Ao Juízo da ___ Vara da Fazenda Pública do Foro Central da Comarca da Capital – SP

A **DEFENSORIA PÚBLICA DO ESTADO DE SÃO PAULO**, por seus Núcleos Especializados de Defesa do Consumidor (NUDECON), de Cidadania e Direitos Humanos (NCDH), de Defesa da Diversidade e da Igualdade Racial (NUDDIR) e da Infância e Juventude (NEIJ), pelas Defensoras Públicas e Defensores Públicos que os coordenam e esta subscrevem, com lastro no artigo 5o, inciso LXXIV e art. 134 da Constituição Federal, artigo 5o, inciso II da Lei no 7.347/1985, Lei no 8.078/90, artigo 4o, inciso XI da Lei Complementar Federal no 80/1994 e artigo 5o, inciso VI, alínea 'd' da Lei Complementar Estadual no 988/2006;

A **DEFENSORIA PÚBLICA DA UNIÃO,** instituição essencial à função jurisdicional do Estado, a quem incumbe, como expressão e instrumento do regime democrático,

fundamentalmente, a orientação jurídica, a promoção dos direitos humanos e a defesa, em todos os graus, judicial e extrajudicial, dos direitos individuais e coletivos, dos necessitados, pela **Defensoria Regional de Direitos Humanos de São Paulo**, com fundamento no art. 5o, LXXIV e no art. 134, ambos da Constituição Federal, no art. 4o, I, VII, VIII, X e XI, da Lei Complementar n° 80/94, e no art. 5o, II, da Lei no 7.347/85;

IDEC - INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR, entidade civil sem fins lucrativos, legalmente constituída desde 1987, inscrita no CNPJ sob o no 58.120.387/0001-08, com sede na Rua Dr. Costa Júnior, 543 - Água Branca, São Paulo - SP, 05002-000, endereço eletrônico juris@idec.org.br, representado por sua Coordenadora Executiva, Carlota Aquino e por seus procuradores infra-assinados (Doc. 1),

INTERVOZES – COLETIVO BRASIL DE COMUNICAÇÃO SOCIAL, associação civil sem fins lucrativos, inscrita no CNPJ sob o no 06.040.910/0001-84, com sede na cidade de São Paulo, Estado de São Paulo, na Rua Rego Freitas, 454, 9o andar, CEP 01220-010, por seus advogados (Doc. 2),

ARTIGO 19 BRASIL, associação civil sem fins lucrativos, inscrita no Cadastro Nacional de Pessoas Jurídicas/MF sob o n. 10.435.847/0001-52, com sede na Rua João Adolfo, 118, conjunto 802, CEP 01050-020, Centro, São Paulo, SP, endereço eletrônico denisedora@article19.org, por seus advogados (Doc. 3),

vêm respeitosamente à presença de Vossa Excelência, com fundamento na Constituição da República Federativa do Brasil e nas Leis 7.347/85, 8.078/90 e 13.709/2018 propor

AÇÃO CIVIL PÚBLICA

com pedido de tutela de urgência assecuratória

em face da **COMPANHIA DO METROPOLITANO DE SÃO PAULO**, pessoa jurídica de direito privado, empresa pública inscrita no CNPJ sob no 62.070.362/0001-06, com sede e endereço para citação e intimação na Rua Augusta, 1626, CEP 01304-902, Cerqueira César, São Paulo/SP, por seu Presidente Sr. Silvani Alves Pereira, nos termos a seguir expostos.

1. Resumo da demanda

A disciplina da proteção de dados pessoais é nova, ainda que derive de direitos à privacidade e à intimidade há muito reconhecidos. No Brasil, a proteção de dados pessoais foi legalmente introduzida como um direito autônomo pela Lei nº 13.709/2018, a Lei Geral de Proteção de Dados (LGPD), diante da necessidade de estabelecer parâmetros e diretrizes para tutelar o dado pessoal, enquanto um novo bem jurídico central da vida digital.

Uma vez alçado à condição de bem jurídico especificamente tutelado, possuindo inclusive caráter de direito fundamental, conforme o art. 5º, LXXIX, incluído pela EC nº 115/2022, o dado pessoal passa a ser de controle de seu titular, com a finalidade de proteger os direitos fundamentais de liberdade e de privacidade, e o livre desenvolvimento da personalidade da pessoa natural, nos termos do artigo 1º da LGPD.

A LGPD descreve o que são dados pessoais, como protegê-los e impõe uma série de obrigações a entes públicos e privados, reconhecendo que o acesso, o armazenamento e o tratamento de tais dados pessoais encontram limites nos direitos de seus titulares. Entre os dados pessoais estão os dados biométricos, como impressões digitais, características da face[1] e até a forma de andar, estes considerados inclusive dados pessoais sensíveis (art. 5º, inciso II).

Esta ação civil pública se insere tanto nessa nova disciplina de proteção de dados pessoais, como em campos mais tradicionais de vedação à discriminação e de abuso de direito na prestação de serviços e execução de serviços públicos. Concretamente, esta ação relata fatos sobre a implementação de um sistema de reconhecimento facial - dados pessoais biométricos, sensíveis, portanto – dos usuários do metrô nas estações da empresa Ré.

Os fatos descrevem o processo licitatório internacional no qual foi contratado referido sistema pela Ré. Restou comprovado, a partir de questionamentos judiciais e extrajudiciais das Autoras, que tal sistema foi contratado e implementado à revelia das exigências previstas em múltiplos diplomas legais.

Os fatos desta ação civil pública comprovam que: i) a Ré Companhia do Metropolitano de São Paulo está implementando um sistema de reconhecimento facial em suas estações e faz tratamento de dados pessoais; ii) a Ré Companhia do Metropolitano de São Paulo faz reconhecimento facial dos usuários do metrô e trata dados pessoais sem consentimento dos seus titulares; iii) a Ré Companhia do Metropolitano de São Paulo faz reconhecimento facial e

[1] Segundo definição trazida pela Lei 13.079/2018: Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável.

trata dados pessoais dos usuários do metrô sem a devida transparência e disponibilização de informações necessárias aos titulares de referidos dados pessoais, como a finalidade do tratamento; iv) a Ré Companhia do Metropolitano de São Paulo não adotou quaisquer medidas para avaliação de impacto e mitigação de riscos inerentes à tecnologia de reconhecimento facial, conforme exigido em lei; v) o uso de tecnologia de reconhecimento facial pela Companhia do Metropolitano de São Paulo é abusivo, desproporcional e violador de direitos humanos, fundamentais e dos consumidores, além de ocasionar danos ao usuário do transporte público.

Primordialmente, tratando-se de sistema de reconhecimento facial que lidará com dados pessoais biométricos, há violações sucessivas à LGPD: aos princípios que regem a proteção de dados (art. 2º da LGPD), aos princípios da atividade de tratamento de dados pessoais (art. 6º da LGPD); aos direitos do titular de dados pessoais, envolvendo o direito à autodeterminação informativa (arts. 17 a 22 da LGPD); à obrigação de ter uma base legal válida que justifique o tratamento, bem como ao consentimento para captura de seus dados biométricos (art. 7º, I, e 8º e 11 da LGPD) – e especificamente ao consentimento qualificado exigido para lidar com dados de crianças e adolescentes (art. 14 *caput* e §1º da LGPD) -; e ao direito à informação sobre o processo de tratamento de seus dados (art. 9º, 18 e 19 da LGPD). Viola, também, as obrigações impostas àqueles que pretendem tratar dados na Administração Pública, desde a possibilidade em si de tratar tais dados biométricos (art. 7º, III da LGPD), passando pelos deveres em relação aos parâmetros para o controlador de dados (art. 37 da LGPD), à transparência e acesso a informações (art. 41 da LGPD) e às precauções quanto aos danos decorrentes da atividade (art. 42 da LGPD).

Porém, não são apenas violações à LGPD.

Os titulares de dados pessoais que têm seus direitos violados pela Ré são, também, usuários de serviços públicos, protegidos por código específico (**CDUSP**) e no âmbito da legislação consumerista (**CDC**), seja em relação aos seus dados, ao tratamento desses dados e às informações que devem estar disponibilizadas.

As violações massivas à privacidade, que se caracterizam como tecnologias de vigilância, afetam de maneira desproporcional alguns grupos. Em relação a crianças e adolescentes, perante os quais as políticas devem ser adotadas tendo em vista o seu melhor interesse (art. 6º do **ECA**), a proteção de dados pessoais assume parâmetros mais exigentes.

Tratando-se de um sistema de reconhecimento facial massivo, implementado sobre todos os usuários do metrô, há uma clara incompatibilidade com o direito à privacidade (art. 5º, X, LXXII e LXXIX da **CRFB**), e à autodeterminação informativa, em seus contornos constitucionais e internacionais, bem como à proporcionalidade, caráter material do devido processo legal (art. 5º, LIV da CRFB). A ofensa à privacidade repercute, ainda, em ofensas aos direitos à liberdade de expressão e à liberdade de associação e reunião, como interpretados à luz do Pacto Internacional de Direitos Civis e Políticos pelo Comitê de Direitos Humanos da ONU e pelas Relatorias Especiais da ONU sobre Liberdade de Reunião e sobre Liberdade de Expressão.

Por fim, o impacto desproporcional de sistemas de reconhecimento facial sobre populações vulneráveis, especialmente pessoas negras e LGBTQIA+, permite afirmar que o sistema implementado pela Ré ofende o direito à igualdade e à não discriminação, entendidos aqui à luz das normas constitucionais (art. 5º, caput e XLI da CRFB) e dos tratados internacionais ratificados pelo Brasil (com destaque ao Pacto Internacional de Direitos Civis e Políticos e a Convenção Americana sobre Direitos Humanos). Em relação às pessoas negras e trans, são muitos os casos, públicos e notórios, aqui e no exterior, nos quais os sistemas de reconhecimento facial resultaram em gravíssimos erros baseados na discriminação algorítmica.

A ação requer uma tutela de urgência para a suspensão imediata da captação e tratamento de dados pessoais biométricos dos usuários do metrô, para reconhecimento facial, com incidência de multa diária pelo seu descumprimento. Ao final, as Autoras requerem, diante das exigências impostas pela Constituição Federal, LGPD, ECA, CDC, CDUPS e tratados internacionais de direitos humanos, que seja proibido o uso da tecnologia de reconhecimento facial massiva e indiscriminada nas dependências do metrô de São Paulo, além do pagamento de indenização por danos morais coletivos no valor de R$ 42.279.438,63 pelo tratamento ilegal de dados pessoais dos usuários realizado até o momento.

2. Preliminares

2.1 Legitimidade das requerentes

As **Defensorias Públicas do Estado de São Paulo e da União** guardam legitimidade para ajuizar a presente demanda, eis que são instituições essenciais à função jurisdicional, as quais incumbem a defesa dos necessitados (art. 134 da CF/88) e a concretização dos objetivos fundamentais da República, como o de construir uma sociedade livre, justa e solidária, e mais

especialmente o de erradicar a pobreza e a marginalidade, reduzindo as desigualdades sociais e regionais (art. 3º, incs. I e III da CF/88). Posto isso, também é indiscutível a pertinência temática do objeto desta ação com a missão constitucional da Defensoria Pública. Mais especificamente, os serviços de transporte público coletivo, segundo dicção do art. 30, inciso V, da Carta Magna, possuem caráter essencial, pois além de garantir a mobilidade urbana para as camadas menos favorecidas, permitem o acesso da população aos demais direitos sociais, tais como o trabalho, saúde, educação, cultura e lazer. Além disso, a EC 90/2015 inseriu o transporte no rol do art. 6º da CF, de maneira a exigir que o Poder Público adote uma nova postura no tocante a esse direito social. Por fim, os dados pessoais também guardam status de direito fundamental. Como a questão ora posta atinge diretamente todos os potenciais usuários do Metrô de São Paulo, não resta qualquer dúvida acerca da pertinência do objeto da ação com as funções institucionais da Defensoria Pública, porque a maioria absoluta dos beneficiários do que ora se requer integra o público-alvo da assistência jurídica por ela prestada.

A **ARTIGO 19** é uma organização internacional de direitos humanos, fundada em Londres no ano de 1987, e cujo foco de atuação é a proteção e promoção dos direitos à liberdade de expressão e acesso à informação pública, previstos pelo artigo 19 da Declaração Universal dos Direitos Humanos. Seu Estatuto Social estabeleceu no art. 3º, incisos V e VI, as prioridades e objetivos de sua atuação voltada para a América do Sul, que contemplam o monitoramento de ações estatais que possam limitar e/ou restringir o exercício dos direitos às liberdades de opinião e de expressão e ao direito à informação. No Brasil, atua há cerca de 15 anos a partir de diversas frentes de trabalho que contemplam, dentre outras abordagens, pesquisa, análise e incidência jurídica em temas que perpassam as liberdades de expressão e informação. No âmbito dos direitos digitais e sua intersecção com a liberdade de expressão, vale destacar que a entidade tem uma forte atuação frente à construção de legislação e políticas públicas. Nesse sentido, já produziu pesquisas e análises sobre temas que incluem desde políticas de vigilantismo até o desenvolvimento de legislações referentes à proteção de dados pessoais no Brasil.

O **Instituto Brasileiro de Defesa do Consumidor**, Idec, é uma associação civil sem fins lucrativos, fundada em julho de 1987, cuja finalidade precípua é a defesa do consumidor desenvolvendo, para tanto, várias atividades, entre elas a propositura de ações judiciais, nos termos da lei. Notadamente, tem em seus fins institucionais a atuação em Juízo como defensor e representante da coletividade consumerista, exercendo a tutela do direito coletivo e relevante de milhões de consumidores do país, conforme se verifica nos artigos 1º, 2º e 3º, alíneas “d, “f”

e “g” do seu Estatuto Social. Os artigos supramencionados, portanto, demonstram que entre as finalidades do Idec está a defesa dos direitos do consumidor por meio de ações judiciais. O Idec atua precisamente para evitar que tais lesões ocorram e para garantir a efetiva proteção de direitos coletivos de consumidores, em especial por tratar-se de tema relacionado a transporte público, considerado serviço essencial, nos termos do artigo 22, do CDC, além de questões ligadas à proteção dos direitos básicos dos usuários, conforme definido pelo Código de Defesa dos Usuários do Serviço Público (Lei Federal n. 13.460/2017).

O **Intervozes** é associação civil sem fins lucrativos, fundada em 2003, que tem entre suas finalidades, conforme está expresso em seu Estatuto Social, o fortalecimento da esfera pública, assim como dos cidadãos como atores sociais, promovendo a democracia participativa; a transformação do sistema de comunicação brasileiro, lutando pela democratização da comunicação de modo a que seja reconhecida como um direito de todo ser humano; a proteção do patrimônio público e social, à ordem econômica; bem como a defesa dos direitos dos usuários de serviços de comunicação e de telecomunicações.

Como se vê, além da legitimidade das Defensorias Públicas do Estado de São Paulo e da União, o grupo de autores presentes no polo ativo da presente demanda tem por objetivo a proteção de direitos de interesse coletivo e, por isso, estão legitimadas à propositura da presente ação nos termos da lei e da Constituição. Ressalte-se, ainda, que as associações autoras não auferem lucro e promovem a educação e a conscientização da população.

Além da previsão constitucional (artigos 5º, XVII, XVIII, XIX, XX, XXI e 174, §2°), a Lei de Ação Civil Pública (LACP, Lei nº 7.347/85), em seu artigo 5º, e o Código de Defesa do Consumidor (CDC, Lei nº 8.078/90), em seus artigos 81 e 82, também disciplinam a legitimidade das autoras para a tutela coletiva. Diz-se tutela coletiva as ações aptas a perseguir os direitos difusos, como no presente caso.

A jurisprudência dos tribunais superiores tem, ademais, caminhado no sentido de prestigiar o princípio do acesso à justiça na análise da legitimidade ativa de associações civis[2].

As Autoras propõem a presente demanda na qualidade de substituto processual dos usuários, pois o tema trata, indubitavelmente, de interesses e direitos difusos, por envolver todos os usuários que tiveram seus dados pessoais biométricos e sensíveis tratados sem autorização.

[2] STJ. REsp 1357618 / DF e STF. **ADPF 527 MC / DF**

2.2 Legitimidade passiva

A Companhia do Metropolitano de São Paulo, relacionada no polo passivo, é a responsável direta pela contratação, implementação e operação de sistema de reconhecimento facial com o tratamento de dados pessoais sensíveis. Como narrado nos fatos desta petição e como será demonstrado, a empresa Ré viola direitos dos usuários do metrô.

Sublinha-se que a Companhia do Metropolitano de São Paulo é a fornecedora dos serviços apontados nesta inicial, nos termos do que define o artigo 3º e seu §1° do Código de Defesa do Consumidor. Tem-se, portanto, configurada também a relação de consumo.

2.3 Competência

As varas de Fazenda Pública processam e julgam causas cíveis em que figurem como parte o Estado, os municípios, suas autarquias, as empresas públicas, as sociedades de economia mista e as fundações de direito público.

Por ser a Companhia do Metropolitano de São Paulo uma empresa pública, parte integrante da administração indireta do Estado de São Paulo, regendo-se pelas Leis Federais nº 6.404/1976 e 13.303/2016, dentre outras disposições legais aplicáveis, não restam dúvidas da competência da Fazenda Pública para processar e julgar a presente Ação Civil Pública. Não bastasse, configurada a relação de consumo entre usuários e a Ré, também é reforçada a competência da justiça estadual.

Diante do exposto, por se tratar de ação coletiva que atinge a coletividade, envolvendo nítido interesse público, é competente para apreciar a presente demanda o Foro Central da Fazenda Pública do Estado de São Paulo.

3. Fatos: A Ré promove reconhecimento facial e tratamento de dados pessoais dos usuários do metrô sem observar as exigências legais

Previamente à propositura desta ação civil pública, as Autoras buscaram prevenir o litígio por meio de uma ação autônoma de produção de provas, com objetivo de certificar a amplitude, as características e as condições nas quais se daria a implementação de um sistema de reconhecimento facial pela Ré Companhia do Metropolitano de São Paulo.

A ação autônoma de produção de provas, que segue na íntegra como anexo desta ação civil pública (Doc. 4), foi proposta para produzir provas sobre a observância dos direitos do titular de dados pessoais, bem como sobre o cumprimento dos deveres legais impostos àqueles que tratam, controlam e compartilham tais dados pessoais.

Como provas relativas à implementação do sistema de reconhecimento facial à LGPD, a Ré apresentou: atestados de capacidade técnica das empresas licitadas; documentos com especificações técnicas de segurança do sistema (IC-9.83.ME.XX/7XX-001); características do sistema (CS-9.83.ME.XX/7XX-001) e diretrizes de segurança de informações do metrô (NGR-01-202). Estes documentos comprovam, na verdade, a inadequação do sistema de implementação de monitoramento eletrônico com reconhecimento facial (SME-III) à LGPD.

Parecer (Doc. 5) coordenado pelo Prof. Roberto Hirata Jr., professor livre-docente do departamento de Ciência da Computação do Instituto de Matemática e Estatística da Universidade de São Paulo (IME-USP), analisou os documentos apresentados pela Ré Companhia do Metropolitano do Metrô e concluiu:

> [...] o sistema objeto de análise apresenta algumas características e possibilidades referentes: (i) à viabilidade técnica, por exemplo, de rastrear pessoas ou grupos de pessoas pelas dependências do metrô; (ii) a falhas na execução serem inerentes a esse tipo de sistema, não sendo possível mitigar completamente esse tipo de erro (falsos negativos e falsos positivos); (iii) a não existência, na documentação do metrô, de uma análise sobre a taxa de sensibilidade utilizada ou o equilíbrio entre as taxas de falsos positivos falsos negativos; (iv) a potencialidade de o sistema perpetuar desigualdades presentes no Brasil, selecionando de maneira errada com maior frequência indivíduos negros e imigrantes; (v) a ausência de informações referentes à análise forense que sejam capazes de demonstrar a mitigação dos riscos apresentados pelo sistema frente aos usuários do metrô; (vi) a inadequação de uso do sistema para identificação de crianças e adolescentes, incluindo pessoas desaparecidas pertencentes a esses grupos, levando em consideração que medidas para mitigar erros relativos à idade ou ao envelhecimento não estão explicitadas na documentação; (vii) a ausência de especificações relativas à coleta e ao tratamento diferenciado de dados de crianças e adolescentes; (viii) a ausência de indicação do banco de dados a ser utilizado pelo metrô para treinar os

> modelos de reconhecimento facial, ainda que tal informação seja de grande importância para avaliar a eficiência do projeto[3].

Definitivamente, as provas produzidas e homologadas em sentença transitada em julgado na ação autônoma de produção de provas comprovam que a implementação do sistema de reconhecimento facial pela Ré Companhia do Metropolitano de São Paulo nas estações do metrô da cidade de São Paulo está ocorrendo de forma ilícita, em flagrante e frontal violação à legislação ordinária, à Constituição e aos tratados internacionais relativos à matéria, como se verá a seguir.

3.1 A implementação do sistema de reconhecimento facial pela Ré Companhia do Metropolitano de São Paulo

Em 2 de julho de 2019, a Companhia do Metropolitano de São Paulo lançou aviso de edital de licitação para "CONCEPÇÃO DO SISTEMA DE MONITORAÇÃO ELETRÔNICA- SME ETAPA 3 DAS LINHAS 1-AZUL, 2-VERDE E 3-VERMELHA", referido pela Ré em documentos como SME-III[4].

Apesar de não constar expressamente das cláusulas do edital, tal licitação tem por objetivo a implantação não só de um sistema de monitoração eletrônica, mas de um sistema de reconhecimento facial de todos os usuários do Metrô, com capacidade para armazenamento de dados e compartilhamento.

O documento CS-9.83.ME.XX/7XX.001[5], anexo ao processo de licitação LPI nº 10014557, traz os requisitos técnicos mínimos, indicando, dentre outras coisas, que: i) o sistema de monitoração eletrônica envolverá o reconhecimento facial; ii) necessariamente deverá ser usado um software privado, chamado SecurOS; iii) as imagens de todos os usuários serão armazenadas; iv) o sistema deverá estar preparado para carregamento de dados internos e externos; v) o sistema poderá entrar em operação integrada com outros sistemas de monitoração eletrônica com reconhecimento facial.

---

[3] Abello, Araújo e Hirata Jr., p.78-79

[4] Esclarece-se que o projeto de lei estadual PL 865/21, que demandava a instalação de câmeras de reconhecimento facial em todas as estações da Companhia do Metropolitano de São Paulo, não tem qualquer relação com o procedimento licitatório LPI nº 10014557. O PL 865/21 foi aprovado pela Assembleia Legislativa de São Paulo em 16 de fevereiro de 2021 e vetado pelo Governador João Doria em 13 de março de 2021, tramitou posteriormente à abertura e encerramento do procedimento licitatório LPI nº 10014557. O projeto, inclusive, foi vetado por razões formais. Ver a íntegra na tramitação do PL 865/2019 na Assembleia Legislativa do Estado de São Paulo: https://www.al.sp.gov.br/propositura/?id=1000278098.

[5] Páginas 939-1064 da ação autônoma de produção de provas – ref. doc. 4.

Entretanto, nos documentos do edital, no contrato ou nos questionamentos feitos no âmbito do referido processo licitatório, não foi disponibilizada qualquer informação sobre os critérios, condições, propósitos da implementação do sistema de reconhecimento facial pela Ré Companhia do Metropolitano de São Paulo.

Diante de tantas dúvidas, o Instituto Brasileiro de Defesa do Consumidor (Idec), em 27 de setembro de 2019, enviou à Ré Companhia do Metropolitano de São Paulo uma carta[6] solicitando esclarecimentos sobre o objeto do referido processo licitatório LPI nº 10014557.

A Ré Companhia do Metropolitano de São Paulo respondeu em 11 de outubro de 2019[7].

À pergunta sobre "o que levou o metrô de São Paulo a querer implementar tecnologia de reconhecimento facial?", a Ré Companhia do Metropolitano de São Paulo assim respondeu:

> "Neste contexto e considerando o compromisso da empresa com a segurança e inovação tecnológica, a Companhia deve considerar o que há de mais moderno e atual para cumprimento desta finalidade e sua missão institucional, incluindo a implementação de tecnologia de inteligência artificial com diversas funcionalidades para o SME, o que inclui a detecção de invasão de perímetros, rastreamento de objetos, reconhecimento facial entre outras, com vistas a coibir infrações penais e incrementar a segurança dos passageiros".

O processo licitatório seguiu seu curso, não sem litígios administrativos e judiciais alegando direcionamento e irregularidades no processo de contratação. A empresa declarada vencedora de referido processo licitatório foi o Consórcio Engie, Ineo e Johnson; o resultado foi homologado e foi feita a adjudicação do objeto do contrato, no valor de R$ 42.798.438,63 (quarenta e dois milhões, setecentos e noventa e oito mil quatrocentos e trinta e oito reais e sessenta e três centavos)[8].

Quando questionada sobre o sistema de reconhecimento facial licitado, em ação autônoma de produção de provas, a Ré afirmou:

> A funcionalidade do software que permite a identificação facial de pessoas somente será utilizada em casos muito específicos, para o atendimento de demandas esporádicas, como por exemplo, busca de pessoas desaparecidas, ou identificação de um usuário que eventualmente tenha praticado algum crime nas dependências do Metrô, bem como busca após determinação judicial. [...]

[6] Páginas 202 a 206 da ação autônoma de produção de provas – ref. doc. 4.
[7] Páginas 207 a 211 da ação autônoma de produção de provas – ref. doc. 4.
[8] Página 298 da ação autônoma de produção de provas – ref. doc. 4.

> [...] a guarda das imagens atenderá a todos os requisitos legais de segurança, sendo que os métodos de anonimização e armazenamento serão melhor detalhados na fase de elaboração do Projeto Executivo, que faz parte do escopo da contratação. [...]
>
> De toda forma, por ora, não há intenção formalizada a respeito de compartilhamento da base de dados com outras entidades públicas e, muito menos, privadas, muito embora a lei permita sua concretização através de convênio.[...] [9]

Há uma clara tentativa por parte da Ré de escamotear a implementação deste sistema de reconhecimento facial para, como isso, fugir aos deveres legais impostos pela LGPD para qualquer operação de tratamento de dados. Em sua segunda petição na referida ação, a Ré resolveu negar o que já havia afirmado, mudando totalmente as informações e contrariando os documentos técnicos que ela mesma juntara:

> [...] não haverá tratamento nem monitoramento de "dados pessoais" ou de "dados pessoais sensíveis", como equivocamente entendem os Autores. [...]
>
> A atualização futura do Sistema de Monitoramento Eletrônico, denominado SME-III, objeto do processo de licitação LPI 10014557, também não prevê a coleta de dados pessoais de usuários. [...]
>
> Não haverá armazenamento de dados pessoais de usuários, como já esclarecido. [...][10]

A versão apresentada pela Ré não se sustentou. O Secretário de Transportes Metropolitanos de São Paulo, Alexandre Baldy, concedeu entrevista em 24 de junho de 2021 à Agência Estado, assumindo tratar-se da implementação de um sistema de reconhecimento facial nas linhas 1-Azul, 2-Verde, 3-Vermelha e 15-Prata. Na entrevista, o Secretário Alexandre Baldy afirma: "Não é um reconhecimento de cidadãos. Ninguém quer fiscalizar ou vigiar ninguém. É para perda de objetos sensíveis, importunação sexual, reconhecimento de pessoas que estejam na lista de procurados da polícia. Não vamos ter acesso ao nome e CPF das pessoas" [...] "[as imagens] serão armazenadas por um período maior, em um contrato seguro, para que as ocorrências possam ser investigadas"[11].

[9] Excertos das páginas 552-564 da ação autônoma de produção de provas – ref. doc. 4
[10] Excertos das páginas 1130 e seguintes da ação autônoma de produção de provas – ref. doc. 4.
[11] Agência Estado, https://sao-paulo.estadao.com.br/noticias/geral,metro-de-sp-tera-cameras-que-disparam-alerta-de-objeto-esquecido-ou-crianca-

De fato, o documento CS-9.83.ME.XX/7XX-001[12] detalha como deve ser a implementação de um software de "análise forense" que possibilita o reconhecimento e busca de objetos e pessoas por variados critérios, como cor, roupas e reconhecimento facial.

Relatório técnico produzido por Abello, Araújo e Hirata Jr. que acompanha esta petição inicial, explica que:

> No edital não são especificadas características da operação do software de análise forense além do fato de que ele deve ser compatível com o software de vigilância SecurOS, que é desenvolvido pela empresa russa ISS (Intelligent Security Systems). A empresa comercializa atualmente módulos de reconhecimento de faces e o software já provê um subsistema de visão computacional. Ambos sistemas têm capacidade para detecção de diversos tipos de eventos. Por exemplo, o subsistema de visão computacional provê:
>
> - detecção de uma pessoa correndo;
> - detecção de objetos largados, ou removidos;
> - detecção de aglomerações;
> - detecção de intrusão;
> - contagem de objetos/pessoas;
> - detecção de cruzamento de limites;
> - detecção de pessoas paradas a mais de um certo tempo em algum local;
> - detecção de movimento em uma direção errada/proibida.[13]

Até o mês de julho de 2021, pelo que se tem noticiado, já foram instaladas 91 câmeras com tecnologia para reconhecimento facial em estações de metrô na zona leste da cidade de São Paulo (Linha 3 - Vermelha) [14]; a previsão é a instalação de mais de 5.000 câmeras.

Ainda que o secretário afirme que o reconhecimento facial será usado para "pessoas que estejam na lista de procurados da polícia", é importante frisar que, para tanto, inevitavelmente, o sistema implementado pela Ré Companhia do Metropolitano de São Paulo promoverá a

desacompanhada,70003756967#:~:text=O%20objetivo%20principal%2C%20diz%20o,dos%20pontos%20reconhecidos%20como%20cr%C3%ADticos.

[12] Páginas 939 a 1064 da ação autônoma de produção de provas – ref. doc. 4.

[13] Abello, Araújo e Hirata Jr., p. 63

[14] Segundo reportagem, as 91 câmeras instaladas estão assim distribuídas: 37 na estação Carrão, 29 da estação Guilhermina Esperança, 25 da estação Belém). Mais informações em https://domtotal.com/noticia/1523868/2021/06/metro-de-sao-paulo-tera-cameras-com-reconhecimento-facial/

captura de dados biométricos de todos os usuários do metrô. **Aí residem a ilegalidade e a desproporcionalidade da medida**.

O reconhecimento facial é feito em várias etapas: captura da imagem por câmeras digitais, filtragem para avaliação de qualidade, localização das regiões da face, extração de características da face, modelagem em 3D, reorientação frontal e de escala da imagem, classificação e reconhecimento da face. Ao capturar, ler, copiar, medir e registrar pontos do rosto de uma pessoa, cria-se um dado com peculiaridades capazes de permitir sua individualização e identificação, como a distância entre os olhos, nariz e queixo. Transformadas em representações numéricas, estas informações podem ser classificadas e comparadas a outras imagens pertencentes a bancos de dados diversos[15]. Ademais, as faces capturadas e registradas podem passar a compor um novo banco de dados.

As faces reconhecidas por sistemas como o que está em implementação pela Ré Companhia do Metropolitano de São Paulo compõem um dado biométrico, isto é, um dado biológico ou comportamental exclusivo, único, individual e – em grande medida – insubstituível. **Diferentemente de senhas, dados biométricos não são substituíveis, o que torna sua captura, tratamento e utilização muito mais arriscada e condicionada a uma estrita e insubstituível necessidade.**

Relatório técnico produzido por Abello, Araújo e Hirata Jr. explica detalhadamente o processo pelo qual se dá o reconhecimento facial: ele indica quão próximas ou distantes duas imagens (uma capturada digitalmente e outra presente em um banco de dados) estão.

> Essencialmente, um modelo de reconhecimento facial diz quão próximas, ou distantes, duas imagens de faces humanas estão uma da outra. Munido dessa métrica de proximidade, pode-se realizar diferentes tarefas, as mais comuns sendo verificação e identificação.
>
> A verificação é um problema binário, onde se compara duas imagens dadas, por exemplo, a imagem da foto do passaporte de uma pessoa e a imagem da foto de uma câmera que está apontando para ela no momento da apresentação do passaporte para um dispositivo de liberação de entrada. O resultado é a simples decisão de se as imagens correspondem à mesma pessoa, ou não. Se forem, o sistema libera a catraca. Se o sistema disser que não são, deve-se proceder uma verificação por um ser humano.

[15] IDEC e INTERNET LAB. Reconhecimento facial e o setor privado: guia para a adoção de boas práticas. 2020, p. 24-35. Disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf.

> Em uma tarefa de identificação, o modelo possui uma lista de imagens associadas a identidades conhecidas, também chamada de galeria. A tarefa do algoritmo é, então, analisar uma nova imagem dada e compará-la, calculando-se a distância dela contra todas as faces da galeria. Essa distância é uma medida de semelhança, ou dissemelhança, entre as faces. O modelo, então, produz uma lista ordenada pela distância, em geral da menor para a maior, da face dada a cada uma das faces da galeria[16].

O sistema implementado pelo Metrô promoverá a tarefa de identificação: mapeará as faces de todos os usuários do metrô e as classificará – em grau de semelhança e dissemelhança – com imagens de um banco de dados.

Não há como realizar o reconhecimento facial sem que todas as faces, de todos os usuários do metrô, sejam lidas, copiadas, medidas e registradas. Ainda que o banco de dados - usado para dar a combinação com as faces capturadas no sistema de monitoramento por reconhecimento facial do metrô – contenha imagens apenas de pessoas procuradas ou desaparecidas (o que tampouco foi comprovado), fato é que, para atingir ao propósito de sua identificação, todos os usuários do metrô terão suas faces lidas, copiadas, medidas e registradas, armazenadas em um "contrato seguro", conforme disse o Secretário de Transportes Metropolitanos, Alexandre Baldy.

Assim, não restam dúvidas de que a Ré Companhia do Metropolitano de São Paulo licitou, contratou e está implementando sistema de monitoração eletrônica com uso de reconhecimento facial, fato comprovado pela análise dos documentos técnicos de referido processo licitatório e assumido pelos gestores públicos responsáveis por sua implementação.

A Ré Companhia do Metropolitano de São Paulo, ao captar, registrar, comparar e eventualmente armazenar os dados biométricos dos usuários do metrô, fará o que a LGPD chama de tratamento de dado pessoal, ou seja, "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", nos termos do artigo 5º, X da LGPD.

Deste fato, aliado ao fato de que a Ré presta um serviço público essencial, decorrem múltiplos deveres legais violados pela Ré Companhia do Metropolitano de São Paulo: o dever de obter

[16] Abello, Araújo e Hirata Jr., março de 2021, p. 24.

consentimento dos titulares para tratamento de seus dados pessoais; o dever de agir com transparência e dispor de todas as informações necessárias de como será o tratamento de dados; o dever de adotar medidas de avaliação e mitigação de riscos; o dever de adotar políticas proporcionais; e o dever de segurança e qualidade e de não causar dano ou abuso de direito ao usuário de serviço público. Todos esses deveres foram violados, como se provará a seguir.

3.2 Ausência de medidas para obtenção de consentimento e ausência de consentimento ao tratamento de dados pessoais biométricos dos usuários do metrô pela Ré Companhia do Metropolitano de São Paulo

Trata-se de coleta e tratamento de dados pessoais biométricos. A disciplina legal para essas atividades exige um cuidado qualificado do controlador ou operador, ante o potencial lesivo exacerbado desses dados.

Contudo, verifica-se que a Ré não observou os cuidados obrigatórios para a coleta de tratamento de dados pessoais, tampouco para dados pessoais biométricos sensíveis (art. 5º, II, da LGPD), tornando ainda mais evidente a ausência de fundamento legal para sua conduta.

Conforme já informado, a Ré Companhia do Metropolitano de São Paulo foi questionada por uma das organizações autoras, o Idec, através de uma carta[17], sobre as características do sistema de reconhecimento facial objeto da licitação LPI nº 10014557. Diante dos deveres impostos pela lei de obter consentimento dos usuários do metrô para tratamento de seus dados biométricos, perguntou-se à Ré se o sistema estaria de acordo com exigências impostas pela LGPD, dentre elas a de consentimento do usuário do metrô, titular de dados pessoais biométricos.

A Ré Companhia do Metropolitano de São Paulo nada respondeu em relação ao consentimento. Informou genericamente que "o sistema foi concebido prevendo o atendimento a toda legislação aplicável, incluindo a Lei 13.709/19" [18].

Diante da ausência de informações, a exigência de consentimento foi questionada em tópico específico da ação autônoma de produção de provas proposta pelas autoras. Demandou-se, naquele momento, mediante decisão judicial, que a Ré apresentasse prova sobre qual consentimento foi dado:

[17] Páginas 202-206 da ação autônoma de produção de provas – ref. doc. 4.
[18] Página 203 da ação autônoma de produção de provas - ref. doc. 4.

> 3. Prova documental sobre o já existente banco de dados a ser utilizado no sistema de monitoração eletrônica, contendo: i) a data de criação do banco de dados; ii) a forma de aquisição do banco de dados (se foi criação própria, comprado, emprestado); iii) quais informações de usuários do metrô compõem esse banco de dados; iv) **qual consentimento foi dado, pelos usuários, para uso de suas informações**; v) a forma e frequência de atualização de referido banco de dados; vi) quem terá acesso aos dados pessoais coletados e quais serão os graus de privilégios de acesso. [19]

A Ré Companhia do Metropolitano de São Paulo foi demandada, ainda, para provar o consentimento específico exigido pela LGPD para tratamento de dados pessoais de crianças e adolescentes – prova cuja produção também foi deferida judicialmente, nos seguintes termos:

> 4. Prova documental sobre como o Metrô obterá consentimento de pais ou responsáveis para obtenção, guarda e uso de dados pessoais de crianças e adolescentes, nos termos do Estatuto da Criança e do Adolescente[20].

Em resposta, a Ré Companhia do Metropolitano de São Paulo **afirma categoricamente que não possui consentimento e que tampouco o obterá** para tratamento de dados pessoais de crianças e adolescentes e de demais usuários do metrô para tratamento de seus dados. Assume, também, que não há finalidade pré-definida e depois indica, genericamente, que usará para "segurança pública".

> Ocorre que a análise sistemática da norma permite concluir que o consentimento não é a única base legal capaz de legitimar o tratamento desses dados. Em verdade, há outras bases legais em que o referido armazenamento poderá ser fundamentado, hipóteses em que o tratamento independerá de consentimento do titular. [...]
>
> **O tratamento de dados pessoais de crianças e adolescentes – bem como dos demais passageiros – certamente não se baseará no consentimento.**
>
> O enquadramento da base legal específica para cada caso, todavia, dependerá da finalidade para a qual o dado será coletado[21] (grifo nosso).

A Ré **confessa** o fato: tratará dados pessoais dos usuários do metrô, sem consentimento dos usuários e não adotará medidas para sua obtenção, em prova produzida e homologada por

[19] Página 533 da ação autônoma de produção de provas – ref. doc. 4.
[20] Página 536 da ação autônoma de produção de provas – ref. doc. 4.
[21] Páginas 559-560 da ação autônoma de produção de provas – ref. doc. 4.

decisão judicial transitada em julgado, recaindo sobre tal confissão os efeitos do artigo 374, II, do Código de Processo Civil.

> Art. 374. Não dependem de prova os fatos:
>
> II – admitidos por uma parte e confessados pela parte contrária.

Provada a confissão – e independente de outra prova, portanto – sobre a ausência de medidas para obtenção de consentimento e ausência de consentimento ao tratamento de dados pessoais biométricos dos usuários do metrô pela Ré Companhia do Metropolitano de São Paulo.

Não bastasse, confrontada com a ausência de provas sobre consentimento, a Ré resolveu informar banalidades sobre "sistema atual" de filmagem geral. Deu a entender que uma placa com os dizeres "O ambiente está sendo filmado. As imagens gravadas são confidenciais e protegidas, nos termos da lei (Lei Municipal 13.541, de 24 de março de 2003)"[22], daria conta das exigências da LGPD.

Esta foi a prova sobre consentimento homologada judicialmente em ação autônoma de produção de provas, ou seja, ausência de consentimento do titular de dados, tal como exigido por lei.

3.3 Ausência de transparência e informações sobre as características e riscos oferecidos na execução de serviço público e sobre o tratamento de dados pessoais dos usuários do metrô pela Ré Companhia do Metropolitano de São Paulo

Comprovados os fatos que apontam, inequivocamente, que a Ré implementa sistema de reconhecimento facial nas estações do metrô e de que o faz, assumidamente, sem obter ou pretender obter o consentimento dos usuários do metrô, titulares de dados pessoais, resta averiguar se a Ré cumpre com seus deveres de transparência e informação sobre os riscos do funcionamento da tecnologia no serviço público e sobre o tratamento dos dados.

De forma geral, os documentos juntados nesta ação civil pública mostram que a Ré Companhia do Metropolitano de São Paulo não promoveu transparência sobre a finalidade, requisitos e forma de tratamento de dados – tanto que foi necessário envio de carta com pedido de informações e proposição de ação autônoma de produção de provas. Quando demandada, ofereceu respostas evasivas, incompletas e contraditórias. É quase possível afirmar que a Ré

[22] Página 1133 da ação autônoma de produção de provas – ref. doc. 4.

ocultou e desinformou, propositadamente, sobre o processo de implementação de reconhecimento facial nas estações do metrô.

As informações sobre o tratamento de dados biométricos, desde o banco de dados utilizado, as hipóteses de seu compartilhamento, os graus de privilégio de acesso a ele e as regras de governança, anonimização, até a explicitação da finalidade do tratamento de dados, compõem um conjunto de deveres apontados pela Lei 13.709/19, em seu artigo 9º, como será argumentado a seguir. Para além da referida normativa, a Ré, ao não informar adequadamente as características, as qualidades e os riscos do serviço prestado, não cumpre os deveres apontados na Lei nº 8.078/1990 (Código de Defesa do Consumidor) e tampouco na Lei nº 13.460/2017 (Código de Defesa dos Usuários de Serviços Públicos). Neste momento, importa ressaltar serem tais informações decorrentes de obrigação expressa em lei, devendo ser **ostensivas, claras e adequadas**.

A relatada carta do Idec[23] direcionada à Ré já havia apresentado uma série de questões neste sentido. A Ré simplesmente não respondeu a várias das questões, descumprindo com seu dever de informação:

> 8. A realização do reconhecimento facial pelo software irá ocorrer em tempo real?
>
> Resposta: Sim.
>
> 9. Qual banco de dados será utilizado para a comparação entre as imagens para a identificação das pessoas? Mais de um banco de dados será utilizado?
>
> 10. Haverá procedimentos posteriores de anonimização dos dados pessoais coletados? Haverá posterior descarte das informações e imagens não utilizadas? De qual forma isso será realizado?
>
> Resposta: Em um primeiro instante, reconhecimento fica restrito ao banco de dados do metrô, sendo que uma maior abrangência da atuação voltada à segurança pública dependerá de convênios com os Órgãos Públicos responsáveis por tal atuação, os quais possuem banco com imagens de contraventores, criminosos, procurados, desaparecidos, dentre outros.
>
> Quanto à anonimização dos dados, conforme já se destacou alhures, todas as informações e irão trafegar pelo sistema são sigilosas e criptografadas,

[23] Páginas 203-206 da ação autônoma de produção de provas – ref. doc. 4.

> incluindo a função SHA-1, combinado com um par de chaves públicas privadas para cada imagem gravada.
>
> 11. Por quanto tempo as imagens serão armazenadas e como serão descartadas? Onde serão localizados os terminais de armazenamento das imagens e informações?
>
> Resposta: As imagens serão armazenadas pelo período de 30 (trinta) dias e, após o período, serão descartadas automaticamente, por sobreposição.
>
> 12. Quem e quais instituições terão acesso aos dados? A empresa fornecedora da tecnologia terá acesso aos dados? De qual forma isso será conduzido?
>
> 13. Haverá possibilidade que o sistema seja futuramente usado para outras finalidades? Como isso está previsto para ocorrer?
>
> 14. Está previsto algum tipo de accountability e/ou de auditoria com relação ao sistema de inteligência artificial e reconhecimento facial, para garantia da transparência da administração pública?
>
> 15. O Metrô de SP irá realizar compartilhamento desses dados com terceiros, sejam instituições públicas ou privadas?
>
> 16. De qual forma esse compartilhamento irá ocorrer? Quais dados serão compartilhados?
>
> Resposta: A utilização e acesso são restritas a órgãos públicos e autoridades voltadas a proteção da segurança pública, tais como: Poder Judiciário, Autoridades Policiais e Ministério Público, os quais somente terão acesso às imagens por meio de solicitação formal, via Ofício, ou por convênio firmados com os respectivos Órgãos da Segurança Pública.[24]

Diante da evidente insuficiência das informações, provas foram demandadas judicialmente, nos seguintes termos:

> 3) Prova documental sobre o já existente banco de dados a ser utilizado no sistema de monitoração eletrônica, contendo: i) a data de criação do banco de dados; ii) a forma de aquisição do banco de dados (se foi criação própria, comprado, emprestado); iii) quais informações de usuários do metrô compõem esse banco de dados; iv) qual consentimento foi dado, pelos usuários, para uso de suas informações; v) a forma e frequência de atualização de referido banco

[24] Página 210 da ação autônoma de produção de provas – ref. doc. 4.

> de dados; vi) quem terá acesso aos dados pessoais coletados e quais serão os graus de privilégios de acesso;
>
> [...]
>
> 5) Prova documental sobre como será observada a anonimização e a guarda dos dados Pessoais;
>
> 6) Prova documental sobre análise de impacto financeiro de eventuais falhas e vazamentos na atividade de monitoração eletrônica, considerando como potencialmente afetados todos os usuários do metrô;
>
> 7) Prova documental sobre a governança do futuro banco de dados decorrente desta contratação, incluindo detalhamento de seu controlador, critérios de segurança do armazenamento, usos, formas de acesso e mecanismos de controle social da sua utilização com fundamento e base legal nas finalidades indicadas;
>
> 8) Prova documental da proposta de compartilhamento da base de dados com outras entidades estatais e/ou privadas e das hipóteses de tratamento antevistas, permitidas e almejadas, uma vez que a pretensa base legal refere-se à segurança pública e a finalidade institucional da entidade licitante não se relaciona a esse objetivo de política pública, também em virtude dos requisitos mínimos previstos no item 6.9.6 no anexo CS983MEXX7XX001 do edital[25].

A ênfase em perguntas das Autoras sobre banco de dados reside em fundamentos: num primeiro momento, as características do banco de dados usado para efeitos comparativos com as imagens capturadas definirão sua precisão, confiabilidade e adequação ao contexto aplicado (afinal, um banco de dados enviesado reproduzirá inconsistências); em segundo lugar, é direito do titular saber se seus dados (no caso, sua face, dado biométrico, personalíssimo) constará de banco de dados, direito este oriundo não só da LGPD como também das normas consumeristas.

Acerca de banco de dados, a Ré apresentou como prova a seguinte informação: "o objetivo principal da contratação [...] não é a captação de imagens faciais dos usuários para compará-las a um determinado banco de dados de propriedade da Companhia do Metrô"[26].

[25] Página 536 da ação autônoma de produção de provas – ref. doc. 4.
[26] Página 557 da ação autônoma de produção de provas – ref. doc. 4.

Porém, antes disso, em resposta enviada ao Idec, a Ré informou que seria usado um banco de dados interno[27]. Entretanto, na ação autônoma de produção de provas, a Ré não apresentou qualquer prova documental sobre referido banco de dados, limitando-se a informar que "atenderá todos os requisitos legais"[28], informação genericamente repetida em edital de licitação.

Além da diversidade de respostas dada pela Ré – não criará banco de dados; usará de banco de dados internos, criará novo banco de dados -, também há insuperável violação do dever de informação quando se refere a sua governança, isto é, a forma e duração do tratamento de dados, informação do controlador, incluído seu contato, formas de compartilhamento, e responsabilidades dos agentes de tratamento de dados, nos termos do artigo 9º da LGPD.

O documento CS-9.83.ME.XX1/7XX-001[29] juntado como prova pela Ré para mostrar que cumpre com as obrigações legais relativas ao banco de dados não traz estas informações, o que, por si só, prejudica a avaliação da confiabilidade e precisão do sistema de reconhecimento facial implementado pelo metrô. É o que concluiu o estudo de Relatório técnico produzido por Abello, Araújo e Hirata Jr. a partir da análise dos documentos e informações oferecidas pelo metrô:

> O projeto não descreve qual banco de dados será utilizado para treinar os modelos de reconhecimento facial. Como mostramos, essa informação é de grande importância para avaliar a eficiência do projeto, uma vez que um modelo treinado em uma base de dados de rostos pouco diversa, ou com composição étnica muito distinta da brasileira pode acarretar perdas significativas de performance ou efeitos demográficos que prejudiquem desproporcionalmente minorias.
>
> Ademais, para galeria de identidades a serem buscadas, se alude na resposta a questionamentos do IDEC, a um "banco de dados local do Metrô". Não se especifica sua composição, se é, por exemplo, de funcionários ou cidadãos no geral, nem o propósito dessa busca. Há também o prospecto de utilização de bases de dados de entes de segurança pública, com a possibilidade de integração sendo um requisito descrito na Concepção de Sistema (CS).[30]

[27] Página 210 da ação autônoma de produção de provas – ref. doc. 4.
[28] Página 510 da ação autônoma de produção de provas – ref. doc. 4.
[29] Páginas 939 -1064 da ação autônoma de produção de provas – ref. doc. 4.
[30] Relatório técnico produzido por Abello, Araújo e Hirata Jr, p. 74

A Ré não dispôs e continua a não apresentar as informações relativas ao tratamento de dados pessoais; as informações técnicas que oferece certamente não cumprem com o dever de dispor de acesso facilitado ao titular de dados e de forma clara, adequada e ostensiva nos termos da lei, tampouco permitem analisar a sua confiabilidade.

Não estranha, assim, que a prova de confiabilidade do sistema de reconhecimento facial apresentada pela Ré se resuma a atestados de capacidade técnica de todos os licitantes no processo LPI nº 10014557, isto é, documentos de habilitação para participação da licitação. Obviamente, os documentos de habilitação consubstanciados em atestados de capacidade técnica (art. 30, Lei de Licitações) não se confundem com relatórios e estudos de impacto amplamente utilizados em empreitadas e obras na área ambiental e incluídas no regime de proteção da Lei Geral de Proteção de Dados, especificamente em seus artigos 37 e 50.

3.4 Ausência de medidas de avaliação e impacto e mitigação de riscos na implementação do sistema de monitoração eletrônica com reconhecimento facial pela Ré Companhia do Metropolitano de São Paulo

Nos tópicos anteriores ficou comprovado que a Ré faz tratamento de dados biométricos de usuários do metrô através da implantação de sistema de reconhecimento facial contratado pelo processo licitatório LPI nº 10014557 para "CONCEPÇÃO DO SISTEMA DE MONITORAÇÃO ELETRÔNICA- SME ETAPA 3 DAS LINHAS 1-AZUL, 2-VERDE E 3-VERMELHA DA COMPANHIA DO METROPOLITANO DE SÃO PAULO".

Ficou comprovado também que, não obstante fazer tratamento de dados pessoais, não obteve consentimento dos titulares dos dados, nem pretende fazê-lo. Comprovou-se, da mesma forma que a Ré não dispôs de informações coerentes, claras, adequadas e ostensivas sobre o tratamento de dados pessoais e sobre os deveres no fornecimento de serviço público, como por exemplo o banco de dados usado ou criado, suas características e governança, violando direitos de transparência e informação previstos em lei.

Não bastasse, a Ré não adotou qualquer medida para avaliar o impacto do uso massivo de reconhecimento facial e para mitigação de seus graves e inerentes riscos, dado o funcionamento da tecnologia e a amplitude de sua aplicação.

A **segurança**, a **prevenção** e a **responsabilização** são princípios impostos às atividades de tratamento de dados pessoais por força de lei, previstas no artigo 6º da LGPD, bem como a

proteção e segurança contra serviços perigosos e nocivos é um direito básico do consumidor (CDC, Art. 6º, inciso I c/c arts. 8 e ss.) e, igualmente, a segurança é um princípio e direito do usuário de serviço público (CDUSP, arts 4º e 5º, incisos VIII e X, da Lei nº 13.460/2017). Este arcabouço jurídico impõe uma série de deveres correspondentes àquele que trata ou pretende tratar dados, como faz a Ré ao implementar o sistema de reconhecimento facial.

Na prática, tais princípios se traduzem em cautelas na **governança do banco de dados** (que, já vimos, não existem); em características de **confiabilidade do sistema**; em **anonimização dos titulares de dados**; **avaliação de impacto e plano de mitigação de riscos** na hipótese de vazamentos ou outras violações aos direitos de titulares de dados pessoais.

Mais uma vez, diante da recalcitrância da Ré em disponibilizar informações essenciais, foram exigidas pelas requerentes uma série de documentos e provas sobre a confiabilidade, a análise de impacto da implementação do sistema de reconhecimento facial e as medidas de mitigação de seus riscos, sendo tais pedidos deferidos judicialmente.

Sobre a segurança de dados, Ré informou:

> "[...] qualquer sistema de informação do Metrô de São Paulo, em implantação ou já em uso, deve seguir, necessariamente, o disposto nas normas de controle de tratamento e proteção de dados constante de sua lista das Normas Gerais. No caso específico da contratação em debate, trata-se da NGR 01-202, que versa a respeito das diretrizes de segurança da informação da Companhia, e que segue em anexo (Doc. 4)"[31].

Este documento NGR 01-202 juntado pela Ré como prova de adequação à LGPD **trata os dados pessoais como "ativos" do metrô e não como direitos de seus titulares**. De fato, implementam um sistema de reconhecimento facial desprezando que os dados pessoais são direitos de seus titulares, apropriando-se destes dados e ignorando as exigências legais. A LGPD sequer é referida no citado documento[32], muito menos os seus critérios para tratamento de dados.

Uma vez estabelecido que a Ré está implementando um sistema de reconhecimento facial e que, portanto, está fazendo tratamento de dados pessoais, é preciso enfrentar a segurança com que tais dados serão tratados.

[31] Página 563 da ação autônoma de produção de provas – ref. doc. 4.
[32] Página 1103 da ação autônoma de produção de provas – ref. doc. 4.

O documento com especificações técnicas de segurança do sistema (IC-9.83.ME.XX/7XX-001), apresentado pela Ré como prova de segurança do sistema, traz disposições que dificultam, mas não eliminam, a possibilidade de invasão ou roubo de dados. Não traz nenhuma informação sobre como será a conexão do sistema SecurOS com a internet – elemento essencial para sua atualização, por exemplo, e oportunidade de vazamentos massivos.

Quanto às provas relativas à guarda e à segurança das informações, sobretudo dos dados biométricos, o mesmo documento faz menção a critérios de acesso das câmeras – como a necessidade de cadastro de pessoas autorizadas. Porém, não há qualquer informação sobre medidas a serem adotadas em caso de incidentes de segurança ou acessos não autorizados. Em entrevista já mencionada nos fatos desta ação, o Secretário de Transportes Metropolitanos afirmou que tais dados serão objeto de "um contrato seguro". Desconhece-se tal contrato e as câmeras já estão em funcionamento.

E desconhece-se qual será a segurança no que tange à possível anonimização dos dados.

O documento CS-9.83.ME.XX/7XX.0[33] apresenta a capacidade do sistema de promover o reconhecimento facial "ao vivo" ou após o armazenamento das imagens. Em ambos os casos, o sistema está apto a acompanhar a trajetória de uma determinada pessoa nas dependências do metrô e, também, identificá-la, seja através de um banco de dados com o qual as imagens capturadas serão contrastadas, seja a partir da identificação do usuário do metrô pelo bilhete único, hipótese em que será possível identificar a acompanhar a trajetória de uma pessoa mesmo sem o reconhecimento facial.

Explicam Abello, Araújo e Hirata Jr.:

> [...] os métodos de Visão Computacional atual são suficientes para que se faça um rastreamento limitado de pessoas, mesmo que não façam o reconhecimento facial do usuário. Se eles integrarem as informações do bilhete único (mesmo que não esteja sendo usado pelo seu proprietário), com as informações das câmeras, eles vão conseguir um rastreamento ainda melhor.
>
> O novo sistema pode facilitar sim, esse rastreamento. Uma das especificações da Concepção de Sistema é a fácil integrabilidade do software de análise forense com imagens ou bases de dados externas. Por meio de uso indevido ou não-autorizado, uma pessoa pode rastrear alguma outra nas dependências do metrô, desde que em mãos de uma galeria de imagens pertencendo a ela. O ator

[33] Páginas 939-1064 da ação autônoma de produção de provas – ref. doc. 4.

> mal-intencionado conseguiria identificar todas as aparições da pessoa registradas pelo sistema de vigilância nos últimos 30 dias, podendo depreender seu trajeto, horário, rotina entre outros.[34]

A Ré, em suas posições contraditórias, informa que a face reconhecida (dado pessoal biométrico) não seria dado pessoal porque não estaria atrelado a um CPF ou nome. Depois, afirma que os dados serão criptografados, e, em outra oportunidade, que os métodos de anonimização serão mais bem elaborados em projeto executivo, no decorrer da contratação. O CPF das pessoas é um dos dados obrigatórios para a aquisição de bilhete único[35].

Pressupondo-se boa-fé, é preciso afirmar que a Ré compreende equivocadamente o conceito de anonimização e de dado pessoal.

Como definido em lei, dado anonimizado é aquele com "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", nos termos do artigo 5º, XI LGPD. Ou seja, é aquele que impede a identificação do titular. Criptografia, como é público e notório, não têm o condão de impedir a identificação do titular, já que todos que tenham a chave de encriptação, decifram o código e acessam a integralidade do dado.

Por fim, importante ponderar a posição contraditória que a Companhia do Metropolitano de São Paulo assume ao afastar o fato de que dados pessoais são relativos à pessoa identificada ou identificável (art. 5º, inciso I, da LGPD) e ao tentar elucidar o propósito, a justificativa, para a implementação do sistema de monitoração eletrônica com reconhecimento facial nas estações do metrô. Por um lado, informa que os preceitos da LGPD foram cumpridos; por outro, afirma situar-se no regime excepcional direcionado à segurança pública, previsto no artigo 4º, III, *a* e *d*, da Lei Geral de Proteção de Dados (Lei 13.709/18), sem informar, contudo, como cumprirá com as condições impostas pelo §1º do mesmo artigo[36] e na ausência de legislação específica para essa hipótese.

Não se trata apenas de uma postura adotada pela Ré. Entidades públicas e privadas, resistentes aos novos parâmetros normativos, passaram a enquadrar suas atividades como "segurança

[34] Abello, Araújo e Hirata Jr., p. 69.
[35] Ver em https://bilheteunico.sptrans.com.br/cadastro.aspx.
[36] Lei 13.709/2018: Art. 4º. § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

pública", com o objetivo de se desincumbir das obrigações impostas pela LGPD à obtenção e tratamento de dados pessoais.

O tema aqui traz elementos de fato e de direito. No aspecto fático, é preciso reconhecer que a Companhia do Metropolitano de São Paulo não é autoridade competente responsável por atividades de segurança pública, seja na prática ou a partir de seu enquadramento legal e institucional, inclusive nos termos do art. 144 da Constituição Federal.

Ainda que seja óbvio, faz-se importante ressaltar: a razão de existir da Ré enquanto pessoa jurídica de direito privado – determinada e circunscrita por seu estatuto social - é o transporte, "planejamento, projeto, construção, implantação, operação e manutenção de sistemas de transportes públicos, metroviário, ferroviário e sobre pneus, na Região Metropolitana de São Paulo"[37].

Eventuais colaborações com autoridades competentes para a atividade de segurança pública não a transformam em uma a ponto de autorizar o enquadramento em regime excepcional de proteção de dados previsto pela LGPD e, muito menos, a coletar e tratar dados biométricos sem quaisquer parâmetros[38].

3.5 Desproporcionalidade da implantação do reconhecimento facial pela Companhia do Metropolitano de São Paulo

[37] O objeto da empresa Ré, previsto no artigo 2º de seu estatuto social, é: ARTIGO 2o - Constitui objeto da empresa:
I. planejamento, projeto, construção, implantação, operação e manutenção de sistemas de transportes públicos metroviário, ferroviário e sobre pneus, na Região Metropolitana de São Paulo;
II. execução das obras e dos serviços complementares ou correlatos, necessários à integração do sistema de transporte de passageiros ao complexo urbanístico da cidade;
III. construção e operação de terminais de passageiros; implantação e operação de estacionamentos;
IV. construção e comercialização, direta e indireta, admitida a coparticipação da iniciativa privada, de prédios residenciais e ou comerciais, bem como projetar, executar, administrar, direta ou indiretamente, outra qualquer obra de interesse público e da empresa;
V. comercialização de marca, patente, nome e insígnia; comercialização de áreas e espaços para propaganda; prestação de serviços complementares de suporte ao usuário, por si ou através de permissionários, com ou sem cessão de uso predial;
VI. comercializaçãodetecnologia,diretaouindireta,inclusiveemsociedadeouconsórcios;bem como a prestação de serviços de consultoria, apoio técnico e prestação de serviços na operação e na manutenção de equipamentos; construção e implantação de sistemas de transporte e de terminais de passageiros, no país e no exterior;
VII. edição, vedada a impressão, de jornais, revistas e outras publicações de cunho técnico e comercial, permitida a propaganda.

[38] O anteprojeto da Lei Geral de Proteção de Dados no âmbito penal (LGPD penal), produzido por uma comissão de juristas instituída por ato do presidente da Câmara dos Deputados explicita ainda mais o argumentado nesta ação: nem a Ré é autoridade competente em matéria de segurança pública, nem o reconhecimento facial massivo e indiscriminado poderia ser adotado. Ver a íntegra em: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf

Assim como o não enquadramento da Ré Companhia do Metropolitano de São Paulo como autoridade competente responsável por atividades de segurança pública tem contornos de fato e de direito, o mesmo ocorre com a desproporcionalidade da implementação massiva de sistemas de monitoração eletrônica com reconhecimento facial. Há um aspecto fático da desproporcionalidade que é inerente à tecnologia de reconhecimento facial.

Questionada sobre as razões e motivação para contratação, via procedimento licitatório, de sistema de monitoração eletrônica com reconhecimento facial, bem como sua finalidade, a Ré respondeu que seriam justificativas para a implantação do sistema, resumidamente:

a) aumentar a quantidade de locais monitorados;

b) melhorar a qualidade do armazenamento de imagens, bem como seu tempo;

c) implementar um sistema capaz de gerar alarmes;

d) integrar sistemas de monitoração eletrônica em um só;

e) centralização de equipamentos;

f) monitorar áreas de circulação restrita para pessoas/animais[39].

Ocorre que nenhuma dessas medidas exige um sistema de reconhecimento facial com a individualização, em tempo real, de todos os usuários do metrô. De partida, não estariam demonstradas a **adequação** e a **necessidade** da medida.

Para além destes dois pontos, parte-se para a exposição fática de que a implementação massiva do reconhecimento facial é **desproporcional**.

Conforme já explicado e comprovado, o sistema de reconhecimento facial se dá a partir da captura da imagem por câmeras digitais, filtragem para avaliação de qualidade, localização das regiões da face, extração de suas características, modelagem em 3D, reorientação frontal e de escala da imagem, classificação e reconhecimento da face, o dado biométrico, com as peculiaridades capazes de permitir a individualização e a identificação de uma pessoa.

Este dado biométrico, transformado em uma representação numérica, é confrontado com bancos de dados (de pessoas desaparecidas, procurados pela justiça ou quaisquer outros) criando a verificação da semelhança ou diferença entre as duas imagens: a capturada e a do banco de dados. Quanto maior a distância numérica entre as imagens, maior a diferença entre as imagens.

[39] Página 208 da ação autônoma de produção de provas – ref. doc. 4.

Há dois tipos de erros que podem ocorrer neste processo de verificação: falsos positivos, quando o sistema identifica equivocadamente duas pessoas distintas, isto é, associa um dado biométrico de uma pessoa à imagem de outra; falsos negativos, quando o sistema deixa de reconhecer a identidade entre duas imagens de uma mesma pessoa.

Falsos positivos e falsos negativos ocorrem em todo e qualquer sistema de reconhecimento facial. É inerente, portanto, à tecnologia. Isso porque, ao comparar as duas representações numéricas das imagens das faces, é estabelecido um limiar (*threshold*) e/ou posição em uma lista de classificações a partir do qual o sistema identifica a imagem reconhecida a outra em um determinado banco de dados. As imagens que superam esse limiar e/ou essa posição da lista servem para cálculo da taxa de falsos positivos e a proporção de vezes que a imagem buscada no banco de dados fica abaixo do limiar e/ou posição em uma lista de classificações serve para definir a taxa de falsos negativos[40].

> Em geral, a relação entre a quantidade de falsos positivos e a quantidade de falsos negativos é inversamente proporcional e pode-se escolher um balanço adequado ajustando-se à sensibilidade do modelo. Desta forma, modelos mais "sensíveis" são mais criteriosos para inferir identidade, portanto deixando de encontrar relações possíveis e consequentemente aumentando a quantidade de falsos negativos. Esses modelos também evitam encontrar relações espúrias e consequentemente há um decréscimo de falsos positivos. Modelos menos sensíveis encontram mais relações adequadas (decréscimos de falsos negativos) ao custo de mais relações espúrias (aumento de falsos positivos)[41].

Ou seja, quanto maior a quantidade de faces submetidas à identificação, maior a quantidade de falsos positivos e falsos negativos. Neste momento, fica claro o aspecto fático da desproporcionalidade da medida adotada pela Ré: aplicado o reconhecimento facial sobre uma média de 4 milhões de usuários por dia, a identificação de falsos positivos tende a ser altíssima – mesmo com um sistema considerado de alta acurácia, o que não se sabe se é o caso.

Conforme já demonstrado, a Ré já afirmou que pretende usar o sistema de reconhecimento facial para, entre outras coisas, identificar pessoas que constem em bancos de dados de pessoas procuradas. Submeterá, assim, todos os usuários dos serviços de transportes públicos a um sistema de identificação que tem, em sua essência, em razão da natureza do atual estado tecnológico, falsos positivos.

[40] Ver Abello, Araújo e Hirata Jr., p. 26.
[41] Abello, Araújo e Hirata Jr., p. 26

Assim, para além da violação da privacidade e captura indiscriminada dos dados biométricos de todos os usuários pelo sistema de monitoramento eletrônico com reconhecimento facial – o que por si só é capaz de comprovar a desproporcionalidade -, há também a já estatisticamente previsível identificação falsa positiva dos usuários como pessoas procuradas. O dano, aqui, é imensurável.

Adiciona-se à inerente característica de falsos positivos do sistema, majorada quando a tecnologia é aplicada sobre grande número de faces – como os 4 milhões de usuários diários do metrô de São Paulo – os vieses dos bancos de dados que, por sua vez, acarretam vieses no reconhecimento facial em si.

É a conclusão de Abello, Araújo e Hirata Jr.:

> O sistema de reconhecimento facial do metrô incorre no risco de apresentar falhas na execução: o sistema executa normalmente, mas, no entanto, retorna uma resposta incorreta. Vale lembrar que esse é um risco inerente a todo sistema de aprendizado computacional e nunca pode ser completamente mitigado.
>
> [...] Como explicamos, as taxas de falsos negativos e falsos positivos tendem a ser inversamente correlacionadas, podendo-se ajustar a sensibilidade dos modelos para alcançar um equilíbrio mais adequado. Não há entre a documentação do metrô uma análise sobre esse equilíbrio ou referência a taxa de sensibilidade utilizada.
>
> [...] modelos de reconhecimento facial podem incorrer em efeitos demográficos, onde a performance do modelo é pior para certas demografias. Entre efeitos tipicamente observados é a maior taxa de falsos positivos entre indivíduos de pele escura e indivíduos de etnias que não são apropriadamente representadas na base de dados. Não havendo referência a tratamento do sistema para mitigar esses vieses, é razoável supor que eles ocorram no sistema contratado pelo metrô. Isso faz com que o sistema potencialmente seja um perpetuador de desigualdades presentes na sociedade brasileira, selecionando erroneamente mais vezes indivíduos negros e imigrantes.[42]

Não é por outro motivo que sistemas de reconhecimento facial têm sido banidos em várias cidades. O banimento ou a imposição de restrições ao uso dessa tecnologia são crescentes à medida em que ficam mais evidentes os riscos à privacidade que o uso dessa tecnologia

[42] Abello, Araújo e Hirata Jr., p. 70-71.

envolve, assim como o potencial de uso indevido, além dos vieses raciais incorporados, com impactos danosos para grupos socialmente marginalizados.[43]

4. As inconstitucionalidades, as ilegalidades e a desconformidade com os tratados internacionais de direitos humanos da implementação de sistema de reconhecimento facial pela Ré Companhia do Metropolitano de São Paulo

Os fatos descrevem o processo licitatório internacional no qual foi contratado sistema de monitoramento eletrônico com reconhecimento facial pela Ré. Restou comprovado, a partir de questionamentos judiciais e extrajudiciais das Autoras, que tal sistema foi contratado e implementado à revelia das exigências previstas em múltiplos diplomas legais.

Conforme já mencionado, sendo um sistema reconhecimento facial que lida com dados pessoais biométricos, sensíveis, incide a LGPD onde são reparadas múltiplas violações: aos princípios que regem a proteção de dados (art. 2º da LGPD), aos princípios da atividade de tratamento de dados pessoais (art. 6º da LGPD); aos direitos do titular de dados pessoais, envolvendo o direito à autodeterminação informativa (arts. 17 a 22 da LGPD); à obrigação de ter uma base legal válida que justifique o tratamento, sequer o consentimento para captura de seus dados biométricos (art. 7º, I, 8º e 11 da LGPD) – muito menos o consentimento qualificado exigido para lidar com dados de crianças e adolescentes (art. 14 *caput* e §1º da LGPD) -; e o direito à informação sobre o processo de tratamento de seus dados (art. 9º, 18 e 19 da LGPD). Violam, também, as obrigações impostas àqueles que pretendem tratar dados na Administração Pública, desde a possibilidade em si de tratar tais dados biométricos (art. 7º, III da LGPD), passando pelos deveres em relação aos parâmetros para o controlador de dados (art. 37 da LGPD); à transparência e acesso a informações (art. 41 da LGPD); às precauções quanto aos danos decorrentes da atividade (art. 42 da LGPD).

Sendo o sistema de reconhecimento facial aplicado sobre usuários de serviço público, a Ré viola também direitos previstos no Código de Defesa dos Usuários de Serviços Públicos

[43] O uso de ferramentas que operam com base em reconhecimento facial foi banido em cidades como Portland, San Francisco, Oakland e Boston, nos Estados Unidos. Bélgica e Luxemburgo também se opuseram oficialmente ao uso da tecnologia de reconhecimento facial. A respeito, confira-se: https://edition.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html
https://www.uol.com.br/tilt/noticias/redacao/2019/05/16/por-que-uma-das-maiores-cidades-dos-eua-baniu-o-reconhecimento-facial.htm
https://canaltech.com.br/seguranca/reconhecimento-facial-e-banido-em-uma-segunda-cidade-nos-eua-142979/

(CDUSP) e no âmbito da legislação consumerista (CDC), seja em relação aos seus dados, ao tratamento desses dados e às informações que devem estar disponibilizadas.

As violações massivas à privacidade promovidas por tecnologias de vigilância – como é o sistema de reconhecimento facial -, afetam de maneira desproporcional crianças e adolescentes, para os quais as políticas devem ser adotadas tendo em vista o seu melhor interesse (art. 6º do ECA); e as pessoas negras, promovendo discriminação racial (art. 5º, caput e XLI da CRFB). De igual forma, pessoas trans também sofrem discriminação algorítmica[44].

Tratando-se de um sistema de reconhecimento facial massivo, implementado sobre todos os usuários do metrô, há uma clara incompatibilidade com o direito à privacidade (art. 5º, X, LXXII e LXXIX da CRFB), e à autodeterminação informativa, em seus contornos constitucionais e internacionais, bem como à proporcionalidade, caráter material do devido processo legal (art. 5º, LIV da CRFB). A ofensa à privacidade repercute, ainda, em ofensas aos direitos à liberdade de expressão e à liberdade de associação e reunião, como interpretados à luz do Pacto Internacional de Direitos Civis e Políticos pelo Comitê de Direitos Humanos da ONU e pelas Relatorias Especiais da ONU sobre Liberdade de Reunião e sobre Liberdade de Expressão.

Todas essas ilegalidades, violações à Constituição e aos tratados internacionais estão especificados a seguir.

4.1 A implementação do reconhecimento facial pela Ré viola a Lei Geral de Proteção de Dados - LGPD

A Lei Geral de Proteção de Dados (LGPD - Lei 13.079/2018) é uma resposta normativa[45] à apropriação generalizada de dados pessoais, por entes públicos e privados, levada a cabo nas últimas décadas.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[44] https://www.uol.com.br/tilt/noticias/redacao/2021/02/14/nao-e-so-racismo-reconhecimento-facial-tambem-erra-mais-em-pessoas-trans.htm

[45] Por se tratar de desafio global, a LGPD é contemporânea de legislações de outros países e de um crescente debate normativo. Ver em http://pensando.mj.gov.br/dadospessoais2011/contexto-internacional/

> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Possui, assim como as legislações internacionais que lidam com o tema, dois núcleos principais: um que enuncia e conforma o direito à proteção de dados pessoais como um direito autônomo, decorrente da autodeterminação informativa e da privacidade; e outro, que expõe quais são os deveres dos entes públicos e privados diante desses direitos.

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - o respeito à privacidade;
>
> II - a autodeterminação informativa;
>
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV - a inviolabilidade da intimidade, da honra e da imagem;
>
> V - o desenvolvimento econômico e tecnológico e a inovação;
>
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Para sairmos de um ambiente de apropriação generalizada de dados e abusos de toda sorte, as relações entre o titular de dados pessoais e entes públicos e privados que pretendem lidar com estes dados passa a ser mediada, por imposição legal, pela exigência de **consentimento** para obtenção e tratamento de dados, pela **transparência** na forma pela qual tais dados serão obtidos e tratados e pela **estrita proporcionalidade** entre o uso deste dado pessoal e a sua finalidade.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Os fundamentos da disciplina de proteção de dados previstos no art. 2º da LGPD trazem o sentido teleológico da norma e os princípios, dispostos no art. 6º da LGPD, operam como diretrizes necessárias de interpretação da lei em tese e no caso concreto. Incidem, assim, em toda argumentação apresentada nesta ação civil pública.

No presente caso, a Ré Companhia do Metropolitano de São Paulo implementa um sistema de monitoração eletrônica por meio de reconhecimento facial – ou seja, através da obtenção e tratamento de dados pessoais biométricos de todos os usuários do metrô, sem cumprir com os deveres impostos pela lei: consentimento do titular, transparência e estrita proporcionalidade.

a) Violação aos deveres de consentimento do titular de dados pessoais e ausência de base legal para reconhecimento facial massivo

A lei traz uma série de disposições sobre o **consentimento** do **titular de dados** que os entes públicos e privados devem obter para que seja permitido o **tratamento** de **dados pessoais**.

A legislação, em seu artigo 5º, traz a definição para cada um destes termos:

- **consentimento**: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII, LGPD)
- **titular**: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, V LGPD)
- **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. (art. 5º, X LGPD)
- **dado pessoal**: informação relacionada a pessoa natural identificada ou identificável (art. 5º, I, LGPD)

Como ficou provado nos fatos desta ação civil pública, o sistema de monitoração eletrônica mediante reconhecimento facial implementado pela **Ré faz tratamento de dados pessoais**, mais especificamente de dados biométricos, estando sujeita, portanto, à Lei Geral de Proteção de Dados, nos termos do seu artigo 3º, uma vez que os dados são coletados e tratados em território nacional.

O tratamento de dados pessoais – com todas as condutas pertinentes, definidas pelo art. 5º, X acima reproduzido – **somente** poderia ser realizado mediante fornecimento de consentimento do titular, nos termos do artigo 7º, I da LGPD, dada a total irrazoabilidade de todas as demais bases legais.

> Art. 7º O tratamento de dados pessoais **somente** poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;

Considerando serem os dados pessoais biométricos dados sensíveis, o art. 11, I da LGPD exige um consentimento deve ser qualificado: de forma específica, destacada e para finalidades específicas:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

O consentimento, aqui, também definido por lei, se refere à "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5º, XII LGPD).

Nos termos da LGPD, o consentimento é ativo: deve ser obtido por escrito ou por outro meio que expresse a manifestação de vontade, e, por se referir ao direito do titular dos dados pessoais, pode ser revogado a qualquer momento. Diz o artigo 8º da LGPD:

> Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
>
> § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
>
> § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
>
> § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
>
> § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
>
> § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
>
> § 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração.

Ademais, é ônus da Ré, enquanto controladora, ou seja, da pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, VI), provar a obtenção do consentimento, nos termos do §2º do artigo 8º supratranscrito.

A prova de consentimento dos usuários para tratamento de seus dados pessoais biométricos, exigido pelos artigos 7º, I e 11, I da LGPD, não existe, conforme restou comprovado em decisão transitada em julgado na já mencionada ação autônoma de produção de provas.

Ademais, não incide, no caso, nenhuma hipótese legal para afastamento do consentimento, previsto nos demais incisos do artigo 7º e do artigo 11, que abrangem obrigações legais ou regulatórias (art. 7º, II e 11, II, a); necessidade para execução de políticas públicas (artigo 7º, III e 11, II, b); estudos e pesquisas (art. 7º IV e 11, II, c). no exercício regular de direitos, inclusive em processo judicial, administrativo e arbitral (art. 7º V, VI e 11, II, d); para proteger a vida do titular em ameaça iminente (art. 7ª, VII e 11, II, e), por profissionais de saúde e no âmbito de ações e serviços de saúde (art. 7º, VIII e 11, II, f), quando necessário para atender aos interesses legítimos do controlador ou de terceiro, respeitados os direitos e liberdades do titular (art. 7º, IX) ou para proteção de crédito (art. 7º, X) ou para prevenção à fraude (art. 11, II, g).

Os dados biométricos dos usuários do metrô não são dados pessoais **necessários** à execução de política pública de transporte metropolitano, diferentemente do que se percebe, por exemplo, para inscrição de programas de renda. No mesmo sentido, tampouco a coleta de dados biométricos é obrigação legal ou regulatória imposta ao metrô e, mesmo nestas hipóteses, o titular deveria ser informado das hipóteses em que tal tratamento seria admitido, nos termos do §1º do artigo 7º da LGPD.

Assim, a Ré viola o dever de obter o consentimento, na forma da LGPD. Tampouco poderia cumpri-lo, pela opacidade, falta de transparência e de informações sobre o sistema de reconhecimento facial em implementação.

b) Violações ao dever de transparência e informações sobre o tratamento de dados pessoais

Sendo o **consentimento** uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (art. 5º, XII da LGPD), a lei impõe ao **controlador**, obviamente, o dever de informar de forma clara, adequada e ostensiva sobre o tratamento de dados pessoais ao titular.

O dever de transparência que se impõe - independentemente da base legal utilizada, como princípio do tratamento de dados (art. 6º, VI) - ao controlador de dados pessoais, posição que a Ré assume quando implementa sistema de reconhecimento facial nas estações do metrô, é

uma obrigação positiva de informar ao titular de dados pessoais sobre seus direitos, a **finalidade específica** do tratamento de dados, sua forma e duração, se os dados serão ou não compartilhados, quais as responsabilidades dos agentes (profissionais no âmbito privado ou público), além da identificação do controlador, nos termos do artigo 9º, incisos I a VII da LGPD.

Na hipótese de informações não serem apresentadas, serem falseadas ou abusivas, o consentimento previamente dado se torna sem efeito e a captura e o tratamento de dados se tornam ilegais, por disposição expressa dos parágrafos do referido artigo 9º da LGPD:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
>
> I - finalidade específica do tratamento;
>
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
>
> III - identificação do controlador;
>
> IV - informações de contato do controlador;
>
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
>
> VI - responsabilidades dos agentes que realizarão o tratamento; e
>
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.
>
> § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.
>
> § 2º Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

> § 3º Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer os direitos do titular elencados no art. 18 desta Lei.

A lei impõe ao controlador a obrigação de explicar o porquê da captura e do tratamento de dados, para que o titular possa exercer a sua autodeterminação informativa de maneira plena, que, neste caso, se dá através do consentimento.

A Ré foi questionada quanto aos requisitos exigidos pelo artigo 9º da LGPD. Afinal, estando em processo de contratação e implementação de um sistema de monitoração eletrônica com reconhecimento facial, a Ré deveria possuir um plano, uma orientação, uma política para dar conta de suas obrigações legais. Nada mais óbvio, diante das obrigações legais expressas.

No entanto, o sistema de reconhecimento facial nas estações do metrô já está em operação e não foi obtido o consentimento, não foi informada a finalidade específica da sua coleta e tratamento, tampouco disponibilizada de forma clara, adequada e ostensiva a informação sobre controlador, processos e compartilhamentos. Os direitos dos titulares de dados pessoais foram ignorados.

A Ré atua, assim, como se não houvesse a Lei Geral de Proteção de Dados, como se ainda estivéssemos em um ambiente de apropriação generalizada de dados pessoais, em clara violação ao artigo 6º da LGPD que exige observância de **boa-fé, transparência**, **segurança**, **prevenção**, **responsabilização e prestação de contas**.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
>
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> [...]
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Os fatos mostram que a Ré deixou de apresentar provas na ação autônoma de produção de provas, alegando serem provas negativas e, portanto, impossíveis. Erro crasso e conduta ilegal. A LGPD explicitamente exige a comprovação da observância e do cumprimento das normas de proteção de dados pessoais.

c) Violações à estrita proporcionalidade para coleta e tratamento de dados pessoais

A esta altura já é perceptível a incompatibilidade da captura e tratamento massivos de dados pessoais por sistemas de reconhecimento facial com a legislação: por ser massivo e indiscriminado, não cumpre o requisito da finalidade específica, além de se mostrar desproporcional.

Não havendo clareza quanto à finalidade específica, não há condições para o consentimento livre e informado[46]. E, mesmo que a obtenção do consentimento seja possível, a sua revogação não será: como um usuário do metrô deixará de ter a sua face não capturada? A opção não pode ser deixar de usar o serviço de transporte público, direito social constitucional, direito do consumidor, direito de usuário de serviço público.

Por isso, a LGPD também se aplica aos órgãos públicos, incluídos evidentemente aqueles da administração pública direta e indireta, e demanda que os dados pessoais sejam coletados e tratados apenas e para estritamente garantir a execução daquela política pública (art. 7º, III da LGPD e art. 11, II, c, da LGPD).

A LGPD incorporou em seu texto legal o **conceito de proporcionalidade**, enquanto juízo prévio necessário às atividades de tratamento de dados. Pela disciplina legal, sendo as atividades de tratamento de dados pessoais devem observar a **finalidade, a adequação e a necessidade da medida**, com vistas a restringir, o mínimo possível, o direito do titular.

[46] Ou qualquer outra base legal.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados [...]

Em um primeiro momento, o tratamento de dados pessoais precisa atender a propósitos legítimos e específicos, seu processo precisa ser compatível com a finalidade e limitado ao mínimo necessário para atingir essas finalidades. Tais conceitos dialogam com as teorias que impõem a mínima restrição aos direitos fundamentais. Sendo o direito à proteção de dados um direito autônomo, sua restrição (ou seja a coleta e tratamento desses dados) só pode ocorrer com o consentimento do titular, com clareza de informações sobre o processo e para atender a específica finalidade, e na medida estrita desta.

É evidente que o tratamento massivo e indiscriminado de dados pessoais através de sistemas de reconhecimento facial em equipamentos públicos, ou mesmo na rua, são desproporcionais. Entre as respostas incoerentes e confusas dadas pela Ré, extrai-se a informação que a Ré pretende usar o sistema de reconhecimento facial para identificar pessoas que constem em bancos de dados de pessoas procuradas, submetendo todos os usuários dos serviços de transportes públicos a um sistema de identificação que tem, em sua essência, em sua natureza do atual estado tecnológico, falsos positivos, que inclusive são potencialmente mais comuns, como já demonstrado, em relação a grupos já historicamente vulnerabilizados, como as pessoas negras.

4.2 A implementação do sistema de reconhecimento facial pela Ré Companhia do Metropolitano do São Paulo viola o Código de Defesa do Consumidor

O caso em comento trata da prestação de um serviço público, devendo ser analisado sob o prisma das normas de Direito Público. A análise da relação aqui discutida envolve bem

essencial para a vida em comunidade, tendo que prezar pela aplicação de leis que visem proteger o usuário do serviço metroviário (consumidor deste serviço), em razão da sua vulnerabilidade e hipossuficiência.

Importa, portanto, destacar que o ordenamento jurídico deve ser interpretado como único, harmônico e coordenado entre si, sendo possível a aplicação em caráter complementar tanto do CDC como da LGPD sobre esta temática. Isto também porque o art. 7º do CDC permite uma interpretação sistemática de diferentes normas, prevalecendo sempre a aplicação mais favorável ao consumidor. A LGPD, por sua vez, coloca como fundamento da proteção de dados pessoais a defesa do consumidor (art. 2º, VI), reconhece o exercício de direitos perante os organismos de defesa do consumidor (art. 18, § 8º), bem como o regime de responsabilidade do CDC nas relações de consumo (art. 45).

O usuário do metrô, destaca-se, é a parte vulnerável dessa relação, devendo ter como pressuposta a sua condição, devendo receber tratamento desigual na medida de sua desigualdade.

Sua vulnerabilidade também é manifesta ao estudar os usuários desse serviço. Ao considerar as relações sociais hoje existentes e a extensão geográfica do Município, não há como imaginar que as pessoas consigam se locomover, como regra, sem a utilização, no mínimo, do transporte público, a qual tem que ser vista como regra. Isso porque a sua não utilização apenas é possível se o cidadão ou cidadã possuir condições econômicas suficientes para optar por um meio de transporte privado todos os dias da semana. Este recorte permite inferir que apenas um segmento muito específico da população não será submetido à coleta de seus dados ao realizar o transporte diário. O **transporte público representa para muitos o mínimo necessário para que seja possível a locomoção dentro do Município de São Paulo e de sua Região Metropolitana, ou seja, é o mínimo necessário para que o exercício do direito de ir e vir seja possível.**

Além disso, o direito ao transporte público não é apenas um direito em si mesmo, **mas é também uma garantia necessária para o direito de acesso à cidade**, ou seja, ao acesso a inúmeros outros equipamentos indispensáveis para o exercício de direitos fundamentais, como o direito à saúde (acesso a hospitais, UBS etc.), à educação (acesso a escolas, creches e universidades), à cidadania (acesso ao colégio eleitoral e participação em manifestações políticas), à segurança pública (acesso a delegacias de polícia), à cultura (acesso a cinemas,

teatros etc.), ao emprego (acesso aos locais de trabalho), à liberdade econômica (acesso a novos mercados, reduzindo o peso do fator geográfico e ampliando a concorrência) etc.

Imprescindível, portanto, a necessária harmonização e equilíbrio dos interesses na relação de consumo, com base também na boa-fé objetiva (art. 4º, III). Sendo deste modo inviável uma relação na qual inexista informações claras sobre o que está sendo coletado e, muito menos, sem o consentimento expresso dos usuários da via férrea.

Destaca-se ainda que **o direito à informação nas relações consumeristas é a base para o exercício de todos os demais direitos**, **considerando justamente uma relação caracterizada pela vulnerabilidade dos consumidores e pela assimetria informacional entre as partes.**

Assimetria esta que fica mais clara quando se considera a relação indivíduos e Estado, tendo este último toda a máquina estatal em funcionamento a seu favor e o acesso a enormes bases de dados e a qual é exacerbada pela assimetria informacional presente, por natureza, com o emprego de uma tecnologia nova, com fluxo informacional pouco ou nada transparente aos usuários.

É necessário que as informações sejam completas, adequadas e eficientes. Sem o respeito ao direito à informação, não é possível afirmar que uma conduta foi praticada de acordo com o princípio da boa-fé objetiva, que consubstancia os deveres éticos mínimos exigíveis nas relações jurídicas.

O Direito do Consumidor possui inclusive um regramento específico sobre bancos de dados e cadastros de consumidores, determinando o art. 43 do CDC que o consumidor tem direito de acesso às suas informações cadastradas/registradas (caput); de qualidade e precisão sobre seus dados (§1º), de comunicação sobre uso de seus dados (§2º); de correção de dados incorretos (§3) e de acesso à suas informações de maneira acessível (§6º); bem como determina que os bancos de dados relativos a consumidores, serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

Deste modo, entende-se que os bancos de dados com informações dos consumidores (no caso, os usuários do serviço do metrô) se referem à personalidade destes, não implicando em dados empresariais, mas sim dados públicos. Por esse motivo, esta base deve respeitar limites legais. No caso em comento, discute-se sobre o grande armazenamento de uma série de dados pessoais sensíveis sem sequer o conhecimento, muito menos o consentimento dos consumidores do serviço metroviário. O consumidor não dispõe de informações de caráter técnico, econômico e

jurídico, aptos a ensejar sua escorreita interpretação sobre a aplicação e alcance do contrato, estabelecendo como direito básico seu, a informação clara e adequada (art. 6º, III, CDC).

A assimetria informacional ainda é exacerbada pelo fato de se tratar de tecnologia ainda desconhecida da população e cujos danos e riscos **são ainda menos informados e compreensíveis**.

Soma-se ao exposto o fato de que não se sabe sequer qual é a finalidade que a Ré dará aos dados pessoais de todos os usuários do metrô. A população não tem qualquer informação sobre o processo de tomada de decisão resultante do uso da tecnologia de reconhecimento facial. Decisões capazes de intervir em suas vidas seriam tomadas com base em algoritmos e automação, sujeitas a erros e potencialmente violadoras de diversos direitos, sem que os consumidores soubessem nada sobre o funcionamento desse processo.

Além da falta de informações sobre a coleta de dados em si, vale apontar que não foi oferecida qualquer garantia por parte do Metrô de que os dados coletados não poderiam ser utilizados para atividades diversas daquelas expressamente declaradas.

Conforme defendido por Laura Schertel Mendes, extrai-se desse dispositivo o conceito segundo o qual "qualquer registro de dados pessoais deve se submeter ao crivo da legalidade, na medida em que a lei determina que os bancos de dados e cadastros relativos a consumidores são considerados públicos e, portanto, devem respeitar os limites legais"[47]. Assim, qualquer armazenamento de dados pessoais, "por se referir à personalidade do consumidor, não diz respeito à esfera empresarial apenas, mas sim ao público e, portanto, a ele se aplica o regime constitucional e legal"[48].

A ausência de consentimento informado sobre a coleta de dados pessoais sensíveis (dados biométricos) também implica em grave violação, em especial nos direitos básicos do consumidor relativos à compreensão dos riscos informacionais da coleta de sua emoção e seus dados biométricos (CDC, art. 6º, I) e das características básicas de como funciona o serviço de análise desses dados (CDC, art. 6º, III). Diz o Código nesse aspecto:

Art. 6º São direitos básicos do consumidor:

[47] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 146.
[48] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014, p. 143.

> I - a proteção da vida, saúde e segurança contra os riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos;
>
> II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações;
>
> III - a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem;

No mesmo caminho, é possível destacar os direitos dos usuários e usuárias dos serviços públicos previstos na Lei nº 13.460/2017:

> Art. 5º O usuário de serviço público tem direito à adequada prestação dos serviços, devendo os agentes públicos e prestadores de serviços públicos observar as seguintes diretrizes: (...)
>
> IV – adequação entre meios e fins, vedada a imposição de exigências, obrigações, restrições e sanções não previstas na legislação; (...)
>
> VIII - adoção de medidas visando a proteção à saúde e a segurança dos usuários;
>
> Art. 6º São direitos básicos do usuário:
>
> III - acesso e obtenção de informações relativas à sua pessoa constantes de registros ou bancos de dados, observado o disposto no inciso X do caput do art. 5º da Constituição Federal e na Lei nº 12.527, de 18 de novembro de 2011;
>
> IV - proteção de suas informações pessoais, nos termos da Lei nº 12.527, de 18 de novembro de 2011;

Ainda que se considere a possibilidade de haver consentimento para a coleta e tratamento dos dados pessoais sensíveis no presente caso, como não há consentimento livre, específico, informado e em destaque dos titulares dos dados os quais não concordaram ou deram seu consentimento informado -, há uma violação do ordenamento jurídico brasileiro, colocando os consumidores e pessoais naturais em situação de ausência de controle e autodeterminação informativa sobre seus dados biométricos, em violação ao art. 5º da Constituição, art. 21 do Código Civil e art. 6º do Código de Defesa do Consumidor.

A situação até aqui relatada assemelha-se quase a um contrato de adesão, no qual há extrema mitigação na possibilidade de negociação entre as partes. Em verdade, no caso concreto, não há qualquer possibilidade de negociação, cabendo ao cidadão ou à cidadã aceitar os termos do contrato tal qual fixados unilateralmente pelo fornecedor do serviço. Em razão desses fatores, um maior rigor na análise das práticas comerciais realizadas pelo Metrô se mostra necessário.

Como visto, por se tratar de relação entre pessoas e o Estado em prestação de serviço essencial, cuja utilização é obrigatória para o exercício de diversos direitos, de monopólio natural e, ainda, de emprego de tecnologia complexa de difícil compreensão do consumidor, a assimetria de poder e informacional e a vulnerabilidade do consumidor são exacerbadas, de modo que se faz necessária especial atenção às disposições de práticas abusivas do CDC.

A conduta da Ré constitui prática abusiva por exigir do usuário vantagem manifestamente excessiva, ao obrigá-lo a ceder informações da sua esfera privada, sem informações claras e adequadas e para uma finalidade não justificada e desproporcional, em clara violação ao art. 39, V do CDC. A prática configura 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 fundamental à privacidade do consumidor; (ii) restringe direitos fundamentais inerentes ao contrato, em especial, direito de escolha e de informação, ao não limitar os cruzamentos de bancos de dados e suas finalidades; e (iii) é excessivamente onerosa ao consumidor, uma vez que ignora seus interesses ao investir em contratação de tecnologia desproporcional, em detrimento de melhorias no serviço. Há, portanto, manifesta violação à proteção do consumidor com métodos comerciais desleais e práticas abusivas, previstas no art. 6º, inc. IV do CDC.

Em sentença do caso análogo ocorrido com a tecnologia a ser implantada na Via 4 do metrô, caso que ainda tramita sob o nº 1090663-42.2018.8.26.0100, tem-se o entendimento de que

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

Destaca-se ainda que segundo o artigo 37, §2ª do Código de Defesa do Consumidor dispõe que: "É abusiva, dentre outras a publicidade discriminatória de qualquer natureza, a que incite à violência, explore o medo ou a superstição, se aproveite da deficiência de julgamento e experiência da criança, desrespeita valores ambientais, ou que seja capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa à sua saúde ou segurança." Assim, 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.

Sobre o dever de se observar a proporcionalidade entre os direitos e deveres dos usuários de serviços públicos, ele está positivado, no caso do Estado de São Paulo, na Lei Estadual nº 10.294/1999:

> Art. 7º - O direito à qualidade do serviço exige dos agentes públicos e prestadores de serviço público: (...)
>
> V – adequação entre meios e fins, vedada a imposição de exigências, obrigações, restrições e sanções não previstas em lei;

Conforme já mencionado, é desproporcional violar indiscriminadamente a privacidade e o direito autônomo à proteção de dados de cerca de 4 milhões de pessoas diariamente, sem qualquer consentimento de seus titulares, sem qualquer clareza sobre como tais dados serão tratados sob a justificativa da segurança pública, ainda mais quando se considera que o sistema é falho, é inerente à sua tecnologia apresentar falsos negativos e falsos positivos, e, portanto, ineficaz.

Desse modo, tem-se que as disposições do caso em comento violam o direito ao consumidor, em função de sua abusividade, falta de proporcionalidade, desrespeito ao direito de informação, autodeterminação, violação do princípio da vulnerabilidade e hipossuficiência, desconsideração do direito a cidade e direito ao consentimento livre e informado previsto tanto no CDC como na LGPD. Em função do exposto deve a Ré ser condenada em função da manifesta ilegalidade de sua conduta.

4.3 A implementação do sistema de reconhecimento facial pela Ré Companhia do Metropolitano do São Paulo viola o Estatuto da Criança e do Adolescente

As preocupações suscitadas nos tópicos anteriores assumem contornos ainda mais gravosos quando se constata que, dentre os passageiros do metrô que serão submetidos ao reconhecimento facial compulsório, estão crianças e adolescentes – sujeitos que gozam de

proteção integral com absoluta prioridade, em razão do peculiar estágio de desenvolvimento que atravessam. A proteção integral da criança e adolescente está consagrada no artigo 227 da CF/88:

> Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, **com absoluta prioridade**, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, **à dignidade, ao respeito**, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

Como se viu, a implementação de câmeras de reconhecimento facial no transporte coletivo, longe de representar medida inócua, constitui grave ameaça aos direitos fundamentais à imagem, à privacidade, e à autodeterminação informativa de todos os usuários do metrô, e, portanto, também de crianças e adolescentes. Desse modo, deve-se perquirir se as condutas da Ré harmonizam-se com o melhor interesse desses indivíduos, levando-se em conta, ainda, os marcos normativos que tutelam especificamente os direitos fundamentais acima elencados na seara da infância e da adolescência.

No que tange à inviolabilidade física, psíquica e moral das crianças e adolescentes, o Estatuto da Criança e Adolescente traz normas específicas a lhe dar concretude. **O direito à imagem**, assim, reveste-se como direito ao respeito, que consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, conforme preceitua o art. 17 do ECA:

> Artigo 17. O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo **a preservação da imagem**, **da identidade**, da autonomia, dos valores, ideias e crenças, dos espaços e objetos pessoais.

Como se vê, o direito à imagem de crianças e adolescentes deve assumir lugar de especial atenção em razão da gravidade e longevidade dos impactos que podem advir de sua violação. Tratando mais especificamente das normas de proteção aos dados pessoais - os quais, por representarem verdadeira extensão da subjetividade humana, têm sua tutela intrinsecamente ligada à garantia da privacidade - percebe-se que o legislador nacional, a exemplo do que foi feito na Europa, consagrou normas especiais no que diz respeito aos dados de crianças e adolescentes. A LGPD, em seu art. 14, dispõe que:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes **deverá ser realizado em seu melhor interesse**, nos termos deste artigo e da legislação pertinente.
>
> §1º O tratamento de dados pessoais de crianças deverá ser **realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal**" (grifos nossos).

Depreende-se, da leitura do artigo acima colacionado e das normas do Estatuto da Criança e do Adolescente que o tratamento dos dados pessoais de crianças e adolescentes **deverá ser sempre realizado em seu melhor interesse, mesmo aqueles com consentimento parental específico.** Logo, um projeto de implementação de câmeras tal como o intentado pela Ré pressupõe, necessariamente, a demonstração a priori de que o tratamento realizado nos dados coletados de crianças e adolescentes está consoante ao seu melhor interesse, bem como a obtenção de consentimento específico das mães, pais ou responsáveis para esse fim.

O Comitê dos Direitos das Crianças da ONU, em seu Comentário Geral n° 25 sobre os direitos das crianças no ambiente digital, **tratando especificamente das práticas de vigilância digital de crianças**, estabelece que tais práticas não podem ser realizadas indiscriminadamente, inadvertidamente e sem que haja possibilidade de objeção; ou seja, à margem do consentimento das crianças e, quando cabível, de seus pais ou responsáveis:

> "75. Qualquer vigilância digital de crianças, associada a qualquer processamento automatizado de dados pessoais, deve respeitar o direito da criança à privacidade e **não deve ser realizada rotineiramente, indiscriminadamente ou sem o conhecimento da criança ou, no caso de crianças muito novas, o de sua mãe, pai ou cuidador; nem deve ocorrer sem o direito de objeção a essa vigilância**, em ambientes comerciais e educativos e de cuidados, e deve sempre ser considerado o meio menos invasivo à privacidade disponível para cumprir o propósito desejado." (grifos nossos).

No entanto, o projeto que o Metrô pretende realizar de forma alguma respeita as normas mencionadas, constituindo gravíssima violação a direitos de crianças e adolescentes.

A realização do reconhecimento facial importará, portanto, em violação aos direitos de imagem, privacidade e direitos fundamentais correlatos de crianças e adolescentes, os quais, sem o consentimento de seus pais, sem o seu próprio consentimento ou a possibilidade de evitá-lo, acabarão tendo suas imagens coletadas pelo Metrô e submetidas a programas de

reconhecimento facial - afinal, como já mencionamos, não há como realizar qualquer tipo de reconhecimento facial sem que todas as faces, de todos os usuários do Metrô, sejam lidas, copiadas, medidas, registradas e comparadas ao(s) banco(s) de dados eventualmente utilizado(s).

Mas, além dessa ilegalidade de plano, é importante ressaltar que a possibilidade de reconhecimentos equivocados é ainda mais alta em relação a crianças e adolescentes, o que torna ainda mais problemática a utilização de tal tecnologia. Assim apontaram Abello, Araújo e Hirata Jr., indicando drástica redução de eficiência do sistema, já que, "como esperado, o efeito do envelhecimento é acentuado para crianças e adolescentes pois as mudanças de fisionomia são mais acentuadas"[49].

Portanto, o argumento de que o reconhecimento facial possibilitaria a localização de crianças e adolescentes desaparecidos cai por terra. A possibilidade de acerto diminui consideravelmente em crianças pequenas (que seriam evidentemente o foco de uma política de localização de crianças desaparecidas), ainda mais se considerando que, quanto mais o tempo passa, menor a chance de um reconhecimento correto. Dessa forma, não se poderia argumentar que o tratamento de dados destas crianças está sendo feito para a sua proteção, nos termos do art. 14, §3º da LGPD, considerando, além do baixo índice de acerto, as violações aos seus direitos.

Ainda, as dificuldades da tecnologia frente à rápida alteração das faces das crianças revelam a inadequação do tratamento destes dados para a finalidade anunciada, bem como o tratamento, a todo momento, de todas as crianças e adolescentes que utilizam o serviço público se mostra excessivo e desnecessário para a localização de crianças e adolescentes desaparecidos.

Ao revés, não se pode perder de vista o evento traumático que pode constituir a uma criança ou adolescente uma abordagem equivocada por autoridades em virtude de um falso reconhecimento positivo (seja a que título se der).

---

[49] Abello, Araújo e Hirata Jr., p. 47. Estudo publicado pelo National Institute of Standards and Technology, instituto da administração pública estadunidense, no qual se realizou uma série de avaliações periódicas em algoritmos de reconhecimento facial, encontrou "elevados falsos positivos nos idosos e nas crianças; os efeitos foram maiores nos adultos mais velhos e nas crianças mais novas". Isso se deve evidentemente às mudanças mais agudas na aparência ocasionadas pelo envelhecimento neste período de vida das pessoas, tornando o reconhecimento facial ainda mais precário em termos de efetividade, ver em BAN FACIAL RECOGNITION TECHNOLOGIES FOR CHILDREN AND FOR EVERYONE ELSE - LINDSEY BARRETT, Boston University Journal of Science and Technology Law. Volume 26.2. Disponível em: https://www.bu.edu/jostl/files/2020/08/1-Barrett.pdf; The Impact of Age-Related Variables on Facial Comparisons with Images of Children: Algorithm and Practitioner Performance, Dana Jaclyn Michalski. Disponível em: https://digital.library.adelaide.edu.au/dspace/handle/2440/111184.

Por fim, não foram previstos, em qualquer lugar, tratamentos especiais para os dados de crianças e adolescentes, como acesso restrito a funcionários responsáveis pelas buscas de desaparecidos, tempo de armazenamento e descarte especiais, dentre outros procedimentos de segurança e minimização de risco que poderiam ser adotados.

4.4 A implementação do sistema de reconhecimento facial pela Ré Companhia do Metropolitano do São Paulo é incompatível com o direito à privacidade

A Constituição da República assegura a inviolabilidade da privacidade, intimidade, vida privada, honra e imagem das pessoas (art. 5º, X).

A Constituição também assegura o direito de autodeterminação informativa, previsto no artigo 5º, LXXII, da Constituição, designação dada para a prerrogativa individual de impedir a indevida recolha, armazenamento, utilização e transmissão de seus dados pessoais, pressupondo conhecimento e consentimento sobre a existência e uso de bancos de dados, bem como possibilidade de sua correção, sem os quais será impossível ao cidadão promover medidas de responsabilização por seu uso inadequado, desautorizado ou impreciso.

Portanto, em âmbito constitucional, com *status* de direitos individuais fundamentais encontram-se os direitos à privacidade, intimidade, vida privada, honra e imagem, bem como à autodeterminação informativa – corolário à privacidade.

É a partir dos direitos fundamentais à privacidade e à intimidade que a legislação reconhece a proteção dos dados pessoais como um direito autônomo, com espraiamento em outras tantas legislações, como o Código de Defesa do Consumidor, o Estatuto da Criança e do Adolescente, o Código Civil e o Marco Civil na Internet.

O direito internacional dos direitos humanos também oferece insumos e ferramentas de análise quando se discute as relações entre privacidade e utilização de tecnologias como as de reconhecimento facial em espaços públicos ou outros espaços acessados pelo público.

O artigo 17 do Pacto Internacional de Direitos Civis e Políticos diz especificamente que:

> 1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação.
>
> 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.

O Comentário Geral n.º 16[50], por meio do qual o Comitê desenvolve as prerrogativas e diretrizes que devem ser inferidas diante do que é previsto no artigo 17 acima mencionado, assentou que**,** não apenas deve haver uma lei regulamentando interferências e restrições ao direito à privacidade pelos Estados, como também essa lei deve estar de acordo com os princípios e direitos que são garantidos pelo Pacto Internacional sobre Direitos Civis e Políticos.

E, mesmo nos casos em que haja uma legislação específica regulamentando a interferência do Estado na privacidade dos indivíduos, a mera existência da legislação não é suficiente para que as garantias do direito à privacidade sejam observadas. A existência da lei é compulsória, assim como é necessário que o conteúdo da lei esteja de acordo com os parâmetros internacionais aplicáveis, sendo também importante que as circunstâncias específicas em que o direito à privacidade é relativizado seja previsto na legislação.

Relatório do Alto Comissariado da ONU para Direitos Humanos[51] reafirma que a legislação que autoriza a interferência dos Estados no direito à privacidade deve especificar em detalhes as circunstâncias específicas na qual tal ingerência é permitida e ser interpretada restritivamente.

No caso, a LGPD e uma série de outras leis nacionais dispõem sobre as estritas hipóteses onde é possível interferir na privacidade, permitindo o tratamento de dados pessoais. Tais bases legais, desenvolvidas no tópico 4.1 dessa ação, não podem ser interpretadas para ampliar a intervenção no direito à privacidade, sob pena das estritas hipóteses legais que permitem essa intervenção se tornarem regra, e não exceção.

O relatório ainda menciona expressamente que "**o direito à privacidade entra em jogo quando um governo está monitorando um espaço público**, como um mercado ou **uma estação de trem**, observando os indivíduos" (tradução livre e grifos nossos) e que "a mera existência de vigilância secreta equivale a uma interferência no direito à privacidade" (tradução livre).

Isto porque as interferências ilegais e/ou arbitrárias no direito à privacidade potencialmente afetam outros direitos. Aqui, destaca-se nesse sentido a **liberdade de expressão** e a **liberdade**

[50] Comitê de Direitos Humanos da ONU, General Comment No. 16 (Artigo 17 PIDCP), 8 de abril de 1988. "Comentários gerais" são os documentos por meio dos quais os órgãos da ONU interpretam oficialmente as provisões dos respectivos tratados. Mais informações sobre os comentários gerais podem ser encontradas em https://www.ohchr.org/en/hrbodies/pages/tbgeneralcomments.aspx (em inglês).
[51] Disponível em: https://digitallibrary.un.org/record/1640588

de associação e reunião pacífica, fundamentais e basilares em qualquer sistema democrático. A privacidade e liberdade de expressão se reforçam mutuamente, tendo em vista que, para que alguém tenha espaço para pensar, falar e ter sua voz escutada, é um pré-requisito fundamental que não se esteja submetido(a) à vigilância constante (especialmente por parte do Estado) e que o direito à vida privada seja respeitado.

Nesse contexto, vale destacar ainda que a Relatoria Especial para Liberdade de Expressão da ONU já se manifestou no sentido de reconhecer o **direito ao anonimato** como um aspecto importante do direito à liberdade de expressão e à privacidade[52]. Trata-se de um fator bastante relevante quando se pensa que câmeras equipadas com sistemas de reconhecimento facial instaladas nas dependências do metrô podem representar a impossibilidade de que se possa transitar nesses espaços e usar o serviço de transporte de maneira incógnita. Ainda no tocante à liberdade de expressão, é importante destacar que o então relator especial para Liberdade de Expressão da ONU fez uma chamada em junho de 2019 em favor de uma **moratória global** imediata da **venda, transferência e o uso de ferramentas de vigilância, o que inclui tecnologias de reconhecimento facial**. Nesse sentido, o relator afirmou que "ferramentas de vigilância podem interferir nos direitos humanos, desde o direito à privacidade e liberdade de expressão até os direitos de associação e reunião, crença religiosa, não discriminação e participação pública". E ainda não estão sujeitos a nenhum controle global ou nacional eficaz".[53] Defendeu ainda que os Estados adotem salvaguardas nacionais que estejam de acordo com o direito internacional dos direitos humanos para proteger os indivíduos da vigilância ilegal, incluindo o desenvolvimento de mecanismos públicos que aprovem e supervisionem tecnologias de vigilância.

Conectadas aos riscos à liberdade de expressão, há também as ameaças à liberdade de associação trazidas pelo uso de reconhecimento facial em espaços públicos. A **liberdade de associação e reunião pacífica**, garantida pelo Artigo 20, parágrafo 1 da Declaração Universal dos Direitos Humanos (DUDH) e reforçada no Artigo 21 do PIDCP, no artigo 15 da Convenção Americana sobre Direitos Humanos e no Artigo 5(d), ix da Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial[54]. O Relator Especial da ONU sobre Liberdade de Reunião e Associação Pacífica declarou que "deve ser proibido o uso de técnicas

[52] Relatório sobre criptografia, anonimato e a estrutura dos direitos humanos da Relatoria Especial para a liberdade de expressão, A/HRC/29/32, 22 de maio de 2015.
[53] Disponível em: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736
[54] Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial, 21 de dezembro de 1965, UN Treaty Series, vol. 660, p. 195.

de vigilância para fins de vigilância indiscriminada e não direcionada daqueles que exercem seu direito de reunião e associação pacífica, tanto em espaços físicos quanto digitais"[55].

Em geral, as ameaças ao exercício desses direitos estão relacionadas ao **efeito inibidor** (ou efeito inibitório - em inglês, *chilling effect*) que pode ser causado pelo uso dessas tecnologias em espaços públicos ou acessíveis ao público e diz respeito à alteração do comportamento por indivíduos submetidos a monitoramento[56]. Por exemplo: o uso de tecnologias de reconhecimento facial durante protestos pode desencorajar as pessoas a participar desse tipo de movimentação e até mesmo facilitar o rastreamento e perseguição de ativistas, impactando negativamente o exercício da democracia participativa[57].

Para se movimentar pela cidade para participar de reuniões, protestos e manifestações artísticas, por exemplo, é necessário o uso do transporte público. Isso quer dizer que estações de metrô que possuam câmeras de reconhecimento facial podem interferir na possibilidade de ir e vir, em decorrência do receio de ser rastreado(a) ou mapeado(a).

Como se vê, a discussão sobre vigilância em espaços públicos representa uma limitação do direito à privacidade, desde a perspectiva constitucional e internacional.

Por isso, o Comitê de Direitos Humanos da ONU em seu parágrafo 10, reconhece expressamente a proteção de dados pessoais como fator fundamental da privacidade. O mesmo dispositivo ainda destaca que o respeito ao direito à privacidade dos indivíduos também envolve o direito à informação sobre a coleta e o uso de seus dados pessoais.

O relatório dedicado ao direito à privacidade na era digital[58] do Alto Comissariado da ONU para Direitos Humanos explicita que a mera geração e coleta desses dados afeta o direito à privacidade, uma vez que por meio dessas etapas o indivíduo perde algum controle a respeito

---

[55] A/HRC/41/41 17 de maio de 2019, para 57.

[56] O relatório do Alto Comissariado das Nações Unidas para Direitos Humanos sobre o impacto de novas tecnologias na promoção e proteção dos direitos humanos no contexto de assembleias, incluindo protestos pacíficos, traz em seu parágrafo 34 que: O surgimento da **tecnologia de reconhecimento facial levou a uma mudança de paradigma** [...] pois aumenta drasticamente a capacidade de identificar todos ou muitos participantes em uma reunião de forma automatizada. Isso é particularmente problemático se a tecnologia de reconhecimento facial em tempo real for implementada, permitindo a identificação em tempo real, bem como a vigilância direcionada e o rastreamento dos participantes. **A identificação incorreta em tempo real também pode levar a intervenções indevidas em assembleias pacíficas pelas forças de segurança.** Os efeitos negativos do uso de tecnologia de reconhecimento facial sobre o direito de reunião pacífica podem ser de amplo alcance [...]. Muitas pessoas se sentem desencorajadas a se manifestar em locais públicos e expressar livremente suas opiniões, quando temem ser identificadas e sofrer consequências negativas. (Tradução livre, grifos nossos)

[57] Para dar um exemplo, o Ministério do Interior na Índia, em fevereiro de 2020, prendeu 1100 pessoas que participaram de protestos pacíficos, identificando-as com o uso do reconhecimento facial. Ver India Today, Amit Shah on Delhi riots probe: 1100 people identified using face recognition tech, 300 came from UP (em inglês)

[58] Disponível em: https://digitallibrary.un.org/record/1640588

de informações que podem colocar em risco sua privacidade[59]. O mesmo relatório traz ainda **preocupações específicas sobre dados biométricos**, frente ao fato de que "alguns Estados estão embarcando em amplos projetos baseados em dados biométricos sem contar com as salvaguardas legais e procedimentais adequadas" (tradução livre). Exatamente o que se vê no caso trazido por esta ação.

Não por outra razão recente relatório do Conselho de Direitos Humanos da ONU especificamente alertou para os riscos que o reconhecimento facial traz para o direito à privacidade e para o direito à não-discriminação, dada a baixíssima acurácia destas tecnologias quando aplicadas a qualquer grupo que, resumidamente, não sejam homens brancos:

> Reconhecendo que, apesar de seus efeitos positivos, o uso de inteligência artificial que requer o processamento de grandes quantidades de dados, muitas vezes relacionados a dados pessoais, incluindo comportamento, relações sociais, preferências privadas e identidade de um indivíduo, pode representar sérios riscos para a direito à privacidade, em particular quando empregado para identificação, rastreamento, criação de perfil, reconhecimento facial, previsão de comportamento ou pontuação de indivíduos,
>
> Observando com preocupação relatos indicando menor precisão das tecnologias de reconhecimento facial com certos grupos, em particular indivíduos não brancos e mulheres, inclusive quando são usados dados de treinamento não representativos, que o uso de tecnologias digitais pode reproduzir, reforçar e até exacerbar a desigualdade racial, e neste contexto a importância de remédios eficazes,
>
> 6. Apela a todos os Estados:
>
> (a) Respeitar e proteger o direito à privacidade, inclusive no contexto das comunicações digitais e tecnologias digitais novas e emergentes;
>
> (b) Adotar medidas para acabar com as violações e abusos do direito à privacidade e criar as condições para prevenir tais violações e abusos, inclusive

[59] No mesmo sentido, a normativa europeia (GDPR) dispõe sobre os dados biométricos utilizados para fins de identificação como "dados de categoria especial". Dados como aqueles relacionados ao reconhecimento facial, portanto, considerados mais sensíveis e que necessitam de maior proteção. A mesma abordagem é adotada nas Normas de Proteção de Dados Pessoais para os Estados Ibero-Americanos[#] e pela LGPD, que os categoriza como dados sensíveis, demandando uma proteção mais rígida devido a seu potencial discriminatório. Quando se aborda reconhecimento facial, assim, é necessário que se leve em consideração que os dados envolvidos nesse tipo de sistema correm o risco de instrumentalização para discriminação racial, de gênero e político-ideológica, por exemplo.

> assegurando que a legislação nacional pertinente cumpra suas obrigações sob o direito internacional dos direitos humanos; (...)
>
> (e) Garantir que as tecnologias de identificação e reconhecimento biométrico, incluindo tecnologias de reconhecimento facial por atores públicos e privados, não permitam a vigilância arbitrária ou ilegal, inclusive daqueles que exercem seu direito à liberdade de reunião pacífica[60]. (tradução livre)

É um fato, público e notório, reconhecido nacional e internacionalmente: os sistemas de reconhecimento facial têm reforçado a discriminação racial e não foram criados ou pensados para reconhecer padrões que não sejam de homens brancos.

Em um país marcado e definido pelo racismo estrutural, a implementação destas tecnologias servirá ao propósito discriminatório.

4.5 A implementação do sistema de reconhecimento facial pela Ré Companhia do Metropolitano de São Paulo é incompatível com o direito à igualdade e à não discriminação

Conforme já demonstrado, o sistema de reconhecimento facial opera por meio da captura da imagem de pessoas através de câmeras digitais, sendo que a imagem capturada fornece o dado biométrico que contém as peculiaridades capazes de permitir a individualização e a identificação de uma pessoa.

Esse dado biométrico, transformado em uma representação numérica, é confrontado com um banco de dados (de pessoas desaparecidas, foragidos da justiça, pessoas com antecedentes criminais, por exemplo) possibilitando a verificação da semelhança ou diferença entre a imagem capturada e aquelas constantes de um determinado e específico banco de dados.

Há, contudo, vieses que operam no desenvolvimento da tecnologia de reconhecimento facial que resultam em distorções nos resultados apresentados por essa ferramenta, conforme traz, em sua essência, falsos positivos: todas as faces aproximadas a esta representação numérica apontarão como "reconhecimento positivo" pelo sistema.

O desenvolvimento desse tipo de tecnologia envolve a utilização massiva de dados para ensinar máquinas a identificar e classificar diferentes padrões. Em outras palavras: "as máquinas são ensinadas a realizar o reconhecimento facial a partir de exemplos que são oferecidos a respeito

[60] HRC, A/HRC/48/L.9/Rev.1, disponível em https://digitallibrary.un.org/record/3945627?ln=en

do que desejamos que elas aprendam a reconhecer. Assim, "se eu quero que uma máquina seja capaz de detectar um rosto, eu dou vários exemplos do que é rosto e do que não é rosto".[61] Ocorre que os dados utilizados para informar tais sistemas refletem vieses que resultam em resultados distorcidos.

Com efeito, os sistemas são compostos, prevalentemente, por dados de homens de pele clara e, consequentemente, não são familiarizados com rostos que não atendem a esse padrão. Os/as especialistas apontam que os algoritmos performam melhor com rostos masculinos do que com rostos femininos e com rostos claros do que com rostos escuros. Mesmo os melhores algoritmos possuem dificuldades em reconhecer corpos negros e corpos de pessoas que fizeram a transição de gênero.

Parte dessa distorção está atrelada ao fato de que o grupo que elabora e desenvolve essas tecnologias é extremamente restrito geograficamente e racialmente homogêneo, sendo composto por alguns poucos homens brancos atuantes em multinacionais que controlam o desenvolvimento dessas ferramentas tecnológicas, assim como a sua venda para o resto do mundo.[62]

Ocorre que as pessoas que compõem esse seleto grupo são pautadas, como todos nós, por vieses inconscientes. Mas o que são vieses inconscientes? Basicamente, são padrões mentais sistemáticos que guiam nossos pensamentos e atitudes de maneira inconsciente. Eles não se baseiam em julgamento racional a partir do cotejo das informações relevantes em uma dada situação concreta, mas são informados por fatores como educação, contexto familiar, cultura, religião e experiências pessoais pelas quais passamos[63]. Com base nesses elementos, construímos padrões de julgamento e tomamos decisões de forma automática e não consciente em relação a pessoas e situações.

Uma vez que a tecnologia de reconhecimento facial é desenvolvida por pessoas, suas escolhas acabam influenciando negativamente o aprendizado e aplicação dos algoritmos, pois refletem

[61] Documentário "Coded Bias" (2020) - Netflix.
[62] Disponível em https://www.thomasnet.com/articles/top-suppliers/ai-software-companies/
[63] O Prof. Adilson José Moreira descreve com precisão em que medida os vieses inconscientes informam as escolhas e decisões de atores institucionais: "Os conteúdos sociais presentes nos diferentes tipos de representações culturais de grupos sociais também motivam as reações inconscientes dos indivíduos, fazendo com que eles discriminem os outros, mesmo não estando conscientes disso. A discriminação inconsciente designa então aqueles atos que afetam o julgamento do agente de membros de outros grupos, sendo que o agente pode não estar ciente do que está fazendo. Um empregador pode tentar ser objetivo na sua avaliação da competência dos candidatos a um emprego, mas as falsas ideias sobre grupos podem fazer com que a sua decisão de empregar uma ou outra pessoa pode ser consequência da ação inconsciente de falsas percepções de grupos sociais (Lawrence III, 1986, p. 328 - 350)". MOREIRA, Adilson José. O que é discriminação? Belo Horizonte: Letramento: Casa do Direito: Justificando, 2017.

os preconceitos e opiniões hegemônicos em uma sociedade estruturada pelo racismo. Vale dizer: as máquinas são programadas por pessoas que, inevitavelmente, embutem nelas, consciente ou inconscientemente, todos os seus padrões mentais e estereótipos.

Note-se: não é que a estrutura matemática, em si, do algoritmo seja racista, mas os modelos de aprendizagem de máquinas utilizados no desenvolvimento do algoritmo incorporam vieses inconscientes que resultam em efeitos discriminatórios.

Reconhecido como uma consequência de enviesamento tecnológico, situação em que se percebe parcialidade em funções computacionais, o **racismo algorítmico** ocorre quando algoritmos discriminam imagens ou qualquer conteúdo digital de pessoas negras. O termo vem sendo empregado para abarcar situações em que se observa que a discriminação racial é praticada por meio de robôs e pode ser definido como:

> [...] distorções nas bases de dados de algoritmos que geram distorções nos resultados obtidos, sendo mais comuns os resultados de falso positivo em desfavor de pessoas negras que de pessoas brancas, criando situações de constrangimento e discriminação contra essa parcela da população que já é vítima de um racismo estrutural.[64]

Nenhum software de reconhecimento facial desenvolvido até agora oferece 100% de precisão; pelo contrário, a pouca acurácia coloca em xeque a eficácia para seu propósito, como já argumentado. Os erros e distorções inerentes ao emprego dessa tecnologia acometem, em virtude do racismo algorítmico, com maior frequência, pessoas negras. O mesmo erro é frequente para qualquer indivíduo que não seja homem e branco.

É sabido que a maioria dos sistemas de reconhecimento facial até agora existentes foi desenvolvida para lidar de forma binária e estereotipada com dois grupos, homens e mulheres, o que torna a tecnologia imprecisa e discriminatória em relação a outras expressões de gênero, como pessoas não binárias e trans.[65]

Nesse contexto, as tecnologias de reconhecimento facial operam na interconexão entre nome, sexo e dados biométricos (no caso dessa tecnologia em específico, a imagem do rosto) configurando deste modo uma política de massa de identificação civil, através dos velhos paradigmas de classificação das diferenças entre homens e mulheres.

---

[64] AMPARO, Thiago. Polícia algorítmica. Folha de São Paulo, São Paulo, 2020. Disponível em: https://www1.folha.uol.com.br/colunas/thiago-amparo/2020/01/policia-algoritmica.shtml.

Relatos de pessoas trans indicam que, mesmo quando a checagem de documentos é feita por humanos, sem a implementação dessas tecnologias, constantemente seus dados retornam como "falsos" quando buscam acessar serviços essenciais. Tal impasse tende a se acentuar à medida em que pessoas trans conseguirem realizar a retificação civil de nome e gênero em seus documentos pessoais[66].

Em outras palavras: a máquina replica o mundo como ele existe, não toma decisões éticas. Se continuarmos utilizando modelos de aprendizagem de máquina para replicar nosso mundo como ele é, não vamos progredir socialmente enquanto sociedade, muito pelo contrário.

Essa preocupação foi sublinhada pelo Comitê para a Eliminação da Discriminação Racial da ONU. No âmbito da Recomendação Geral n. 36[67], o CERD observou que o aumento do uso pelas forças policiais de algoritmos, inteligência artificial, reconhecimento facial e de outras tecnologias aumenta os riscos de aprofundamento do racismo, da discriminação racial, da xenofobia e consequentemente de violação de muitos direitos humanos. Segundo a membra do Comitê Verene Shepard explica: "Os dados históricos sobre prisões em um bairro determinado (que alimentam a inteligência artificial) podem refletir muito bem as práticas policiais preconceituosas" e, como consequência, "aumentam o risco de um excesso de presença policial que poderia levar a realizar mais prisões e, desse modo, criar um ciclo vicioso". Isto é: "Dados incorretos provocam maus resultados"[68].

Um exemplo: o banco de dados de imagens que venha a ser composto por um rol de pessoas foragidas pela justiça ou portadoras de antecedentes criminais vai compor parte do treinamento de inteligência artificial e vai refletir, necessariamente, um padrão histórico ainda vigente de perseguição e criminalização racialmente dirigidas a corpos negros.[69]

Assim, se as pessoas negras preponderam nas estatísticas de pessoas presas e encarceradas como resultado do racismo institucionalizado e estrutural, elas estarão sobrerepresentadas nos

---

[66] Estudo da Universidade do Colorado (EUA) de 2019, essa tecnologia erra mais em rostos de pessoas trans em comparação às cisgêneros (que se identificam com o sexo biológico atribuído no nascimento). Enquanto em mulheres cis a precisão foi de 98,3%, para trans o índice médio era de 87,3%. Entre homens, a diferença é maior: a precisão entre cisgêneros ficou em 97,6%, enquanto a média foi de 70,5% entre homens trans. Para pessoas não-binárias (que vão além do masculino-feminino), agêneros (quem se identifica como gênero neutro) e queer (que não correspondem a um padrão cis-heteronormativo), o sistema errou em todas as tentativas. Disponível em https://www.colorado.edu/today/2019/10/08/facial-recognition-software-has-gender-problem

[67] ACNUDH, Recomendação Geral 36, Comitê para a Eliminação da Discriminação Racial - CERD, disponível em https://acnudh.org/load/2020/12/CERD_C_GC_36_PORT_REV.pdf

[68] https://noticias.uol.com.br/ultimas-noticias/rfi/2020/11/26/especialistas-da-onu-advertem-sobre-vies-racista-em-algoritmos.htm

[69] FLAUZINA, Ana. Corpo negro caído no chão: o sistema penal e o projeto genocida do Estado brasileiro. Brado.2019

bancos de dados utilizados pelos softwares de reconhecimento pessoal (dos quais constem, por exemplo, pessoas com antecedentes criminais ou foragidas da justiça) e, consequentemente, estarão mais propensas a serem "alvo" desse sistema de reconhecimento facial, com todas as suas consequências prejudiciais, que vão desde erros de identificação (falsos positivos), passando pelo aumento da vigilância dirigida a corpos negros e, finalmente, estarão mais sujeitas ao emprego excessivo e arbitrário da violência, dentre outras violações de direitos humanos que vitimam pessoas que sejam previamente identificadas como "perigosas".

Em síntese, podemos dizer que: a) **há vieses inconscientes** que pautam o desenvolvimento dos algoritmos em que se baseiam as tecnologias de reconhecimento facial e que acabam distorcendo os seus resultados, isto é, aumentando as chances de erros, ou seja, de falsos positivos, em relação à população negra; b) a **filtragem ou perfilamento racial** que historicamente informa a atuação das forças de segurança é responsável por fazer com que os bancos de dados que continuamente alimentam o funcionamento da tecnologia de reconhecimento facial sejam compostos majoritariamente por pessoas negras, fomentando maior perseguição a pessoas negras, por meio dessas ferramentas tecnológicas, em um círculo vicioso de reprodução e agravamento do racismo.

O perfil racial como uma tática adotada por supostas razões de segurança pública motivada por estereótipos baseados em raça, cor, etnia, língua, descendência, religião, nacionalidade ou local de nascimento, ou uma combinação desses fatores, em vez de suspeitas objetivas, tende a destacar indivíduos ou grupos de forma discriminatória com base na suposição errônea de que pessoas com tais características são propensas a incorrerem em tipos específicos de crimes.[70]

O CERD destaca que a filtragem racial ou perfilamento racial está atrelado a estereótipos e vieses, que podem ser conscientes ou inconscientes, individuais, institucionais ou estruturais, sendo que essas suposições estereotipadas a respeito de pessoas que integram grupos raciais historicamente discriminados produzem um impacto negativo no gozo de direitos civis e políticos, incluindo os direitos à vida (artigo 6º do Pacto Internacional sobre Direitos Civis e Políticos), liberdade e segurança da pessoa (art. 9), privacidade (art. 17), liberdade de movimento (art. 12), liberdade de associação (art. 22) e um remédio efetivo (art. 2 (3)).

Especificamente quanto ao uso crescente de novas ferramentas tecnológicas, incluindo a tomada de decisões algorítmicas e a inteligência artificial, não apenas em áreas como segurança

[70] Recomendação Geral 36/2020 do Comitê para a Eliminação da Discriminação Racial da ONU - CERD, disponível em https://acnudh.org/load/2020/12/CERD_C_GC_36_PORT_REV.pdf

e controle de fronteiras, mas também no tocante ao **acesso a serviços sociais**, o CERD sublinhou o seu potencial de aprofundar o racismo, a discriminação racial, a xenofobia e outras formas de exclusão.[71]

Outrossim, o CERD registra: "a opacidade da análise algorítmica e da tomada de decisões, em particular quando os métodos de inteligência artificial são empregados. Assim, os resultados discriminatórios do perfil algorítmico podem muitas vezes ser menos óbvios e mais difíceis de detectar do que os das decisões humanas e, portanto, mais difíceis de contestar. Além disso, os defensores dos direitos humanos geralmente não estão adequadamente equipados tecnologicamente para identificar tais métodos discriminatórios (para. 34)".

Esse aspecto é extremamente preocupante, pois há erros no funcionamento desses algoritmos que nem mesmo os desenvolvedores e programadores são capazes de prever ou explicar, indicando, portanto, e mais uma vez, que a falibilidade é inerente à tecnologia. Consequentemente, muitas empresas adotam sistemas de inteligência artificial apenas cientes das suas finalidades, mas não do processo que fundamenta o funcionamento desses sistemas. Dessa maneira, **resta inviável garantir que essa tecnologia produza um resultado justo**, se não há, nem por parte dos programadores, total compreensão acerca da maneira pela qual esses algoritmos funcionam.

A nossa preocupação reside em que padrões de filtragem ou perfilamento racial que têm sido debatidos amplamente e combatidos na atuação das forças de segurança correm o risco de serem retomados sob o manto da neutralidade da Inteligência artificial, o que significaria um retrocesso democrático imensurável.

Não é demais lembrar que as falhas do reconhecimento pessoal, sem uso de inteligência artificial, já são amplamente documentadas pela literatura jurídica, notadamente quando o reconhecimento é realizado por meio fotográfico. Da mesma forma, vem sendo demonstrado que os equívocos de reconhecimento vitimam preferencialmente pessoas negras. Em levantamento recente da Defensoria Pública do Rio de Janeiro e do Colégio Nacional de Defensores Públicos Gerais (CONDEGE), concluiu-se que 83% dos presos injustamente por reconhecimento fotográfico no Brasil são negros.[72]

[71] Recomendação Geral 36/2020 do CERD

[72] Disponível em http://condege.org.br/2021/04/19/relatorios-indicam-prisoes-injustas-apos-reconhecimento-fotografico/

Neste contexto, há recente julgado da 6ª Turma do STJ, que concluiu que a inobservância do procedimento descrito no art. 226 do CPP torna inválido o reconhecimento da pessoa suspeita e fixou o entendimento de que o reconhecimento do suspeito por simples exibição de fotografia(s) ao reconhecedor, a par de dever seguir o mesmo procedimento do reconhecimento pessoal, há de ser visto como etapa antecedente a eventual reconhecimento pessoal e, portanto, não pode servir como prova em ação penal, ainda que confirmado em juízo. (STJ. 6ª Turma. HC 598.886-SC, Rel. Min. Rogerio Schietti Cruz, julgado em 27/10/2020).

Isso implica reconhecer que a discriminação ocorre não apenas quando há intenção deliberada de tratar de maneira diferenciada e injustificada um determinado indivíduo ou grupo de pessoas, mas também por meio de práticas aparentemente neutras das instituições que acabam impactando desproporcionalmente o gozo de liberdades fundamentais por determinados grupos racializados.

A Lei Geral de Proteção de Dados estabelece que tratamento de dados pessoais, inclusive nos meios digitais, deve ter como fundamento o respeito aos direitos humanos, a dignidade e o exercício da cidadania pelas pessoas naturais (art. 2º), sendo que a atividade de tratamento de dados pessoais deve observar o princípio da não discriminação (art. 6), do que decorre a **impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos**.

A discriminação sistêmica ou estrutural ocorre "quando a acumulação de desvantagens sociais causadas por diversas formas de discriminação concorrem para a estratificação, o que coloca certos grupos em uma situação de subordinação DURÁVEL ou PERMANENTE."[73] Ísis Conceição, comentando sobre o conceito de racismo estrutural pontua:

> "Os recentes esforços de definição da categoria e ferramenta, utilizada em relatórios da ONU, têm sido no sentido de apresentar o racismo estrutural como um sistema no qual políticas públicas, práticas institucionais, representações culturais e outras normas funcionam de várias formas, frequentemente reforçando maneiras de perpetuação de desigualdade de um grupo, ou como a normalizada e legitimada ampla gama de políticas, práticas e atitudes que rotineiramente produzem cumulativos e crônicos resultados adversos para as pessoas não brancas (...) ou como uma prática coletiva que existe em ambientes

[73] MOREIRA, Adilson José, O que é discriminação?

> de trabalho e na sociedade manifestando-se na forma de atitudes, comportamentos, ações e processos."[74]

Diante dos elementos fáticos e jurídicos expostos, a implementação da tecnologia de reconhecimento facial, na prática, produzirá impactos negativos desproporcionais para a população negra em razão do enviesamento racial inerente ao uso dessa tecnologia, assim como para as pessoas transgênero, independentemente das boas intenções que eventualmente norteiem a adoção desta tecnologia pelos gestores da Companhia Metropolitana de São Paulo, contribuindo para reprodução e até aprofundamento da marginalização social historicamente imposta a esse grupo.

5. Pedidos

5.1 As violações de direitos pela Ré acarretaram dano moral coletivo

Os fatos narrados denotam que potencialmente milhões de usuários do metrô já tiveram seus dados captados e utilizados sem seus consentimentos específicos, sem identificação da finalidade e do modo de uso. Ainda, os dados tratados foram dados pessoais biométricos, que não comportam substituição após uma exposição indevida ou um vazamento. Esse notório abuso perpetrado pela ré é causador de dano moral coletivo:

> "O dano extrapatrimonial coletivo prescinde da comprovação de dor, de sofrimento e de abalo psicológico, suscetíveis de apreciação na esfera do indivíduo, mas inaplicável aos interesses difusos e coletivos" (REsp n. 1.410.698/MG, Rel. Ministro Humberto Martins, Segunda Turma, DJe 30/6/2015).

O dano moral coletivo atinge direitos de personalidade do grupo ou coletividade como realidade massificada, que a cada dia reclama mais soluções administrativas, legislativas e jurídicas para sua proteção. Isso não importa exigir da coletividade "dor, repulsa, indignação tal qual fosse um indivíduo isolado, pois a avaliação que se faz é simplesmente objetiva, e não personalizada, tal qual no manuseio judicial da boa-fé objetiva. Na noção inclui-se tanto o dano moral coletivo indivisível (por ofensa a interesses difusos e coletivos de uma comunidade) como o divisível (por afronta a interesses individuais homogêneos)" (REsp n. 1.574.350/SC, Rel. Ministro Herman Benjamin, Segunda Turma, julgado em 3/10/2017, DJe 6/3/2019). Nesse

[74] CONCEIÇÃO, 2020, "Racismo e pandemia uma análise jurídica: dimensões de justiça e suas interseções", Revista UERJ, p. 16

sentido também o precedente desta Segunda Turma: REsp n. 1.057.274, Segunda Turma, Rel. Ministra Eliana Calmon, Dje 26/2/2010." (STJ - AgInt no AREsp 1.413.621/MG – Segunda Turma – Rel. Francisco Falcão – Julgado em 06.05.2020 – DJe 11.05.2020).

A proteção de dados pessoais é a nova fronteira da garantia da privacidade como um anteparo do indivíduo contra o Estado e, hoje, também contra as grandes conglomerações. **O tratamento ilegal ou irregular de dados é ato ilícito**, nos termos do artigo 44 da LGPD. Tais fatos não podem passar ilesos, ainda mais diante de uma lei que já vige há algum tempo e esclarece exatamente como se deve garantir a proteção de dados pessoais, como é a LGPD.

A LGPD prevê especificamente que o controlador de dados - no caso, a ré - que causar danos ao titular é obrigado a repará-lo, reconhecendo a possibilidade da tutela coletiva dos direitos, nos termos do artigo 42, §3º da LGPD:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> §3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

O metrô conta com 4 milhões de usuários por dia. Imaginando um valor irrisório de R$ 1.000,00 (hum mil reais) de reparação para usuários cujos dados já estão sendo tratados de forma ilegal e irregular há meses, já se teria um valor de 4 bilhões de indenização, o que certamente extrapolará a capacidade da ré em pagar a verba indenizatória.

Por isso, as autoras apresentam como parâmetro de indenização para esta ação o valor contratado pela ré para implementação do sistema de reconhecimento facial através do Sistema de Monitoração Eletrônica – SME Etapa 3, resultante do processo licitatório LPI nº 10014557: R$ 42.798.438,63 (quarenta e dois milhões, setecentos e noventa e oito mil quatrocentos e trinta e oito reais e sessenta e três centavos). Ainda mais levando-se em conta que tal contratação se deu no período de vacância da LGPD, destinado justamente a à adequação dos agentes públicos e privados aos seus termos.

5.2 Pedido de tutela provisória de urgência

Presentes os requisitos do art. 300 do CPC, deve-se, desde logo, conceder-se a tutela provisória de urgência, para impedir qualquer possibilidade de que o tempo corroa o resultado útil do processo. A probabilidade do direito está amplamente demonstrada ao longo desta petição inicial. O risco ao resultado útil do processo, por seu turno, também está clarificado pela urgência que decorre da necessidade de impedir que a ré continue a realizar o reconhecimento facial dos seus usuários ou mesmo apenas captar esses dados pessoais. **O dano já aconteceu, está acontecendo e continuará a acontecer caso não seja concedida a medida liminar ora pleiteada**.

O resultado útil do processo só será assegurado caso alguma medida judicial produza eficácia desde logo, posto que aguardar o trânsito em julgado, no caso presente, seria o mesmo que negar acesso ao Judiciário, vez que até lá certamente já terá havido o tratamento de dados pessoais biométricos ilegal de milhões de usuários do metrô.

É de se destacar, ainda, que a lesão aos direitos dos usuários pode ser irreparável, na medida que, conforme foi demonstrado ao longo da petição, os dados já estão sendo tratados e, como não há qualquer protocolo quanto ao consentimento da obtenção desses dados e quanto à finalidade, a violação já está posta, lembrando-se que os dados do reconhecimento fotográfico são insubstituíveis, ou seja, uma vez expostos, não podem ser trocados, como medida de segurança, como se faz com uma senha, por exemplo.

A segurança da titularidade de dados pessoais, garantindo os direitos fundamentais de liberdade, intimidade e privacidade (art. 17 da LGPD) foi corrompida, visto que não estão sendo informados sobre a captação e tratamento de dados, tampouco o propósito da colheita destes.

A demora não desejada, mas esperada, pelo provimento final, imporá que a população tenha seus dados pessoais expostos, sem seu conhecimento ou anuência, em perfeita afronta à legislação de proteção de dados pessoais.

Com efeito, o perigo de dano e a probabilidade do direito estão sobejamente demonstrados, preenchendo, portanto, os requisitos para a tutela provisória, nos termos do artigo 300 do Código de Processo Civil, sem prejuízo de medidas outras que visem o resultado prático equivalente.

O risco é evidente já que a utilização de sistema de reconhecimento facial, tratamento de dados sensíveis e proteção dados de hipervulneráveis, sem o seu consentimento, tampouco sem a previsão de agentes de tratamento de dados pessoais, irrompe a proteção prevista pela LGPD.

Ademais, não há qualquer risco para o Metrô, uma vez que a suspensão da captação e tratamento de dados biométricos para reconhecimento facial no âmbito da implementação do Sistema de Monitoração Eletrônica – SME Etapa 3, não está relacionado com os objetivos da Ré, sua interrupção não acarretará prejuízos para a operação ou impedirá a realização dos serviços de transporte prestados aos usuários.

5.3 Dos pedidos especificados

Ante o exposto, **a DEFENSORIA PÚBLICA DO ESTADO DE SÃO PAULO, a DEFENSORIA PÚBLICA DA UNIÃO, o IDEC, a INTERVOZES e a ARTIGO 19 BRASIL** requerem:

a.1) liminarmente, seja determinada à **Companhia do Metropolitano de São Paulo** a imediata suspensão da captação e tratamento de dados biométricos para reconhecimento facial no âmbito da implementação do Sistema de Monitoração Eletrônica – SME Etapa 3, resultante do processo licitatório LPI nº 10014557, estabelecendo multa diária na hipótese de descumprimento;

a.2) liminarmente, seja determinada à **Companhia do Metropolitano de São Paulo** a imediata suspensão da instalação de novos equipamentos que promovem captura e tratamento de dados biométricos para reconhecimento facial, no âmbito do Sistema de Monitoração Eletrônica – SME Etapa 3, resultante do processo licitatório LPI nº 10014557, estabelecendo multa diária na hipótese de descumprimento;

a.3) liminarmente, seja determinada à **Companhia do Metropolitano de São Paulo** obrigação de não fazer, consistente em deixar de adotar qualquer sistema de captação e tratamento de dados biométricos dos usuários de metrô para sua utilização em sistemas de reconhecimento facial, até o trânsito em julgado da presente demanda, estabelecendo multa diária na hipótese de descumprimento;

b) sejam convolados em definitivos os provimentos liminares requeridos;

c) no mérito, seja a **Companhia do Metropolitano de São Paulo** condenada a abster-se de usar qualquer mecanismo ou sistema de captação de dados biométricos para reconhecimento facial dos usuários do metrô no âmbito das suas estações, composições, vagões e quaisquer instalações adjacentes onde haja circulação de usuários, em dependências sob supervisão da **Companhia do Metropolitano de São Paulo**;

d) no caso de ser permitido à **Companhia do Metropolitano de São Paulo** a utilização de algum sistema de captação e tratamento de dados biométricos para reconhecimento facial dos usuários, requerem os autores, de forma **subsidiária e necessariamente cumulativa:**

d.1) seja determinado à ré a obtenção do consentimento específico, livre, informado e inequívoco dos usuários do metrô para o uso de seus dados pessoais, individualmente e por escrito, em documento no qual conste claramente as finalidades e o uso que se darão para os dados, que seja dissociado do contrato de adesão normalmente utilizado, e que contenha expressamente as formas gratuitas para a revogação do consentimento do usuário a qualquer tempo, nos termos dos artigos 6º, 7º, I e 8º da LGPD;

d.2) seja determinado à ré que apresente protocolo sobre como será programada a taxa de sensibilidade do sistema e como isso afetará a incidência de falsos negativos e ou falsos positivos, apresentando documentos que comprovem que o sistema não apresenta vieses potencialmente discriminatórios em relação a gênero, raça, etnia, cor da pele, idade ou quaisquer outras características que possam influenciar o reconhecimento fenotípico, apresentando-se avaliação de impacto e plano de mitigação de riscos, antes do início do processo de captação, nos termos dos artigos 2º, 6º, 9º, 18, 19, 42 e 50, §2º, I, d da LGPD e 5º caput, X, XLI, LXXII, e LIV da CRFB;

d.3) seja determinado à ré que se abstenha de compartilhar seu banco de dados com terceiros e que se abstenha de utilizar-se de bancos de dados de terceiros, nos termos do artigo 7º, §5º da LGPD;

d.4) seja determinado à ré que se abstenha de captação de dados biométricos para reconhecimento facial, em quaisquer circunstâncias, de crianças e adolescentes, nos termos do artigo 6º do ECA e 227 da CRFB; **subsidiariamente**, que seja adotado o procedimento do art. 14, § 1º, da LGPD;

d.5) seja determinado à ré que se abstenha de impedir o acesso dos usuários que, por qualquer motivo, deixem de permitir a captação e o tratamento de dados biométricos para reconhecimento facial, já que isto não é essencial para a prestação do serviço de transporte que oferece a ré, nos termos do artigo 7º, III da LGPD;

e) seja a Companhia do Metropolitano de São Paulo condenada a pagar indenização por danos morais coletivos, em valor não inferior a R$ 42.798.438,63 (quarenta e dois milhões, setecentos e noventa e oito mil quatrocentos e trinta e oito

reais e sessenta e três centavos) ante o tratamento, até o momento, de dados biométricos de milhões de usuários do metrô, sem seus consentimentos específicos, sem identificação da finalidade e do modo de uso, devendo-se a condenação ser revertida para o financiamento de projetos voltados à proteção de dados pessoais de usuários de serviços públicos, nos termos do artigo 42, §3º, 44 e 45 da LGPD;

f) a citação da ré para que, querendo, possa defender-se;

g) o acolhimento das provas produzidas no âmbito de ação autônoma de produção de provas e produção de outras por todos os meios admitidos, sem prejuízo de que, no curso da instrução, seja concedida inversão do ônus da prova, nos termos do art. 6º, inciso VIII do CDC, dada a vulnerabilidade do consumidor e a verossimilhança das alegações;

h) a condenação da ré nos ônus sucumbenciais;

i) a intimação do Ministério Público, nos termos do art. 5º, § 1º, da L. 7.347/85;

j) conforme determina o art. 319, inciso VII do CPC, vêm as Autoras informar que não têm interesse na audiência de conciliação (art. 334, caput do CPC).

Dá-se a causa o valor de R$ 42.798.438,63 (quarenta e dois milhões, setecentos e noventa e oito mil quatrocentos e trinta e oito reais e sessenta e três centavos).

São Paulo, 03 de março de 2022.

Eloísa Machado de Almeida
OAB/SP 201.790
Advogada do CADHu e Intervozes

Estela Waksberg Guerrini
Defensora Pública do Estado de São Paulo
Núcleo Especializado de Defesa do Consumidor

Luiz Fernando Baby Miranda
Defensor Público do Estado de São Paulo

Núcleo Especializado de Defesa do Consumidor

Davi Quintanilha Failde de Azevedo
Defensor Público do Estado de São Paulo
Núcleo Especializado de Cidadania e Direitos Humanos

Letícia Marquez de Avelar
Defensora Pública do Estado de São Paulo
Núcleo Especializado de Cidadania e Direitos Humanos

Fernanda Penteado Balera
Defensora Pública do Estado de São Paulo
Núcleo Especializado de Cidadania e Direitos Humanos

Isadora Brandão Araujo da Silva
Defensora Pública do Estado de São Paulo
Núcleo Especializado de Defesa da Diversidade e da Igualdade Racial

Vinicius Conceição Silva Silva
Defensor Público do Estado de São Paulo
Núcleo Especializado de Defesa da Diversidade e da Igualdade Racial

Daniel Palotti Secco
Defensor Público do Estado de São Paulo
Núcleo Especializado de Infância e Juventude

Gustavo Samuel da Silva Santos
Defensor Público do Estado de São Paulo
Núcleo Especializado de Infância e Juventude

João Paulo de Campos Dorini
Defensor Público Federal
Defensoria Regional de Direitos Humanos em São Paulo

Christian Tárik Printes

OAB/SP 316.680

Advogado do Idec

Sheila Santana de Carvalho

OAB/SP 343.588

Advogada da Artigo 19 Brasil

Raquel da Cruz Lima

OAB/SP 331.949

Advogada da Artigo 19 Brasil

Flávia Lefèvre Guimarães

OAB/SP 124.443

Advogada do Intervozes

LISTA DE DOCUMENTOS:

1. Documento 01 - Estatuto social, Ata da Assembleia, Termo de Posse do Conselho Diretor, Ato de nomeação da coordenadora executiva e Procuração do Idec

2. Documento 02 – Estatuto Social, Ata e Procuração do Intervozes

3. Documento 03 - Estatuto social, Ata e Procuração da Artigo 19

4. Documento 04 – Ação Cautelar de Produção Antecipada de Provas

5. Documento 05 – Parecer coordenado pelo Prof. Roberto Hirata Jr., professor livre-docente do departamento de Ciência da Computação do Instituto de Matemática e Estatística da Universidade de São Paulo (IME-USP)