Dados Biométricos no Setor Financeiro e de Pagamentos

Zetta VLK ADV

Sumário

Mensagem do Presidente da Zetta e do VLK Advogados

A transformação digital do setor financeiro brasileiro é uma realidade consolidada, que tem impulsionado a inclusão, a inovação e a conveniência para milhões de pessoas. Nesse cenário de rápida evolução, a tecnologia biométrica surge como uma ferramenta indispensável, reforçando a segurança e a integridade de um ecossistema cada vez mais dinâmico. Contudo, o avanço tecnológico deve, necessariamente, caminhar lado a lado com a responsabilidade e a proteção dos dados pessoais.

É com grande satisfação que nós, da Zetta, em parceria com o VLK Advogados, apresentamos a "Cartilha de Boas Práticas para o Tratamento de Dados Biométricos no Setor Financeiro e de Pagamentos". Esta iniciativa reflete nosso compromisso com um ambiente de negócios competitivo, ético e, acima de tudo, seguro para o consumidor.

O expressivo aumento das tentativas de fraude no Brasil, que geram prejuízos bilionários e afetam a confiança no sistema, exige de nós uma postura proativa e colaborativa. A biometria, quando utilizada de forma correta, é uma das mais eficazes barreiras contra ações fraudulentas, protegendo o patrimônio e a identidade dos cidadãos em operações críticas como a abertura de contas, a contratação de crédito e o acesso a benefícios sociais.

Contudo, a potência dessa tecnologia demanda uma governança robusta. O tratamento de dados biométricos, por sua natureza sensível, convoca-nos a um patamar elevado de cuidado, transparência e conformidade. É neste ponto que a autorregulação setorial se revela um pilar estratégico. A Lei Geral de Proteção de Dados (LGPD), em seu artigo 50, não apenas incentiva, mas valoriza a criação de códigos de conduta e boas práticas como um mecanismo de demonstração de boa-fé e conformidade.

Esta cartilha materializa esse princípio. Ela não é apenas um guia, mas um convite à ação coletiva. Por meio dela, buscamos estabelecer um denominador comum de excelência para o setor, traduzindo as exigências da LGPD e das regulações financeiras em diretrizes práticas e eficazes. Queremos fomentar um diálogo construtivo com reguladores, legisladores e a sociedade, demonstrando que é possível inovar de forma responsável e sustentável.

Ao oferecermos clareza sobre a correta caracterização dos dados biométricos, as bases legais aplicáveis — com especial destaque para a prevenção à fraude —, e as salvaguardas técnicas e administrativas indispensáveis, estamos fortalecendo todo o ecossistema. Nosso objetivo é claro: garantir que a tecnologia sirva ao seu propósito primordial de proteção, sem abrir mão dos direitos fundamentais à privacidade e à não discriminação.

Temos a convicção de que este documento será um instrumento de referência valioso para empresas, profissionais e autoridades, contribuindo para a construção de um setor financeiro digital cada vez mais seguro, confiável e inclusivo para todos os brasileiros.

Eduardo Lopes (Presidente da Zetta) e VLK Advogados

Apresentação

A Cartilha traz explicações sobre dados brutos e processados, tecnologias tradicionais e emergentes, e o uso legítimo de biometria para autenticação, prevenção de fraudes e proteção dos indivíduos, na qualidade de titulares dos dados. Além disso, fornece subsídios para a adoção de políticas e processos alinhados à legislação vigente e às melhores práticas do setor.

Esta Cartilha serve como instrumento de referência para orientação e disseminação de conhecimento, enriquecendo o debate informado e a implementação de práticas seguras e responsáveis.

Sobre a Zetta

A Zetta é uma associação sem fins lucrativos que representa empresas de tecnologia que vêm liderando a transformação digital do setor financeiro. Trabalhamos por um ambiente econômico competitivo que resulte em maior inclusão financeira, inovação e satisfação para as pessoas. Nossa missão é dar visibilidade às ideias do setor a reguladores, legisladores e outros atores envolvidos no processo de formulação, implementação e avaliação de políticas públicas.

Sobre o VLK Advogados

O VLK é uma boutique de Direito Digital, Proteção de Dados, Cibersegurança, Inteligência Artificial e Legal Marketing, movida por entregas que fazem a diferença.

No VLK, o Direito não é barreira. É impulso para inovar, para viabilizar negócios e para construir uma sociedade mais próspera e justa, conciliando: risco e oportunidade; complexidade e clareza; e proteção e progresso.

Participamos ativamente da construção de marcos regulatórios e atuamos em inúmeros projetos inovadores e estratégicos, o que nos permite antecipar tendências e gerar segurança jurídica.

1. Conceitos e Princípios

1.1 Como caracterizar um dado biométrico?

Dados biométricos são aqueles que, ao mesmo tempo, atendam os seguintes critérios[1]:

- Estar vinculado a características físicas, fisiológicas, comportamentais ou traços de personalidade de um titular de dados;
- Resultem de tratamento técnico específico (em regra, uma forma de medição); e
- Tenha como finalidade a identificação ou autenticação única do titular.

Fotos, vídeos e gravações de voz, por si só, não são dados biométricos. Eles só passam a ser considerados biométricos quando processados tecnicamente com o objetivo de identificar alguém, de forma única.

O European Data Protection Board (EDPB) reforça esse entendimento, ao declarar que imagens em vídeo não são biometria, se não forem tratados para identificação específica de um indivíduo. A definição do EDPB distingue **dados brutos com potencial biométrico de dados biométricos efetivos**, garantindo segurança jurídica e evitando que o regime de dados sensíveis se aplique a situações de risco menor.

Vejamos alguns exemplos práticos:

- Instituição financeira que armazena a foto do rosto de um cliente para simples cadastro não está tratando dado biométrico,
- Por outro lado, se essa imagem for submetida a algoritmo de reconhecimento facial para autenticar o usuário no login de forma única (com extração e comparação de padrões únicos com vetores faciais), aí sim ocorre o tratamento biométrico nos termos do art. 5º, II da LGPD.

Portanto, o elemento central não é a natureza do dado (como uma foto), mas o **tratamento aplicado com a finalidade de identificação unívoca ou autenticação biométrica**. Essa distinção preserva a proporcionalidade regulatória e evita impactos desnecessários em operações de baixo risco.

[1] Para conceituar dado biométrico nos apoiamos nos entendimentos da Autoridade de Proteção de Dados do México (“INAI”), do Comitê Europeu de Proteção de Dados (“EDPB”) e do art. 16, ter da Lei de Proteção de Dados Chilena.

Na prática, imagine que uma instituição financeira use sistema de reconhecimento facial para validar a identidade de clientes. Nesse processo, são extraídas características biométricas únicas do titular (como a distância entre os olhos e formato do maxilar) [2] e comparadas à selfie tirada na hora. Ao aplicar o entendimento do EDPB, os dados biométricos seriam esses pontos específicos extraídos, não as fotos em si. Portanto, se houver vazamento apenas da imagem do cliente, a exposição será de dado pessoal (fotografia), e não de dado sensível biométrico.

No mercado financeiro, a biometria facial serve para autenticação e prevenção a fraudes, mas o tratamento técnico desses dados ocorre de duas formas distintas:

1. **Desbloqueio do aplicativo:** o dispositivo do titular realiza a autenticação (ex.: Face ID ou Touch ID). O tratamento dos dados ocorre no aparelho e o aplicativo apenas recebe resposta binária (verdadeiro ou falso). A instituição não acessa a imagem ou biometria do cliente.

2. **Verificação de identidade e prevenção à fraude:** em situações como cadastro inicial e atualizações, ativação de novos aparelhos ou suspeita de fraude, a instituição processa a imagem do rosto do titular para confirmar a identidade de forma segura.

1.2 Transparência no tratamento de dados biométricos

A Autoridade de Proteção de Dados do Reino Unido (ICO) considera os seguintes **fatores de transparência eficiente sobre uso de dados biométricos:**[3]

- O caso de uso;
- A natureza de relacionamento com o titular;
- Os dados envolvidos na atividade de tratamento.

Quanto mais transparente for o tratamento de dados para o titular, considerando práticas comuns do setor e a relação prévia com ele, menor é a necessidade de medidas adicionais de transparência.

[2] https://blog.zapsign.com.br/en/reconhecimento-facial/

[3] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/

Quando o reconhecimento biométrico é usado para confirmar a identidade do titular em transações (acesso a conta, solicitações de crédito ou *chargebacks*), o tratamento é realizado dentro de ambiente autenticado e sob relacionamento ostensivo como o titular, em regra de acordo com as exigências do Banco Central do Brasil, como as previstas na Resolução CMN nº 4.893/21, que já impõem controles de segurança e mecanismos robustos de autenticação. **Essa prática é exigida pelo regulador e esperada pelos usuários.** Nesses casos, é suficiente indicar a Política de Privacidade ao longo da jornada do cliente ou prestar explicações sobre o tratamento, quando solicitadas (na tela do dispositivo utilizado, por exemplo).

1.3 Biometria comportamental e biometria tradicional: comparações, obrigações e cuidados

A legislação atual não diferencia biometria comportamental e tradicional e, como consequência, não estabelece obrigações distintas para cada uma delas. Assim, eventuais normas infralegais não podem criar novas exigências, sob pena de violar o princípio da legalidade. Por exemplo, embora outras autoridades, como o INAI[4][5]e o ICO[6], distingam dados biométricos físicos/fisiológicos e biométricos comportamentais, nenhuma delas impõem deveres específicos ou diferenciados de acordo com essa classificação.

No setor financeiro, regulamentos como a Resolução Conjunta nº 6/23 e a Resolução CMN nº 4.893/21 **reforçam a necessidade de mecanismos robustos de prevenção à fraude, baseados em dados íntegros, relevantes e completos**. Isso vale para qualquer tipo de dado biométrico utilizado como fator de autenticação ou detecção de risco, desde que sejam observadas as regras de governança e uso legítimo das informações, atendendo a propósitos específicos e informados, e com salvaguardas de auditoria e performance dos modelos.

Estudos do Grupo de Trabalho do Artigo 29 (WP29) e da Autoridade de Proteção de Dados de Singapura (PDPC) apontam que a **biometria comportamental aumenta a detecção de fraudes e a agilidade em disputas financeiras, reforçando sua utilidade prática.**

[4] https://blog.zapsign.com.br/en/reconhecimento-facial/

[5] https://blog.zapsign.com.br/en/reconhecimento-facial/

[6] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/biometric-recognition/

2. Hipóteses (Bases) Legais

2.1 Consentimento e suas limitações para o uso de dados biométricos

O consentimento não é, e não deve ser, a única base legal para o tratamento de dados biométricos, especialmente no setor financeiro, em que prevalecem a segurança e integridade do sistema financeiro nacional.

Além disso, **casos de recusa do titular em consentir com o tratamento de dados biométricos podem justificar a restrição a determinadas funcionalidades**. Nas instituições financeiras que permitem a confirmação de transações por biometria ou senha, a recusa do consentimento pode, legitimamente, resultar na indisponibilidade da funcionalidade biométrica ao titular, estando disponíveis apenas os serviços acessíveis por senha[7].

Nos casos em que o tratamento não se baseia no consentimento, a recusa deve ser tratada como exercício legítimo do direito de oposição. A negativa será lícita apenas quando:

For tecnicamente impossível oferecer a funcionalidade sem biometria; ou

Houver interesse legítimo da organização que prevaleça sobre o direito do titular, como a proteção de um bem relevante[8].

Quando o consentimento for a base legal aplicável ao tratamento de dados biométricos, o controlador deve observar os requisitos da LGPD para a coleta de manifestação válida. Nos negócios digitais, isso se dá por meio da apresentação clara das informações sobre a finalidade do tratamento, a existência da coleta e uso dos dados biométricos e a disponibilização de checkbox de opt-in. Além disso, um botão “saiba mais” pode direcionar o titular a segunda camada de informações, contendo, por exemplo, a política de privacidade e o termo de consentimento específico.

[7] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-lawfully/

[8] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/

2.2 Prevenção à fraude como hipótese legal

A hipótese do art. 11, II, "g" da LGPD **(uso de dados para prevenção à fraude e segurança) é fundamental na legitimação do uso de dados biométricos para autenticação e validação de identidade e para subsidiar tarefas de prevenção, resposta e investigação de incidentes de fraude.** É o caso, por exemplo de:

- Abertura de contas;
- Recuperação de acesso ou de senha;
- Acesso e visualização de informações financeiras sensíveis;
- Autorização de transações financeiras relevantes ao contexto do titular;
- Atualizações cadastrais;
- Autenticação em canais de atendimento;
- Operações de prevenção, resposta e investigação de fraudes em si (elaboração de relatórios, cooperação técnica, acompanhamento de casos);
- Autenticação em processos de contestação comercial e recuperação de crédito;
- Dentre outras situações.

Já o art. 11, II, "a", da LGPD autoriza o tratamento de dados biométricos quando indispensável ao cumprimento de obrigação legal ou regulatória pelo controlador, mantidas as obrigações de transparência e garantindo ao titular o pleno exercício dos seus direitos.

No âmbito do Sistema Financeiro Nacional, as autoridades supervisoras impõem às instituições reguladas a adoção de medidas adequadas para assegurar a segurança de suas operações, **incluindo requisitos de segurança da informação e cibernética, bem como a validação efetiva da identidade de seus clientes e a autenticidade e legitimidade de suas transações**, englobando processos de KYC e AML/CFT (conhecer clientes e prevenção à lavagem de dinheiro e financiamento ao terrorismo).

O problema das fraudes no Brasil reforça a necessidade dos referidos mecanismos robustos de segurança, sendo o uso de dados biométricos forma legítima de alcançar a redução de golpes proporcional ao benefício gerado. Alguns números relevantes:

- 51% dos brasileiros já foram vítimas de fraude (Serasa Experian);
- Prejuízo médio por golpe: US$ 1.032,00 (cerca de R$5.500,00) (TransUnion); e
- Em 2025, já houve mais de 2,8 milhões de tentativas de fraude, com impacto potencial superior a R$ 40 bilhões (DataSenado).

A biometria, nesse contexto, é proporcional e necessária, pois é mais eficaz do que senhas ou tokens, reduzindo vulnerabilidades, em casos como phishing, engenharia social e vazamento de dados. Isso é especialmente relevante, considerando a baixa maturidade da população brasileira em geral no uso de mecanismos tecnológicos mais complexos.

A jurisprudência também reforça essa obrigação: o Superior Tribunal de Justiça (STJ) já decidiu que instituições financeiras devem **adotar mecanismos eficazes, utilizando dados pessoais, para evitar transações fora do perfil do cliente** (REsp 2.052.228/DF).

A base legal de garantia da prevenção à fraude e da segurança do titular será legítima quando seguir os seguintes critérios:

Finalidade específica	limitada às atividades necessárias para alcançar a finalidade;
Proporcionalidade	os benefícios devem ser proporcionais aos riscos;
Segurança	adoção de medidas técnicas e administrativas contra riscos de exposição interna, vazamentos etc.; e
Transparência	mesmo sem consentimento, o titular deve receber informações claras sobre o uso dos dados e os canais para exercício de direitos básicos de privacidade.

A elaboração de **Relatório de Impacto à Proteção de Dados (RIPD) pode ser desejável em casos setoriais**, registrando a proporcionalidade e necessidade do uso dos dados, os riscos e medidas de mitigação.

Ainda, para mitigar os riscos de tratamento dos dados biométricos, é sugerida a adoção de salvaguardas técnicas e organizacionais já reconhecidas por autoridades como o ICO[9], o INAI[10] e a PIPC[11], **as quais podem ser agrupadas em dois conjuntos:**

[9] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure

[10] https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pd

[11] https://www.pipc.go.kr/eng/user/lgp/law/ordinancesList.do#none

Prioritárias	**(i)** controles mais rígidos de acesso; **(ii)** testes de invasão (pentests) periódicos; **(iii)** política robusta de segurança da informação; **(iv)** criptografia dos dados biométricos, em trânsito e armazenados; **(v)** varredura de vulnerabilidades e correções; **(vi)** registro de logs das interações e acessos aos dados biométricos; **(vii)** armazenamento segregado dos dados biométricos das outras informações pessoais; e **(viii)** due diligence em fornecedores.
Complementares	**(i)** o armazenamento apenas do template biométrico (vetores matemáticos), e não da impressão digital; e **(ii)** a adoção dos controles previstos em normas internacionais relevantes, como ISO/IEC 24745:2022.

2.3 Cumprimento de obrigação legal ou regulatória, mitigação de riscos e direito dos titulares

No contexto do sistema financeiro nacional, **há leis e normas infralegais que fundamentam o tratamento de dados biométricos**, em linha com o art. 11, II, "a", da LGPD. De forma geral, tais normas têm como finalidade a prevenção à fraude, a segurança das transações e identificação inequívoca do titular.

Para que o tratamento de dados biométricos seja legítimo nesses casos, devem ser observados três critérios principais:

- existência de obrigação legal ou regulatória específica que torne indispensável o uso desses dados, proporcionalmente ao risco a ser mitigado;
- adequação, de modo que o uso da biometria seja justificado pelo grau de sensibilidade e criticidade da operação, não havendo alternativa menos intrusiva com eficácia equivalente; e
- finalidade, restringindo o tratamento aos objetivos da obrigação legal ou regulatória, como nos processos de prevenção à lavagem de dinheiro, autenticação de identidade e segurança cibernética, abrangendo também o atendimento de ordens judiciais.

A norma que dá suporte ao tratamento deve indicar de forma clara a necessidade de identificação ou autenticação robusta, ou a adoção de medidas de segurança compatíveis com o risco, ainda que não utilize expressamente o termo "biometria".

Seguem exemplos de leis e regulações que exigem a identificação e manutenção de registro de clientes compatíveis com o risco, endereçando também aspectos de segurança da informação e prevenção a fraudes:

- Lei nº 9.613/1998 (prevenção à lavagem de dinheiro);
- Lei nº 12.865/2013 (medidas de segurança para usuários);
- Circular BCB nº 3.978/2020 (PLD/CFT);
- Resolução CMN nº 4.893/2021 (Política de Segurança Cibernética);
- Resolução Conjunta nº 1/2020 (Open Finance);
- Resolução Conjunta nº 6/2023 (abertura e manutenção de contas);
- Resolução BCB nº 142/2021 (prevenção de fraudes);
- IN nº 138/2022 (biometria no empréstimo consignado).

As mesmas salvaguardas aplicáveis no contexto da hipótese legal de prevenção à fraude (art. 11, II, "g", LGPD) são também válidas nesta situação. Isso porque as medidas técnicas e organizacionais devem ser proporcionais à natureza dos dados e aos riscos associados ao seu tratamento, independentemente da base legal utilizada. Tal entendimento é compatível com a orientação do ICO[12], que não diferencia medidas de segurança conforme a base legal adotada, mas a partir da natureza, sensibilidade dos dados e do impacto potencial sobre os titulares.

3. Tecnologias de Reconhecimento Facial (FRTs) e Tecnologias Emergentes

3.1 Princípios aplicáveis ao uso do reconhecimento facial na proteção contra discriminação

Conforme visto, a tecnologia de reconhecimento facial é ferramenta importante no setor financeiro, não como instrumento de vigilância, mas para **segurança, conformidade regulatória e inclusão financeira.**

Para garantir que o uso dessa tecnologia esteja em linha com a LGPD, devem ser observados os seguintes princípios:

Transparência ativa e contextual no setor financeiro

O princípio da transparência, como visto anteriormente, deve ser **aplicado de forma contextual**. Há diferença entre o uso de biometria em espaços públicos, nos quais o titular não tem expectativa de tratamento desse tipo e o seu uso em processos de contratação de serviços financeiros.

[12] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure

Nas **plataformas digitais, o tratamento biométrico é esperado e comunicado ao usuário** quando ele abrir uma conta, contratar produtos ou autorizar transações. Nesse cenário, a **biometria é percebida como camada de proteção** para os próprios recursos do cliente.

Assim, a transparência é atendida com a apresentação de **Avisos de Privacidade claros, objetivos e acessíveis** durante a jornada do usuário, preferencialmente no momento do cadastro ou antes da coleta biométrica.

Necessidade e proporcionalidade no contexto financeiro

O princípio da necessidade deve ser avaliado à **luz da mitigação de riscos de segurança, prevenção de fraudes e cumprimento de obrigações regulatórias.**

A biometria facial combinada a mecanismos de prova de vida é hoje o meio mais eficaz e proporcional para garantir, de forma remota e escalável, a identidade do usuário, diante do volume de fraudes e considerando a regulação do Banco Central. Em algumas situações, pode ser necessário manter tanto a fotografia original quanto o template biométrico, uma vez que a foto compõe o conjunto probatório relevante para prevenção e combate a fraudes, investigações e litígios. A guarda dessas informações de acordo com prazos prescricionais também é necessária para o exercício regular de direitos em processos judiciais, administrativos e arbitrais.

Quanto à minimização e finalidade, o setor privilegia sistemas de verificação 1:1, em que o dado fornecido é comparado ao *template* previamente cadastrado pelo titular. Métodos de identificação 1:N, voltados a descobrir a identidade do titular a partir de uma base não são prática comum.

Além disso, a biometria facial é usada exclusivamente para identificação e autenticação, sem inferência de outros dados sensíveis (como religião ou condições de saúde, por exemplo).

Mitigação de vieses discriminatórios

No desenvolvimento interno de soluções ou contratação de tecnologia externa, recomenda-se seguir orientações como as do ICO[13][14]: **(i)** assegurar no treinamento bases de dados diversas, especialmente em termos de etnia e gênero; **(ii)** realizar testes para identificar vieses discriminatórios; **(iii)** usar ferramentas de análise de métricas e estrutura da IA; **(iv)** testar acurácia estatística; e **(v)** implementar processos de correção de erros.

Além disso, o uso de biometria em serviços não essenciais exige atenção para evitar práticas discriminatórias, especialmente em relação a acessibilidade de pessoas com deficiência visual, que podem encontrar barreiras para utilizar soluções biométricas.

[13] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination

[14] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-process-biometric-data-fairly/

Para lidar com isso, as organizações devem avaliar esses riscos e adotar medidas que reduzam obstáculos. Quando houver confirmação da deficiência, pode ser necessário oferecer, em caráter excepcional, métodos alternativos de autenticação, ainda que com menor nível de proteção.

3.2 Alta eficácia e confiabilidade dos sistemas

As medidas destinadas a assegurar eficácia e confiabilidade dos sistemas de reconhecimento facial devem ser proporcionais aos riscos associados ao seu uso. Por isso, as recomendações a seguir devem ser vistas como boas práticas a serem avaliadas conforme o risco do sistema, e não como obrigações universais.

Nessa linha, para sistemas de reconhecimento facial que usam inteligência artificial, aplicam-se a eles as recomendações de boas práticas trazidas no Guia de IA e Proteção de Dados do ICO[15] e na sua matriz de riscos[16]. Em síntese, sugerimos considerar os seguintes controles:

Planejamento	Definir, já na concepção da solução, o nível mínimo de acurácia estatística necessário.
Seleção e coleta de dados	Assegurar que os dados de treinamento sejam representativos, completos, precisos e rotulados, de acordo com o público-alvo da solução, além de avaliar e mitigar riscos de sobreajuste (*overfitting*) e subajuste (*underfitting*).
Testes e validação	Realizar testes documentados para: **(i)** verificar a acurácia estatística da solução de forma geral e em relação a grupos relevantes, garantindo o cumprimento do nível mínimo definido; **(ii)** identificar problemas de sobreajuste (overfitting) e subajuste (underfitting); e **(iii)** aplicar correções, como retreinamento ou ajuste de parâmetros, quando necessário.
Implantação e monitoramento	**(i)** disponibilizar aos usuários mecanismos para questionar resultados; **(ii)** adotar monitoramento contínuo ou testes periódicos para assegurar a manutenção da acurácia estatística; e **(iii)** manter cópias das versões anteriores de modelos que continuam aprendendo após o lançamento, possibilitando retorno a versões estáveis em caso de degradação de desempenho.

[15] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-ensure-our-processing-of-biometric-data-is-transparent/

[16] https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fico.org.uk%2Fmedia2%2Fkr3mveig%2Fai_and_data_protection_risk_toolkit_v11.xlsx&wdOrigin=BROWSELINK

3.3 Quando o reconhecimento facial não é recomendado?

O **reconhecimento facial não deve ser utilizado quando houver métodos adequados e proporcionais para alcançar o mesmo resultado sem recorrer à biometria**. Ou seja, sempre que existirem alternativas significativamente menos invasivas que garantam nível equivalente de eficácia diante dos riscos envolvidos, essa tecnologia deve ser evitada.

Alguns contextos em que o uso **não é recomendado:**

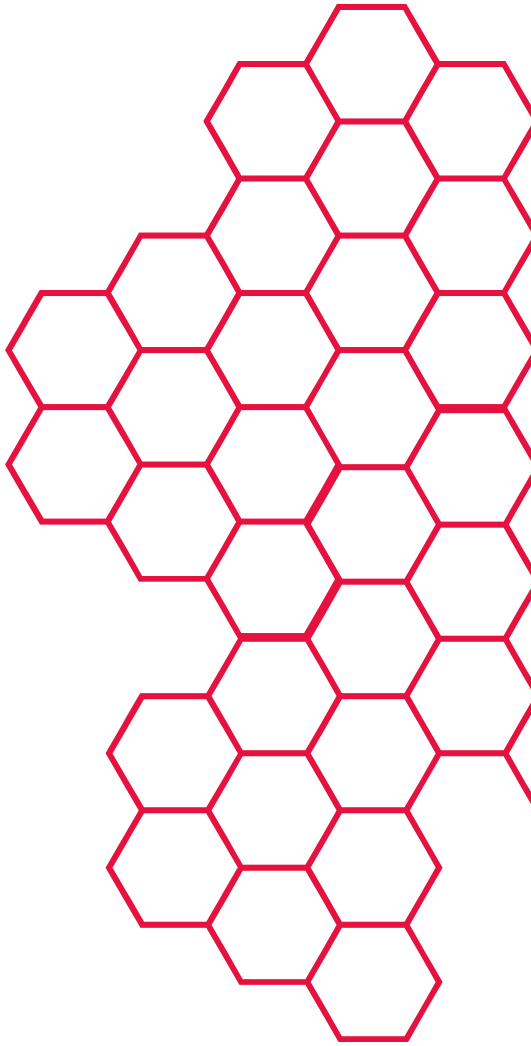
- **Controle de presença/ausência em escolas:** pode gerar monitoramento excessivo e afetar o direito à educação;
- **Locais públicos sem justificativa clara:** risco de vigilância em massa, com exceções de segurança pública;
- **Processos seletivos e contratações:** análise de expressões faciais pode reforçar vieses algorítmicos e comprometer a justiça do processo;
- **Eventos políticos ou manifestações:** possibilidade de identificação e perseguição de manifestantes.

Como alternativas à biometria facial, a PIPC[17], em seu Guia sobre Dados Biométricos, apresenta exemplos de soluções eficazes:

- Verificar se telefone e informações de contato correspondem a registros das operadoras;
- Confirmar se a localização da transação coincide com a do dispositivo do titular;
- Identificar fraudes, como a troca ilegítima de chip (SIM swap).

A Anatel[18] ressalta que essas informações já são utilizadas por instituições financeiras para prevenir fraudes, permitindo a adoção de medidas preventivas em movimentações financeiras relacionadas a trocas de chip.

Em resumo, para que alternativas ao reconhecimento facial sejam realmente viáveis, é essencial que a **ANPD incentive a criação de ambiente regulatório que fomente pesquisa, inovação e adoção de soluções seguras. Sem essa regulamentação, organizações tendem a recorrer de forma excessiva à biometria facial**, mesmo em situações de risco desproporcional.



[17] https://www.pipc.go.kr/eng/user/lgp/law/ordinancesList.do#none

[18] https://www.gov.br/anatel/pt-br/assuntos/dicas-contra-fraudes/golpes-atuais-mais-comuns

4. Segurança, Governança e Boas Práticas

4.1 Medidas indispensáveis de segurança e parâmetros mínimos de avaliação de riscos

Dado o impacto significativo de violações de dados biométricos, algumas medidas de segurança devem ser tratadas como indispensáveis. Com base nas orientações da ICO, INAI e PIPC, destacam-se:

- controle rigoroso de acesso aos dados;
- realização periódica de testes de penetração;
- implementação de políticas robustas de segurança da informação;
- criptografia dos dados durante a transmissão e armazenamento;
- varreduras regulares de vulnerabilidades, com correções adequadas;
- registro em logs de todos os acessos e interações;
- segregação dos dados biométricos em relação a outros dados pessoais; e
- due diligence, em caso de contratação de terceiros.

A ISO/IEC 27005:2023[19] fornece parâmetros gerais sobre mensuração e monitoramento dos riscos de segurança, os quais também são aplicáveis à biometria facial:

a) Definição de critérios de risco: estabelecer as regras e os parâmetros para aceitação de riscos, alinhados ao apetite de risco da organização;

b) Identificação dos riscos: identificação dos ativos, das ameaças, controles existentes e vulnerabilidades. Entre as ameaças específicas à biometria facial, o Guia do NCSC[20] do Reino Unido apresenta estas:

- ataques de apresentação (uso de artefatos, como fotografias, para falsificar a validação de identidade);
- interceptação dos resultados dos sensores (visa modificar ou interceptar ;
- subversão da integridade da inscrição;
- ataques a bancos de dados;

[19] https://www.normas.com.br

[20] https://www.ncsc.gov.uk/collection/biometrics

- Ameaças internas;
- Ataques à infraestrutura de TI; e
- Ataques de negação de serviço.

c) Análise de riscos: avaliação de consequências e probabilidade de ocorrência;

d) Tomada de decisão: definir se o risco será mitigado, aceito, compartilhado ou evitado, com plano de ação específico quando necessário;

e) Monitoramento contínuo: ajuste constante frente a novas ameaças e mudanças de contexto.

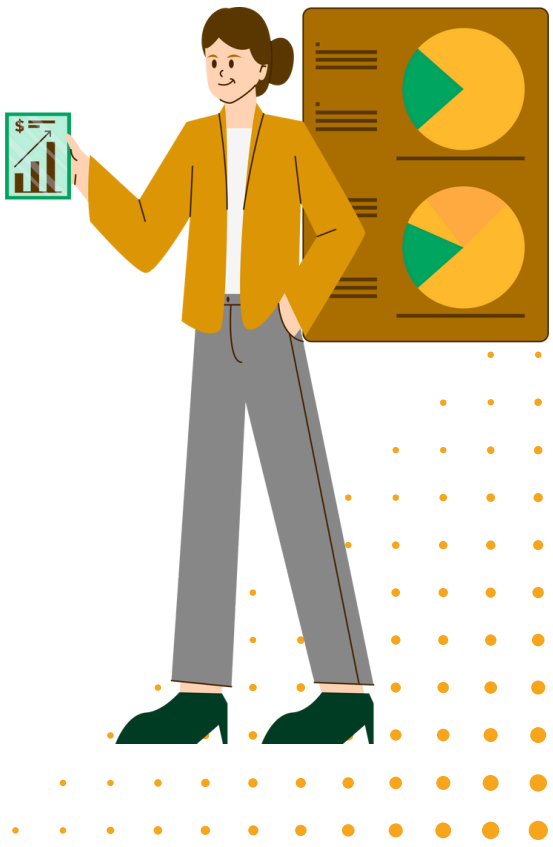
4.2 Como garantir a autodeterminação informativa em tratamentos massivos de dados biométricos

Em contextos de **tratamento contínuo e em larga escala** de dados biométricos, como em **cidades inteligentes, monitoramento de estádios e outros espaços públicos**, os controladores precisam **adotar medidas específicas** para respeitar a autodeterminação informativa dos titulares.

Quanto ao direito à informação, quando os titulares não esperam que seus dados biométricos sejam coletados, especialmente em situações sem vínculo prévio com o controlador, é necessário esforço adicional para garantir transparência.

Para atender a essa exigência, algumas medidas concretas podem ser adotadas:

- **Sinalizações visíveis nos locais de coleta**, contendo informações básicas sobre o tratamento;
- **Indicação de canais** pelos quais os titulares podem acessar informações completas e **exercer seus direitos**; e
- **Utilização de QR Codes** em estruturas fixas, como paredes, painéis ou telas, que direcionem para o **Aviso de Privacidade da organização**, contendo todas as informações exigidas pela legislação.]



Quanto à orientação da ANPD, a Agência Nacional de Proteção de Dados já analisou situação semelhante e considerou adequadas essas medidas de prestação de informações, conforme Nota Técnica nº 29/2024/FIS/CGF/ANPD (§ 6.1.4).[21]

[21] https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/nota-tecnica-29_2024.pdf

5. Direitos dos Titulares e Grupos Vulneráveis

5.1 Direitos dos titulares em tratamento automatizado de dados biométricos

Em contextos de tratamento automatizado de dados biométricos, os agentes de tratamento devem assegurar que os titulares possam exercer seus direitos de forma adequada. Seguem particularidades relacionadas a cada um desses direitos.

Direito de acesso

O ICO[22] reconhece que existem limitações técnicas para fornecer diretamente dados biométricos, pois eles normalmente se apresentam como representações matemáticas complexas e não inteligíveis para o titular. Essas representações, os *templates*, não possuem valor informativo direto e, se fornecidas, poderiam expor o sistema a riscos de engenharia reversa ou outros vetores de ataque.

Para que haja transparência significativa sem comprometimento da segurança, o controlador deve fornecer:

- A confirmação da existência do tratamento e a finalidade específica;
- O tipo de dado biométrico tratado;
- A fonte dos dados, informando que o *template* foi gerado a partir da foto (“selfie”) ou imagem fornecida pelo titular durante o cadastro;
- A possibilidade de acesso à amostra original que deu origem ao *template*, caso ainda esteja armazenada pelo controlador; e
- Outras informações vinculadas ao processo, como data e hora das últimas autenticações bem-sucedidas ou falhas, e o identificador da conta associado (como CPF).

Direito à correção

O ICO[23] pontua que o direito à correção não se aplica ao resultado estatístico de uma comparação biométrica, que é baseado em cálculo de probabilidade. No entanto, ele é aplicável quando:

- Há erro na associação, como quando a biometria de um indivíduo foi vinculada ao CPF de outra pessoa;

[22] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/

[23] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-consider-rights-requests-for-biometric-data/

- Existe necessidade de atualização, por mudanças físicas relevantes no titular (como envelhecimento ou acidentes), degradando a qualidade da autenticação. Para garantir o acesso contínuo e seguro do cliente, as plataformas devem oferecer fluxo de recadastramento biométrico, permitindo que o *template* antigo seja descartado e substituído por um novo e mais acurado[24].

Nesses casos, as plataformas devem oferecer fluxo de recadastramento biométrico, permitindo descartar o template antigo e substituí-lo por um novo e mais preciso.

Direito à revogação do consentimento

Esse direito deve ser ponderado com as demais bases legais que legitimam o tratamento de dados no setor financeiro, como cumprimento de obrigação legal ou regulatória e prevenção à fraude. O uso da base legal do consentimento é residual nesse setor, mas, quando aplicável, a revogação deve permitir a inutilização ou exclusão do *template* biométrico, impedindo seu uso em futuras autenticações.

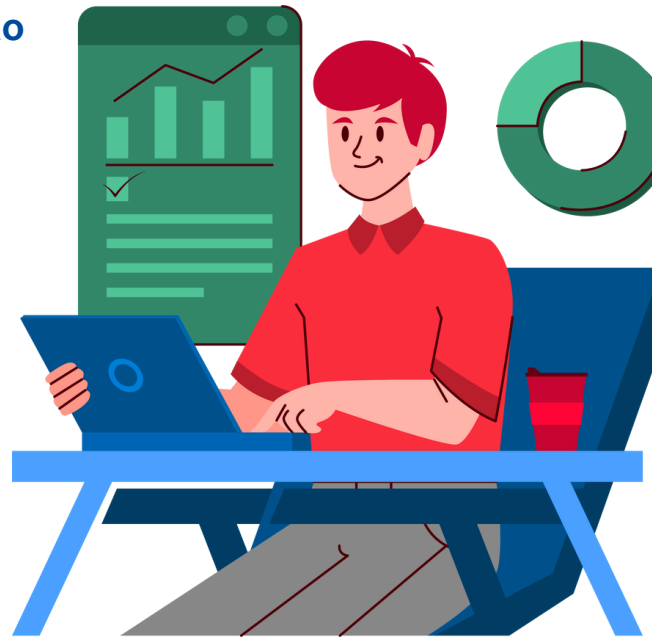
A revogação não elimina automaticamente os registros históricos de validações biométricas. Instituições financeiras e de pagamento devem manter registros, de acordo com obrigações do BCB, CVM e outros supervisores do Sistema Financeiro Nacional, incluindo legislações de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo. Esses registros são essenciais para:

- Auditorias regulatórias e de segurança;
- Investigações de fraudes e disputas de transações; e
- Comprovação do cumprimento de deveres perante órgãos reguladores.

A revogação, nesses casos, cancela o uso futuro da biometria, mas os registros históricos devem ser mantidos pelo período exigido pela regulamentação setorial aplicável.

5.2 Critérios para verificação ou estimação de idade em plataformas digitais

A escolha de mecanismos de verificação de idade por meio de dados biométricos deve considerar três fatores principais: o contexto em que a verificação ocorre; nível de precisão da tecnologia adotada; e a disponibilidade de alternativas menos invasivas que alcancem o mesmo resultado.



[24] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/biometric-data-guidance-biometric-recognition/how-do-we-keep-biometric-data-secure

Contexto de verificação

A definição do método mais adequado depende da finalidade e criticidade do serviço prestado. O princípio da necessidade deve ser entendido não apenas como limitação ao menor volume de dados, mas como uso dos dados essenciais para finalidades legítimas.

É preciso ponderar cuidadosamente a privacidade com outras obrigações, como a proteção do melhor interesse da criança ou adolescente. Em alguns casos, a coleta de um dado específico pode ser a medida mais adequada para proteger esse grupo vulnerável. Conforme orientações do ICO, a técnica utilizada para confirmar a idade deve ser proporcional aos riscos oferecidos pelo serviço e pelo tratamento de dados aos menores de idade.

> **Exemplo:** uma plataforma de serviço financeiro digital pode usar biometria facial combinada com verificação de documento de identidade digital para confirmar idade e titularidade. A verificação do documento confirma a identidade registrada e a biometria reforça que quem está usando o dispositivo ou serviço é realmente o titular, prevenindo fraudes.

Acurácia da tecnologia

O grau de confiabilidade e precisão da tecnologia adotada devem ser considerados, pois tecnologias que estimam idade por biometria frequentemente apresentam margem de erro significativa[25]e[26]. Métodos que combinam verificação documental e confirmação visual costumam ser mais eficazes.

Soluções alternativas menos invasivas

É necessário avaliar se existem métodos menos intrusivos capazes de atingir nível de acurácia semelhante ou minimamente satisfatório, considerando o risco de acesso indevido de menores. Exemplos de alternativas incluem[27] e[28]:

- Declaração direta da idade pelo usuário, fornecendo data de nascimento ou autodeclaração;
- Confirmação via cartão de crédito, com cobrança simbólica (R$ 0,01) para verificar titularidade e idade;
- Análise de comportamento digital, inferindo idade a partir do padrão de uso e conteúdos acessados;
- Verificação presencial de documentos oficiais antes de conceder acesso; e
- Obtenção de consentimento do responsável legal, desde que sua identidade e autoridade possam ser confirmadas de forma confiável.

[25] https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

[26] https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf

[27] https://www.cnil.fr/en/online-age-verification-balancing-privacy-and-protection-minors

[28] https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/739350/EPRS_ATA(2023)739350_EN.pdf

6. Considerações Finais

O tratamento de dados biométricos é realidade consolidada, regulada e necessária para prevenção a fraudes, sobretudo no setor financeiro e em serviços digitais. A LGPD e normas setoriais estabelecem parâmetros claros para sua utilização, reconhecendo sua natureza sensível e exigindo salvaguardas de segurança, proporcionalidade e transparência.

Em síntese, o uso de dados biométricos traz **benefícios em termos de segurança e inclusão financeira**, mas deve ser constantemente equilibrado com a **proteção da privacidade e das liberdades individuais.**

O futuro do uso de biometria no Brasil dependerá da **capacidade de equilibrar inovação e proteção de dados**, assegurando que cada avanço tecnológico esteja alinhado com os valores democráticos de privacidade, dignidade e não discriminação.

Coordenação

Daniel Stivelberg
Rony Vainzof
Caio Lima

Colaboradores

Amanda Coelho
Ana Soares
Caio Reinhardt
Gisele Karassawa
Isabela Garcia de Souza
Jean Santana
Luciana Sabino
Luiza Rocha
Mirella Miranda
Raíssa Moura
Renato Anholon
Ricardo Oliva
Samanta Oliveira
Sofia Chang
Sofia Franco

Zetta

VLK ADV

@somoszetta /somoszetta somoszetta.com.br

@vlkadvogados /vlk-advogados vlklaw.com.br