

AUTENTICAÇÃO FACIAL E RECONHECIMENTO FACIAL

Distinções Técnicas, Finalidade do Tratamento e Proporcionalidade na LGPD

Wendel de Oliveira Babilon

Escritor, Auditor e Encarregado de Proteção de Dados (DPO),

Sumário: Introdução: O erro técnico no debate sobre biometria no Brasil; Natureza do dado sensível versus natureza do tratamento; Classificação jurídica da biometria na LGPD; Autenticação facial (1:1); Estrutura técnica e enquadramento jurídico; Reconhecimento facial (1:N); identificação em massa e impacto coletivo; Princípio da proporcionalidade como critério decisório; Segurança real versus sensação de segurança; Expansão biométrica no Brasil: dados empíricos e percepção social; Setor público versus setor privado: limites constitucionais; RIPD como instrumento de controle constitucional do tratamento; Deepfake, fraude sintética e o novo cenário de risco digital; Tabela de balanceamento: critérios comparativos entre 1:1 e 1:N; Conclusão: O tratamento define a legitimidade; Referências

RESUMO: O presente capítulo examina as distinções técnicas e jurídicas entre autenticação facial (1:1) e reconhecimento facial (1:N), à luz da Constituição Federal e da Lei Geral de Proteção de Dados Pessoais. Parte-se da premissa de que o debate nacional tem concentrado atenção excessiva na natureza sensível do dado biométrico, negligenciando a centralidade do tratamento efetivamente realizado. Sustenta-se que a legitimidade do uso da biometria facial depende do contexto operacional, da finalidade específica, da necessidade demonstrada e da aplicação estruturada do princípio da proporcionalidade. Analisa-se ainda o impacto da expansão biométrica no Brasil, a distinção entre segurança real e sensação de segurança e o papel do Relatório de Impacto à Proteção de Dados como instrumento de controle constitucional do tratamento. Conclui-se que autenticação e reconhecimento facial não podem ser juridicamente equiparados, sendo a escala e a finalidade determinantes para a aferição de validade normativa.

Palavras-chave: biometria; reconhecimento facial; autenticação facial; LGPD; RIPD; proporcionalidade; sensação de segurança

INTRODUÇÃO

A Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) classifica dados biométricos como dados pessoais sensíveis. Contudo, a legislação não regula apenas a natureza do dado, mas principalmente o tratamento realizado.

O debate público brasileiro tem tratado “biometria facial” como categoria homogênea. Entretanto, autenticação facial e reconhecimento facial são operações técnicas distintas, com impactos jurídicos diversos. A análise adequada exige compreender que o ***objeto de regulação é o tratamento de dados pessoais***, definido como qualquer operação realizada com dados pessoais.

O erro técnico que está contaminando o debate sobre biometria no Brasil

O debate sobre biometria entrou em um território perigoso: opiniões fortes, pouca diferenciação técnica e análises jurídicas superficiais.

A hipótese defendida é que autenticação facial (1:1) e reconhecimento facial (1:N) não podem ser equiparados juridicamente, pois produzem impactos normativos distintos em razão da escala, finalidade e expectativa legítima do titular.

O mercado está discutindo errado e isso está gerando decisões equivocadas

Nos últimos anos, o mercado brasileiro foi inundado por soluções chamadas genericamente de “reconhecimento facial” para:

- Condomínios
- Prédios corporativos
- Escolas
- Academias
- Hospitais
- Controle de acesso em geral
- Plataforma do Governo
- Bancos

Grande parte das discussões públicas, jurídicas e até técnicas mistura duas tecnologias diferentes:

- Reconhecimento Facial (1:N)
- Autenticação Facial (1:1)

Elas utilizam biometria facial, mas não são a mesma coisa e juridicamente não podem ser analisadas da mesma forma.

ALARMISMO GENÉRICO

Afirmações como:

- “Reconhecimento facial é proibido”
- “Biometria é sempre ilegal”
- “LGPD impede uso em condomínios”

- “A LGPD proibiu biometria. ”
- “Condomínio não pode usar reconhecimento facial. ”
- “Empresa que usa biometria vai ser multada pela ANPD. ”
- “Só o governo pode usar reconhecimento facial. ”
- “Biometria é inconstitucional. ”
- “Sem consentimento é sempre ilegal.”
- “Se é dado sensível, não pode usar.”
- “Colocou aviso na parede, já está legal.”
- “Se o morador assinou ata, acabou o problema.”

Não se pode condenar ou aprovar tecnologia por rótulo.

Está se discutindo o **dado biométrico**, quando o que deve ser analisado é o **tratamento realizado com esse dado**. A LGPD regula tratamento de dados (art. 5º, X), não “a existência do dado”.

O art. 5º, II, da LGPD classifica biometria como dado sensível.

Entretanto, o art. 5º, X define tratamento como qualquer operação realizada com dados pessoais. A norma não proíbe categorias abstratas de dados. Regula operações concretas.

O art. 11 estabelece hipóteses de tratamento de dados sensíveis, como:

- Cumprimento de obrigação legal
- Execução de políticas públicas
- Prevenção à fraude
- Proteção da vida

Logo, a pergunta juridicamente adequada não é: “Biometria é lícita? ”

Mas: “Este tratamento biométrico, neste contexto, é constitucionalmente proporcional?”

E é aqui que a diferença entre **autenticação facial** e **reconhecimento facial** muda completamente o debate

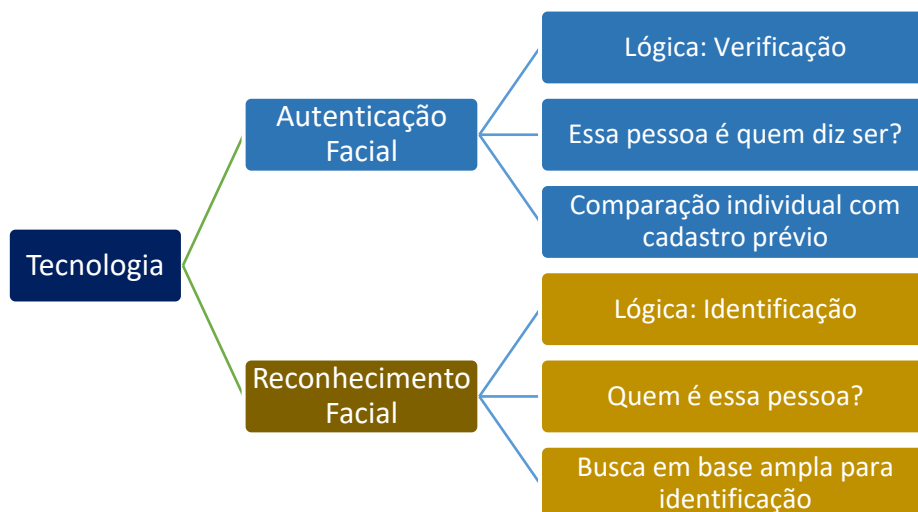
Tecnologia	Lógica	Pergunta do Sistema	Estrutura
Autenticação Facial (1:1)	Verificação	“Essa pessoa é quem ela diz ser?”	Comparação individual com cadastro prévio
Reconhecimento Facial (1:N)	Identificação	“Quem é essa pessoa?”	Busca em base ampla para identificar

Ambas utilizam biometria. Mas o tratamento é completamente diferente.

E é o tratamento que define:

- Risco
- Impacto
- Necessidade
- Proporcionalidade
- Justificativa jurídica

LGPD { **Uso Legal:** A LGPD regula o tratamento de dados, não a existência de dados biométricos. O uso pode ser legal se cumprir obrigações legais, prevenir fraudes ou proteger vidas.
Uso Ético: A ética depende do contexto e da proporcionalidade. A autenticação facial pode ser mais ética do que o reconhecimento facial, dependendo do uso.



PRECISÃO TERMINOLÓGICA E FINALIDADE DO TRATAMENTO

No Segundo Encontro de Encarregados de Dados da Autoridade Nacional de Proteção de Dados (ANPD), Luís Felipe Monteiro (VP de Relações Institucionais Unico)¹ destacou que os termos utilizados no debate público “parecem sinônimos, mas possuem finalidades diferentes”.

Segundo sua exposição, a biometria pode funcionar como:

- Digital para emissão de título;
- Mecanismo de autenticação para acesso a serviços digitais;
- Instrumento de monitoramento de segurança.

Essa distinção é central para o enquadramento jurídico, ela não é semântica é funcional

Pode-se sistematizar:

- Coleta biométrica: captura inicial do dado;
- Verificação biométrica (1:1): confirmação de identidade declarada;
- Reconhecimento biométrico (1:N): identificação em base ampla;
- Monitoramento biométrico: identificação contínua em fluxo.

Conforme observa Doneda², a proteção de dados exige análise contextual e finalística do tratamento.

AUTENTICAÇÃO FACIAL (1:1)

A autenticação facial consiste na verificação entre a biometria apresentada e um template previamente associado ao titular.

Pergunta operacional: “*Esta pessoa é quem afirma ser?*”

¹ MONTEIRO, Luis Felipe. Exposição no Segundo Encontro de Encarregados de Dados da ANPD, 2024

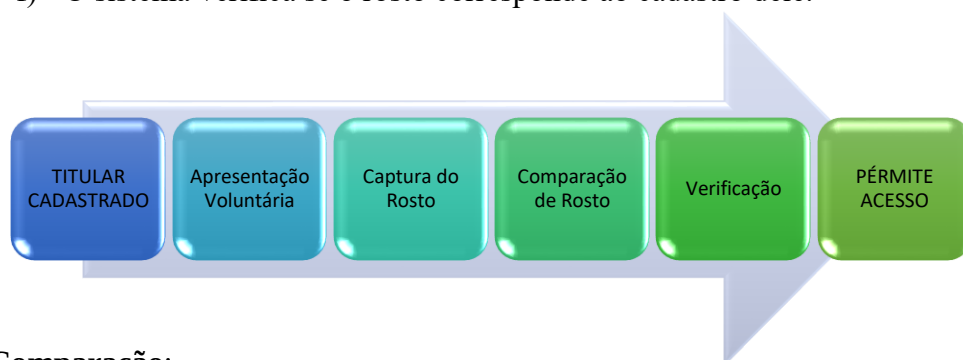
² DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Renovar, 2006.

Trata-se de operação individualizada, com identidade previamente declarada.

Em determinados serviços digitais, pode não haver alternativa igualmente segura, especialmente diante do crescimento de fraudes sintéticas.

Funciona assim:

- a) O titular já está previamente cadastrado.
- b) Ele se apresenta voluntariamente.
- c) O sistema compara o rosto capturado com o template previamente vinculado àquele indivíduo.
- d) Morador ao entrar no condomínio.
- e) Ele olha para a câmera.
- f) O sistema verifica se o rosto corresponde ao cadastro dele.



Comparação:

É o equivalente biométrico de digitar senha ou usar impressão digital. Validação antifraude em serviços digitais

Características:

- Base fechada
- Identidade previamente declarada
- Comparação individual
- Controle de acesso
- Finalidade delimitada

RECONHECIMENTO FACIAL (1:N)

O reconhecimento facial realiza identificação em base ampla de dados.

Pergunta operacional: “Quem é esta pessoa? ”

Essa modalidade envolve:

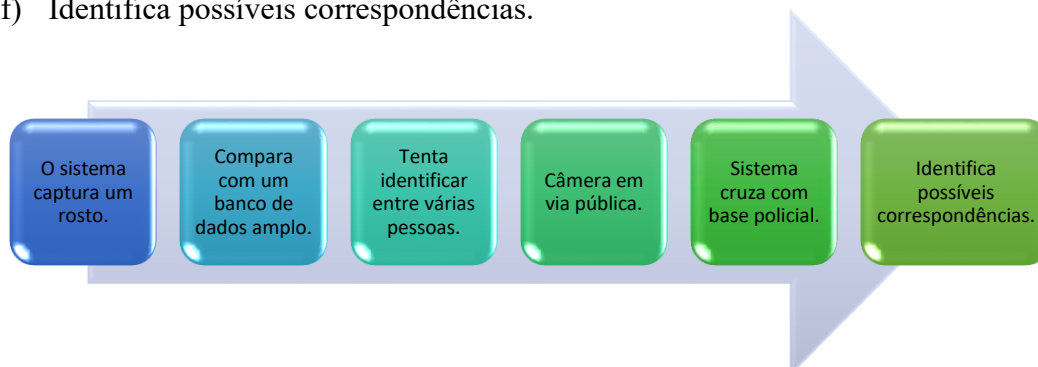
- Base massiva;
- Identificação sem declaração prévia;
- Potencial monitoramento coletivo;
- Maior risco de falsos positivos.
- Identificação em espaços públicos.

Estudos demonstram que sistemas de reconhecimento facial podem apresentar vieses significativos, especialmente em relação a gênero e raça.

Funciona assim:

- a) O sistema captura um rosto.

- b) Compara com um banco de dados amplo.
- c) Tenta identificar entre várias pessoas.
- d) Câmera em via pública.
- e) Sistema cruza com base policial.
- f) Identifica possíveis correspondências.

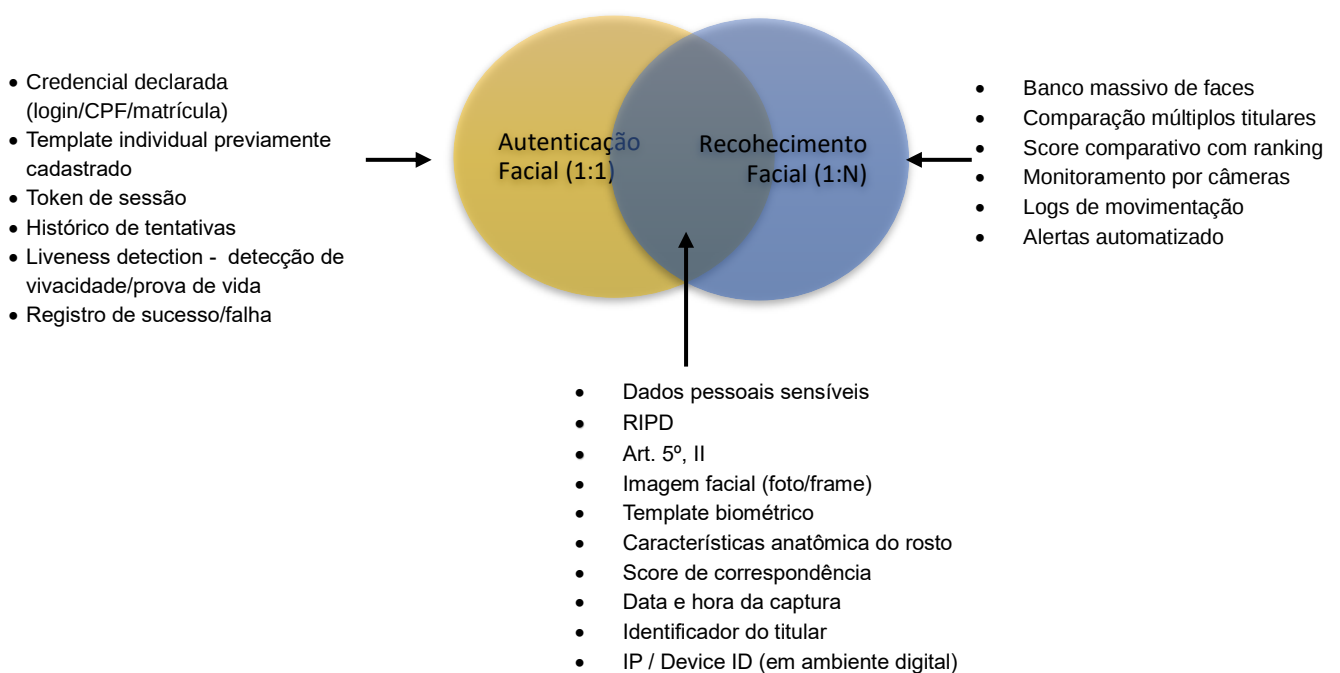


Características:

- Base ampla
- Identidade não declarada
- Busca em massa
- Pode envolver vigilância

O que muda é:

- Escala
- Expectativa legítima do titular
- Grau de monitoramento
- Risco de discriminação
- Impacto coletivo



CONTEXTO CONTEMPORÂNEO: DEEPFAKE E FRAUDE SINTÉTICA

O crescimento de técnicas de deepfake no Brasil alterou significativamente o cenário de risco digital. Fraudadores passaram a estruturar ambientes sofisticados para simular identidades e manipular imagens com o objetivo de obter vantagens indevidas.

Nesse contexto, mecanismos tradicionais de autenticação (senha, OTP) tornaram-se mais vulneráveis.

Como observa Hartzog³, privacidade e segurança devem ser analisadas sob perspectiva estrutural, considerando riscos reais do ambiente tecnológico.

Nesse contexto:

- Senhas e OTPs tornaram-se vulneráveis;
- Documentos digitalizados são facilmente replicáveis;
- A autenticação biométrica com prova de vida passou a desempenhar função antifraude relevante.

A análise jurídica deve considerar o ambiente tecnológico real, sob pena de produzir soluções descoladas da realidade.

ACESSO DIGITAL VERSUS CONTROLE DE ACESSO FÍSICO

Luis Felipe Monteiro (VP de Relações Institucionais Unico) ressaltou que, em determinados serviços digitais, pode não existir alternativa tão segura quanto a autenticação biométrica. Por outro lado, em ambientes como condomínios, pode haver meios menos intrusivos, devendo-se realizar análise concreta de risco.

Aqui incide o princípio da necessidade, previsto no art. 6º, III, da LGPD.

Monitoramento biométrico em larga escala, especialmente em espaços públicos, aproxima-se da lógica de segurança pública e exige escrutínio mais rigoroso.

SENSAÇÃO DE SEGURANÇA VERSUS SEGURANÇA EFETIVA

Em sua exposição, Fabrício Lopes (Fiscalização ANPD)⁴, representante da área de fiscalização da ANPD, trouxe reflexão relevante: a biometria frequentemente gera sensação de segurança, mas não necessariamente segurança real.

Segundo ele:

Não se vê detectores de metais em condomínios como padrão de segurança, mas observa-se biometria sendo amplamente adotada;

- Há uma crença de que biometria é sinônimo de proteção;
- A centralização do dado biométrico pode ser comparada a “colocar a senha na testa”.
- A metáfora revela preocupação com a irreversibilidade do dado biométrico.

³ HARTZOG, Woodrow. *Privacy's Blueprint*. Harvard University Press, 2018.

⁴ LOPES, Fabrício. Exposição no Segundo Encontro de Encarregados de Dados da Autoridade Nacional de Proteção de Dados (ANPD). Brasília, 2024.

EXPANSÃO INDISCRIMINADA E BANALIZAÇÃO DA COLETA

Fabício Lopes relatou que, ao analisar três processos envolvendo dados pessoais, todos apresentavam interseção com biometria sob argumento de segurança pública.

Segundo sua crítica:

- Todos querem coletar biometria;
- Muitas vezes coletam porque “todos coletam”;
- Pergunta-se: é realmente necessário?
- Cada local precisa ter minha biometria?

A analogia apresentada foi a de possuir “uma carteira em cada lugar”. Essa banalização compromete o princípio da necessidade.

SETOR PÚBLICO VERSUS SETOR PRIVADO

Outro ponto levantado por Fabício Lopes refere-se à diferença de confiança entre setor público e privado. Ele afirmou acreditar ser mais seguro fornecer dados ao setor público quando há finalidade específica e delimitada.

No setor privado, surgem preocupações como:

- Compartilhamento com terceiros;
- Ausência de canal de comunicação com o titular;
- Falta de transparência;
- Uso para finalidade diversa da declarada.

A LGPD impõe limitação de finalidade e vedação ao desvio. A alegação genérica de “segurança pública” por entes privados é juridicamente problemática, pois segurança pública é atividade típica do Estado.

Segurança pública é típica do Estado (art. 144 da Constituição). Entes privados não podem invocar genericamente essa finalidade. O art. 144 da Constituição define segurança pública como dever do Estado. Contudo, não elimina:

- Presunção de inocência
- Liberdade de locomoção
- Direito ao anonimato

Tratamentos massivos exigem justificativa reforçada.

BIOMETRIA COMO CAMADA ADICIONAL, NÃO SOLUÇÃO ÚNICA

Fabício Lopes enfatizou que biometria deve ser:

- Camada extra de segurança;
- Não única barreira de proteção.

A ideia de unicidade como garantia absoluta é ilusória.

Além disso, defendeu que:

- Devem existir alternativas (senha, cartão, token);
- A biometria deve ter finalidade específica;
- O titular deve possuir poder de oposição.

O direito de oposição está previsto no art. 18 da LGPD¹.

RIPD: ANTES, DURANTE E DEPOIS

Outro ponto marcante foi a afirmação de que o tratamento biométrico exige Relatório de Impacto à Proteção de Dados (RIPD):

- Antes da implementação;
- Durante a operação;
- Após a implantação, como mecanismo contínuo de avaliação.

A ausência de avaliação prévia pode indicar descumprimento do dever de responsabilização e prestação de contas. Conforme Mendes, a governança em proteção de dados exige avaliação estruturada de risco e documentação formal.

EXPANSÃO DO USO BIOMÉTRICO NO BRASIL

Segundo dados apresentados por Manuela Ribeiro (CETIC.BR), em 2023:

- 30% das empresas brasileiras coletavam dados biométricos;
- Houve aumento expressivo de dispositivos inteligentes e IoT;
- Cresceu o uso de biometria para controle e segurança;
- 12% das escolas utilizavam reconhecimento biométrico;
- 1 a cada 4 escolas no Paraná coletava dados biométricos de alunos.

A coleta ocorre por diferentes modalidades:

- Reconhecimento facial;
- Digital;
- Palma da mão;
- Autenticação visual.

Observa-se maior adoção na rede privada do que na pública.

PERCEPÇÃO SOCIAL DO RISCO BIOMÉTRICO

Ainda conforme Manuela Ribeiro, em 2023:

- A biometria era o dado que mais gerava preocupação;
- Titulares têm mais receio em fornecer biometria do que outros dados sensíveis;
- Religião, orientação política e sexual geravam menor preocupação.

Esse dado revela distorção perceptiva: o titular tende a associar “dado sensível” apenas à biometria facial, ignorando que outras categorias também são sensíveis¹.

Há, portanto, um fenômeno curioso:

- O usuário resiste a fornecer biometria a empresas físicas;
- Mas utiliza biometria diariamente em seus próprios dispositivos móveis;
- Demonstra medo maior de “foto” do que de outros dados sensíveis.

Observou-se maior receio social quanto à biometria facial do que a outros dados sensíveis. A percepção de proximidade gera falsa sensação de segurança.

A existência de falsos positivos e vieses algorítmicos pode gerar consequências concretas à esfera jurídica do indivíduo. Sem mecanismos de auditoria, transparência, revisão humana e contestação, o uso automatizado da biometria pode comprometer garantias processuais.

Nesse ponto, a distinção entre autenticação (verificação voluntária) e reconhecimento (identificação não declarada) assume densidade constitucional. A primeira tende a ocorrer com anuência do titular e finalidade delimitada; a segunda pode produzir efeitos jurídicos sem ciência prévia ou possibilidade imediata de contestação

SEGURANÇA VERSUS SENSÇÃO DE SEGURANÇA

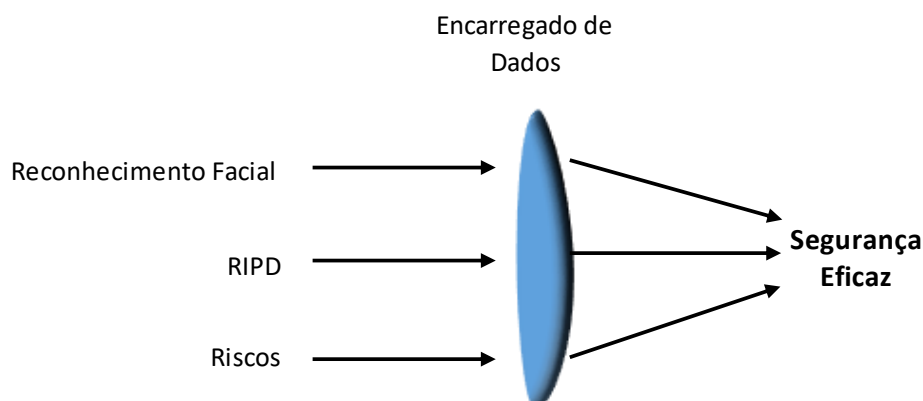
A pesquisadora Bianca Kremer (FGV/RJ)⁵, com mais de 10 anos de atuação na área de biometria, destacou que segurança é diferente de sensação de segurança.

Segundo sua exposição:

- O reconhecimento facial exige grande volume de dados e poder computacional;
- Trata-se de tecnologia complexa, dependente de base pré-treinada;
- Governo vêm realizando RIPDs, mas questiona-se:
 - Há indicadores de falsos positivos?
 - Há avaliação de potencial de dano?

Além disso, mencionou a ocorrência de três megavazamentos utilizados para fraudes.

A crença de que reconhecimento facial é “bala de prata” para segurança pública é ilusória.



⁵ KREMER, Bianca. Exposição no Segundo Encontro de Encarregados de Dados da ANPD, 2024.

SETOR PÚBLICO, OBRIGATORIEDADE E TRANSPARÊNCIA

Bianca Kremer também destacou a ampliação normativa do uso biométrico pelo Estado:

- Lei nº 15.077/2024 (cadastro biométrico obrigatório no INSS);
- Decreto nº 12.561/2024 (regulamentação);
- Portaria nº 961/2025 do MJSP (uso em investigações criminais).

O uso governamental é significativamente maior que o privado em matéria de segurança pública.

Contudo, questiona-se:

- Onde estão os indicadores públicos?
- Onde está o RIPD amplamente divulgado?
- Onde estão dados de acurácia e taxas de erro?

A obrigatoriedade para milhões de cidadãos altera a lógica de consentimento.

Tabela de Balanceamento (comparativo de proporcionalidade)

Critério	Autenticação Facial (1:1)	Reconhecimento Facial (1:N)
Alternativa menos intrusiva	Avaliar caso concreto	Frequentemente existente
Alternativas	Devem existir	Frequentemente existem
Contexto típico	Serviços digitais	Segurança pública
Direito de oposição	Deve ser garantido	Complexo em monitoramento
Escala	Restrita	Massiva / Base ampla ou indeterminada
Exigência de RIPD	Recomendada	Altamente recomendável
Finalidade	Acesso específico, Controle de acesso e segurança patrimonial	Identificação ampla, Identificar indivíduos desconhecidos
Identidade declarada	Sim	Não
Impacto coletivo	Restrito	Elevado / Alto (liberdade, anonimato, não discriminação) / Falsos positivos e vieses algorítmicos
Natureza do dado	Sensível - Biometria facial (dado sensível)	Sensível - Biometria facial (dado sensível)
Risco coletivo	Baixo a moderado	Elevado / Identificação sem consentimento ou declaração prévia de identidade.
Risco de viés	Reduzido	Significativo
Sensação de segurança	Pode ser técnica	Pode ser ilusória
Tratamento realizado	Verificação individual / Base restrita (Titular cadastrados)	Identificação em massa / Identificação em base ampla sem identidade previamente declarada
Uso por privado sob "segurança pública"	Restritivo	Problemático
Necessidade	Existem meios menos invasivos, Reduzir fraude, Evitar compartilhamento indevido, Aumentar segurança real / Pode ser necessária se houver risco de compartilhamento de cartões/senhas	Contexto de segurança pública
Adequação	Controla acesso restrito, Reduz invasões, Evita uso indevido de credenciais	Reconhecimento
Pergunta a Responder	Há alternativa real? O banco é restrito? O armazenamento é seguro? Há opção alternativa para quem não quer aderir?	Vigilância massiva? Erros de identificação? Discriminação algorítmica? Impacto na liberdade individual?
Expectativa do Titular	Alta previsibilidade (ambiente fechado e controlado)	Baixa previsibilidade (monitoramento constante)
Alternativas	Cartão, senha, QR Code	Controle de acesso tradicional, vigilância humana / Validação em tempo Real
Segurança	Criptografado, retenção limitada, alternativa para quem não quiser aderir	Criptografado, retenção limitada, alternativa para quem não quiser aderir
Conclusão do balanceamento	Pode ser juridicamente defensável se houver governança, transparência e proporcionalidade	Exige justificativa extremamente robusta e forte demonstração de necessidade

AVALIAÇÃO BIOMÉTRICA



CONCLUSÃO

Autenticação facial não é reconhecimento facial, aquela é: Controle individualizado de acesso, já essa é: Identificação em massa.

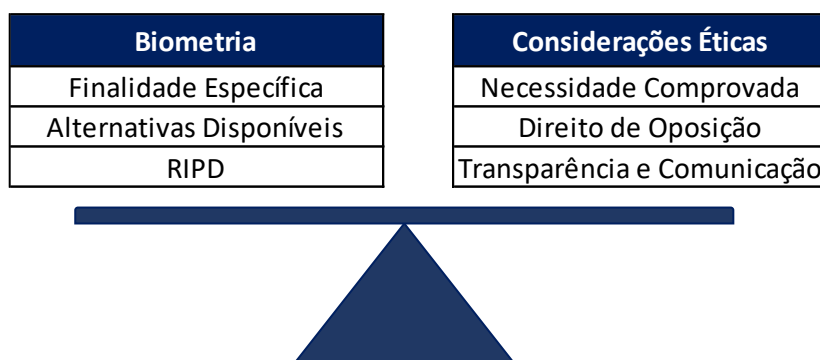
Se vamos discutir biometria, precisamos discutir com precisão técnica, caso contrário, o debate vira ideológico

As exposições de Luis Felipe Monteiro, Manuela Ribeiro, Bianca Kremer e Fabrício Lopes convergem para conclusão central. *O dado pode ser o mesmo. Mas o tratamento, a finalidade e o contexto determinam sua legitimidade. É o contexto operacional que define o risco*

Biometria não é solução mágica, não é segurança por si só, e não pode ser banalizada.

Seu uso exige:

- **Finalidade específica:** A tecnologia deve ser utilizada para um propósito claro e definido.
- **Necessidade comprovada:** Deve haver uma justificativa sólida para o uso da biometria, demonstrando que é a melhor opção disponível.
- **Alternativas disponíveis:** É importante considerar se existem outras opções que possam atender à mesma necessidade sem os riscos associados à biometria.
- **Direito de oposição:** Os indivíduos devem ter o direito de se opor ao uso de seus dados biométricos.
- **RIPD estruturado:** A realização de um Relatório de Impacto à Proteção de Dados (RIPD) deve ser uma prática padrão para avaliar os riscos envolvidos.
- **Transparência e canal de comunicação:** As organizações devem ser transparentes sobre como os dados biométricos são coletados, armazenados e utilizados, além de oferecer canais de comunicação para esclarecer dúvidas e preocupações.



Sem a observância dessas diretrizes, a tecnologia biométrica pode deixar de ser uma ferramenta de segurança e se transformar em um risco estrutural. Portanto, é essencial que o debate sobre biometria seja conduzido com responsabilidade, levando em consideração as implicações éticas e sociais do seu uso. A segurança deve ser equilibrada com a proteção da privacidade e dos direitos individuais, garantindo que a tecnologia sirva ao bem comum e não se torne uma ameaça.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 15 ago. 2018.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

MONTEIRO, Luis Felipe. Exposição no Segundo Encontro de Encarregados de Dados da Autoridade Nacional de Proteção de Dados (ANPD). Brasília, 2024.

LOPES, Fabrício. Exposição no Segundo Encontro de Encarregados de Dados da Autoridade Nacional de Proteção de Dados (ANPD). Brasília, 2024

KREMER, Bianca, Exposição no Segundo Encontro de Encarregados de Dados da Autoridade Nacional de Proteção de Dados (ANPD). Brasília, 2024

BRASIL. Constituição da República Federativa do Brasil de 1988.

EUROPEAN UNION. Artificial Intelligence Act. Regulation (EU) 2024. https://www.eeas.europa.eu/delegations/council-europe/european-commission-signs-historic-council-europe-framework-convention-artificial-intelligence-and_en?utm_source=chatgpt.com
Acessado em: 22/02/2026