CONSELHO NACIONAL DOS DIREITOS HUMANOS

RESOLUÇÃO Nº 17, DE 10 DE NOVEMBRO DE 2025

Dispõe sobre o uso de tecnologias de reconhecimento facial em espaços públicos dos estados e do Distrito Federal.

O CONSELHO NACIONAL DOS DIREITOS HUMANOS - CNDH, no uso das atribuições que lhe foram conferidas pelos art. 4º e art. 8º, §3º, da Lei nº 12.986, de 02 de junho de 2014, e dando cumprimeito à deliberação tomada, por unanimidade, em sua 93ª Reunião Ordinária, realizada nos dias 30 e 31 de outubro de 2025;

CONSIDERANDO que a República Federativa do Brasil tem, como um de seus fundamentos, a dignidade da pessoa humana, nos termos do art. 1º, III, da Constituição da República de 1988;

CONSIDERANDO que o art. 3º da Constituição da República de 1988 prevê que constituem objetivos fundamentais da República construir uma sociedade livre, justa e solidária (inciso I), garantir o desenvolvimento nacional (inciso II); erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais (inciso III); e promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação (inciso IV);

CONSIDERANDO, ainda, que o art. 5º, §2º, da mesma Constituição prescreve que os direitos e garantias nela expressos não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte;

CONSIDERANDO que o art. 5º da Constituição da República de 1988 define que todos os cidadãos brasileiros são iguais perante a lei, sem distinção de qualquer natureza;

CONSIDERANDO, ainda, que o art. 5º, inciso LXXIX da Constituição da República de 1988 garante o direito a todos os cidadãos brasileiros à proteção de seus dados pessoais e que o inciso X garante o direito à privacidade de todos os cidadãos;

CONSIDERANDO a Convenção Interamericana contra o Racismo, a Discriminação Racial e Formas Correlatas de Intolerância, recepcionada pelo Brasil em 2021, veta o uso de quaisquer mecanismos que discriminem direta ou indiretamente pessoas negras, sobretudo na gestão da segurança pública;

CONSIDERANDO o relatório “Surveillance and human rights” do relator especial para a promoção e proteção da liberdade de opinião e expressão do Conselho dos Direitos Humanos da Organização das Nações Unidas demanda uma moratória no uso e no desenvolvimento de ferramentas de vigilância, como o reconhecimento facial;

CONSIDERANDO o relatório “Racial discrimination and emerging digital technologies: a human rights analysis” da relatora especial em formas contemporâneas de racismo, discriminação racial, xenofobia e intolerância do Conselho dos Direitos Humanos da Organização das Nações Unidas defende que novas

tecnologias exarcebam e colaboram com formas existentes de desigualdades, muitas delas relacionadas a raça, etnia e origem nacional, produzindo discriminação direta e indireta.

CONSIDERANDO o relatório "On artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters" do Committee on Civil Liberties, Justice and Home Affairs do Parlamento Europeu que pede pelo banimento de tecnologias de reconhecimento facial em espaços públicos;

CONSIDERANDO o relatório "Brasil, Relatório de avaliação de prontidão para ética na Inteligência Artificial" da UNESCO que traz como recomendação número 10 a suspensão do uso de tecnologias como reconhecimento facial e policiamento preditivo até sua eficácia seja comprovada;

CONSIDERANDO o Objetivo de Desenvolvimento Sustentável (ODS) 16, promover sociedades pacíficas e inclusivas para o desenvolvimento sustentável, proporcionar o acesso à justiça para todos e construir instituições eficazes, responsáveis e inclusivas em todos os níveis;

CONSIDERANDO a Recomendação 49 da Revisão Periódica Universal (RPU) das Nações Unidas: "Continuar a implementar medidas destinadas a erradicar a discriminação das mulheres afro-brasileiras com base no seu gênero e etnia";

CONSIDERANDO a Recomendação 37 da Revisão Periódica Universal (RPU) das Nações Unidas: "Tomar medidas para eliminar casos de discriminação contra determinados grupos da sociedade.";

CONSIDERANDO a Recomendação 98 da Revisão Periódica Universal (RPU) das Nações Unidas: "Intensificar os esforços para abolir a prática do perfilamento racial (*racial profiling*) e a prisão arbitrária praticadas pela polícia e pelas forças de segurança";

CONSIDERANDO o artigo 19 da Declaração Internacional dos Direitos Humanos, adotada e proclamada pela Assembleia Geral das Nações Unidas em 10 de dezembro de 1948. Todo ser humano tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras;

CONSIDERANDO a prerrogativa de elaboração de atos normativos relacionados com a matéria de competência deste Conselho Nacional dos Direitos Humanos, nos termos do art. 4º, IX, da Lei nº 12.986/14;

CONSIDERANDO o disposto no art. 21, III, do Regimento Interno do Conselho Nacional dos Direitos Humanos;

CONSIDERANDO a ADPF 347, cuja sentença reconhece que existe um estado de coisas inconstitucional no sistema carcerário brasileiro;

CONSIDERANDO que o art. 4o, III e alíneas, e §1o, da lei 13.709/18, prevê que não se aplica a Lei Geral de Proteção de Dados a atividades com fins: segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais, e que nesses casos, o tratamento de dados listados anteriormente, serão feitos em lei específica;

CONSIDERANDO que diante da inexistência de lei específica que regulamente o tratamento de dados pessoais e dados pessoais sensíveis para fins de segurança pública, o Supremo Tribunal Federal, através do julgamento da Ação Direta de Inconstitucionalidade 6.649 e da Ação de Descumprimento de Preceito Fundamental 649, determinou que o tratamento de dados no setor público precisa seguir os requisitos da Lei Geral de Proteção de Dados, sendo então aplicáveis os princípios da proteção de dados, como o princípio da não discriminação (art.6°, inc IX);

CONSIDERANDO que em matéria de direito processual penal, a Constituição Federal em seu art. 5o, LVI são inadmissíveis provas ilícitas no processo penal. Na mesma linha segue o art. 156 do Código de Processo Penal;

CONSIDERANDO que a Lei no 12.288 de 2010 que institui o Estatuto da Igualdade Racial efetivando a igualdade de oportunidades, a defesa dos direitos étnicos individuais, coletivos e difusos e do acesso à justiça assegurando o direito as vítimas de discriminação étnica o acesso aos órgãos de Ouvidoria Permanente, à Defensoria Pública, ao Ministério Público e ao Poder Judiciário, em todas as suas

instâncias, para a garantia do cumprimento de seus direitos;

CONSIDERANDO o Art. 3º, § 5º, da RESOLUÇÃO nº 4, da Autoridade Nacional de Proteção de Dados, reiterado pelo item 7.5 da sanção do processo administrativo 00261.001969/2022-41 e pelo item 7.3 da sanção do processo administrativo 00261.001886/2022-51, afasta a incidência de multas simples e diárias sobre entes da Administração Pública, ademais, que a ausência de impacto financeiro direto decorrente da não aplicação de multas pode ser compreendida como um fator objetivo de aumento da tolerância a riscos e, consequentemente, de majoração do apetite de risco por parte da Administração Pública, criando um ambiente em que eventuais falhas de conformidade podem ser tratadas com menor rigor, ainda que gerem riscos significativos aos direitos fundamentais dos titulares de dados;

CONSIDERANDO que as imagens utilizadas no treinamento dos sistemas e na criação de bancos de dados de reconhecimento facial podem ter origem na coleta ou raspagem de dados de imagens (web scraping) realizada de forma ilegal ou abusiva, em desrespeito às normas de países como França, Itália e Grécia, conforme processos analisados pelo European Data Protection Board, respectivamente nos casos Clearview AI – CNIL França (Processo SAN-2022-019), Garante per la Protezione dei Dati Personali Itália (Processo 9751362) e Autoridade Helênica de Proteção de Dados Grécia (Processo 35/2022); ou ainda que podem ser fornecidas por empresas condenadas por tais práticas;

CONSIDERANDO que sistemas de reconhecimento facial, mediante intrusão ou uso inadequado, também poderão, direta ou indiretamente, rastrear e viabilizar atentados contra forças de segurança, inimigos políticos, jornalistas, dissidentes políticos e ativistas de direitos humanos, podendo levar a danos físicos e psicológicos a estes indivíduos;

CONSIDERANDO, ainda, que tais sistemas, conforme alertado pela Anistia Internacional, amplificam práticas de policiamento racista, como exemplificado durante as manifestações do *Black Lives Matter* aumentando a exposição desproporcional de grupos vulneráveis a abordagens discriminatórias e violações de direitos fundamentais;

CONSIDERANDO relatório produzido pela National Institute of Standards and Technology (NIST) demonstrando que 189 algoritmos de reconhecimento facial, produzidos por 99 desenvolvedores diferentes, falharam em identificar igualmente pessoas de diversas em termos de raça, nacionalidade, etnia e gênero. O relatório mostrou que alguns algoritmos são 100 vezes melhores em identificar rostos brancos do que de pessoas de outras raças, etnias e nacionalidades;

CONSIDERANDO que grandes empresas de tecnologia, como a I BM, Amazon e a Microsoft deixaram de investir em tecnologias de reconhecimento facial usadas por forças policiais;

CONSIDERANDO a pesquisa "Gender Shades" que analisou diversos algoritmos de reconhecimento facial e demonstrou que estes erram cerca de 34% mais com mulheres negras do que com homens brancos;

CONSIDERANDO os vieses discriminatórios de sistemas de reconhecimento facial e inteligência artificial documentados cientificamente, especialmente no que diz respeito ao tratamento de dados de pessoas negras, mulheres, pessoas trans e não binárias;

CONSIDERANDO estudos realizados pela Rede de Observatórios da Segurança em 2021, que monitorou os casos de prisões e abordagem com o uso de reconhecimento facial indicam que os casos em que havia informações, 90,5% das pessoas presas eram negras;

CONSIDERANDO as salvaguardas estabelecidas na Portaria MJSP nº 961, DE 24 DE JUNHO DE 2025, que estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública;

RESOLVE:

Art. 1º Esta Resolução dispõe sobre o uso de tecnologias de reconhecimento facial pelo Poder Público na União, nos estados, no Distrito Federal e nos municípios, nas situações relativas ao reconhecimento facial para fins de emprego imediato, excluindo-se o tratamento para emprego posterior ou do tipo pós-evento.

Art. 2º Para os fins desta Resolução, considera-se:

I. Reconhecimento facial: pesquisa automatizada de uma imagem facial em um banco de dados biométrico, resultando em uma lista de candidatos classificados por similaridade, a partir da avaliação de um algoritmo computacional;

II. Sistema de Reconhecimento Facial: qualquer software, serviço ou sistema que realize reconhecimento facial;

III. Reconhecimento Facial em Tempo Real: pesquisa automatizada de uma ou mais imagens faciais em um banco biométrico, a partir de capturas realizadas em tempo real, ou seja, identificando a imagem do rosto durante a filmagem e, na sequência, realizando a comparação em tempo real;

IV. Reconhecimento Facial Posterior: pesquisa automatizada de uma ou mais imagens faciais em um banco biométrico, a partir de capturas de imagens realizadas, para fins de subsidiar a produção de provas em investigações em curso;

V- Verificação Facial: execução de uma comparação rápida de imagem facial contra imagem facial ou imagem facial contra pessoa, normalmente com imagens controladas, realizada em aplicações de fluxo contínuo;

VI. Verificador Facial: servidor com treinamento técnico específico, responsável por executar a verificação facial;

VII. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais, conforme disposto na Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

Art.3º O desenvolvimento, a implementação e o uso de tecnologias de reconhecimento facial, em qualquer hipótese, deverão observar os seguintes princípios:

I. A boa-fé e os princípios de não discriminação;

II. Justiça, equidade e inclusão;

III. Proteção dos direitos e garantias fundamentais, incluindo o devido processo legal, contestabilidade e contraditório;

IV. Prevenção, precaução e mitigação de riscos e danos;

V. Não maleficência e proporcionalidade entre os métodos empregados e as finalidades determinadas e legítimas das tecnologias de reconhecimento facial;

VI. Governança transparente, participativa e orientada à proteção de direitos fundamentais individuais, sociais e coletivos;

VII. A responsabilização civil e criminal de autoridades e/ou agentes que comprovadamente malversem o uso dessa tecnologia;

VIII. Capacitação dos profissionais que atuarão no serviço de reconhecimento facial, com o objetivo de torná-los verificadores faciais;

IX. O treinamento adequado dos servidores responsáveis pela abordagem do indivíduo a ser reconhecido, em procedimentos de reconhecimento facial presencial ou remoto, assegurando sempre o respeito aos princípios da dignidade da pessoa humana;

X. A proibição de retrocesso em matéria de direitos humanos, de modo que a adoção de tecnologias de reconhecimento facial não reduza garantias já consolidadas no ordenamento jurídico nacional e em tratados e convenções internacionais das quais a República Federativa do Brasil seja signatária.

XI. A proibição da utilização de tecnologia de reconhecimento facial como prova única para a tomada de decisões que afetem direitos fundamentais, devendo ser sempre complementados por revisão pericial humana e outros meios de prova.

§ 1º Os dados biométricos faciais coletados deverão ser armazenados e tratados por procedimentos de segurança técnica e administrativa, em conformidade com a Lei Geral de Proteção de Dados, a fim de prevenir acessos não autorizados, vazamentos ou usos indevidos.

§ 2º Nos casos relacionados à utilização de tecnologias de reconhecimento facial para fins de persecução penal, a coleta e o tratamento de dados biométricos faciais deverão ser restritos às finalidades estritamente necessárias e proporcionais, com base em suspeita individualizada, evitando-se a vigilância massiva e indiscriminada.

Art. 4º Recomenda-se que, no âmbito das atividades de segurança pública, a utilização de tecnologias de reconhecimento facial em tempo real seja precedida pelas seguintes salvaguardas mínimas:

I. Demonstração científica de sua eficácia e de estudos que considerem os impactos negativos da inferência algorítmica;

II. Avaliação sobre a inexistência de vieses discriminatórios;

III. Avaliações dos impactos desta tecnologia;

IV. Justificativa formal por parte de autoridade policial ou de órgãos de inteligência, acompanhada de imagem de referência;

V. Registro detalhado e individualizado de cada operação, com acesso logado e auditável, apto à responsabilização funcional em caso de uso indevido;

VI. Garantia de que o uso da ferramenta, por si só, não embasará qualquer medida repressiva ou processual, devendo sempre ser tratado como subsídio auxiliar a outras fontes;

VII. Garantia de que a ferramenta será utilizada exclusivamente como meio de apoio investigativo sob comando humano direto, e jamais de forma autônoma.

VIII – Supervisão independente por órgãos de controle externo, como Ministério Público, Defensoria Pública e Ouvidorias de Polícia, com a participação da sociedade civil nos processos de monitoramento e avaliação; e

Parágrafo único. O disposto no caput deverá ser observado sempre que a Administração Pública se dispuser a:

I. Obter, adquirir, reter, vender, possuir, receber, solicitar, acessar, desenvolver, aprimorar ou utilizar tecnologias de reconhecimento facial em tempo real ou informações derivadas de uma tecnologia de reconhecimento facial em tempo real;

II. Celebrar contrato com terceiro com a finalidade ou objetivo de obter, adquirir, reter, vender, possuir, receber, solicitar, acessar, desenvolver, aprimorar ou utilizar tecnologias de reconhecimento facial em tempo real, informações derivadas de uma tecnologia de reconhecimento facial ou manter acesso à tecnologia de reconhecimento facial;

III. Celebrar contrato com terceiro que o auxilie no desenvolvimento, melhoria ou expansão das capacidades da tecnologia de reconhecimento facial em tempo real ou forneça ao terceiro acesso a informações que o auxiliem a fazer isso;

IV. Instruir pessoa jurídica de direito público ou privado a adquirir ou usar tecnologias de reconhecimento facial em tempo real em seu nome;

V. Permitir que pessoa jurídica de direito público ou privado use tecnologias de reconhecimento facial em tempo real em áreas urbanas, rurais ou mistas de sua circunscrição;

VI. Implantar ou operacionalizar tecnologias de reconhecimento facial em tempo real nos espaços públicos e privados da União, dos estados, Distrito Federal e municípios;

§1º Para avaliação científica da eficácia, sugere-se a adoção da norma ISO/IEC 19795 6:2012 – (Information technology – Biometric performance testing and reporting. Part 6: Testing methodologies for operational evaluation) e, como sugestão para avaliação de vieses discriminatórios, sugere-se a adoção da norma ISO/IEC 19795-10:2024 (Information technology – Biometric performance testing and reporting. Part 10: Quantifying biometric system performance variation across demographic groups).

§2º Recomenda-se ainda que tais testes sejam conduzidos ou validados por uma terceira parte independente, como, por exemplo, entidade de auditoria ou órgão técnico governamental, no lugar de se basear unicamente nas informações declaradas pelo fornecedor da tecnologia, conferindo-se maior

credibilidade.

Art. 5º Constatada a posse irregular ou o uso inadvertido de tecnologia de reconhecimento facial ou de informação dela derivada, em condições que comprometam sua segurança e confiabilidade, o ente público deverá:

I. Adotar imediatamente as medidas corretivas e, se for o caso, a suspensão temporária do uso;

II. Lavrar registro interno identificando a origem do material, as providências tomadas e as medidas de prevenção de reincidência;

III. Identificação do agente público que realizou mau uso da ferramenta, aplicando-se as medidas disciplinares cabíveis e necessárias;

IV. Notificação imediata da concessionária do serviço de reconhecimento facial, em caso de notável erro de software.

Art. 6º Deverá haver a disponibilização de uma versão pública do relatório de impacto à privacidade e do relatório de impacto algorítmico pelos entes da Administração Pública e entes privados, no prazo de 90 (noventa) dias, observadas as exigências do art. 5º.

§1º A implantação de novos sistemas de reconhecimento facial deve ser precedida de comunicação prévia à Autoridade Nacional de Proteção de Dados (ANPD), acompanhada de Relatório de Impacto à Proteção de Dados, nos termos do art. 38 da Lei nº 13.709/2018.

§2º Os relatórios de impacto à privacidade e impacto algorítmico conterão avaliação específica sobre populações historicamente vulnerabilizadas, incluindo pessoas negras, pessoas com deficiência, povos indígenas, mulheres, pessoas trans e não binárias, migrantes e populações em situação de rua dentre outros.

§3º Constatada discriminação sistêmica nesses relatórios, o uso da tecnologia deve ser suspenso até a completa correção do viés identificado.

Art. 7º Esta Resolução não se aplica ao dispositivo eletrônico pessoal, tais como telefone celular ou tablet, de propriedade do Estado, que realiza reconhecimento facial com o único propósito de autenticação do usuário pertencente a seu quadro de servidores.

Art. 8º O descumprimento desta Resolução poderá ensejar comunicação:

I. Ao Ministério Público, para as Promotorias ou Procuradorias de Justiça de Defesa dos Direitos Humanos, e outras competentes, para as medidas cíveis ou penais cabíveis;

II. À Autoridade Nacional de Proteção de Dados, quando houver tratamento de dados pessoais em desacordo com a LGPD;

III. Aos órgãos de controle interno e externo, para apuração de responsabilidade administrativa e reparação de danos;

IV. Aos órgãos competentes pelo uso da ferramenta, via requisição de informações ou outros meios possíveis, sobre o motivo do descumprimento, com fundamento na Lei de Acesso à Informação (LAI – Lei 12.527/2011).

§1º O uso indevido ou discriminatório de tecnologias de reconhecimento facial será objeto de apuração para fins de eventual responsabilização funcional, administrativa, civil e penal do agente público envolvido, bem como do ente federativo responsável pela implementação.

§2º A responsabilização incluirá medidas de reparação às vítimas de discriminação ou violação de direitos

Art. 10. Não se aplica o disposto nesta Resolução ao uso de tecnologias de reconhecimento facial:

§ 1º pela Polícia Federal em ambientes específicos e restritos, durante a execução de ações de segurança de autoridades em grandes eventos, desde que:

I. O uso seja justificado por razões de prevenção de riscos à integridade física de autoridades nacionais ou estrangeiras;

II. A coleta e o tratamento de dados pessoais tenham como finalidade exclusiva a comparação com bases de dados de pessoas condenadas, previamente autorizadas e mantidas por órgãos competentes;

III. Seja elaborado e disponibilizado relatório de impacto à privacidade e relatório de impacto algorítmico, conforme previsto no art. 6º desta Resolução;

IV. O uso da tecnologia esteja restrito ao período e ao local do evento, com controle de acesso e supervisão por autoridade competente

§ 2º em pesquisas científicas realizadas por institutos, centros de pesquisa ou universidades.

Art. 11º. Esta Resolução entra em vigor na data de sua publicação.

CHARLENE BORGES

Presidenta

Conselho Nacional dos Direitos Humanos – CNDH

Documento assinado eletronicamente por **Charlene da Silva Borges**, **Presidente**, em 11/11/2025, às 12:24, conforme horário oficial de Brasília, com fundamento no **§ 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020**.

A autenticidade deste documento pode ser conferida no site https://sei.mdh.gov.br/autenticidade, informando o código verificador **4957447** e o código CRC **734F398D**.

Setor Comercial Sul, Edifício Parque Cidade Corporate, Quadra 9, Lote C, Torre A, 9ª Andar, Asa Sul - Telefone: (61) 2027-3907
CEP 70308-200 Brasília/DF - https://www.gov.br/participamaisbrasil/cndh