Parecer do Idec sobre o uso de dispositivos de reconhecimento facial em condomínios e estabelecimentos comerciais[1]

O Idec - Instituto Brasileiro de Defesa do Consumidor é uma associação de consumidores sem fins lucrativos, criada em julho de 1987 e mantida por seus associados. A missão do Idec é a defesa dos consumidores, na sua concepção mais ampla, representando-os nas relações jurídicas de qualquer espécie, promovendo a educação, a conscientização, a defesa dos direitos do consumidor e a ética nas relações de consumo, com total independência política e econômica.

Este breve parecer foi elaborado por especialistas do Idec para pessoas associadas a fim de corroborar com sua legítima reivindicação de direito à privacidade e ao uso de meios alternativos que resguardem seus dados pessoais sensíveis quando da imposição mandatória de reconhecimento facial para acesso a serviços e espaços.

O Idec atua nacionalmente representando consumidores e tem legitimidade reconhecida por autoridades do poder público. Em sua atuação nos temas de proteção de dados pessoais, o Idec mantém constante monitoramento de práticas de mercado que possam ferir direitos dos consumidores, especialmente no que tange ao aumento de sua vulnerabilidade.

Aqui, não se almeja tratar de políticas públicas de segurança que utilizam dispositivos de reconhecimento facial, mas proteger consumidores que têm seus rostos coletados e identificados sem o seu adequado consentimento e aprovação em condomínios, que utilizam a tecnologia como método de identificação para entrada.[2]

Definições

Consideram-se dispositivos de **reconhecimento facial** todo o tipo de tecnologia capaz de capturar o registro facial de indivíduos, de maneira automatizada, com o objetivo de identificar, verificar ou categorizar os titulares de dados/consumidores[3].

---

[1] Esse parecer aprofunda o disposto em "Câmeras em condomínios: o uso de reconhecimento facial e os direitos de consumidores", disponível em: https://idec.org.br/dicas-e-direitos/cameras-em-condominios-o-uso-de-reconhecimento-facial-e-os-direitos-de-consumidores

[2] Nesse sentido, o Idec recomenda o uso de seu Guia de Boas Práticas (2020) para o uso de reconhecimento facial no setor privado, disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf

[3] https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf

Biometria facial é o dado individual de cada pessoa representando seu rosto, capaz de identificá-lo individualmente.

Dado pessoal sensível é aquele dado pessoal que recebe proteção especial da lei em função do potencial danoso que possui para o indivíduo se for tratado de forma inadequada ou compartilhado com terceiros não autorizados.

Base legal é a aplicação da permissão legal da LGPD que ampara o tratamento de dados pessoais no caso concreto.

Consentimento é a permissão concedida pelo titular dos dados pessoais para o tratamento de seus dados, que deve ser feita de maneira expressa, informada e livre.

Pressupostos legais do uso dessa tecnologia

Com a Emenda Constitucional n.º 115 de 2022, o direito à proteção dos dados pessoais foi alçado como um direito fundamental no ordenamento jurídico brasileiro (Constituição Federal, Art. 5º, inciso LXXIX). Essa alteração segue a tendência de legislação protetiva aos direitos dos titulares de dados à privacidade e o estabelecimento de regras para uso de dados pessoais, como foi visto na Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Neste contexto, ressalta-se que a LGPD, em seu artigo 6º, estabelece que todo e qualquer tratamento de dados pessoais devem observar, dentre outros, os princípios de (i) finalidade, (ii) adequação, (iii) necessidade, (iv) transparência, (v) não discriminação, (vi) responsabilização e prestação de contas.

Em termos práticos, a coleta e o tratamento de dados pessoais devem ser precedidos por uma análise se este é o único meio de se atingir os fins desejados – no caso, a identificação do ingressante em determinado condomínio – e se é proporcional exigir este método na existência de outros meios que podem representar riscos significativamente menores aos titulares de dados pessoais. Vigora em nosso sistema de proteção de dados pessoais a garantia de tratamento do mínimo necessário de dados pessoais (princípio da necessidade) para se atingir uma finalidade, como forma de se mitigar riscos aos titulares. Além disso, deve ser capaz de comprová-lo, sendo transparente e prestando conta para titulares de dados pessoais, além de garantir seus direitos (Arts. 9 e 18), como a eliminação de dados.

Uso abusivo da biometria facial, nos termos da LGPD e do CDC

Feito todo este exercício, é essencial que o titular de dados seja adequadamente informado sobre o tratamento de seus dados pessoais e a finalidade do uso de seus dados, com garantias de transparência e segurança. O indivíduo deve ser capaz de exercer seus direitos

de titular de dados, como previsto nos artigos 9 e 18 da **LGPD**. Somente atendidas estas condições é possível fazer um regular tratamento de dados pessoais.

No caso de tecnologias de reconhecimento facial, deve-se ressaltar que se trata de um dado biométrico e que, conforme estabelecido no artigo 5º, II da LGPD, possui garantias especiais por se tratar de um dado pessoal sensível. No artigo 11, a LGPD dispõe as condições para o tratamento de dados pessoais sensíveis, sendo necessário enquadrar esse tratamento em uma base legal.

O Idec entende que a melhor prática para o atendimento do padrão legal da LGPD é que esse tratamento só poderia ocorrer mediante o **consentimento** livre, informado e inequívoco do titular de dados - ou seja, de cada um dos condôminos. Além disso, que o tratamento seja condicionado a forma e finalidades específicas.

O afastamento do consentimento enquanto base legal para tratamento de dados pessoais sensíveis é restrito, já que é a base legal prioritária para o tratamento de dados pessoais sensíveis (Art. 11, inciso I). Porém, frequentemente se utiliza a garantia de prevenção à fraude como uma dispensa do consentimento para o uso de biometria facial, pelo disposto no artigo 11, II, inciso "g" da LGPD. Entretanto, esse inciso dispõe que a base legal de prevenção à fraude somente pode ser utilizada quando "resguardados os direitos mencionados no art. 9º (direito dos titulares) e **exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais"** (grifo nosso). Considerando que o reconhecimento facial é reconhecidamente falho e traz diversos problemas relativos à discriminação, a condicionante de equilíbrio com direitos e liberdades fundamentais não está presente na prática.

Se os dados biométricos armazenados no contexto dessa tecnologia não forem cuidados com o devido zelo, ou se forem compartilhados com autoridades policiais e governamentais, por exemplo, podem servir de base também a ferramentas de vigilância. Estão em questão, portanto, riscos potenciais a direitos fundamentais, entre eles o direito à **proteção de dados pessoais**.

Outra fonte de risco diz respeito ao "viés algorítmico", i.e., a reprodução de padrões discriminatórios nos resultados apresentados ou no uso feito pelos algoritmos. Por exemplo, no caso de uma ferramenta de reconhecimento facial treinada com referência a um banco de dados constituído majoritariamente por pessoas de pele branca, sua acurácia será reduzida quando usada para identificar pessoas de pele negra, gerando resultados discriminatórios e situações que podem acarretar a violações de honra e privacidade dos indivíduos. Estudos vêm mostrando que a taxa de erro dessas ferramentas é sistematicamente maior para mulheres negras em comparação a outros grupos, por exemplo[4]. A discriminação por

[4] https://ieeexplore.ieee.org/document/6327355; Buolamwini e Gebru conduziram um estudo que analisou três ferramentas de reconhecimento facial disponíveis no mercado que detectam o gênero do indivíduo. A pesquisa testou a acurácia desse sistema e concluiu que as taxas de erro das três

algoritmos pode levar a práticas discriminatórias (negação de serviços, distinção de preços), tecnologias essenciais que não funcionam bem com toda a população (autenticação facial de pessoas negras, por exemplo), e outros potenciais problemas.

Desta maneira, o Idec entende que a base legal prioritária para esse caso deve ser o consentimento e entende ser menos recomendável a utilização da base legal de prevenção a fraudes, quando do tratamento de dados pessoais sensíveis. De qualquer maneira, independentemente da base legal, é necessário o respeito aos princípios de finalidade, adequação e necessidade.

Ademais, justamente pelos problemas relativos à (falta de) eficácia dessa tecnologia e pelas sérias preocupações relativas à discriminação, o Idec recomenda que haja sempre uma medida alternativa para identificação. Em especial, que essa alternativa não utilize dados biométricos (incluindo digitais).

É evidente que há outros métodos de identificação que são eficazmente utilizados há décadas em condomínios, que apresentam um menor risco ao usuário. O titular de dados que não deseja ter seu rosto capturado por tecnologia sem as adequadas informações sobre como se dará a classificação, utilização e armazenamento de sua biometria e se as informações serão compartilhadas com terceiros deve ter seu direito à privacidade resguardado. São raríssimas as experiências e os relatos de consumidores que foram adequadamente informados antes da coleta de sua biometria facial por essas tecnologias.

Ainda que sejam oferecidas todas as informações disponíveis e elas estejam adequadamente, a obrigatoriedade de fornecimento de biometria facial para que um titular adentre sua residência ou em prédio comercial configura uma prática abusiva e um abuso de direito, à luz do **Código de Defesa do Consumido**r (art. 39, I e VI, CDC), por limitar o acesso de indivíduos quando há outros meios para identificação com coletas de dados que não apresentam tamanho risco ao titular. Ademais, por ser um tema relacionado à segurança do serviço prestado (Art. 4º, Art. 6º e Art. 8º e seguintes).

Deve-se possibilitar o exercício de métodos alternativos de identificação aos usuários que assim desejarem, como apresentação de documento caso não haja armazenamento de dados pessoais ou o fornecimento de chave, sensor ou código ou de biometria por impressão digital, evitando a coleta de um dado pessoal tão sensível como o rosto dos titulares.

Embora seja amplamente justificado como mecanismo de segurança, não há estudos que comprovem a eficácia da biometria facial em face de outros métodos, já que está sujeita aos mesmos riscos de uma chave ou da impressão digital – ocorrer a coação da entrada por criminosos, utilizando o titular de refém - pois os demais métodos também evitam a entrada fraudulenta de indivíduos.

---

ferramentas são significativamente maiores em mulheres negras quando comparadas a homens brancos.

Objetivamente, não há um efetivo ganho na segurança do condomínio e de seus titulares pelo uso dessa tecnologia, em contrapartida à coleta de dados sensíveis e que podem incorrer em graves danos à vida e privacidade dos usuários em caso de vazamentos, compartilhamento ou uso não autorizado dessas informações.

Ainda que o método se apresente seguro à primeira vista, vigora em nosso sistema de proteção de dados o princípio de minimização da coleta de dados e de mitigação de riscos ao titular, de forma que devem ser apresentados métodos alternativos de identificação ao usuário, que possui o direito de oposição e de proteção da sua privacidade.

Conclusão

Desta maneira, tendo em vista disposições da LGPD, do CDC e da Constituição Federal, o Idec recomenda que sejam evitadas implementações de sistemas de acesso biométrico para identificação de condôminos ou para acesso a estabelecimentos. Entretanto, caso seja implementado, a recomendação é que haja uma alternativa menos invasiva para os direitos de consumidores.

Igor Rodrigues Britto
Diretor de Relações Institucionais

Luã Fergus Oliveira da Cruz
Coordenador do Programa de Direitos Digitais

Camila Leite Contri
Coordenadora do Programa de Direitos Digitais
OAB/SP [redacted]

Lucas Martho Marcon
Advogado
OAB/SP [redacted]

Marina Fernandes de Siqueira
Pesquisadora em Direitos Digitais