BIOMETRIA FACIAL, ACESSO À SAÚDE E DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Nota técnica sobre o uso de dados biométricos em estabelecimentos de saúde suplementar

idec
Instituto Brasileiro de Defesa do Consumidor

BIOMETRIA FACIAL, ACESSO À SAÚDE E DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS

Nota técnica sobre o uso de dados biométricos em estabelecimentos de saúde suplementar[1]

Julho de 2023

SUMÁRIO

I. INTRODUÇÃO **2**
II. A PROTEÇÃO DE DADOS E A COLETA DE DADOS BIOMÉTRICOS **2**
III. O USO DA BIOMETRIA FACIAL NA SAÚDE SUPLEMENTAR **5**
IV. RISCOS RELACIONADOS AO USO DA BIOMETRIA PARA FINALIDADES SECUNDÁRIAS **7**
V. SUGESTÕES PARA O USO DE BIOMETRIA FACIAL NA VALIDAÇÃO DE IDENTIDADE DE USUÁRIOS DE PLANOS DE SAÚDE **8**
VI. CONSIDERAÇÕES FINAIS **10**

[1] A presente nota técnica foi produzida pela equipe de pesquisadores dos programas de saúde e telecomunicações e direitos digitais do Instituto Brasileiro de Defesa do Consumidor (Idec): Ana Carolina Navarrete, Camila Leite Contri, Luã Cruz, Matheus Falcão, Marina Fernandes e Marina Paullelli.

I. INTRODUÇÃO

1. O Idec (Instituto Brasileiro de Defesa do Consumidor) é uma organização da sociedade civil brasileira criada em 1986 com o objetivo de defender os direitos do consumidor - incluindo os direitos dos usuários de serviços públicos, a luta por relações econômicas justas e equilibradas, e a ampliação do acesso a bens e serviços essenciais. O Idec é uma associação de consumidores que atua em completa independência de governos, empresas e partidos políticos.

2. O Idec é composto por sete programas temáticos[2], dois dos quais envolvidos na produção desta Nota Técnica: os programas de saúde e de telecomunicações e direitos digitais. Juntos, eles compõem a interface de saúde digital[3], em um esforço para unir os debates sobre proteção de dados pessoais e direito à saúde.

3. É necessário reconhecer que a digitalização dos sistemas de saúde já é uma realidade. A saúde digital, entretanto, vive um impasse: por um lado, pode ser usada em prol da melhoria de vida das pessoas e em benefício do direito à saúde; ou, na contramão, pode aprofundar desigualdades de longo prazo enquanto cria preocupações adicionais relacionadas à vigilância e à proteção de dados pessoais.

4. No caso, tomando conhecimento de práticas no mercado e da discussão de definição de padrões e melhores práticas de Biometria Facial na Saúde Suplementar e com objetivo de contribuir com soluções que de fato sejam capazes de auxiliar em eventual regulamentação do tema, o Idec apresenta esta Nota Técnica, na qual expõe reflexões sobre os riscos relacionados ao tratamento de dados biométricos no setor de saúde suplementar à luz da proteção de dados pessoais e do direito do consumidor.

II. A PROTEÇÃO DE DADOS E A COLETA DE DADOS BIOMÉTRICOS

---

[2] Alimentação Saudável, Energia, Consumo Sustentável, Saúde, Telecomunicações e Direitos Digitais, Serviços Financeiros e Mobilidade.

[3] Na interface de saúde digital, o Idec também (i) questionou o uso de biometria e tratamento de dados em farmácias (https://idec.org.br/idec-na-imprensa/droga-raia-e-drogasil-desistem-de-pedir-biometria-para-liberar-descontos-0), (ii) questionou a proposta de open health anunciada em 2022 (https://idec.org.br/idec-na-imprensa/open-health-novas-tecnologias-velhas-ideias-e-muito-risco) e (iii) solicitou a abertura de inquérito para apuração de responsabilidades por vazamentos de dados no Ministério da saúde (https://idec.org.br/noticia/vazamentos-de-dados-de-saude-coloca-consumidor-em-risco-veja-o-que-fazer)

5. A utilização de biometria facial, dado pessoal sensível nos termos da Lei Geral de Proteção de Dados ("LGPD", Lei nº 13.709/2018), está relacionada ao tratamento de dados pessoais sensíveis em decorrência do uso de tecnologias de reconhecimento facial, digital, ou outro meio de reconhecimento a partir de identificação de características físicas que permitam a identificação de indivíduos para, por exemplo, controle de acesso a sistemas. Desde logo, se faz necessário apontar que, se mal utilizadas, tanto de forma deliberada quanto pela negligência em mitigar riscos, estas tecnologias podem servir como ferramentas de controle e resultar em práticas abusivas, discriminatórias e violadoras de privacidade[4].

6. Caso os dados biométricos coletados a partir dessa tecnologia não sejam tratados com o devido cuidado - por exemplo, se forem compartilhados com autoridades policiais e governamentais -, podem servir como ferramentas de vigilância. Inclusive, o Idec se posiciona pelo banimento do uso de tecnologias de reconhecimento facial na segurança pública e em locais públicos devido ao alto risco que o uso destas ferramentas pode ocasionar, especialmente em relação aos direitos à privacidade, proteção de dados, liberdade de reunião e de associação, igualdade, não-discriminação e liberdade de expressão.[5-6-7]

7. De maneira geral, entidades do mercado e prestadores de serviços privados têm utilizado cada vez mais a biometria facial para reconhecimento dos usuários de planos privados de saúde e prevenção à fraude. Entretanto, **por se tratarem de dados sensíveis com um alto potencial de risco aos usuários, o Idec se posiciona no sentido da não utilização, coleta e tratamento de dados biométricos, em especial pelo setor de saúde suplementar e sem a oferta de** alternativa para a identificação.

8. Em que pese a justa preocupação de todas as partes em relação ao combate às fraudes, cabe dizer que, em qualquer caso, a prática de coleta de dados sem informação clara quanto ao tratamento das informações pode violar direitos básicos do consumidor, a quem é garantido o direito à segurança, à liberdade de escolha e à

---

[4] SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. InternetLab/IDEC, São Paulo, 2020. Disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf

[5] Para mais informações da campanha #TireMeuRostoDaSuaMira, acesse: https://tiremeurostodasuamira.org.br/

[6] IDEC. Parlamentares de todas as regiões do Brasil apresentam projetos de lei pelo banimento do reconhecimento facial em espaços públicos. 20 jun. 2022. Disponível em: https://idec.org.br/release/parlamentares-de-todas-regioes-do-brasil-apresentam-projetos-de-lei-pelo-banimento-do.

[7] Carta aberta para banimento global de usos de reconhecimento facial e outros reconhecimentos biométricos remotos que permitam vigilância em massa, discriminatória e enviesada. Disponível em: https://www.accessnow.org/wp-content/uploads/2021/06/BanBS-Portuguese.pdf

informação adequada e clara sobre os serviços prestados, previstos no art. 6º, incisos I, II e III, do Código de Defesa do Consumidor ("CDC", Lei nº 8.078/90).

9. Ainda, a LGPD determina requisitos para o devido tratamento dos dados pessoais, impondo como seus princípios a adequação, necessidade e não discriminação, independentemente da base legal utilizada para o tratamento. Para tanto, a Lei impõe que qualquer processo de tratamento de dados pessoais seja proporcional, de acordo com as finalidades pretendidas, e norteado pela transparência e segurança a seus titulares.

10. É particularmente preocupante, para este instituto, a disseminação indiscriminada da coleta de dados biométricos, que exigem especial cautela em sua utilização. Tratam-se de dados pessoais sensíveis dos consumidores, em relação aos quais qualquer operação sujeita-se à necessidade de consentimento livre, informado, específico e destacado do titular ou justificado por outra base legal, nos termos da LGPD, de forma transparente ao consumidor. Frise-se, ainda, que o uso desse tipo de informações requer um exame detido de proporcionalidade, no qual devem ser considerados os riscos aos cidadãos - como o risco de vazamento de dados - em relação aos seus potenciais benefícios. Ou seja, havendo medidas de menor risco para os direitos de titulares de dados, essas devem ser tomadas.

11. A partir disso, cabe dizer que a prática da coleta de dados por meio de reconhecimento facial sem informação transparente e clara ao consumidor quanto ao seu tratamento, assim como sem base legal válida e informada, viola direitos fundamentais do cidadão, garantidos pelo artigo 5º, incisos X e LXXIX, da Constituição Federal, estes sendo a intimidade, a vida privada, a imagem e a proteção de dados pessoais. Também viola direitos expressos no CDC, como segurança (artigo 6º, inciso I), liberdade de escolha (artigo 6º, inciso II), acesso à informação adequada e clara sobre os serviços prestados pela loja (art. 6º, inciso III) e a informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais (Lei nº. 12.965/2014 - Marco Civil da Internet - art. 7º, inciso VIII).

12. Destaca-se que este Instituto, por meio de Ação Civil Pública (processo nº 1090663-42.2018.8.26.0100) ajuizada em face da ViaQuatro, responsável pela construção e manutenção da Linha 4 - Amarela do metrô de São Paulo, obteve decisão judicial favorável na primeira e segunda instância, com fixação de multa, contra a utilização de reconhecimento facial sem o expresso consentimento dos consumidores. Adotando posicionamento similar, em 2020, a Senacon (Secretaria Nacional do Consumidor) condenou a Hering por ter utilizado reconhecimento facial em sua loja no Shopping Morumbi, em São Paulo. O processo administrativo foi aberto após a Senacon ter

conhecimento da notificação do Idec, que solicitou à empresa esclarecimentos sobre a adoção da tecnologia.

13. Entretanto, reconhecendo que o uso da biometria facial já é uma realidade no Brasil[8], o Idec traz algumas considerações e sugestões para seu uso responsável, de forma que as pessoas consumidoras sejam efetivamente respeitadas.

III. O USO DA BIOMETRIA FACIAL NA SAÚDE SUPLEMENTAR

14. Inicialmente, é importante considerar que tanto dados pessoais de saúde quanto dados biométricos são dados pessoais sensíveis, sendo fundamental, portanto, que sejam tratados de acordo com a LGPD. Nessa categoria, que demanda maiores cuidados devido ao seu potencial discriminatório, o tratamento de dados deve ser amparado exclusivamente nas bases legais previstas no art. 11 da referida legislação. Neste sentido, é fundamental a priorização da base legal do **consentimento - que deve ser livre, expresso e informado dos titulares**. Em complemento, é essencial que os dados sejam utilizados exclusivamente para as **finalidades específicas e adequadas** ao tratamento.

15. No caso em questão, o consumidor deve consentir, de forma prévia, específica e destacada, com o tratamento de seus dados biométricos decorrentes de reconhecimento facial. Entretanto, o consumidor não pode ser forçado a se identificar exclusivamente por via de biometria facial, sendo **essencial que a operadora forneça alternativa** para identificação ou simplesmente se abstenha de exigir identificação facial.

16. Ressalta-se que o art. 11 também permite excepcionalmente outras bases legais para o tratamento de dados (caso não seja possível o fornecimento de consentimento, considerado prioritário para o tratamento de dados sensíveis). Dentre elas, quando o tratamento de dados for ***indispensável*** **à garantia de prevenção a fraudes e segurança do titular.** Entretanto, mesmo que se utilize esta base legal, é essencial que haja **alternativa à biometria facial**, especialmente considerando os altos riscos no tratamento de dados biométricos e a existência de maneiras menos gravosas de atingir o mesmo objetivo.

17. No caso de **crianças e adolescentes**, as hipóteses de tratamento de dados são ainda mais restritas, dada a necessária proteção absoluta deste grupo e em seu melhor interesse, conforme expressamente previsto tanto no Estatuto da Criança e do

[8] IDEC. Mães e pais do Norte e Nordeste do Brasil denunciam abusos da Hapvida. 03 fev. 2023. Disponível em: https://idec.org.br/noticia/maes-e-pais-do-norte-e-nordeste-do-brasil-denunciam-abusos-da-hapvida

Adolescente (ECA, Lei 8069/90), quanto no art. 14, § 1º da LGPD. Desta maneira, o **consentimento específico e em destaque dos pais e responsáveis (e, no caso de adolescentes entre 16 e 18 anos, cumulativamente ao seu próprio consentimento) é o mínimo essencial para o tratamento de crianças e adolescentes**. Ainda assim, considerando o princípio do melhor interesse, recomenda-se a não utilização de tecnologias de biometria facial a crianças e adolescentes. Afinal, no tratamento de seus dados pessoais a satisfação de seus direitos e melhor interesse deve ser absoluta, logo, **formas menos intrusivas de realizar a identificação pessoal devem ser privilegiadas**.[9]

18. Independentemente da base legal para o tratamento desses dados, qualquer finalidade de tratamento divergente daquela decorrente da base legal utilizada é completamente ilícita, mesmo quando não comprovado dano para o usuário, conforme os arts. 42 da LGPD e 14 do CDC. No mesmo sentido, ainda mais por se tratar de dados sensíveis, é de responsabilidade dos controladores de dados estabelecer **protocolos de segurança para mitigação dos riscos de incidentes e vazamento de dados**. Além disso, caso ocorram, devem ser empregados esforços para que os riscos para os afetados sejam mínimos, com protocolos de incidentes já estabelecidos e que incluam, entre outros aspectos, a comunicação aos titulares dos dados.

19. O tratamento de dados pessoais sensíveis apresenta riscos consideráveis, tais como riscos à privacidade, como os citados em relação a vazamentos e incidentes de segurança; discriminação e ameaças à proteção de grupos vulneráveis, como pessoas com deficiência, não-brancas, transgênero e/ou crianças e adolescentes. Assim, é certo que a **atividade de biometria facial implica, por sua natureza, risco para os direitos dos consumidores**, motivo pelo qual é inquestionável a aplicação da **responsabilidade objetiva e solidária** (art. 927 do CC, arts. 12 e 14 do CDC e art. 42 da LGPD).

IV. RISCOS RELACIONADOS AO USO DA BIOMETRIA PARA FINALIDADES SECUNDÁRIAS

[9] ASOCIACIÓN POR LOS DERECHOS CIVILES; ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA; INSTITUTO ALANA. Dados e direitos na infância e adolescência no ambiente digital: caminhos para a proteção jurídica no Brasil e Argentina. 2022. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2022/07/dados-e-direitos-na-infancia-e-adolescencia-no-ambiente-digital.pdf. Acesso em: 07 nov. 2022. Pág. 28.

20. O que se discute no presente momento é o uso da biometria facial para fins de identificação e reconhecimento dos usuários de planos privados de saúde. Ao mesmo tempo, não podemos deixar de considerar os riscos e a proibição da utilização destes dados sensíveis para outros fins (finalidades secundárias).

21. Ainda, levantam-se preocupações relacionadas ao uso indevido destes dados para **reconhecimentos de emoções[10-11] e até mesmo para discriminações, especialmente no atendimento automatizado** (como priorização de pessoas brancas no atendimento médico[12-13-14], ou óbices ao acesso de pessoas com deficiência a serviços de saúde[15]). Tratam-se de formas escusas de uso de dados e algoritmos, que podem resultar em danos irreversíveis aos consumidores, além de não estarem no escopo da finalidade do tratamento deste tipo de dado.

22. Para garantir que tais dados não sejam usados indevidamente, é fundamental fortalecer a fiscalização e a regulamentação, tanto pela Agência Nacional de Saúde Suplementar (ANS) quanto pela Autoridade Nacional de Proteção de Dados (ANPD). Os dados biométricos, inclusive, estão destacados na Agenda Regulatória 2023-2024 da ANPD. Entretanto, o setor da saúde ainda não tem regulamentação específica prevista por parte das autoridades competentes[16].

23. Por fim, a eficiência dos sistemas de reconhecimento facial é reconhecidamente baixa. Em geral, a ponderação é que os potenciais riscos não se sobrepõem a eventuais

---

[10] G1. Xiaomi apresenta robô humanoide que reconhece tristeza e 'consola'. Portal G1, ago. 2022. Disponível em: https://g1.globo.com/inovacao/noticia/2022/08/12/xiaomi-apresenta-robo-humanoide-que-reconhece-tristeza-e-consola.ghtml

[11] RHUE, Lauren. Emotion-reading tech fails the racial bias test. The Conversation, 3 jan. 2019. Disponível em: https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404 Acesso em: 06 fev. 2023.

[12] JOHNSON, Carolyn. Negros são discriminados por algoritmo médico nos EUA. Terra Uol, out. 2019. Disponível em: https://www.terra.com.br/byte/negros-sao-discriminados-por-algoritmo-medico-nos-eua,51f372103597d307cd0d11a7bc8cc8e2ru6c4yf0.html

[13] SIMONITE, Tom. How an Algorithm Blocked Kidney Transplants to Black Patients. Wired, 26 oct. 2020. Disponível em: https://www.wired.com/story/how-algorithm-blocked-kidney-transplants-black-patients/ Acesso em: 06 fev. 2023

[14] OBERMEYER, Z; POWERS, B; VOGELI, C; MULLAINATHAN, S. Dissecting racial bias in an algorithm used to manage the health of populations. Science, 2019. Disponível em: https://www.science.org/doi/10.1126/science.aax2342. Acesso em: 06 fev. 2023

[15] VASCONCELLOS, H. Plano Hapvida é notificado por exigir biometria de crianças com autismo. Uol, jan. 2023. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2023/01/25/hapvida-e-notificada-por-exigir-biometria-a-autistas-abusivo-diz-idec.htm

[16] Mais informações sobre a Agenda Regulatória 2023-2024 da ANPD disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-agenda-regulatoria-2023-2024.

benefícios decorrentes da utilização desses sistemas, especialmente frente à existência de outros meios menos gravosos de atingir os mesmos objetivos[17].

24. A opção prioritária deve ser sempre não utilizar a biometria facial. Entretanto, considerando que algumas operadoras de planos de saúde já se utilizam da biometria, o Idec gostaria de oferecer as seguintes sugestões para o uso de Biometria Facial na identificação de consumidores de planos privados de saúde em Prestadores e Operadoras.

V. SUGESTÕES PARA O USO DE BIOMETRIA FACIAL NA VALIDAÇÃO DE IDENTIDADE DE USUÁRIOS DE PLANOS DE SAÚDE

25. As sugestões indicadas são baseadas primordialmente no Guia para a Adoção de Boas Práticas de Reconhecimento Facial no Setor Privado, elaborado pelo próprio instituto em parceria com o centro independente de pesquisa interdisciplinar InternetLab[18].

- **Transparência**: É necessário garantir a transparência no tratamento de dados sensíveis através da prestação de informações completas e precisas aos titulares, especialmente sobre: a utilização de dispositivos de coleta de imagens; os dados coletados, sua forma de tratamento e as finalidades para as quais este é realizado; o prazo, as condições de armazenamento e as medidas de segurança adotadas para a sua proteção; as hipóteses de compartilhamento com terceiros; os direitos dos titulares sobre seus dados e os riscos envolvidos neste tratamento de dados.

- **Consentimento e inaplicabilidade da base legal do legítimo interesse**: Por se tratar de tratamento de dados sensíveis, a obtenção de consentimento é a base legal prioritária para esta forma de tratamento de dados pessoais. É imprescindível que titulares permaneçam podendo ter acesso ao produto, serviço ou funcionalidade ainda que não consintam com a captura dos dados de seu rosto. Especialmente por se tratar do acesso a serviços de saúde, é fundamental que as operadoras forneçam outros meios de identificação, como a apresentação de carteirinhas e documentos pessoais. Além disso, a obtenção do consentimento deve ocorrer antes do início da captura de imagens, que, portanto, dependerá de uma ação positiva do titular (como a sua concordância expressa por meio de um dispositivo disponível na entrada da

[17] Para mais informações, acesse: https://tiremeurostodasuamira.org.br/
[18] SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico; Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas. InternetLab/IDEC, São Paulo, 2020. Disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf

loja ou por meio de um código QR de ativação). Como a tecnologia envolve dados sensíveis, o tratamento não pode ocorrer com base no legítimo interesse.

- **Finalidade específica**: Os dados somente poderão ser tratados para os usos específicos informados qualificadamente aos titulares - a saber, estritamente para validação de identidade, quando demonstradamente necessário -, sem utilização para finalidades secundárias.

- **Alternativas à biometria facial**: a biometria facial não pode ser a única maneira para validar a identidade de pessoas. O Idec entende que o consentimento deve ser a base legal prioritária, mas ainda que a base legal utilizada seja de prevenção a fraudes, este objetivo pode ser atingido também por outras maneiras, que inclusive podem ser menos gravosas em relação a possíveis discriminações. Consideramos que o mais importante é garantir que a pessoa que está sendo alvo do tratamento de dados tenha sempre a opção de consentir ou não, sem que isso inviabilize o acesso ao serviço ou à obtenção do produto.

- **Medidas Antidiscriminatórias:** Em todos os momentos do desenvolvimento e uso desse tipo de sistema, especial atenção deve ser dada para que categorias como raça, gênero, etnia, orientação sexual, idade, estado e/ou condições de saúde e outras não sejam acionadas de forma discriminatória.

- **Exclusão, anonimização e proteção dos dados biométricos**: Uma vez coletadas as imagens e delas extraídas as características desejadas, as imagens devem ser permanentemente excluídas, de forma que não seja possível, nem pelos desenvolvedores do sistema, seu posterior resgate. Por fim, sem prejuízo do emprego de outras medidas de segurança, recomenda-se que todo armazenamento (temporário) de imagens de rostos se dê em ambientes seguros e criptografados, separados logicamente dos ambientes onde os dados anonimizados são armazenados. Idealmente, o armazenamento desses dados deve ser sempre offline, e qualquer conexão utilizada para acessá-los deve ser criptografada.

- **Crianças e adolescentes:** Em conformidade com a legislação brasileira, e buscando interpretá-la nos melhores interesses das crianças e adolescentes, o reconhecimento facial desse grupo não poderá ocorrer, exceto se consentido especificamente por seu responsável legal. No caso de adolescentes entre 16 e 18 anos, ainda, seu consentimento também deverá ser coletado. Além disso, a coleta deve ocorrer em seu melhor interesse, o que exclui a possibilidade de uso de seus dados em pesquisa de mercado, como direcionamento de publicidade ou inteligência de negócio.

- **Incidentes de segurança**: Por se tratar de atividade eminentemente sensível e de elevado risco social, todo e qualquer incidente de segurança deve ser investigado, informado imediatamente às autoridades públicas, à sociedade civil e aos titulares dos dados, especialmente se acarretar risco ou dano relevante.

VI. CONSIDERAÇÕES FINAIS

26. Conforme exposto nesta breve nota técnica, o uso de biometria facial pode gerar riscos irreparáveis aos consumidores, além de ser desnecessário, considerando que a identificação pode se dar por meios alternativos e já disponíveis para uso do mercado. Ao mesmo tempo, por se tratar de uma realidade no sistema suplementar de saúde, o Idec trouxe suas ponderações e sugestões de forma a colaborar para o debate e aprimorar a proteção de dados pessoais no âmbito da saúde, que possuem grande potencial danoso às pessoas consumidoras.