisquer leis nacionais em matéria de proteção de dados.

4.1.5. Oferecer resolução alternativa de litígios em conformidade com a lei

Nos termos do artigo 7.º das diretivas relativas às normas, os OIs devem poder oferecer às partes a possibilidade de procurarem uma resolução alternativa para o seu litígio. Esse processo pode ser conduzido pelo próprio organismo para a igualdade ou por outra entidade competente, em conformidade com a legislação e a prática nacionais; nesse caso, o organismo para a igualdade pode apresentar observações a essa entidade. Essa resolução alternativa de litígios pode assumir diferentes formas, tais como a mediação ou a conciliação, em conformidade com a legislação e a prática nacionais. A ausência de uma decisão não impede as partes de exercerem o seu direito de agir em processos judiciais. Os Estados-Membros devem assegurar que o prazo de prescrição seja suficientemente longo para garantir que as partes num litígio tenham acesso aos tribunais, por exemplo, suspendendo o prazo de prescrição enquanto as partes participam num processo de resolução alternativa de litígios.

4.1.6. Litígios em matéria de não discriminação e direitos humanos

Os organismos para a igualdade devem ter o direito de intervir em processos judiciais em matéria civil e administrativa, incluindo o direito de apresentar observações relativas às diretivas em matéria de não discriminação, em conformidade com a legislação e a prática nacionais. Isto varia consoante o Estado.

Nos termos do artigo 10.º das diretivas relativas às normas, o direito do organismo para a igualdade de intervir em processos judiciais deve incluir, pelo menos, uma das seguintes opções:

- ▶ o direito de intentar uma ação judicial em nome de uma ou várias vítimas;
- ▶ o direito de participar em processos judiciais em defesa de uma ou várias vítimas;
- ▶ o direito de intentar ações judiciais em seu próprio nome, para defender o interesse público.

Isto incluirá decisões de execução relativas a pareceres vinculativos emitidos pelo OI nos termos do artigo 9.º (ver abaixo). Ao ponderarem a possibilidade de intentar uma ação judicial estratégica, os organismos para a igualdade devem consultar as considerações pormenorizadas contidas no “Manual de litígio estratégico” da Equinet (Equinet 2017: 17).

É provável que haja oportunidades significativas para o recurso a litígios estratégicos no que diz respeito aos sistemas de IA, uma vez que tanto a tecnologia como a legislação são relativamente recentes. O litígio estratégico não será necessariamente a melhor abordagem em todos os casos. Por exemplo, a obtenção de um resultado pode demorar demasiado tempo para a pessoa afetada, podem faltar as informações necessárias para apresentar uma queixa bem-sucedida, pode ser mais eficaz iniciar processos de análise e negociação, entre vários outros fatores que terão de ser considerados caso a caso.

4.1.7. Recolha de dados, acesso a dados relativos à igualdade e apresentação de relatórios

O acesso a dados relativos à igualdade é fundamental para determinar a existência de discriminação por parte dos sistemas de IA e TDA. Os organismos para a igualdade podem aproveitar os novos poderes para recolher dados sobre a ocorrência de discriminação algorítmica de forma mais abrangente. Ao longo desta metodologia, foram formuladas recomendações sobre os tipos de informação a registar, as quais poderão ajudar os OIs a compilar dados relativos à igualdade relacionados com sistemas algorítmicos. As estatísticas recolhidas podem ser úteis, por exemplo, para fundamentar um caso *prima facie* de discriminação em tribunal. Se o OI constatar que existem pedidos frequentes de assistência relacionados com um determinado setor ou caso de utilização de um sistema algorítmico, tal poderá exigir uma investigação mais aprofundada ou a atribuição de prioridade.

A recolha de dados relativos à igualdade é insuficiente em muitos países, sobretudo porque está frequentemente sujeita a restrições legais, uma vez que os OIs não conseguem, muitas vezes, tratar categorias sensíveis de dados pessoais para efeitos de medição e mitigação de enviesamento, nos termos da alínea g) do n.º 2 do artigo 9.º do RGPD e do n.º 5 do artigo 10.º do Regulamento sobre a IA. Os OIs poderiam recomendar a reforma das regras e práticas de recolha de dados, a fim de melhorar os conhecimentos atuais sobre a discriminação algorítmica (ver Conselho da Europa 2025b).

Identificar problemas estruturais e apresentar relatórios sobre os mesmos anualmente

A recolha de dados deverá permitir ao OI identificar e dar conta das desigualdades estruturais nos sistemas algorítmicos. Nos casos em que o OI utilize uma base de dados para registar os pormenores dos casos e os conselhos prestados, deverá ser adicionada uma nova categoria de caso para permitir ao OI acompanhar a utilização discriminatória, efetiva ou suspeita, dos sistemas de IA. A longo prazo, esta metodologia poderá ser utilizada para conceber campos específicos na base de dados, de modo a permitir a recolha e a análise de dados relativos a estes casos.

A título de inspiração, ao longo do passo 3 da metodologia, são identificados, no final de cada secção, indicadores do tipo de informação que poderia ser registada numa base de dados, sendo apresentada uma ficha de trabalho sugerida no [Anexo K](#).

As questões estruturais podem incluir:

- ▶ indícios de discriminação decorrentes de um determinado tipo de sistema algorítmico ou tecnologia;
- ▶ indícios de discriminação que surgem quando se utilizam sistemas algorítmicos em determinados setores;
- ▶ indícios de que possa estar a ocorrer discriminação num determinado setor ou tipo de sistema algorítmico;
- ▶ indícios de que determinados grupos estão a ser afetados de forma desproporcionada pela adoção de sistemas algorítmicos em vários setores;
- ▶ Sistemas de IA ou casos de utilização que deveriam, mas que atualmente não são:
 - proibidos;
 - classificados como de risco elevado;
 - modelos de finalidade geral com risco sistémico;
 - incluídos em qualquer uma destas categorias, mas que, mesmo assim, representam um risco inaceitável de discriminação;
- ▶ falhas sistémicas no cumprimento das disposições do Regulamento sobre a IA relevantes em matéria de discriminação, tais como testes inadequados de enviesamento ou de equidade e práticas inadequadas de recolha de dados.

4.2. Vias de recurso adicionais para sistemas de IA de risco elevado

4.2.1. Medidas tomadas pela AFM em cooperação com o OI

Para além dos poderes conferidos aos OIs nos termos do artigo 77.º do Regulamento sobre a IA, a AFM tem a obrigação de colaborar com um OI na qualidade de autoridade nos termos do artigo 77.º, sempre que se trate de um “incidente grave” (artigo 73.º do Regulamento sobre a IA), quando os sistemas de IA apresentam riscos (artigo 79.º do Regulamento sobre a IA) e quando se investiga um sistema em conformidade que represente um risco para os direitos fundamentais (artigo 82.º do Regulamento sobre a IA). Uma AFM poderá também ter de consultar um OI ao

analisar um sistema de IA que tenha sido indevidamente classificado por uma entidade prestadora como não sendo de risco elevado (artigo 80.º do Regulamento sobre a IA). Estes processos são abordados com mais pormenor a seguir.

Um OI pode decidir remeter um sistema à AFM, acompanhado de provas obtidas ao abrigo desta metodologia, para comunicar um incidente grave, realizar testes, efetuar uma avaliação ou exercer os poderes que lhe são conferidos pelo Regulamento sobre a IA ou pelo Regulamento AFM, a fim de exigir medidas corretivas, a suspensão ou a retirada do produto do mercado, ou outras medidas.

Resposta da AFM a uma notificação de um incidente grave (artigo 73.º do Regulamento sobre a IA)

A AFM dispõe de poderes e responsabilidades significativos ao abrigo do Regulamento (UE) n.º 2019/1020 no que diz respeito à gestão de incidentes graves.

A AFM deve informar o órgão previsto no artigo 77.º sempre que for notificada por uma entidade prestadora sobre um incidente grave (n.º 3 do artigo 73.º do Regulamento sobre a IA). Um incidente grave é definido como qualquer incidente ou anomalia num sistema de IA que, por exemplo, conduza, direta ou indiretamente, à infração de obrigações decorrentes do direito da União destinadas a proteger os direitos fundamentais, incluindo o direito à não discriminação (artigo 3.º, n.º 49, alínea c), do Regulamento sobre a IA). A Comissão publicará orientações oportunamente.

Nesses casos, tenha em conta o seguinte.

- ▶ O incidente grave envolveu algum risco de discriminação?
 - Se sim, as pessoas afetadas deveriam ter direito a vias de recurso?
 - Se sim, considere a via de recurso mais eficaz (por exemplo, RAL, ação judicial ou inquérito).
 - Se as pessoas afetadas tiverem direito a uma indemnização pecuniária, certifique-se de que a via de recurso escolhida não impede tal indemnização. Certifique-se de que cumpre todos os prazos aplicáveis.
- ▶ É provável que isto tenha impactos adicionais e duradouros para outras pessoas? Por exemplo, o sistema é utilizado pelos bancos para determinar a solvabilidade?
- ▶ Tome medidas imediatas para sensibilizar para esta questão (artigo 5.º das diretivas relativas às normas ou através da AFM, com base na regulamentação em matéria de segurança dos produtos).
- ▶ Analise se o sistema de IA interage com outros dispositivos ou software e chame a atenção para quaisquer sistemas que possam estar a ser afetados de forma semelhante.

Registe o tipo de tecnologia e o setor em que a questão surgiu, para utilização nos relatórios do OI e na análise de dados relativos à igualdade.

As medidas corretivas necessárias dependerão dos problemas identificados. No entanto, as informações, passos e abordagens descritas no passo 3 deverão ajudar o OI a identificar possíveis vias de recurso.

Investigação da AFM ao abrigo do n.º 3 do artigo 79.º do Regulamento sobre a IA: produto que representa um risco grave para os direitos fundamentais, incluindo a discriminação

Caso a AFM (por si só ou em cooperação com um organismo nos termos do artigo 77.º) constatare que o sistema de IA não cumpre os requisitos estabelecidos no regulamento, deverá exigir, sem demora injustificada:

- ▶ medidas corretivas adequadas para garantir a conformidade do sistema de IA;
- ▶ informar a Comissão e os outros Estados-Membros sobre os resultados da avaliação e as medidas que a entidade prestadora deverá tomar;
- ▶ retirar o sistema de IA do mercado (n.º 5 do artigo 79.º do Regulamento sobre a IA);
- ▶ uma *recall* num prazo que a AFM possa estabelecer, no prazo de 15 dias úteis ou conforme previsto no direito da União (o que exigirá, nesta fase, uma verificação da legislação pertinente);
- ▶ que a AFM informe o organismo notificado competente.

Procedimento da AFM para o tratamento de sistemas de IA classificados pela entidade prestadora como de risco não elevado, em aplicação do Anexo III (artigo 6.º, n.º 4, e artigo 80.º do Regulamento sobre a IA)

Ao analisar se um sistema de IA foi classificado incorretamente ao abrigo do procedimento de autoavaliação com opção de exclusão (n.º 4 do artigo 6.º e o procedimento previsto no artigo 80.º), a AFM deve realizar uma avaliação para determinar se o n.º 3 do artigo 6.º é aplicável.

Neste caso, é possível que não exista uma avaliação de risco fundamental relevante nem qualquer consideração relativa à discriminação. As questões em análise são se o sistema de IA:

- ▶ desempenha uma tarefa processual específica;
- ▶ melhora o resultado de uma atividade humana já concluída;
- ▶ deteta padrões de tomada de decisão ou desvios em relação a padrões de tomada de decisão anteriores;
- ▶ realiza uma tarefa preparatória para uma avaliação.

No entanto, é possível que mesmo estes sistemas possam representar riscos para os direitos fundamentais e para o princípio da não discriminação. Os OIs podem reter um sistema para a AFM, a fim de que esta avalie se o sistema de IA foi classificado incorretamente, e apresentar as provas em que se baseiam para tal remessa.

Sistemas de IA de risco elevado, em conformidade com o Regulamento sobre a IA, que representem um risco para a saúde ou a segurança das pessoas, para os direitos fundamentais ou para outros aspetos da proteção do interesse público (artigo 82.º do Regulamento sobre a IA)

A AFM dispõe de poderes relativamente a um sistema em conformidade que represente um risco nos termos do artigo 82.º do Regulamento sobre a IA. Antes de tomar estas medidas, a AFM deve dispor de ambos:

- ▶ realizou uma avaliação nos termos do artigo 79.º do Regulamento sobre a IA; e
- ▶ consultou o órgão competente nos termos do artigo 77.º.

A entidade operadora será obrigada a tomar “todas as medidas adequadas para assegurar que, quando for colocado no mercado ou colocado em serviço, o sistema de IA em causa já não apresenta esse risco”.

Embora tal não esteja explicitamente previsto no Regulamento sobre a IA, o OI deve ser consultado, pelo menos, quando a AFM pretender determinar se os riscos para os direitos fundamentais e/ou para a igualdade foram devidamente eliminados.

4.3. O que fazer quando um sistema ou caso de utilização representa um risco para os direitos fundamentais, mas não é classificado como “de risco elevado” ou “proibido”

Esta situação pode ocorrer quando:

- ▶ uma entidade prestadora tenha avaliado, por conta própria, que o seu sistema algorítmico não constitui um sistema de IA, de acordo com a definição do artigo 3.º, e, por conseguinte, se encontra totalmente fora do âmbito de aplicação do regulamento;
- ▶ um sistema algorítmico que deveria ser proibido devido ao risco que representa não está incluído na lista de sistemas proibidos prevista no artigo 5.º do Regulamento sobre a IA;
- ▶ um sistema algorítmico que deveria ser classificado como de risco elevado não está incluído no Anexo III do Regulamento sobre a IA porque nem o setor nem o caso de utilização estão abrangidos;
- ▶ uma entidade prestadora aplicou a derrogação prevista no n.º 3 do artigo 6.º a um sistema de IA que, de outro modo, seria classificado como de risco elevado.

Nota: quem é responsável pela implantação tem a obrigação de monitorizar os seus sistemas de risco elevado e de notificar a AFM sempre que tenham motivos para considerar que a utilização do sistema de IA, em conformidade com as instruções, possa fazer com que esse sistema represente um risco grave para os direitos fundamentais (artigo 26.º, em conjugação com o artigo 79.º do Regulamento sobre a IA).

Nota: se um sistema de IA for um “produto que apresenta um risco”, tal como definido no artigo 3.º, ponto 19, do Regulamento (UE) 2019/1020, a AFM é obrigada a avaliar o sistema e, caso sejam identificados riscos para os direitos fundamentais, a cooperar com

as autoridades competentes nos termos do artigo 77.º. As vias de recurso aplicáveis a um produto deste tipo ao abrigo do Regulamento sobre a IA limitam-se aos sistemas de risco elevado que cumprem os requisitos. Podem estar disponíveis vias de recurso alternativas ao abrigo do Regulamento AFM e da legislação relativa à segurança geral dos produtos, do direito contratual ou do direito da responsabilidade civil, da legislação em matéria de não discriminação ou da legislação em matéria de direitos humanos.

Para as pessoas singulares ou grupos afetados, o facto de um sistema não ser classificado como de risco elevado ou proibido não significa que não possa causar discriminação ou resultar em violações dos direitos fundamentais ou ser utilizado de forma a violá-los. Os OIs têm à sua disposição todas as vias de recurso habituais contra a discriminação previstas nas diretivas relativas à não discriminação e na legislação nacional.

4.3.1. Pedido de alteração do Regulamento sobre a IA

Se o OI considerar que uma prática de IA contradiz fundamentalmente os valores da União em matéria de respeito pela dignidade humana, liberdade, igualdade, democracia e Estado de direito, bem como os direitos fundamentais consagrados na Carta, devem ser apresentadas observações à AFM e à Comissão no sentido de alterarem o Regulamento sobre a IA. o Regulamento sobre a IA estabelece um procedimento através do qual é possível introduzir alterações ao próprio Regulamento sobre a IA em diversas circunstâncias.

O artigo 112.º exige que a Comissão avalie anualmente a necessidade de alterar a lista constante do Anexo III (risco elevado) e do artigo 5.º (sistemas proibidos) e apresente as conclusões dessa avaliação ao Parlamento Europeu. Por conseguinte, é importante comunicar à Comissão, nos termos dos procedimentos previstos no Regulamento sobre a IA, quaisquer preocupações relativas a sistemas de IA que devam ser proibidos ou que apresentem um risco elevado em domínios ou casos de utilização que não constem do Anexo III.

Durante os primeiros cinco anos de vigência do Regulamento sobre a IA da UE (até 1 de agosto de 2029, sendo posteriormente prorrogado automaticamente, salvo oposição), a Comissão tem o poder de adotar atos delegados nas seguintes circunstâncias.⁶⁰

N.º 6 do artigo 6.º	Adicionar, alterar ou eliminar condições para a autoavaliação como de risco não elevado
Artigo 7.º	Alterar o Anexo III, adicionando ou modificando casos de utilização (mas não áreas) e retirando sistemas da lista
N.º 3 do artigo 11.º	Alterar a documentação técnica exigida pelo Anexo IV (nomeadamente à luz do progresso técnico)
N.º 5 do artigo 47.º	Atualizar o conteúdo da declaração de conformidade da UE constante do Anexo V

60 A Comissão dispõe de poderes delegados no que diz respeito à IAFG, mas isso está fora do âmbito do presente documento.

Embora a Comissão não tenha competência para adotar um ato delegado com vista a alterar as rubricas de domínios no Anexo III, deve avaliar, até 2 de agosto de 2028, a necessidade de quaisquer alterações às rubricas de domínios existentes ou de adição de novas rubricas de domínios no Anexo III, bem como de alterações às listas de sistemas que exigem maior transparência e de alterações destinadas a reforçar a eficácia do sistema de supervisão/governança. A Comissão é, então, obrigada a apresentar a sua avaliação ao Parlamento Europeu e ao Conselho.

O Serviço para a IA desenvolverá uma metodologia para a avaliação destes critérios.

4.3.2. Sistema utilizado num setor de risco elevado cujo caso de utilização não está registado no Anexo III do Regulamento sobre a IA

Se um determinado “caso de utilização” não constar do Anexo III do Regulamento sobre a IA, a Comissão tem o poder, nos termos do artigo 7.º, de alterar o referido anexo, adicionando ou modificando casos de utilização, sempre que:

- ▶ o sistema se destine a ser utilizado num domínio abrangido pelo Anexo III; e
- ▶ o impacto negativo sobre os direitos fundamentais (incluindo a discriminação) é equivalente ou superior ao risco de danos ou de impacto negativo representado pelos sistemas de risco elevado já incluídos no Anexo III.

Por conseguinte, se o OI considerar que um caso de utilização que cumpra estes critérios tem um impacto negativo nos direitos fundamentais, mas não consta das listas do Anexo III, deve ponderar a possibilidade de comunicar esse caso de utilização à Comissão, para que seja adicionado à lista nos termos do artigo 7.º do Regulamento sobre a IA.

Os fatores a ter em conta pela Comissão estão previstos no n.º 2 do artigo 7.º do Regulamento sobre a IA e devem ser abordados na elaboração de um relatório:

- ▶ a finalidade prevista do sistema de IA;
- ▶ em que medida um sistema de IA foi utilizado ou é provável que venha a ser utilizado;
- ▶ a natureza e a quantidade dos dados tratados e utilizados pelo sistema de IA, nomeadamente se são tratadas categorias especiais de dados pessoais;
- ▶ o grau de autonomia com que o sistema de IA atua e a possibilidade de um ser humano anular uma decisão ou recomendações que possam conduzir a potenciais danos;
- ▶ em que medida a utilização de um sistema de IA já causou danos à saúde e à segurança, teve um impacto negativo nos direitos fundamentais ou suscitou preocupações significativas relativamente à probabilidade de tais danos ou impacto negativo, tal como demonstrado, por exemplo, por relatórios ou alegações documentadas apresentadas às autoridades nacionais competentes ou por outros relatórios, conforme o caso;
- ▶ a extensão potencial desse dano ou impacto adverso, nomeadamente em termos da sua intensidade e da sua capacidade de afetar várias pessoas ou de afetar de forma desproporcionada um determinado grupo de pessoas;

- ▶ em que medida as pessoas que possam ser prejudicadas ou sofrer um impacto adverso dependem do resultado produzido por um sistema de IA, em particular porque, por razões práticas ou jurídicas, não é razoavelmente possível recusar esse resultado;
- ▶ em que medida existe um desequilíbrio de poder, ou em que as pessoas que possam ser prejudicadas ou sofrer um impacto adverso se encontram numa posição vulnerável em relação a quem é responsável pela implantação de um sistema de IA, nomeadamente devido ao seu estatuto, autoridade, conhecimentos, circunstâncias económicas ou sociais, ou idade;
- ▶ em que medida o resultado produzido por um sistema de IA é facilmente corrigível ou reversível, tendo em conta as soluções técnicas disponíveis para o corrigir ou reverter, não sendo considerados facilmente corrigíveis ou reversíveis os resultados que tenham um impacto adverso na saúde, na segurança ou nos direitos fundamentais;
- ▶ a magnitude e a probabilidade dos benefícios decorrentes da implementação do sistema de IA para pessoas singulares, grupos ou a sociedade em geral, incluindo possíveis melhorias na segurança dos produtos;
- ▶ em que medida o direito da União em vigor prevê:
 - medidas de reparação eficazes relativamente aos riscos decorrentes de um sistema de IA, com exclusão dos pedidos de indemnização;
 - medidas eficazes para prevenir ou minimizar substancialmente esses riscos.

Referências

Bibliografia

Adams-Prassl J., Binns R. and Kelly-Lyth A. (2022), “Directly discriminatory algorithms”, *The Modern Law Review*, 86(1), pp. 144-175. Disponível em: <https://doi.org/10.1111/1468-2230.12759> (consultado a 17 de outubro de 25).

Ahmed M. (2020), “UK passport photo checker shows bias against dark-skinned women”, BBC News. Disponível em: www.bbc.co.uk/news/technology-54349538.amp (consultado a 13 de outubro de 2025).

Allen R. and Masters D. (2019), “Artificial intelligence: the right to protection from discrimination caused by algorithms, machine learning and automated decision-making”, *Journal of the Academy of European Law*. DOI: 10.1007/s12027-019-00582-w (consultado a 19 de junho de 2025).

Allen R. and Masters D. (2020), “Regulating for an equal AI: a new role for equality bodies” Equinet. Disponível em: https://equineteurope.org/publications/regulating-for-an-equal-ai-a-new-role-for-equality-bodies/?__cf_chl_f_tk=3KwuXAuy-Y1rQSy6KKjf6WQaiw8Fzq0tVZpxUk2K39Qs-1782916549-1.0.1.1-nTAmmM4fODMeHv8UOjuY4hye5_yL66T80oAESRgxorA (consultado a 20 de outubro de 2025).

Algorithm Audit (2024a), “Preventing prejudice”. Disponível em: https://algorithmaudit.eu/algoprudence/cases/aa202401_preventing-prejudice/ (consultado a 11 de outubro de 2025).

Algorithm Audit (2024b), “Addendum to preventing prejudice”. Disponível em: https://algorithmaudit.eu/algoprudence/cases/aa202402_preventing-prejudice_addendum/ (consultado a 1 de outubro de 2025)

Algorithm Watch (2022), “Automated decision-making systems and discrimination: A guidebook for anti-discrimination counselling”. Disponível em: <https://algorithmwatch.org/en/autocheck/> (consultado a 29 de setembro de 2025).

Amnesty International (2021), “Xenophobic machines: discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal”. Disponível em: <https://www.amnesty.org/en/documents/eur35/4686/2021/en/> (consultado a 13 de outubro de 2025).

Article 29 Data Protection Working Party (2017a), “Guidelines on data protection impact assessment (DPIA) and determining whether processing is ‘likely to result in a high risk for the purposes of Regulation 2016/679’”. Disponível em: <https://ec.europa.eu/newsroom/article29/items/611236/en> (consultado a 8 de novembro de 2025).

Article 29 Data Protection Working Party (2017b), “Opinion on some key issues of the law enforcement directive (EU 2016/680) – wp258”, European Commission. Disponível em: <https://ec.europa.eu/newsroom/article29/items/610178/en> (consultado a 17 de outubro de 2025).

Article 29 Data Protection Working Party (2018a), “Guidelines on automated individual decision-making and profiling for the purposes of Regulation 2016/679 (WP251rev.01, 17/EN)”, European Commission. Disponível em: <https://ec.europa.eu/newsroom/article29/items/612053/en> (consultado a 10 de novembro de 2025).

Article 29 Data Protection Working Party (2018b), “Guidelines on transparency under Regulation 2016/679 (WP260, 17/EN)”, European Commission. Disponível em: www.edpb.europa.eu/our-work-tools/our-documents/article-29-working-party-guidelines-transparency-under-regulation_en (consultado a 10 de novembro de 2025).

Autoriteit Persoonsgegevens (2024), Final recommendation on supervision of AI: sector and centrally coordinated. Disponível em: www.autoriteitpersoonsgegevens.nl/en/current/final-recommendation-on-supervision-of-ai-sector-and-centrally-coordinated (consultado a 1 de outubro de 2025).

Barocas S., Hardt M. and Narayanan A. (2023), *Fairness and machine learning: limitations and opportunities*, MIT Press, Cambridge, MA.

Barros Vale S. and Zanfir-Fortuna G. (2022), “Automated decision-making under the GDPR: practical cases from courts and data protection authorities”, Future of Privacy Forum. Disponível em: <https://fpf.org/blog/fpf-report-automated-decision-making-under-the-gdpr-a-comprehensive-case-law-analysis/> (consultado a 1 de outubro de 2025).

Big Brother Watch (2025), “Suspicion by design”. Disponível em: <https://bigbrotherwatch.org.uk/campaigns/welfare-data-watch/> (consultado a 10 de novembro de 2025).

Bird K. A., Castleman B. L. and Song Y. (2024), “Are algorithms biased in education? Exploring racial bias in predicting community college student success”, *Journal of Policy Analysis and Management*, Vol. 44 (2), Disponível em: <https://onlinelibrary.wiley.com/doi/full/10.1002/pam.22569> (consultado a 17 de outubro de 2025).

Boscarol F. (2022), “Costly birthplace: discriminating insurance practice”, Algorithm Watch. Disponível em: <https://algorithmwatch.org/en/discriminating-insurance/> (consultado a 13 de outubro de 2025).

Ceross A. (2025), *Understanding artificial intelligence: concepts, limitations, and risks*, Equinet. Disponível em: <https://equineteurope.org/publications/understanding-artificial-intelligence-concepts-limitations-and-risks/> (consultado a 1 de outubro de 2025).

College voor de Rechten van de Mens (2023), “Oordeelnummer 2023-111”. Disponível em: <https://oordelen.mensenrechten.nl/oordeel/2023-111#kop> (consultado a 14 de outubro de 2025).

College voor de Rechten van de Mens (CRM) (2025), “Toetsingskader risicoprofiling”. Disponível em: www.mensenrechten.nl/actueel/nieuws/2025/01/28/nieuw-toetsingskader-tegen-discriminatie-door-risicoprofiling (consultado a 29 de setembro de 2025).

Council of Europe and European Union Agency for Fundamental Rights (2018), *Handbook on European non-discrimination law*, 2nd edn, Publications Office of the European Union. ISBN: 978-92-871-9851-8.

Council of Europe (2025a), "Legal protection against algorithmic discrimination in Europe: current frameworks and remaining gaps". Disponível em: <https://rm.coe.int/legal-protection-eng-web/48802a38d7> (consultado a 4 de junho de 2026).

Council of Europe (2025b), "European policy guidelines on AI and algorithm-driven discrimination for equality bodies and other national human rights structures". Disponível em: <https://rm.coe.int/policy-guidelines-eng-web/48802a38a5> (consultado a 4 de junho de 2026).

Council of Europe (2025c), "Methodology for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of Law (HUDERIA Methodology)". Disponível em: <https://rm.coe.int/prems-002726-gbr-2006-huderia-texte-web-a4/48802ba7b1> (consultado a 19 de junho de 2025).

Council of Europe (2026), "Model for the risk and impact assessment of artificial intelligence systems from the point of view of human rights, democracy and the rule of law (HUDERIA Methodology)". Disponível em: <https://rm.coe.int/prems-002726-gbr-2006-huderia-texte-web-a4/48802ba7b1> (consultado a 19 de junho de 2025).

Crenshaw K. (1991), "Mapping the margins: intersectionality, identity politics, and violence against women of color", *Stanford Law Review*, 43(6), pp. 1241-1299. Disponível em: www.jstor.org/stable/1229039 (consultado a 1 de outubro de 2025).

Crenshaw K. (2015), "Why intersectionality can't wait", *The Washington Post*. Disponível em: www.washingtonpost.com/news/in-theory/wp/2015/09/24/why-intersectionality-cant-wait/ (consultado a 1 de outubro de 2025).

Crowley N. (2023), *Informing the policy agenda: equality bodies making recommendations*, Equinet. Disponível em: <https://equineteurope.org/informing-the-policy-agenda-equality-bodies-making-recommendations/> (consultado a 1 de outubro de 2025).

Dastin J. (2018), "Amazon scraps secret AI recruiting tool that showed bias against women", *Reuters*. Disponível em: www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G (consultado a 10 de novembro de 2025).

Dimitrova D. and De Hert P. (2024), "The LED's right of access to one's data: loopholes on proper access, legality review and data protection authority accountability", *New Journal of European Criminal Law*, 15(1), pp. 12-32. Disponível em: <https://doi.org/10.1177/20322844231214484> (consultado a 17 de outubro de 2025).

Equinet (2017), *Strategic litigation handbook*. Disponível em: <https://equineteurope.org/publications/strategic-litigation-handbook/> (consultado a 29 de setembro de 2025).

Equinet (2022), *Equality Bodies working on cases without an identifiable victim: Actio popularis*. Disponível em: <https://equineteurope.org/equality-bodies-working-on-cases-without-an-identifiable-victim-actio-popularis/> (consultado a 29 de setembro de 2025).

Equinet (2025), Webinar series: equality by design, deliberation and oversight. Disponível em: <https://equineteurope.org/webinar-series-equality-by-design-empowering-equality-bodies-and-civil-society-on-the-interface-between-technical-standards-and-legal-requirements/> (consultado a 1 de outubro de 2025).

Erdogan I. (2023), "Transparency in the face of new technologies: information rights under the law enforcement directive", *Jean Monnet Network on EU Law Enforcement Working Paper Series*. Disponível em: <https://jmn-eulen.nl/papers/events-on-ai/> (consultado a 17 de outubro de 2025).

Erdogan I. (2024), "Diving into the iceberg: establishing transparency in AI for law enforcement", *European Papers*, 9(3), pp. 956-977. Disponível em: www.europeanpapers.eu/e-journal/diving-into-iceberg-establishing-transparency-ai-for-law-enforcement (consultado a 17 de outubro de 2025).

Eticas Foundation (2024), Automating (in)justice? An adversarial audit of riscanvi. Disponível em: <https://www.eticasfoundation.org/automating-injustice-an-adversarial-audit-of-riscanvi/> (consultado a 13 de outubro de 2025).

European Center for Not-for-Profit Law and Danish Institute for Human Rights (2025), A guide to fundamental rights impact assessments (FRIA). Disponível em: <https://ecnl.org/publications/guide-fundamental-rights-impact-assessments-fria> (consultado a 30 de abril de 2026).

European Commission (2019), *Equality law review: European network of legal experts in gender equality and non-discrimination*, Publications Office of the European Union. Disponível em: <https://op.europa.eu/s/AiAN> (consultado a 19 de junho de 2026).

European Commission (2021), *Guidelines on improving the collection and use of equality data*, Publications Office of the European Union. Disponível em: <https://data.europa.eu/doi/10.2838/9725> (consultado a 17 de outubro de 2025).

European Commission (2025), "Supporting the implementation of the AI ACT with clear guidelines". Disponível em: <https://digital-strategy.ec.europa.eu/en/news/supporting-implementation-ai-act-clear-guidelines> (consultado a 1 de maio de 2025).

European Court of Human Rights (2025), "Guide on Article 14 of the European Convention on Human Rights and on Article 1 of Protocol No. 12 to the Convention". Disponível em: https://ks.echr.coe.int/documents/d/echr-ks/guide_art_14_art_1_protocol_12_eng (consultado a 10 de novembro de 2025).

Farkas L. and O'Farrell O. (2015), *Reversing the burden of proof: practical dilemmas at the European and national level*, Publications Office of the European Union. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/a763ee82-b93c-4df9-ab8c-626a660c9da8/language-en> (consultado a 10 de novembro de 2025).

FRA (2018), *Handbook on European non-discrimination law – 2018 edition*. Disponível em: <https://fra.europa.eu/en/publication/2018/handbook-european-non-discrimination-law-2018-edition#> (consultado a 1 de julho de 2026).

FRA (2025), “Assessing high-risk artificial intelligence: fundamental rights risks”. Disponível em: *Assessing High-risk Artificial Intelligence: Fundamental Rights Risks – European Union Agency for Fundamental Rights* (consultado a 4 de junho de 2026).

Fredman S. (2016), *Intersectional discrimination in EU gender equality and non-discrimination law*, European Equality Law Network, Publications Office of the European Union. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/d73a9221-b7c3-40f6-8414-8a48a2157a2f/language-en> (consultado a 17 de outubro de 2025).

González Fuster G. (2020), “Artificial intelligence and law enforcement. Impact on fundamental rights”. European Parliament. Disponível em: <https://op.europa.eu/s/AiyD> (consultado a 12 de novembro de 2025).

Howard E. (2024), “Intersectional discrimination and EU law: time to revisit Parris”, *Sage Journals*. Disponível em: <https://journals.sagepub.com/doi/10.1177/13582291241285336> (consultado a 1 de maio de 2026).

Ilieva S. (2024), *Handbook on identifying and using equality data in legal casework*, Equinet. Disponível em: <https://equineteurope.org/publications/handbook-on-identifying-and-using-equality-data-in-legal-casework/> (consultado a 29 de setembro de 2025).

Information Commissioner’s Office and Equality and Human Rights Commission (2023), *Memorandum of understanding between the Information Commissioner and the Equality and Human Rights Commission*. Disponível em: <https://ico.org.uk/about-the-ico/our-information/working-with-other-bodies/> (consultado a 1 de outubro de 2025).

JuLIA Project (2024), *Handbook: artificial intelligence, judicial decision-making and fundamental rights*, JuLIA 101046631, European Commission (DG JUST – JUST-2021-JTRA). Disponível em: <https://www.julia-project.eu/resources> (consultado a 1 de outubro de 2025).

Lighthouse Reports (2025), “How we investigated Amsterdam’s attempt to build a ‘fair’ fraud detection model”. Disponível em: www.lighthousereports.com/methodology/amsterdam-fairness/ (consultado a 19 de junho de 2026).

Lighthouse Reports (2024), “How we investigated Sweden’s suspicion machine”. Disponível em: www.lighthousereports.com/methodology/sweden-ai-methodology/ (consultado a 20 de outubro de 2025).

Lighthouse Reports (2023), “How we investigated France’s mass profiling machine”. Disponível em www.lighthousereports.com/methodology/how-we-investigated-frances-mass-profiling-machine/ (consultado a 19 de outubro de 2025).

Mahieu R. L., Asghari H. and van Eeten M. (2018), “Collectively exercising the right of access: individual effort, societal effect”, *Internet Policy Review*, 7(3). Disponível em: <https://doi.org/10.14763/2018.3.927> (consultado a 10 de novembro de 2025).

Makkonen T. (2007), *Measuring discrimination: data collection and EU equality law*, Publications Office of the European Union. Disponível em: <https://op.europa.eu/en/publication-detail/-/publication/7d20295d-212c-4acb-bd9f-6f67f4c7ce67> (consultado a 10 de novembro de 2025).

Makkonen T. (2016), *European handbook on equality data: 2016 revision*, Publications Office of the European Union. Disponível em: https://ec.europa.eu/newsroom/just/document.cfm%3Faction%3Ddisplay%26doc_id%3D43205ve-d=2ahUKEwiysrmm&-eeQAxXiWAIHHUBOH9MQFnoECBgQAQusg=AOvVaw1a-G86yvlJ51QDEGbA_FR7L (consultado a 10 de novembro de 2025).

Mantelero A. (2024), “The fundamental rights impact assessment (FRIA) in the AI Act: roots, legal obligations and key elements for a model template”, *Computer Law & Security Review*, 54, p. 106020. Disponível em: www.sciencedirect.com/science/article/pii/S0267364924000864 (consultado a 10 de novembro de 2025).

Mittelstadt B. (2024), *How to use the Artificial Intelligence Act to investigate AI bias and discrimination: a guide for equality bodies*, Equinet. Disponível em: <https://equineteurope.org/publications/how-to-use-the-artificial-intelligence-act-to-investigate-ai-bias-and-discrimination-a-guide-for-equality-bodies/> (consultado a 1 de outubro de 2025).

Mittelstadt B., Wachter, S. and Russell, C. (2023), *The Unfairness of Fair Machine Learning: Levelling down and strict egalitarianism by default*. Available at: <https://arxiv.org/abs/2302.02404> (consultado a 17 de julho de 2026).

Norwegian Data Protection Authority (2023), “Evaluation of the Norwegian Data Protection Authority’s regulatory sandbox for artificial intelligence”. Disponível em: <https://www.datatilsynet.no/en/news/aktuelle-nyheter-2023/the-sandbox-has-been-evaluated/> (consultado a 17 de outubro de 2025).

Parviainen H. (2024), “Challenges of direct discrimination in algorithmic recruitment: insuperable or not?“, *International Journal of Comparative Labour Law and Industrial Relations*, 40, 4 December 2024, pp. 437-466. Disponível em: <https://doi.org/10.54648/ijcl2024017> (consultado a 17 de outubro de 2025).

Purificato I. (2021), “Behind the scenes of Deliveroo’s algorithm: in the blindness of ‘frank’ its discriminatory potential”, *Italian Labour Law e-Journal*, 14(1), pp. 169–194. Disponível em: [doi:10.6092/issn.1561-8048/12990](https://doi.org/10.6092/issn.1561-8048/12990) (consultado a 22 de junho de 2026).

PWC (2024), *Onderzoek misbruik uitwonendenbeurs*. Disponível em: www.twee-dekamer.nl/kamerstukken/detail?id=2024D07564&did=2024D07564 (consultado a 12 de novembro de 2025).

Research Institute – Digital Human Rights Center (2025), “Enlightenment 4.0 – human understanding of AI decision-making: report on the theoretical basis of the right to explanation of individual decision-making under Article 86 AI Act”, Federal

Ministry of Labour and Social Affairs, Health Care and Consumer Protection Republic of Austria. Disponível em: <https://researchinstitute.at/en/enlightenment-4-0-project-results-published-in-english/>; Sítio Web do Ministério dos Assuntos Sociais (consultado a 29 de setembro de 2025).

Schot E. and Davidson D. (2025), “*Onbetrouwbaar algoritme bestempelt jongeren als toekomstig crimineel*, Follow the money”. Disponível em: www.ftm.nl/artikelen/algoritme-bestempelt-jongeren-onterecht-als-toekomstig-crimineel?share=Uom-mUbfeHZLpB371b2sHbWwyodKB4uUhl7QNw2Jm6lIWxJmeq7VOeP7i73ixL-PA%3D (consultado a 13 de outubro de 2025).

Skiotytė G. and Sadauskaitė A. (2026), “A Digital Omnibus: identifying interlinks and possible overlaps between different legal acts in the field of digital legislation to streamline tech rules”, European Parliament, Policy Department for Economy and Growth, Brussels. Disponível em: [https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU\(2026\)772641](https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU(2026)772641) (consultado a 30 de abril de 2026).

Smith E. and Vogell H. (2022), “How your shadow credit score could decide whether you get an apartment”, ProPublica. Disponível em: www.propublica.org/article/how-your-shadow-credit-score-could-decide-whether-you-get-an-apartment (consultado a 17 de outubro de 2025).

Soler Garrido J., De Nigris S., Bassani E., Sanchez I., Tatjana E., Antoine-Alexandre A. and Boulangé T. (2024), *Harmonised standards for the European AI Act*, Joint Research Centre, European Commission. Disponível em: <https://publications.jrc.ec.europa.eu/repository/handle/JRC139430> (consultado a 17 de outubro de 2025).

The Guardian (2021), “What happened when a ‘wildly irrational’ algorithm made crucial healthcare decisions”. Disponível em: www.theguardian.com/us-news/2021/jul/02/algorithm-crucial-healthcare-decisions (consultado a 17 de outubro de 2025).

United Nations (2011), “Guiding principles on business and human rights: implementing the United Nations ‘protect, respect and remedy’ framework”, United Nations, New York and Geneva. Disponível em: <https://digitallibrary.un.org/record/720245?v=pdf> (consultado a 1 de outubro de 2025).

Vogiatzoglou P. and Marquiene T. (2022), Assessment of the implementation of the Law Enforcement Directive, European Parliament. Disponível em: [https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2022\)740209](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740209) (consultado a 17 de outubro de 2025).

Wachter, Mittelstadt, and Russell, 2020, Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, Volume 41, July 2021. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0267364921000406> (consultado a 1 de julho de 2026).

Weerts H., Xenidis R., Tarissan F., Olsen H. P. and Pechenizkiy M. (2023), “Algorithmic unfairness through the lens of EU non-discrimination law: or why the law is not a decision tree”, *Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency*, pp. 805-816.

Weerts H., Kelly-Lyth A., Binns R. and Adams-Prassl J. (2024), “Unlawful proxy discrimination: a framework for challenging inherently discriminatory algorithms”, *The 2024 ACM Conference on Fairness, Accountability, and Transparency*, pp. 1850-1860. doi:10.1145/3630106.3659010.

Xenidis R. (2021), “Tuning EU equality law to algorithmic discrimination: three pathways to resilience”, *Maastricht Journal of European and Comparative Law*, 27(6), pp. 736-758.

Zuiderveen Borgesius F. (2018), “Discrimination, artificial intelligence and algorithmic decision making”, Directorate General of Democracy, Council of Europe. Disponível em: <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73> (consultado a 10 de novembro de 2025).

Legislação

Decisão 2007/533/JAI do Conselho, de 12 de junho de 2007, relativa ao estabelecimento, ao funcionamento e à utilização do Sistema de Informação de Schengen de segunda geração (SIS II), *Jornal Oficial da União Europeia*, L 205.

Diretiva 76/207/CEE do Conselho, de 9 de fevereiro de 1976, relativa à concretização do princípio da igualdade de tratamento entre homens e mulheres no que se refere ao acesso ao emprego, à formação e promoção profissionais e às condições de trabalho, *Jornal Oficial das Comunidades Europeias*, JO, L 39, 14 de fevereiro de 1976, pp. 40-42.

Diretiva 97/80/CE do Conselho, de 15 de dezembro de 1997, relativa ao ónus da prova nos casos de discriminação baseada no sexo, *Jornal Oficial das Comunidades Europeias*, JO, L 014, 20 de janeiro de 1998, pp. 6-8.

Diretiva 2000/43/CE do Conselho, de 29 de junho de 2000, que aplica o princípio da igualdade de tratamento entre as pessoas, sem distinção de origem racial ou étnica, *Jornal Oficial das Comunidades Europeias*, JO, L 180, 19 de julho de 2000, pp. 22-26.

Diretiva 2000/78/CE do Conselho, de 27 de novembro de 2000, que estabelece um quadro geral de igualdade de tratamento no emprego e na atividade profissional, *Jornal Oficial das Comunidades Europeias*, JO, L 303, 2 de dezembro de 2000, pp. 16-22.

Diretiva 2004/113/CE do Conselho, de 13 de dezembro de 2004, que aplica o princípio da igualdade de tratamento entre homens e mulheres no acesso a bens e serviços e seu fornecimento, *Jornal Oficial da União Europeia*, JO, L 373, 21 de dezembro de 2004, pp. 37-43.

Diretiva (UE) 2024/1499 do Conselho, de 7 de maio de 2024, que estabelece as normas aplicáveis aos organismos para a igualdade em questões de igualdade de tratamento entre as pessoas independentemente da sua origem racial ou étnica, de igualdade de tratamento no emprego e na atividade profissional entre as pessoas, independentemente da sua religião ou crença, deficiência, idade ou orientação sexual, e de igualdade de tratamento entre homens e mulheres em matéria

de segurança social e no acesso a bens e serviços e seu fornecimento, e que altera as Diretivas 2000/43/CE e 2004/113/CE, *Jornal Oficial da União Europeia*, JO L, 2024/1499, 2024/1500, 29 de maio de 2024.

Conselho da Europa (1950), Convenção Europeia dos Direitos Humanos, Roma, 4 de novembro de 1950, Série de Tratados Europeus n.º 5.

Conselho da Europa (2000), Protocolo n.º 12 à Convenção para a Proteção dos Direitos Humanos e das Liberdades Fundamentais, Roma, 4 de novembro de 2000, Série de Tratados Europeus n.º 177.

Conselho da Europa (2024), Convenção-Quadro sobre Inteligência Artificial e Direitos Humanos, Democracia e Estado de Direito, Vilnius, 5 de setembro de 2024, Série de Tratados do Conselho da Europa n.º 225.

Diretiva 2006/54/CE do Parlamento Europeu e do Conselho, de 5 de julho de 2006, relativa à aplicação do princípio da igualdade de oportunidades e igualdade de tratamento entre homens e mulheres em domínios ligados ao emprego e à atividade profissional. *Jornal Oficial da União Europeia*, JO, L 204, 26 de julho de 2006, pp. 23-36.

Diretiva (UE) 2023/970 do Parlamento Europeu e do Conselho, de 10 de maio de 2023, para reforçar a aplicação do princípio da igualdade de remuneração por trabalho igual ou de valor igual entre homens e mulheres através de transparência remuneratória e mecanismos que garantam a sua aplicação (Texto relevante para efeitos do EEE), JO L 132, 17 de maio de 2023, pp. 21-44.

Diretiva (UE) 2024/1385 relativa ao combate à violência contra as mulheres e à violência doméstica, JO L, 2024/1385, 24 de maio de 2024.

Diretiva (UE) 2024/1500 do Parlamento Europeu e do Conselho, de 14 de maio de 2024, que estabelece normas aplicáveis aos organismos para a igualdade, *Jornal Oficial da União Europeia*, JO, L, 2024/1500, 29 de maio de 2024.

Orientações da Comissão Europeia sobre práticas proibidas no domínio da inteligência artificial, estabelecidas pelo Regulamento (UE) n.º 2024/1689 (Regulamento sobre a IA), C(2025) 5052 final, 29 de julho de 2025.

Regulamento (UE) 2026/1744 do Parlamento Europeu e do Conselho, de 8 de julho de 2026, que altera os Regulamentos (UE) 2024/1689, (UE) 2018/1139 e (UE) 2023/1230 no que diz respeito à simplificação da aplicação das regras harmonizadas em matéria de inteligência artificial (Regulamento Omnibus Digital em matéria de IA). Disponível em: <https://eur-lex.europa.eu/eli/reg/2026/1744/oj/eng>, consultado a 24 de julho de 2026.

Regulamento (UE) n.º 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 (Regulamento Geral sobre a Proteção de Dados, RGPD), *Jornal Oficial da União Europeia*, JO, L 119, 4 de maio de 2016, pp. 1-88.

Proposta de Regulamento do Parlamento Europeu e do Conselho que altera os Regulamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 e (UE) 2023/2854 e as Diretivas 2002/58/CE, (UE) 2022/2555 e (UE) 2022/2557 no respeitante à simplifi-

cação do quadro legislativo digital e que revoga os Regulamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 e a Diretiva (UE) 2019/1024 (Omnibus Digital), COM/2025/837 final, [EUR-Lex - 52025PC0837 - EN - EUR-Lex](#).

Resolução legislativa do Parlamento Europeu, de 16 de junho de 2026, sobre a proposta de regulamento do Parlamento Europeu e do Conselho no respeitante à simplificação da aplicação das regras harmonizadas em matéria de inteligência artificial. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-10-2026-0198_EN.html#title2, consultada a 25 de junho de 2026.

Regulamento (UE) n.º 2019/1020 do Parlamento Europeu e do Conselho, de 20 de junho de 2019, relativo à fiscalização do mercado e à conformidade dos produtos, *Jornal Oficial da União Europeia*, JO, L 169, 25 de junho de 2019, pp. 1-44.

Regulamento (UE) n.º 2023/988 do Parlamento Europeu e do Conselho, de 10 de maio de 2023, relativo à segurança geral dos produtos, que altera o Regulamento (UE) n.º 1025/2012 do Parlamento Europeu e do Conselho e a Diretiva (UE) 2020/1828 do Parlamento Europeu e do Conselho e que revoga a Diretiva 2001/95/CE do Parlamento Europeu e do Conselho e a Diretiva 87/357/CEE do Conselho (Texto relevante para efeitos do EEE), *Jornal Oficial da União Europeia*, JO L 135, 23 de maio de 2023, pp. 1-51.

Regulamento (UE) n.º 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial (Regulamento sobre a Inteligência Artificial), *Jornal Oficial da União Europeia*, JO, L 2024/1689, 12 de julho de 2024.

Regulamento (CE) n.º 767/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, relativo ao Sistema de Informação sobre Vistos (VIS) e ao intercâmbio de dados entre os Estados-Membros sobre os vistos de curta duração (Regulamento VIS), *Jornal Oficial da União Europeia*, JO, L 218, 13 de agosto de 2008, pp. 60-81.

Regulamento (UE) n.º 603/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo à criação do sistema «Eurodac» de comparação de impressões digitais para efeitos da aplicação efetiva do Regulamento (UE) n.º 604/2013, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de proteção internacional apresentado num dos Estados-Membros por um nacional de um país terceiro ou um apátrida, e de pedidos de comparação com os dados Eurodac apresentados pelas autoridades responsáveis dos Estados-Membros e pela Europol para fins de aplicação da lei e que altera o Regulamento (UE) n.º 1077/2011 que cria uma Agência europeia para a gestão operacional de sistemas informáticos de grande escala no espaço de liberdade, segurança e justiça (reformulação), *Jornal Oficial da União Europeia*, JO, L 180, 29 de junho de 2013, pp. 1-30.

Lei sueca contra a discriminação, de 2008: 567.

Jurisprudência

Andersen contra Region Syddanmark, (2010), Tribunal de Justiça da União Europeia, Processo C-499/08. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TX-T/?uri=oj:JOC_2010_346_R_0007_01 (consultado a 1 de julho de 2026)

Association Belge des Consommateurs Test-Achats ASBL e outros contra Conseil des ministres (2011), Tribunal de Justiça da União Europeia, Processo C-236/09; ECLI:EU:C:2011:100. Disponível em: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62009CJ0236> (consultado a 12 de novembro de 2025).

CHEZ Razpredelenie Bulgaria AD contra Komisia za zashtita ot diskriminatsia (2015), Tribunal de Justiça da União Europeia, Processo C-83/14; ECLI:EU:C:2015:480. Disponível em: <https://eur-lex.europa.eu/legal-content/NL/ALL/?uri=CELEX:62014CJ0083> (consultado a 10 de novembro de 2025).

David L. Parris contra Trinity College Dublin e outros (2016), Tribunal de Justiça da União Europeia, Processo C-232/09; ECLI:C:2010:674. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62015CJ0443> (consultado a 1 de maio de 2026).

D.H. e outros contra a República Checa (2007), Tribunal Europeu dos Direitos Humanos, Recurso n.º 57325/00. Disponível em: [https://hudoc.echr.coe.int/fre#{%22itemid%22:\[%22001-83256%22\]}](https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-83256%22]}) (consultado a 1 de outubro de 2025).

Enderby contra Frenchay Health Authority e Secretary of State for Health (1993), Tribunal de Justiça da União Europeia, Processo C-127/92; ECLI:EU:C:1993:313. Disponível em: <https://curia.europa.eu/juris/liste.jsf?num=C-127/92> (consultado a 1 de outubro de 2025).

Filcams Cgil de Bolonha e outros contra (...) S.R.L. (2020), Tribunal de Bolonha, Despacho n.º 2949/2019. Disponível em: <https://apps.eurofound.europa.eu/platformeconomydb/italian-court-rules-that-the-deliveroo-algorithm-discriminates-workers-106121>.

Frédéric Hay contra Crédit Agricole mutuel de Charente Maritime et des Deux-Sèvres (2012), Tribunal de Justiça da União Europeia, Processo C-267-12; ECLI:EU:C:2013:823. Disponível em: <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62012CJ0267> (consultado a 12 de novembro de 2025).

Galina Meister contra Speech Design Carrier Systems GmbH (2012), Tribunal de Justiça da União Europeia, Processo C-415/10; ECLI:EU:C:2012:217. Disponível em: <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62010CJ0415> (consultado a 12 de novembro de 2025).

Glukhin contra a Rússia (2023), Tribunal Europeu dos Direitos Humanos, Recurso n.º 11519/20. Disponível em: <https://hudoc.echr.coe.int/eng?i=001-225655> (consultado a 7 de outubro de 2025).

Handels- og Kontorfunktionærernes Forbund I Danmark contra Dansk Arbejdsgiverforening, em nome da Danfoss (1989), Tribunal de Justiça da União Europeia, Processo C-109/99; ECLI:EU:C:1989:383. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61988CJ0109> (consultado a 12 de novembro de 2025).

Helga Nimz contra Freie und Hansestadt Hamburg (1991), Tribunal de Justiça da União Europeia, Processo C-184/89; ECLI:EU:C:1991:50. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:61989CJ0184> (consultado a 12 de novembro de 2025).

Hoogendijk contra os Países Baixos (2005), Tribunal Europeu dos Direitos Humanos, Recurso n.º 58641/00. Disponível em: <https://hudoc.echr.coe.int/eng?i=001-68064> (consultado a 1 de outubro de 2025).

Inge Nolte contra Landesversicherungsanstalt Hannover (1995), Tribunal de Justiça da União Europeia, Processo C-317-93; ECLI:EU:C:1995:438. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:61993CJ0317> (consultado a 12 de novembro de 2025).

Ingeniørforeningen i Danmark contra Region Syddanmark (2010), Tribunal de Justiça da União Europeia, Processo C-499/08; ECLI:EU:C:2010:600. Disponível em: <https://curia.europa.eu/juris/documents.jsf?critereEcli=ECLI:EU:C:2010:600> (consultado a 1 de outubro de 2025).

Ingrid Rinner-Kühn contra FWW Spezial-Gebäudereinigung GmbH & Co. KG (1989), Tribunal de Justiça da União Europeia, Processo C-171/88; ECLI:EU:C:1989:328. Disponível em: <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:61988CJ0171> (consultado a 12 de novembro de 2025).

IX contra Wabe eV e MH Müller Handels GmbH contra MJ (2021), Tribunal de Justiça da União Europeia, Processos C-804/18 e C-341/19; ECLI:EU:C:2021:144. Disponível em: <https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:62019CC0341> (consultado a 7 de outubro de 2025).

James contra Câmara Municipal de Eastleigh (1990), Câmara dos Lordes, 2 AC 751. Disponível em: <https://www.bailii.org/uk/cases/UKHL/1990/6.html> (consultado a 12 de novembro de 2025).

Jyske Finans contra Ligebehandlingsnævnet (2017), Tribunal de Justiça da União Europeia, C-668/15; ECLI:EU:C:2017:278. Disponível em: <https://curia.europa.eu/juris/liste.jsf?num=C-668/15> (consultado a 10 de novembro de 2025).

Kelly contra National University of Ireland (University College, Dublin) (2011), Tribunal de Justiça da União Europeia, Processo C-104/10; ECLI:EU:C:2011:506. Disponível em: <https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:62010CJ0104> (consultado a 10 de novembro de 2025).

La Quadrature du Net e outros contra Premier ministre e Ministre de la Culture (2024), Tribunal de Justiça da União Europeia, Processo C-470/21; ECLI:EU:C:2024:370. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0470> (consultado a 14 de novembro de 2025).

(Loredas) HJ contra os EUA e a MU (2024), Tribunal de Justiça da União Europeia, Processo C-531-23; ECLI:EU:C:2024:1050. Disponível em: <https://eur-lex.europa.eu/legal-content/nl/TXT/?uri=CELEX:62023CJ0531> (consultado a 12 de novembro de 2025).

M. A. De Weerd, née Roks, e outros contra Bestuur van de Bedrijfsvereniging voor de Gezondheid, Geestelijke en Maatschappelijke Belangen e outros (1994), Tribunal de Justiça da União Europeia, Processo C-343/92; ECLI:EU:C:1994:71. Disponível em: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:61992CJ0343> (consultado a 12 de novembro de 2025).

Manjang contra Uber Eats UK Ltd e outros (2021), Tribunal do Trabalho, Processo n.º 3206212/2021. Disponível em: www.gov.uk/employment-tribunal-decisions/mr-p-e-manjang-v-uber-eats-uk-ltd-and-others-3206212-slash-2021 (consultado a 7 de outubro de 2025).

Maria Kowalska contra Freie und Hansestadt Hamburg (1990), Tribunal de Justiça da União Europeia, C-33-89; ECLI:EU:C:1990:265. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:61989CJ0033> (consultado a 12 de novembro de 2025).

Minoo Schuch-Ghannadan contra Medizinische Universität Wien (2019), Tribunal de Justiça da União Europeia, C-274/18; ECLI:EU:C:2019:828. Disponível em: <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62018CJ0274> (consultado a 10 de novembro de 2025).

Tadao Maruko contra Versorgungsanstalt der deutschen Bühnen (2008), Tribunal de Justiça da União Europeia, C-267/06; ECLI:EU:C:2008:179. Disponível em: <https://curia.europa.eu/juris/liste.jsf?num=C-267/06> (consultado a 12 de novembro de 2025).

Verli Hariev Belov contra CHEZ Elektro Bulgaria AD e outros (2013), Tribunal de Justiça da União Europeia, Processo C-394/11; ECLI:EU:C:2013:48. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62011CJ0394> (consultado a 17 de outubro de 2025).

VL contra Szpital Kliniczny im. dra J. Babińskiego Samodzielny Publiczny Zakład Opieki Zdrowotnej w Krakowie (2021), Tribunal de Justiça da União Europeia, Processo C-16/19; ECLI:EU:C:2021:64, n.º 48. Disponível em: <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:62019CJ0016> (consultado a 7 de outubro de 2025).

Anexo A

Modelo de pedido de acesso da pessoa titular dos dados (PAPTD)

Nota: um PAPTD pode ser redigido em termos gerais ou de forma mais específica, tendo cada abordagem as suas próprias vantagens e riscos.

Os pedidos específicos podem aumentar a probabilidade de se obter a informação exata pretendida, reduzindo a necessidade de correspondência de acompanhamento e agilizando o processo. No entanto, na prática, as organizações contactadas só costumam dar uma resposta personalizada após um pedido de acompanhamento. Os pedidos definidos de forma restrita numa fase inicial podem sobrecarregar a pessoa titular dos dados, que poderá não ter conhecimento das atividades de tratamento relevantes ou da terminologia utilizada, aumentando o risco de omissão de informações e dando azo a interpretações restritivas por parte de quem é responsável pelo tratamento de dados.

Ao abrigo da proposta de regulamento “*Omnibus Digital*”⁶¹, tal será formalizado. Estabelece que os PAPTD devem ser “tão específicos quanto possível”, ao passo que “os pedidos excessivamente genéricos e indiferenciados também devem ser considerados excessivos”, sugerindo que os pedidos genéricos e indiferenciados podem ser rejeitados por serem excessivos.

Este modelo serve apenas como exemplo e deve ser adaptado ao caso específico.

[Nome e morada da pessoa titular dos dados]

[opcional: número de telefone e endereço de e-mail da pessoa titular dos dados]

[Data do pedido]

[Dados de quem é responsável pelo tratamento de dados – Endereço da empresa]⁶²

61 Considerando 35, artigo 3.º, da Proposta de Regulamento do Parlamento Europeu e do Conselho que altera os Regulamentos (UE) 2016/679, (UE) 2018/1724, (UE) 2018/1725 e (UE) 2023/2854 e as Diretivas 2002/58/CE, (UE) 2022/2555 e (UE) 2022/2557 no respeitante à simplificação do quadro legislativo digital e que revoga os Regulamentos (UE) 2018/1807, (UE) 2019/1150, (UE) 2022/868 e a Diretiva (UE) 2019/1024 (Omnibus Digital)

62 Enviar a quem é responsável pelo tratamento de dados: os seus dados de contacto encontram-se normalmente na política de privacidade ou no aviso legal da organização, no seu sítio Web. Nos casos que envolvam um sistema de IA, quem é responsável pelo tratamento de dados será, normalmente, quem é responsável pela implantação do sistema (a organização que o utiliza, ou seja, a entidade com a qual a pessoa titular dos dados interagiu durante o processo em questão, como um banco, uma seguradora, uma universidade ou uma entidade empregadora). A organização sem fins lucrativos Datenanfragen.de e.V., que gere o sítio Web datarequests.org (disponível também em várias outras línguas), mantém uma [base de dados de empresas](#) com as informações de contacto relevantes para pedidos relacionados com a privacidade de muitas empresas.

Pedido de acesso da pessoa titular dos dados nos termos do artigo 15.º do RGPD

A quem possa interessar,

Por meio do presente, exerço os meus direitos ao abrigo do **artigo 15.º do Regulamento Geral sobre a Proteção de Dados (RGPD)** e solicito a confirmação de se estão ou não a tratar dados pessoais que me dizem respeito.

Caso estejam a tratar os meus dados pessoais, peço-lhes que me forneçam as seguintes informações, em conformidade com o artigo 15.º do RGPD.

1. Acesso aos meus dados pessoais para as finalidades X

- ▶ Uma cópia de todos os dados pessoais que me dizem respeito e que tenham sido utilizados ou tidos em conta para os seguintes fins: [Insira aqui os objetivos centrais do seu caso; por exemplo, abrir ou gerir uma conta bancária em meu nome/celebrar, renovar ou prorrogar o meu contrato de telemóvel/tratar ou avaliar a minha elegibilidade para [insira o benefício específico]/ tratar ou avaliar a minha candidatura a um emprego/determinar o meu acesso a contas online, aplicações ou subscrições digitais/atribuir-me viagens ou encomendas de entrega na plataforma, etc.]

2. Informações sobre finalidades adicionais do tratamento de dados

- ▶ Informações sobre quaisquer outras finalidades para as quais os meus dados pessoais tenham sido ou estejam a ser tratados, para além das acima referidas.
- ▶ Uma descrição das categorias de dados pessoais em causa.

3. Divulgação de informações a entidades terceiras

- ▶ As/Os destinatárias/os ou categorias de destinatárias/os a quem os meus dados pessoais foram divulgados, juntamente com cópias dos dados partilhados e a finalidade da partilha, bem como a(s) data(s) da divulgação.

4. Tomada de decisões automatizada e definição de perfis

- ▶ Informações sobre se foi realizada uma tomada de decisão automatizada, tal como referida nos números 1 e 4 do artigo 22.º do RGPD, relativamente aos meus dados pessoais.
- ▶ Se for esse o caso, peço-lhes que me forneçam informações relevantes sobre a lógica subjacente, incluindo as categorias de dados pessoais, os procedimentos e princípios utilizados para obter um resultado específico, bem como as consequências previstas desse tratamento para mim.

5. Detalhes da definição de perfis

- ▶ Informações sobre se foi realizada alguma definição de perfis com base nos meus dados pessoais.
- ▶ Se for esse o caso, por favor, forneçam-me o conteúdo desse perfil e expliquem como foi criado.

Caso os meus dados pessoais sejam transferidos para um país terceiro ou para uma organização internacional, solicito que me sejam comunicadas as garantias adequadas, nos termos do artigo 46.º do RGPD, relativas a essa transferência.

Peço que me disponibilizem os dados pessoais que me dizem respeito, tal como solicitei, num formato estruturado, de uso comum e legível por máquina, conforme previsto no n.º 1 do artigo 20.º do RGPD.

O meu pedido inclui explicitamente quaisquer outros serviços e empresas relativamente aos quais seja responsável pelo tratamento, tal como definido no n.º 7 do artigo 4.º do RGPD.

Conforme previsto no n.º 3 do artigo 12.º do RGPD, devem fornecer-me as informações solicitadas sem demora injustificada e, em qualquer caso, no prazo de um mês a contar da receção do pedido. Caso seja necessária uma prorrogação de, no máximo, mais dois meses, por favor, informem-me em conformidade.

De acordo com o n.º 3 do artigo 15.º do RGPD, devem responder a este pedido sem que isso me acarrete quaisquer custos.

[Como prova da minha identidade, junto uma cópia do meu passaporte/carta de condução, etc.] ou

[Introduza aqui os seus dados de identificação. Isto inclui frequentemente informações como o seu nome, a sua data de nascimento, a sua morada, o seu endereço de e-mail e assim por diante.]

Caso não respondam ao meu pedido dentro do prazo indicado, reservo-me o direito de intentar uma ação judicial contra vocês e de apresentar uma queixa junto da autoridade de controlo competente.

Desde já, muito obrigado.

Com os melhores cumprimentos,

[Introduza aqui o seu nome]

Anexo B

Modelo para solicitar explicações nos termos do artigo 86.º do Regulamento sobre a IA

O modelo que se segue incorpora uma versão desenvolvida pelo Instituto de Investigação – Centro de Direitos Humanos Digitais (2025b), tal como publicada no [sítio Web do Ministério dos Assuntos Sociais da Áustria](#).

[Nome e morada da pessoa afetada]

[opcional: número de telefone e endereço de e-mail da pessoa afetada]

[Data do pedido]

[Informações sobre quem é responsável pela implantação dos sistemas de IA⁶³]

Pedido de explicações nos termos do artigo 86.º do Regulamento sobre a IA

A quem possa interessar,

Refiro-me à decisão que me diz respeito [descrição da decisão, por exemplo, a recusa de um pedido de empréstimo, a avaliação de risco recebida, a atribuição de uma pontuação de crédito], que recebi em [data de receção da decisão].

Esta decisão [] tem efeitos jurídicos para mim, uma vez que [explique sucintamente o impacto da decisão, por exemplo, a rejeição de um pedido de empréstimo, a recusa de acesso a determinados serviços, o aumento dos preços dos seguros, etc.].

[ou] tem um impacto significativo e negativo sobre mim, uma vez que [apresente as razões para essa limitação, tais como discriminação com base em critérios diferenciadores, ou a orientação de anúncios de apostas desportivas para pessoas com dependência do jogo].

Por meio do presente, faço valer o meu direito a explicações, nos termos do artigo 86.º do Regulamento (UE) n.º 2024/1689 (Regulamento sobre a IA), e solicito uma explicação clara e substantiva sobre o papel do sistema de IA no processo de tomada de decisão e sobre os principais elementos da decisão tomada.

63 Enviar a quem é responsável pela implantação do sistema de IA: a organização que o utiliza – ou seja, a entidade com a qual a pessoa titular dos dados interagiu durante o processo em questão, como um banco, uma seguradora, uma universidade ou uma entidade empregadora. Se se tratar de uma autoridade pública - ou de uma entidade que atue em seu nome -, consulte os dados de contacto na Parte C da base de dados da UE. Em qualquer outro caso, procure os dados de contacto de quem é responsável pela implantação na interface do sistema de IA, na política de privacidade da organização ou no aviso legal disponível no seu sítio Web. Se não for explicitamente indicado quem é responsável pela implantação, utilize os dados de contacto de quem é responsável pelo tratamento de dados, que, normalmente, será também responsável pela implantação do sistema.

Para o efeito, solicito as seguintes informações.

1. Papel do sistema de IA no processo de tomada de decisões

- ▶ Em que medida e de que forma o sistema de IA utilizado contribuiu para o processo de tomada de decisão?

2. Principais elementos da decisão tomada

- ▶ Quais foram as principais razões por detrás da decisão, incluindo os critérios determinantes, os dados de entrada e as decisões preliminares que influenciaram a decisão tomada?
- ▶ Que outras implicações tem esta decisão para mim e como é que esses efeitos foram avaliados?
- ▶ Como foram ponderados os critérios que influenciaram a decisão e porquê?

3. Revisão humana e fundamentação [não obrigatório]

- ▶ A decisão foi tomada pelo sistema de IA de forma totalmente automatizada ou foi revista por um responsável humano? Se for este o caso, como é que essa revisão decorreu exatamente e quem ou que departamento foi responsável por ela?
- ▶ [opcional, se aplicável] Em que base contratual ou jurídica se fundamenta a decisão?

[Como prova da minha identidade, junto uma cópia do meu passaporte/carta de condução, etc.] ou

[Introduza aqui os seus dados de identificação. Estes incluem frequentemente informações como o seu nome, a sua data de nascimento, a sua morada, o seu endereço de e-mail e assim por diante.]

Solicito formalmente que me forneçam as informações solicitadas no prazo de [x mês/es], [por escrito], gratuitamente e de forma compreensível. Em caso de dúvida, não hesitem em contactar-me [para o envio em papel, utilize os dados de contacto indicados acima].

Agradeço desde já pela tramitação do meu pedido e aguardo com expectativa a vossa resposta atempada.

Com os melhores cumprimentos,

[Nome da pessoa afetada]

Anexo C

Exemplos da utilização de algoritmos e IA

Este anexo inclui exemplos em que os algoritmos e os sistemas de IA são frequentemente utilizados. Está ordenado por setor, para que se possa facilmente determinar a provável intervenção algorítmica. Para elaborar esta lista, recorremos a Allen e Masters (2020) e à Algorithm Watch (2022), cujos dados podem ser consultados na lista de referências.

Setor	Exemplo
Setor bancário	Pontuação de crédito
	Automatização do procedimento de aceitação de clientes
	Deteção de fraudes ou de atividades relacionadas com o branqueamento de capitais
Serviços de assistência social para crianças e jovens	Prever as necessidades futuras de serviços de assistência social para uma criança
Educação	Admissão
	Automatização da distribuição de estudantes pelas escolas, universidades ou cursos
	Supervisão automatizada
	Prever ou detetar o absentismo escolar e o abandono escolar precoce
	Detetar problemas de aprendizagem
Emprego	Seleção de candidaturas a empregos ou seleção de currículos
	Agências de (des)emprego que preveem a probabilidade de encontrar emprego
	Atribuição de ofertas de emprego às pessoas que se candidatam
	Alocação de pessoas que se candidatam a emprego a formação ou acompanhamento
	Análise de entrevistas (de saída)
Cuidados de saúde	Prever o risco de doença
	Sistemas de diagnóstico
	Prever o número de idosas e idosos que necessitam de cuidados adicionais

Setor	Exemplo
Habitação	Avaliação automatizada de potenciais inquilinas/os
	Formulários online
	Verificação de solvabilidade
	Anúncios de apartamentos em plataformas online: que anúncios são apresentados a quem? (Colocação automática)
Imigração e gestão das fronteiras	Reconhecimento facial de pessoas que constam numa lista de vigilância
	Automatização do processo de aceitação dos pedidos de visto
	Análise automatizada de documentos de viagem
Seguros	Formulários online
	Algoritmos de fixação de preços
	Automatização do procedimento de aceitação de clientes
	Tratamento automático de sinistros
	Deteção de fraudes
Processo judicial	Colaboração na elaboração de leis
Justiça	Sugestão de pena com base nos dados
Polícia	Prever a ocorrência de crimes em determinados bairros ou zonas (polícia preditiva geográfica)
	Prever comportamentos desordeiros ou violentos
	Ferramentas de avaliação de risco ou de definição de perfis utilizadas para prever o risco futuro de uma pessoa singular cometer um crime, incluindo a reincidência, ou, de forma mais geral, para identificar pessoas “perigosas” ou “relevantes” (polícia preditiva individual)
	Avaliar ou estimar a probabilidade de uma pessoa ser autor(a) de um crime já cometido (polícia preditiva individual)
	Vigilância por câmaras que deteta atividades criminosas
Prestações sociais	Formulários online
	Prever fraudes ou erros
	Automatização no processamento de prestações sociais
Impostos	Prever fraudes ou erros

Anexo D

Exemplos de discriminação algorítmica ou de risco de discriminação

Setor ou tecnologia	Descrição do algoritmo	Descrição da prática discriminatória	Fonte
Setor bancário	“Pontuação” ou avaliação da solvabilidade	O sistema TDA tinha regras em vigor que o levaram a concluir que uma “mulher de 40 anos” não era solvente.	Algorithm Watch (2022) (p. 6) (Caso semelhante na Finlândia, disponível aqui)
Educação	Algoritmo de previsão da conclusão de um curso ou grau académico	Aos grupos minoritários sub-representados foi-lhes atribuído, de forma consistente, um risco mais elevado, a par de uma pontuação de exatidão mais baixa.	Bird, Castleman e Song (2024)
Tecnologia de reconhecimento facial	Tecnologia capaz de identificar ou comparar imagens faciais	Existem diferenças de exatidão entre diferentes grupos demográficos, tais como a idade, o género e a cor da pele. Estas diferenças podem dar origem a casos de discriminação. O organismo para a igualdade neerlandês afirmou que as organizações têm de provar que a sua tecnologia não discrimina, invertendo o ónus da prova.	College voor de Rechten van de Mens (2023)
Cuidados de saúde	Algoritmo para a atribuição de “cuidados necessários” a pacientes	Sistema de pontuação arbitrário, que conduz a uma distribuição diferente das horas em casos semelhantes.	The Guardian (2021)

Setor ou tecnologia	Descrição do algoritmo	Descrição da prática discriminatória	Fonte
Habitação	Algoritmos de seleção de inquilinas/os, atribuição de pontuação de risco	Seleção de inquilinas/os com base em características cuja ligação ao risco não foi comprovada.	Smith e Vogell (2022)
Seguros	Algoritmo de fixação de preços	A discriminação direta com base na cidadania/nacionalidade influenciou o preço do seguro automóvel em perfis que, de resto, eram idênticos.	Boscarol (2022)
Imigração e gestão de fronteiras	Análise de documentos de viagem, tecnologia de reconhecimento facial	Discriminação direta, na medida em que a tecnologia produzia resultados errados com maior frequência nas imagens de pessoas de pele mais escura do que nas de pele mais clara.	Ahmed (2020)
Sistema judicial/ assistência social para crianças e jovens	Avaliação do risco de reincidência	Certas nacionalidades resultaram numa pontuação de risco mais elevada, aumentando a probabilidade de serem alvo de um processo judicial.	Schot e Davidson (2025)
Polícia/ aplicação da lei	Avaliação do risco de reincidência	O sistema de IA não apresentava transparência, explicabilidade nem robustez. Pontuações de risco mais elevadas e inconsistentes para pessoas sem “fatores de estabilidade social”, na sua maioria pessoas singulares mais jovens.	Fundação Éticas (2024)
Prestações sociais	Detetar pedidos incorretos ou fraudulentos de subsídios para cuidados infantis	Discriminação racial, em que aos pedidos apresentados por cidadãs e cidadãos não neerlandeses eram sistematicamente atribuídas pontuações de risco mais elevadas.	Amnistia Internacional (2021)

Setor ou tecnologia	Descrição do algoritmo	Descrição da prática discriminatória	Fonte
Prestações sociais	O sistema de assistência social agrava a exclusão	Discriminação indireta através de um critério aparentemente neutro que coloca os grupos demográficos protegidos em desvantagem.	Amnistia Internacional (2023)
Deteção de fraudes na segurança social	Sistema de pontuação do risco de fraude utilizado para identificar beneficiárias/os de prestações sociais para uma análise mais aprofundada	O modelo identificou de forma desproporcional mulheres, migrantes, pessoas com baixos rendimentos e pessoas sem formação universitária como suspeitas.	Lighthouse Reports (2024)
Deteção de fraudes na segurança social	Sistema de pontuação do risco de fraude utilizado para identificar beneficiárias/os de prestações sociais para uma análise mais aprofundada (CNAF)	O sistema foi contestado por gerar efeitos discriminatórios, diretos e indiretos, para mulheres, pessoas com deficiência e pessoas em situação de pobreza.	La Quadrature du Net (2024) Lighthouse Reports (2023)

Anexo E

Proxies

Do ponto de vista da ciência de dados e da análise de dados, as variáveis proxy substituem outras variáveis, por exemplo, quando estas não podem ser observadas ou medidas diretamente. As variáveis proxy permitem tirar conclusões sobre determinadas características sem registrar essas características diretamente. Por exemplo, “30 anos de experiência profissional” indica que a pessoa deve ter, pelo menos, cerca de 45 anos (Algorithm Watch 2022).

No contexto da legislação em matéria de não discriminação e de sistemas algorítmicos/de IA, os termos “proxies” referem-se a características, atributos ou combinações destas que, por si só, não constam da lista dos motivos de discriminação explicitamente proibidos ao abrigo do quadro jurídico relevante, mas que estão correlacionadas com esses motivos de tal forma que a sua utilização pode conduzir a uma discriminação ilegal.

A este respeito, é possível identificar dois tipos de proxies.

- a. Proxies estatísticos: características (ou combinações das mesmas) que se correlacionam com motivos legalmente protegidos e cuja utilização pode prejudicar de forma desproporcionada as pessoas pertencentes a um grupo protegido. Esses proxies estão normalmente associados à discriminação indireta. Por exemplo, na maioria dos países europeus, existe uma correlação entre o nível de escolaridade e a raça ou a origem étnica.
- b. Proxies indissociáveis: uma característica (ou combinações das mesmas) que estão indissociavelmente ligadas a um atributo protegido, de tal forma que a sua utilização reflete uma prática intrinsecamente discriminatória. Esses proxies estão normalmente associados à discriminação direta. Por exemplo, a gravidez tem sido considerada indissociável do sexo (ver tabela 8 abaixo).

Embora ainda não esteja esclarecido que nível de correspondência entre um proxy e um grupo protegido deve existir para constituir discriminação direta, uma ligação indissociável não exige uma correspondência total (100%) (Parviainen 2024). Adams-Prassl, Binns e Kelly-Lyth consideraram que é necessário um “grau suficiente de correspondência” (2023), ao passo que Weerts et al. (2024) propuseram que o proxy e o fator protegido devem estar “pelo menos fortemente associados e, possivelmente, até mesmo relacionados de forma determinística”. Weerts et al. salientam a relevância da questão do “se não fosse por”: uma pessoa requerente num país onde a idade de reforma varia consoante o sexo poderia argumentar, com razão, que teria atingido a idade de reforma se não fosse pelo seu sexo; um casal do mesmo sexo que viva num país onde o casamento entre pessoas do mesmo sexo é proibido poderia facilmente afirmar que estaria casado se não fosse pela sua orientação sexual; uma mulher poderia argumentar, com razão, que não estaria grávida se não fosse pelo seu sexo; e uma mulher muçulmana poderia argumentar que não usaria o véu se não fosse pela sua religião.

A existência de uma ligação indissociável num determinado caso requer uma avaliação judicial caso a caso, na qual se deve atribuir especial importância a critérios contextuais - em vez de limiares estatísticos precisos -, em consonância com a abordagem do TJUE em processos de discriminação (ver, por exemplo, IX contra WABE eV e MH Müller Handels GmbH contra MJ, parágrafo 78, em que foi atribuída importância ao tipo de sinais em causa). Consulte a tabela abaixo para ver exemplos de diferentes tipos de proxies para características protegidas.

Tabela 8. Exemplos de proxies conhecidos (conforme referido, entre outros, em CRM 2025, Weerts et al. 2024, Algorithm Watch 2022)

Característica	Proxy para	Tipo de proxy
30 anos de experiência profissional (Algorithm Watch 2022)	Pessoa com mais de 45 anos	Indissociável
Gravidez (<i>Dekker contra Stichting voor Jong Volwassenen (VJV-Centrum) Plus</i> , 1990)	Sexo	Indissociável
Estado civil (<i>Tadao Maruko contra Versorgungsanstalt der deutschen Bühnen</i> , 2008; <i>Frédéric Hay contra Crédit Agricole mutuel de Charente Maritime et des Deux-Sèvres</i> , 2012)	Orientação sexual, em países que não permitem o casamento entre pessoas do mesmo sexo	Indissociável, em países que não permitem o casamento entre pessoas do mesmo sexo
Idade de reforma em função do sexo (<i>James contra Câmara Municipal de Eastleigh</i> , 1990, §10)	Sexo	Indissociável
Língua ou nível de proficiência linguística	Raça	Proxy estatístico ou indissociável
Alfabetização	Raça (dependendo do país, este critério pode também servir como proxy da idade e do sexo)	Proxy estatístico
Nível de escolaridade	Raça ou origem étnica	Proxy estatístico
Código postal ou bairro	Raça (embora nos bairros haja segregação)	Proxy estatístico
Rendimento	Raça, sexo	Proxy estatístico
Número de pessoas no agregado familiar ou na família imediata	Raça (sexo)	Proxy estatístico

Característica	Proxy para	Tipo de proxy
Local de nascimento	Raça	Proxy estatístico
Receção de prestações financeiras essenciais	Raça	Proxy estatístico
Religião	Raça	Proxy estatístico
Nomes que incluam, terminem ou comecem com uma combinação específica de letras	Raça	Proxy estatístico
Ausências ao trabalho/ cancelamentos de última hora/disponibilidade reduzida para trabalhar (<i>Filcams Cgil Bologna e outros contra Deliveroo Italia S.R.L.</i> , 2020)	Crença (filiação sindical), género ou estado de saúde	Proxy estatístico
Artigos de vestuário e acessórios para cobrir a cabeça (como o uso de um lenço na cabeça) (<i>IX contra WABE e MH Müller Handels</i> , 2021)	Religião e crença	Proxy estatístico (referindo-se a quaisquer símbolos de convicções políticas, filosóficas ou religiosas, por exemplo) ou indissociável (referindo-se explicitamente a símbolos visíveis e de grandes dimensões, por exemplo)

Anexo F

Lista de registos de IA e algoritmos na Europa

Âmbito geográfico	Título	Âmbito	Ligação	Data de atualização
Bélgica	Observatório de IA da BoSA	Lista de todas as aplicações e projetos de IA conhecidos utilizados por instituições e agências federais	https://bosa.belgium.be/fr/themes/administration-numerique/cooperation-et-partage-des-connaissances/cooperation-nationale-5	
Base de dados da UE para sistemas de IA de risco elevado — em breve		Sistemas de IA de risco elevado		
Cada país da UE – em breve		Sistemas de IA de risco elevado relacionados com infraestruturas críticas		
UE	Casos selecionados de IA no setor público	IA no setor público	Catálogo de Dados do Centro Comum de Investigação – Casos selecionados de IA no setor público (JRC129301), Comissão Europeia	31 de dezembro de 2021

Âmbito geográfico	Título	Âmbito	Ligação	Data de atualização
UE	Public Sector Tech Watch	Observatório dedicado à monitorização, análise e divulgação da utilização de tecnologias emergentes	https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch	
Alemanha			Plataforma de Casos de Utilização – Instituto de IA Aplicada	
Helsínquia	Os sistemas de inteligência artificial da cidade de Helsínquia	IA no setor público	Tekoälyrekisteri – Helsingin kaupungin tekoälyrekisteri	Atualizações contínuas
Países Baixos	Registo de Algoritmos do Governo Neerlandês	Sistemas algorítmicos no setor público	Registo de Algoritmos do Governo Neerlandês	Atualizações contínuas
Reino Unido	Centro de registo de normas de transparência algorítmica	Governo do Reino Unido (norma voluntária)	Descubra como as ferramentas algorítmicas são utilizadas nas organizações públicas – GOV. UK	Atualizações contínuas
Reino Unido	Registo não governamental: Registo do Projeto de Legislação Pública para o Acompanhamento da Administração Pública Automatizada (TAG)		Registo TAG	Atualizações contínuas

Anexo G

Diretivas em matéria de não discriminação, motivos protegidos e âmbito

Diretiva	Motivos protegidos	Âmbito	Diretiva relativa às normas
2000/43/CE (Diretiva relativa à igualdade racial)	Raça e origem étnica – e não nacionalidade, e sem prejuízo do tratamento decorrente do estatuto jurídico de nacionais de países terceiros e de apátridas	Emprego, formação profissional, proteção social, educação, bens e serviços, incluindo a habitação	2024/1499
Diretiva 2000/78/CE	Religião ou crença, deficiência, idade, orientação sexual	Emprego e profissão	2024/1499
Diretiva 2004/113/CE (Diretiva relativa à igualdade de tratamento entre homens e mulheres no acesso a bens e serviços)	Sexo	Bens e serviços	2024/1499
Diretiva 2006/54/CE (Diretiva relativa à igualdade de género, na sua versão reformulada)	Sexo (incluindo gravidez e maternidade)	Emprego e profissão (incluindo regimes de segurança social)	2024/1500
2010/41/UE (Diretiva relativa à igualdade de tratamento entre homens e mulheres que exerçam uma atividade independente)	Sexo	Trabalhadoras/es independentes, cônjuges ou companheiras/os de trabalhadoras/es independentes	2024/1500
2023/970/UE Diretiva relativa à igualdade de remuneração (transposição até junho de 2026)		Emprego	2024/1500 (mas note-se que sem prejuízo de disposições mais específicas previstas na própria diretiva)

Anexo H

Outros regulamentos e orientações potencialmente relevantes

Conselho da Europa

Não discriminação

Recomendação CM/Rec(2019)1 do Comité de Ministros aos Estados-Membros sobre a prevenção e o combate ao sexismo: <https://search.coe.int/cm?i=090000168093b26a>.

Recomendação CM/Rec(2020)1 do Comité de Ministros aos Estados-Membros sobre os impactos dos sistemas algorítmicos nos direitos humanos (adotada pelo Comité de Ministros a 8 de abril de 2020, na 1373.^a reunião dos Adjuntos dos Ministros): <https://search.coe.int/cm?i=09000016809e1154>.

Recomendação CM/Rec(2026)1 do Comité de Ministros sobre igualdade e inteligência artificial, GEC/ADI-AI, no âmbito do GEC e do CDADI: <https://search.coe.int/cm?i=09125948802acd7f>.

Estudos

Relatório sobre a prevenção da discriminação resultante da utilização da inteligência artificial – Assembleia Parlamentar do Conselho da Europa, Comissão para a Igualdade e a Não Discriminação; relator: Sr. Christophe Lacroix (Bélgica, SOC), 29 de setembro de 2020: <https://pace.coe.int/en/files/28807>

Shrishak, Kris e Pénicaud, Soizic (2025) Proteção jurídica contra a discriminação algorítmica na Europa: quadros jurídicos atuais e lacunas remanescentes, Conselho da Europa. (também em francês, holandês, português, finlandês e sueco). Disponível em: <https://www.coe.int/en/web/inclusion-and-antidiscrimination/upholding-equality-and-non-discrimination-by-equality-bodies-regarding-the-use-of-artificial-intelligence-ai-in-public-administrations1> (consultado a 1 de julho de 2026)

Estudo sobre discriminação, inteligência artificial e tomada de decisões algorítmica – ECRI, novembro de 2018: <https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73>.

Estudo sobre o impacto dos sistemas de inteligência artificial, o seu potencial para promover a igualdade, incluindo a igualdade de género, e os riscos que podem acarretar em matéria de não discriminação – GEC/CDADI, agosto de 2023: <https://rm.coe.int/prems-112923-gbr-2530-etude-sur-l-impact-de-ai-web-a5-1-2788-3289-7544/1680ac7936>.

Xenidis, Raphaële (2025) Orientações políticas europeias sobre IA e discriminação baseada em algoritmos para organismos para a igualdade e outras estruturas nacionais de direitos humanos (também disponível em francês, holandês, português, finlandês, sueco), Conselho da Europa. Disponível em: <https://www.coe.int/en/web/inclusion-and-antidiscrimination/upholding-equality-and-non-discrimination-by-equality-bodies-regarding-the-use-of-artificial-intelligence-ai-in-public-administrations1> (consultado a 1 de julho de 2026)

Género

Recomendação CM/Rec(2026)2 do Comité de Ministros sobre a responsabilização pela violência contra mulheres e raparigas facilitada pela tecnologia: <https://search.coe.int/cm?i=09125948802acd83>.

Justiça e aplicação da lei

Ferramenta de avaliação para a implementação da Carta Ética Europeia sobre a utilização da inteligência artificial nos sistemas judiciais e no seu contexto – CEPEJ(2023)16 Final: <https://rm.coe.int/cepej-2023-16final-operationalisation-ai-ethical-charter-en/1680adcc9c>.

Carta Ética Europeia sobre a utilização da inteligência artificial (IA) nos sistemas judiciais e no seu contexto – CEPEJ(2018)14: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c>.

Orientações sobre o reconhecimento facial, Comité Consultivo da Convenção para a Proteção das Pessoas relativamente ao tratamento automatizado de dados de carácter pessoal, Convenção n.º 108, 28 de janeiro de 2021: <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3>.

Assistência social e rede de segurança social

Decl(17/03/2021)2 – Declaração do Comité de Ministros sobre os riscos da tomada de decisões assistida por computador ou baseada em inteligência artificial no domínio da rede de segurança social (aprovada pelo Comité de Ministros a 17 de março de 2021, na 1399.^a reunião dos Adjuntos dos Ministros) <https://search.coe.int/cm?i=0900001680a1cb98>.

Educação

Havinga, Beth, Holmes, Wayne e Persson, Jen (2024), Regulamentação da utilização de sistemas de inteligência artificial na educação: Estudo preparatório sobre a elaboração de um instrumento jurídico. Disponível em: <https://www.coe.int/en/web/education/-/regulating-the-use-of-artificial-intelligence-systems-in-education>.

Recomendação sobre o impacto da inteligência artificial (IA) no setor da educação, adotada pela Conferência das Organizações Não Governamentais Internacionais – CONF-AG(2023)REC4. Disponível em: <https://rm.coe.int/conf-ag-2023-rec4-draft-recommendation-on-the-impact-of-artificial-int/1680ac8e25>.

Migração, imigração e asilo

Recomendação CM/Rec(2022)17 do Comité de Ministros aos Estados-Membros sobre a proteção dos direitos das mulheres e raparigas migrantes, refugiadas e requerentes de asilo (em particular os n.º 5 a 8 e 22 a 25): <https://rm.coe.int/prems-092222-gbr-2573-recommandation-cm-rec-2022-17-a5-bat-web-1-/1680a6ef9a>.

Ver também: Resumo da política da IT Flows: <https://bura.brunel.ac.uk/handle/2438/27982>.

Anexo I

Práticas de IA de risco elevado

Domínio de risco elevado	Caso de utilização
1. Biometria	Sistemas de Identificação biométrica à distância, excluindo a verificação
	Categorização biométrica de atributos sensíveis ou protegidos, ou inferência de características com base nesses atributos
	Reconhecimento de emoções
2. Infraestruturas críticas	Componentes de segurança na gestão e no controlo de infraestruturas críticas
3. Educação e formação profissional	Determinar o acesso ou a admissão, ou atribuir a pessoas singulares o nível de escolaridade
	Avaliar os resultados da aprendizagem e/ou orientar o processo de aprendizagem no âmbito da educação ou da formação profissional
	Avaliar o nível de educação adequado
	Monitorizar ou detetar comportamentos proibidos por parte de estudantes durante os exames
4. Emprego, gestão de pessoal e acesso ao emprego por conta própria	Recrutamento ou seleção de pessoas singulares, anúncios de emprego direcionados ou avaliação de pessoas que se candidatam/candidaturas a emprego
	Tomada de decisões relativas às relações no âmbito do trabalho (como, por exemplo, uma promoção), à atribuição de tarefas e ao acompanhamento ou avaliação do desempenho
5. Acesso a serviços essenciais	Avaliar a elegibilidade para benefícios e serviços públicos
	Avaliar a solvabilidade ou determinar a pontuação de crédito, excluindo a fraude financeira
	Avaliar riscos e fixar prémios nos seguros de vida e de saúde
	Avaliar e/ou classificar chamadas de emergência para efeitos de envio de equipas, ou estabelecer prioridades no envio de equipas de primeira resposta em situações de emergência ou na triagem de cuidados de saúde

Domínio de risco elevado	Caso de utilização
6. Aplicação da lei	Avaliar o risco de ser vítima de um crime
	Polígrafo ou instrumentos semelhantes
	Avaliar a fiabilidade dos elementos de prova
	Avaliar o risco de (re)incidência, ou avaliar traços de personalidade ou comportamento criminoso
	Prestar assistência na deteção, investigação ou ação penal relativas a infrações penais
7. Gestão da migração, asilo e controlo de fronteiras	Polígrafo ou instrumentos semelhantes
	Avaliar os riscos em matéria de segurança, migração irregular ou saúde decorrentes da entrada no território de um Estado-Membro
	Analisar pedidos de asilo, visto, autorização de residência ou queixa relativas aos requisitos para a obtenção desse estatuto
	Detetar, reconhecer ou identificar pessoas singulares; aplica-se uma exceção no que diz respeito à verificação (de documentos de viagem)
8. Administração da justiça e processos democráticos	Apoiar a autoridade judicial na investigação e interpretação dos factos e da lei, bem como na aplicação da lei a factos concretos
	Sistemas destinados a influenciar o comportamento eleitoral em eleições e/ou referendos

Nota: a Comissão publicou um projeto de orientações sobre a classificação de sistemas de IA de risco elevado, que se encontra em fase de consulta até junho de 2026.⁶⁴

⁶⁴ Saiba mais aqui: [A Comissão solicita comentários sobre o projeto de orientações para a classificação de sistemas de inteligência artificial de risco elevado](#), Moldar o futuro digital da Europa, consultado a 5 de junho de 2026.

Anexo J

Práticas proibidas em matéria de IA

Tabela 9. Lista de práticas proibidas relativas à utilização de sistemas de IA

Prática proibida	Artigo	Considerando
Manipular ou enganar deliberadamente, distorcer significativamente o comportamento ou comprometer a capacidade de tomar uma decisão informada, de forma que seja razoavelmente provável que tal cause danos significativos, incluindo a produção de conteúdos sexuais e íntimos sem consentimento ou de material relacionado com abuso sexual de menores.	5(1)(a); 5(1)(ba) & (bb), 5(1a) and (1b)	Considerando 29
Aproveitar-se de qualquer vulnerabilidade decorrente da idade, deficiência ou situação socioeconómica, com o objetivo ou o efeito de distorcer significativamente o comportamento, de forma que seja razoavelmente provável que tal cause danos significativos.	5.º, n.º 1, alínea b)	Considerando 29
Classificar ou avaliar uma ou mais pessoas singulares ao longo de um determinado período de tempo com base no seu comportamento social ou nas suas características pessoais (ou de personalidade), através de uma pontuação social que conduza a um tratamento prejudicial ou desfavorável em qualquer uma das seguintes situações: ▶ num contexto diferente daquele em que foi originalmente recolhido; ▶ de forma injustificada ou desproporcionada.	5.º, n.º 1, alínea c)	Considerando 31
Avaliação do risco ou previsão da prática de um crime, com base exclusivamente na definição de perfis de uma pessoa singular.	5.º, n.º 1, alínea d)	Considerando 42
Recolha indiscriminada de imagens faciais a partir de câmaras de vigilância ou da Internet, com o objetivo de ampliar ou criar uma base de dados de reconhecimento facial.	5.º, n.º 1, alínea e)	Considerando 43

Reconhecimento de emoções no local de trabalho; aplicam-se exceções por motivos médicos e de segurança.	5.º, n.º 1, alínea f)	Considerando 44
Categorização biométrica de pessoas singulares com o objetivo de deduzir a raça, a opinião política, a filiação sindical, as convicções religiosas ou filosóficas, a vida sexual ou a orientação sexual.	5.º, n.º 1, alínea g)	Considerando 30
Identificação biométrica à distância “em tempo real” em locais de acesso público para efeitos de aplicação da lei, sendo aplicáveis exceções.	5.º, n.º 1, alínea h)	Considerandos 32, 33, 38, 39, 40 e 41

Tabela 10. Práticas proibidas no domínio da IA que podem estar relacionadas com a IA de risco elevado

Sistemas de IA de risco elevado (Artigo 6.º, n.º 2, Anexo III)	Prática proibida (Artigo 5.º)	Exemplos de casos de utilização proibidos e potencialmente proibidos e respetiva explicação
1. Biometria 1a) Sistemas de identificação biométrica à distância (IBD)	(h) Identificação biométrica à distância “em tempo real” em espaços públicos para fins de aplicação da lei, a menos que seja utilizada para: i. a busca de uma vítima de rapto; ii. prevenir uma ameaça específica, substancial e iminente; iii. identificar uma pessoa por crimes específicos (especificados no Anexo II).	Elementos-chave: a utilização de IBD em: i. “em tempo real” ii. espaços públicos iii. por parte das autoridades de aplicação da lei, ou em nome destas O considerando 32 afirma que a utilização de sistemas de IBD pode “dar origem a uma sensação de vigilância constante e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais”. Exemplo: a polícia utilizar câmaras de vigilância com reconhecimento facial em tempo real para identificar e deter uma pessoa procurada. Após identificar um manifestante pacífico, a polícia de Moscovo (<i>Glukhin contra a Rússia</i> , 2024) recorreu a imagens de videovigilância para identificar e localizar uma pessoa singular através de identificação biométrica “em tempo real”.

Sistemas de IA de risco elevado (Artigo 6.º, n.º 2, Anexo III)	Prática proibida (Artigo 5.º)	Exemplos de casos de utilização proibidos e potencialmente proibidos e respetiva explicação
1a) Sistemas de identificação biométrica à distância (IBD)	(e) Recolha indiscriminada de imagens faciais com o objetivo de criar ou ampliar uma base de dados	Elementos-chave: o método de criar ou ampliar uma base de dados de reconhecimento através da recolha de dados não direcionada, em vez de se identificar. É proibido, uma vez que a recolha indiscriminada de dados funciona como um “aspirador”, tal como previsto na alínea e) do n.º 1 do artigo 5.º, recolhendo indiscriminadamente imagens faciais sem visar pessoas singulares específicas. O considerando 43 reforça a justificação baseada no “sentimento de vigilância em larga escala” e na possibilidade de violação dos direitos fundamentais. Exemplo: autoridades fronteiriças que criam uma base de dados de reconhecimento facial através da recolha em massa de dados Pode haver a possibilidade de as autoridades fronteiriças recolherem imagens faciais a partir das redes sociais, de artigos noticiosos e de imagens de câmaras de vigilância, sem visar pessoas singulares específicas. Se esses dados forem posteriormente introduzidos numa base de dados para fins de identificação biométrica, tal seria proibido nos termos do artigo 5.º, n.º 1, alínea e).
1b) Categorização biométrica com base em características protegidas (ou inferência das mesmas)	(g) Categorização biométrica que permita inferir a raça, opiniões políticas, filiação sindical, convicções religiosas ou filosóficas, vida sexual ou orientação sexual	Elementos-chave: o objetivo específico de inferir as características protegidas enumeradas (raça, opiniões políticas, filiação sindical, religião, vida sexual ou orientação sexual) com base em dados biométricos. A categorização biométrica é já considerada, de imediato, de risco elevado, sendo que a alínea g) do n.º 1 do artigo 5.º proíbe categoricamente a utilização de dados biométricos para inferir estes atributos específicos. Exemplo: um sistema de IA que analisa as fotografias de uma pessoa nas redes sociais para inferir a sua orientação sexual a partir dos seus dados biométricos, com o objetivo de lhe enviar publicidade direcionada.

Sistemas de IA de risco elevado (Artigo 6.º, n.º 2, Anexo III)	Prática proibida (Artigo 5.º)	Exemplos de casos de utilização proibidos e potencialmente proibidos e respetiva explicação
1c) Reconhecimento de emoções	(f) Reconhecimento de emoções no local de trabalho e em instituições de ensino (exceção: fins médicos e de segurança)	Elementos-chave: inferir emoções ou intenções no contexto do local de trabalho e da educação, onde não se aplicam as isenções por motivos médicos ou de segurança. A alínea f) do n.º 1 do artigo 5.º proíbe a utilização da prática de reconhecimento de emoções de risco elevado nestes contextos específicos. O considerando 44 salienta ainda a preocupação quanto à base científica desses sistemas de IA que, especialmente quando combinados com desequilíbrios de poder num contexto laboral ou educativo, podem ter efeitos prejudiciais. Nota: o reconhecimento de estados físicos, por exemplo, se um/uma motorista de autocarro está ou não cansado/a, não é proibido neste contexto. Exemplo: um sistema de IA que determina se as trabalhadoras e trabalhadores saem do local de trabalho “felizes”, “zangadas/os” ou “tristes”. Uma entidade empregadora que tenta avaliar as emoções das suas trabalhadoras e trabalhadores de um restaurante a partir de imagens de videovigilância.
3) Educação e formação profissional Determinar o acesso/admissão	(a) Manipulação, engano ou interferência numa decisão informada, causando danos	Elementos-chave: a utilização de uma técnica manipuladora ou enganosa que distorça significativamente (ou que seja razoavelmente provável que distorça) o comportamento de uma pessoa singular. A alínea a) do n.º 1 do artigo 5.º proíbe técnicas que tenham por objetivo ou efeito distorcer o comportamento, através de técnicas que prejudiquem a tomada de decisões informadas e causem danos significativos. Elementos-chave: a utilização de uma técnica manipuladora ou enganosa que distorça significativamente (ou que seja razoavelmente provável que distorça) o comportamento de uma pessoa singular.

Sistemas de IA de risco elevado (Artigo 6.º, n.º 2, Anexo III)	Prática proibida (Artigo 5.º)	Exemplos de casos de utilização proibidos e potencialmente proibidos e respetiva explicação
		A alínea a) do n.º 1 do artigo 5.º proíbe técnicas que tenham por objetivo ou efeito distorcer o comportamento, através de técnicas que prejudiquem a tomada de decisões informadas e causem danos significativos.
3) Educação e formação profissional b) Avaliar os resultados da aprendizagem e orientar o processo de aprendizagem c) Avaliar o nível de escolaridade (adequado) d) Monitorizar/detetar comportamentos proibidos por parte de estudantes	(f) Reconhecimento de emoções no local de trabalho e em instituições de ensino (exceção: fins médicos e de segurança)	Elemento-chave: a inferência dos estados emocionais ou das intenções de estudantes e a influência destes no seu processo de aprendizagem. Os sistemas de IA podem ser utilizados para avaliar estudantes; no entanto, é proibido reconhecer as suas emoções ou intenções. O considerando 44 salienta ainda a preocupação quanto à base científica desses sistemas de IA que, especialmente quando combinados com desequilíbrios de poder num contexto laboral ou educativo, podem ter efeitos prejudiciais. Exemplo: uma universidade utiliza uma plataforma de aprendizagem personalizada que tem em conta as emoções das/dos estudantes captadas pelas suas câmaras web durante as aulas online, a fim de orientar o processo de aprendizagem.
4) Emprego e gestão de trabalhadoras e trabalhadores a) Recrutamento (publicidade direcionada) ou seleção (avaliação de candidaturas a emprego)	(a) Manipulação, engano ou interferência numa decisão informada, causando danos (b) Exploração de uma vulnerabilidade	Elementos-chave: a utilização de uma técnica manipuladora ou enganosa que distorça significativamente (ou que seja razoavelmente provável que distorça) o comportamento de uma pessoa singular. A alínea a) do n.º 1 do artigo 5.º proíbe técnicas que tenham por objetivo ou efeito distorcer o comportamento, através de técnicas que prejudiquem a tomada de decisões informadas e causem danos significativos. Exemplo: uma plataforma de recrutamento baseada em IA que recorre a uma sensação de urgência inventada e a manobras enganosas para levar à assinatura de um contrato.

Sistemas de IA de risco elevado (Artigo 6.º, n.º 2, Anexo III)	Prática proibida (Artigo 5.º)	Exemplos de casos de utilização proibidos e potencialmente proibidos e respetiva explicação
		A alínea a) do n.º 1 do artigo 5.º proíbe técnicas que tenham por objetivo ou efeito distorcer o comportamento, através de técnicas que prejudiquem a tomada de decisões informadas e causem danos significativos. Nota: não é necessária a intenção; basta o efeito. Uma agência de recrutamento que utilize um sistema de IA que apresente salários ou benefícios exagerados, ou que crie uma sensação de urgência que prejudique uma decisão informada, seria proibida ao abrigo deste artigo.
4) Emprego e gestão de trabalhadoras e trabalhadores b) Decisões que afetam as relações laborais, tais como o despedimento ou a atribuição de tarefas	(a) Manipulação, engano ou interferência numa decisão informada, causando danos (b) Exploração de uma vulnerabilidade	Elementos-chave: a utilização de uma técnica manipuladora ou enganosa que distorça significativamente (ou que seja razoavelmente provável que distorça) o comportamento de uma pessoa singular. A alínea a) do n.º 1 do artigo 5.º proíbe técnicas que tenham por objetivo ou efeito distorcer o comportamento, através de técnicas que prejudiquem a tomada de decisões informadas e causem danos significativos. Nota: não é necessária a intenção; basta o efeito. Exemplo: uma empresa de logística que utiliza IA para atribuir tarefas de entrega e monitorizar o desempenho dos/das motoristas. Existe um cenário plausível em que, através de um sistema deste tipo, o comportamento dos/das motoristas possa ser distorcido, levando a trabalhar mais do que o número de horas permitido por lei, o que teria repercussões na saúde e na segurança e causaria danos significativos. Um sistema desse tipo seria, portanto, proibido.

Sistemas de IA de risco elevado (Artigo 6.º, n.º 2, Anexo III)	Prática proibida (Artigo 5.º)	Exemplos de casos de utilização proibidos e potencialmente proibidos e respetiva explicação
4) Emprego e gestão de trabalhadoras e trabalhadores b) Decisões que afetam as relações laborais, tais como o despedimento ou a atribuição de tarefas	(f) Reconhecimento de emoções e/ou intenções no local de trabalho e em instituições de ensino	Elemento-chave: a inferência dos estados emocionais ou das intenções das trabalhadoras e trabalhadores e a influência destes no seu trabalho. Os sistemas de IA podem ser utilizados para apoiar a tomada de decisões. No entanto, é proibido basear qualquer assistência na utilização do reconhecimento de emoções. O considerando 44 salienta ainda a preocupação quanto à base científica desses sistemas de IA que, especialmente quando combinados com desequilíbrios de poder num contexto laboral ou educativo, podem ter efeitos prejudiciais. Exemplo: um centro de atendimento que utiliza IA para monitorizar trabalhadoras/es recorre ao seu estado emocional para avaliar o seu desempenho. No exemplo, se um sistema de IA deduzisse os estados emocionais das trabalhadoras e trabalhadores com base em gravações de voz e tivesse isso em conta na avaliação de desempenho, tal constituiria uma prática proibida.
5) Acesso a serviços e prestações essenciais a) Avaliar a elegibilidade de uma pessoa singular	(c) Classificação social que conduz a um tratamento desfavorável: i) num contexto diferente do dos dados recolhidos e/ou ii) de forma injustificada ou desproporcionada.	Elementos-chave: tratamento desfavorável com base no seu comportamento social num contexto não relacionado e/ou desproporcionado no seu efeito. Se for utilizado um sistema de IA para avaliar a elegibilidade, pode não ser o caso de este utilizar dados de um contexto diferente. Exemplo: as autoridades públicas implementam um sistema de IA para atribuir prestações sociais que utiliza dados não relacionados. Nestes casos proibidos, é importante que o contexto em que os dados são recolhidos seja substancialmente diferente do contexto em que são utilizados.

Sistemas de IA de risco elevado (Artigo 6.º, n.º 2, Anexo III)	Prática proibida (Artigo 5.º)	Exemplos de casos de utilização proibidos e potencialmente proibidos e respetiva explicação
5b) Avaliação da solvabilidade	(c) Classificação social que conduz a um tratamento desfavorável: i) num contexto diferente do dos dados recolhidos e/ou ii) de forma injustificada ou desproporcionada.	Elementos-chave: tratamento desfavorável com base no seu comportamento social num contexto não relacionado e/ou desproporcionado no seu efeito. Se for utilizado um sistema de IA para avaliar a solvabilidade de uma pessoa, este poderá fazê-lo com base no historial financeiro, mas não noutros contextos não relacionados. Exemplo: as instituições financeiras utilizam um sistema de IA para avaliar empréstimos, mas também acedem a outras bases de dados não financeiras. Se um banco também analisasse as ligações nas redes sociais ou tivesse em conta a morada da pessoa ao decidir se o empréstimo da pessoa requerente deve ou não ser aprovado, tal poderia ser proibido nos termos do artigo 5.º, n.º 1, alínea c).
5c) Avaliação de riscos no que diz respeito à fixação dos prémios dos seguros de saúde ou de vida	(c) Classificação social que conduz a um tratamento desfavorável: i) num contexto diferente do dos dados recolhidos e/ou ii) de forma injustificada ou desproporcionada.	Elementos-chave: tratamento desfavorável com base no seu comportamento social num contexto não relacionado e/ou desproporcionado no seu efeito. Se for utilizado um sistema de IA para a fixação dos prémios de um seguro de vida, este poderá fazê-lo com base no historial médico, mas não noutros contextos não relacionados. Exemplo: uma seguradora implementa um sistema de IA para avaliar os preços com base em informações provenientes de um contexto não relacionado. Se uma seguradora analisasse as ligações e o comportamento nas redes sociais, tal poderia ser proibido nos termos do artigo 5.º, n.º 1, alínea c).

Sistemas de IA de risco elevado (Artigo 6.º, n.º 2, Anexo III)	Prática proibida (Artigo 5.º)	Exemplos de casos de utilização proibidos e potencialmente proibidos e respetiva explicação
6) Aplicação da lei a) Avaliação do risco de vitimização b) Polígrafos c) Avaliação da fiabilidade das provas d) Avaliação do risco de (re)incidência ou avaliar características e) Definição de perfis durante a deteção, investigação ou ação penal	(d) Avaliação do risco de criminalidade baseada exclusivamente na definição de perfis	Elementos-chave: a avaliação baseia-se em traços e características de personalidade e não em factos objetivos. Nota: se um sistema permitir uma decisão humana, poderá aplicar-se uma exceção. A alínea d) do n.º 1 do artigo 5.º proíbe as avaliações de risco relativas a infrações penais baseadas exclusivamente na análise de traços de personalidade, sem factos objetivos e verificáveis que as relacionem com atividades criminosas. Exemplo: sistema de policiamento preditivo, que define perfis de pessoas singulares com base nos seus dados demográficos. Se a polícia pretendesse prever a probabilidade de ocorrência de atividades criminosas com base em características como a idade, a nacionalidade ou o bairro, tal constituiria um sistema proibido nos termos da alínea d) do n.º 1 do artigo 5.º.

Sistemas de IA de risco elevado (Artigo 6.º, n.º 2, Anexo III)	Prática proibida (Artigo 5.º)	Exemplos de casos de utilização proibidos e potencialmente proibidos e respetiva explicação
6) Aplicação da lei e) Definição de perfis durante a deteção, investigação ou ação penal	(h) Identificação biométrica à distância “em tempo real” em espaços públicos para fins de aplicação da lei, a menos que seja utilizada para: i. a busca por uma vítima de rapto; ii. prevenir uma ameaça específica, substancial e iminente; iii. identificar uma pessoa por crimes específicos (especificados no Anexo II).	Elementos-chave: a utilização de IBD em: i. “tempo real” ii. espaços públicos iii. por parte das autoridades de aplicação da lei, ou em nome destas O considerando 32 afirma que a utilização de sistemas de IBD pode “dar origem a uma sensação de vigilância constante e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais”. Exemplo: a polícia utilizar câmaras de vigilância com reconhecimento facial em tempo real para identificar e deter uma pessoa procurada. Após identificar um manifestante pacífico, a polícia de Moscovo (<i>Glukhin contra a Rússia</i>, 2024) recorreu a imagens de videovigilância para identificar e localizar uma pessoa singular através de identificação biométrica “em tempo real”.
7) Migração, asilo e controlo de fronteiras a) Avaliação de riscos em matéria de segurança, irregularidades ou saúde b) Avaliação de pedidos de asilo, vistos e autorizações, elegibilidade e queixas	(d) Avaliação do risco de criminalidade baseada exclusivamente na definição de perfis	Elementos-chave: a avaliação baseia-se em traços de personalidade e não em factos objetivos. Nota: se um sistema permitir uma decisão humana, poderão aplicar-se exceções. A alínea d) do n.º 1 do artigo 5.º proíbe as avaliações de risco relativas a infrações penais baseadas exclusivamente na análise de traços de personalidade, sem factos objetivos e verificáveis que as relacionem com atividades criminosas. Exemplo: as autoridades fronteiriças utilizam um sistema de IA que baseia a avaliação de risco das pessoas singulares nos seus dados demográficos. Se as autoridades fronteiriças fossem prever o risco de prática de infrações com base em características como a nacionalidade ou a região, tal poderia constituir um sistema proibido nos termos da alínea d) do n.º 1 do artigo 5.º.

Sistemas de IA de risco elevado (Artigo 6.º, n.º 2, Anexo III)	Prática proibida (Artigo 5.º)	Exemplos de casos de utilização proibidos e potencialmente proibidos e respetiva explicação
7) Migração, asilo e controlo de fronteiras (b) Avaliação de riscos em matéria de segurança, irregularidades ou saúde	(h) Identificação biométrica à distância “em tempo real” em espaços públicos para fins de aplicação da lei, a menos que seja utilizada para: i. a busca por uma vítima de rapto; ii. prevenir uma ameaça específica, substancial e iminente; iii. identificar uma pessoa por crimes específicos (especificados no Anexo II).	Elementos-chave: a utilização de IBD em: i. “tempo real” ii. espaços públicos iii. por parte das autoridades de aplicação da lei, ou em nome destas O considerando 32 afirma que a utilização de sistemas de IBD pode “dar origem a uma sensação de vigilância constante e dissuadir indiretamente o exercício da liberdade de reunião e de outros direitos fundamentais”. Exemplo: a utilização de câmaras de vigilância com reconhecimento facial em tempo real na fronteira para identificar pessoas procuradas.
7) Migração, asilo e controlo de fronteiras (d) Detetar, reconhecer ou identificar pessoas singulares (com exceção da verificação de documentos de viagem)	(e) Recolha indiscriminada de imagens faciais	Elementos-chave: o método de criar ou ampliar uma base de dados de reconhecimento através da recolha de dados não direcionada, em vez de se identificar. É proibido, uma vez que a recolha indiscriminada de dados funciona como um “aspirador”, tal como previsto na alínea e) do n.º 1 do artigo 5.º, recolhendo indiscriminadamente imagens faciais sem visar pessoas singulares específicas. O considerando 43 reforça a justificação baseada no “sentimento de vigilância em larga escala” e na possibilidade de violação dos direitos fundamentais. Exemplo: autoridades fronteiriças que criam uma base de dados de reconhecimento facial através da recolha em massa de dados.

Sistemas de IA de risco elevado (Artigo 6.º, n.º 2, Anexo III)	Prática proibida (Artigo 5.º)	Exemplos de casos de utilização proibidos e potencialmente proibidos e respetiva explicação
		Pode haver a possibilidade de as autoridades fronteiriças recolherem imagens faciais a partir das redes sociais, de artigos noticiosos e de imagens de câmaras de vigilância, sem visar pessoas singulares específicas. Se esses dados forem posteriormente introduzidos numa base de dados para fins de identificação fronteiriça, tal seria proibido nos termos do artigo 5.º, n.º 1, alínea e).

Anexo K

Ficha de registo para o passo 3

Esta ficha foi concebida como um exemplo de como uma pessoa responsável, seguindo os passos descritos na secção 3, poderia registar as suas conclusões. Os exemplos são fictícios e servem para dar uma ideia dos tipos de informação que poderiam ser registados. Prevê-se que o registo efetivo seja significativamente mais pormenorizado. A última coluna destina-se a permitir a análise das provas na sequência de qualquer divulgação por parte da parte inquirida.

Passo		Presunção de discriminação	Na sequência da divulgação feita pela parte inquirida
3.1. Risco conhecido e suspeito 3.1.1 Tipo de sistema	Indique se o sistema é ou não um sistema de risco elevado ou se se destina a ser utilizado em algum dos setores ou domínios identificados como apresentando um risco de discriminação no Regulamento sobre a IA.	Exemplos Setor: Caso de utilização:	
3.1.2 Riscos conhecidos de discriminação	Registe o domínio em que existe um risco conhecido, o tipo de tecnologia utilizado e quaisquer outras informações e provas relevantes.	Exemplos Setor: aplicação da lei Tecnologia: reconhecimento facial, biometria Fonte: Investigação realizada por uma ONG/instituição académica, Regulamento sobre a IA da UE, artigo 5.º (sistemas proibidos), artigo 6.º (risco elevado) e Anexo III.	

Passo		Presunção de discriminação	Na sequência da divulgação feita pela parte inquirida
3.2 Características protegidas e proxies	Registe a utilização direta de características protegidas. Onde é que são utilizadas e como?	Características protegidas Como são utilizadas: dados de entrada, por exemplo	
Analisar aprofundadamente a conceção técnica do sistema e a influência dos proxies (presumíveis) nos resultados do sistema. O facto de se utilizar um proxy como dado de entrada não é, por si só, prova suficiente de discriminação. O próximo passo consiste em avaliar os dados para compreender se a utilização destes fatores conduz a um tratamento desigual.	Registe qualquer utilização identificada de características protegidas ou proxies que tenham, ou se presume que tenham, impacto no resultado do sistema. Registe também, para cada proxy, a razão pela qual o OI considera que se tratam de proxies.	Exemplos Proxies: por exemplo, um código postal como proxy de raça, a gravidez como proxy de género. Provas e argumentos	
3.3 Avaliações de risco, incluindo a AIDF	Registe quaisquer riscos de discriminação identificados pela entidade prestadora ou por quem é responsável pela implantação, bem como quaisquer medidas identificadas para mitigar esses riscos.	Exemplos Risco: discriminação racial devido a enviesamentos históricos Identificado onde: avaliação de riscos Medida de mitigação: técnica de eliminação de enviesamento	

Passo		Presunção de discriminação	Na sequência da divulgação feita pela parte inquirida
	Analise e registe se existem falhas claras e evidentes na avaliação de riscos, na AIPD ou na AIDF.	A avaliação de riscos refere-se à discriminação, mas não à raça. AIPD: não considera a raça como pertencente à categoria especial de dados. AIDF: não considera a discriminação racial e artigo 14.º da Convenção Europeia dos Direitos Humanos.	
	Considere e registe a existência e o impacto de qualquer intervenção humana no processo. Quem é a pessoa responsável? A pessoa responsável possui a competência, a formação e a autoridade necessárias para anular uma decisão tomada por um sistema de IA? A pessoa responsável recebeu formação para compreender e interpretar os resultados do sistema e para reconhecer em que situações podem surgir enviesamentos e ser necessária uma intervenção?	Pessoa de contacto: Função: analisa as decisões, mas não analisa os dados que estiveram na origem da decisão. Será que isto é suficiente?	

Passo		Presunção de discriminação	Na sequência da divulgação feita pela parte inquirida
	Existem orientações ou protocolos dirigidos às partes decisoras para as ajudar a compreender como utilizar o sistema de IA ou a interpretar os resultados?		
3.4: Objetivo do sistema	Registe a finalidade do sistema e o que este visa otimizar.	Finalidade do sistema: Concebido para otimizar:	
	Registe os proxies e as características protegidas que influenciam os resultados do sistema e, quando disponíveis, os parâmetros relativos ao seu peso/influência nos resultados.	Características protegidas que influenciam o sistema: Proxies que influenciam o sistema: Parâmetros relativos ao peso/influência:	
3.5 Dados de treino, teste e validação	Registe quaisquer problemas gerais relacionados com os dados, incluindo problemas relacionados com a qualidade dos dados.	Por exemplo, a amostra de dados é muito pequena, antiga ou diz respeito a uma área geográfica diferente.	
	Questões relacionadas com os dados relativas à desigualdade e à discriminação.		
	Questões relacionadas com documentação insuficiente.		
	Preocupações relativamente às medidas de mitigação.		
	Argumentação sobre a forma como as questões relacionadas com os dados e as medidas de mitigação conduziriam a um tratamento desigual no presente caso.		

Passo		Presunção de discriminação	Na sequência da divulgação feita pela parte inquirida
	Registe quaisquer indicadores de incumprimento das disposições do Regulamento sobre a IA relevantes em matéria de dados.		
3.6 Testes e avaliação	Lacunas ao nível dos resultados ou do tratamento, tal como reveladas nas estatísticas.		
	Problemas relacionados com as estatísticas apresentadas (tais como parâmetro incorreto ou problemas com os dados).		
	Lacunas nos testes identificadas.		
Conclusão	Analise a informação e registe os fundamentos com base nos quais se pode argumentar que existe um caso <i>prima facie</i> de discriminação ou conclua que tal não é o caso.		
	Analise todos os passos após a apresentação de provas adicionais, a fim de determinar se a parte inquirida conseguiu refutar a presunção ou justificar a discriminação.		

A inteligência artificial (IA) está a remodelar as nossas sociedades e a afetar os direitos fundamentais e a igualdade. Estes sistemas podem reforçar e criar discriminação, uma vez que são frequentemente concebidos para diferenciar as pessoas: classificando-as, ordenando-as por importância ou direcionando-lhes ações específicas. Em combinação com as desigualdades históricas e os preconceitos humanos incorporados nos dados, nas regras e nas escolhas de conceção dos sistemas algorítmicos, os padrões discriminatórios podem ser reproduzidos e ampliados, a menos que sejam identificados e mitigados de forma proativa.

Esta metodologia fornece orientações, passo a passo, a organismos para a igualdade e outras organizações de direitos humanos na Europa para avaliar casos de discriminação relacionados com a IA ou com sistemas algorítmicos. Destina-se a pessoas responsáveis pelos processos, consultores/as e advogados/as de entidades que investigam queixas de discriminação que envolvam, ou se suspeite que envolvam, IA ou tomada de decisão automatizada.

A metodologia baseia-se no quadro regulamentar europeu em matéria de IA, nomeadamente no Regulamento sobre a IA da UE e na Convenção-Quadro do Conselho da Europa sobre Inteligência Artificial e Direitos Humanos, Democracia e Estado de Direito, bem como na legislação antidiscriminação, e faz referência a outra legislação, como a relativa à proteção de dados, casos exemplificativos e jurisprudência, quando relevante.



YHDENVERTAISUUSVALTUUTETTU
NON-DISCRIMINATION OMBUDSMAN



COMISSÃO PARA A CIDADANIA
E A IGUALDADE DE GÉNERO

Os Estados-Membros da União Europeia decidiram associar os seus conhecimentos, recursos e destinos. Juntos, construíram uma zona de estabilidade, democracia e desenvolvimento sustentável, mantendo simultaneamente a diversidade cultural, a tolerância e as liberdades individuais. A União Europeia está empenhada em partilhar as suas realizações e os seus valores com países e povos para além das suas fronteiras.

<http://europa.eu>

O Conselho da Europa é a principal organização de direitos humanos no continente. Integra 46 Estados-Membros, incluindo todos os membros da União Europeia. Todos os Estados-Membros do Conselho da Europa assinaram a Convenção Europeia dos Direitos Humanos, um tratado destinado a proteger os direitos humanos, a democracia e o Estado de direito. O Tribunal Europeu dos Direitos Humanos controla a implementação da Convenção nos Estados-Membros.

www.coe.int

Co-funded
by the European Union



EUROPEAN UNION

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

Co-funded and implemented
by the Council of Europe