São Paulo, 13 de maio de 2020.

À Secretaria Nacional do Consumidor
Departamento de Proteção e Defesa do Consumidor
Coordenação-Geral de Consultoria Técnica e Sanções Administrativas

A/C: Juliana Oliveira Domingues, Diretora do Departamento de Proteção e Defesa do Consumidor

A/C: Leonardo Albuquerque Marques, Coordenador-Geral de Consultoria Técnica e Sanções Administrativas

Ref.: ***Resposta ao Ofício nº 95/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ - Processo nº 08012.001387/2019-11***

Prezada Senhora Diretora do DPDC,

Prezado Senhor Coordenador-Geral de Consultoria Técnica e Sanções Administrativas,

O Instituto Brasileiro de Defesa do Consumidor - Idec, já qualificado nos autos do Processo Administrativo em epígrafe, vem, respeitosamente, por seus advogados abaixo assinados, em cumprimento ao definido no teor do Despacho nº 188/2020/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ, que deferiu o pedido de ingresso do Idec como terceiro interessado nos presentes autos, apresentar a presente manifestação que, em tópicos simplificados, têm a finalidade de expor um resumo imprescindível para o conhecimento da demanda, para fins de subsidiar e reforçar, ainda mais, os argumentos expostos e comprovados na carta enviada por este Instituto, em 15/08/2019, como Resposta ao Ofício 159/2019/CSA-SENACON, e nos demais documentos que já constam nos autos, nos termos que passa a expor.

Ressaltamos que o interesse do Idec pelo caso tem como pano de fundo uma atuação consistente da organização neste tema. Em 2018, o Instituto protocolou a primeira Ação Civil Pública no Brasil sobre reconhecimento facial[1], utilizando-se como fundamento jurídico o direito constitucional, em interpretação em conjunto com o direito consumerista, antes mesmo de entrar em vigor a Lei Geral de Proteção de Dados - LGPD, a Lei Federal nº 13.709/18. Ao

[1] Processo nº 1090663-42.2018.8.26.0100 da 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo. C.f. https://idec.org.br/noticia/idec-vai-justica-contra-coleta-de-emocoes-de-usuarios-do-metro-de-sp.

longo do ano de 2019 também monitoramos a implementação da tecnologia pelo setor privado, enviando cartas para diversas empresas[2], questionando o cumprimento dos direitos do consumidor no tocante ao reconhecimento facial, tendo em vista os grandes riscos que a tecnologia apresenta.

O emprego de tecnologia de reconhecimento facial tem se intensificado ao redor do mundo, trazendo consigo grandes investidas para sua regulação, com estabelecimento de parâmetros para um uso adequado, ou até mesmo através de moratórias ou banimentos[3]. A preocupação decorre dos graves riscos às liberdades civis e direitos fundamentais, uma vez que a tecnologia utiliza dados sensíveis dos indivíduos analisados, podendo servir como ferramenta de controle e ocasionar práticas abusivas, discriminações e incidentes de vazamentos. O caso da Hering se destaca pelo alto grau de impacto sobre a esfera íntima do consumidor, com a utilização de tecnologias invasivas capazes de detectar gênero, faixa etária, emoção e movimentação dentro da loja, somado à grave falta de informação ao consumidor.

Em meio à crescente digitalização de todos os aspectos da relação de consumo, incluindo as estratégias de publicidade baseadas no comportamento do consumidor, a Secretaria Nacional do Consumidor - Senacon - tem papel importantíssimo para a definição e proteção dos direitos básicos do consumidor, o que demonstra a relevância do caso para o estabelecimento dos padrões necessários para garantia da defesa efetiva dos consumidores e prevenção da reincidência da prática pela própria empresa e por outras empresas**.**

Por isso, a presente manifestação é dividida nos seguintes tópicos: (i) breve síntese deste procedimento administrativo; (ii) proteção constitucional dos dados dos consumidores; (iii) definição de reconhecimento facial e por que o sistema utilizado não realiza apenas detecção facial; (iv) o reconhecimento facial pressupõe tratamento de dados pessoais, mesmo que posteriormente anonimizados; (v) violação do direito à informação e da necessidade de consentimento; (vi) a vulnerabilidade do consumidor como pressuposto de todas relações de

[2] C.f. https://www.tecmundo.com.br/seguranca/142100-idec-notifica-itau-quod-99-uso-reconhecimento-facial.htm.

[3] São exemplos: na França, proibiu-se o uso de reconhecimento facial em escolas. Já nos Estados Unidos da América, foi aprovada no Estado de Washington uma lei que regula o uso para entidades governamentais, proibindo seu uso para ameaçar liberdades democráticas e civis, disponível em: https://app.leg.wa.gov/billsummary?billnumber=6280&year=2019&initiative=False&utm_source=Mailing+Seman%C3%A1rio&utm_campaign=2f7295444d-EMAIL_CAMPAIGN_2020_02_04_10_03_COPY_01&utm_medium=email&utm_term=0_723d7d1345-2f7295444d-228035981. Outras cidades americanas proibiram o uso para segurança pública, como São Francisco, Berkley, Okland, Summerville, além do governo da California ; C.f. https://www1.folha.uol.com.br/ilustrissima/2019/12/movimento-por-banir-uso-de-reconhecimento-facial-cresce-no-mundo.shtml.

consumo; (vii) do abuso de direito e violações ao Código de Defesa do Consumidor; (viii) conclusões sobre as práticas abusivas perpetradas.

1. BREVE SÍNTESE DO PROCEDIMENTO

Trata-se de procedimento administrativo instaurado de ofício pelo Departamento de Proteção e Defesa do Consumidor (DPDC), em face da empresa Cia. Hering, destinado a averiguar práticas abusivas da empresa por conta de tecnologias instaladas em sua loja localizada no Shopping Morumbi (São Paulo - SP), que realizam o reconhecimento facial e mapeamento de calor para análise dos dados pessoais de seus clientes.

A averiguação foi instalada após o conhecimento deste DPDC de investigação realizada por este Instituto sobre o caso em tela. Em sua resposta de 29/07/2019, a empresa afirmou que as tecnologias utilizadas não realizavam tratamento de dados pessoais, uma vez que todos os dados são anonimizados e agrupados de modo a produzir apenas dados estatísticos, informando que não mais possuía a tecnologia em questão, além de informar que caso viesse a se decidir por utilizar alguma tecnologia semelhante em suas lojas, o faria em respeito ao CDC e à LGPD. Na sequência, em 15/08/2019, instado por meio do Ofício 159/2019/CSA-SENACON, o Idec apresentou informações acerca da investigação conduzida e enviou cópia das documentações.

Ante os indícios de violação aos artigos 4º, incisos I e III; 6º, incisos II, III, IV e VI; 39, IV; e 43 do CDC, o então Diretor do DPDC acolheu a Nota Técnica nº 294/2019/CSA-SENACON/CGCTSA/DPDC/SENACON/MJ (SEI nº 9494076) elaborada pela Coordenação-Geral de Consultoria Técnica e Sanções Administrativas (CGCTSA), determinando a instauração de processo administrativo, em 30/08/2019.

Em 24/09/2019, houve reunião presencial no âmbito do Ministério da Justiça, com a presença dos membros da Senacon juntamente com os representantes da empresa, momento em que foram apresentados esclarecimentos pelo órgão público acerca da instauração do processo.

Em 27/09/2019, a empresa apresentou defesa no presente processo administrativo, com alguns esclarecimentos técnicos sobre as tecnologias "*video analytics*" e "*digital signage*", alegando que há uma diferença entre detecção facial e reconhecimento facial, de modo que as tecnologias seriam compatíveis com os direitos do consumidor e com a Lei Geral de Proteção de Dados. Em 16/12/2019, a empresa pediu a juntada de novo parecer elaborado pelo Instituto Brasileiro de Peritos.

Instada a requerer provas, a empresa declarou em 16/01/2020 que não havia interesse na produção de mais provas, requerendo nova audiência com esta Senacon. Então, foi intimada para impugnar a média da receita mensal bruta apontada, apresentando manifestação em 09/03/2020. Foi realizada nova audiência no âmbito deste processo em 24/03/2020, tendo a Representada protocolizado alegações finais na data de 23/03/2020.

Em 31/03/2020 foi deferida a participação do Idec no presente processo administrativo como terceiro interessado, nos termos do artigo 9º, incisos III e IV, da Lei nº 9.784, de 29 de janeiro de 1999.

É a síntese do necessário.

2. PROTEÇÃO CONSTITUCIONAL DOS DADOS DOS CONSUMIDORES

Antes de se passar para análise dos principais pontos deste caso, é necessário enfatizar as raízes constitucionais da proteção de dados, assim como o regime jurídico que tem regido às questões pertinentes à proteção de pessoais. No Brasil, não há dúvidas de que a proteção de dados pessoais é um direito decorrente do direito constitucional à vida privada e intimidade, conforme definido pela Constituição Federal[4].

Recentemente, o Supremo Tribunal Federal referendou esse entendimento, ao julgar medida liminar em face da Medida Provisória (MP) n. 954, de 2020, por meio da qual autorizou-se o **compartilhamento de dados pessoais** de consumidores de serviços de telefonia com o IBGE (Instituto Brasileiro de Geografia e Estatística) para fins de "produção estatística oficial". Em face da referida MP, foram propostas cinco Ações Diretas de Inconstitucionalidade[5], tendo sido deferida a medida liminar pela Relatora dos casos, Ministra Rosa Weber, em decisão que foi confirmada pela maioria do Plenário do STF, tendo sido vencido apenas o Min. Marco Aurélio.

Em sua decisão liminar, a Min. Relatora Rosa Weber defendeu que as informações "*relacionadas à identificação – efetiva ou potencial – de pessoa natural, configuram dados pessoais e integram, nessa medida, o âmbito de proteção das cláusulas constitucionais*

[4] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação";

[5] "propostas pelo Conselho Federal da Ordem dos Advogados do Brasil – OAB (ADI 6387), pelo Partido da Social Democracia Brasileira - PSDB (ADI 6388), pelo Partido Socialista Brasileiro – PSB (ADI 6389), pelo Partido Socialismo e Liberdade – PSOL (ADI 6390) e pelo Partido Comunista do Brasil (ADI 6393)." C.f. http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=442823.

assecuratórias da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII)."[6].

A Relatora enfatizou que é necessário respeitar aos preceitos fundamentais de liberdade individual, privacidade e livre desenvolvimento da personalidade individual. Ressaltou, ainda, que o adiamento da LGPD por meio da Medida Provisória 959, de 2020, para maio de 2021, faz com que todas as medidas relacionadas aos dados dos consumidores e cidadãos devam ser escrutinadas com maior cuidado, devendo-se adotar requisitos mínimos para respeito dos direitos constitucionais sobre dados pessoais.

Já o Min. Gilmar Mendes, em voto extremamente didático, após tecer comentários e considerações sobre a dogmática e tratamento doutrinário sobre a proteção de dados, afirmou que hodiernamente, a partir de interpretação da Constituição Federal, é possível entender "um verdadeiro direito fundamental à proteção de dados pessoais". Diante da evolução do conceito de privacidade e das novas tecnologias, o Min. Gilmar Mendes enfatiza que há um "*direito à autodeterminação informacional como um contraponto a qualquer contexto concreto de coleta, processamento ou transmissão de dados passível de configurar situação de perigo*"[7]. Nas palavras do Min. Gilmar Mendes,

> O direito fundamental à igualdade – enquanto núcleo de qualquer ordem constitucional – é submetido a graves riscos diante da evolução tecnológica. A elevada concentração de coleta, tratamento e análise de dados possibilita que governos e de empresas utilizem algoritmos e ferramentas de data analytics, que promovem classificações e esteriotipações discriminatórias de grupos sociais para a tomada de decisões estratégias para a vida social, como a alocação de oportunidades de acesso a emprego, negócios e outros bens sociais. Essas decisões são claramente passíveis de interferência por viesses e inconsistências que naturalmente marcam as análises estatísticas que os algoritmos desempenham.[8]

Ainda o Min. Ricardo Lewandoski inclusive ressaltou que o *"maior perigo para a democracia nos dias atuais não é mais representado por golpes de Estado tradicionais, perpetrados com fuzis, tanques ou canhões, mas agora pelo* ***progressivo controle da vida privada dos cidadãos****, levado a efeito por governos de distintos matizes ideológicos,* ***mediante a coleta maciça e indiscriminada de informações pessoais, incluindo, de maneira crescente, o reconhecimento facial****"*[9].

---

[6] ADI 6387 MC/DF, Rel. Min. Rosa Weber, decisão monocrática de 24 de abril de 2020, referendada pelo Plenário em 07 de maio de 2020. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf.

[7] Voto do Min. Gilmar Mendes: https://www.youtube.com/watch?v=t15mesEgqSU. Disponível em: https://www.conjur.com.br/dl/pandemia-reforca-necessidade-protecao.pdf.

[8] Ibidem, p. 10.

[9] Voto do Min. Ricardo Lewandowski: https://www.youtube.com/watch?v=t15mesEgqSU.

A referida decisão paradigmática do Supremo Tribunal Federal no julgamento da Medida Cautelar na ADI 6.387/DF, Rel. Min. Rosa Weber, confirma o que o Idec defendeu em sua manifestação preliminar neste procedimento, de que a proteção de dados pessoais dos consumidores deve-se dar a partir da interpretação conjunta dos direitos fundamentais garantidos pela **Constituição Federal** e das legislações federais, entre elas o **Código Civil** (em especial o Capítulo II, que trata dos direitos da personalidade), o **Código de Defesa do Consumidor** (em especial o capítulo "Dos Bancos de Dados e Cadastros de Consumidores"), a **Lei de Acesso à Informação** (em especial da seção V intitulada "Das Informações Pessoais"), o **Marco Civil da Internet** (Lei 12.965/2014) e a **Lei do Cadastro Positivo** (Lei 12.414/2011).

A sistematização jurídica da Constituição e da legislação Federal acima citada leva aos direitos básicos de transparência, na proteção das pessoas naturais e na definição do princípio da "autodeterminação informativa", enfatizado na importância do consentimento livre e informado decorre principalmente do disposto no CDC, na Lei do Cadastro Positivo e no Marco Civil da Internet (MCI).

3. UMA QUESTÃO PRELIMINAR: DEFINIÇÃO DE RECONHECIMENTO FACIAL E POR QUE A HERING NÃO REALIZA APENAS DETECÇÃO FACIAL

Em todas suas manifestações no procedimento administrativo, a empresa afirma que não realiza reconhecimento facial, mas apenas detecção facial. Para a empresa, reconhecimento facial se trata de um método automatizado de biometria utilizado apenas para criação de assinatura facial e a identificação de pessoas através de imagens ou vídeos, enquanto a detecção seria, sob sua ótica, método capaz de perceber a presença de faces numa imagem e extrair informações como gênero, raça e emoções.

Tais definições de reconhecimento e detecção facial são incompatíveis com a literatura técnica. Tanto é que a empresa não apresenta embasamento teórico e legal para dar suporte a suas alegações[10]. Conforme consenso na literatura técnica[11], **detecção facial é <u>apenas</u> contagem de rostos, sem atribuição de características como idade e gênero.** Trata-se de

[10] As respostas da empresa fazem referência a um blog educacional e à menção, não comprovada, a definições de autoridades de proteção de dados pessoais, as quais não foram especificadas.

[11] Jain, Anil K., and Stan Z. Li. *Handbook of face recognition*. New York: Springer, 2011. Disponível em: https://static.googleusercontent.com/media/research.google.com/pt-BR//pubs/archive/36368.pdf. DATA PROTECTION WORKING PARTY. *Opinion 02/2012 on facial recognition in online and mobile services.* [S.l.]. 2012. (00727/12/EN WP 192); COSERARU, R. *Facial Recognition Systems and their Data Protection Risks under the GDPR*. Tilburg University. Tilburg. 2017; ROWLEY, Henry A.; BALUJA, Shumeet; KANADE, Takeo. Neural network-based face detection. *IEEE Transactions on pattern analysis and machine intelligence*, v. 20, n. 1, p. 23-38, 1998; LEWINSKI, P.; TRZASKOWSKI, J.; LUZAK, J. Face and Emotion Recognition on Commercial Property under EU Data Protection Law. *Psychology & Marketing*, v. 33, n. 9, p. 729-746, Setembro 2016.

apenas uma das etapas necessárias para o reconhecimento facial. Da mesma forma, a concepção de reconhecimento facial da Hering é muito mais restrita que a definição técnica, uma vez que a identificação de pessoas é apenas uma das utilidades apresentadas pela tecnologia.

A Representada ainda tenta deslustrar o funcionamento da tecnologia implementada ao compará-la ao monitoramento manual, feito por um funcionário, do gênero e idade de seus clientes, revelando incompreensão da complexidade da sua operação, bem como do diferente grau de intrusão na esfera privada do indivíduo analisado por uma máquina e por uma pessoa. Se a capacidade de reconhecer e analisar rostos é trivial para um ser humano, a mesma categorização feita por uma máquina exige um processamento complexo de dados pessoais que só se tornou possível recentemente (e ainda é realizado com taxas de erros altas para determinados públicos[12]). Dessa forma, dada a confusão causada pela empresa, é fundamental esclarecer o funcionamento da tecnologia adotada.

O reconhecimento facial, uma das funcionalidades dos algoritmos classificatórios, passa ao menos por quatro etapas, sendo a detecção facial apenas uma delas.

A primeira etapa necessária é a **(1) *captura da imagem da pessoa***. A segunda etapa do reconhecimento facial, e somente esta, é a **(2) *detecção facial,*** trata-se de identificar o que é determinante para a análise, segmentando as faces do restante do quadro, como paisagem e objetos, ou seja, basicamente classifica-se a imagem em "face humana" ou "face não humana". Nota-se que **a única informação possível de se extrair na detecção facial é a contagem de rostos**.

Em seguida ocorre a **(3) *normalização***, por meio da qual as imagens selecionadas são padronizadas quanto a cor, rotação e iluminação, para minimizar fatores externos que podem alterar sua percepção. Essa etapa é essencial para permitir uma análise uniforme da imagem e a extração correta de seus atributos.

Somente a partir desta fase é possível realizar a **(4) *extração de atributos***, **em que os pontos de referência da face -** isto é, a forma, localização e distância entre os componentes faciais, como boca, nariz e sobrancelha - **são extraídos para a obtenção das informações úteis à análise pretendida**.

[12] Brendan F. Klare Noblis, Falls Church, U.S.A. ; Mark J. Burge ; Joshua C. Klontz ; Richard W. Vorder Bruegge ; Anil K. Jain. Face Recognition Performance: Role of Demographic Information. *IEEE Transactions on Information Forensics and Security.* Volume: 7, Issue: 6, Dec. 2012. Disponível em: https://ieeexplore.ieee.org/document/6327355. E BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. [S.l.]: [s.n.]. Disponível em: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Apenas após a quarta etapa da operação, em que os atributos da face foram extraídos e possivelmente agregados, é que a imagem e os dados biométricos coletados podem ser descartados. Sendo a quinta etapa o **(5a)** ***descarte do dados***, que tem como objetivo a categorização.

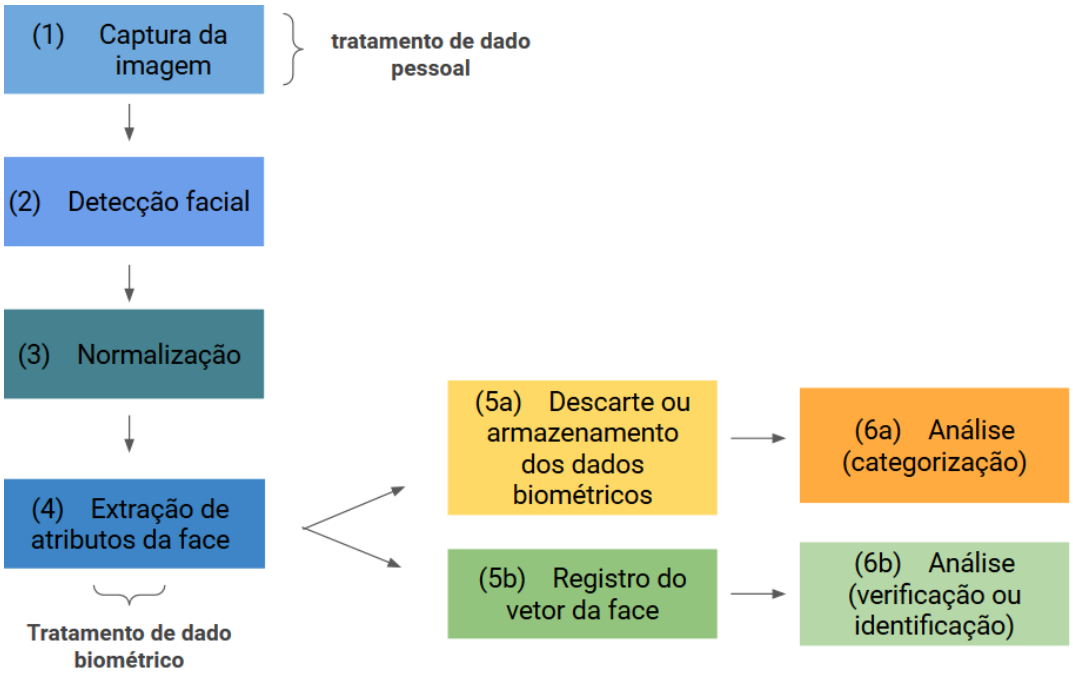
Por fim, a última etapa é a **(6)** ***análise dos dados obtidos***, que se trata da verificação de similaridades entre a amostra que se pretende analisar e um banco de dados previamente registrado no sistema. Ou seja, compara-se os pontos de referência da face de uma pessoa ou grupo a um banco de dados previamente classificado, de modo que seja possível analisar o gênero, idade e emoção desta pessoa ou grupo de pessoas.

Outro caminho possível seria, após a extração dos atributos da face (quarta etapa), realizar o (5b) registro do vetor da face, que permite a posterior comparação entre a imagem armazenada e aquela obtida em tempo real. Esta é somente necessária para duas das funcionalidades do reconhecimento facial, a autenticação (ou verificação) e a identificação de uma pessoa, a qual a Hering erroneamente considera como definição de reconhecimento facial.

No entanto, a tecnologia de reconhecimento facial apresenta três finalidades possíveis: autenticação, identificação e categorização. As duas primeiras intenções precisam passar pela etapa de registro do vetor da face (5b) e servem, respectivamente, para o reconhecimento pelo sistema de uma pessoa como ela mesma - como uma substituição de *login* - e para identificar um indivíduos com dados previamente armazenados ou também para armazenar dados para novas identificações. Já a terceira utilidade trata-se de processo em que se extrai características da imagem do indivíduo para categorizá-lo de acordo com classificações definidas, por exemplo, humor, idade, gênero, vestimenta, dentre outras.

Todo o processo de funcionamento do reconhecimento facial, de acordo com as três finalidades possíveis, pode ser resumido da seguinte maneira[13]:

[13] Imagem e explicações extraídas do Jain, Anil K., and Stan Z. Li. *Handbook of face recognition*. New York: springer, 2011.



Conforme amplamente comprovado nestes autos do procedimento administrativo e enfatizado pelo Idec em sua manifestação preliminar (fls. 15-28), os sistemas adotados pela representada, *Digital Signage* e *Video Analytics*, realizam, além de um controle demográfico, diagnóstico de gênero e idade de seus clientes. Ressalta-se que o sistema de reconhecimento facial da *Video Analytics* ainda é capaz de identificar as emoções dos consumidores no caixa da loja.

Conforme detalhado acima, para a obtenção dessas informações estatísticas de seus consumidores, era necessário realizar: (i) a captura da imagem, (ii) detecção facial, (iii) normalização da imagem obtida, (iv) a extração de atributos da face e, somente então, (v) a análise dos dados obtidos. **Ambos sistemas adotados, portanto, vão muito além da simples detecção facial.**

É possível **afirmar sem sombra de dúvidas com fundamento em toda a literatura técnica disponível que a empresa realizava reconhecimento facial, com fins de categorização**. A implementação dessa tecnologia pressupõe o tratamento de dados pessoais, como se verá a seguir.

4. O RECONHECIMENTO FACIAL PRESSUPÕE TRATAMENTO DE DADOS PESSOAIS, MESMO QUE POSTERIORMENTE ANONIMIZADOS

A Representada insiste em classificar a tecnologia adotada como detecção facial no intuito de simplificá-la e maquiar o tratamento de dados pessoais que intrinsecamente ocorria na loja conceito do shopping Morumbi.

No entanto, **independentemente da nomenclatura adotada, existe tratamento de dados pessoais, uma vez que, para a obtenção da análise almejada sobre gênero, faixa etária e emoção dos consumidores, mesmo que estatisticamente, é necessária a *coleta* da imagem** (primeira etapa do reconhecimento facial), bem como sua *utilização, acesso, processamento, modificação* e *eliminação.*

Todos esses processos de utilização da imagem, que são definidos como tratamento de dados pessoais pela LGPD[14], são necessários para as etapas de funcionamento do reconhecimento facial, isto é, captura da imagem, detecção facial, normalização da imagem, extração de atributos e, por fim, seu descarte.

A imagem dos indivíduos analisados pelo reconhecimento facial é um dado pessoal[15]. Assim, a ampla utilização necessária da imagem dos consumidores para o funcionamento dos sistemas de *Digital Signag*e e *Video Analytics*, implica tratamento de dado pessoal. **A posterior eliminação da imagem e anonimização das informações extraídas não imuniza a empresa, tampouco apaga o fato de que houve tratamento de dados pessoais sem qualquer informação, transparência e consentimento dos consumidores.**

A própria empresa assume, em sua manifestação de 27/09/2019 que há coleta e processamento da imagem dos clientes, de modo que há tratamento de dados pessoais:

> "No caso da ferramenta *vídeo analytics*, **o processamento das imagens é feito no computador e, <u>após</u> o envio dos resultados anonimizados ao servidor, nenhum dado permanece armazenado no computador** localizado no ambiente de loja". (p. 21)
>
> "Conforme consta no parecer do IBP, **as imagens coletadas são destruídas logo <u>após</u> a geração dos dados estatísticos"** (p. 28)

[14] Art. 5º Para os fins desta Lei, considera-se: X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[15] Art. 5º. Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

Como se sabe, a imagem é característica protegida pelo ordenamento jurídico, inclusive anteriormente à própria LGPD. O artigo 20 do Código Civil proíbe a utilização da imagem da pessoa, sem sua autorização, para fins comerciais, devendo o dispositivo ser entendido como o direito da pessoa não ter sua imagem mercantilizada, em proveito de outros interesses que não os próprios, independente identificação específica do indivíduo[16].

Da mesma forma, o Código de Defesa do Consumidor estabelece em seu artigo 43 o direito de acesso à informação e de comunicação de dados pessoais armazenados de consumidores, o que não foi respeitado pela Representada. Como parâmetro para análise do caso, por exemplo, a LGPD estabelece bases legais para a utilização de dados pessoais, que não estão presentes.

Para além do tratamento do dado pessoal em decorrência do tratamento da imagem dos consumidores, **todo reconhecimento facial - incluindo, portanto, os sistemas utilizados pela Representada - envolve tratamento de dado biométrico.** Ainda que supostamente o objetivo final da tecnologia não fosse a identificação de uma pessoa determinada, para que aconteça o diagnóstico de gênero, faixa etária e emoção, é necessária a **extração de atributos da face**, isto é, a identificação e armazenamento das características geométricas da face com a forma, localização e distância dos componentes faciais (como boca, nariz e sobrancelha).

Esses pontos faciais precisam ser armazenados para que seja possível a análise posterior, através da comparação entre os dados obtidos com um banco de dados previamente registrado no sistema. Os pontos de face de um consumidor serão comparados com o banco de dados do algoritmo, para determinar se se trata de uma mulher ou homem, qual faixa de idade e sob qual emoção se encaixa, dentre as categorias estabelecidas.

Dessa forma, **para extrair informação do consumidor analisado é necessário: *coletar, classificar, utilizar, processar, armazenar* e *avaliar* os seus pontos de referência da face**, além da posterior ***eliminação*** destes dados. São todos processos que implicam tratamento de dados pessoais dos consumidores, conforme art. 5º, X, da LGPD c/c Lei nº. 12.965/2014 - Marco Civil da Internet - art. 7º, inc VIII.

A legislação brasileira, apesar de enquadrar o dado biométrico como dado pessoal sensível, não traz sua definição, de modo que se pode ter como referência a definição do

[16] "[O] direito à imagem é o direito de não vê-la mercantilizada, usada, sem o seu exclusivo consentimento, em proveito de outros interesses que não os próprios ". E acrescenta que " o risco à integridade moral do sujeito, objeto do direito à privacidade, não está no nome, mas na exploração do nome, não está nos elementos de identificação que condicionam as relações privadas, mas na apropriação dessas relações por terceiros a quem elas não dizem respeito" (FERRAZ JUNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito, Universidade de São Paulo, vol. 88, 1993, p. 444-50)

Regulamento Geral de Proteção de Dados europeu (art. 4º, item 14, Regulamento 2016/679, RGPD), segundo a qual são "*dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos*".

Portanto, os **pontos de referência da face são dados biométricos, uma vez que a localização, formato e distância desses atributos faciais são características físicas de uma pessoa singular que permitem a sua identificação única**.

Por considerar um tratamento de maior risco, a LGPD estabelece uma abordagem mais rígida para o tratamento de dados pessoais sensíveis, como, por exemplo, a impossibilidade de realizá-lo com base no legítimo interesse e o maior incentivo à produção de relatório de impacto à proteção de dados.

Assim, novamente, percebe-se que o principal argumento da Representada - de que não haveria tratamento de dados pessoais, porque não há identificação única dos consumidores, uma vez que são dados estatísticos e anonimizados - é completamente inválido. **O funcionamento da tecnologia de reconhecimento facial pressupõe o tratamento de dados pessoais (a imagem) e de dados pessoais sensíveis (dados biométricos, no caso os dados de referência da face)**.

Por fim, mesmo que se adotasse a concepção equivocada da empresa de que só há reconhecimento facial quando o fim é a identificação ou verificação do indivíduo - o que se admite apenas para fins de debate -, deve-se considerar que **o consumidor é facilmente identificável a partir do cruzamento de dados pessoais em posse da empresa.**

A Representada realiza o tratamento, através dos operadores de dados *Video Analytics* e *Digital Signage* ou por ela própria, dos seguintes dados pessoais: **localização** e trajeto (por meio de mapa de calor detecta sinais de celular para avaliar regiões mais quentes da loja); **gênero, faixa etária e humor** de quem passa pelo caixa (por reconhecimento facial); gênero e faixa de idade de quem assiste ao painel de publicidade (por reconhecimento facial). Além disso, não há dúvidas de que também faz tratamento de **dados de pagamento**, como cartão de crédito e **dados de cadastro**, como nome completo, endereço e data de nascimento.

Com todas essas informações em mãos, a empresa poderia facilmente identificar unicamente cada consumidor (mesmo considerando que não seja possível realizá-lo apenas pelo reconhecimento facial realizado) e, a partir disso, estabelecer um profundo perfil deste consumidor e de sua trajetória. Para ilustrar, pode-se inferir que: o consumidor "A" entrou na

loja, comprou determinada roupa, ficou vinte minutos no provador, demonstrou alegria no caixa e conectá-lo aos dados cadastrais e de pagamento.

Ressalta-se que **é desnecessária a comprovação ou não de que os dados pessoais são cruzados de modo a permitir a reversão do processo de anonimização,** uma vez que a LGPD estabelece que dados anonimizados serão considerados dados pessoais quando o processo de anonimização **puder ser revertido** com esforços razoáveis[17]. Pode-se considerar que **os esforços para identificação são razoáveis, tendo em vista que são necessários somente dados em posse da empresa, isto é, *utilizando exclusivamente meios próprios***.

Assim, mesmo que o caso em análise seja anterior à vigência da LGPD, os conceitos, deveres e direitos estabelecidos pela Constituição Federal, pela legislação brasileira e pela jurisprudência pátria podem servir como parâmetro para ilustrar a complexidade d**o sistema de reconhecimento facial e como ele implica extrema inserção não autorizada na esfera da vida privada do consumidor, através da extração, análise e exploração de elementos da intimidade e particularidade do indivíduo**.

Mesmo que essas informações sejam posteriormente anonimizadas e agregadas, deve-se considerar que a sua exploração sem base legal não pode ser apagada, tampouco desconsiderar a esfera difusa de proteção da privacidade e da proteção de dados pessoais. Referente intrusão na esfera privada do consumidor, como já exposto por este Instituto, acarreta violação dos direitos da personalidade, protegidos constitucionalmente, e dos direitos do consumidor, como será descrito nos tópicos seguintes.

5. HÁ VIOLAÇÃO DO DIREITO À INFORMAÇÃO E À NECESSIDADE DE CONSENTIMENTO

Em sua manifestação, a Representada insiste em afirmar que o consentimento do consumidor não é necessário, visto não se tratar de um dado pessoal, não havendo incursão nos direitos de personalidade ou intimidade do consumidor.

Como já refutado, resta claro que a tecnologia operada pela empresa realiza, de fato, **tratamento de dado pessoal**. Não apenas de dado pessoal, mas de **dado pessoal sensível**, visto

[17] Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido.
§ 1º A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios.

que a tecnologia é capaz de analisar a imagem de uma pessoa com precisão suficiente para extrair seus pontos de referência na face e, consequentemente, inferir as suas reações emocionais.

Havendo tratamento de dados pessoais, não há qualquer sentido na alegação de que o sistema não incorre na dimensão dos direitos de personalidade do consumidor. O consumidor é parte vulnerável na relação de consumo e se sujeita aos riscos de ter ferida a sua autonomia quanto à possibilidade de discriminação no mercado de consumo. Isso acontece por meio de atividades de tratamento de dados que ocorrem com suas informações pessoais por tecnologias as quais muitas vezes o consumidor sequer é capaz de entender plenamente. Nesse sentido, diante da ampla vulnerabilidade técnica, o consumidor pode ser tido como hipervulnerável.

O direito do consumidor à proteção de dados visa justamente tutelar essa hipervulnerabilidade, envolvendo, conforme ensina Laura Schertel Mendes, uma dupla dimensão: "*(i) a **tutela da personalidade do consumidor** contra os riscos que ameaçam a sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais; e (ii) a **atribuição ao consumidor da garantia de controlar o seu fluxo de dados** na sociedade"*[18].

O **consentimento é o elemento que garante ao consumidor a retomada da sua autonomia, por meio do controle sobre o fluxo de suas informações**, isto é, a sua **autodeterminação informativa**.[19]

Frisa-se, ainda, que não apenas o consentimento, mas também critérios como a **boa-fé objetiva, as expectativas legítimas do consumidor, e os impactos e riscos do tratamento de dados** para o consumidor devem ser observados por qualquer atividade de tratamento de dados pessoais.[20]

Não parece ser este o caso em tela, no qual a Representada inseriu as câmeras em seu estabelecimento comercial, que não eram aquelas de segurança (as quais haver-se-ia uma expectativa legítima de estarem instaladas), sem pedir qualquer autorização para se utilizar das imagens dos consumidores ou prestar informação adequada aos consumidores ali presentes. Embora a empresa alegue que a tecnologia pretendia melhorar a experiência do consumidor, não se deve fazer isso em detrimento de sua própria autonomia, de sua própria vontade. É por

[18] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor* - Linhas gerais de um novo direito fundamental. p. 203.
[19] Idem, p. 60.
[20] Idem, lp. 204

este motivo que pesquisas de mercado e de estilo de vida em geral, mesmo que feitas para melhoria de serviços, precisam ser informadas e consentidas pelo consumidor:

> *"(...) as pesquisas de mercado e de estilo de vida tornam-se um meio legítimo de coleta de dados,* ***desde que se apresente ao consumidor claramente a finalidade da coleta e como esses dados serão processados. Ademais, é necessário que a empresa obtenha o consentimento expresso do consumidor****, caso tenha interesse em compartilhar ou ceder tais dados a terceiros ou de utilizá-los com a finalidade de marketing direto."* [21]

Ainda, para alegar que o consentimento não seria sempre obrigatório nas relações de consumo, a empresa cita a Súmula nº 550 do e. Superior Tribunal de Justiça, a qual foi editada a partir do julgamento do Recurso Especial nº 1.419.697/RS. No julgamento, a Corte entendeu pelo afastamento da necessidade de consentimento do consumidor na utilização de dados estatísticos em sistemas de *credit score*, ou pontuação de crédito. A Representada alega que ambos os casos seriam análogos, devendo portanto o consentimento ser dispensado.

A analogia entre os dois casos, porém, também não tem sentido lógico.

Na decisão do Superior Tribunal de Justiça, o relator Min. Paulo de Tarso Sanseverino entendeu que a pontuação de crédito não seria um banco de dados. A pontuação consistiria em uma **metodologia de avaliação de risco**, que usaria **apenas informações publicamente disponíveis**, por exemplo, em registros públicos, protestos e ações judiciais.

Não há qualquer semelhança, assim, com atividades quaisquer de tratamento de dados a partir de tecnologias que reúnam informações sobre a imagem de consumidores de maneira a extrair características particulares sobre ele no ambiente privado de uma loja - informações as quais, não há dúvidas, consistem em bancos de dados. Ademais, enquanto o sistema de pontuação de crédito é atividade que, ao menos em teoria, deve servir para fornecer maior segurança jurídica e financeira aos concedentes de crédito, sendo assim considerada, nos termos da decisão, indispensável para a vida econômica atual, situação muito diversa é a do tratamento de dados para *marketing* direcionado.

6. A VULNERABILIDADE DO CONSUMIDOR COMO PRESSUPOSTO DE TODAS RELAÇÕES DE CONSUMO

Outra alegação referente ao direito do consumidor que está totalmente em desacordo com a legislação brasileira é de que as práticas abusivas descritas no art. 39, do CDC, seriam

[21] Idem, p. 100.

aplicadas somente nos casos de consumidores hipossuficientes, ainda mais a prática de se prevalecer da "*fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços*". Não há sentido na argumentação da Representada.

Como é sabido, a Constituição Federal (art. 5º, inc. XXXII; art. 170, inc. IV e V) e o próprio Código Consumerista (art. 4, *caput*, CDC) buscam equilíbrio entre direitos do consumidor, direitos da liberdade econômica e o desenvolvimento tecnológico e inovação. A proteção ao livre mercado deve, como bem expressa o Código, visar à harmonia nas relações de consumo de modo que as práticas comerciais não podem violar os direitos básicos do consumidor (saúde, segurança, informação, sua dignidade etc.), dispondo o Código o princípio da vulnerabilidade do consumidor nas relações de consumo (art. 4º, inc. I, CDC).

A vulnerabilidade do consumidor é presumida, tendo como fundamento a assimetria de informação existente entre o fornecedor e seu cliente, o que é ainda mais exacerbado frente ao uso de novas tecnologias, especialmente quando há o esforço ativo da empresa para maquiar seu uso. O art. 39, IV, do CDC diz respeito à vedação de práticas que se aproveitem de consumidores hipossuficientes que não possuem total discernimento para avaliar o produto ou serviço oferecido, sendo aplicável a todos os consumidores, até mesmo porque, ao não seguir o direito à informação clara e adequada, a empresa tenta prevalecer ante a ignorância do consumidor, pois o consumidor ignora, ou seja, não sabe, da existência dessa tecnologia e dos riscos que lhe são inerentes.

7. DO ABUSO DE DIREITO E VIOLAÇÕES AO CÓDIGO DE DEFESA DO CONSUMIDOR

Como ficou demonstrado nesta manifestação, o tratamento ilícito de dados pessoais, é necessário para o funcionamento da tecnologia de reconhecimento facial, acarretando inserção não autorizada da representada na esfera privada de seus consumidores. No entanto, a despeito da importância do debate acerca da operação técnica do reconhecimento facial e da interpretação dos conceitos da proteção constitucional de dados pessoais e da LGPD, a empresa violou os direitos do consumidor, empregando práticas abusivas que se aproveitam de sua posição de fornecedor, conforme relatado nos tópicos a seguir.

7.1. Da pesquisa de opinião compulsória

A empresa extrai informações referentes ao comportamento de seus consumidores, através da instalação, sem qualquer informação, de sistemas tecnológicos complexos em sua loja. Os dados extraídos (independente de anonimização posterior) são utilizados para incorporar valor e precisão as suas análises mercadológicas e publicitárias. Não se duvida que

conhecer todos os passos, reações e movimentos dentro da loja - a trajetória do consumidor - é um ativo valiosíssimo para qualquer empresa e análise de *marketing*.

No entanto, as informações provenientes do consumidor não podem ser exploradas economicamente sem qualquer autorização e informação ao consumidor, sob pena de, para além da violação à privacidade dos consumidores, implicar enriquecimento sem causa.

A empresa extrai informações (gênero, idade, emoção e movimento na loja) de seus consumidores para inferir análises e opiniões sobre seus produtos e atendimento. Ainda, as informações são extraídas compulsoriamente de todos os consumidores que adentram a loja. Dadas as semelhanças, são inócuas as tentativas da empresa de desvincular seu experimento a uma pesquisa de opinião compulsória, argumentando que pesquisas de opinião são realizadas com coleta de dados estruturada e critérios metodológicos específicos, alta precisão e em larga escala.

Ora, o reconhecimento facial pressupõe, por sua lógica intrínseca, uma coleta estruturada de dados, com metodologias e critérios específicos, conforme detalhado nas etapas de funcionamento da tecnologia no item três desta manifestação. A alta precisão dos dados coletados (pontos da face), por exemplo, é essencial para a extração correta dos atributos. Assim como a análise dos dados extraídos, em comparação com a base de dados do algoritmo, depende de metodologia específica fornecida pela *Digital Signage* e *Video Analytics*. Por fim, ainda que em menor abrangência de público que uma pesquisa de opinião clássica, o grau de profundidade sobre a intimidade do consumidor - que tem sua emoção extraída sem sequer perceber - é muito maior. **É nítida, portanto, a realização de pesquisa de mercado compulsória**.

7.2. Do abuso de direito e violação aos direitos do consumidor

A Representada pôde realizar toda essa operação, em valorização a sua marca, graças a sua posição de fornecedora, se aproveitando (i) da assimetria de informação inerente à relação de consumo e exacerbada com o uso de tecnologias e (ii) da marca e confiança que detém frente a seus consumidores.

A **assimetria informacional entre consumidores e fornecedores é agravada com o emprego de tecnologias** opacas aos consumidores, tanto por seu funcionamento técnico complexo, quanto pelos segredos comerciais envolvidos nos algoritmos. A omissão ao consumidor também é acentuada pelo fato de que muitas dessas tecnologias de monitoramento são realizadas remotamente, sem que o consumidor, por exemplo, ativamente insira a mão para leitura da digital.

Todos esses fatores contribuem para revelar a gravidade da violação ao direito de informação na pesquisa compulsória realizada pela Representada. Sem informar o consumidor sobre a operação da tecnologia e dos riscos envolvidos, **a empresa falha em informar adequadamente sobre as características e riscos da prestação do serviço, em desrespeito ao art. 6º, III do CDC**.

A violação do dispositivo não é casual, mas fundamental para **tolher o direito de escolha do consumidor (art. 6º, II do CDC), uma vez que muitos consumidores poderiam optar por não entrar na loja, se devidamente informados do monitoramento realizado e de seus riscos.** Incorrendo, consequentemente, em **ofensa ao art. 4º, IV do CDC**, por falhar em informar os consumidores sobre seus direitos.

Assim, a Representada se aproveita da posição de vulnerabilidade do consumidor que entra em sua loja com a simples intenção de comprar roupas e acaba contribuindo com uma pesquisa de opinião compulsória, sem seu conhecimento. Em outras palavras, **a empresa se *prevalece da ignorância* do consumidor, perante a incompletude de informações acerca do fornecimento de produto, para aprimorar suas vendas**. **Configura-se, portanto, prática abusiva vedada pela legislação, conforme art. 39, IV do CDC**.

Nesse sentido, a conduta da Representada também constitui **prática abusiva por exigir do consumidor vantagem manifestamente excessiva, ao obrigá-lo a repassar suas opiniões (expressadas por suas reações) para aprimoramento da publicidade da marca, em clara violação ao art. 39, V do CDC**. A prática exige vantagem excessiva, pois, nos termos da definição presente no art. 51, §1º do CDC: (i) ofende os princípios fundamentais do ordenamento jurídico, em especial o direito à privacidade do consumidor; (ii) restringe direitos fundamentais ao contrato de compra e venda, em especial, direito de escolha e de informação; e (iii) é excessivamente onerosa ao consumidor, uma vez que ignora completamente seus interesses.

Há, portanto, **manifesta violação à proteção do consumidor com métodos comerciais desleais e práticas abusivas, previstas no art. 6º, inc. IV do CDC**.

Assim, mesmo que se considere que não há tratamento de dados pessoais - o que se admite apenas para efeitos de debate -, **é evidente que a empresa ultrapassa os limites concedidos para exercício da atividade econômica, pela boa-fé e pelos bons costumes, constituindo verdadeira prática abusiva.** Dessa forma, se a empresa estaria exercendo seu direito ao vender os produtos e avaliar o nível de satisfação de seus clientes com consentimento, nitidamente os limites desse direito são ultrapassados quando se aproveita da ignorância e boa-fé dos consumidores e da capacidade das tecnologias de monitoramento remotas, para aprimorar a análise de publicidade da empresa, de maneira compulsória.

A conduta da empresa configura abuso de direito, partindo-se de critérios estabelecidos em precedente do Superior Tribunal de Justiça, o Recurso Especial nº 1.348.532/SP**,** conforme detalhado na manifestação deste Instituto de 15/08/2019.

Embora o precedente tenha como objeto a abusividade em cláusula em contrato de adesão que permitia o compartilhamento de dados pessoais a terceiros - como apontado pela Representada -, é evidente sua relação com o presente caso. **Ambos tratam do direito do consumidor de controlar os dados gerados a partir do seu comportamento** e, em correspondência, do direito da empresa de utilizar esses dados em seu proveito sem consentimento, seja no momento do compartilhamento ou na coleta e processamento dos dados. Em outras palavras, ambos casos tratam do direito à privacidade do consumidor[22].

É notório, portanto, a presença de desvio de finalidades do direito inicialmente concedido à fornecedora, restando configurada prática abusiva pelo Código Civil e Código de Defesa do Consumidor.

7.3. O desequilíbrio entre direito do consumidor e desenvolvimento tecnológico

Dessa forma, as inovações tecnológicas implementadas pela Representada falharam em alcançar equilíbrio entre os interesses e direitos dos consumidores com o desenvolvimento econômico e tecnológico, princípio previsto no art. 4º, III do CDC.

As inovações tecnológicas podem ser benéficas ao consumidor, não é o caso, contudo, da tecnologia de reconhecimento facial perpetrada pela Representada que se baseia na prática de condutas abusivas, com violação ao direito de informação e escolha do consumidor. Viola-se, portanto, a previsão constitucional de que a ordem econômica observe a defesa do consumidor (art. 170, CF/88).

7.4. Da prevenção e reparação de danos ao consumidor

Por fim, as violações ao direito de informação e de escolha e as práticas abusivas culminam na violação do direito do consumidor de "prevenção e reparação de danos patrimoniais e morais, individuais, coletivos e difusos", previsto no art. 6º, VI, do CDC.

O reconhecimento facial apresenta diversos riscos, uma vez que envolve tratamento de dados pessoais sensíveis, os dados biométricos. Há **o risco de vazamento no**

[22] O consumidor tem o direito de exercer sua opção de **autorizar ou não o compartilhamento de dados, conforme lhe faculta o direito previsto na Constituição da República** […] Com efeito, a controvérsia dos autos, conforme dito, está na determinação da **abusividade de cláusula contratual que retire do consumidor a possibilidade de optar, válida e livremente**, pelo compartilhamento dos dados que dá a conhecimento de certo e determinado banco, no momento que com ele contrata o serviço de cartão de crédito. (SUPERIOR TRIBUNAL DE JUSTIÇA, Recurso Especial nº 1.348.523-SP, Min. Luis Felipe Salomão, DJe 30/11/2017).

tratamento de dados biométricos - mesmo com os melhores protocolos de segurança -, o que pode causar infindáveis danos aos consumidores, já que esses dados são identificadores únicos e não substituíveis, como a sujeição a fraudes em serviços autenticados por dados biométricos. Outro ilícito possível que pode gerar grandes danos é a **discriminação ilícita** com base em gênero e raça, uma vez que o reconhecimento facial comprovadamente apresenta índices de erros maiores na análise de pessoas negras e mulheres - por exemplo, com a atribuição mais frequente de emoções negativas a pessoas negras[23].

Dessa forma, **a Representada não demonstra efetiva <u>prevenção</u> a danos patrimoniais ou morais, pois muitos consumidores não estariam expostos aos riscos envolvidos,** já que optariam por não ter seus dados coletados, se houvesse mecanismo de consentimento acoplado à tecnologia.

Tampouco há a devida <u>reparação</u> aos danos morais sofridos pelos consumidores. O dano moral coletivo é categoria autônoma de dano que não está relacionado à verificação de atributos da pessoa humana - como dor e sofrimento -, mas consiste na ofensa, de maneira intolerável, a valores éticos fundamentais da comunidade lesada. Dessa forma, é irrelevante se a tecnologia realizava identificação de cada consumidor, pois o objetivo da tutela dos interesses transindividuais é proteger os interesses de uma população indeterminada ou indeterminável.

Como já restou demonstrado, o funcionamento do sistema de reconhecimento facial pressupõe a inserção na esfera privada do indivíduo analisado, mesmo que não haja finalidade de identificação e que os dados pessoais sejam posteriormente descartados. A exploração não autorizada de atributos particulares dos consumidores viola o direito constitucional de proteção à privacidade, intimidade e imagem, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (art. 5º, X, CF).

A proteção de dados pessoais e o direito à privacidade têm como intuito a preservação da esfera íntima do cidadão, garantindo-lhe a escolha e determinação do que será feito do seu fluxo de informações geradas por suas características físicas, atos e movimentos. Essa garantia é fundamental em uma sociedade que se baseia na ideia de liberdade e respeito à dignidade humana. Assim, **o direito de se informar sobre e escolher o que é feito com seus dados são derivações de valores éticos e legais fundamentais ao Estado Democrático de Direito, de modo que a sua violação configura dano *in re ipsa*.**

Nesse sentido **são irrelevantes as jurisprudências trazidas pela Representada**, uma vez que ambos casos não se violam valores fundamentais da comunidade lesada. No

[23] BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research.* Disponível em: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

Recurso Especial 1.726.270/BA, a violação de direito é somente sobre a não comunicação ao consumidor sobre a inscrição em "cadastro de passagem", não havendo obrigação de exigir consentimento, já que o tratamento não envolvia dados biométricos, além de ter como finalidade a proteção do crédito, que é considerado de interesse especial pela legislação.

Da mesma forma, a jurisprudência estrangeira citada (caso Google vs. Lloyd) tampouco envolve tratamento de dados biométricos. Ademais, o ordenamento jurídico brasileiro de direito do consumidor e tutela coletiva é bastante peculiar, de modo que uma jurisprudência britânica, protocolada por um indivíduo em nome da coletividade e que pouco discute dano moral coletivo, não pode ser aplicável ao presente caso.

7.5. Das sanções administrativas por infração às normas de defesa do consumidor

Eventual decisão pela ausência de dano moral coletivo e não violação ao art. 6º, VI do CDC não invalida as demais ofensas ao Código de Defesa do Consumidor indicadas pela Nota Técnica da Senacon: indícios de violação aos artigos 4º, incisos I e III; 6º, incisos II, III e IV; 39, IV; e 43 do CDC.

As condutas da Representada constituem ilícito, como demonstrado ao largo desta manifestação, estando sujeitas a imposição de sanções administrativas, previstas no art. 56 do CDC, em especial multa, imposição de contrapropaganda e até suspensão temporária da atividade, caso retomado o reconhecimento facial dos consumidores.

Destaca-se que a imposição de multa, nos termos do art. 57, é graduada de acordo com a gravidade da infração, a vantagem auferida e a condição econômica do fornecedor. Deve-se considerar, portanto, a vantagem obtida com a utilização da tecnologia. A pesquisa de opinião forçada tomado a cabo na loja da Representada revela o comportamento de seus consumidores, sendo extremamente valiosa às análises de publicidade da marca, bem como aplicável às demais lojas. A vantagem econômica obtida, ainda que de difícil precificação, deve ser considerada no estabelecimento de eventual multa.

8. CONCLUSÃO

Em suma, resta claro que a Representada ofendeu valores fundamentais resguardados pela Constituição Federal e pelas legislações infraconstitucionais ao não informar seus consumidores sobre a extração e análise de seus dados, sem dar-lhes oportunidade de escolha. Não há **informação transparente e clara** ao consumidor, assim como seu devido e expresso **consentimento**.

A empresa violou a privacidade de seus consumidores, incorreu em abuso de direito, com violação aos direitos de informação e de escolha. Há expressa violação de direitos básicos do consumidor, garantidos pelo artigo 5º, inc. X, da Constituição Federal, estes sendo intimidade, vida privada e a imagem. Também viola direitos expressos no Código de Defesa do Consumidor como segurança (art. 6º, inc. I), o direito à liberdade de escolha (art. 6º, inc. II), o direito à informação adequada e clara sobre os serviços prestados pela loja (art. 6º, inc. III) e o direito à informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais (Lei nº. 12.965/2014 - Marco Civil da Internet - art. 7º, inc VIII).

Diante de todas as violações às normas do sistema jurídico brasileiro que realizam a proteção e privacidade dos dados dos consumidores, faz-se necessário a aplicação de sanção condizente com as práticas abusivas que foram detectadas durante o curso deste procedimento administrativo, levando em consideração as conclusões do item 7.5 deste parecer, de modo a coibir e reprimir novas práticas pela empresa, para que direitos básicos dos consumidores não sejam violados. Mais do que um sinal de boa-fé nas relações de consumo, a utilização de novas tecnologias deve ser lícita e com respeito aos consumidores. Diante dos riscos impostos pelo reconhecimento facial trata-se de uma necessidade ética e legal para as empresas que pretendem promover a inovação de forma responsável.

Dessa forma, o Idec espera ter colaborado com o procedimento.

Michel Roberto Oliveira de Souza
OAB/SP 323.983

Juliana Oms
OAB/SP 442.657

Bárbara Prado Simão
OAB/SP 428.335

Diogo Moyses Rodrigues
CPF 291.054.538-52

Christian Tárik Printes
OAB/SP 316.680