INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE

I. Sobre o Instituto de Referência em Internet e Sociedade - IRIS

O *Instituto de Referência em Internet e Sociedade* - IRIS, de acordo com seu estatuto consolidado em 28 de abril de 2017, constitui-se como associação civil sem fins lucrativos de cunho científico e formulação de políticas nas áreas direito e tecnologia, internet e inovação. Suas atividades buscam servir como uma plataforma independente de estudos, centrada na articulação entre teoria e prática. O Instituto busca consolidar-se como referência no contexto nacional, cooperando com organizações governamentais, empresariais, da sociedade civil e da academia, no Brasil e exterior, em temas relativos às suas áreas de atuação. Encontram-se, entre os objetivos do Instituto, o desenvolvimento e plena participação em projetos de advocacia pública, com relacionamento em processos judiciais e extrajudiciais de elevado impacto em questões de interesse público e coletivo, em áreas afins aos temas do IRIS. Entre suas atividades, o IRIS foi aceito como *amicus curiae*[1] do Supremo Tribunal Federal para atuar na Ação Direta de Constitucionalidade nº 51/2017, que se refere ao acesso extraterritorial a dados pelas autoridades brasileiras. Além disso, também ofereceu representação ao Ministério Público de Minas Gerais em processos relativos à coleta e uso de CPFs de consumidores em redes de drogarias atuantes no estado.

II. Síntese da demanda e temas abordados

O presente processo trata-se de Ação Civil Pública em que figuram como partes Autora e Ré, respectivamente, o Instituto Brasileiro de Defesa do Consumidor - IDEC - e a Concessionária da linha 4 do metrô de São Paulo S.A. - ViaQuatro. Tem-se por objeto a cessação de atividades do sistema de Portas Interativas Digitais, implementado por esta última em suas atividades junto à linha de metrô que opera, bem como a condenação da ViaQuatro por danos coletivos, referentes à violação de direitos dos usuários consumidores da rede metroviária.

Tal pedido tem fundamento em violação pela ViaQuatro à legislação consumerista e à referente a dados pessoais, identificada pelo IDEC em razão do funcionamento deste sistema, que, por meio de câmeras e software, tem as funcionalidades de reconhecer a presença de rostos humanos e identificar a quantidade de pessoas que transitam em sua área de abrangência, além de detectar suas emoções, gênero e faixa etária. Na Exordial, relatam-se as seguintes práticas abusivas: i) não houve informação clara e adequada aos consumidores quanto à operação das Portas Interativas Digitais; ii) não foi respeitado o direito de escolha dos

1 IRIS. Pedido de ingresso como *Amicus Curiae* na ADC 51. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=729220092&prcID=5320379#>. Acesso em 07/05/2019. IRIS. Memorial apresentado ao STF na condição de *Amicus Curiae* na ADC 51. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=747870981&prcID=5320379#>. Acesso em 07/05/2019. G1. Drogaria Araújo é multada em mais de R$ 7 milhões por condicionar descontos a fornecimento de CPF. 05 de dezembro de 2018. Disponível em: <https://g1.globo.com/mg/minas-gerais/noticia/2018/12/05/drogaria-araujo-e-multada-em-mais-de-r7-milhoes-por-condicionar-descontos-a-fornecimento-de-cpf.ghtml>. O Estado de Minas. Drogaria Araújo é multada em quase R$ 8 milhões por pedir CPF de clientes. 06 de dezembro de 2018. Disponível em: <https://www.em.com.br/app/noticia/economia/2018/12/06/internas_economia,1011120/drogaria-araujo-e-multada-em-quase-r-8-milhoes-por-pedir-cpf-de-clien.shtml>.

passageiros quanto à coleta de seus dados por esse sistema; e iii) nem mesmo é detalhado seu funcionamento, o qual pode envolver o reconhecimento facial e tratamento individualizado de dados para formação de perfis de consumo.

Citada, a ViaQuatro apresentou defesa fundamentada na distinção entre reconhecimento e detecção facial, relatando que: i) somente realizaria esta última, o que não implica em formação de perfis de consumo individuais, mas apenas em levantamento demográfico sobre o público em geral; ii) não armazenaria dados dos passageiros, pois as informações individualizadas seriam apagadas imediatamente após a sua coleta e agregação ao banco de dados; e iii) os dados armazenados de forma agregada seriam anonimizados, e portanto não realizaria tratamento de dados pessoais protegidos por lei, tendo em vista que seu banco de dados seria de finalidade estatística.

Também se manifestaram a Defensoria Pública do Estado de São Paulo, tendo em consideração que a ViaQuatro é concessionária de serviço de transporte público; o Ministério Público, tendo em consideração a tutela de direitos coletivos; e o Instituto Alana, instituição que atua em programas que buscam a garantia de condições para a vivência plena da infância, na condição de amicus curiae, tendo em vista que o sistema também coleta informações sobre passageiros menores de idade.

Considerada a atuação do Instituto de Referência em Internet e Sociedade - IRIS - e suas temáticas de pesquisa, este parecer abordará esclarecimentos em diversos pontos do processo: em especial, aqueles que são permeados por assuntos de fronteira entre Direito e tecnologia. Para tanto, serão analisados: i) os conceitos mais relevantes relacionados ao tratamento de dados pessoais, bem como a descrição de suas fases, com base no funcionamento da tecnologia envolvida; ii) os elementos essenciais para se verificar se houve a utilização de técnicas de anonimização adequadas; iii) a discussão internacional sobre detecção facial; iv) as considerações técnicas apresentadas pela ViaQuatro no âmbito da ACP; e v) efeitos derivados da assimetria de informação entre a empresa concessionária e os consumidores.

III. O que pode ser compreendido como “tratamento de dado pessoal” na produção de informação sobre grupos de pessoas?

Em um primeiro momento, é importante considerar o principal elemento que fundamenta normas que visam a proteção de dados pessoais nos diversos sistemas jurídicos do mundo, e que se relaciona intrinsecamente ao presente caso: o processamento automatizado.

A legislação europeia sobre proteção de dados pessoais, por exemplo, desde os anos 1980, tem como fundamento a preocupação com os riscos advindos do rápido desenvolvimento tecnológico do processamento automatizado de dados, que permite que diversas informações sobre cidadãos sejam facilmente acessadas e utilizadas, aumentando-se, portanto, os riscos de

violação a direitos e liberdades fundamentais.[2] Esta consideração fica clara quando se verifica que o escopo material das leis europeias (a antiga Diretiva de Proteção de Dados 96/45/EC e a atual Regulação Geral de Proteção de Dados Pessoais 2016/679 [GDPR]) é estabelecido como "tratamento de dados pessoais por meios total ou parcialmente automatizados"[3]. Foram nessas legislações, inclusive, que se basearam a Lei nº 13.709/2018 e as demais leis, resoluções e normativas setoriais sobre proteção de dados pessoais brasileiras (cerca de 40, no total), a exemplo do art, 43 da Lei nº 8.078/90, relativo a bancos de dados de consumidores.

Esse fato ressalta a importância do presente caso para o futuro do cenário brasileiro de proteção de dados pessoais, pois o uso de algoritmos de Inteligência Artificial (I.A.) da AdMobilize permite o processamento quantitativo e qualitativo de milhares de rostos de pessoas que utilizam diariamente a linha amarela do metrô. Esse processamento ocorre a baixo custo e em escala incomparável a qualquer equipe de seres humanos, como fica demonstrado nas informações juntadas pela ViaQuatro ao processo. Os avanços observados na capacidade de processamento de dados têm influência direta na interpretação jurídica das normas que regulam essas tecnologias, como esclarece o doutrinador brasileiro Marcel Leonardi[4]: "[...] uma diferença *quantitativa* trazida pela tecnologia gera uma diferença *qualitativa* no modo de interpretar as normas jurídicas."

Ao longo do presente processo, ambas as partes, baseadas tanto no direito nacional como nas melhores interpretações advindas da União Europeia, definiram dado pessoal, de forma ampla, como qualquer informação relacionada à pessoa natural identificada ou identificável. É essa característica, inclusive, que permite que o direito possa acompanhar o desenvolvimento tecnológico, pois caso o conceito fosse demasiadamente restritivo – ou associado somente a determinadas tecnologias –, sua utilidade jurídica rapidamente se perderia diante do avanço da tecnologia.

O tratamento de qualquer dado pessoal deve ser compreendido como uma cadeia de procedimentos, os quais devem estar em consonância com o ordenamento jurídico brasileiro e suas leis esparsas sobre proteção de dados pessoais[5]. Em relação à presente ação civil pública, podem ser utilizados dois enfoques sobre o funcionamento da cadeia de processamento dos dados pessoais dos usuários do metrô, para que melhor se entenda o caso.

Numa perspectiva da **(i) cadeia como um todo**, têm-se a coleta de dados pessoais brutos (imagem do rosto) para que deles se extraiam informações sobre a reação às publicidades ofertadas, que, por sua vez, serão utilizadas posteriormente para otimizar as novas publicidades

2 UNIÃO EUROPEIA. Article 29 Working Party. **Opinion 4/2007 on the Concept of Personal Data - 01248/07/EN**. p. 5. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm#maincontentSec11>. Acesso em: 06/04/2019.

3 Artigo 3 da Diretiva 95/46/EC e Artigo 2 da Regulação 2016/679.

4 LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011. p. 365.

5 Art. 11 da Lei 12.965/2014 (Marco Civil da Internet): "Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros."

expostas no metrô[6]. Nesse sentido, o tratamento de dados não é um processo que ocorre "no vácuo" - despretensiosamente - sendo o consumidor tanto a origem como o destinatário final da cadeia de tratamento, já que ele é a fonte das informações que têm como objetivo final influenciar seu próprio comportamento de consumo.

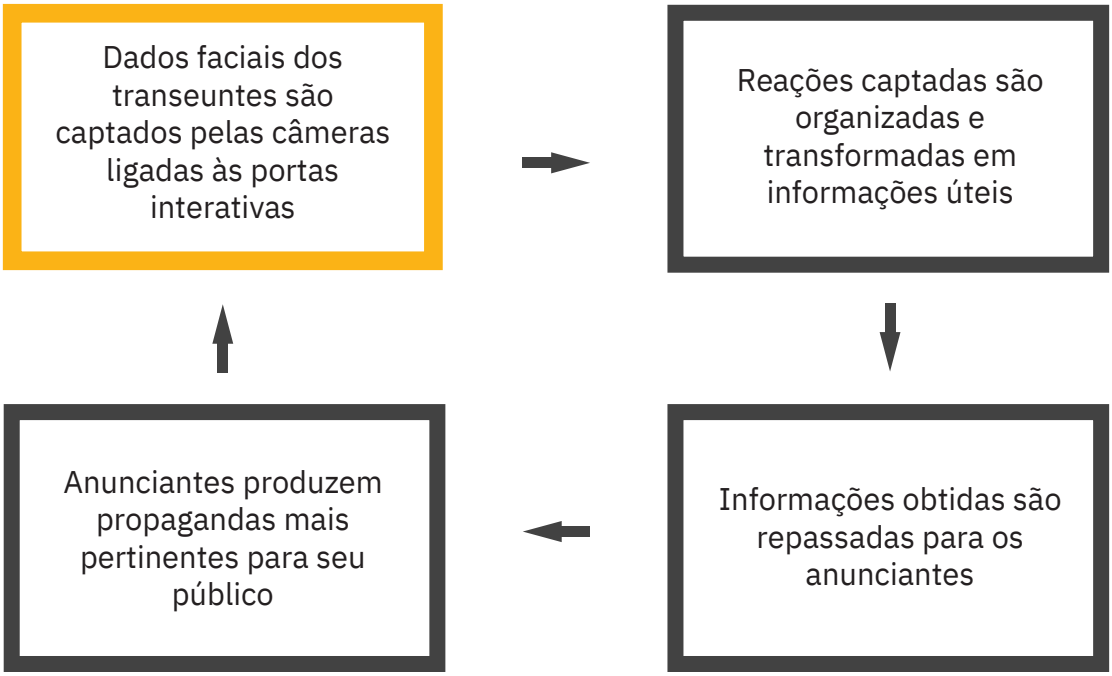


Figura 1: Visão Geral da cadeia de processamento dos dados pessoais das portas interativas.

Um segundo enfoque sobre a cadeia de processamento dos dados pessoais dos usuários se concentra em explicar **(ii) o que ocorre técnica e juridicamente entre o momento da captura da imagem até a produção das informações extraídas**. Essa visão específica da cadeia de tratamento, pode ser divida em 3 fases:

6 Segundo Bruno Ricardo Bioni, a mineração de dados envolve a captura dos dados brutos (*input*) para posterior processamento dos mesmos e saída (*output*) de uma informação. Essa informação, por sua vez, é revertida para a tomada de uma decisão, como o direcionamento de publicidade. A questão, portanto, não diz respeito apenas a dados ou bancos de dados, mas sim a toda uma dinâmica de um sistema de informação que permite a um manancial de dados brutos ser estruturado, organizado e gerenciado para produzir um conhecimento que possa ser empregado para um fim específico. BIONI. Bruno Ricardo. **Proteção de dados pessoais:** A função e os limites do consentimento. Rio de Janeiro: Forense, 2018. p. 35-39.

Figura 2: Fluxo do tratamento de dados faciais, desde sua coleta até o suposto processo de anonimização. Fonte: autoria própria. Imagens: retiradas do vídeo institucional e do parecer técnico do IBP, fl. 437 e 442

Apesar de ainda não estar claro se há ou não um processo de anonimização e agregação adequado dos dados na etapa final do tratamento (fase 3), em razão da superficialidade das provas produzidas pela ViaQuatro constantes no processo (tópico que será devidamente desenvolvido em momento posterior deste documento), é importante a atenção especial às fases 1 e 2.

Na fase 1, a primeira ação relacionada ao tratamento de dados deste caso é a filmagem feita pelas câmeras de propriedade da ViaQuatro, que fornece a matéria-prima para o algoritmo de inteligência artificial da AdMobilize. Nesse processo, a captura da imagem do rosto de uma pessoa indubitavelmente se caracteriza como um tratamento de dado pessoal, mesmo que se considere que este dure apenas algumas frações de segundo e que haja o descarte da imagem em uma fase posterior do tratamento.

Não se pode sustentar que a foto de um rosto é um dado anônimo *ab initio*, como procura argumentar a ViaQuatro, pois é intrínseco da natureza do rosto de uma pessoa ser caracterizado como dado pessoal. Se não fosse o rosto um elemento intrinsecamente pessoal, não haveria necessidade, por exemplo, da utilização de fotos em documentos de identificação - inclusive aqueles oficiais, atribuídos pelo Estado.

Além disso, considerando o intuito de proteção dos indivíduos em relação às técnicas automatizadas viabilizadas pelo desenvolvimento tecnológico, as leis de proteção de dados da Europa e Brasil, bem como em outras partes do mundo, não apresentam nenhuma exigência quanto ao tempo mínimo de processamento entre a captura e a anonimização[7]. Isso significa

7 A preocupação com os tratamentos automatizados de dados se reflete na ausência de previsão legal em relação

que, mesmo o processamento ocorrendo em milésimos de segundo, ainda assim há tratamento de dados pessoais, sujeito aos deveres e garantias previstos em lei.

Na fase 2, a imagem é analisada por meio de um algoritmo de I.A. que produz um modelo matemático do rosto da pessoa, para que se possa, posteriormente, fazer a inferência sobre a emoção sentida no momento da captura da imagem, além de permitir a identificação do gênero, faixa etária, etc.[8] Essa análise utiliza pontos de referência do rosto para que se identifiquem características físicas associadas a emoções, como posição da boca (para a detecção de um sorriso, por exemplo) ou posição das sobrancelhas (para a indicação de surpresa, reprovação, etc).[9] Esse processo também é descrito, inclusive, pela AdMobilize, ao esclarecer que seu produto "funciona por meio de algoritmos que detectam cerca de 80 (oitenta) pontos no rosto de uma pessoa e, a partir da detecção, os convertem em números binários", nas fls. 426 dos autos.

Assim, a representação matemática de um rosto configura-se claramente como um dado pessoal sensível, ao representar as **características biométricas únicas** que permitem a identificação de um indivíduo. A mesma lógica é utilizada na coleta de impressões digitais pelo Estado, pois é o posicionamento singular das papilas das polpas dos dedos, dado inerentemente biométrico, que permite a identificação do indivíduo. O risco de utilização de dados biométricos é considerável, uma vez que eles representam identificadores únicos e praticamente imutáveis, acompanhando os titulares ao longo de toda a vida. Considerados esses aspectos, a captura das estruturas faciais contidas nas imagens demanda uma cautela especial na análise deste feito pelo Judiciário.

Há o risco de que os dados da distância entre elementos faciais de um rosto sejam cruzados com outras informações, como data e hora da coleta da imagem, ou mesmo com o banco de dados do Bilhete Único[10]. Caso isso aconteça, é possível haver a identificação do titular e o uso dos seus dados para perfilamento (*profiling*) com base nas suas preferências

à duração dos processos de tratamento, historicamente, no desenho legislativo sobre a matéria. Para uma introdução dos fundamentos históricos, ver: IRIS. *GDPR e suas repercussões no direito brasileiro:* Primeiras impressões de análise comparativa. 2018. Disponível em: <http://irisbh.com.br/wp-content/uploads/2018/06/GDPR-e-suas-repercuss%C3%B5es-no-direito-brasileiro-Primeiras-impress%C3%B5es-de-an%C3%A1lise-comparativa-PT.pdf>. Acesso em 09/04/2018.

8 Geralmente, o reconhecimento da expressão facial é realizado por uma abordagem em três etapas. O primeiro passo é a detecção de rostos dentro de uma imagem (*face detection*). O segundo passo é obter uma representação numérica da estrutura do rosto (*facial expression data extraction*). Características do rosto são extraídas para reduzir a grande quantidade de dados da imagem e para obter uma representação abstrata do conteúdo da imagem. Finalmente, na terceira etapa, a expressão facial é determinada a partir desses dados extraídos na segunda etapa, geralmente por um classificador (*facial expression classification*). PANTIC, Maja e ROTHKRANTZ, Leon J.M. **Automatic Analysis of Facial Expressions: The State of the Art.** Institute of Electrical and Electronics Engineers (IEEE) Transactions on Pattern Analysis and Machine Intelligence. Vol. 22, nº 12. 2001. p. 1.424. Disponivel em: <https://www.researchgate.net/publication/3193199_Automatic_Analysis_of_Facial_Expressions_The_State_of_the_ArtvVT>. Acessado em: 10/04/2019. A descrição acima, embora publicada há um tempo considerável, encontra-se em sintonia com a apresentada no site da empresa de tecnologia Norton em sua página na internet. NORTON. How does facial recognition work? Disponível em: <https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html>. Acesso em 31/05/2019.

9 *Ibid*.

10 As críticas e riscos relativos ao Bilhete Único na cidade de São Paulo giram em torno dos bancos de dados dos usuários e potencial venda desses dados para entidades terceiras. Essas e outras preocupações são apontadas por especialistas em: <https://www.vice.com/pt_br/article/panq7n/mudancas-no-bilhete-unico-acendem-alerta-sobre-coleta-indevida-de-dados>. Acesso em 08/04/2019.

inferidas por meio da reação às publicidades expostas. Desse modo, na fase 2 do tratamento há também o tratamento de dados pessoais, estes de natureza ainda mais sensível por serem informações biométricas das faces do indivíduos.

É elucidativo citar a seguinte explicação sobre dados biométricos do Grupo de Trabalho do Artigo 29 europeu (*Working Party 29 [WP 29]*)[11]-[12] - referência internacional em matéria de proteção de dados:

> *[...] Esses dados podem ser definidos como propriedades biológicas, características fisiológicas, traços vivos ou ações repetíveis, onde essas características e/ou ações únicas para aquele indivíduo e mensuráveis, mesmo que os padrões usados na prática para medi-los tecnicamente envolvam um certo grau de probabilidade. Exemplos típicos de tais dados biométricos são fornecidos por impressões digitais, padrões da retina,* **estrutura facial***, vozes, mas também, geometria da mão, padrões de veias ou mesmo alguma habilidade profundamente enraizada ou outras características comportamentais (como assinatura manuscrita, padrões de digitação em teclados, modo particular de caminhar ou para falar, etc ...). [...]* **Como tal, eles podem funcionar como "identificadores". De fato, por causa de sua ligação única com um indivíduo específico, dados biométricos podem ser usados para identificar indivíduos** .[13] *(grifo nosso)*

Seria somente num terceiro momento do tratamento (fase 3), conforme apresentado na Figura 2, que se poderia falar em dados anonimizados, caso houvesse sido comprovado que a AdMobilize não armazena nenhuma imagem e/ou modelo matemático dos rostos dos usuários do metrô de forma individualizada, em conjunto com as inferências feitas sobre eles.

Para que se entenda o que é um processo de anonimização adequado, deve-se ter como premissa que a anonimização só pode ocorrer caso haja como matéria-prima um conjunto de dados pessoais que serão anonimizados, conforme bem esclarece o relatório sobre técnicas de anonimização do Grupo de Trabalho do Artigo 29 europeu:

> *Primeiramente,* **anonimização é uma técnica aplicada a dados pessoais** *cujo objetivo é torná-los desidentificados de forma irreversível. Portanto,* **a presunção inicial é que primeiramente dados pessoais foram coletados e processados em conformidade com a legislação sobre retenção de**

11 O Grupo de Trabalho do Artigo 29.º (sigla em inglês, WP 29) é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade no cenário anterior à vigência do Regulamento Europeu de Proteção de Dados (*General Data Protection Regulation nº 2016/679*). Reune opiniões altamente qualificadas sobre proteção de dados pessoais e privacidade, disponibilizando suas opiniões oficiais no site: <https://edpb.europa.eu/our-work-tools/article-29-working-party_pt>.

12 Com a entrada em vigor da GDPR, este grupo de trabalho se transformou na *European Data Protection Board*.

13 Tradução Livre. UNIÃO EUROPEIA. Article 29 Working Party. **Opinion 4/2007 on the Concept of Personal Data** - *01248/07/EN*. p.8. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>. Acesso em: 06/04/2019.

dados pessoais identificáveis.

> *Nesse contexto, o processo de anonimização, significando o processamento de dados pessoais para transformá-los em dados anonimizados,* **é um exemplo de "processamento posterior***".*[14] *(grifo nosso)*

Este entendimento é comparável à doutrina dos "frutos da árvore envenenada"[15], pois se o tratamento inicial dos dados pessoais - nesse caso, a detecção facial - viola o direito aplicável, mesmo que sejam utilizadas técnicas adequadas de anonimização em momento posterior, todas as outras fases do processamento também acabam por violar o sistema legal. O raciocínio é o mesmo por exemplo, no caso em que uma prova obtida ilicitamente contamina as provas posteriores, tornando-as inválidas, ainda que as últimas tenham sido obtidas de forma lícita da primeira.

Assim, o tratamento dos dados pessoais do presente caso já teria sido "contaminado" inicialmente por uma ilicitude na sua captura e posterior modelação matemática, considerando as normas de proteção ao consumidor, os direitos dos usuários de transportes públicos e, em especial, os direitos de privacidade e imagem, conforme será detalhado abaixo.

Para que houvesse a coleta da imagem do rosto, modelação matemática da face e análise das emoções, seria necessária uma base legal que permitisse o tratamento, como o consentimento do usuário do metrô, conforme o art. 7º, VII e IX, da Lei nº 12.965/2014. Para que o consentimento fosse válido, também é pré-requisito que informações claras sejam repassadas, a fim de garantir o direito à informação do consumidor– arts. 6º, III, e 31, entre outros, do Código de Defesa do Consumidor –, conforme será desenvolvido em momento posterior.

Ademais, é preciso considerar, conforme o estado atual da técnica, que a aprimoração de algoritmos de inteligência artificial (I.A.) para detecção facial se beneficiaria do armazenamento dos dados resultantes das análises faciais (modelo matemático do rosto e as características detectadas como, emoção, gênero, etc.). Isso porque é possível empregar esses dados para verificar a eficiência desses algoritmos, bem como para aprimorar sua precisão[16]. Cabe recordar que algoritmos de I.A., como *machine learning* e *neural networks*, funcionam

14 Tradução Livre. UNIÃO EUROPEIA. Article 29 Working Party. **Opinion 05/2014 on Anonymisation Techniques** - *0829/14/EN*. p. 7. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>. Acesso em: 06/04/2019.

15 Robert M. Pitler. **The Fruit of the Poisonous Tree Revisited and Shepardized**, 56 Cal. L. Rev. 579 (1968). Disponível em: <http://scholarship.law.berkeley.edu/californialawreview/vol56/iss3/2>. Acessado em: 09/04/2019

16 "Os sistemas automatizados de identificação de expressões faciais enfrentam vários desafios. Em primeiro lugar, é difícil obter dados para treinamento do algoritmo, especialmente para imagens faciais que expressam emoções como tristeza ou medo. Está dificuldade advém do fato de que os bancos de dados publicamente disponíveis consistem em expressões faciais encenadas [...]" [tradução livre]. MAYER, C, EGGERs, M, e RADIG B. **Cross-Database Evaluation for Facial Expression Recognition.** Pattern Recognition and Image Analysis. Vol. 24, nº 1. p.1. Disponível em: <https://link.springer.com/article/10.1134/S1054661814010106>.

basicamente por meio do acesso a grandes conjuntos de dados, através dos quais eles possam detectar padrões e, subsequentemente, aplicar esse conhecimento adquirido na análise de novos conjuntos de dados.[17]

Assim, tecnicamente, é possível afirmar que, quanto mais dados forem utilizados para treinar um algoritmo de I.A., melhor será sua precisão. Seria, portanto, de interesse da AdMobilize armazenar os dados pessoais tratados no presente caso (modelo matemático do rosto e as correspondentes emoções detectadas), para que a empresa possa melhor avaliar a eficiência de seu algoritmo de I.A. e treiná-lo para detecção facial. Conforme nossa análise do parecer técnico do IBP, apresentada em momento posterior deste texto (item VII), não ficou demonstrado quais dados são armazenados pela AdMobilize.

IV. O que significa "anonimização de dados pessoais"?

As técnicas de anonimização referem-se ao **processamento de dados** a fim de evitar a identificação de seu titular. É importante que, ao conduzir processos de anonimização, empresas possam garantir que, uma vez anonimizados , não haverá chance razoável de reidentificação dos dados. Como opinou o Grupo de Trabalho do Artigo 29, "dados anonimizados são, consequentemente, dados que previamente referiram-se a uma pessoa identificável, mas que a identificação não é mais possível"[18].

Por essa razão, é necessário que as técnicas de anonimização utilizadas sejam descritas de forma clara, para que se possa verificar se elas estão em conformidade com as melhores práticas atuais. Não é possível observar nos documentos apresentados pela ViaQuatro nenhuma descrição ou nomeação da técnica de anonimização supostamente utilizada, que permita garantir que nenhum usuário do metrô exposto à tecnologia seria identificado ou identificável. Explicações acerca de quais são os procedimentos utilizados para anonimização são fundamentais para afirmar que uma tecnologia não processa dados pessoais.

Em uma perspectiva comparada com o direito europeu, o processo de anonimização de dados foi inicialmente conceituado por meio da Diretiva 95/46/CE, relativa ao tratamento de dados pessoais. A experiência europeia, para além de qualquer exercício de direito comparado, é referência internacional sobre proteção de dados, uma vez que a normatização do tema encontra espaço na agenda da comunidade desde a década de 1980[19]. Segundo essa diretiva, a anonimização consiste em uma técnica de processamento de dados por meio da qual se desvincula uma pessoa natural da titularidade de um dado qualquer. Isso significa

17 *RUSSELL, Stuart J.; NORVIG, Peter.* **Artificial intelligence: a modern approach**. Malaysia; Pearson Education Limited, 2016, p.26.

18 WP29.Opinion 05/2014 on Anonymisation Techniques. 10/04/2014.p.8. Disponível em : <https://www.pdpjournals.com/docs/88197.pdf>.

19 Para mais informações sobre a evolução da matéria na União Europeia, bem como sua influência doutrinária e legislativa no ordenamento brasileiro, conferir: IRIS, GDPR e suas repercussões no Direito Brasileiro. 2018. Disponível em: <http://irisbh.com.br/pt/blog/gdpr-e-suas-repercussoes-no-direito-brasileiro/>

que, após a anonimização, uma pessoa natural, inicialmente identificável por meio de um determinado dado, não mais será associável ao referido dado. Portanto, uma vez que dados anonimizados implicam a não aplicação das normas de proteção de dados pessoais, torna-se ainda mais importante que o dever de transparência seja observado por parte do responsável pelo tratamento.

Essa definição de anonimização de dados prevista na Diretiva foi praticamente reiterada no texto final do recente Regulamento Geral de Proteção de Dados Pessoais da União Europeia (GDPR), que substitui a diretiva dos anos 90. O regulamento, aprovado em 2016, que entrou em vigor em 2018, influenciou, inegavelmente, a Lei Geral de Proteção de Dados Pessoais brasileira (lei nº 13.709/2018), cujo artigo 5º, III e XI, enuncia:

> *"Art. 5º Para os fins desta Lei, considera-se:*
> *III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;*
>
> *[...]*
>
> *XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo."*

Importante mencionar que a possibilidade de se identificar um indivíduo por meio de um dado não se resume a informações como nome, número de CPF ou outras informações pessoais demasiadamente óbvias.

A identificação de uma pessoa natural, principalmente com o advento da internet e do processamento em massa de dados, pode ser feita mediante o emprego de informações muito mais vagas - denominadas metadados. Tratam-se de dados que fornecem informações sobre outros dados. Podem ser considerados metadados, por exemplo, de acordo com a legislação brasileira: "Art. 5º - VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP"[20]. Metadados como geolocalização e horário em que o dado foi gerado, endereço de IP, porta lógica de origem, entre outros, também podem ser empregados, individualmente ou em conjunto, para identificar uma pessoa natural com precisão.

Dessa forma, é evidente que há processamento automatizado de dados pessoais, e que não há prova ou menção ao procedimento de anonimização realizado neste procedimento.

V. Importância da anonimização adequada

20 BRASIL. Lei 12.965/ 2014. Marco Civil da Internet.

Observe-se que não há uma técnica específica prevista para a anonimização de dados. Dessa forma, ao se estabelecer um serviço que envolva essa técnica, é possível escolher uma ou mais opções disponíveis dentre uma gama de possibilidades.

Na prática, a técnica necessária deve ser apresentada e justificada caso a caso. Por essa razão, também se reforça a necessidade de que as técnicas utilizadas sejam apresentadas a este Juízo, a fim de comprovar que a tecnologia presente nas "portas interativas" não envolve o uso ou a possibilidade de uso, com o avanço da tecnologia, de dados pessoais. O Grupo de Trabalho do Artigo 29, em uma de suas publicações[21], enumera algumas práticas disponíveis para anonimização de dados, bem como recomendações para emprego de cada uma delas, possíveis vulnerabilidades e casos concretos nos quais foi possível reverter o anonimato promovido por cada técnica.

Nesses casos, a implementação dessas medidas não é mera consequência de uma obrigação legal decorrente da aplicação da proteção de dados pessoais. Mais que isso, a devida anonimização dos dados representa uma condição para que não sejam qualificáveis como dados pessoais - reiterando-se que, como demonstrado na Figura 2, o momento da coleta (fase 1) e posterior elaboração do modelo matemático da face para análise das emoções (fase 2) caracterizam-se como tratamento de dados pessoais. A anonimização dos referidos dados (fase 3 demonstrada na Figura 2), portanto, é imperativa para que esse tratamento não se sujeite ao regime jurídico previsto para dados pessoais no Marco Civil da Internet (Lei nº 12.965/2014) e, futuramente, na Lei Geral de Proteção de Dados, conforme se manifesta a defesa.

Imperioso destacar que, pelo princípio da precaução, vigente na proteção ao consumidor brasileiro, ao lançar mão de uma tecnologia, a empresa que presta serviço (público, inclusive) tem a obrigação de conhecer holisticamente o processamento envolvido e estar apta a prestar esclarecimentos completos em relação à tecnologia, especialmente em Juízo.

A adoção de medidas organizacionais e de técnicas adequadas de anonimização são elementos fundamentais para se verificar se um determinado tratamento envolve ou não dados pessoais. Em nenhum momento deste processo foram apresentadas quais seriam as eventuais técnicas adotadas pela ViaQuatro. Nem mesmo foi anexado o contrato firmado entre as partes, o qual poderia conter cláusulas que exigissem o emprego adequado de técnicas de anonimização, além de se exigir contratualmente que a AdMobilize não trate dados pessoais dos usuários de metrô, e nem busque re-identificá-los, caso venha tratar o dados que supostamente foram anonimizados na fase 3 do tratamento.

Em relatório com indicação de melhores práticas para garantir a privacidade dos consumidores, a *Federal Trade Commision* estadunidense recomenda que empresas que tratam dados anonimizados - a fim de diminuir os riscos de que sejam re-identificados, por processos

21 UNIÃO EUROPEIA. Article 29 Working Party. Opinion 05/2014 on Anonymisation Techniques - 0829/14/EN. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf>

de correlações com outros dados (*linkability*) - tomem as seguintes precauções:

> *os dados de uma empresa não seriam razoavelmente vinculáveis a um determinado consumidor ou dispositivo, na medida em que a empresa implementa três proteções significativas [...] (1) adote medidas razoáveis que garantam a desidentificação dos dados [...] (2) a empresa se comprometa publicamente a não re-identificá-los, e (3) a empresa exija que as outras empresas que utilizarão os dados mantenham-nos em formato não identificável [...].* [22]

Tais cláusulas seriam um importante incentivo para se evitar qualquer violação das leis de proteção de dados pessoais esparsas do ordenamento brasileiro, e de garantir a segurança dos usuários do metrô operado pela ViaQuatro. A apresentação dessas cláusulas seria um demonstrativo de que a ViaQuatro, ao menos quanto à proteção dos dados dos consumidores, realiza as atividades relativas às portas interativas com algum grau de boa-fé.

Cabe apontar, contudo, que a demonstração de disposições contratuais nesse sentido não anula qualquer irregularidade na atividade realizada pela ViaQuatro que seja porventura comprovada no decorrer do processo judicial em curso, e tampouco supriria o dever de informar e a exigência de consentimento inerentes ao direito dos usuários enquanto consumidores.

Como resultado, tem-se uma situação na qual informações sobre o real método de tratamento de dados empregado nas portas interativas constituem uma "caixa preta". Resta aos usuários do metrô de São Paulo - bem como ao presente Juízo e a terceiros - acreditar, em plena confiança, no discurso reiterado pela concessionária da linha 4 amarela, sem maiores questionamentos, apesar do fundado receio já demonstrado por especialistas, inclusive pelo Instituto Brasileiro de Defesa do Consumidor e pelo Instituto Alana, e mesmo pelo próprio Ministério Público e pela Defensoria Pública do Estado de São Paulo nos autos processuais.

Acerca dos argumentos apresentados em Juízo e que, alegadamente, seriam suficientes para esclarecer quaisquer pontos controversos relativos à tecnologia utilizada nas portas interativas, mostra-se pertinente um tópico à parte (item VII). Em específico, será realizada uma análise do parecer encomendado pela ViaQuatro.

VI. Implicações de uma possível falta de anonimização adequada dos dados

Uma das possibilidades para a fase 3 de tratamento dos dados realizada pelas Portas Interativas Digitais seria, caso não haja anonimização adequada, a formação de perfis para cada passageiro, contendo detalhes sobre seu comportamento, como horário em que costuma

22 FEDERAL TRADE COMMSION. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*. 2012. p.21-22. Disponível em: <https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers>

estar em determinada estação, seu humor, suas características físicas e sua idade.

Considerando esta hipótese, destacam-se alguns riscos que esta prática impõe ao consumidor e a forma como a atuação do poder público tem se orientado a fim de evitar violações. Para isso, será realizada análise em paralelo com outro caso, semelhante ao da hipótese de perfilamento aqui considerada.

Em suas atuações institucionais, o Instituto de Referência em Internet e Sociedade (IRIS) ofereceu uma representação ao Ministério Público de Minas Gerais, em caso no qual farmácias incorrem em práticas com efeitos similares ao caso em questão.

Em Belo Horizonte e outras cidades brasileiras, tem sido prática comum que estabelecimentos solicitem o número do Cadastro Nacional de Pessoas Físicas - CPF - dos clientes na realização de qualquer compra. O caso tem relação com este feito em alguns aspectos: i) o uso e a coleta de dados pessoais dos consumidores sem consentimento livre, expresso e informado (Marco Civil da Internet, art. 7º, §VII); ii) a violação do dever de informar o consumidor sobre sua participação em bancos de dados, ainda que sejam de natureza demográfica; iii) a possibilidade de uso de dados objetivando a formação de perfis. No caso de cadastro de CPF, o risco era imediato, enquanto que no presente caso, é uma possibilidade, podendo decorrer também de falha de segurança nos sistemas de câmera ou de função secundária do sistema que produz os dados demográficos; e iv) a falta de políticas de privacidade que contenham informações claras sobre o uso, coleta, objetivos e níveis de segurança dos dados tratados.

No caso das farmácias, após tramitação do procedimento administrativo nº 0024.18.002027-3, instaurado pelo Ministério Público de Minas Gerais, foi apurada a irregularidade da prática através assinatura de Termo de Ajuste de Conduta (TAC) entre a drogaria e o MPMG[23]. O processo resultou em precedente sobre determinações corretivas em relação ao cadastro e à participação de consumidores em levantamentos com fins comerciais. A informação e a autodeterminação dos consumidores, enquanto titulares de dados, foram destaques na conclusão do Ministério Público sobre a prática.

O caso é importante para ilustrar que, mesmo que ainda não esteja em vigor a Lei Geral de Proteção de Dados – o que acontecerá em 2020 –, os dispositivos esparsos no ordenamento podem ser bases legais para ações que busquem a proteção no uso de dados pessoais no Brasil. Dessa forma, as bases legais de ambos os casos se assemelham por tratarem do mesmo objetivo em circunstâncias semelhantes: a ausência de informação, consentimento e segurança do consumidor, com objetivo de se realizar análise de mercado e influenciar o consumidor. Se no caso em questão as emoções, idade, gênero e outros dados são empregados para otimizar a publicidade e incentivar o consumo, no outro o uso de padrões de consumo

23 **Acordo com o MPMG prevê que drogaria Araújo cesse captação de CPF dos consumidores**. Disponível em: https://www.mpmg.mp.br/areas-de-atuacao/defesa-do-cidadao/consumidor/noticias/acordo-com-o-mpmg-preve-que-drogaria-araujo-cesse-captacao-de-cpf-dos-consumidores.htm. Acesso em 09/04/2019.

médico-farmacêuticos foram utilizados para a atribuição de descontos relacionados aos hábitos individualizados dos clientes, também incentivando o consumo.

Ademais de funcionarem como forma de manipular o comportamento dos consumidores, direcionando individualmente publicidade com base em dados coletados de forma massiva, as técnicas de perfilamento incidem sobre outras searas da vida social, possibilitando a discriminação de uma pessoa. Deve-se ter em conta, no cenário de falta de anonimização adequada, que há empresas interessadas em adquirir e comercializar bancos de dados - as chamadas *data brokers*[24]. Esse modelo de negócios é fundado na compra e oferta de bancos de dados pessoais a terceiros que possam utilizá-los para avaliar valores de planos de saúde, seguros de vida, admissão em vagas de emprego e outros processos seletivos.

Sendo assim, a decisão administrativa no caso das farmácias é importante pelo reconhecimento da necessidade, pela sociedade e seus representantes, da proteção daquelas informações que possam envolver liberdade de escolha dos consumidores, especialmente aquelas que possam referir-se a questões de saúde ou de características físicas. Faz-se a ressalva de que, nos moldes da legislação atual, o uso e tratamento desses dados pessoais não configura ilícito, desde que sejam respeitados os limites e garantias estabelecidos pelo sistema de proteção do consumidor e de dados pessoais. Como no presente caso há análise comportamental dos consumidores, estas devem respeitar os limites estabelecidos pelo sistema de proteção do consumidor no sentido da tutela da sua autodeterminação, privacidade e da transparência nas relações negociais.

VII. Considerações sobre o parecer técnico apresentado

Tendo os riscos de uma possível prática de perfilamento em consideração, é pertinente analisar o documento apresentado pela ViaQuatro a fim de corroborar suas alegações de que não realiza coleta de dados identificados ou identificáveis.

O parecer técnico apresentado pelo respeitável Instituto Brasileiro de Peritos (IBP) às fls. 427 dos autos, sobre os dados coletados por meio das Portas Interativas Digitais, não é suficiente para demonstrar a ausência de tratamento de dados pessoais. Não deve, portanto – com todo respeito ao IBP –, ser considerado como prova técnica neste feito por não ser completamente sustentável de um ponto de vista técnico.

Os recursos analisados pelo parecer técnico não são suficientes para demonstrar precisamente quais são os dados coletados e enviados pela internet à empresa detentora do

24 Vermont foi o primeiro estado nos EUA a aprovar, ainda em 2018, uma lei específica para regular a atuação de *data brokers.* A lei define o que são *data brokers,* a obrigatoriedade das empresas se registrarem perante as autoridades estaduais, o dever de transparência para com os consumidores sobre o tratamento de seus dados, quando é possível se retirar do tratamento, e o dever de informar os afetados em caso de vazamento de dados. COLDEWEY, Devin. *Vermont passes first law to crack down on data brokers.* Techcrunch. 27/05/2018. Acessado em: 04/06/2018. Disponível em: <https://techcrunch.com/2018/05/27/vermont-passes-first-first-law-to-crack-down-on-data-brokers/>

software, AdMobilize, apesar de a ViaQuatro alegar somente ter acesso aos resultados agregados, pois a análise se restringiu: i) à mera imagem de um diagrama do fluxo de dados (fls. 433); ii) ao livro informativo do painel de controle da solução contratada (*dashboard*) (fls. 433-441); iii) ao pacote de dados com o resultado final do tratamento realizado pela AdMobilize ("contêiner forense") e enviado por e-mail à ViaQuatro (fls. 438-440); e iv) ao simples vídeo publicitário[25] sobre o funcionamento da solução da AdMobilize (fls. 441-446). Esses itens são insuficientes para demonstrar que não seriam armazenadas, nem pela ViaQuatro e nem pela AdMobilize, os pontos característicos dos rostos com as respectivas emoções detectadas e/ou as imagens das câmeras (que estão conectadas à internet, como se verifica nas perguntas e respostas, às fls. 1.132 e 1.133).

A imagem de um diagrama do fluxo de dados e o vídeo publicitário, ambos de autoria da própria AdMobilize, não podem sustentar uma conclusão técnica, pois têm o mesmo peso de uma declaração e não comprovam, de fato, que o alegado corresponde à realidade. Já a *dashboard* e o contêiner forense, apesar de serem indicativos, não demonstram tecnicamente a quais dados a AdMobilize tem acesso e armazena no momento posterior à identificação das emoções (fase 3).

Pelo que se depreende, as técnicas empregadas não refletem as noções atuais para a explicação do funcionamento de softwares[26] e a necessidade do uso adequado de métodos, como o de engenharia reversa, para a elucidação do caso em questão, relativo ao uso de tecnologia complexa, que emprega inteligência artificial. Tecnicamente, é necessário ressaltar, a engenharia reversa possibilita a auditoria sobre o software sem que seja exposto o código-fonte[27].

Também deve-se ter em mente que não foram explicitadas quais as medidas de segurança da informação adotadas, o que é grave, considerando-se o perigo de se expor[28] dados sensíveis (biométricos) de milhares de usuários da linha amarela do metrô.

A título ilustrativo, pensemos no conhecido caso envolvendo Facebook e Cambridge Analytica. O caso ganhou notoriedade quando, em 17 de março de 2018, os jornais The New York Times[29] e The Guardian[30] reportaram que a Cambridge Analytica usou informações pessoais de milhões de perfis com intuito de direcionamento de campanha política.

Guardadas as proporções e especificidades do caso, é interessante ponderar sobre a

25 Disponível em:<https://www.youtube.com/watch?v=_zj_51eU-kU>

26 SAMUELSON, Pamela; SCOTCHMER, Suzanne. **The law and economics of reverse engineering**. Yale Law Journal. 111.7, p.1575-1663, Maio. 2002. p.1608

27 Idem.

28 Sobre os riscos do uso de inteligência artificial, sem que seus mecanismos estejam esclarecidos, principalmente para as autoridades, ver: O'NEILL, Cathy. **Weapons of math destruction: How big data increases inequality and threatens democracy.** Nueva York, NY: Crown Publishing Group, 2016.

29 THE NEW YORK TIMES. **How Trump Consultants Exploited the Facebook Data of Millions**. 17, March, 2018. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

30 THE GUARDIAN. **Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach**. 17, March, 2018. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>

elaboração de uma explicação técnica mais detalhada do caso – a simples apresentação descritiva da *dashboard*, de um vídeo institucional, e de uma imagem do fluxo de dados fornecidos pelo Facebook não bastaria para que os peritos constatassem um compartilhamento de dados pessoais sem autorização dos titulares. Portanto, se o objetivo for entender o fluxo dos dados utilizados, deve-se lançar mão de ferramentas de engenharia reversa, ferramentas de análise do tráfego na rede ao qual estão conectadas e análises dos bancos de dados e servidores da aplicação.

Ou seja, os esclarecimentos técnicos sobre softwares, para serem conclusivos, demandam um processo para descobrir os princípios tecnológicos e o funcionamento de um dispositivo, objeto ou sistema, através da análise de sua estrutura, função e operação. Esses elementos não são encontrados no parecer apresentado pela ViaQuatro, o qual, de forma ampla, apenas analisou o produto final do tratamento de dados que é fornecido à ViaQuatro, sem maiores ponderações quanto ao papel da AdMobilize.

Isso não quer dizer que o parecer chega a conclusões inverídicas, mas que, a fim de demonstrar como se chegou inequivocamente até elas, deveria esclarecer quais os materiais que comprovam tecnicamente a inexistência de armazenamento das imagens e/ou informações sobre a configuração biométrica dos rostos em conjunto com as emoções detectadas, bem como a ausência de individualização dos dados coletados de cada usuário.

Ao observar o produto gerado pelo sistema, o parecer técnico intenta concluir se, para chegar àquelas informações, haveria tratamento individualizado de dados biométricos ou não - como uma tática de "engenharia reversa". Cabe pontuar que a engenharia reversa consiste no processo por meio do qual se consegue extrair conhecimento ou modelos de design de qualquer coisa produzida pelo homem[31]. Assim, consiste em entender o funcionamento de algo através da análise de sua estrutura e de seu comportamento.

Diferente do que ocorre com objetos corpóreos - os quais podem ser observados "fisicamente" -, a engenharia reversa de software se dá através de programas de computador diversos, que permitem, inclusive a análise de softwares de código fechado (proprietário) de forma não intrusiva, por meio da análise das instruções emanadas pelo software analisado para o processador[32]. Em outras palavras, há técnicas de engenharia reversa de software que possibilitam que o funcionamento do programa seja inspecionado sem que seja necessário acesso direto ao seu código fonte, evitando infrações aos direitos de Propriedade Intelectual e segredos de negócios.

Dessa maneira, para fornecer informações conclusivas sobre o software analisado, o parecer técnico deveria ter se dedicado a verificar se fora realmente utilizado algum processo de anonimização dos dados, e analisar quais informações são repassadas à AdMobilize, a fim de tornar claro quais dados são tratados ao longo de toda a cadeia. A ausência de tais

31 EILAM, Eldad. **Reversing**: Secrets of Reverse Engineering. Indianapolis: Wiley Publishing Inc. 2005. p. 3-4.
32 Idem. p. 8-9.

explicações é ainda mais grave quando se considera o papel fundamental que um parecer técnico deve ter diante da complexidade de um software de Inteligência Artificial.

A título de exemplo, não se pode ter acesso a todos os dados que um software como o motor de busca do Google ou a rede social Facebook têm de determinado usuário apenas acessando login e conta daquele usuário. Sabe-se, na verdade, que há muito mais informação no banco de dados dessas empresas em comparação ao que é disponibilizado em um reduzido painel de controle fornecido ao usuário, ou mesmo às empresas que compram publicidade nessas ferramentas.

Assim, afirmações como a de fls. 444-445, analisando o vídeo publicitário fornecido pela própria AdMobilize acerca de como, em teoria, funcionaria o software, carecem de fundamentação técnica robusta. Ao se verificar o trecho "*o quadrado muda de cor, indicando, portanto, que o software não guarda informações pessoais, pois apesar de o software já ter detectado essa pessoa anteriormente, ele gera novos dados anonimizados, como se de fato fosse outra pessoa*", constata-se que a fundamentação do parecer se baseia em elemento de valor técnico nulo, a mera cor do quadro colocada no vídeo publicitário. Não se esclarece, no parecer técnico, de que forma o vídeo é fiel ao que efetivamente faz o software, ou mesmo o que significam as cores e quadrados para o código-fonte que opera o sistema da AdMobilize.

As representações gráficas que aparecem na *dashboard* e no vídeo publicitário podem não ser as únicas informações geradas pelo software, sendo possível o processamento e armazenamento de informações que geram bancos de dados somente em segundo plano, que podem ser acessados por usuários com acesso administrativo ao sistema, como, por exemplo, programadores da AdMobilize. A título exemplificativo, no próprio sistema "Google Docs", em que se pode escrever colaborativamente, a cada vez que um mesmo usuário logado abre o arquivo em seu navegador, ele recebe uma cor diferente; isso não significa que o sistema não o reconheceu ou que ele está anônimo.

Dessa forma, o parecer técnico não pode ser considerado conclusivo, uma vez que não apresenta parâmetros técnicos do funcionamento do algoritmo, sobre o fluxo de dados entre as câmeras, a AdMobilize e a ViaQuatro, ou as eventuais possibilidades de armazenamento ou não de identificador único dos usuários do serviço de metrô.

Assim, ressalta-se que o parecer técnico ateve-se, em suas conclusões (i) a (vii) de fls. 447, a realizar afirmações sobre o resultado final do processamento disponibilizado ao cliente (dados em formato csv), bem como realizar afirmações inconclusivas, como "não foram identificadas quaisquer evidências", o que não significa que ficou suficientemente demonstrado se há ou não tratamento de dados pessoais.

Quanto ao ponto (viii) das conclusões, em que o parecer técnico conclui que "o software da 'ADMobilize' não tem memória", não há como saber de que forma se chegou a esta suposta conclusão, visto que em momento algum aqueles pareceristas afirmam ter tido acesso aos

dados brutos - imagens que as câmeras gravam - ou ao pacote que elas enviam à solução AdMobilize para ser fornecido posteriormente o resultado no painel de controle. O acesso apenas a uma solução interativa de painel de controle para a ViaQuatro, bem como a e-mail enviado pelo software após o tratamento de dados não permitem constatar se o software tem memória ou não, pois são produtos que não demonstram claramente a origem das informações que apresentam.

Por fim, conforme a melhor doutrina, o parecer técnico tem como objetivo trazer clareza ao processo[33], auxiliando o juízo a respeito das técnicas e conhecimento específicos envolvidos no caso a ser apreciado. Nesse sentido, o parecer técnico oferecido no presente caso deveria esclarecer sobre o modo de funcionamento da tecnologia em questão, e não se restringir apenas à análise visual dos painéis de controle do software disponibilizados ao cliente final.

A finalidade de trazer mais clareza técnica ao processo está relacionada à apresentação e explicação significativa da tecnologia em questão. Não é possível que se configurem como suficientes os elementos analisados no parecer apresentado pela ViaQuatro, porque tais elementos não demonstram o funcionamento mais detalhado do sistema, o verdadeiro fluxo de dados a que a AdMobilize tem acesso, e se, porventura, foram utilizadas técnicas de anonimização adequadas.

Cabe acrescentar, ainda, que igualmente inconclusiva se mostra a ata notarial solicitada ao 26º Tabelionato de Notas (fls. 486-497). Isso porque o documento em questão, assim como o parecer técnico do IBP, refere-se somente a aspectos superficiais da tecnologia ofertada pela AdMobilize, acrescidas de informações situacionais sobre a ocasião da confecção da ata - informações estas que limitam-se à descrição da interface do software utilizado nas Portas Interativas Digitais - juntamente com o detalhamento situacional sobre a ocasião da confecção da ata, o que não atribui valor técnico-probatório ao documento.

A referida ata notarial, portanto, não permite que se obtenha conhecimento acerca dos processos envolvidos no funcionamento do software da AdMobilize, haja vista que para tal seria necessária uma análise técnica do "*back end*" da tecnologia, como abordado durante a análise do parecer técnico do IBP acima. Dessa forma, também é impossível realizar qualquer inferência tecnicamente sustentável a partir da ata notarial juntada aos autos do presente processo.

VIII. Casos internacionais com elementos comuns ao feito

O uso de tecnologias de detecção e/ou reconhecimento facial para fins comerciais, por meio da prática dos displays interativos, pode ser encontrado em outros países do mundo, oferecendo parâmetros de análise para o caso em questão. Pode-se traçar o

33 THEODORO, Humberto Jr. **Curso de Direito Processual Civil**. Volume 1. 56ª edição. Rio de Janeiro: Editora Forense. 2015. p. 1262.

início dessa tendência até meados do ano de 2012, quando a Nike iniciou sua campanha publicitária denominada "Nike Free", por meio da qual indivíduos poderiam interagir com um tênis mediante o reconhecimento de seus movimentos faciais por uma webcam[34].

Desde então, observou-se um aumento gradativo no uso dessas tecnologias, bem como de sua precisão, o que resultou em uma recente intensificação da presença dessas técnicas. Diversas empresas de publicidade passaram a ofertar serviços de implementação de *smart ads* – e estes, por sua vez, superaram o ambiente exclusivamente digital e passaram a ocupar também o mundo físico, inclusive espaços públicos.

De acordo com estudo realizado em 2015 pela First Insight[35], 75% dos clientes alegam que não comprariam em uma loja que empregasse tecnologias de reconhecimento facial para fins comerciais. Esse percentual foi reduzido para 55% quando os entrevistados foram questionados acerca do uso de reconhecimento facial que resultasse em uma contraprestação benéfica e individualizada para os clientes – na forma de descontos, por exemplo.

Ambas as estatísticas indicam que a aceitação desse tipo de tecnologia não é pacífica entre os consumidores que transitam pelos locais de captação de suas imagens. Cabe também mencionar que 70% dos entrevistados nem ao menos sabiam o que são os "beacons", ou seja, os sensores utilizados na leitura facial. Isso reforça a assimetria de informação entre aqueles que implementam a tecnologia e os que têm suas imagens capturadas.

A discussão sobre detecção facial no âmbito das relações de consumo ganhou evidência também na Noruega. Um caso ocorrido nesse país, e que traz paralelos com o presente feito, diz respeito a uma pizzaria em Oslo, chamada Peppe's Pizza. Em 2017, um consumidor passava em frente ao restaurante e reparou que o anúncio digital do estabelecimento havia passado por alguma falha de software, que tornou visível a área de trabalho do computador ligado à tela em questão. As imagens a seguir representam as informações que constavam na tela:

Figura 3: Imagem do display interativo na frente da Peppe's Pizza. A câmera, voltada para um espaço público, pode ser

34 NIKE FREE LACE (case study video). Disponível em: https://vimeo.com/123158970. Acesso em 09/04/2019.
35 FIRST INSIGHT. Consumer Survey Report. Agosto de 2018. Disponível em: https://cdn2.hubspot.net/hubfs/160569/First_Insight-In_Store_Experience_Report.pdf. Acesso em 09/04/2019.

vista acima da tela, apesar de pouco perceptível para pessoas desinformadas sobre a tecnologia. Fonte: Diinside

Figura 4: Detalhe do software que funcionava em segundo plano no display interativo, registrando informações sobre os transeuntes.Fonte: Diinside

O consumidor percebeu que a janela exibida na tela parecia preencher-se com informações relativas a ele próprio: seu sexo, idade aproximada, se usava óculos, se tinha pelos faciais, seu tempo de atenção ao conteúdo mostrado na tela e sua reação ao mesmo. Após postar a foto em suas redes sociais , ela passou a ser fortemente compartilhada e foi motivo para muitos questionamentos[36], em que se percebe o receio gerado entre os consumidores quanto ao uso dessa tecnologia. A repercussão do caso fez com que ele se tornasse manchete em veículos de notícias ao redor do mundo[37]. Receosos com a repercussão negativa que haviam alcançado, os responsáveis pela Peppe's Pizza rápida e voluntariamente removeram o sensor facial do anúncio, alegando tratar-se apenas de um período de testes e que a tecnologia estava prevista para ser removida naquela mesma semana. Dessa forma, recuaram em relação à prática e não prestaram esclarecimentos técnicos sobre a tecnologia, para além das capturas de tela que o consumidor havia divulgado.

Importante pontuar, contudo, que, quando entrevistado sobre o caso, o conselheiro sênior da autoridade de proteção de dados da Noruega, Stian D. Kringlebotn, manifestou

36 Alguns exemplos de fóruns onde a matéria foi discutida: https://www.reddit.com/r/norge/comments/67jox4/denne_kræsjede_skjermen_på_peppespizza_viser_en/dgrltgl/ e https://linustechtips.com/main/topic/777448-pizzeria-billboard-in-oslo-analyzes-people/

37 Algumas reportagens noticiando o caso: TURTON, William. **A restaurant used facial recognition to show men ads for pizza and women ads for salad**. The Outline. 2017. Disponível em: <https://theoutline.com/post/1528/this-pizza-billboard-used-facial-recognition-tech-to-show-women-ads-for-salad?zi=iq3iltht&zd=6>. Acesso em: 09/04/2019; VENTURA, Felipe. **Outdoor de pizzaria usava câmera para escanear e analisar rosto das pessoas**. Tecnoblog. 2017. Disponível em: https://tecnoblog.net/214548/pizzaria-camera-analise-facial/. Acesso em 09/04/2019; STOKKE, Ole. **Reklamer på Oslo S med kameraer analyserer fjeset ditt** - Reklameskilt ser hvem du er *[Advertise in Oslo with cameras that analyze your face - Advertisement signs see who you are]*. Dinside. 2017. Disponível em: https://www.dinside.no/okonomi/reklameskilt-ser-hvem-du-er/67552025. Acesso em 09/04/2019; STOKKE, Ole. **Peppes Pizzas overvåkningsreklamer er fjernet** *[Peppe's Pizza's surveillance ads removed]*. Diniside. 2017. Disponível em: https://www.dinside.no/okonomi/jeg-synes-det-er-skummelt/67560027. Acesso em 09/04/2019.

considerável receio sobre a tecnologia de detecção facial para fins comerciais. Segundo o conselheiro, como uma câmera é utilizada para captura e tratamento das estruturas faciais dos consumidores, o regulamento vigente na Noruega acerca do uso de câmeras de segurança seria aplicável ao caso, a fim de preservar os direitos das pessoas que passavam pelo local. Ademais, o conselheiro pontuou que, a partir desse ponto de vista, a prática da Peppe's Pizza seria considerada ilegal. Isso porque o uso de câmeras de vigilância da Noruega exige uma autorização expressa e justificada, com o fim de salvaguardar o direito à imagem e à privacidade da população, o que reflete a preocupação em relação aos direitos dos consumidores, cuja detecção facial para fins publicitários não seria reconhecida como um motivo legítimo para autorizar a pizzaria a utilizá-la.

A experiência internacional e as perspectivas da sociedade, nas quais a detecção facial foi empregada, demonstram a relevância da decisão deste feito. Isso porque o presente julgamento apresenta um caso fronteiriço para o Direito – tanto de um ponto de vista nacional quanto internacional - em matéria de tecnologia. Assim, trata da criação de um precedente relevante para o cenário de proteção de dados pessoais no Brasil, em relação a processamento automatizado de grande escala, em local público, e com a utilização de tecnologia de inteligência artificial. Dessa forma, é importante considerar obrigações relativas à transparência, informação, segurança e cautela daqueles que transitam na Linha Amarela do metrô da maior cidade da América Latina.

IX. Ainda que eventualmente haja anonimização adequada dos dados, quais as implicações jurídicas da assimetria de informação com os consumidores?

IX.I. Quanto à adequação entre meios e fins

A ViaQuatro, ao prestar serviços de transporte urbano, é concessionária de serviço público. Assim, está sujeita à legislação sobre serviço público e também aos termos e limites fixados em seu contrato de concessão - Contrato nº 4232521201 - Concessão Patrocinada para fins da Operação dos Serviços de Transporte de Passageiros da Linha 4 Amarela do Metrô de São Paulo.

O metrô é um serviço público com milhões de usuários[38], os quais não dispõem de alternativas para se locomoverem até seus trabalhos, lares e outros locais da cidade. Os usuários do metrô esperam, deste serviço, a capacidade de locomoção entre um ponto e outro da estrutura urbana. Ou seja, não faz parte de sua atividade-fim realizar pesquisas demográficas com fins de mercado. Tampouco a realização desse tipo de coleta de dados, a qual é feita com a participação compulsória dos usuários da rede metroviária, pode ser considerada essencial à adequada prestação dos serviços.

38 "Linha 4-Amarela transporta mais de 3,5 milhões de passageiros durante o carnaval". Fonte: <http://www.viaquatro.com.br/imprensa/noticias/linha-4-amarela-transporta-mais-de-3-5-milhoes-de-passageiros?releaseid=31507>.

Coletar dados sobre quantas pessoas transitam poderia ser considerado útil no cálculo de horários, quantidade de trens e a configuração dos vagões na linha da qual a ViaQuatro é concessionária. Entretanto, as demais informações que estão sendo captadas pelos dispositivos de detecção facial, alegadamente de forma anônima, com dados sobre gênero, idade, reação, não guardam vínculo com a melhoria da atividade de transporte concedida pelo poder público.

Ao compelir os usuários a participar de uma pesquisa, há violação aos direitos dos usuários e descumprimento com os deveres. E isso ocorre ainda que eles sequer saibam ao certo que tipo de informação é coletada (algo que não ficou inteiramente esclarecido nos autos, pois o parecer técnico foi incompleto).

O fato de saberem a posteriori que uma máquina detectava seus rostos a fim de computar reações e características do público não torna esta prática menos intrusiva em relação a todos os usuários do sistema de metrô. Exigir que, para poder locomover-se pela cidade, uma pessoa tenha de colaborar com pesquisas de mercado que em nada se vinculam à prestação do serviço metroviário viola a adequação entre meios e fins da prestação do serviço, obrigação prevista no art. 5º, IV, da Lei 13.460 de 26 de junho de 2017. E a participação na pesquisa é uma exigência imposta ao usuário do transporte público, vez que não é uma situação na qual ele tem o poder de não participar, o que fere diretamente aquele dispositivo legal.

IX.II. Quanto às práticas permitidas pelo contrato de concessão

Seguindo na análise da situação, percebe-se que a concessão em comento trata-se de uma parceria público-privada[39], o que tornaria possível que a concessionária se utilizasse das permissões concedidas enquanto prestadora desse serviço para, no exercício delas, auferir lucro. Este ponto é comprovado pelo contrato de concessão apresentado, o qual permite, em sua cláusula 10.1.1, o uso do espaço para exploração comercial.

Neste sentido, percebe-se que o uso comercial tem um caráter exclusivo, eis que integra o contrato em que a única concessionária é a ViaQuatro. Assim, ela detém isoladamente os direitos de explorar atividades naquele local sob sua administração, no que concerne aos metrôs e estações. Isso quer dizer que somente a concessionária tem a possibilidade jurídica de ceder onerosamente a terceiros espaço para anúncio, bem como instalar ali equipamentos como câmeras e telas.

Assim, a única empresa que possui direitos de exploração comercial do espaço das linhas e metrôs da ViaQuatro é a própria. Por isso, a concessionária exerce um poder desequilibrado em relação àquele mercado, em que não há nenhuma outra empresa apta a fazer o levantamento feito por ela, que torna as informações demográficas por ela coletadas

39 Fonte: <http://www.viaquatro.com.br/a-via-quatro>.

valiosas para venda a terceiros.

Devido a este valor econômico, esta atividade de detecção facial integra prática comercial. E, nesse âmbito, seu caráter é abusivo, pois uma pessoa, ao utilizar o serviço de transporte público, contribui obrigatoriamente com uma atividade de pesquisa mercadológica, sem a possibilidade de não fazê-lo. Isso fere a liberdade de escolha dos cidadãos. Ou seja, além de obrigar seus usuários a integrar pesquisa demográfica compulsória, a ViaQuatro o faz com exclusividade, sendo a única empresa que tem esse poder naqueles espaços, o que torna essa coleta de informações algo vantajoso economicamente à ViaQuatro.

Esta prática está em dissonância com a previsão contratual de "restrições à publicidade", na cláusula 10.1.2 do contrato de concessão, a qual afirma serem proibidas atividades que atentem contra a legislação, a moral e os bons costumes.

Cabe lembrar o que diz Cavalieri Filho em sua obra sobre direito do consumidor: "o lucro é permitido e primordial numa economia capitalista, mas não pode transbordar para o abuso, para a exploração dos consumidores [...]"[40].

A atividade de mercado, para ser adequada ao contrato de concessão, não pode ferir o dever de informar e a livre escolha do indivíduo sobre suas ações. Não se pode obrigar o cidadão a participar na geração de lucro da concessionária. No momento em que são detectadas a presença e a reação emocional dos usuários por aparelhos que não exigem consentimento nem possibilitam *opt out*, os usuários estão tendo essa liberdade violada. Ademais, ao não publicizar que esta coleta é feita, a concessionária incorre em negligência quanto ao dever de informar.

IX.III. Quanto ao dever de informar

Fora as previsões mais amplas sobre a transparência e o dever de informar, constantes nos artigos 4º, caput, e 6º, III, do CDC, este dever também é previsto nos artigos 46 e 54 da mesma lei, que estabelecem que as cláusulas de um contrato de consumo - mais especificamente, de adesão, como é o do caso sob análise - devem ser claras ao consumidor, para que ele tenha fácil compreensão sobre os termos da relação com o fornecedor.

Na condição de fornecedora de serviços na modalidade de adesão, em que os usuários do metrô não têm o poder de negociar os termos da contratação do serviço de transporte, a ViaQuatro tem o dever de observar essa norma. Deve ela informar ostensivamente de maneira compreensível a todo usuário todos os termos de uso daquele serviço.

A concessionária, conforme é constatado pela leitura dos autos, não manteve avisos, em suas estações e trens, de que os usuários estavam submetidos a coleta de suas reações às

40 CAVALIERI FILHO, Sérgio. Programa de direito do consumidor. 2a. ed. São Paulo: Atlas, 2010. p. 150

portas interativas. O fato de os usuários da linha de metrô sob concessão da ViaQuatro não saberem que, ao adquirirem um bilhete e usarem o trecho, também estariam participando de pesquisa com fins comerciais, infringe o dever de informar.

Esse dever é a base para que haja a escolha consciente e motivada do consumidor sobre se deseja ou não participar da atividade geradora de lucro do fornecedor de bens e serviços. O consumidor usuário dos serviços de metrô, ao ser submetido de forma obscura a uma atividade na qual seus dados pessoais geram informação, que é transformada em produto pela concessionária, é tratado como matéria-prima.

Neste caso, a violação é relativa ao preço cobrado sobre os bens e serviços adquiridos - vez que uma parte do pagamento por utilizar o serviço de transporte público é na forma de dados pessoais obtidos diretamente a partir do comportamento dos usuários. Como os usuários participam de tal atividade, e por ela integrar o preço do serviço prestado pela concessionária, é direito desses usuários saberem deste custo que lhes é imposto.

Uma importante característica humana sobre a qual é fundado nosso sistema jurídico é a autodeterminação, ou seja, a capacidade de decidir e determinar a própria identidade, as atividades que se quer integrar e que definem as experiências que o sujeito tem ao longo de sua vida. Em casos envolvendo o tratamento de dados pessoais, fala-se, mais especificamente, do conceito de autodeterminação informacional[41], que consiste na ideia do controle do indivíduo sobre seus dados e informações, exigindo-se, portanto, o consentimento - e, para tal, a informação - dos titulares para possibilitar o uso dessas informações por terceiros. Ocultar que uma pessoa participa de determinada situação, especialmente considerando que a atividade desta pessoa gerará lucro a terceiro, é ferir a autodeterminação dela enquanto sujeito.

IX.IV. Quanto à liberdade de escolha do consumidor

Apenas a informação quanto à coleta de dados para fins de levantamento comercial também não é suficiente; pois, mesmo que informado, se não houver escolha sobre participar ou não, o sujeito continua sendo violado em sua autodeterminação. Não é a informação sobre violação de direitos uma forma de anular essa violação.

Os usuários estão gerando, com sua detecção facial compulsória, um lucro exclusivo à concessionária - algo que foge totalmente à exploração comercial e atividade mercadológica permitida, pois pessoa nenhuma pode ser obrigada a participar de atividades que geram lucro para terceiro que presta serviço público, sem que tenha consciência ou escolha sobre isso.

Além da liberdade do consumidor sobre em que situações deseja onerosamente

41 Bruno Ricardo Bioni aponta para o princípio da autodeterminação informacional, garantida por meio da informação e do consentimento do titular de dados, como preceito fundamental da proteção do consumidor nos dias atuais.

adquirir bens e serviços, tendo para isso direito de ser informado da extensão do ônus (seja o pagamento feito com dinheiro ou com outros bens e serviços, como a monetarização das informações extraídas de seus dados pessoais - emoções detectadas ao ver a publicidade), o cidadão tem, no preâmbulo da Constituição, direito à liberdade, consagrada no conjunto de direitos sociais e individuais sobre os quais se erige nossa sociedade.

No portal da concessionária, lê-se que é direito do usuário "obter e utilizar o serviço com liberdade de escolha, observadas as normas estabelecidas pelo Estado de São Paulo"[42].

É pertinente apontar que as relações entre a concessionária de serviço público e seus usuários deve se pautar pela boa-fé, ou seja, nas palavras de Cláudia Lima Marques, "atuação refletida, pensando no outro, no parceiro contratual, respeitando-o, respeitando seus interesses legítimos, suas expectativas razoáveis, seus direitos, agindo com lealdade, sem abuso, sem obstrução, sem causar lesão ou desvantagem excessiva, cooperando para atingir o bom fim das obrigações: o cumprimento do objetivo contratual e a realização dos interesses das partes"[43].

A exploração comercial permite contratualmente que haja atividade geradora de lucro, porém, esta atividade deve se basear na liberdade do usuário sobre a participação ou não dela. A prática de obrigar o usuário a gerar lucro à concessionária por meio de situação inclusa em outro bem adquirido por ele pode ser, em exercício de analogia, equiparada à situação de venda casada.

Poder-se-ia arguir, sob o fundamento desta permissão contratual, que a atividade de coleta de dados demográficos para fins comerciais é semelhante à atividade, lícita e já consolidada em concessões, de aluguel de espaços para anúncios publicitários. Isto é, terceiros estariam remunerando a concessionária em troca de alguma vantagem para eles próprios, em que o usuário não escolhe se quer ver aquele anúncio ou não.

Ocorre que a situação narrada não se equipara à de ofertar espaço para anúncios publicitários, e isso pode resumir-se em um motivo: o que se está disponibilizando como contrapartida lucrativa não advém de algo de propriedade da concessionária, mas de seus usuários. Isto é, em vez de cobrar um valor do terceiro para ofertar em contrapartida *um espaço* detido e controlado pela concessionária nos trens ou estações, na situação ora sob análise cobra-se valor para entregar em contrapartida *dados obtidos a partir de atividade dos usuários* que transitam pelos trens e estações[44].

Considerando que os usuários não estão vinculados comercialmente à concessionária

42 Fonte: <http://www.viaquatro.com.br/guia-do-usuario/direitos-deveres>.

43 MARQUES, Cláudia Lima. Contratos no código de defesa do consumidor. 5a. ed. São Paulo: Revista dos Tribunais, p. 216.

44 Esse fenômeno, em que os usuários de determinado serviço são usados como matéria-prima para seus produtos lucrativos, é a base do modelo denominado "capitalismo de vigilância" pela pesquisadora e professora da Harvard Business School, Shoshana Zuboff. Ela alerta para os riscos à liberdade e autonomia levantados por esse sistema de produção em ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização da informação. In: **Tecnopolíticas da vigilância**: perspectivas da margem.BRUNO, Fernanda et al (org.). Boitempo, 2018

para além da aquisição do serviço de transporte, não poderiam estar participando diretamente na contrapartida desta atividade geradora de lucro sem poderem escolher informadamente acerca dela.

IX.V. Quanto ao preço oculto do serviço fornecido - vantagem manifestamente excessiva

Isto é, se um consumidor não pode ser obrigado a adquirir um produto anexado a outro que ele não escolhe, por óbvio é porque o preço de ambos está incluído no preço do primeiro produto e isso fere o dever de transparência e a liberdade de escolha sobre o que se deseja adquirir. Isto é o que ocorre com o usuário de metrô ao ser obrigado a gerar lucro para a concessionária com a captação de seus dados; ele não apenas paga em dinheiro para usar o serviço de transporte, ele paga à concessionária com seus dados, de maneira oculta e sem qualquer possibilidade de escolha.

A situação se enquadra também na hipótese de publicidade enganosa por omissão, em que o anúncio deixa de afirmar algo relevante e que seria essencial na conduta do consumidor. Ao omitir que todos os usuários de seu sistema de transporte integrariam obrigatoriamente pesquisa demográfica por meio de detecção facial compulsória, a concessionária omitiu fator essencial do que estava sendo adquirido por quem utilizava o transporte urbano por ela fornecido.

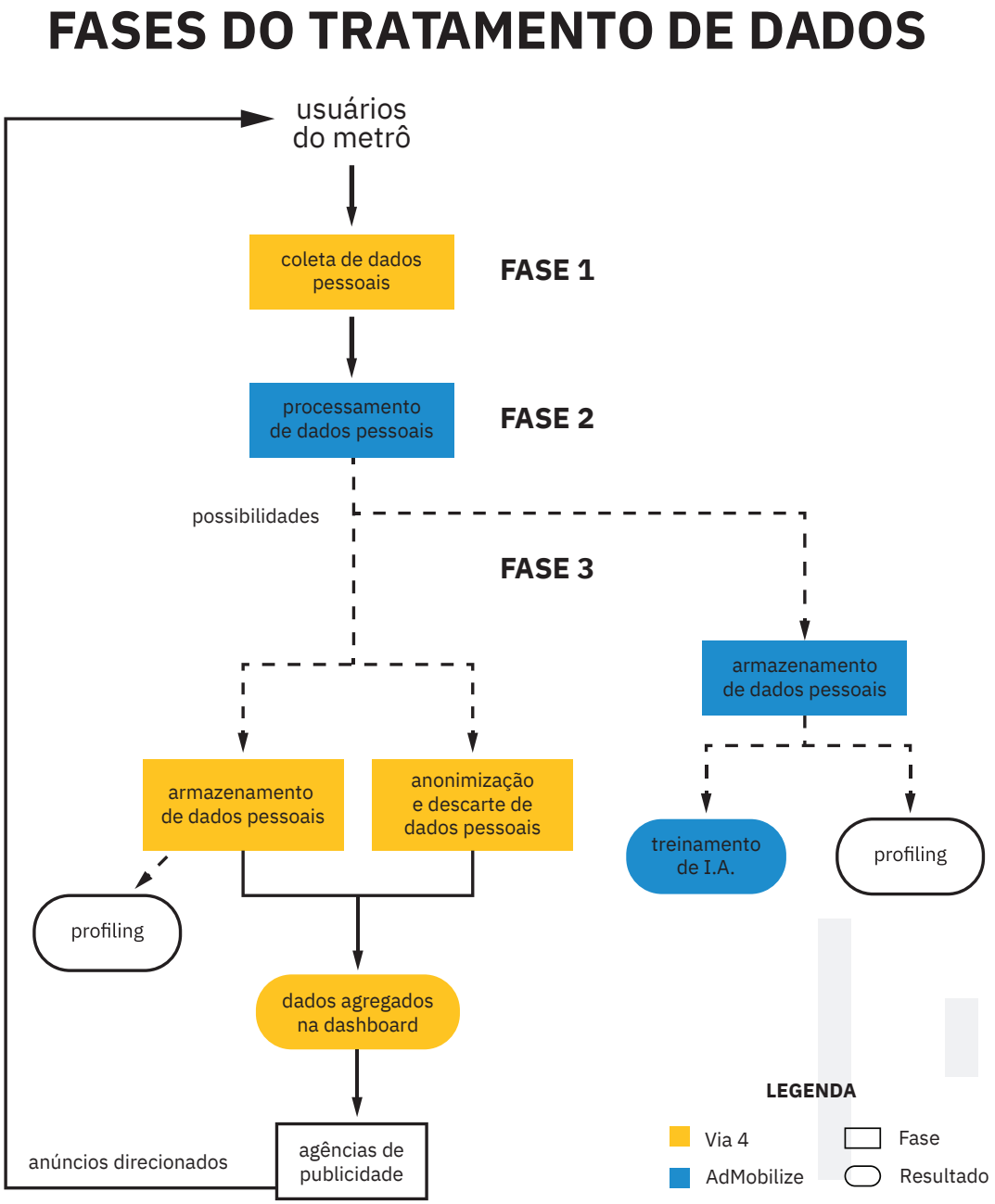
Ao adquirir e usar o serviço de metrô prestado pela ViaQuatro, o cidadão também fornece dados com sua participação na pesquisa demográfica ali realizada, prática abusiva indicada na hipótese do art. 39, do CDC, o qual aponta que é vedado ao fornecedor “exigir do consumidor vantagem manifestamente excessiva”. Ainda, viola previsão do art. 6º, CDC, que afirma, no inciso IV, serem direitos básicos do consumidor proteção contra “métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas”.

O usuário resta sem liberdade de escolha sobre o que adquire e há total opacidade sobre o preço real do bem adquirido, que fica mascarado por uma situação inevitável ao consumidor

X. Conclusões

Verifica-se, a partir do material que consta no processo, que a situação analisada consiste na violação à Constituição Federal, aos direitos dos Consumidores e Usuários de Transporte Público, bem como aos direitos de proteção de dados pessoais e direitos dos consumidores pela concessionária de serviço público de transporte ViaQuatro, por meio do serviço Portas Interativas, que captam reações dos usuários a anúncios publicitários, por meio de câmeras nas estações.

O procedimento constitui-se em 3 fases técnicas às quais se deve dar atenção: 1) coleta de imagens dos rostos das pessoas por meio das câmeras; 2) tratamento destas imagens para elaboração do modelo matemático do rosto, e subsequente extração das informações de idade, gênero, e emoção sentida ao se visualizar a publicidade; e 3) suposta eliminação das imagens e do modelo matemático dos rostos, com a suposta agregação das informações sobre as emoções detectadas dos usuários por técnica de anonimização, encaminhado à ViaQuatro



Fonte: autoria própria

Existe, nas fases 1 e 2, o claro tratamento de dados pessoais relativo à imagem coletada dos usuários do metrô e a subsequente elaboração do modelo matemático do rosto (dado pessoal sensível), para inferência das emoções sentidas no momento da visualização da publicidade pelo algoritmo de I.A. da AdMobilize. Na fase 3, ocorre o repasse dos dados supostamente anonimizados por meio de agregação à ViaQuatro. Entretanto, a ViaQuatro não demonstrou se existe e qual seria a técnica de anonimização utilizada nessa fase do processamento dos dados. A transparência em relação à técnica utilizada é importante pois a anonimização não é um processo caracterizado como absoluto, mas sim um que admite gradações, conforme o estado de desenvolvimento da tecnologia e o contexto em que os dados pessoais são tratados. Para dados mais sensíveis, como as informações biométricas e sobre emoções captadas, o adequado seria a utilização de técnicas mais robustas, de forma a se evitar a possibilidade de reversão da anonimização, ainda mais quando se considera a maior facilidade atual de cruzamento de diversas categorias de dados, a qual facilita a reidentificação dos dados. Ademais, acrescenta-se que a anonimização é uma medida abarcada pelo atual arcabouço normativo esparso de proteção de dados pessoais brasileiro, principalmente para garantir inviolabilidade da segurança da informação, como estabelecido, pelo Decreto nº 8.771/2016. Ainda em relação à Fase 3, também resta dúvida razoável, em relação à AdMobilize, sobre a real eliminação dos registros individualizados, seja das imagens, seja do modelo matemático dos rostos associados com as emoções detectadas.

Assim, é imprescindível considerar que os documentos juntados pela ViaQuatro não apresentam caráter abrangente, tampouco cientificamente substanciais, sobre o procedimento de coleta e tratamento de dados realizada por meio das Portas Interativas. Assim, não ficam evidenciadas quais informações são transmitidas ao software AdMobilize, por quais locais e servidores essas informações transitam e se são armazenadas ou não de maneira individualizada em alguma das etapas, para se verificar se a AdMobilize armazena dados pessoais, e se houve anonimização adequada dos dados encaminhados à ViaQuatro.

Mesmo que se considere que a anonimização ocorreu adequadamente para envio dos dados à ViaQuatro e que a AdMobilize não armazena nenhum dado, ainda assim, o tratamento como um todo possui vícios nas fases 1 e 2 por haver violação do direito dos usuários no que toca o dever de informá-los sobre o tratamento, bem como a liberdade de escolha de participar ou não desta atividade (consentimento sobre o uso de sua imagem). Essa situação, por si só, já viola a autodeterminação, que fundamenta nosso sistema de direitos. Assim, a cadeia de tratamento se torna viciada, devido à ilicitude inicial, à semelhança do teoria dos frutos da árvore envenenada.

Reitera-se, a situação narrada não se equipara à de ofertar espaço para anúncios publicitários, e isso pode resumir-se em um motivo: em vez de ceder onerosamente a uma empresa publicitária *um espaço* detido e controlado pela concessionária nos trens ou estações,

na situação ora sob análise o bem lucrativo ofertado pela concessionária são *dados obtidos a partir de atividade dos usuários*, seus clientes, que transitam pelos trens e estações.

Dado que a ViaQuatro é responsável, como concessionária, por certificar-se de que não há violação aos direitos de seus usuários, essa responsabilidade permeia também as contratações que realize com terceiros. A dúvida razoável sobre o que efetivamente ocorre com os dados na fase 3 é fundada no valor econômico que softwares de reconhecimento de rostos e emoções detêm no mercado, e na relevância que um banco de dados abrangente pode ter para o treinamento desses algoritmos de inteligência artificial.

A existência da anonimização e seu grau de adequação não afastam a violação apontada nas fases iniciais do processamento, mas devem ser levadas em conta pelo judiciário no que se refere à resposta às práticas de cada empresa. Esse parâmetro pode evitar a possibilidade de duas situações indesejadas ao consumidor: i) que as empresas insiram os custos judiciais com violações em seu custo de oportunidade e se neguem a produzir provas do que efetivamente é feito dos dados, sem que se possa saber a extensão dos danos causados aos usuários, os níveis de anonimização e segurança, assim como compreensão do funcionamento da cadeia que envolve dados pessoais ou ii) que haja forte antagonização entre empresas de tecnologia e sistema jurídico brasileiro, o que dificulta o andamento de projetos regulatórios sobre tecnologia, influenciado por receio do setor industrial de novas situações de instabilidade. Essas situações podem gerar um cenário de retrocesso aos direitos dos consumidores e levar ao emprego cada vez mais obscuro e distante do conhecimento da população de tecnologias que tratam seus dados.

É fundamental que a decisão relativa ao caso tenha em vista os pilares de proteção contra tratamentos automatizados e aqueles relativos à autodeterminação, presentes tanto no quadro de direitos constitucionais e consumeristas , quanto na lógica das normas esparsas de proteção de dados em vigor, como o Marco Civil da Internet.

Não há dúvida, portanto, que houve dano, vez que todo o exposto indica que é evidente a violação aos direitos coletivos relacionados ao consentimento, à informação e autodeterminação dos usuários do metrô. Destaca-se, no entanto, que os documentos juntados pela ViaQuatro não são suficientes para excluir a possibilidade de dano causado caso existam dados pessoais armazenados de forma insuficientemente anonimizada ou não anonimizada, que é ainda mais grave. Considerando que um possível armazenamento levaria ainda a tratamento ulterior de dados individualizados, o que pode levar à re-identificação das pessoas e de suas emoções, estariam inerentes a essa situação todos os riscos vinculados ao tratamento de dados pessoais, e, mais gravemente, de dados sensíveis, possibilitando discriminações a essas pessoas e ocasionando dano de cunho moral a todos os usuários da linha de metrô.

Luiza Couto Chaves Brandão
Diretora plenipotenciária do Instituto de Referência em Internet e Sociedade

Odelio Porto Junior
Vice-Diretor do IRIS
Pesquisador

Lahis Pasquali Kurtz
Pesquisadora IRIS
OAB 70.722

Victor Barbieri Rodrigues Vieira
Pesquisador IRIS
Acadêmico em Direito

Davi Teófilo Nunes de Oliveira
Técnico em Informática
Acadêmico em Direito