

PROGRAMAS DE DIVERSIDADE E INCLUSÃO E PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS: BOAS PRÁTICAS PARA O TRATAMENTO DE DADOS NAS RELAÇÕES DE TRABALHO

Bernardo Araujo

Doutor em Direito Público pela Universidade do Estado do Rio de Janeiro (UERJ). Mestre em Direito da Cidade pela UERJ. Bacharel em Direito pela UERJ. Advogado e *Data Protection Officer*.

Resumo: O objetivo do estudo é analisar a legalidade de uma organização promover levantamento de indicadores de diversidade entre o seu público interno, com o propósito de estruturar e implementar políticas de afirmação no formato de programas de diversidade e inclusão para grupos sociais em condição de vulnerabilidade. Para tal, realizamos levantamento de publicações nacionais e internacionais que permitiram análise e reflexão crítica das questões teóricas envolvidas. Em um primeiro momento, apresentamos o escopo e as atividades comuns aos programas de diversidade e inclusão, bem como o contexto em que as iniciativas de diversidade e inclusão se inserem nos programas de responsabilidade corporativa nos cenários internacional e nacional. Em um segundo momento, abordamos o escopo de aplicabilidade da Lei Geral de Proteção de Dados aos processos de coleta de informações pessoais utilizadas no mapeamento dos indicadores de diversidade, o manejo dessas informações pelos times internos e por terceiros, bem como as exceções (controversas) à aplicabilidade da legislação. Visando contribuir com essa atividade de interesse público de forma propositiva, sugerimos, na sequência, modelo de instrumento de transparência e coleta de consentimento adequado aos requisitos específicos da legislação de proteção de dados, considerando os riscos de invalidez do uso do consentimento em âmbito de relação empregatícia. Por fim, são feitas recomendações acerca das boas práticas para a condução das ações, a fim de mitigar riscos de exposição dos titulares e da organização. Sendo a proteção dos dados sensíveis especialmente relevante para a garantia dos direitos e liberdades fundamentais, devendo ser tutelados de forma mais específica e cuidadosa, busca-se avaliar, em particular, os desafios em matéria de privacidade e proteção de dados na implementação de programas de diversidade e inclusão que requerem o tratamento de dados sensíveis.

Palavras-chave: Programas de diversidade e inclusão. Dados sensíveis. Proteção de dados pessoais. Privacidade. LGPD.

Sumário: **1** Introdução – **2** O que são os programas de diversidade e inclusão: escopo e atividades comuns – **3** Os programas de diversidade e inclusão no contexto internacional de incentivo à responsabilidade das organizações – **4** Contexto jurídico dos programas de diversidade e inclusão – **5** Aplicação da LGPD aos programas de diversidade e inclusão – **6** Dados anonimizados e a (controvertida) não aplicação da LGPD – **7** Enquadramento legal na LGPD para o tratamento de dados pessoais coletados em programas de diversidade e inclusão – **8** Declaração de coleta e termo de consentimento para mapeamento de indicadores de diversidade e inclusão no âmbito das relações de trabalho – **9** Coletando dados pessoais para programas de diversidade e inclusão: requisitos mínimos de transparência – **10** Considerações finais – Referências

1 Introdução

Os programas de diversidade e inclusão são legais no ordenamento jurídico nacional? Quem pode implementar políticas afirmativas? Como devem ser estruturados os procedimentos de coleta e uso dos dados pessoais em mapeamentos de diversidade? Quais são as leis que respaldam os programas de diversidade e inclusão? Quais são os limites desses programas? Como identificar um tratamento de informações que possa ter efeitos discriminatórios ilícitos ou abusivos? O que torna uma informação pessoal um dado sensível? Quais cuidados precisam ser observados no tratamento dessa categoria de dados?

Com o propósito de responder a tais indagações, este artigo tem como objetivo geral analisar a legalidade de uma organização, na perspectiva de controladora de dados pessoais, e promover “programas de diversidade e inclusão” com o propósito de estruturar e implementar políticas de afirmação¹ para grupos sociais em condição de vulnerabilidade.² Buscaremos avaliar, em especial, os desafios em matéria de privacidade e proteção de dados na condução de pesquisas com dados sensíveis.³

A metodologia central empregada neste estudo baseou-se primariamente em uma abordagem de análise e reflexão crítica de questões teóricas, com o objetivo principal de avaliar a legalidade e os desafios envolvidos na promoção, por

¹ Acerca do tema da promoção de ações afirmativas pelo Estado e pelo Poder Público, é oportuno mencionar dois precedentes paradigmáticos do Supremo Tribunal Federal (STF) que oferecem importantes parâmetros normativos para a aplicação do sistema de cotas raciais em concursos públicos. No primeiro deles, a ADPF nº 186/DF, o Plenário da Corte apreciou a constitucionalidade material dessa modalidade de política de ação afirmativa, adotada no âmbito do ensino universitário. No julgamento, os ministros acompanharam por unanimidade o voto do relator, o ministro Ricardo Lewandowski, corroborando a prática adotada pela Universidade de Brasília de reservar parcela das vagas disponíveis ao ingresso no ensino superior para pessoas negras. No julgamento da ADC nº 41/DF, o STF reconheceu a validade da Lei nº 12.990/2014, que reserva vagas à população negra nos concursos da administração pública federal. Relatada pelo ministro Luís Roberto Barroso, a ação declaratória de constitucionalidade analisou, para além da compatibilidade do sistema de cotas raciais com o princípio constitucional da igualdade, outros aspectos do regime de seleção diferenciado, como o critério de heteroidentificação e a ordem de nomeação dos aprovados.

² “Consideram-se em condição de vulnerabilidade aquelas pessoas que, por razão da sua idade, gênero, estado físico ou mental, ou por circunstâncias sociais, econômicas, étnicas e/ou culturais, encontram especiais dificuldades em exercer com plenitude perante o sistema de justiça os direitos reconhecidos pelo ordenamento jurídico. Poderão constituir causas de vulnerabilidade, entre outras, as seguintes: a idade, a incapacidade, a pertença a comunidades indígenas ou a minorias, a vitimização, a migração e o deslocamento interno, a pobreza, o gênero e a privação de liberdade. A concreta determinação das pessoas em condição de vulnerabilidade em cada país dependerá das suas características específicas, ou inclusive do seu nível de desenvolvimento social e econômico.” Cf.: ASSOCIAÇÃO NACIONAL DAS DEFENSORAS E DEFENSORES PÚBLICOS (ANADEP). *Regras de Brasília sobre acesso à justiça das pessoas em condição de vulnerabilidade*. Brasília, DF: ANADEP, 2008. Disponível em: <https://www.anadep.org.br/wtksite/100-Regras-de-Brasilia-versao-reduzida.pdf>. Acesso em: 3 dez. 2025.

³ MULHOLLAND, Caitlin S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, [S. l.], v. 19, n. 3, p. 159-180, 2018. DOI: 10.18759/rdgf.v19i3.1603.

organizações controladoras de dados pessoais, do levantamento de indicadores de diversidade para a estruturação de políticas afirmativas. Para tal fim, o método incluiu um levantamento de publicações nacionais e internacionais, permitindo uma visão detalhada do escopo dos programas de diversidade e inclusão, das pesquisas e mapeamento de indicadores que os precedem, bem como dos requisitos e do contexto de aplicabilidade da Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018 – aos processos de coleta de informações pessoais, especialmente de dados pessoais sensíveis. A pesquisa buscou responder a indagações críticas sobre a estruturação dos procedimentos de coleta e uso de dados pessoais em mapeamentos de diversidade, os limites desses programas e os cuidados necessários no tratamento de dados pessoais – que, em muitos casos, revelam informações sensíveis dos empregados.

Do ponto de vista das fontes de dados e da contribuição prática, uma parcela substancial do trabalho foi desenvolvida com pesquisa na internet, e utilizou-se também material próprio, proveniente da atuação profissional do autor com a temática. Essa combinação de análise bibliográfica com *insights* da prática profissional permitiu que o estudo oferecesse uma contribuição propositiva ao tema. Especificamente, a metodologia levou à sugestão de um modelo de instrumento de transparência e coleta de consentimento adequado aos requisitos específicos da legislação de proteção de dados, abordando, inclusive, os riscos inerentes à validade do consentimento em relações de trabalho. Por conseguinte, foram elaboradas recomendações objetivas e boas práticas de condução das ações, com o intuito de mitigar riscos de exposição e garantir a conformidade do tratamento de dados sensíveis no âmbito dos programas de diversidade e inclusão.

Iniciamos o estudo apresentando o contexto em que os programas de diversidade e inclusão se inserem nos programas de responsabilidade corporativa no cenário internacional e no contexto nacional. Em um segundo momento, abordamos o escopo de aplicabilidade da LGPD aos processos de coleta de informações pessoais utilizadas no mapeamento dos indicadores de diversidade, o manejo dessas informações pelos times internos e por terceiros, bem como as exceções à aplicabilidade da legislação. Considerando que uma parcela do conjunto normativo que dá respaldo ao uso de dados pessoais é recente, apresentamos os fundamentos legais na legislação federal que criam obrigações legais e regulatórias aos controladores de dados. Sabendo que uma parcela do tratamento de dados deve ser feita com base no consentimento de dados – algo potencialmente problemático em matéria de proteção de dados pessoais –, sugerimos, na sequência, modelo de instrumento de transparência e coleta de consentimento adequado aos requisitos específicos da legislação de proteção de dados pessoais, visando contribuir com essa atividade de interesse público de forma propositiva. Por fim, são feitas

recomendações acerca das boas práticas para a implementação dos programas de diversidade e inclusão, a fim de diminuir riscos de exposição dos titulares e da organização.

Em síntese, a fim de implementar pesquisas de diversidade, entendemos ser recomendável que as organizações iniciem um “projeto de diversidade” amplo, com participação de diferentes departamentos internos, com vistas à adoção de decisões estratégicas, registro das operações de tratamento de dados e realização de avaliações de risco e impacto. Nos termos da LGPD, parte das informações pessoais coletadas se qualifica na categoria de “dados pessoais sensíveis”, com alto potencial discriminatório, o que pode demandar atenção especial e cuidados adicionais para qualquer atividade que envolva o uso dessas informações. Por fim, ainda que a decisão sobre a escolha da base legal mais adequada para fundamentar as principais atividades de tratamentos de dados no âmbito das pesquisas preparatórias e da implementação dos programas deva ser sempre feita caso a caso, é possível recomendar, abstratamente, como aplicar as bases legais presentes na legislação federal, bem como as melhores práticas nas formas de coleta do consentimento para o tratamento dos dados pessoais do público interno de uma organização, com várias particularidades devido à natureza das relações trabalhistas.

2 O que são os programas de diversidade e inclusão: escopo e atividades comuns

Os programas de diversidade e inclusão são instrumentos essenciais para a construção de um ambiente de trabalho mais justo, acolhedor e representativo. Essas ações visam promover a equidade e o respeito à diversidade, abrangendo aspectos como gênero, raça, etnia, orientação sexual, identidade de gênero, idade e pessoas com deficiência. Essas iniciativas são especialmente importantes no Brasil, país marcado pela desigualdade de oportunidades que atinge negativamente categorias de indivíduos histórico e socialmente desfavorecidos. É nesse contexto que os programas de diversidade e inclusão ganham especial relevância, pois representam poderosos instrumentos de transformação e inclusão social. Colocando em contexto, um levantamento⁴ produzido pelo Instituto Ethos e lançado no painel de abertura da Conferência Ethos em São Paulo, com participação do

⁴ INSTITUTO ETHOS. *Perfil social, racial e de gênero das 1.100 maiores empresas do Brasil e suas ações afirmativas 2023-2024*. São Paulo, 2024. Disponível em: <https://www.ethos.org.br/publicacao/perfil-social-racial-e-de-genero-das-1-100-maiores-empresas-do-brasil-e-suas-acoes-afirmativas-2023-2024/>. Acesso em: 3 dez. 2025.

Ministério da Igualdade Racial, apresentou números alarmantes. O estudo analisou as práticas de inclusão em 1.100 das maiores empresas do Brasil. Entre outros indicadores, o levantamento destacou a baixa representatividade de pessoas negras, sobretudo mulheres, em posições de liderança. De acordo com a pesquisa, pessoas pretas e pardas compõem menos de 6% dos conselhos nas empresas e menos de 14% dos cargos executivos e de diretoria, apesar de representarem 55% da população brasileira.

Diante de uma sociedade e de consumidores significativamente mais atentos às condutas e práticas empresariais mais inclusivas, igualitárias e justas a seus empregados, percebe-se um aumento no número de lideranças e executivos se engajando com as iniciativas de diversidade e buscando transformar sua cultura organizacional, convictos de que essa boa prática contribui fortemente como um todo na qualidade do ambiente organizacional, bem como para a continuidade dos negócios, a inovação e a criação de valor a longo prazo.

A discussão sobre diversidade e inclusão no ambiente de trabalho, juntamente com suas múltiplas facetas – como a realização de censos e diagnósticos, oferecimento de treinamentos e capacitações, formação de comitês de diversidade, encontros de grupos de afinidade e a revisão de práticas de gestão, políticas e processos de recrutamento –, vem ampliando a compreensão das empresas sobre a importância de cultivar uma “sinergia com as diferenças”. Isso tem promovido cada vez mais a valorização de princípios como respeito, ética, transparência e uma busca incessante pela igualdade de condições.

De um lado, é crescente a importância de uma organização proporcionar um ambiente que não só facilite o compartilhamento de informações, dados e conteúdo, mas também promova a troca de experiências sobre a implementação de programas de diversidade. No entanto, é sabido que a condução dessas iniciativas pode acarretar riscos significativos, especialmente porque envolve o uso de dados pessoais, incluindo dados sensíveis. Por isso, a adoção de boas práticas para garantir a conformidade dessas ações é essencial para manter a balança de riscos vs. benefícios equilibrada. Assim, nosso objetivo é apresentar soluções práticas que aprimorem a gestão organizacional das empresas e promovam efeitos positivos nas práticas adotadas por executivos, lideranças e departamentos de recursos humanos, *compliance*, jurídico e privacidade.

Para explorarmos as melhores práticas na proteção de dados pessoais, é essencial, inicialmente, compreender o que envolve os programas de diversidade e inclusão e oferecer uma visão geral sobre as principais atividades relacionadas ao tratamento de dados pessoais. Em seguida, é necessário nos aprofundarmos no contexto internacional, destacando como esses programas incentivam a responsabilidade das organizações em relação à diversidade, inclusão e segurança no

ambiente de trabalho. Abaixo, listamos as ações mais comuns que compõem um programa de diversidade e inclusão. Também aproveitamos a oportunidade para apresentar o conjunto de normas que fundamentam legalmente essas ações, servindo de possíveis bases legais adequadas para o uso de dados pessoais.

RESUMO DE UM PROGRAMA DE DIVERSIDADE E INCLUSÃO (D&I)			
Ação de D&I	Obrigação legal	Possível base legal da LGPD	Recomendações gerais
Projeto de diversidade e inclusão <i>lato sensu</i>	Sem obrigação legal específica	• Consentimento	• Elaborar política de privacidade e regulamento. • Manter registro de coleta do consentimento. • Garantir o direito de revogação do consentimento.
Processos seletivos de vagas afirmativas	• Art. 93 da Lei nº 8.213/1991 • Art. 39 da Lei nº 12.288/2010 • Lei nº 14.553/2023	• Consentimento • Cumprimento de obrigação legal	• Elaborar política de privacidade. • Manter registro de coleta do consentimento. • Garantir o direito de revogação do consentimento.
Programa de aceleração de pessoas com deficiência	• Art. 93 da Lei nº 8.213/1991	• Consentimento • Cumprimento de obrigação legal	• Elaborar política de privacidade e regulamento. • Manter registro de coleta do consentimento. • Garantir o direito de revogação do consentimento.
Censos	• Art. 93 da Lei nº 8.213/1991 • Art. 39 da Lei nº 12.288/2010 • Lei nº 4.553/2023	• Consentimento • Cumprimento de obrigação legal	• Coletar dados de forma voluntária. • Implementar medidas de anonimização e pseudonimização. • Comunicar de maneira clara sobre os objetivos da iniciativa.
Relatório de transparência salarial e critérios remuneratórios	• Lei nº 14.611/2023 • Decreto nº 11.795/2023 • Portaria MTE nº 3.714/2023	• Cumprimento de obrigação legal	• Implementar medidas de anonimização e pseudonimização.
Grupos de afinidade	Sem obrigação legal específica	• Consentimento	• Garantir proteção dos dados e a confidencialidade dos participantes.

3 Os programas de diversidade e inclusão no contexto internacional de incentivo à responsabilidade das organizações

Em 2026, completamos quinze anos em que dois importantes marcos internacionais⁵ impactaram de forma paradigmática nas áreas de responsabilidade social corporativa e direitos humanos. Foi no ano de 2011 que os *Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos* (UNGPs)⁶ foram aprovados por unanimidade pelo Conselho de Direitos Humanos da ONU⁷ e a *Responsabilidade Corporativa de Respeitar os Direitos Humanos*, tema do segundo pilar, foi adotada como padrão de conduta esperada nas *Diretrizes da OCDE para Empresas Multinacionais*,⁸ confirmando, assim, seu *status* como direito internacional não vinculativo.⁹ Os referidos princípios orientadores da ONU sobre empresas e direitos humanos fornecem orientação para governos e empresas globais na prevenção e tratamento de abusos de direitos humanos relacionados a negócios.¹⁰ Consistem em trinta e um princípios orientadores, cada um com comentários integrados. Eles são baseados em uma estrutura de três pilares, interdependentes: “Proteger, Respeitar e Remediar”.

No primeiro pilar, os Estados-Membros têm o dever de proteger os direitos humanos de abusos por parte de terceiros, incluindo empresas, por meio de leis,

⁵ Vale destacar que tais normas possuem natureza de *soft law*, ou seja, são normas de direito internacional que não possuem força vinculante, servindo como diretrizes a serem observadas pelos Estados-Membros e, naturalmente, pelas organizações que os integram. A obrigatoriedade de sua aplicação dependeria, assim, da edição de diplomas normativos ou da sua implementação por meio de políticas públicas, ainda inexistentes de forma harmonizada em matéria de diversidade.

⁶ RUGGIE, John. Guiding Principles on Business and Human Rights: Implementing the “United Nations “Protect, Respect and Remedy” Framework. 2011. (A/HRC/17/31). *Relatório do Representante Especial do Secretário-Geral sobre a questão de direitos humanos e corporações transnacionais e outras empresas de negócios*. Disponível em: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/121/90/PDF/G1112190.pdf?OpenElement>. Acesso em: 3 dez. 2025.

⁷ UNITED NATIONS. Human Rights Council. *Resolution 17/4*. 2011. (A/HRC/RES/17/4). Disponível em: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/17/4. Acesso em: 3 dez. 2025.

⁸ ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *OECD Guidelines for Multinational Enterprises*. Paris: OECD, 2011. Disponível em: <https://oecd.org/daf/inv/mne/48004323.pdf>. Acesso em: 3 dez. 2025.

⁹ Existem várias definições de “*soft law*” no direito internacional público, mas todas elas compartilham a característica comum de que, como declarações ou declarações de organizações de estados ou organizações governamentais internacionais, elas representam opiniões autorizadas sobre princípios e práticas que podem ter efeito legal. Cf.: SHAFFER, Gregory C.; POLLACK, Mark A. *Hard vs. Soft Law: Alternatives, Complements and Antagonists in International Governance*. University of Minnesota Law School, 2009. (Legal Studies Research Paper Series, n. 09-23).; e acerca da “*soft law*” fora do campo do direito internacional público, ver: CALLIESS, Graft-Peter; ZUMBANSEN, Peer. *Rough Consensus and Running Code: a Theory of Transnational Private Law*. Oxford: Hart Publishing, 2010. p. 225-260.

¹⁰ UN GUIDING PRINCIPLES REPORTING FRAMEWORK. *View Disclosures*. [S. l.]: Shift, [2025]. Disponível em: <https://www.ungpreporting.org/database-analysis/explore-disclosures/>. Acesso em: 3 dez. 2025.

políticas, regulamentos e julgamentos apropriados (UNGPs 1-10). No segundo, as empresas têm a responsabilidade de respeitar os direitos humanos; isso significa que elas devem identificar, evitar e lidar com danos aos direitos humanos por meio de suas atividades e relações comerciais (UNGPs 11-24). No terceiro, em que indivíduos e comunidades sofreram danos, tanto os Estados quanto as empresas têm um papel a desempenhar no fornecimento de acesso a um remédio eficaz (UNGPs 25-31). Acerca do respeito aos direitos humanos em ambientes corporativos, também há no escopo de atuação da Organização das Nações Unidas (ONU) o Pacto Global das Nações Unidas (UNGC), lançado em 2000 pelo então secretário-geral Kofi Annan. O Pacto Global é a maior iniciativa de sustentabilidade corporativa do mundo, com mais de 16 mil membros, entre empresas e organizações, distribuídos em 69 redes locais, que abrangem 160 países. Ele fornece 10 princípios para as empresas incorporarem em suas estratégias, políticas e procedimentos.¹¹ Esses princípios são:

Direitos Humanos: (1) *As empresas devem apoiar e respeitar a proteção dos direitos humanos proclamados internacionalmente; e (2) certificar-se de que não são cúmplices de abusos de direitos humanos.* Trabalho: (3) As empresas devem defender a liberdade de associação e o reconhecimento efetivo do direito à negociação coletiva; (4) a eliminação de todas as formas de trabalho forçado e obrigatório; (5) a abolição efetiva do trabalho infantil; e (6) *a eliminação da discriminação em relação ao emprego e à ocupação.* Meio Ambiente: (7) As empresas devem apoiar uma abordagem preventiva aos desafios ambientais; (8) empreender iniciativas para promover maior responsabilidade ambiental; e (9) incentivar o desenvolvimento e difusão de tecnologias ecologicamente corretas. Anticorrupção: (10) As empresas devem combater a corrupção em todas as suas formas, incluindo extorsão e suborno.

Vê-se que os programas de diversidade e inclusão e a introdução, de forma mais ampla, de ações afirmativas para grupos em condição de vulnerabilidade social são medidas práticas que perseguem a implementação, de forma direta, de pelo menos três princípios listados acima (1, 2 e 6). Os programas de diversidade

¹¹ Os Dez Princípios do Pacto Global das Nações Unidas são derivados da Declaração Universal dos Direitos Humanos, da Declaração da Organização Internacional do Trabalho sobre Princípios e Direitos Fundamentais no Trabalho, da Declaração do Rio sobre Meio Ambiente e Desenvolvimento e da Convenção das Nações Unidas contra a Corrupção (UNGC, 2018).

e inclusão inseridos em programas de governança e integridade¹² em ambientes corporativos podem, portanto, ser percebidos dentro de um contexto mais amplo de aplicação de normas internacionais sobre direitos humanos.¹³

Mas como implementar esses princípios na prática? A sustentabilidade corporativa começaria com um sistema de valores de uma empresa e uma abordagem baseada em princípios para “fazer negócios”. Isso significa que, para receber o selo referendado pela ONU, a organização deve buscar operar de maneira que, no mínimo, atenda às responsabilidades fundamentais nas áreas de direitos humanos, trabalho, meio ambiente e anticorrupção, algumas das principais pautas dos recentes movimentos resumidos na sigla ESG.¹⁴ Nesse sentido, empresas consideradas responsáveis adotariam os mesmos valores e princípios onde quer

¹² Quanto ao tema de integridade, há parâmetros básicos nos seguintes documentos: (i) Decreto nº 8.420/2015; (ii) Coleção Programa de Integridade da CGU, incluindo principalmente as Diretrizes para Empresas Privadas, o Manual para Implementação de Programas de Integridade e o Manual Prático de Avaliação do Programa de Integridade em PAR; (iii) Convenção Anticorrupção da OCDE; (iv) Convenção das Nações Unidas contra Corrupção; (v) Pacto Empresarial pela Integridade e contra a Corrupção (Ethos); e (vi) Movimento Empresarial pela Integridade e Transparência (Ethos). Incluem-se também as boas práticas de governança sugeridas pelo IBGC em seu Código de Melhores Práticas e demais guias e cadernos temáticos.

¹³ São considerados parâmetros internacionais e nacionais de direitos humanos aqueles expressos, por exemplo, nos seguintes documentos: Pacto Global da Organização das Nações Unidas de 2000; Objetivos do Desenvolvimento Sustentável (ODS) de 2015, com ênfase nos ODS 1, 2, 3, 4 e 11; Princípios Orientadores sobre Empresas e Direitos Humanos de 2011; Diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) para empresas Multinacionais, com atualização de 2011; Cartilha do Governo Federal, em parceria com a Fundação Getúlio Vargas, de 2017, “Implementando os Princípios Orientadores sobre Empresas e Direitos Humanos da ONU”; Convenções da Organização Internacional do Trabalho (OIT), com destaque para as Convenções nº 182, 138, 111, 105, 100, 98, 87 e 29; Declaração Tripartida de Princípios sobre Empresas Multinacionais e Política Social, adotada pela OIT em 1977 com última atualização em 2017; Primeira versão de Instrumento Internacional; Carta Empresarial pelos Direitos Humanos e pela Promoção do Trabalho Decente (Ethos). Importante atentar também a instrumentos que tratam sobre determinados grupos sociais em estado de vulnerabilidade, dentre os quais se destacam, (i) sobre as pessoas com deficiência: a Convenção Internacional sobre os Direitos das Pessoas com Deficiência da ONU, a Lei Brasileira de Inclusão e a Convenção nº 159 da OIT; (ii) sobre crianças: a Convenção sobre os Direitos da Criança da ONU, o Estatuto da Criança e do Adolescente e a Convenção sobre Proibição das Piores Formas de Trabalho Infantil da OIT; (iii) sobre gênero: Convenção sobre os Direitos Políticos da Mulher, Convenções nº 100, 103, 111, 156, 171 da OIT, Convenção para Eliminar todas as Formas de Discriminação contra a Mulher, Convenção Interamericana para Prevenir, Punir e Erradicar a Violência contra a Mulher (Convenção Belém do Pará); e (iv) sobre raça: a Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial da ONU, o Estatuto da Igualdade Racial (Lei nº 12.288/2010), a Lei nº 7.716/1989, que define crimes de preconceito de raça ou de cor (racismo), artigo 5º da CRFB de 1988, que considera racismo como crime inafiançável e imprescritível, e artigo 140 do Código Penal, que trata sobre injúria racial.

¹⁴ Os pilares da ESG vêm ganhando espaço nas maiores empresas do mundo e na imprensa. A sigla ESG corresponde às medidas adotadas pelas empresas referentes a *Environmental, Social and Corporate Governance* (tradução livre para ambiental, social e governança corporativa) com o intuito de obterem um selo de confiabilidade e responsabilidade. Dessa forma, o tema “diversidade e inclusão” se enquadra nas medidas referentes ao “social”. O selo ESG, atualmente, também tem função na propaganda institucional de uma empresa e é um aspecto que gera e demonstra valor para o mercado. Por isso, as organizações, por iniciativa própria, ou seja, sem que tenha havido qualquer interferência do Estado, passaram a adotar a pauta ESG.

que estivessem presentes. A ideia é que, ao incorporar os dez princípios do Pacto Global da ONU em suas estratégias, políticas e procedimentos, e estabelecer uma cultura de integridade, as empresas não estariam apenas cumprindo suas responsabilidades básicas para com as pessoas e o planeta, mas também preparando o cenário para tentar ampliar o seu sucesso em longo prazo, principalmente no que diz respeito à retenção de talentos e à formação de um eficiente time de colaboradores.¹⁵

Em relação aos direitos humanos, busca-se, em geral, forçar as companhias (e os Estados) a impactarem positivamente na comunidade e seu entorno, atuando com responsabilidade para a manutenção e proteção do meio ambiente e garantia dos direitos da comunidade, por meio do diálogo e iniciativas que assegurem, por exemplo, a segurança do território e das populações afetadas direta e indiretamente pelos negócios. Os programas de governança e integridade, por sua vez, buscam impactar diretamente no público interno. Por exemplo, no tema da diversidade e inclusão, tentam proporcionar um ambiente corporativo de maior inclusão, adotando medidas que permitam paridade de conhecimento e garantam tratamento equânime a todas as pessoas, independentemente de diferenças físicas, étnico-raciais ou de gênero, entre outras, nas etapas de contratação, formação, tratamento e desenvolvimento de carreira.

Diante do aumento do número de organizações que procuram adotar e aprimorar, cada vez mais, suas políticas relacionadas à diversidade e inclusão na força de trabalho, as pesquisas que permitem o mapeamento dos indicadores de diversidade ganham papel de destaque no ambiente corporativo, pois são um dos primeiros passos para o entendimento adequado do contexto em que as políticas e os programas de diversidade e inclusão serão introduzidos. Considerando a tendência de serem realizados cada vez mais mapeamentos de diversidade, sejam eles realizados manualmente ou com o auxílio de ferramentas tecnológicas, é imperativo que os processos de coleta e tratamento das informações estejam alinhados também com as boas práticas em matéria de privacidade e proteção de dados pessoais.

4 Contexto jurídico dos programas de diversidade e inclusão

É importante destacar que este estudo parte do pressuposto de que a maioria das organizações brasileiras ainda não possui programas robustos de governança em privacidade, sobretudo quando se trata de empresas de médio e pequeno

¹⁵ HALF, Robert. *Diversidade e Inclusão*. [S. l.], 2019. Disponível em: <https://www.roberthalf.com.br/sites/roberthalf.com.br/files/documents/robert-half-diversidade-inclusao-2019.pdf>. Acesso em: 3 dez. 2025.

porte. Muitas estão em fases intermediárias de projetos de adequação e ainda não realizaram avaliações detalhadas das atividades de tratamento de dados dos departamentos internos, especialmente as atividades da área de recursos humanos. Nesse contexto, podemos imaginar um cenário realista para o contexto brasileiro: organizações que até possuem uma noção geral sobre quais dados pessoais são usados nas operações diárias, mas que ainda não possuem processos estruturados para criar projetos inovadores baseados nas melhores metodologias de garantia da privacidade. Além disso, devemos considerar realidades em que falta experiência prática na implantação de novas operações de tratamento de dados que envolvem informações sensíveis, as quais inerentemente trazem maiores riscos de efeitos discriminatórios para os titulares e que, por conseguinte, podem expor as organizações a sérios problemas reputacionais, e os empregados, a riscos e danos. Nesse contexto, partimos de um lugar de cuidado e preocupação redobrada com os riscos trazidos pela implementação de programas de diversidade. Embora essas ações devam ser incentivadas, é necessário reconhecer que elas podem trazer riscos e danos significativos para as organizações – em especial, em contextos políticos de insegurança jurídica. No Brasil, há, inclusive, ação civil pública que discutiu o tema.¹⁶

Sendo assim, levamos em consideração o atual contexto social, geopolítico e judicial em que a temática de ações afirmativas encontra espaço nas cortes e nos principais veículos de imprensa para justificar uma posição conservadora quanto ao risco e uma atenção intensificada. É possível dizer que, no contexto brasileiro, os responsáveis pela implementação de programas de diversidade e inclusão precisam navegar por um ambiente de insegurança jurídica e normas esparsas. Isso porque, no plano das normas cogentes, salvo melhor juízo, não há legislação que aborde o tema das ações afirmativas para diferentes grupos em condição de vulnerabilidade, pelo menos de forma ampla e harmonizada. Ainda assim, é possível citar normas que tangenciam a temática, a exemplo do Estatuto da Igualdade Racial,¹⁷

¹⁶ A respeito do tema, já houve ajuizamento de ação civil pública (ACPCiv nº 0000790-37.2020.5.10.0015) pela Defensoria Pública da União (DPU), em face da empresa Magazine Luiza S.A., com a pretensão de impugnar seu “Programa de Trainee 2021”, que oferece vagas com exclusividade a pessoas negras.

¹⁷ Sendo talvez a legislação que mais se aproxima de uma instituição formal de política pública, importa transcrever os artigos 38 e 39 da Lei nº 12.288/2010. Cf.: Art. 38. A implementação de políticas voltadas para a inclusão da população negra no mercado de trabalho será de responsabilidade do poder público, observando-se: I - o instituído neste Estatuto; II - os compromissos assumidos pelo Brasil ao ratificar a Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial, de 1965; III - os compromissos assumidos pelo Brasil ao ratificar a Convenção no 111, de 1958, da Organização Internacional do Trabalho (OIT), que trata da discriminação no emprego e na profissão; IV - os demais compromissos formalmente assumidos pelo Brasil perante a comunidade internacional. Art. 39. O poder público promoverá ações que assegurem a igualdade de oportunidades no mercado de trabalho para a população negra, inclusive mediante a implementação de medidas visando à promoção da igualdade nas

normas que versam sobre acessibilidade em prédios públicos¹⁸ e em transporte público, o Estatuto da Pessoa com Deficiência,¹⁹ produção de Relatório de Transparência Salarial e Critérios Remuneratórios,²⁰ bem como a recente regra para cotas eleitorais femininas.²¹ Além disso, importa mencionar que diversas entidades vêm criando estatutos internos e regras de compromisso que buscam instaurar alguma forma de ação afirmativa, sendo possível citar as recentes normas para as eleições da Ordem dos Advogados do Brasil (OAB).²² Para facilitar a compreensão e enquadramentos das ações afirmativas no ordenamento, apresentamos abaixo um resumo do quadro normativo:

contratações do setor público e o incentivo à adoção de medidas similares nas empresas e organizações privadas. §1º A igualdade de oportunidades será lograda mediante a adoção de políticas e programas de formação profissional, de emprego e de geração de renda voltados para a população negra. §2º As ações visando a promover a igualdade de oportunidades na esfera da administração pública far-se-ão por meio de normas estabelecidas ou a serem estabelecidas em legislação específica e em seus regulamentos. §3º O poder público estimulará, por meio de incentivos, a adoção de iguais medidas pelo setor privado. §4º As ações de que trata o caput deste artigo assegurarão o princípio da proporcionalidade de gênero entre os beneficiários. §5º Será assegurado o acesso ao crédito para a pequena produção, nos meios rural e urbano, com ações afirmativas para mulheres negras. §6º O poder público promoverá campanhas de sensibilização contra a marginalização da mulher negra no trabalho artístico e cultural. §7º O poder público promoverá ações com o objetivo de elevar a escolaridade e a qualificação profissional nos setores da economia que contem com alto índice de ocupação por trabalhadores negros de baixa escolarização.

¹⁸ Sobre a temática, é possível citar o Decreto nº 5.296/2.004, que regulamenta as Leis nº 10.048/2000 e 10.098/2000, e a Convenção sobre os Direitos das Pessoas com Deficiência, assinada em 2007 e que teve seu texto aprovado pelo Decreto Legislativo nº 186, de 2008. Em âmbito prático, vale mencionar também as normas técnicas de acessibilidade da ABNT (NBR 9050 e a NBR 13994).

¹⁹ A Lei nº 13.146/2015 reforça a obrigatoriedade que as empresas prestadoras de serviços de transportes – sejam por trens, ônibus ou metrô – tenham com seus veículos e a garantia da acessibilidade. Um aspecto importante é que a lei impõe condições de acessibilidade não apenas aos veículos, mas também às estações, pontos de parada e sistema viário em geral.

²⁰ A produção do relatório é exigência da Lei nº 14.611/2023, que dispõe sobre a igualdade salarial e de critérios remuneratórios entre mulheres e homens, com regras estabelecidas no Decreto nº 11.795/2023 e na Portaria MTE nº 3.714/2023. Assim, trata-se de atividade necessária para o cumprimento de obrigação legal aplicável aos controladores de dados. Os dados coletados são, sempre que possível, anonimizados ou pseudonimizados, de modo a proteger a privacidade dos respectivos titulares.

²¹ O Congresso Nacional aprovou recentemente o Projeto de Lei nº 1.951/2021, que altera o §3º do art. 10 da Lei nº 9.504, de 30 de setembro de 1997, que prevê percentual de preenchimento mínimo de vagas para candidaturas de cada sexo, acrescentando também o art. 16-E, para dar destinação proporcional aos gastos de campanha com recursos do Fundo Eleitoral, e o art. 16-F, para obrigar o preenchimento mínimo de 15% das cadeiras às mulheres nas eleições proporcionais.

²² O Conselho Federal da Ordem dos Advogados do Brasil (OAB) aprovou a aplicação de 30% de cotas raciais e de 50% para mulheres nas chapas que concorrerem às eleições da entidade. A nova regra começou a valer em 2021 para as votações nas seccionais e, em 2022, para votação do Conselho Federal.

Resumo do quadro normativo	
Lei nº 8.213/1991 (planos de benefícios da Previdência Social)	Art. 93: define a obrigatoriedade das cotas e detalha a porcentagem de vagas a serem destinadas a pessoas com deficiência.
Lei nº 12.288/2010 (Estatuto da Igualdade Racial)	Art. 39, §8º: determina que registros administrativos e instrumentos de coleta de informações no mercado de trabalho incluam campos destinados à autodeclaração de cor ou raça.
	Art. 39, §9º: estabelece a extensão obrigatória do disposto no §8º acima a outros documentos ou registros relacionados, como: (i) formulários de admissão e demissão no emprego; (ii) formulários de acidente de trabalho; (iii) instrumentos de registro do Sistema Nacional de Emprego (Sine) ou estrutura equivalente; (iv) Relação Anual de Informações Sociais (Rais) ou documentos similares criados futuramente; e (v) documentos destinados à inscrição de segurados e dependentes no Regime Geral de Previdência Social.
Lei nº 14.611/2023 (igualdade salarial e de critérios remuneratórios entre mulheres e homens)	Regras estabelecidas em: • Decreto nº 11.795/2023; e • Portaria MTE nº 3.714/2023.

Em resumo, queremos destacar que, embora bem-intencionados, projetos voltados para abordar a desigualdade de oportunidades podem representar riscos para as empresas. Isso ocorre devido às diversas normativas aplicáveis e à sensibilidade do tema, que envolve questões de proteção de dados, relações públicas e o contexto das atuais relações geopolíticas. Sendo assim, para a hipótese analisada neste estudo, ainda que as organizações desejem manter um escopo restrito de um programa de diversidade e inclusão, por exemplo, focando apenas em questões raciais e de pessoas com deficiência (PCD) e dando pouca ou nenhuma ênfase para outras informações relacionadas a outras condições de vulnerabilidade (como pessoas LGBTQIAPN+), elas devem se precaver no que tange aos potenciais efeitos discriminatórios, bem como a exposições da organização e de suas marcas.

5 Aplicação da LGPD aos programas de diversidade e inclusão

A LGPD é o marco regulatório da proteção de dados pessoais no Brasil. Ela regulamenta as operações envolvendo o tratamento de dados pessoais, seja por meio físico ou digital, dentro ou fora da internet. A LGPD trata, entre outras questões, dos direitos dos titulares, das obrigações dos agentes de tratamento, do encarregado, dos parâmetros para segurança da informação, dos requisitos para

a transferência internacional de dados, das sanções e da atuação da Autoridade Nacional de Proteção de Dados (ANPD). A lei se aplica a qualquer pessoa física ou jurídica, de direito público ou privado, que realize operações de tratamento de dados pessoais em território nacional, caso o tratamento tenha como objetivo a oferta ou fornecimento de bens ou serviços, o tratamento de dados seja de indivíduos em território nacional, ou ainda os dados pessoais tenham sido coletados em território nacional. Importante frisar que a LGPD não é aplicável nos casos em que o tratamento dos dados pessoais seja realizado: por pessoa física, para fins particulares e não comerciais; para fins exclusivamente jornalísticos, artísticos ou acadêmicos; pelo Poder Público, nas hipóteses de utilização para a promoção da segurança pública, da defesa nacional, da segurança do Estado ou de atividades de investigação e repressão de infrações penais; ou quando esses dados pessoais forem provenientes de fora do território nacional e não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência (desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na lei brasileira).

A LGPD define dado pessoal como “informação relacionada a pessoa natural identificada ou identificável”.²³ O legislador não definiu expressamente o significado de “identificável”; todavia, determina que estarão fora do escopo de aplicação da lei apenas os “dados anonimizados”, por exemplo, dados relativos a titular que não possa ser identificado (ou reidentificado), considerando a utilização de meios próprios do controlador ou esforços razoáveis, levando-se em conta fatores objetivos, como custo, tempo e tecnologias disponíveis.²⁴ Neste ponto, destaca-se que o Regulamento Geral de Proteção de Dados europeu (GDPR), que inspirou em grande parte o texto da LGPD, determina que é identificável a pessoa natural “que possa ser identificada, direta ou indiretamente”, em especial por referência a um

²³ Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais, artigo 5º, inciso I.

²⁴ Em resumo, a anonimização de dados refere-se à conversão de dados pessoais em “dados anonimizados”, aplicando uma série de “técnicas de anonimização”. Normalmente, o processo de anonimização dos dados seria “irreversível”, e o destinatário do conjunto de dados anonimizado não seria capaz de recriar os dados originais. No entanto, pode haver casos em que uma organização que aplica a anonimização mantenha a capacidade de recriar os dados originais a partir dos dados anônimos; nesses casos, o processo de anonimização é “reversível”. Nos termos do artigo 12 da LGPD, os dados anonimizados não serão considerados dados pessoais para os fins da legislação, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios. Isso parece algo simples, mas, na verdade, não é quando se considera que os dados supostamente anônimos podem ser combinados com outras informações disponíveis para deduzir a identidade dos titulares dos dados.

identificador, que pode ser um nome, um número de identificação, dados de localização, identificadores eletrônicos ou outros elementos específicos relacionados a essa pessoa natural, como a denominação de um cargo que ocupa ou ocupou em determinada estrutura organizacional.

Ainda que a LGPD não tenha esclarecido diretamente em seu texto o que significa “pessoa natural identificada ou identificável”, é razoável esperar que os intérpretes da norma (tanto a ANPD quanto outros órgãos administrativos e o Poder Judiciário) adotem interpretação similar à do GDPR. Como se vê, não estando o caso em questão em qualquer das hipóteses de exclusão acima mencionadas e estando as informações pessoais coletadas, tanto em etapa de levantamento de indicadores (pesquisas de diversidade) quanto na etapa de implementação de programas de diversidade, dentro da definição de “dado pessoal” e/ou de “dado pessoal sensível”, não há como fugir à conclusão de que a LGPD se aplica às atividades de tratamento de dados realizadas no âmbito de implementação e manutenção de programas de diversidade e inclusão.

6 Dados anonimizados e a (controvertida) não aplicação da LGPD

O processo de anonimização de dados e as suas respectivas técnicas têm relevantes repercussões jurídicas quanto à aplicação do regime de proteção de dados.²⁵ Para o escopo deste estudo, as informações coletadas para monitoramento da diversidade em organizações são consideradas “dados pessoais”, tanto nos quadros legislativos europeus quanto na legislação brasileira de proteção de dados, desde que a pessoa ou organização que coleta os dados conheça (ou possa conhecer) a identidade do titular dos dados. São, portanto, dados pessoais no sentido de que se relacionam com uma pessoa natural identificada ou identificável. Entretanto, há casos em que os dados coletados não são capazes de identificar os indivíduos a que eles pertencem ou que não são capazes de identificá-los diretamente. Trata-se, respectivamente, das hipóteses em que estão sendo coletados dados anonimizados e pseudoanonimizados.

Segundo a LGPD, “dado anonimizado” é um “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”. Por sua vez, a “anonimização”

²⁵ MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudononimização de dados. *Caderno Especial – A regulação da Criptografia no Direito Brasileiro*, [S. l.], p. 99-128, dez. 2018.

constitui-se na “utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo”. A respeito do tema, a legislação garante também a anonimização de quaisquer dados pessoais excessivos, desnecessários ou tratados de forma inadequada se solicitados pelo titular a qualquer momento.²⁶ A lei assegura também o direito à anonimização de alguns processamentos específicos, como estudos realizados por institutos de pesquisa.²⁷ Além disso, a anonimização é um requisito caso o controlador decida manter os dados pessoais após o término da operação de tratamento.²⁸

Por mais que a LGPD não tenha trazido uma definição no artigo 5º para os “dados pseudonimizados” nem para a “pseudonimização”, é possível encontrar inteligência sobre esses conceitos em outros dispositivos legais. Conforme dispõe o §4º do artigo 13, “pseudonimização” é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro. Dessa forma, a pseudonimização ocorre, por exemplo, quando os identificadores, como nome, endereço, data de nascimento, são substituídos por um pseudônimo, código ou outra referência única para que os dados sejam identificáveis apenas para quem possui o código ou referência.

Como vimos, a definição de dados pessoais determina o escopo de aplicação da lei e é, portanto, de suma importância para o tema. Não obstante, o que constitui “dados pessoais” é uma das principais causas de dúvida no atual contexto de proteção de dados. A dificuldade de determinar o que conta como um dado pessoal está ancorada em vários fatores. Primeiro, os desenvolvimentos técnicos contínuos facilitam a identificação de indivíduos com base em dados que não eram percebidos como pessoais, ou seja, além das possibilidades de engenharia reversa com dados anonimizados, também é possível a combinação com outras informações externas. Segundo, a ampla definição de dados pessoais abrange cada vez mais pontos de dados. Terceiro, há muita incerteza a respeito das noções de pseudonimização e anonimização; e, finalmente, apesar de a tendência de harmonização internacional, permanecem divergências consideráveis nas leis e políticas de cada país.

Por exemplo, o GDPR adota uma perspectiva binária entre dados pessoais e dados não pessoais e sujeita apenas os primeiros ao seu escopo de aplicação.²⁹

²⁶ Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais, artigo 18, inciso IV.

²⁷ Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais, artigo 7º, inciso IV.

²⁸ Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais, artigo 16, inciso IV.

²⁹ A direção desse debate parece, inclusive, estar moldando as novas discussões sobre proteção de dados pessoais no continente Europeu e a atualização (ou como alguns preferem dizer, a simplificação) do GDPR.

Nos termos do Considerando 26,³⁰ o regulamento, em regra, não se aplica a dados anonimizados. Em contraste com essa perspectiva jurídica binária, as pesquisas que visam ao levantamento de indicadores de diversidade podem operar em um espectro entre dados claramente pessoais, dados claramente anonimizados e qualquer classificação no meio. Em síntese, o debate (em andamento) é, antes de tudo, sobre se os dados pessoais podem ser manipulados para se tornarem, de fato, anonimizados. Vê-se que essas tensões se desenrolam em vários domínios. Embora muitas vezes seja razoável presumir que os dados anonimizados não são pessoais, em interpretações frias do ordenamento, provavelmente esses dados se qualificariam como pessoais, o que significa que as leis de proteção de dados se aplicariam. Mais amplamente, essa análise também destaca a dificuldade em determinar se os dados que antes eram dados pessoais podem ser suficientemente anonimizados para atender ao limite de anonimização imposta pelos ordenamentos.

De acordo com a opinião do Grupo de Trabalho do Artigo 29, em *paper* não encampado pela *European Data Protection Board* (EDPB), há três critérios diferentes que devem ser considerados para determinar se a desidentificação é irreversível ou se pode ser classificada como tão permanente e irreversível quanto um apagamento, ou seja, se (i) ainda é possível destacar um indivíduo; (ii) ainda é possível vincular registros relacionados a um indivíduo; e (iii) se as informações relativas a um indivíduo ainda podem ser inferidas. Quando a resposta a essas três perguntas

Decisão do Tribunal de Justiça da União Europeia (TJUE) no caso EDPS v SRB (C 413/23 P), emitida em 4 de setembro de 2025, marca um importante precedente na área de proteção de dados, ao abordar o conceito de “dados pessoais”, um tema central na prática. O litígio envolveu o Supervisor Europeu de Proteção de Dados (EDPS) e o Conselho Único de Resolução (SRB), originado da resolução do Banco Popular e do procedimento de “direito a ser ouvido”, em que dados foram coletados por meio de um registro e formulário *online*. As discussões focaram se dados pseudonimizados são, por padrão, dados pessoais ou podem ser considerados “não pessoais” para quem não consegue associá-los a um indivíduo sem esforço desproporcional. O debate opõe a abordagem absoluta, que considera como dados pessoais qualquer informação que possa ser associada a um indivíduo, à abordagem relativa, que restringe essa classificação a dados vinculáveis por meios razoáveis. Tradicionalmente, autoridades de proteção de dados aplicam a primeira por segurança, mas decisões do TJUE, como nos casos Breyer e Scania, apoiam a segunda. A relevância da decisão do TJUE no caso EDPS v SRB vai além de reafirmar a abordagem relativa, pois esclarece que dados pseudonimizados podem ser considerados pessoais para um controlador, mas não para outro destinatário incapaz de ligá-los razoavelmente a um indivíduo. Essa posição tem impactos práticos significativos e contrasta com orientações restritivas como as das Diretrizes 1/2025 do Conselho Europeu de Proteção de Dados, que ainda preferem uma visão mais absoluta.

³⁰ UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, Luxemburgo, L 119, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 12 dez. 2025.

é negativa, os dados podem ser considerados anonimizados.³¹ Em 16 de janeiro de 2025, o EDPB adotou suas Diretrizes 01/2025 sobre pseudonimização. As diretrizes preliminares estabelecem os requisitos legais e técnicos que o EDPB considera necessários para que a pseudonimização seja eficaz.³²

Embora o debate sobre a identificação tenha sido vigoroso e produtivo, ainda não há uma direção clara para um entendimento mundialmente uniforme. A doutrina considera que uma anonimização perfeita de conjuntos de dados com informações pessoais seria impossível. Como resultado, as legislações vêm demorando a se adaptar às abordagens holísticas e às tecnologias emergentes. Por isso, a melhor maneira de avançar para além das supostas falhas da anonimização é se concentrar no processo de minimizar o risco de reidentificação e a divulgação de atributos sensíveis, impondo uma abordagem baseada em risco para determinar se os dados são qualificados como dados pessoais. Sendo assim, quando existir um risco razoável de identificação, os dados podem (ou devem) ser tratados como dados pessoais. Nos casos em que o risco existente depende meramente da negligência (ou seja, a identificação provavelmente não depende de todos os meios razoavelmente passíveis de serem utilizados por agente externo, mas de algum erro interno), é possível tratá-lo como dado anonimizado, mesmo que a identificação não possa ser excluída com absoluta certeza.

Para efeitos deste estudo, as organizações podem considerar se e em quais circunstâncias seria apropriado para elas considerarem a possibilidade de coletar dados sobre diversidade anonimamente. Em primeiro lugar, devem avaliar a utilidade de coletar dados anonimizados para as finalidades pretendidas. Em segundo, devem avaliar se de fato conseguem utilizar as informações mapeadas de forma anônima. De todo modo, caso optem por tentar coletar dados anônimos, isso poderia ser feito por meio de uma pesquisa sem identificação direta, o que inclui, por exemplo, não coletar determinadas informações que poderiam indiretamente identificar o indivíduo, como a posição em que ocupa ou eventual característica singular dentro de determinado grupo. É possível utilizar também um sistema em que os indivíduos estão vinculados a um número de identificação, mas onde uma “chave” que ligaria esses números de volta a indivíduos não é armazenada, ou melhor, não está sob controle da mesma organização que coleta os dados anonimizados.

³¹ ARTICLE 29 WORKING PARTY. *Opinion 05/2014 on data anonymization techniques*. 2014. Disponível em: <https://www.pdpjournals.com/docs/88197.pdf>. Acesso em: 3 dez. 2025.

³² As diretrizes também contêm um anexo com 10 exemplos práticos. Cf.: COMITÊ EUROPEU DE PROTEÇÃO DE DADOS (EDPB). *Guidelines 01/2025 on Pseudonymisation*. [S. l.], 2025. Disponível em: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf. Acesso em: 3 dez. 2025.

7 Enquadramento legal na LGPD para o tratamento de dados pessoais coletados em programas de diversidade e inclusão

O uso de dados pessoais, independentemente da finalidade pretendida, somente poderá ocorrer se estiver amparado em alguma das hipóteses autorizativas estabelecidas na LGPD. Essas hipóteses são conhecidas como bases legais para o tratamento de dados pessoais e estão previstas nos arts. 7º e 11 da LGPD. O art. 7º da lei enumera dez hipóteses que fundamentam a utilização de dados pessoais não sensíveis, ao passo que o art. 11 prevê oito circunstâncias em que é permitida a realização de atividades de tratamento envolvendo dados pessoais de natureza sensível. A avaliação a ser realizada pelo controlador para a definição da base legal mais adequada e segura para que um dado pessoal possa ser coletado, armazenado e processado deve considerar a finalidade específica a ser alcançada por meio do tratamento, além do contexto do caso concreto. Nesse sentido, para que as operações de tratamento de dados pessoais sejam consideradas lícitas e legítimas, além do respeito aos princípios estabelecidos na LGPD, o agente de tratamento deve confirmar, antes de qualquer utilização do dado pessoal, a existência de alguma das hipóteses previstas na legislação (art. 7º ou, no caso de dados sensíveis, art. 11 da LGPD).

Embora a LGPD forneça um amplo leque de bases legais – que não possuem superioridade hierárquica entre si – autorizando o tratamento de dados pessoais com fins de pesquisa de mapeamento de indicadores de diversidade e implementação de programas e ações afirmativas, pode ser considerado uma boa prática, especialmente à luz da ética,³³ confiar no consentimento como base legal para o

³³ No ordenamento brasileiro, mesmo antes da LGPD, há exemplos de normas que buscam garantir a proteção do participante e a ética nas pesquisas. Por exemplo, no âmbito das pesquisas em saúde envolvendo seres humanos, temos as Resoluções nº 466/2012 e 510/2016 do Conselho Nacional de Saúde (CNS). Estas Resoluções dispõem, em resumo, sobre as normas aplicáveis a pesquisas em Ciências Humanas e Sociais cujos procedimentos metodológicos envolvam a utilização de dados diretamente obtidos com os participantes ou de informações identificáveis ou que possam acarretar riscos maiores do que os existentes na vida cotidiana. As pesquisas que envolvem seres humanos devem atender aos fundamentos éticos e científicos pertinentes. Como consequência, as Resoluções obrigam que os participantes forneçam consentimento livre e esclarecido. O convidado a participar deve se manifestar de forma autônoma, consciente, livre e esclarecida por meio de Termo de Consentimento Livre e Esclarecido (TCLE), que deve ser elaborado pelo pesquisador responsável em linguagem acessível à compreensão do participante da pesquisa. O TCLE deverá ser obtido após o participante da pesquisa e/ou seu responsável legal estar suficientemente esclarecido de todos os possíveis benefícios, riscos e procedimentos que serão realizados, bem como fornecidas todas as informações pertinentes à pesquisa. O TCLE é um documento recomendado por declarações internacionais, códigos de ética, resoluções e leis específicas para ser utilizado no cotidiano de pesquisas em saúde. A prática ou a obtenção do consentimento informado no exercício da medicina e da pesquisa em humanos é própria das últimas décadas e caracteriza o aperfeiçoamento da ética biomédica, constitui um requerimento legal e ético na pesquisa clínica envolvendo humanos.

tratamento de dados para algumas das atividades. Isso porque, se considerarmos que a LGPD restringe o uso de certas bases legais para o tratamento de dados sensíveis, o consentimento, presente tanto no artigo 7º quanto no artigo 11, se mostra como uma hipótese autorizativa estratégica para o tratamento de dados pessoais e dados pessoais sensíveis. Naturalmente, quando houver uma obrigação legal que deve ser cumprida pelo controlador, por exemplo, nos casos em que o controlador precisa validar que possui o número mínimo de pessoas com deficiência entre o seu quadro de funcionários (conforme a Lei nº 8.213/1991), ou quando precisa realizar um levantamento dos critérios remuneratórios e publicar um Relatório de Transparência Salarial e Critérios Remuneratórios (conforme a Lei nº 14.611/2023), a utilização das bases legais do cumprimento de obrigação legal ou regulatória (art. 7º, II, ou art. 11, II, “a”) se mostra mais adequada – e menos arriscada do ponto de vista corporativo. Importante considerar, contudo, que há atividades de tratamento dentro do contexto dos programas de diversidade e inclusão que não podem, em tese, ser sustentadas pela base legal da obrigação legal e regulatória. Nesse sentido, restam poucas opções ao controlador, que não o uso da hipótese de coleta do consentimento. Dessa forma, se o consentimento for escolhido, a organização deverá lidar com certas particularidades dessa base legal.³⁴ Em resumo, deverá ter precaução com as formalidades e levar em conta (i) o contexto da relação de trabalho e/ou de emprego e a disparidade entre as partes envolvidas; (ii) o fato de que os titulares terão o direito de se opor ao tratamento e de revogar o consentimento; (iii) a existência (ou não) de dados sensíveis; (iv) o formato da coleta (“adjetivos do consentimento”) e o gerenciamento posterior dos consentimentos fornecidos pelos titulares.

Para dados sensíveis, o consentimento recebe mais qualificações, devendo ser (i) livre, (ii) informado, (iii) inequívoco e dado (iv) de forma específica e (v) destacada para (vi) finalidades específicas. Ele deve ser expressamente confirmado em palavras, e não por qualquer outra ação positiva. Assim, se a organização for confiar nessa base, é recomendável estudar as boas práticas de obtenção de consentimento contidas nas orientações dos reguladores – inclusive as autoridades de proteção de dados estrangeiras. No Brasil, ainda que a ANPD não tenha emitido orientação específica sobre a base legal do consentimento, por exemplo, por meio de guia com casos abstratos objeto de consultas, é possível colher posicionamentos do regulador em outras orientações. Por exemplo, no

³⁴ TEFFÉ, Chiara Spadaccini de; VIOLA, Mário. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civillistica.com*, Rio de Janeiro, v. 9, n. 1, p. 1-38, 2020. p. 6.

guia³⁵ denominado *Hipóteses legais de tratamento de dados pessoais: legítimo interesse*, a ANPD analisou como escolher a base legal no caso de uso de dados sensíveis, inclusive mediante casos práticos hipoteticamente exemplificados. Há manifestação do regulador também no guia³⁶ elaborado em parceria entre a ANPD e o Tribunal Superior Eleitoral (TSE) acerca da aplicação da LGPD por agentes de tratamento no contexto eleitoral.

Para cumprir com os objetivos deste estudo e aterrissarmos na prática, e para indicar formas concretas de cumprir com as particularidades do consentimento, bem como com os nortes impostos pelo princípio da transparência, sugerimos uma declaração de coleta de dados sensíveis de público interno e termo de consentimento que podem ser adaptados para a coleta de informações para mapeamento de indicadores de diversidade. Esse formulário, naturalmente, foi preparado apenas para fins informativos.

8 Declaração de coleta e termo de consentimento para mapeamento de indicadores de diversidade e inclusão no âmbito das relações de trabalho

Depois de lerem as informações gerais sobre os programas de diversidade e inclusão introduzida, é importante fornecer um meio para que os participantes, ou seja, o público interno de uma organização, deem consentimento para o tratamento de suas informações. Isso pode ocorrer, por exemplo, por meio de caixas para que haja marcação digital (*check boxes*) em ambientes corporativos digitais ou em caixas para serem marcadas em um formulário de papel, preferencialmente com a assinatura do colaborador. A maioria das organizações com robustez para introduzir programas amplos de diversidade e inclusão possui sistemas de tecnologia da informação capazes de gerar formulários anônimos ou pseudoanonimizados, como no caso do Google Forms ou do Microsoft Surveys. Importa lembrar que uma mudança fundamental com a LGPD é que esse consentimento deve ser uma indicação livre, específica, informada e inequívoca dos desejos de uma pessoa:

³⁵ Cf.: AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo: Hipóteses legais de tratamento de dados pessoais: legítimo interesse*. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 3 dez. 2025.

³⁶ Cf.: AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo: aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral*. Brasília, DF: Tribunal Superior Eleitoral, 2021. Disponível em: <https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/guia-orientativo-aplicacao-da-lgpd.pdf>. Acesso em: 3 dez. 2025.

ou seja, não importando se o formato escolhido seja físico ou digital, essas caixas não podem estar pré-preenchidas como “aceito”. Dessa forma, não é válido o consentimento passivo ou presumido, no qual se presume que uma pessoa tenha dado consentimento.

Fundamental destacar também que, no contexto de uma relação de trabalho, o consentimento obtido do empregado pode não se mostrar livre (e, portanto, válido), devido ao desequilíbrio de poder e subordinação entre as partes. Por essa razão, uma análise detalhada deve ser realizada antes de sua eventual aplicação. Sendo assim, eventual tratamento de dados pessoais que não esteja amparado por alguma das bases legais previstas na LGPD poderá ser ultimado através de “termo de consentimento opcional” ou instrumento similar, em que seja coletado o consentimento livre, informado, inequívoco e dado de forma específica e destacada, para finalidades específicas, e sem qualquer imposição por parte do controlador, tampouco penalização em caso de negativa de participação. Para que não restem dúvidas, o referido termo deverá ser opcional e precisa dispor, pelo menos sobre os dados coletados, finalidades, a forma de sua utilização e os procedimentos específicos para o exercício dos direitos, inclusive, o direito de não fornecer o consentimento.

INFORMAÇÕES PARA PARTICIPANTES E TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS			
Programa/projeto	[Inserir resumo do programa / projeto]		
Propósitos e informações gerais da pesquisa, ação ou programa	(i) Público-alvo, (ii) perguntas/indicadores gerais a que se quer responder, (iii) resumos dos tipos, métodos e metodologias de pesquisa, (iv) quem está conduzindo a pesquisa, incluindo informações sobre a organização e como a pesquisa é financiada, (v) informações sobre qualquer terceiro que tenha acesso aos dados sob contrato (e.g. consultor de pesquisa, consultoria de RH) e informações sobre políticas e práticas de privacidade de terceiros; etc.		
Tipos de dados pessoais a que se espera coletar	Dados pessoais/sensíveis (categoria)	Descrição / Dados especificados	Justificativas de uso (finalidades)
	[inserir]	[inserir]	[inserir]
Participação voluntária	Os participantes são livres para deixar o programa a qualquer momento, sem qualquer consequência negativa, como [inserir].		

INFORMAÇÕES PARA PARTICIPANTES E TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

Termo de consentimento para tratamento de dados pessoais e dados pessoais sensíveis

Este Termo de Consentimento ("Termo") trata da participação no programa de [inserir], denominado [inserir] ("Programa"). O Programa é conduzido pela [inserir Controlador] conforme descrito neste Termo, com base nas informações acima especificadas e fornecidas voluntariamente por você. Como o Programa envolve o tratamento de dados pessoais, incluindo dados pessoais sensíveis, como [inserir dados sensíveis de forma específica e destacada], para as finalidades específicas descritas neste Termo, é necessário obter o consentimento para o uso desses dados, o que inclui o compartilhamento dessas informações com [inserir terceiros e finalidades específicas de uso por terceiros]. Caso você concorde em participar do Programa, seus dados pessoais e dados pessoais sensíveis serão tratados conforme descrito neste Termo. Os dados pessoais e informações coletadas do(a) PARTICIPANTE serão mantidos por [inserir prazo de retenção] anos com fundamento no artigo [inserir artigo] da Lei [inserir fundamento legal]. Este Termo é *opcional* e dispõe sobre os dados coletados, finalidades, a forma de sua utilização e os procedimentos específicos para o exercício dos direitos, inclusive, o direito de não fornecer o consentimento.

Benefícios e riscos de participar

Os benefícios podem incluir, por exemplo: (i) recebimento das conclusões do Programa; (ii) metas; (iii) [inserir]. Os riscos podem incluir, por exemplo: (i) levantamento de temas sensíveis, o que pode causar uma reação emocional negativa; etc. Obs.: é importante sinalizar o canal para o suporte adequado no caso de riscos decorrentes e saber para qual suporte direcionar antes de começar com a coleta de dados.

Políticas aplicáveis

Listagem exemplificativa de políticas, códigos e normas internas aplicáveis e resumo das disposições mais relevantes (inserir links): (i) Política e/ou Aviso de Privacidade; (ii) Política e/ou Aviso de Privacidade para público interno; (iii) Política de Segurança da Informação; (iv) Política de *Compliance*; (v) Códigos de Conduta; (vi) Política de Diversidade e Inclusão; (vii) Outras.

Direitos dos titulares e canais de comunicação

Lista indicativa de quais direitos dos Titulares podem ser aplicáveis: Confirmação e acesso; Anonimização, Bloqueio ou eliminação; Correção; Informação sobre a possibilidade de não consentir; Informação sobre o compartilhamento; Oposição; Portabilidade; Revogação do consentimento; Revisão de decisões automatizadas. Caso você acredite que seus Dados Pessoais foram usados de maneira incompatível com este Termo e com a(s) Política(s) acima ou com as suas escolhas enquanto titular, ou, ainda, se você tiver dúvidas, comentários ou sugestões relacionadas ao Programa, entre em contato conosco. Há um Encarregado (DPO) e responsáveis que estão à disposição nos endereços de contato abaixo indicados.

Informações do encarregado de dados | DPO

Identificação (nome) do Encarregado:
E-mail para contato / forma de exercer direito de titular:
Endereço para correspondências:

Outros contatos relevantes

Nome: [e.g. responsável RH]
E-mail para contato:
Telefone para contato:

Consentimento

Eu compreendo que minha participação é totalmente gratuita e voluntária, e que a recusa em participar não implicará em qualquer prejuízo. Compreendo também que posso revogar, a qualquer momento, o meu consentimento. Ademais, confirmo que li este Termo e compreendi como meus dados pessoais e dados pessoais sensíveis serão tratados, bem como as implicações decorrentes do meu consentimento. Por fim, ratifico que possuo ciência e autorizo expressamente neste ato a coleta, armazenamento, tratamento e compartilhamento dos meus dados pessoais e dados pessoais sensíveis, nos exatos termos do presente instrumento, em atenção ao que dispõe a Lei 13.709/2018 e demais normas aplicáveis. Local, _____ de _____ de _____.
Nome: _____
Assinatura do(a) PARTICIPANTE: _____

O modelo acima também pode ser adaptado para uso como formulário impresso ou digital para entrevistas com grupos focais. Também pode ser adaptado com a introdução da pesquisa, seja impressa ou *online*. Da mesma forma, pode ser especificamente projetado para pesquisas em que os dados são anonimizados. Algumas dessas informações também podem ser abordadas nas declarações de privacidade e proteção de dados direcionadas para os sujeitos em questão. Por fim, recomenda-se, inclusive, que uma cópia (ou *link*) da declaração de privacidade geral da organização seja fornecida aos participantes da pesquisa, juntamente com as informações sobre o projeto e o termo de consentimento.

9 Coletando dados pessoais para programas de diversidade e inclusão: requisitos mínimos de transparência

Vimos que os dados sobre diversidade que não são capazes de identificar os indivíduos a que eles pertencem são considerados dados anonimizados e estão fora do escopo de aplicação da LGPD. Além disso, explicamos que os conceitos de anonimização e pseudonimização envolvem uma série de fatores e que as organizações devem tomar cuidado para que esses dados, de fato, não sejam capazes de identificar indivíduos com referência a qualquer outra informação, direta ou indiretamente. Para o escopo deste artigo, partiremos do pressuposto de que os dados pessoais coletados nas iniciativas de diversidade e inclusão realizadas “*in house*” não podem ser considerados anonimizados, seja pelo fato de que os questionários foram propositalmente construídos de maneira a identificar os indivíduos, seja porque, embora tenha sido feito um esforço para desvincular os dados dos indivíduos, ainda é possível, mediante esforços razoáveis, chegar às pessoas que forneceram as informações ou porque o mesmo controlador que coleta as informações pseudonimizadas detém também os códigos de referência capazes de reverter o processo.

Dessa forma, para o recorte proposto neste estudo, desde que a organização conheça a identidade da pessoa entrevistada ou que possa conhecer, a Lei de Proteção de Dados se aplica e será necessário cumprir os requisitos legais, por exemplo, aqueles relativos às informações que devem ser fornecidas aos indivíduos no momento da coleta dos dados. Cuida-se da aplicação prática do princípio da transparência. Para o cumprimento desse princípio, recomenda-se que, no momento da coleta, se forneçam: (i) informações sobre a organização controladora de dados, incluindo nomes e detalhes de contato, detalhes do representante (se for relevante) e detalhes de identidade e contato do encarregado de dados. Pode ser recomendável fornecer também informações sobre os

responsáveis pela condução dos projetos e ações, a exemplo dos departamentos de recursos humanos, *compliance*, jurídico e/ou privacidade; (ii) informações sobre as categorias de dados que serão coletados, os sujeitos objeto das pesquisas, a forma e a duração do tratamento de dados; (iii) o objetivo de coletar os dados, incluindo as finalidades específicas e explícitas (e detalhadas) para as quais eles serão usados e se eles serão usados, por exemplo, para tomar uma decisão automatizada. Além disso, pode ser recomendável ir além³⁷ dos requisitos legais e indicar a base legal para o uso dos dados. Também é importante ser transparente em relação às pessoas, sejam elas físicas ou jurídicas, internas ou externas, que receberão ou terão acesso aos dados, por exemplo, os times internos que utilizarão as informações ou eventual consultoria; (iv) outras informações relevantes, incluindo se os dados serão compartilhados com terceiros, transferidos, armazenados ou tratados fora do país e qual base legal fundamenta a transferência; por quanto tempo os dados serão armazenados; quais arranjos de segurança estão em vigor para proteger os dados; se o fornecimento dos dados pelo colaborador é necessário e as consequências de não fornecê-los (conforme abordamos oportunamente). Caso a organização esteja considerando transferir um grande volume de dados ou quando detectado outro elevado risco para os direitos fundamentais, pode ser aconselhável concluir uma avaliação de impacto à proteção de dados pessoais; (v) informações sobre os direitos dos titulares de dados, formas e canais preferenciais para recebimento de solicitações; (vi) informações de contato, ou seja, com quem os colaboradores podem entrar em contato em relação a perguntas ou reclamações.

Em relação à condução das iniciativas de diversidade e inclusão em si, há uma série de pontos a serem considerados ao coletar os dados. A coleta de informações sobre diversidade provavelmente envolverá o processamento de dados pessoais adicionais do funcionário (em relação àqueles necessários para a execução do contrato), incluindo dados pessoais de “categoria sensível”, como opções sexuais. Como resultado, há uma série de questões de conformidade que precisam ser resolvidas para garantir que os dados possam ser processados legal, legítima e eticamente. Abaixo, algumas recomendações gerais para o tratamento de dados sensíveis:

³⁷ Utiliza-se a expressão “ir além” no sentido de que a LGPD não trouxe obrigação expressa de declarar publicamente a base legal para o tratamento dos dados para cada operação de tratamento.

Recomendação	Detalhamento
Identificação de quais dados devem ser coletados e titulares de dados participantes	O questionário deve ser construído de forma a coletar somente os dados necessários para se chegar às informações buscadas pela organização. Além disso, deve-se avaliar se o público-alvo inclui situações excepcionais, como colaboradores em licença por doença, licença-maternidade ou afastados por outros motivos, se estiverem em contato com a empresa. Deve-se avaliar se “ <i>secondees</i> ” e terceirizados (contratados em modalidade temporária e/ou “pessoa jurídica”) também podem ser incluídos. Pode ser recomendável a exclusão de colaboradores que residam fora do território nacional.
Quando houver dado sensível, indicar base legal disposta no art. 11 da LGPD	Todo tratamento de dados sensíveis deve ser respaldado em uma das bases legais dispostas no art. 11 da LGPD. As opções apresentadas são mais restritas – não englobando, por exemplo, o legítimo interesse – e impõem para a sua aplicação requisitos adicionais de proteção. O consentimento recebe, por sua vez, mais qualificações, devendo ser livre, informado, inequívoco e dado de forma específica e destacada, para finalidades específicas. Entretanto, como já mencionado, cuidando-se de relação de trabalho, o consentimento deve ser coletado com precauções adicionais, a exemplo da transparência acentuada e clareza sobre a participação voluntária.
Considerar o desenvolvimento de uma avaliação preliminar de impacto (relatório de impacto)	O relatório de impacto à proteção de dados pessoais não é necessariamente obrigatório para o tratamento de dados sensíveis, porém, é visto como boa prática e instrumento relevante, podendo ser requerido pela ANPD. Trata-se de documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Nesse sentido, pode ser recomendável que, antes de elaborar um relatório de impacto completo, seja iniciado, paralelamente, uma avaliação de risco preliminar, a fim de entender o escopo dos riscos envolvidos, bem como documentar as medidas técnicas e organizacionais implementadas, ou seja, os cuidados tomados pela organização para a realização do programa.
Aplicar de forma ampliada medidas técnicas, administrativas e de segurança da informação	É fundamental implementar uma Política de Segurança da Informação que estabeleça diretrizes sobre padrões e medidas técnicas internas de segurança; e desenvolver um Plano de Resposta a Incidentes com dados pessoais. Soma-se a isso a implementação de controles para garantir que apenas os membros que precisam de acesso às informações de fato tenham. Neste ponto, mostra-se relevante aplicar também normas de padronização pertinentes. No caso específico das iniciativas de diversidade, deve-se restringir ao máximo possível o acesso aos dados sensíveis, bem como segregar tais informações. Ademais, deve ser criado um protocolo de retenção e exclusão, ou seja, as organizações devem atualizar suas políticas e procedimentos de retenção e exclusão de dados que contemplem as novas atividades.
Dialogar com os princípios do <i>Privacy by Design</i> e do <i>Privacy by Default</i>³⁸	De acordo com os princípios do <i>Privacy by Design</i> e <i>Privacy by Default</i> , a proteção da privacidade deve ser incorporada desde o início e mantida ao longo de todo o ciclo de vida de qualquer projeto, sistema, serviço, produto ou processo que envolva o tratamento de dados pessoais. Como recomendado, isso implica na realização, por parte do controlador, de avaliações de impacto prévias à implementação, além da adoção de medidas técnicas e organizacionais apropriadas e mecanismos de prestação de contas e transparência. É essencial que os dados pessoais sejam claramente especificados e limitados antes do início do tratamento, garantindo-se que os titulares sejam devidamente informados sobre como seus dados serão processados, que seja dada uma escolha verdadeira, e que apenas os dados necessários para atingir o propósito específico sejam utilizados. Nesse contexto, a consulta ao encarregado de proteção de dados, bem como aos departamentos jurídico e de compliance, é crucial para assegurar que esses princípios sejam devidamente integrados. Ademais, incluir responsabilidades quanto ao programa de diversidade no escopo de trabalho das equipes de recursos humanos, tecnologia e segurança da informação pode ajudar a assegurar diligência e a adoção das melhores práticas no manejo de dados pessoais.

³⁸ CF.: BYGRAVE, Lee A. Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review*, Oslo, v. 4, n. 2, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3035164. Acesso em: 3 dez. 2025.

Recomendação	Detalhamento
Atentar-se aos princípios da LGPD, em especial, os da não discriminação, necessidade (minimização) e finalidade	É essencial que as organizações se atentem aos princípios estabelecidos pelas leis de proteção de dados, especialmente aqueles relacionados à não discriminação, necessidade (ou minimização) e finalidade. O princípio da não discriminação assegura que o tratamento de dados não seja utilizado para fins discriminatórios, ilícitos ou abusivos. O princípio da minimização, também conhecido como princípio da necessidade, exige que o tratamento de dados seja estritamente limitado ao que é imprescindível para o cumprimento de suas finalidades, envolvendo apenas dados que sejam pertinentes, proporcionais e não excessivos. O princípio da finalidade, por sua vez, determina que o tratamento de dados deve ser realizado para finalidades legítimas, específicas, explícitas e claramente informadas ao titular dos dados, prevenindo o uso dos dados de maneira incompatível com esses objetivos previamente estabelecidos. Ao seguir esses princípios, as organizações não apenas garantem conformidade legal, mas também fomentam confiança e transparência com os titulares dos dados.
Avaliar a possibilidade de anonimização frente aos objetivos pretendidos	Ao considerar a possibilidade de anonimização de dados em relação aos objetivos previstos, é fundamental entender que a remoção de informações diretamente identificáveis, como nomes, cargos e endereços de <i>e-mail</i> , não garante automaticamente o anonimato dos dados. Assim, ao divulgar resultados, mesmo que de forma interna, a organização deve assegurar que eles não possam ser decompostos ou cruzados de maneira que permita a identificação de participantes específicos. Quando os resultados forem compartilhados com terceiros, especialmente para finalidades como obtenção de selos e certificações de reconhecimento, como “bom lugar para trabalhar” ou “empresa que respeita a diversidade”, é crucial revisar cuidadosamente o conteúdo a ser compartilhado. Além disso, incluir cláusulas de proteção em instrumentos contratuais ajuda a mitigar riscos associados à reidentificação dos dados. Isso não só protege os participantes e a organização, mas também demonstra um compromisso com práticas responsáveis e éticas no tratamento e compartilhamento de dados.
Aumentar a transparência	Declarações, avisos, notificações e políticas de privacidade direcionados aos colaboradores e demais participantes devem ser revisados e atualizados para incorporar informações detalhadas sobre os objetivos do tratamento de dados, além de, quando aplicável, especificar a base legal que justifica esse tratamento. É crucial que os participantes sejam plenamente informados sobre a possibilidade de compartilhamento e divulgação desses dados, caso isso seja relevante ao propósito do tratamento. Caso as pesquisas sejam realizadas regularmente, pode ser aconselhável incluir disposições específicas sobre elas nos avisos e políticas de recrutamento e nos contratos. Isso garante que os indivíduos estejam cientes de como seus dados serão utilizados ao longo da relação e cria um ambiente de transparência e confiança.

As recomendações acima não são exaustivas e ilustram apenas algumas das boas práticas e disposições legais para o tratamento de dados sensíveis. Refletem, também, orientações de autoridades europeias de proteção de dados, uma vez que ainda não temos orientações concretas da ANPD para esse tema. Em geral, essas recomendações se aplicam também, em alguma medida, às operações de tratamento mais críticas de uma organização. Esses são os processos que envolvem dados sensíveis, dados de menores e processos que possam gerar discriminação ou riscos ao titular. Os processos mais críticos para a LGPD dentro de uma empresa são aqueles processos que envolvem o tratamento significativo de dados pessoais e/ou dados pessoais sensíveis em departamentos como RH, *marketing* e jurídico. A título de exemplo, podem ser citados os processos: processos seletivos para candidatos a vagas de emprego; admissão de novos

colaboradores; adesão ao plano de previdência; e participação em grupos de diversidade e afinidade. Caso a organização deseje iniciar um “programa de diversidade” amplo envolvendo uso intenso de dados pessoais sensíveis, pode ser recomendável, objetivamente:

Recomendação objetiva	Detalhamento
Envolvimento multidisciplinar e criação de comitês	Envolver em tais atividades pelo menos os departamentos de recursos humanos e/ou pessoal, jurídico, encarregado e escritório de privacidade, segurança da informação e tecnologia da informação e membros da diretoria/ <i>board</i> , com suporte externo de consultores e especialistas, para que, no formato de um comitê de privacidade ou grupo de privacidade, sejam tomadas decisões alinhadas com o projeto de adequação à LGPD. É recomendável que tal grupo de privacidade elabore o questionário a ser endereçado na pesquisa pretendida, indique as finalidades específicas e explícitas do uso dos dados pessoais, escolha a base legal mais apropriada, defina limites ao acesso aos dados pessoais, bem como estabeleça recomendações gerais para outras ações afirmativas e intervenções em matéria de grupos sociais em condição de vulnerabilidade.
Documentação, responsabilização e prestação de contas	Documentar todas as ações e decisões do projeto, a fim de demonstrar o cumprimento dos princípios da LGPD e criar evidências, em especial, os princípios da finalidade, adequação, necessidade, transparência, segurança, prevenção, não discriminação, minimização, responsabilização e prestação de contas, e se resguardar contra eventuais demandas e/ou solicitações de direito dos titulares de dados.
Avaliação de risco	Iniciar, paralelamente, a confecção de avaliação preliminar de risco, que poderá resultar em relatório de impacto à proteção de dados (RIPD), caso sejam identificados riscos significativos para os titulares de dados, bem como riscos de exposição para a organização.

10 Considerações finais

Conforme se demonstrou neste estudo, entendemos ser possível a realização de mapeamento de levantamento de indicadores de diversidade, bem como a estruturação de outras ações afirmativas em formato de programas de diversidade que partam de investigações sobre o contexto de condições de vulnerabilidade de público interno de organizações. Reforçamos, contudo, que uma série de medidas devem ser adotadas a fim de respaldar as ações da organização, controladora de dados. A proteção dos dados sensíveis é especialmente relevante para a garantia dos direitos e liberdades fundamentais, devendo ser tutelados de forma mais específica e cuidadosa. Em razão da qualidade e da natureza das informações que trazem, seu uso indevido ou eventual vazamento pode gerar riscos significativos às pessoas envolvidas, podendo ser fonte para discriminações ilícitas ou abusivas em face do titular e de grupos – especialmente quando estamos falando de informações de grupos em condição de vulnerabilidade. Diante disso, deve-se

desenvolver o tratamento de dados sensíveis dentro de uma estrutura ampliada de proteção.

A depender do *timing*, estratégia e da concretude dos programas de responsabilidade corporativa, acreditamos que a organização deverá tomar tais decisões quando houver entendimento completo sobre o cenário das pesquisas, finalidades buscadas, metodologias empregadas, ou seja, um programa de diversidade e inclusão mais amplo. Além disso, considerando a provável amplitude das iniciativas afirmativas, pode ser recomendável contar com a participação de grupos diversos e multidisciplinares na própria concepção dos projetos, especialmente, partes interessadas dos departamentos de recursos humanos, jurídico, tecnologia e segurança da informação, escritório de privacidade e encarregado. Finalmente, sugere-se que sejam mapeados todos os riscos envolvidos, avaliações de impacto sejam realizadas desde o início e que as medidas adotadas sejam documentadas.

Diversity and inclusion programs and sensitive personal data protection: best practices for data processing in employment relations

Abstract: This study aims to examine the legality of organizations conducting surveys of diversity indicators within their internal workforce to structure and implement affirmative action policies through diversity and inclusion programs aimed at socially vulnerable groups. To achieve this, we reviewed national and international literature, facilitating a critical analysis of the theoretical issues involved. We begin by outlining the scope and typical activities of diversity and inclusion programs, along with the context in which these initiatives fit within corporate responsibility efforts both internationally and nationally. We then discuss the applicability of Brazil's General Data Protection Law (LGPD) to the processes of collecting personal data for mapping diversity indicators, including how this data is managed by internal teams and third parties, as well as the contentious exceptions to the law's applicability. In an effort to proactively contribute to this area of public interest, we propose a framework for transparency and consent collection that is aligned with the specific requirements of data protection laws, while considering the risks associated with invalidity of consent in employment contexts. Finally, we offer recommendations on best practices for carrying out these activities to minimize the risk of exposure for both data subjects and organizations. Recognizing that the protection of sensitive personal data is critically important for safeguarding fundamental rights and freedoms, this study particularly examines the privacy and data protection challenges involved in implementing diversity and inclusion programs that necessitate processing sensitive personal data.

Keywords: Diversity and Inclusion Programs. Sensitive Data. Personal Data Protection. Privacy. LGPD (Brazilian General Data Protection Law).

Summary: **1** Introduction – **2** What are diversity and inclusion programs: scope and common activities – **3** Diversity and inclusion programs in the international context to encourage the responsibility of organizations – **4** Legal context of diversity and inclusion programs – **5** Application of the LGPD to diversity and inclusion programs – **6** Anonymized data and the (controversial) non-application of the LGPD – **7** Legal framework in the LGPD for the processing of personal data collected in diversity and inclusion programs – **8** Declaration of collection and consent form for mapping diversity and inclusion indicators within the scope of labor relations – **9** Collecting personal data for diversity and inclusion programs: minimum transparency requirements – **10** Final considerations – References

Referências

- ARTICLE 29 WORKING PARTY. *Opinion 05/2014 on data anonymization techniques*. 2014. Disponível em: <https://www.pdpjournals.com/docs/88197.pdf>. Acesso em: 3 dez. 2025.
- ASSOCIAÇÃO NACIONAL DAS DEFENSORAS E DEFENSORES PÚBLICOS (ANADEP). *Regras de Brasília sobre acesso à justiça das pessoas em condição de vulnerabilidade*. Brasília, DF: ANADEP, 2008. Disponível em: <https://www.anadep.org.br/wtksite/100-Regras-de-Brasilia-versao-reduzida.pdf>. Acesso em: 3 dez. 2025.
- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo: aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) por agentes de tratamento no contexto eleitoral*. Brasília, DF: Tribunal Superior Eleitoral, 2021. Disponível em: <https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/guia-orientativo-aplicacao-da-lgpd.pdf>. Acesso em: 3 dez. 2025.
- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). *Guia orientativo: Hipóteses legais de tratamento de dados pessoais: legítimo interesse*. Brasília, DF: ANPD, 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 3 dez. 2025.
- BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, p. 59, 15 ago. 2018.
- BYGRAVE, Lee A. Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review*, Oslo, v. 4, n. 2, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3035164. Acesso em: 3 dez. 2025.
- CALLIESS, Gralf-Peter; ZUMBANSEN, Peer. *Rough Consensus and Running Code: a Theory of Transnational Private Law*. Oxford: Hart Publishing, 2010. p. 225-260.
- COMITÉ EUROPEU DE PROTEÇÃO DE DADOS (EDPB). *Guidelines 01/2025 on Pseudonymisation*. [S. l.], 2025. Disponível em: https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf. Acesso em: 3 dez. 2025.
- INSTITUTO ETHOS. *Perfil Social, Racial e de Gênero das 1.100 Maiores Empresas do Brasil e suas Ações Afirmativas 2023-2024*. São Paulo, 2024. Disponível em: <https://www.ethos.org.br/publicacao/perfil-social-racial-e-de-genero-das-1-100-maiores-empresas-do-brasil-e-suas-acoes-afirmativas-2023-2024/>. Acesso em: 3 dez. 2025.
- MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudononimização de dados. *Caderno Especial – A regulação da Criptografia no Direito Brasileiro*, [S. l.], p. 99-128, dez. 2018.
- MULHOLLAND, Caitlin S. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, [S. l.], v. 19, n. 3, p. 159-180, 2018. DOI: 10.18759/rdgv.19i3.1603.
- ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). *OECD Guidelines for Multinational Enterprises*. Paris: OECD, 2011. Disponível em: <https://oecd.org/daf/inv/mne/48004323.pdf>. Acesso em: 3 dez. 2025.
- ROBERT HALF. *Diversidade e Inclusão*. [S. l.], 2019. Disponível em: <https://www.roberthalf.com.br/sites/roberthalf.com.br/files/documents/robert-half-diversidade-inclusao-2019.pdf>. Acesso em: 3 dez. 2025.
- RUGGIE, John. *Guiding Principles on Business and Human Rights: Implementing the “United Nations “Protect, Respect and Remedy” Framework*. 2011. (A/HRC/17/31). Relatório do Representante Especial do Secretário-Geral sobre a questão de direitos humanos e corporações transnacionais e outras empresas de negócios. Disponível em: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G11/121/90/PDF/G1112190.pdf?OpenElement>. Acesso em: 3 dez. 2025.

SENDEN, Linda. Soft Law, Self-regulation and Co-Regulation in European Law: Where Do They Meet?. *Electronic Journal of Comparative Law*, [S. l.], v. 9, n. 27, 2005. Disponível em: <http://www.ejcl.org>. Acesso em: 3 dez. 2025.

SHAFFER, Gregory C.; POLLACK, Mark A. *Hard vs. Soft Law: Alternatives, Complements and Antagonists in International Governance*. University of Minnesota Law School, 2009. (Legal Studies Research Paper Series, n. 09-23).

TEFFÉ, Chiara Spadaccini de; VIOLA, Mário. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. *Civillistica.com*, Rio de Janeiro, v. 9, n. 1, p. 1-38, 2020.

UN GUIDING PRINCIPLES REPORTING FRAMEWORK. *View Disclosures*. [S. l.]: Shift, [2025]. Disponível em: <https://www.ungpreorting.org/database-analysis/explore-disclosures/>. Acesso em: 3 dez. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, Luxemburgo, L 119, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 12 dez. 2025.

UNITED NATIONS. Human Rights Council. *Resolution 17/4*. 2011. (A/HRC/RES/17/4). Disponível em: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/17/4. Acesso em: 3 dez. 2025.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

ARAUJO, Bernardo. Programas de diversidade e inclusão e proteção de dados pessoais sensíveis: boas práticas para o tratamento de dados nas relações de trabalho. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 19, n. 53, p. 395-425, jul./dez. 2025.

Submissão: 9.7.2025.

Pareceres: 13.10.2025, 17.10.2025.

Aceite para publicação: 20.10.2025.