

# Reconhecimento facial

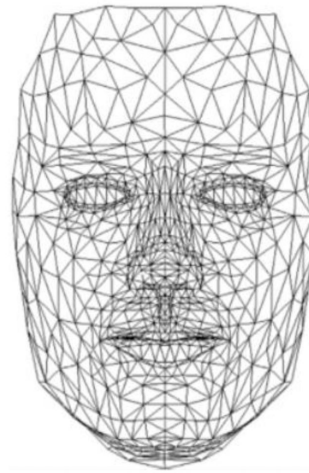
## Aspectos de direito civil e consumidor

Michel R. O. Souza (Derechos Digitales)  
Rafael A. F. Zanatta (Data Privacy Brasil)

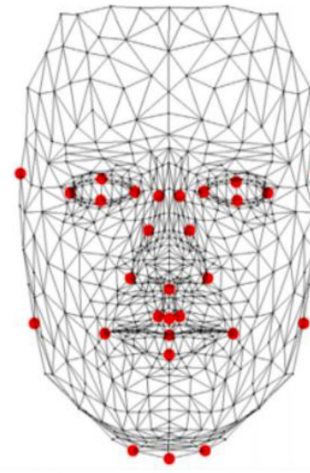
Defensoria Pública de São Paulo  
14/02/2023

# Organização da apresentação

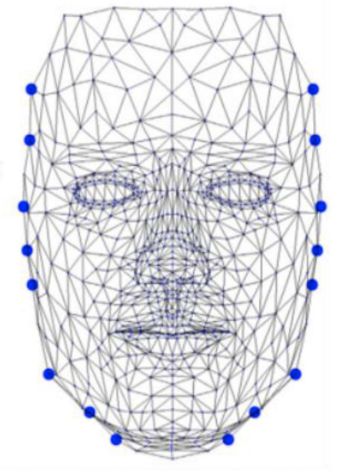
1. Retomando: o que se entende por reconhecimento facial
2. O debate no direito civil
3. Normas jurídicas relevantes
4. Casos paradigmáticos
  - a. Hering
  - b. ViaQuatro
  - c. Companhia Metropolitana
  - d. Hapvida



(a)



(b)



(c)



## Processo de reconhecimento facial:



Uma imagem é capturada



O software de reconhecimento de imagens de IA lê a geometria do rosto na imagem ao olhar para a distância entre as principais funcionalidades faciais, criando um modelo facial exclusivo



O modelo facial é comparado com uma base de dados de rostos conhecidos, armazenados ou disponíveis



É feita uma determinação se for encontrada uma combinação na base de dados existente

# Automated Facial Recognition / Purpose / Decision

## AFR PROCESS

### Capture Video image



Source image



Detect and analyse the face and create a facial map

Suitable camera at the entry or exit point

### Image and identity

Source image

Identifying data

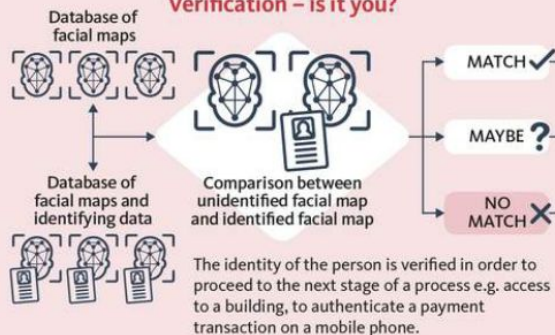


Detect and analyse the face and create a facial map linked to identifying data

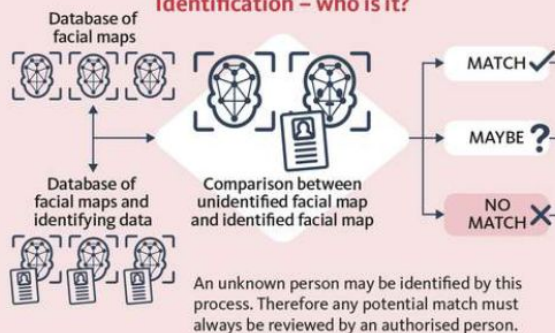
Person provides their ID to the operator e.g. photo passport, photo driving licence, photo with other ID such as bank details. Person may or may not consent to their photo and ID to be held on the database depending on the purpose e.g. private or public use.

## APPLICATION USE/PURPOSE

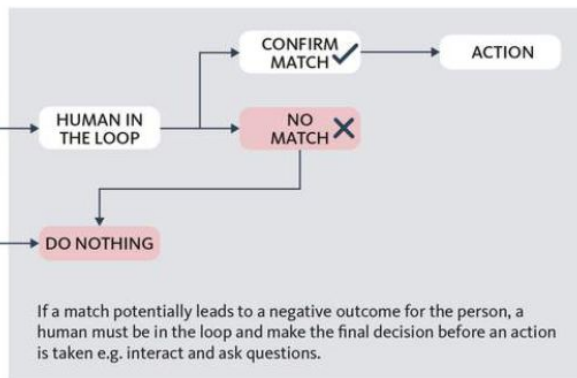
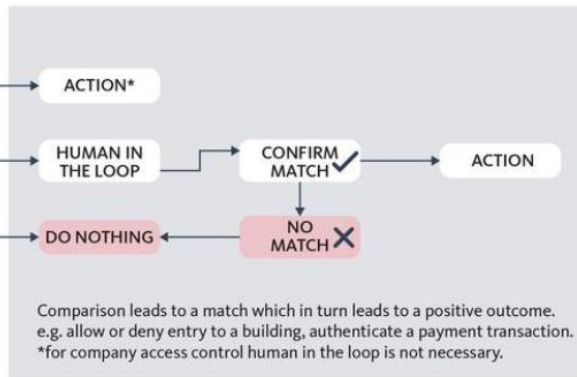
### Verification – is it you?



### Identification – who is it?



## DECISION



"Automated Facial Recognition: a guide to ethical and legal use" (BSIA, 2022)

# PARA QUE FINS

CATEGORIZAÇÃO



O que posso afirmar sobre essa pessoa?



Indivíduo é categorizado de acordo com suas expressões faciais, idade, gênero etc

VERIFICAÇÃO



Essa pessoa é quem ela afirma ser?



Sistema busca verificar se determinado indivíduo é ele mesmo

IDENTIFICAÇÃO



Quem é essa pessoa?



Sistema é capaz de identificar um indivíduo dentre vários

“[Reconhecimento facial e o setor privado](#)” (InternetLab & Idec, 2021)

“Um sistema de reconhecimento facial analisa e compara um determinado rosto com imagens armazenadas previamente em uma base de dados. Utilizando algoritmos, esse sistema rastreia e mapeia os padrões de uma face humana em formatos geométricos e logarítmicos para então identificar as suas características únicas.

Por meio dessas características, é possível mapear o perfil do usuário identificando, por exemplo, o contorno do rosto, distância entre olhos e nariz, profundidade, cicatrizes, entre outros. É por meio da predição que o reconhecimento facial determina a probabilidade de um rosto ser o mesmo que foi apresentado em um documento ou armazenado em uma base de dados” (IDwall, 2022)



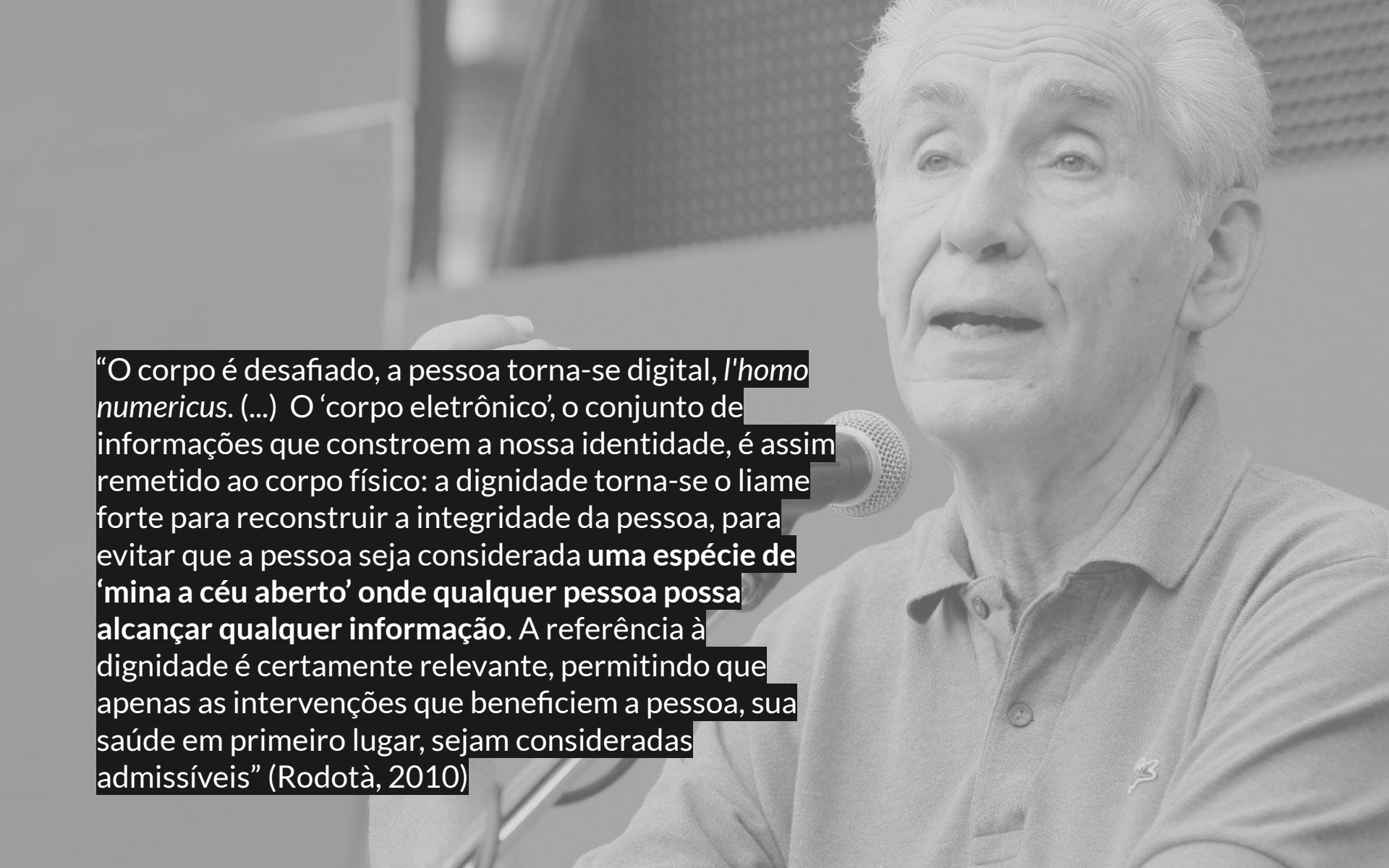




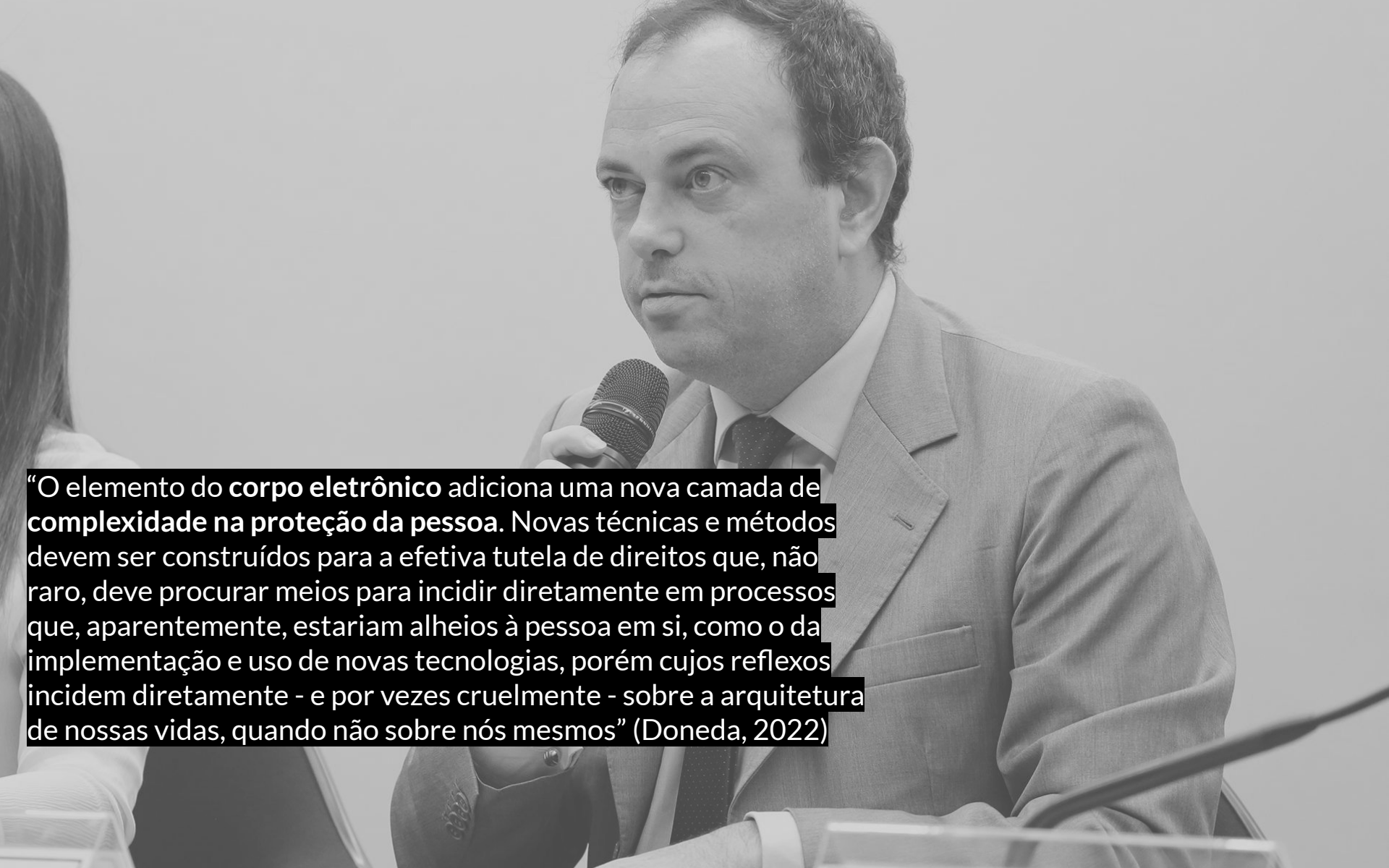
# O debate teórico no direito civil





A black and white photograph of an elderly man with white hair, wearing a light-colored polo shirt, speaking into a microphone. The background is slightly blurred, showing what appears to be a studio or conference setting. A quote is overlaid on the left side of the image.

“O corpo é desafiado, a pessoa torna-se digital, *l'homo numericus*. (...) O ‘corpo eletrônico’, o conjunto de informações que constroem a nossa identidade, é assim remetido ao corpo físico: a dignidade torna-se o liame forte para reconstruir a integridade da pessoa, para evitar que a pessoa seja considerada **uma espécie de ‘mina a céu aberto’ onde qualquer pessoa possa alcançar qualquer informação**. A referência à dignidade é certamente relevante, permitindo que apenas as intervenções que beneficiem a pessoa, sua saúde em primeiro lugar, sejam consideradas **admissíveis**” (Rodotà, 2010)

A black and white photograph of a man in a suit and tie, speaking into a microphone. He is looking slightly to the left of the camera. The image is semi-transparent, with a dark text box overlaid on the lower-left portion. The text is in white, bold font.

“O elemento do **corpo eletrônico** adiciona uma nova camada de **complexidade na proteção da pessoa**. Novas técnicas e métodos devem ser construídos para a efetiva tutela de direitos que, não raro, deve procurar meios para incidir diretamente em processos que, aparentemente, estariam alheios à pessoa em si, como o da implementação e uso de novas tecnologias, porém cujos reflexos incidem diretamente - e por vezes cruelmente - sobre a arquitetura de nossas vidas, quando não sobre nós mesmos” (Doneda, 2022)

Transição do debate sobre “viés endêmico” para debate sobre “opressão endêmica”

O reconhecimento facial oferece um conjunto de “affordances” que permite a opressão e violação sistemática de direitos fundamentais de forma inédita, ensejando novos tipos de contramovimentos jurídicos

Souza & Zanatta (2021)

## The Problem of Automated Facial Recognition Technologies in Brazil: Social Countermovements and the New Frontiers of Fundamental Rights

**Michel R. O. Souza**

Brazilian Institute of Consumer Defense (Idec)

**Rafael A. F. Zanatta**

Data Privacy Brasil Research Association and University of São Paulo

**Keywords:** Facial Recognition Technology, Fundamental Rights, Social Movements, Brazil

### Abstract

This article analyzes the characteristics of automated facial recognition technologies and their response by civil society organizations in Brazil. We analyze two arguments in this debate: the endemic bias argument, which seeks to correct unjust and potentially racist consequences, and the endemic oppression argument, which identifies a set of facilitators of systematic violation of fundamental rights. We present the concept of counter-movements to explain the possibilities of legal contestation of the dissemination of facial recognition and explain how the argument about recognition can move from the logic of bias to that of oppression, with the possibility of changing the regulation to ban this technology in certain uses.



LA  
HRS  
LATIN AMERICAN  
HUMAN RIGHTS  
STUDIES



PDF

Published  
2021-06-30



---

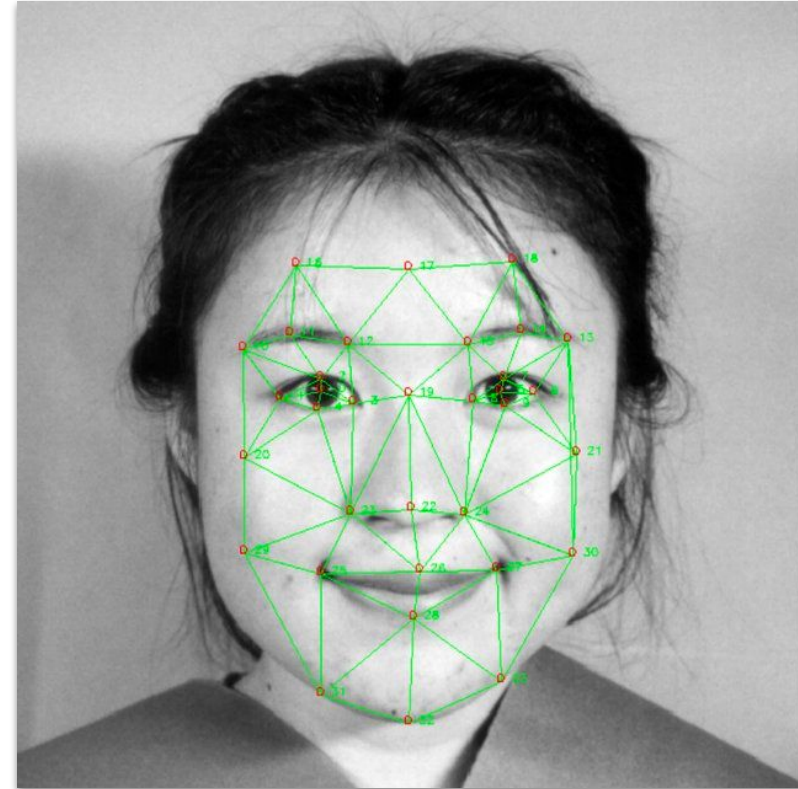
**Que direitos são afetados?**

**Debate jurídico contemporâneo**

---

## Comitê Consultivo do Conselho da Europa - Convenção 108 (2021)

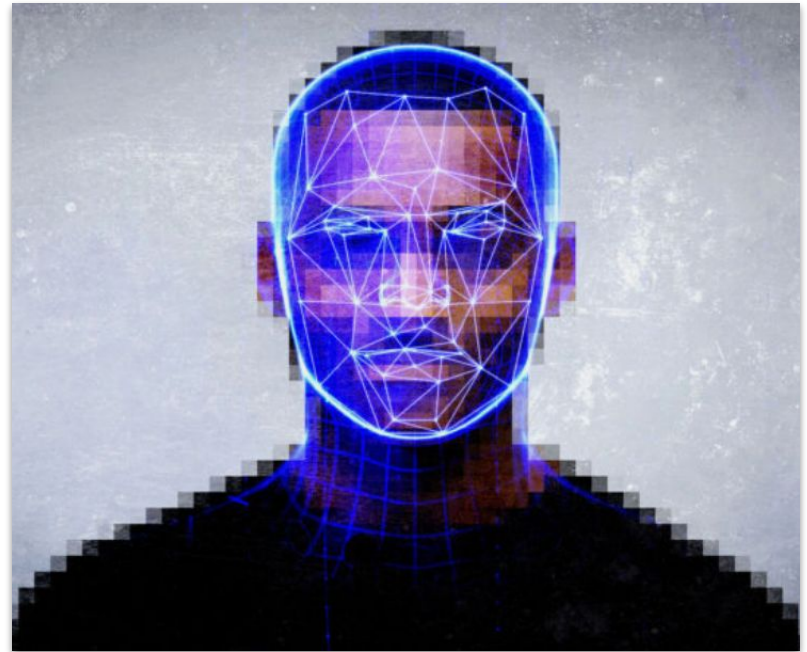
- O uso de sistemas de reconhecimento facial em ambientes abertos e incontrolados **provoca violação de diversos direitos fundamentais** de privacidade e dignidade
- O reconhecimento facial para identificação exclusiva de raça, gênero, cor de pele, religião, condição social ou condição de saúde **deve ser proibido**
- O reconhecimento facial para identificação de sentimentos, emoções e traços de personalidade **deve ser proibido** se atrelado a questões de contratação, educação e seguros



---

## Comitê Consultivo do Conselho da Europa - Convenção 108 (2021)

- O uso de sistemas de reconhecimento facial para fins de segurança pública necessita de fundamento legal e **deve ser executado somente por autoridades de segurança**
- A **necessidade e proporcionalidade** devem ser demonstradas pela designação de local e tempo adequado de utilização das tecnologias de reconhecimento facial na segurança pública
- O consentimento não é uma base legal adequada para o setor público considerando as assimetrias de poder entre o cidadão e o Estado

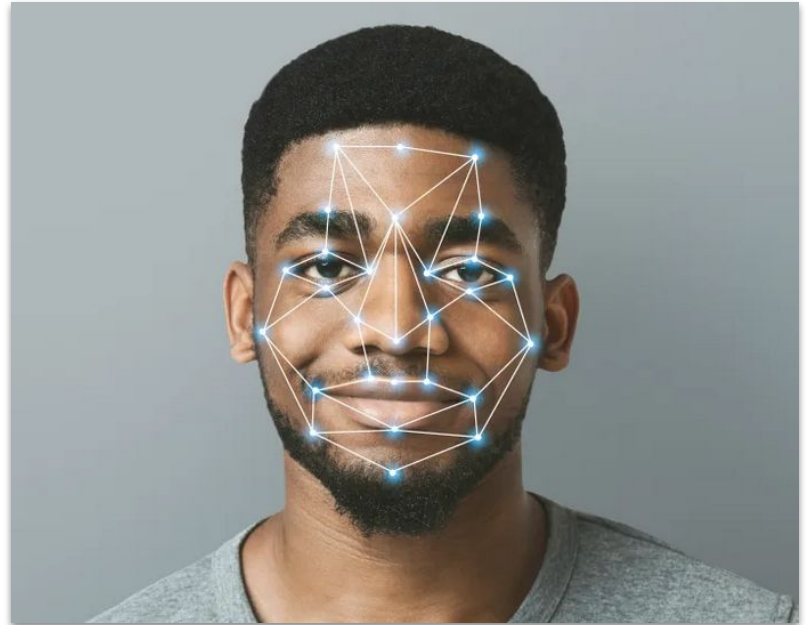




---

## Comitê Consultivo do Conselho da Europa - Convenção 108 (2021)

- Nas relações privadas, o reconhecimento facial necessita de **consentimento livre e informado**, com alternativas para autenticação como senha ou badge de identificação
- O consentimento deve ser para uma **finalidade específica** e os dados não podem ser tratados de forma incompatível com esses propósitos
- Entidades privadas não podem utilizar tecnologias de reconhecimento facial **em ambientes abertos como shoppings**, especialmente para identificar pessoas de interesse para fins de marketing ou para segurança privada



## Automated Facial Recognition Technology Bill (2020, UK)

(1) It is an offence for a person to operate, install, or commission the operation or installation of, equipment incorporating automated facial recognition technology capable of biometrically analysing those present in any public place in the United Kingdom.

For the purposes of subsection (1) “automated facial recognition technology” includes any equipment which can automatically detect and biometrically recognise facial images through data captured by a still or moving image camera, whether the identification takes place at the time the data is captured or at a later time

PL 499/2022

Art. 2º Para os fins desta Lei, considera-se: I – reconhecimento facial o processamento automatizado ou semiautomatizado de imagens que contenham faces de indivíduos, com o objetivo de identificá-los, verificá-los ou categorizá-los;

Art. 3º Fica vedado ao Poder Público no Município de Porto Alegre, em sua Administração Direta e Indireta, bem como às concessionárias e permissionárias de serviços públicos:


I – obter, adquirir, reter, vender, possuir, receber, solicitar, acessar, desenvolver, aprimorar ou utilizar tecnologias de reconhecimento facial ou informações derivadas de tecnologia de reconhecimento facial;



PL 2392/2022

Art. 2o O tratamento de dados biométricos oriundos de tecnologias de reconhecimento facial **deverá atender ao disposto na Lei Geral de Proteção de Dados (LGPD), Lei no 13.709, de 14 de agosto de 2018,** e não poderão ser repassados a terceiros, salvo ao poder público para casos exclusivos de segurança pública, defesa nacional e atividades de investigação e repressão de infrações penais

Art. 3o Dados biométricos oriundos de tecnologias de reconhecimento facial não poderão ser utilizados como forma de identificação **sem realização prévia de relatório de impacto à privacidade de que trata a LGPD,** o qual deverá estar disponível para fiscalização por parte do órgão competente pela proteção dos dados pessoais, demonstrando a sua necessidade e impossibilidade de utilização de outro tipo de identificação que não se utilize de dados biométricos



PL 2537/2019

Art. 1º. Esta Lei visa informar aos consumidores as condições de reconhecimento facial ao adentrarem em estabelecimentos comerciais.

Art. 2º. Os estabelecimentos comerciais que utilizarem programas de reconhecimento facial com o intuito de identificar os consumidores **devem alertá-los na entrada do estabelecimento** com placas e/ou adesivos da análise de características sendo utilizada.

# RECONHECIMENTO

## FACIAL E O SETOR

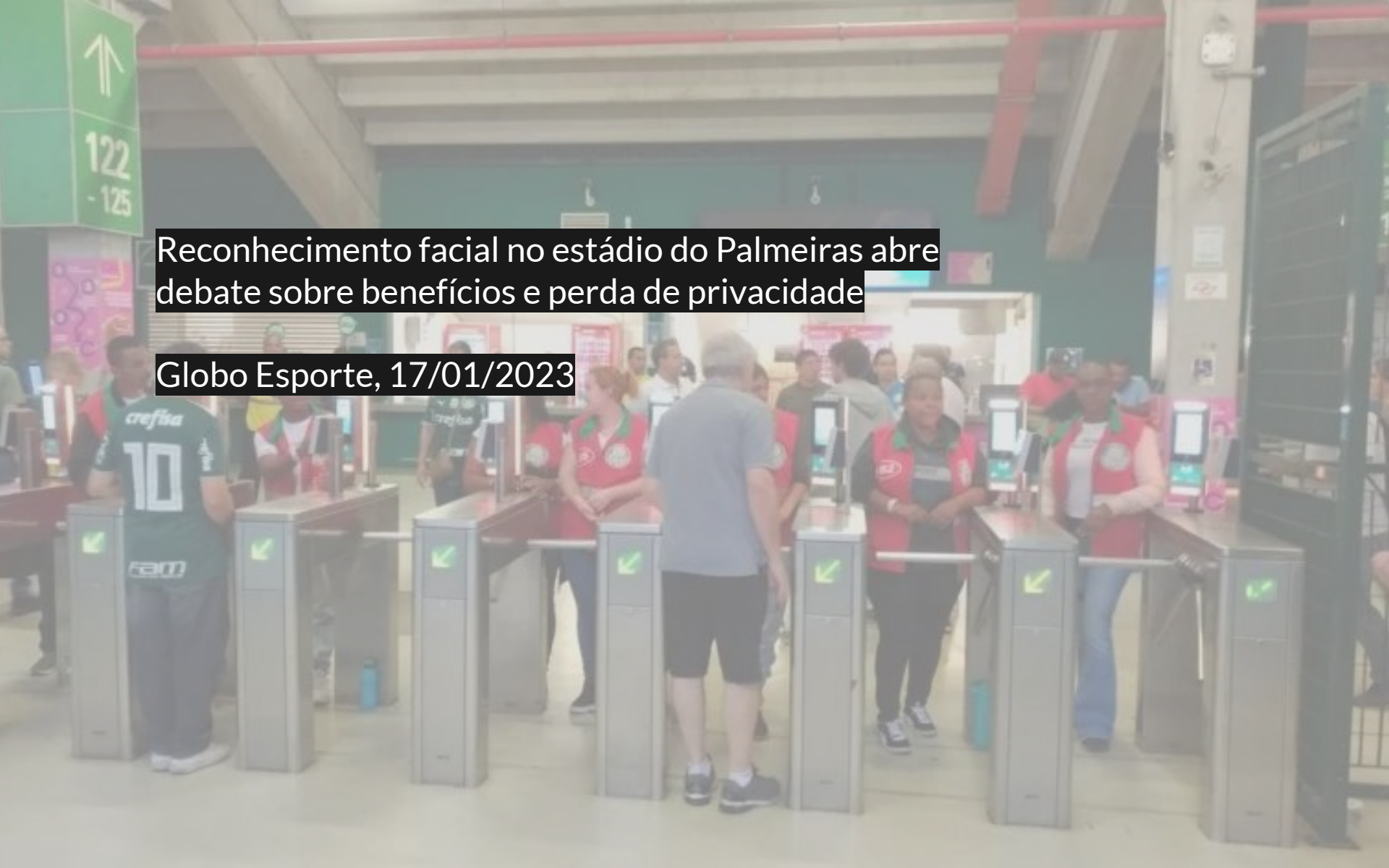
A medida mais importante é garantir que titulares tenham sempre a opção de ter acesso ao produto, serviço ou funcionalidade mesmo que não consentam com a captura dos dados de seu rosto. Isso significa dizer que, para que o consentimento seja, de fato, livre, dele não deve depender o acesso ao serviço.

No caso do Brasil, o consentimento deve obedecer às adjetivações da lei – deve ser livre, expresso e informado, além de, por se tratar do tratamento de dados sensíveis, ser fornecido de forma específica e em destaque.

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 **TCAS** concordância expressa por meio de um dispositivo disponível na entrada da loja ou por meio de um código QR de ativação)





A photograph of a stadium entrance. In the foreground, several grey turnstiles with green arrows pointing right are visible. A man in a grey t-shirt and black shorts is walking through one of the turnstiles. To his left, a man in a dark green t-shirt with 'crefisa' and the number '10' is standing. To the right, several staff members in red vests are standing near the turnstiles. In the background, more people are visible, and a green sign with an upward arrow and the numbers '122 - 125' is on the left. The scene is brightly lit, suggesting an indoor or well-lit outdoor stadium.

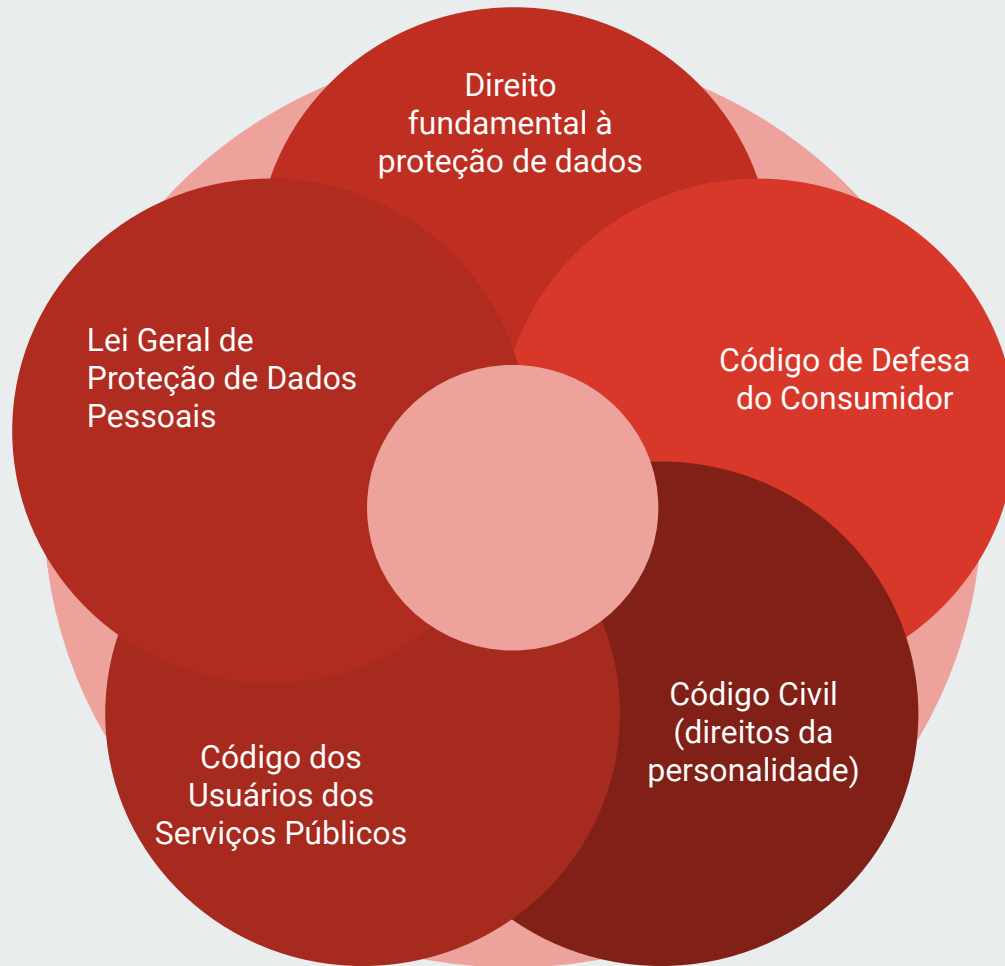
Reconhecimento facial no estádio do Palmeiras abre debate sobre benefícios e perda de privacidade

Globo Esporte, 17/01/2023



**Qual o debate feito na tutela administrativa e judicial?**

---





## Caso Hering (2019)

Secretaria Nacional do  
Consumidor

- **Natureza do ilícito:** implementação de sistema de reconhecimento facial sem informação e consentimento do consumidor
- **Fundamentação jurídica:** Código de Defesa do Consumidor, art. 20, Código Civil e Constituição Federal
- **Desdobramentos:** reconhecimento de violação de “direito da personalidade do consumidor”, inexistência de consentimento e direito à informação pelo consumidor



CRITÉRIO	APLICAÇÃO NO CASO	REFLEXO NA PENA
ENQUADRAMENTO DA INFRAÇÃO	<b>INSERIR OU MANTER REGISTROS</b> , EM DESACORDO COM A LEGISLAÇÃO, NOS CADASTROS OU BANCO DE DADOS DE CONSUMIDORES (ARTIGOS 43 E §§ E 39, CAPUT), QUANTO SUA <b>NATUREZA E GRAVIDADE</b>	FATOR DE MULTIPLICAÇÃO: 2
DANO INDIVIDUAL QUANTO À SUA EXTENSÃO		FATOR DE MULTIPLICAÇÃO: 5
FATURAMENTO DA LOJA HERING EXPERIENCE DO MORUMBI SHOPPING NO EXERCÍCIO DE 2019	R\$ 9.522.980,80	FATOR DE MULTIPLICAÇÃO 60;
RECEITA MENSAL BRUTA	(R\$ 793.581,73) UTILIZA-SE O <b>FATURAMENTO</b> DO ESTABELECIMENTO, UMA VEZ QUE OS <b>FATOS EM APURAÇÃO SE DERAM DENTRO DE SEU RECINTO, SEM DEMONSTRAÇÃO DE USO GENERALIZADO</b> PELO FORNECEDOR E <b>SEM ADOÇÃO DA PRÁTICA DE FORMA GENERALIZADA</b> DENTRO DE SEU MODELO DE NEGÓCIOS	CRITÉRIO 0,025%

PENA BASE: R\$  
117.534,00



AUSÊNCIA DE  
AGRAVANTES




ATENUANTES: : infratora primária, além de ter cessado a prática de forma a minimizar os seus efeitos danosos



DIMINUIÇÃO PELA METADE R\$ 58.767,00

FUNDO DE DEFESA DE DIREITOS DIFUSO



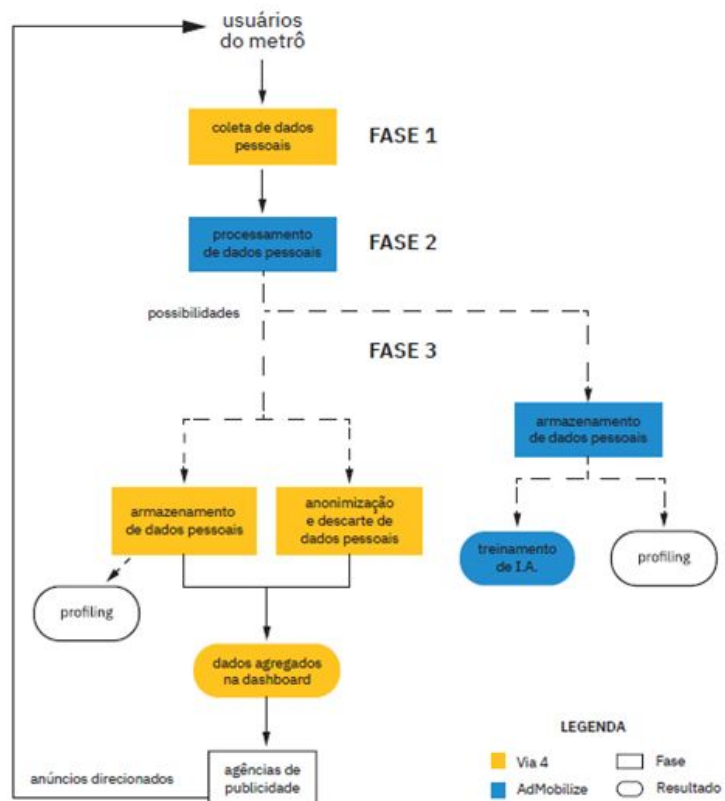


# Caso ViaQuatro (2018)

Tribunal de Justiça de São Paulo

- **Natureza do ilícito:** abuso de direito e adoção de “pesquisa compulsória” com base nas informações biométricas dos usuários do serviço de transporte
- **Fundamentação jurídica:** Código de Defesa do Consumidor, Código de Defesa dos Usuários dos Serviços Públicos e Constituição Federal
- **Desdobramentos:** tutela de urgência concedida e sentença favorável em primeira instância, com reconhecimento de violação dos direitos básicos dos consumidores e abuso de direito por parte da concessionária

## FASES DO TRATAMENTO DE DADOS



O artigo 37, §2<sup>a</sup> do Código de Defesa do Consumidor dispõe que: “*É abusiva, dentre outras a publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, se aproveite da deficiência de julgamento e experiência da criança, desrespeita valores ambientais, ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança.*”

Nota-se que a requerida deixou de impugnar especificamente os argumentos trazidos pelo *amicus curiae*, **principalmente quanto à proteção especial conferida à criança e adolescente, inclusive no que tange à preservação de sua imagem**, limitando-se tecer alegações genéricas sobre a ausência de circunstâncias envolvendo o tratamento de dados pessoais, já refutadas acima.

De todo o exposto, **inegável que conduta da requerida viola patentemente o direito à imagem dos consumidores usuários do serviço público, as disposições acerca da proteção especial conferida aos dados pessoais sensíveis coletados, além da violação aos direitos básicos do consumidor, notadamente à informação e à proteção com relação às práticas comerciais abusivas, daí porque o pedido de obrigação de não fazer consistente em não se utilizar de dados biométricos ou qualquer outro tipo de identificação dos consumidores e usuários do transporte público, sem a comprovação do devido consentimento do consumidor é procedente.**



# Caso Companhia Metropolitana (2022)

Tribunal de Justiça de São Paulo

- **Natureza do ilícito:** implementação de novo parque de câmeras com reconhecimento facial sem avaliação de impacto e sem considerar riscos para população vulnerável
- **Fundamentação jurídica:** Constituição Federal e Lei Geral de Proteção de Dados Pessoais
- **Desdobramentos:** tutela de urgência concedida com suspensão da contratação de empresa responsável pela implementação de novo parque de câmeras. Liminar foi suspensa pelo TJSP. Caso vai para perícia técnica.





## Caso Hapvida (2022)

Procon AM

Procon MA

- **Natureza do ilícito:** implementação de comprovação de identidade por meio de reconhecimento facial para realização de exames e procedimentos diversos por plano de saúde.
- **Fundamentação jurídica:** conduta lesiva à dignidade das crianças com Transtorno de Espectro Autista, e ao CDC.
- **Desdobramentos:** Condenação no Procon/AM e a suspensão da biometria facial em pessoas do espectro autista pelo Procon/MA.



# Consignado

A instituição financeira apresentou os instrumentos da contratação do cartão de crédito consignado (fls. 55/71), um documento intitulado “Recibo de PAG0143 Reserva” (fl. 72) e as faturas de fls. 73/76.

Ora, malgrado o entendimento contrário, depreende-se dos autos não haver prova suficiente acerca dos termos do indigitado contrato, porquanto, embora o demandado defenda a regularidade da assinatura digital, por meio de biometria facial, certo é que não foram indicados os parâmetros utilizados para aferição do suposto aceite da autora.

Sequer há os dizeres “assinado digitalmente” ou expressão semelhante na cédula de crédito bancário que pudesse confirmar o aceite da demandante. Nem mesmo a certificação digital que pudesse permitir conferência foi comprovada nos autos, limitando-se a instituição financeira a apenas colocar uma foto do cliente como se assinatura fosse.

Mesmo que a fotografia da parte em sua carteira de identidade não destoa daquelas que constantes do instrumento contratual, isso não basta para

# Consignado do INSS será liberado a distância com uso de biometria

Bancos deverão adequar ferramentas para conceder empréstimo sem beneficiário precisar ir a uma agência



Cristiane Gercina

**SÃO PAULO** O [crédito consignado](#) do [INSS \(Instituto Nacional do Seguro Social\)](#) deve passar a ser liberado por meio de biometria ainda neste semestre. O instituto prepara instrução normativa com nova regulamentação da medida, que está em fase de preparação nos bancos.

O objetivo é permitir a contratação do empréstimo consignado a

## **Pontos de atenção:**

- **Ressignificação da proteção de dados pessoais pelo prisma constitucional**
- **Ideia de que Estado e setor privado possuem “obrigações positivas” de mitigar riscos aos direitos fundamentais**
- **Tutelas de remoção do ilícito com orientação precaucionária: foco em eliminar o ilícito e não necessariamente buscar ressarcimento**
- **Maior colaboração entre sistema de justiça e organizações da sociedade civil**
- **Expansão da gramática de direitos básicos dos consumidores de serviços públicos (concepção abrangente sobre “consumidores”)**



**dataprivacybr.org**

**derechosdigitales.org**

[zanatta@dataprivacybr.org](mailto:zanatta@dataprivacybr.org)

[michel.souza@derechosdigitales.org](mailto:michel.souza@derechosdigitales.org)

Esta apresentação é licenciada em **Creative Commons CC-BY-NC 4.0**. Você pode utilizar, recriar e expandir para fins não-comerciais, desde que citada a fonte.