Universidade de Brasília - UnB
Faculdade de Direito

Shana Schlottfeldt Santos

TECNOLOGIA DE RECONHECIMENTO FACIAL À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS: RISCOS E DESAFIOS

Brasília
2021

Universidade de Brasília - UnB
Faculdade de Direito

Shana Schlottfeldt Santos

TECNOLOGIA DE RECONHECIMENTO FACIAL À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS: RISCOS E DESAFIOS

Monografia de conclusão de curso apresentada como requisito parcial para a obtenção do título de bacharel em Direito pela Faculdade de Direito da Universidade de Brasília – UnB.

Orientadora: Profa. Dra. Daniela Marques de Moraes.

Coorientadora: Profa. Dra. Laura Schertel Ferreira Mendes.

Brasília
2021

TERMO DE APROVAÇÃO

Shana Schlottfeldt Santos

Tecnologia de Reconhecimento Facial à luz da Lei Geral de Proteção de Dados: riscos e desafios

Trabalho de conclusão de curso aprovado em 21 de outubro de 2021 como requisito parcial para obtenção do grau de bacharel perante a Faculdade de Direito da Universidade de Brasília, pela seguinte banca examinadora:

_____
Professora Doutora Daniela Marques de Moraes – FD/UnB (Orientadora)

_____
Professora Doutora Laura Schertel Ferreira Mendes – FD/UnB (Coorientadora)

_____
Professora Doutora Ana de Oliveira Frazão – FD/UnB

_____
Professor Doutor João Pedro Leite Barros – FD/UnB

Brasília, 21 de outubro de 2021.

AGRADECIMENTOS

Agradeço a minha Orientadora Profa. Dra. Daniela Marques de Moraes e a minha Coorientadora Profa. Dra. Laura Schertel Ferreira Mendes pela coragem de aceitar esse desafio junto comigo, por tudo o que a agudeza e precisão que seus pensamentos provocam, pelo exemplo profissional e humano, por serem faróis que me guiaram a um porto seguro, pela profunda atenção e dedicação com as quais me acompanharam durante a elaboração desta monografia! Vocês são simplesmente incríveis!

Aos professores com que tive a hora de escrever e/ou publicar artigos:

- Profa. Dra. Renata Queiroz Dutra (Direito Coletivo do Trabalho), pela força e doçura com que defende seus posicionamentos.
- Prof. Dr. Alexandre Araújo Costa (Teoria Geral do Estado e Filosofia do Direito), pelas discussões instigantes, no melhor estilo socrático.
- Prof. Dr. Reynaldo Soares da Fonseca (Direito Processual Penal 2), pela generosidade com que compartilhou seu vasto conhecimento. O Sr. representa a própria personificação da "fraternidade"!

Mas também a todos aqueles que me inspiraram a fazê-lo ao longo de minha jornada acadêmica no Direito.

Aos professores de quem tive o prazer de ser monitora:

- Prof. Dr. Vallisney de Souza Oliveira (Teoria Geral do Processo 2) por seu comprometimento e simpatia sem iguais.
- Prof. Dr. Airton Lisle Cerqueira Leite Seelaender (História do Direito) que me ensinou que o Direito é a história das disputas de poder. O Sr. é um verdadeiro "contador de histórias" no melhor sentido da expressão!
- Prof. Dr. Jorge Octávio Lavocat Galvão (Direito Constitucional 2) pela competência e profissionalismo se par.

Aos professores da *Australian National University* (ANU), que me acolheram tão bem durante meu intercâmbio acadêmico na Austrália, a quem me dou a liberdade de me dirigir em seu idioma:

- Prof. Dr. Daniel Stewart (Information Law), for instigating my initial curiosity and interest for data protection. You started all this!
- Prof. Dr. Surendra Dayal (Legislative Drafting) for all your brilliance and for showing me how intertwined with technology the Law is. You also played an important role in this work!
- Prof. Dr. Desmond Manderson and Prof. Dr. Timothy Bonyhady (Law and Art) for introducing me to a flourishing new area of interdisciplinary study, in a process that allowed me to see both, law and art, through different eyes, transforming forever what they mean to me.

- Prof. Dr. Michelle Worthington (Foundations of Australian Law), for teaching a civil law student how amazing, dynamic, and inspiring the common law can be.

Thank you all for sharing so much! For being so supportive and gentle! For showing me how amazing the Aussie culture is and how challenging and interesting the Australian Law can be! Thank you for making me fell so welcome! You are the best!

Aos colegas do Observatório da LGPD-UnB (do qual faço parte desde sua fundação, no 1º semestre de 2020) e do Anuário da LGPD-UnB pelas discussões enriquecedoras, provocativas e apaixonantes!

Na figura da Profa. Dra. Ana de Oliveira Frazão e do Prof. Dr. João Pedro Leite Barros, cujas estrelas brilham com tamanha intensidade e que tão gentilmente aceitaram participar da banca de defesa desta monografia de final de curso, agradeço a todos os fantásticos professores da Universidade de Brasília, de quem tive a oportunidade de ser aluna, que ajudaram a forjar a acadêmica que me tornei e são exemplos da profissional do Direito que desejo me tornar.

Igualmente, na figura da querida amiga, Elaine Sampaio Barros, agradeço aos amigos que fiz ao longo dessa jornada. Que nosso futuro seja repleto de sucessos e que nossos caminhos se cruzem muitas e muitas vezes mais!

Por fim, aos meus pais e irmão, as figuras mais importantes nesta conquista, agradeço pelo respeito e apoio incondicionais, pelo estímulo e pelas palavras de incentivo com que me cercam todos os dias, obrigada pelo amor que nos une e pela paciência e compreensão das horas que não passamos juntos. Amo vocês!

“A teletela recebia e transmitia simultaneamente. [...] enquanto Winston permanecesse no campo de visão enquadrado pela placa de metal, além de ouvido também poderia ser visto. Claro, não havia como saber se você estava sendo observado num momento específico. Tentar adivinhar o sistema utilizado pela Polícia das Ideias para conectar-se a cada aparelho individual ou a frequência com que o fazia não passava de especulação. Era possível inclusive que ela controlasse todo mundo o tempo todo. Fosse como fosse, uma coisa era certa: tinha meios de conectar-se a seu aparelho sempre que quisesse. Você era obrigado a viver — e vivia, em decorrência do hábito transformado em instinto — acreditando que todo som que fizesse seria ouvido e, se a escuridão não fosse completa, todo movimento examinado meticulosamente.” (1984, George Orwell).

RESUMO

O uso da biometria aumentou significativamente nos últimos anos. Isso é verdade não apenas para o setor público, mas para o privado; não só na área de segurança, mas também no comércio, no trabalho e outros domínios da vida. Ao mesmo tempo que o emprego da tecnologia de reconhecimento facial (FRT) vem acompanhado do discurso de benefícios, eficiência, comodidade e conveniência, ele carrega consigo, também, muitas dúvidas e controvérsias, em especial associadas a uma perda gradual de privacidade e do direito à proteção de dados. Este estudo busca discutir as possibilidades, riscos e desafios do uso da FRT à luz da Lei Geral de Proteção de Dados (LGPD), em especial na sua intersecção com a vigilância em massa e espaços públicos. Este estudo possui natureza qualitativa e foi desenvolvido por meio de pesquisa bibliográfica. São apresentados os conceitos básicos associados à FRT, essenciais à construção da base teórica de argumentação. É abordada a maneira como a FRT, ao efetuar tratamento de dados pessoais sensíveis, aciona a incidência da LGPD. Por fim, de posse de todo referencial teórico, é apresentado como estudo de caso o "Caso do Metrô de São Paulo" onde se observa, na prática, a articulação dos conhecimentos previamente adquiridos quanto à FRT e à aplicação da LGPD. O caso é pioneiro e paradigmático no âmbito da proteção de dados pessoais, coordenando temáticas de utilização de FRT; processamento automatizado em larga escala; coleta de dados em local público; obrigações relativas à transparência, informação, segurança e não discriminação. Como contribuições específicas deste trabalho tem-se: (i) a distinção entre videovigilância (pura e simples) e a videovigilância associada à FRT; (ii) a argumentação que a FRT trata dados pessoais sensíveis (atraindo, portanto, todas as salvaguardas associadas a esse tipo especial de dados); (iii) o consentimento, geralmente, não se constitui em base legal válida (ou, pelo menos, não seria a mais adequada) para embasar a utilização de FRT em espaços públicos, fazendo-se necessário o enquadramento em uma das sete hipóteses previstas no art. 11, II da LGPD; (iv) o uso de FRT traz consigo a possibilidade do exercício do direito de revisão das decisões automatizadas; (v) o uso da FRT acarretaria a necessidade de elaboração de relatório de impacto à proteção de dados pessoais (RIPD).

Palavras-chave: Proteção de Dados Pessoais. Reconhecimento Facial. Tecnologia de Reconhecimento Facial. FRT. Lei Geral de Proteção de Dados. LGPD. Biometria. Dados Pessoais Sensíveis. Videovigilância.

ABSTRACT

The use of biometrics has increased significantly in recent years. This is true not just for the public sector, but for the private sector; not only in security, but also in commerce, labor, and other areas of life. While the use of facial recognition technology (FRT) is accompanied by the discourse of benefits, efficiency, and convenience, it also carries with it many doubts and controversies, especially associated with a gradual loss of privacy and of rights to data protection. This study aims to discuss the possibilities, risks and challenges of using FRT in the light of the General Data Protection Act (LGPD), especially in its intersection with mass surveillance and public spaces. This is a qualitative study and was developed through bibliographical research. We present the basic concepts associated with FRT in order to construct the theoretical basis of argumentation. We discuss the way in which FRT, by processing special categories of personal data, triggers the incidence of LGPD. Finally, we present as a case study the "Case of São Paulo's Subway", where we observe, in practice, the articulation of previously acquired knowledge regarding FRT and the LGPD application. The case is pioneering and paradigmatic in the field of personal data protection, coordinating themes related to the use of FRT; large-scale automated processing; data collection in a public place; obligations relating to transparency, information, security, and non-discrimination. The specific contributions of this work are: (i) the distinction between video surveillance and video surveillance associated with FRT; (ii) the argument that FRT handles a special category of personal data (thus attracting all the safeguards associated with this special type of data); (iii) consent, in general, does not constitute a legal basis (or, at least, it would not be the most adequate one) to support the use of FRT in public spaces, making it necessary to fit into one of the seven hypotheses provided by art. 11, II of LGPD; (iv) the use of FRT brings with it the possibility of exercising the right to review automated decisions; (v) the use of FRT would imply the need of a Data Protection Impact Assessment.

Keywords: Personal Data Protection. Facial recognition. Facial recognition technology. FRT. General Data Protection Regulation. GDPR. Privacy Act. Biometrics. Special categories of personal data. Videosurveillance

Lista de siglas e abreviações

AABIS - *Afghan Automatic Biometric Identification System* (Sistema de Identificação Biométrica Automática Afegão)
Abin - Agência Brasileira de Inteligência
ABNT - Associação Brasileira de Normas Técnicas
ACLU - *American Civil Liberties Union*
ADI - Ação Direta de Inconstitucionalidade
ADPF - Arguição de Descumprimento de Preceito Fundamental
AFR - *automatic facial recognition technology* (tecnologia de reconhecimento facial automático)
ANPD - Autoridade Nacional de Proteção de Dados
ANPR - *Automatic Number Plate Recognition* (reconhecimento automático de número de placa)
APD - Autoridades de Proteção de Dados
BIPA - [*Illinois*] *Biometric Information Privacy Act*
BWV - *body worn video* (vídeo usado no corpo)
CC - Código Civil (Lei nº 10.406/2002)
CCJR - Comissão de Constituição, Justiça e Redação
CCO - Centro de Controle Operacional
CCTV - *closed circuit television* (circuito fechado de televisão, CFTV)
CDC - Código de Defesa do Consumidor (Lei nº 8.078/1990)
CEO - *Chief Executive Officer* (Diretor Executivo)
CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CF - Constituição Federal de 1988
CFTV - circuito fechado de televisão (*closed circuit television*, CCTV)
CGI.br - Comitê Gestor da Internet no Brasil
CJEU - *Court of Justice of the European Union* (Tribunal de Justiça da União Europeia)
CNH - Carteira Nacional de Habilitação
Convention 108+ - *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data* (Convenção Modernizada para a Proteção de Indivíduos com Relação ao Processamento de Dados Pessoais, Convenção 108+)
Covid-19 - *corona virus disease-2019* (doença do coronavírus de 2019, ano em que os primeiros casos foram reportados)
CPF - Cadastro de Pessoa Física
CPTM - Companhia Paulista de Trens Metropolitanos
CSIRT - *Computer Security Incident Response Team* (Grupo de Resposta a Incidentes de Segurança)
DataPrev - Empresa de Tecnologia e Informações da Previdência
DoD - *US Department of Defense* (Departamento de Defesa dos Estados Unidos da América)
DPIA - *Data Protection Impact Assessment*
DPSP - Defensoria Pública do Estado de São Paulo
EDPB - *European Data Protection Board* (Conselho Europeu de Proteção de Dados)
EDPS - *European Data Protection Supervisor* (Autoridade Europeia para a Proteção de Dados)

EDRi - *European Digital Rights*
EFS - *UK Eurofins Forensics Services*
e.g. - *exempli gratia* (expressão latina que significa "por exemplo" ou "para fins de exemplo")
EUA - Estados Unidos da América
FAR - *false accept rate* ("taxa de aceitação falsa" ou "falso positivo")
FDD - Fundo de Defesa de Direitos Difusos
FER - *facial emotion recognition* (reconhecimento facial de emoções)
FLoCs - *Federated Learning of Cohorts*
FRR - *false reject rate* ("taxa de rejeição falsa" ou "falso negativo")
FRT- *facial recognition technology* (tecnologia de reconhecimento facial)
GDPR - *General Data Protection Regulation* (Regulamento Geral sobre a Proteção de Dados, RGPD) (Regulamento (UE) 2016/679)
GVM - *gangs violence matrix*
HD - *high definition* (alta definição)
IA - Inteligência Artificial
IBGE - Instituto Brasileiro de Geografia e Estatística
IBP - Instituto Brasileiro de Peritos
ICL - *Imperial College London*
ICO - *Information Commissioner's Office*
IDEC - Instituto Brasileiro de Defesa do Consumidor
i.e. - *id est* (expressão latina que significa "isto é", "ou seja" ou "em outras palavras")
IEC - *International Electrotechnical Commission* (Comissão Eletrotécnica Internacional)
Inmetro - Instituto Nacional de Metrologia, Qualidade e Tecnologia
INSS - Instituto Nacional do Seguro Social
IoT - *Internet of Things* (Internet das Coisas)
IRIS - Instituto de Referência em Internet e Sociedade
ISO - *International Organization for Standardization* (Organização Internacional para Padronização)
ISPS-Code - Código de Segurança para Portos e Embarcações
ITS Rio - Instituto de Tecnologia e Sociedade do Rio
JTC - *Joint Technical Committee* (Comitê Técnico Conjunto)
LAI - Lei de Acesso à Informação (Lei n° 12.527/2011)
LAPIN - Laboratório de Políticas Públicas e Internet
LFR - *live facial recognition* (reconhecimento facial em tempo real)
LGBTQIA+ - lésbicas, gays, bissexuais, transexuais, travestis, *queer*, intersexo, assexuais e outros grupos e variações de sexualidade e gênero
LGPD - Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)
LIA - *Legitimate Interest Assessment* (Teste de Legítimo Interesse)
Met - *London Metropolitan Police* (polícia de Londres) (*vide* MPS)
METRÔ - Companhia do Metropolitano de São Paulo
MIT - *Massachusetts Institute of Technology*
MPS - *Metropolitan Police Service* (polícia de Londres) (*vide* Met)
MPSP - Ministério Público do Estado de São Paulo
NIC.br - Núcleo de Informação e Coordenação do Ponto BR

NIST - *National Institute of Standards and Technology* (Instituto Nacional de Padrões e Tecnologia dos EUA)
NSA - *National Security Agency* (Agência de Segurança Nacional dos EUA)
OAB - Ordem dos Advogados do Brasil
OMI - Organização Marítima Internacional
ONG - organização não governamental
PCdoB - Partido Comunista do Brasil
PEC - Proposta de Emenda à Constituição
PIA - *Privacy Impact Asssessment*
PID - Portas Interativas Digitais
PL - Projeto de Lei
PLS - Projeto de Lei do Senado Federal
PPP - Parceria Público Privada
PSB - Partido Socialista Brasileiro
RFID - *radio frequency identification* (identificação por radiofrequência)
RGPD - Regulamento Geral sobre a Proteção de Dados (*General Data Protection Regulation*, GDPR) (Regulamento (UE) 2016/679)
RIPD - Relatório de Impacto à Proteção de Dados Pessoais
RPAS - *Remotely Piloted Aircraft Systems* (sistemas de aeronaves pilotadas remotamente)
SC - Subcomitê
Senacon - Secretaria Nacional do Consumidor
Serpro - Serviço Federal de Processamento de Dados
SEWA - *Automatic Sentiment Estimation in the Wild*
SF - Senado Federal
SNDC - Sistema Nacional de Defesa do Consumidor
STF - Supremo Tribunal Federal
TIC - Tecnologia da Informação e Comunicação
TJSP - Tribunal de Justiça de São Paulo
TRF3 - Tribunal Regional Federal da 3ª Região (abrange os estados de São Paulo e Mato Grosso do Sul)
UAS - *unmanned aerial systems* (sistemas aéreos não tripulados)
UAV - *unmanned aerial vehicles* (veículos aéreos não tripulados),
UE - União Europeia
UK - *United Kingdom* (Reino Unido)
Unesco - Organização das Nações Unidas para a Educação, a Ciência e a Cultura
US – *United States (of America)* (Estados Unidos da América, EUA)
UTO - *Unattended Train Operation* (operação de trem sem condutor humano)
WP29 - *Article 29 Data Protection Working Party* (ou, simpelsmente, *Article 29 Working Party*)

Sumário

TECNOLOGIA DE RECONHECIMENTO FACIAL À LUZ DA LEI GERAL DE PROTEÇÃO DE DADOS: RISCOS E DESAFIOS

1. INTRODUÇÃO

Há exatos 15 anos, em 2006, um relatório do *Information Commissioner's Office* (ICO)[1], alertava que àquela época já se vivia em uma sociedade de vigilância. O relatório destacava os seguintes pontos (AMOORE *et al.*, 2006, p. 3):

- As câmeras de vídeo nos observam em todos os lugares (em prédios, ruas comerciais, estradas e áreas residenciais).
- Somos constantemente solicitados a provar nossa identidade, para benefícios, saúde e assim por diante. O governo planeja introduzir um sistema de cartões de identificação biométrica (incluindo impressões digitais e varredura da íris) vinculados a um enorme banco de dados de informações pessoais.
- Quando se viaja ao exterior, informações quanto à proveniência, destino e pertences são verificados, monitorados e os detalhes armazenados. Nos passaportes, chips de computador já carregam informações e há propostas de passaportes biométricos.
- Muitas escolas usam cartões inteligentes e até mesmo dados biométricos para monitorar onde as crianças estão, o que comem ou os livros que pegam emprestado da biblioteca.
- Os hábitos de consumo são analisados por software e os dados vendidos para todos os tipos de negócios. Os contatos com centros de serviço, solicitação de empréstimos, seguros ou hipotecas, a rapidez com que se é atendido e o que é oferecido depende de quanto a pessoa gasta, onde ela vive e quem ela é.
- Telefones, e-mails e uso da Internet podem ser grampeados e rastreados em busca de palavras-chave e frases pelos serviços de inteligência.
- O trabalho é cada vez mais monitorado de perto quanto ao desempenho e produtividade, e até mesmo as atitudes e estilo de vida fora do trabalho são examinados pelas organizações que empregam os indivíduos.

De lá para cá, o quadro, que já era digno de distopias como o também britânico "1984" (ORWELL, 2019), apenas se agravou.

O uso da biometria aumentou significativamente nos últimos anos. Isso é verdade não apenas para o setor público, mas para o privado; não só na área de segurança, mas também no comércio, no trabalho e outros domínios da vida, e.g., para desbloqueio de *smartphones*, confirmação de pagamento em aplicativos, identificação automática de pessoas em imagens de mídias sociais, na permissão de entrada em academias, em sistemas de segurança de aeroportos,

[1] A autoridade independente do Reino Unido criada para defender os direitos de informação no interesse público, promovendo a abertura por órgãos públicos e a privacidade de dados para os indivíduos (ICO, 2021a).

em escolas, em sistemas de transporte público, em locais de trabalho e instalações de saúde (ADA, 2019, p. 1).

Esse fenômeno pode indicar que o acesso legitimado está cada vez mais associado à produção de alguns meios de identificação e, por sua vez, os meios de identificação estão cada vez mais associados à biometria (LYON, 2008, p. 500).

Essas inovações tecnológicas comumente são apresentadas apenas em seu aspecto positivo, pela melhora na experiência do usuário (facilidade, rapidez e comodidade), bem como a conveniência representada pelos aplicativos. Temos sido rápidos em receber essa conveniência, mas é preciso ser honestos sobre seus custos (PASQUALE, 2015, p. 6), não se pode perder de vista o potencial negativo associado a uma perda gradual de privacidade e do direito à proteção de dados (WP29, 2012b, p. 2).

Igualmente, a tecnologia de reconhecimento facial está cada vez mais presente no debate público e, como as demais formas de biometria, é frequentemente apresentada como uma solução "conveniente" ou "eficiente" para as pessoas em geral (PASQUALE, 2015, p. 4). Somos levados a acreditar que pagar por nossos mantimentos por reconhecimento facial será uma prática comum em alguns anos, e poderá ser, inclusive, mais eficiente (FAITHFULL, 2021; MARROW, 2021). Ou que teremos identidades digitais baseadas no reconhecimento facial para acessar serviços públicos[2]. Ou que logo poderemos viajar sem ter que apresentar nossos passaportes, mas apenas cruzar as fronteiras "escaneando nossos rostos" (RECEITA FEDERAL, 2017a; 2017b; 2017c; BRASIL, 2021a; G1 SP, 2021; TV BRASIL, 2021). Inciativas com todos esses exemplos já estão sendo realizadas, disfarçadas de "inovação" e "pesquisa" (KUTTERER *et al.*, 2020).

Mas quantas pessoas de fato percebem que essa tecnologia é supostamente empregada para fins comerciais, como rastrear pessoas que entram e saem de prédios comerciais e de apartamentos; monitorar a frequência de funcionários em empresas; ver como as pessoas respondem a anúncios em tempo real. Se soubessem disso, como seria a aceitação por parte desses indivíduos?

A Tabela 1, mostra uma tentativa de resposta para a questão acima, obtida em junho de 2019, entre adultos norte-americanos (PEW RESEARCH CENTER, 2019).

Tabela 1– Porcentagem* de aceitação do uso de tecnologia de reconhecimento facial entre adultos norte-americanos de acordo com a situação.

Situação	**Aceitável (%)**	**Inaceitável (%)**	**Não têm certeza (%)**
Aplicação da lei avaliando ameaças à segurança em espaços públicos	59	15	13

[2] Segundo informação no site do Governo Federal a respeito do uso de reconhecimento facial para prova de vida de aposentados, "[d]epois de baixar o aplicativo Meu gov.br e acessar o reconhecimento facial, o usuário pode buscar o Portal gov.br e solicitar os mais de 1,5 mil serviços digitais já disponíveis com o Login único, sejam federais, estaduais ou municipais [...] Para esses serviços, não há necessidade de memorização de múltiplos *logins* e senhas e a solicitação é realizada sem que a pessoa precise sair de casa" (BRASIL, 2020b).

Situação	Aceitável (%)	Inaceitável (%)	Não têm certeza (%)
Rastreamento de quem entra ou sai do prédio	36	36	15
Empresas monitorando a frequência de seus funcionários	30	41	15
Anunciantes observando como as pessoas reagem à exibição de anúncios públicos	15	54	16

*Os resultados não somam 100%, porque os 13% dos adultos norte-americanos que nunca ouviram falar de tecnologia de reconhecimento facial não são mostrados.

Fonte: Pew Research Center (2019, p. 3, 7), com modificações

Tomando como exemplo a aceitação de tecnologias de reconhecimento facial para fins mercadológicos, percebe-se que não se trata de um ponto pacífico entre os consumidores. De acordo com uma pesquisa de mercado realizada em 2015 (FIRST INSIGHT, 2015, p. 4), 75% dos clientes afirmaram que não fariam compras em lojas que utilizassem tecnologias de reconhecimento facial para fins comerciais. Entretanto, é assustador pensar que esse percentual caia para 55% caso o consumidor soubesse que o uso de reconhecimento facial teria algum benefício associado (e.g., descontos nas compras). Os dados de 2019, da Tabela 1 acima, mostram que esta situação se manteve praticamente inalterada, com 54% de adultos norte-americanos considerando inaceitável o uso de reconhecimento facial para fins de análise de reação a propaganda em lugares públicos (PEW RESEARCH CENTER, 2019). Também merece destaque que, quando se trata de segurança em espaços públicos, mais da metade dos entrevistados considerou a utilização da tecnologia de reconhecimento facial aceitável.

Estudo realizado no Reino Unido pelo Instituto Ada Lovelace[3] (ADA, 2019, p. 4-5, 8-10, 12), também em 2019, mostrou que a maioria das pessoas aceita o emprego da tecnologia de reconhecimento facial onde haja um benefício público claro, especialmente para a segurança social ou pessoal e desde que salvaguardas adequadas estejam em vigor, e.g., 70% aceitam o uso em investigações criminais e 50% em aeroportos para substituir passaportes. A maioria das pessoas disse ficar desconfortável com a ideia de que a tecnologia de reconhecimento facial possa ser usada em escolas (67%) ou no transporte público (61%); em geral, o desconforto está associado à perspectiva de que isso normalizará a vigilância. Além disso, a maioria das pessoas afirmou se sentir desconfortável com a perspectiva de o reconhecimento facial ser usado por empresas para benefício comercial, e.g., por lojas para "conhecer melhor" seus clientes (77%) ou por departamentos de recursos humanos na seleção de candidatos para empregos (76%), o motivo do desconforto é que não confiam nas empresas para usar a tecnologia de forma ética. Por fim, importante pontuar que embora a maioria dos entrevistados informasse estar ciente do uso da tecnologia de reconhecimento facial no Reino Unido (90%), apenas 53% afirmaram saber algo sobre ela, o que, segundo o estudo, limita a capacidade do público para se envolver em um debate informado sobre os benefícios e riscos dessa tecnologia.

[3] Instituto de pesquisa independente cuja missão é garantir que dados e Inteligência Artificial "trabalhem" para as pessoas e a sociedade, de maneira que maximizem o bem-estar social e que a tecnologia esteja a serviço da humanidade. Foi estabelecido em 2018 pela Fundação Nuffield, em colaboração com o Instituto Alan Turing, a *Royal Society*, a *British Academy*, a *Royal Statistical Society*, o *Wellcome Trust*, *Luminate*, *techUK* e o *Nuffield Council on Bioethics* (ADA, 2021).

O debate atual sobre se o uso de um dos recurso mais exclusivo, a face, é social e eticamente desejável, não consegue acompanhar a imaginação daqueles que desenvolvem essa tecnologia e que a estão vendendo para o mercado e para as autoridades (KUTTERER *et al.*, 2020). Como costuma acontecer, há uma defasagem entre as melhorias tecnológicas e a regulamentação (COUNCIL OF EUROPE, 2013, p. 1, § 1; MANN e SMITH, 2017, p. 121-122).

Em um *white-paper*, supostamente elaborado pela Comissão Europeia, vazado em janeiro de 2020 (STOLTON, 2020), é expresso o dilema se uma moratória no uso do reconhecimento facial deveria ou não ser introduzida pelo período de 3 a 5 anos. É ponderado que, se por um lado, tal proibição daria tempo para a identificação e o desenvolvimento de medidas protetivas quanto a um possível uso abusivo, por outro, havia o temor que uma proibição pudesse "atrapalhar o desenvolvimento e a adoção dessa tecnologia" (STRUCTURE..., 2020, p. 15). Mas é necessário refletir seriamente se certas formas de inovação, como as que envolvem vigilância em massa, não exigem um olhar mais criterioso. Quando se afirma que as salvaguardas dos direitos humanos "impedirão a inovação", está-se criando uma falsa dicotomia entre o progresso tecnológico e o social (à semelhança da suposta dicotomia "segurança" *versus* "privacidade") (FUCHS, 2011; COHEN, 2013, p. 1905-1906, 1918-1920), quando, na verdade, uma sociedade saudável precisa e se beneficia de ambos (COHEN, 2013, 1927).

Num levantamento de 2020 que classificou 194 países com base na extensão da vigilância por reconhecimento facial (Tabela 2), o Brasil já se encontrava na classe "em uso" (SURFSHARK, 2020). De fato, dados dão conta que pelo menos desde 2011 o reconhecimento facial vem sendo empregado no País (INSTITUTO IGARAPÉ, 2019), i.e., a discussão, além de oportuna, já é há muito necessária.

Tabela 2 – Países com base na extensão da vigilância por reconhecimento facial.

Status de reconhecimento facial	Número de países
Em uso	98
Aprovado, mas não implementado	12
Considerando o uso	13
Sem evidência de uso	68
Banido	3
Total	**194**

Fonte: Surfshark (2020).

Este trabalho busca discutir o reconhecimento facial sob o aspecto da proteção da dados, seus usos e potencialidades, riscos e desafios, aspectos legais e éticos da aplicação dessa tecnologia.

1.1 Metodologia

Este estudo possui natureza qualitativa e foi desenvolvido por meio de pesquisa bibliográfica.

A pesquisa foi desenvolvida em duas fases. A primeira correspondeu à identificação das atividades de processamento biométrico que se enquadram no escopo de reconhecimento facial. Na segunda fase, foram analisadas questões decorrentes das implantações identificadas à luz das estruturas jurídicas relevantes.

A pesquisa baseou-se em várias fontes, incluindo: legislação nacional e internacional (em especial da União Europeia – UE), declarações à imprensa, publicações governamentais e da sociedade civil organizada, atos jurídicos relevantes e decisões judiciais, artigos acadêmicos e artigos de notícias.

1.2 Objetivo

Busca-se contribuir para o debate sobre a temática de reconhecimento facial à luz da proteção de dados e alertar para as possibilidades, riscos e desafios da aplicação dessa nova tecnologia, em especial na sua intersecção com a vigilância em massa e espaços públicos. Procura-se, desta forma, colaborar com uma discussão que leve à utilização informada, legítima, segura e equilibrada da tecnologia de reconhecimento facial.

O foco deste estudo está no âmbito de incidência da Lei nº 13.079/2018 (Lei Geral de Proteção de Dados, LGPD). Não está incluído no recorte desta pesquisa o tratamento de dados pessoais realizado para fins exclusivos de "segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais" (art. 4º, III, da LGPD)[4]. Tais temas requerem o advento de legislação específica (art. 4°, § 1°, LGPD)[5], e.g., Anteprojeto da LGPD-Penal[6]. Entretanto, quando pertinente para a exposição do tema foco, poderão ser tecidas considerações acerca das implicações do uso de tecnologia de reconhecimento facial nessa interface (e.g., ao tratar dos seus riscos).

[4] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: […] III - realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais;

[5] 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.

[6] Ato do Presidente da Câmara dos Deputados, de 26 de novembro de 2019, "[i]nstitui[u] Comissão de Juristas destinada a elaborar anteprojeto de legislação específica para o tratamento de dados pessoais no âmbito de segurança pública, investigações penais e repressão de infrações penais, conforme o disposto no artigo 4°, inciso III, alíneas "a" e "d" da Lei n. 13.709, de 14 de agosto de 2018" (CÂMARA DOS DEPUTADOS, 2021). Em 5 de novembro de 2020, a Comissão de Jurista apresentou à Presidência da Câmara dos Deputados, o "Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal" (Anteprojeto da LGPD-Penal) (AGÊNCIA CÂMARA DE NOTÍCIAS, 2020; COMISSÃO DE JURISTAS, 2020). O Anteprojeto se encontra na Câmara dos Deputados à espera de um parlamentar que o apresente formalmente como um Projeto de Lei (PL), que seguirá os trâmites do processo legislativo para poder tornar-se lei, i.e., ainda não se tem uma lei que trate da proteção de dados para segurança pública e persecução penal.

Igualmente, apesar de mencionados em alguns momentos como suporte à discussão, não fazem parte do delineamento deste estudo (fogem do escopo desta pesquisa): (i) a questão específica da proteção dos dados pessoais de crianças e adolescentes (ainda que se reconheça sua importância); (ii) a abordagem da proteção dos dados pessoais sob um enfoque da Lei nº 8.878/1990 (Código de Defesa do Consumidor, CDC), apesar de se concordar serem possíveis consequências distintas para um mesmo fato (punitivas e/ou reparadoras) verificando-se a existência de subsistemas sancionadores autônomos, com pressupostos de imputação específicos, como seria o caso do Sistema Nacional de Defesa do Consumidor (SNDC); (iii) a discussão de responsabilidade e do ressarcimento de danos, o que tem potencial para toda uma pesquisa autônoma a este estudo.

Como contribuições específicas, tem-se: (i) a distinção entre videovigilância (pura e simples) e a videovigilância associada à tecnologia de reconhecimento facial; (ii) que a tecnologia de reconhecimento facial trata dados pessoais sensíveis (atraindo, portanto, todas as salvaguardas associadas a esse tipo especial de dados); (iii) que o consentimento geralmente não é uma hipótese válida (ou pelo menos, não é a mais adequada) para embasar o uso de tecnologia de reconhecimento facial em espaços públicos; (iv) que o uso de tecnologia de reconhecimento facial traz consigo a possibilidade do exercício do direito de revisão das decisões automatizadas; (v) que o uso da tecnologia de reconhecimento facial acarretaria a necessidade de elaboração de relatório de impacto à proteção de dados pessoais (RIPD).

1.3 Descrição dos Capítulos

Além desta Introdução, a pesquisa está estruturada em 5 capítulos, organizados da seguinte forma:

Capítulo 2, apresenta os conceitos básicos associados ao reconhecimento facial. Esse capítulo é essencial para construção da base teórica (técnica e jurídica) de argumentação que será utilizada no capítulo seguinte. Adicionalmente, são tratados possíveis usos, bem como riscos potenciais relacionados à tecnologia de reconhecimento facial. Estes usos e riscos ajudam a dar uma dimensão do desafio que a discussão da tecnologia de reconhecimento facial representa.

Capítulo 3, aborda a maneira como a tecnologia de reconhecimento facial, ao efetuar tratamento de dados pessoais, aciona a incidência da LGPD. Inicialmente é apresentada a questão da videovigilância (dado o recorte de monitoramento em espaços públicos), para depois tratar da sua associação à tecnologia de reconhecimento facial e as repercussões dessa combinação. Nesse aspecto, defende-se que a tecnologia de reconhecimento facial lida com dados pessoais sensíveis, o que tem reflexos importantes no que diz respeito ao tratamento de dados pessoais. Em especial, são abordados tópicos relevantes ao tema, como: (i) princípios da proteção de dados de destaque; (ii) hipóteses para o tratamento dos dados; (iii) o direito de revisão das decisões automatizadas; (iv) a questão da elaboração de relatório de impacto. Por fim, são tecidas considerações acerca de contextos de proibição da utilização da tecnologia de reconhecimento facial.

Capítulo 4, de posse de todo referencial teórico trazido pelos capítulos anteriores, é apresentado como estudo de caso o "Caso do Metrô de São Paulo" onde se observa, na prática, a articulação dos conhecimentos previamente adquiridos quanto à tecnologia de reconhecimento facial e à aplicação de conceitos da LGPD[7]. O caso escolhido, apesar de ainda não concluído (o que deve levar algum tempo para acontecer, pois está em etapa de apresentação de recursos à decisão em primeira instância) é pioneiro e paradigmático, coordenando temáticas de proteção de dados pessoais; utilização de tecnologia de reconhecimento facial; processamento automatizado em larga escala; coleta de dados em local público; obrigações relativas à transparência, informação, segurança, não discriminação.

Por fim, a conclusão, considerações finais, bem como trabalhos futuros são apresentados no Capítulo 5.

[7] A Ação foi iniciada em 2019 e, em que pese a LGPD já haver sido promulgada à época, ela não estava ainda em vigor. Entretanto, seus conceitos já foram empregados e articulados na Ação. Cumpre mencionar que a LGPD é uma lei extremamente nova, sua interpretação, seus limites e alcances começam a ser discutidos na academia (contexto no qual este trabalho se insere), na doutrina e na jurisprudência. Fato é que o "Caso do Metrô de São Paulo" é pioneiro, mas ainda assim, conta, até o momento, apenas com a decisão em primeira instância (o que só reforça a novidade e frescor da discussão aqui empreendida).

2. RECONHECIMENTO FACIAL: CONCEITOS, USOS E RISCOS

2.1 Conceitos Básicos

Os dados biométricos, por sua própria natureza, estão diretamente ligados a um indivíduo. O *General Data Protection Regulation* (GDPR, ou Regulamento Geral sobre a Proteção de Dados, RGPD)[8,9] define **dados biométrico** em seu Art. 4º(14) (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016):

> Artigo 4º - Definições
> Para efeitos do presente regulamento, entende-se por: [...]
> 14) «Dados biométricos», dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;

Já o *Article 29 Working Party*[10] apresenta a seguinte definição para dados biométricos (WP29, 2012a, p. 3-4):

> biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability[11].

No âmbito legal brasileiro, o Decreto nº 10.046/2019[12], que "[d]ispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados" traz a seguinte definição para **atributos biométricos** (BRASIL, 2019a):

---

[8] O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, "relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)".

[9] Todas as citações utilizadas são tiradas da tradução oficial para o português do Regulamento Geral sobre a Proteção de Dados. Como o padrão europeu é o português de Portugal, algumas expressões podem ser diferentes das utilizadas no direito brasileiro.

[10] *Article 29 Working Party* é a abreviatura para *Article 29 Data Protection Working Party* (WP29), o grupo de trabalho europeu independente criado pelo art. 29 da Diretiva 95/46/CE, que forneceu à Comissão Europeia aconselhamento independente sobre questões de proteção de dados e ajudou no desenvolvimento de uma implementação harmonizada das regras de proteção de dados nos Estados-Membros da União Europeia (UE) até 25 de maio de 2018 (quando da entrada em vigor do GDPR) (EDPB, 2021a; EDPS, 2021b, *cf*. "Article 29 Working Party"). Com a entrada em vigor do GDPR, este grupo de trabalho se transformou no *European Data Protection Board* (EDPB), órgão europeu independente, que contribui para a aplicação consistente das regras de proteção de dados na UE e para a promoção da cooperação entre as autoridades de proteção de dados da UE (EDPB, 2021b).

[11] "propriedades biológicas, características fisiológicas, traços físicos ou ações reproduzíveis, na medida em que essas características e/ou ações sejam simultaneamente únicas a essa pessoa e mensuráveis, mesmo que os padrões utilizados na prática para medi-las tecnicamente envolvam um certo grau de probabilidade" (livre tradução).

[12] Importa pontuar que o Decreto nº 10.046/2019 está sendo questionado por meio da Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695, ajuizada pelo Partido Socialista Brasileiro (PSB), que pediu a suspensão do compartilhamento de dados de detentores de Carteira Nacional de Habilitação (CNH) pelo Serviço Federal de Processamento de Dados (Serpro) com a Agência Brasileira de Inteligência (Abin). A ADPF foi distribuída ao Ministro Gilmar Mendes (STF, 2020). Também contra o Decreto nº 10.046/2019 foi ajuizada, pelo Conselho Federal da Ordem dos Advogados do Brasil (OAB), a Ação Direta de Inconstitucionalidade (ADI) nº 6.649, distribuída, por prevenção, ao Ministro Gilmar Mendes (STF, 2021).

> Art. 2º Para fins deste Decreto, considera-se: [...]
> II - atributos biométricos - características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar;

A LGPD determina que dados biométricos mais do que dados pessoais, são dados pessoais **sensíveis**[13] (BRASIL, 2019b, grifo meu):

> Art. 5º Para os fins desta Lei, considera-se:
> I - **dado pessoal**: informação relacionada a pessoa natural identificada ou identificável;
> II - **dado pessoal sensível**: dado pessoal sobre **origem racial ou étnica**, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou **biométrico**, quando vinculado a uma pessoa natural;

Importa pontuar que a nossa LGPD adota um conceito amplo de dado pessoal, assim como a matriz europeia, embasada na ideia de que "todo dado pessoal tem importância e valor" (VIOLA e TEFFÉ, 2021, p. 131). Mesmo dados que pareçam irrelevantes em determinadas circunstâncias[14], que não referenciem uma pessoa diretamente, quando tratados, organizados e cruzados, podem resultar em informação específica sobre um indivíduo, que pode ser, inclusive, de caráter sensível, como constatado pela Corte Constitucional Alemã no paradigmático julgamento sobre a Lei do Censo de 1983 (MENDES, 2018, p. 187-192). Neste mesmo sentido, o julgamento histórico no Brasil, de maio de 2020, em sede de controle de constitucionalidade[15] no qual o Supremo Tribunal Federal (STF) reconheceu a proteção de dados pessoais como direito fundamental autônomo, baseado na lógica que não há dados "irrelevantes, neutros ou insignificantes", afirmando a proteção constitucional ao dado pessoal[16] (MENDES, 2020; MENDES e FONSECA, 2020; RUARO e SARLET, 2021, p. 204).

---

[13] Cumpre mencionar que, mesmo antes da LGPD, a definição de "informação sensível" não era estranha ao legislador, uma vez que tal definição já constava na Lei nº 12.414/2011 (Lei do Cadastro Positivo) (apesar de não fazer, àquela época, referência a dados biométricos): "Art. 3º [...] § 3º Ficam proibidas as anotações de: [...] II – informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas" (BRASIL, 2011).

[14] Não raro, dados tidos como "irrelevantes" ou "públicos", quando associados entre si ou a outros dados podem servir de insumo para correlações, predições e ranqueamento acerca do titular dos dados pessoais ou grupos sociais, tendo efeitos práticos e substantivos para o titular dos dados (MENDES e FONSECA, 2021, p. 99).

[15] Por maioria de dez votos favoráveis (vencido o Ministro Marco Aurélio), o Plenário do STF referendou a Medida Cautelar concedida pela Ministra Rosa Weber, relatora das Ações Diretas de Inconstitucionalidade (ADIs) 6.387, 6.388, 6.389, 6.390 e 6.393, suspendendo a eficácia da Medida Provisória nº 954/2020 que determinava às empresas de telecomunicações o compartilhamento do nome, número de telefone e endereço de seus consumidores de telefonia móvel e fixa com o Instituto Brasileiro de Geografia e Estatística (IBGE). Para detalhes do Acórdão *vide* Brasil (2020c).

[16] Está em tramitação no Congresso Nacional a Proposta de Emenda à Constituição (PEC) nº 17/2019, do Senado Federal (SF) que inclui no art. 5º da Constituição (entre os direitos e garantias fundamentais) a garantia à proteção de dados pessoais, inclusive nos meios digitais, e atribui à União competência de organizar e fiscalizar a proteção e o tratamento de dados pessoais (art. 21), bem como de legislar sobre o tema (art. 22) (CÂMARA DOS DEPUTADOS, 2021a; 2021b). Em 31/08/2021, durante a elaboração deste trabalho, a PEC foi aprovada em dois turnos na Câmara dos Deputados (inclusive com votação expressiva: 439 votos a 1, no primeiro turno; 436 votos a 4, em segundo turno), na forma do substitutivo do relator, deputado Orlando Silva (PCdoB-SP) – que foi também

Ademais, o caráter **sensível** de informações de natureza biométrica foi reconhecido explicitamente com a inclusão de dados que identificam exclusivamente uma pessoa nas categorias especiais de dados no art. 6 da *Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data* (*Convention 108+* ou Convenção 108+[17]), realizada em 2018 (COUNCIL OF EUROPE, 2018, grifo meu):

> Article 6 – Special categories of data
> 1. The processing of:
> - genetic data;
> - personal data relating to offences, criminal proceedings and convictions, and related security measures;
> - **biometric data uniquely identifying a person**;
> - personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life,
> shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention[18].

A LGPD também define o que é **tratamento** no âmbito dos dados pessoais (BRASIL, 2019b):

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

Nesse sentido, o tratamento de qualquer dado pessoal em geral, e dos biométricos, em específico, deve ser compreendido como uma cadeia de procedimentos que devem estar de acordo com o ordenamento jurídico brasileiro[19], em especial a LGPD, mas também leis

relator da LGPD –, e retornaria ao SF, seguindo o rito do processo legislativo, para apreciação das mudanças e consequente votação em dois turnos (CÂMARA DOS DEPUTADOS, 2021a; PIOVESAN e MACHADO, 2021).

[17] A Convenção 108, aberta para assinatura em 28 de janeiro de 1981 (completando 40 anos em 2021), foi o primeiro instrumento internacional juridicamente vinculativo na área da proteção de dados. Serve de base para os regimes de proteção de dados dos 47 Estados-Membros do Conselho da Europa, uma organização internacional que defende os direitos humanos, a democracia e o Estado de direito através da Europa. O Uruguai foi o primeiro país não europeu a ratificar a Convenção, em 2013 (atualmente 8 Estados ratificaram a Convenção, mas não integram o Conselho da Europa; o Brasil não é um deles, mas detém o *status* de observador desde outubro de 2018) (ANPD, 2021a). Suas reuniões plenárias ocorrem duas vezes ao ano e participam delas membros signatários, mas também outros países e organizações internacionais na condição de observadores. A Convenção 108 foi modernizada e agora é denominada Convenção 108+, buscando responder aos novos desafios tecnológicos colocados pelo desenvolvimento das tecnologias de informação e comunicação (COUNCIL OF EUROPE, 2021b; 2021a).

[18] "Artigo 6 - Categorias especiais de dados. 1. O processamento de: - dados genéticos; - dados pessoais relativos a infrações, processos e condenações criminais, e medidas de segurança relacionadas; - **dados biométricos que identifiquem exclusivamente uma pessoa**; - dados pessoais pelas informações que revelam em relação à origem racial ou étnica, opiniões políticas, filiação a sindicatos, crenças religiosas ou outras, saúde ou vida sexual, só será permitido quando as salvaguardas apropriadas estiverem consagradas em lei, em complemento às desta Convenção" (livre tradução, grifo meu).

[19] Antes mesmo da sanção da LGPD, o Brasil já contava com mais de 40 normas setoriais de proteção de dados (e.g., Código, Civil, Código de Defesa do Consumidor, Marco Civil da Internet etc.) (GOMES, 2019b, p. 7).

esparsas sobre proteção de dados pessoais (MONTEIRO, 2017, p. 2-4; TEOFILO *et al.*, 2019, p. 8) e normativos que venham a ser editados.

Os dados biométricos podem ser tratados de formas diferentes. Às vezes são armazenados na forma bruta (e.g., impressão digital, fotografia de um rosto), outras vezes, a informação biométrica bruta é processada a fim de se extrair um elemento definido (e.g., distância dos olhos, largura da base do nariz) e apenas este é armazenado (WP29, 2012b, p. 4).

O **processamento biométrico** corresponde ao **tratamento de dados biométricos** e pode "ser referido indistintamente como reconhecimento, identificação, autenticação, detecção ou outros termos relacionados, bem como formas (muitas vezes opacas) de coletar e armazenar dados biométricos, mesmo que os dados não sejam processados imediatamente" (MONTAG *et al.*, 2021, p. 10).

De acordo com o ISO/IEC JTC 1[20], SC 37[21], **reconhecimento biométrico** é o "reconhecimento automatizado de indivíduos com base em suas características biológicas e comportamentais" (ISO e IEC, 2017, p. 2). Dentre as **características biológicas** (físicas e fisiológicas), encontram-se impressões digitais, reconhecimento da íris, o exame da retina, o reconhecimento facial, da voz, do formato da mão, da forma da orelha, do canal auditivo, a detecção do odor corporal, a análise da estrutura de DNA etc.; as **características comportamentais** incluem a verificação da assinatura manuscrita, a análise de padrões de digitação, da marcha (do caminhar) etc. (WP29, 2012b, p. 4). Já o **reconhecimento automatizado** "implica que um sistema baseado em máquina é usado para o reconhecimento, seja para o processo completo, ou auxiliado por um ser humano" (ISO e IEC, 2017, p. 2).

Importante mencionar que a **fonte de dados biométricos** (seja ela um elemento biológico – e.g., uma amostra de tecido humano – ou comportamental) não pode ser considerada dado biométrico em si, apesar disso, pode ser utilizada para a obtenção de dados biométricos pela extração de informações (WP29, 2012b, p. 4).

Modelo biométrico corresponde aos elementos-chave extraídos a partir de dados biométricos brutos (e.g., medições faciais obtidas de uma imagem) que serão armazenados para uso posterior, em lugar dos próprios dados brutos. Aspecto importante com relação ao modelo biométrico diz respeito à definição da quantidade de informação a ser armazenada. Ela deve ser suficientemente grande para garantir segurança, mas não excessiva, a ponto de permitir a reconstituição do dado biométrico bruto, daí dizer-se que sua construção deve ser em "sentido único", i.e., que não se chegue ao dado biométrico bruto a partir do modelo (WP29, 2012b, p. 4).

Sistemas biométricos, numa definição geral, são "sistemas que extraem e posteriormente tratam dados biométricos" (WP29, 2012b, p. 5). Estão intimamente ligados a uma pessoa, pois utilizam uma propriedade única do indivíduo para: (1) *identificação*

[20] Trata-se do comitê técnico conjunto da Organização Internacional para Padronização (*International Organization for Standardization*, ISO) e da Comissão Eletrotécnica Internacional (*International Electrotechnical Commission*, IEC) intitulado "Tecnologia da informação", cujo objetivo é desenvolver, manter e promover padrões nas áreas de tecnologia da informação e comunicação (TIC) (ISO e IEC, 2017, p. iv).

[21] Subcomitê 37, responsável por padrões de biometria (ISO e IEC, 2017, p. iv).

(correspondência um-para muitos; distinguir uma pessoa de um conjunto maior de indivíduos); (2) *autenticação/verificação* (correspondência um-para-um; comparação dos dados biométricos de uma pessoa – obtidos no momento da identificação – com um modelo biométrico armazenado num dispositivo como mecanismos de validação, e.g., leitores de impressão digital, leitores de padrão de veia ou mesmo o reconhecimento de face em uma câmera podem substituir cartões, códigos, senhas e assinaturas); (3) *categorização/classificação* (processo de extração de características de uma pessoa, a fim de a integrar em uma ou várias categorias amplas, e.g., idade, gênero etc.) (WP29, 2012a, p. 3; 2012b, p. 2, 6). Destarte, ainda que os dados biométricos de uma pessoa possam ser excluídos ou alterados, a fonte da qual foram extraídos não pode, em geral, ser alterada nem excluída (WP29, 2012b, p. 2).

Normalmente, um sistema biométrico processa os dados biométricos seguindo as seguintes etapas (WP29, 2012b, p. 5):

1. **Inscrição/cadastramento biométrica(o)**: processos realizados pelo sistema biométrico com o objetivo de extrair dados biométricos a partir de uma fonte biométrica e de os associar a um indivíduo. A quantidade e a qualidade dos dados necessários devem ser adequadas à finalidade do tratamento e ao nível de desempenho do sistema biométrico. Considerando que geralmente é nesta fase que a pessoa tem o primeiro contato com o sistema biométrico e que, usualmente, a inscrição implica a participação da pessoa (e.g., a coleta de impressões digitais, de foto para passaporte ou crachá), este pode ser um momento adequado para fornecer-lhe aviso e informações acerca do tratamento. Sem embargo, também é possível inscrever pessoas sem o seu conhecimento ou consentimento (e.g., sistemas de câmeras de vídeo em circuito fechado com a funcionalidade de reconhecimento facial).
2. **Armazenamento biométrico**: como os dados obtidos no cadastramento são guardados para uso posterior. Podem ser armazenados localmente no centro de operações (e.g., num leitor), ou num dispositivo que a pessoa traz consigo (e.g., num cartão inteligente), ou enviados e armazenados numa base de dados central à qual um ou mais sistemas biométricos têm acesso.
3. **Correspondência biométrica**: processo de comparação dos dados/modelos biométricos (obtidos durante o cadastramento) com dados/modelos biométricos recolhidos a partir de uma nova amostra para efeitos de identificação, verificação/autenticação ou categorização.

No passado, o uso de tecnologia de reconhecimento biométrico era dispendioso, e com isso, o impacto sobre os direitos de proteção de dados dos indivíduos era limitado. Entretanto, à medida que a tecnologia avança, essa realidade vai se transmutando radicalmente. O progresso tecnológico tornou tudo mais barato e acessível (e.g., espaço de armazenamento, capacidade computacional, equipamentos – desde câmeras de segurança e sensores, a aparelhos de análise de DNA) (PASQUALE, 2015, p. 4). Outro elemento que aciona as considerações de proteção de dados é que atualmente é possível conduzir automaticamente esses métodos e possivelmente reconhecer pessoas com precisão mensurável (EDPS, 2021b, *cf*. Biometrics).

Ao mesmo tempo que isso torna procedimentos de identificação e autenticação fáceis, rápidos e convenientes, traz consigo o fantasma de novas e reais ameaças a direitos fundamentais (WP29, 2012b, p. 2).

Muitas tecnologias de reconhecimento biométrico permitem não só o rastreamento automatizado, mas à distância (*frictionless nature*), bem como a criação de perfis de indivíduos, tendo significativo impacto potencial sobre a privacidade e o direito à proteção de dados dos indivíduos. Impacto esse que só vem crescendo com a progressiva implantação dessas tecnologias, no setor público e privado. Provavelmente, todo indivíduo adulto (e muitas crianças e adolescentes) esteja inscrito em um ou vários sistemas biométricos (WP29, 2012b, p. 3).

A **tecnologia de reconhecimento facial** (*facial recognition technology*, FRT)[22] é o processo automatizado de "correspondência" de faces para determinar se elas representam o mesmo indivíduo, utilizando algoritmos[23] e tecnologias de processamento biométrico (GARVIE *et al.*, 2016, p. 116; BFEG, 2019, p. 1). Segundo o *Article 29 Working Party* (2012a, p. 3), a FRT corresponde ao "tratamento automático de imagens digitais que contêm a face de pessoas para efeitos da sua identificação, autenticação/verificação ou categorização", tenha ou não o indivíduo dado consentimento para tal, ou tenha conhecimento da prática.

De um ponto de vista técnico, a FRT é uma subcategoria dentro da Inteligência Artificial (IA) "visão computacional" (*computer vision*). A visão computacional, *lato sensu*, desenvolve algoritmos para extrair informações de imagens, e.g., detectar objetos e sua posição nas imagens; identificar objetos; detectar marcas; categorizar imagens; descrever imagens; detectar características geográficas, esquemas de cores, reconhecimento de texto; detectar imagens inadequadas; detectar faces; analisar faces (detectando o gênero, as emoções ou os acessórios que as pessoas estão usando); identificar faces (AZRIA e WICKERT, 2019, p. 2).

A **aquisição da imagem facial** geralmente ocorre por meio de uma câmera de circuito fechado de televisão (CFTV, ou *closed circuit television*, CCTV) (e.g., localizada em uma van, um poste de luz ou contida em um dispositivo portátil) que tira fotos digitais da face do indivíduo em tempo real. A aquisição pode ocorrer: (i) tirando uma fotografia estática em um ambiente "controlado" (e.g., quando uma pessoa tem sua fotografia tirada em um portão de embarque ao apresentar o passaporte); (ii) capturando uma imagem em movimento quando uma pessoa passa pelo "campo de visão" da câmera (ROYAL COURTS OF JUSTICE RULING, 2019, p. 8).

2.2 Outros conceitos relacionados

[22] Mas também conhecida por *automatic facial recognition technology* (AFR) e, quando usada em tempo real, como *live facial recognition* (LFR) (ROYAL COURTS OF JUSTICE RULING, 2019, p. 8).

[23] De uma maneira bastante simplificada (suficiente para o tema aqui tratado), pode-se dizer que algoritmos são fórmulas (sequência finita de passos) projetadas para se atingir/calcular um determinado objetivo/resultado, i.e., trata-se de uma série de etapas para concluir uma tarefa, descritas com a precisão suficiente para que um computador possa realizá-las. Para uma visão mais aprofundada *vide* Cormen *et al*. (2001, p. 5-12).

Vigilância em massa pode ser considerada "qualquer monitoramento, rastreamento ou outro processamento de dados pessoais de indivíduos de forma geral ou indiscriminada, ou de grupos, que não seja realizado de forma específica e legalmente 'direcionada' contra um indivíduo específico", bem como "a vigilância com alvo arbitrário, dado o potencial de ser arbitrariamente imposta a qualquer indivíduo sem suspeita razoável" (MONTAG *et al.*, 2021, p. 10).

Espaço público, segundo a Unesco (2017), é a "área ou local aberto e acessível a todas as pessoas, independentemente de gênero, raça, etnia, idade ou nível socioeconômico [...], como praças, quadras e parques [...], calçadas e ruas [...]. No século 21, alguns chegam a considerar os espaços virtuais disponibilizados pela internet como um novo tipo de espaço público que desenvolve interação e mistura social". Para fins deste estudo, também podem ser considerados públicos "espaços de propriedade privada, mas de acesso público, como shopping centers, estádios, transporte público e outros serviços de interesse público" (MONTAG *et al.*, 2021, p. 11), mas também os espaços *quase-públicos* como hospitais e instituições de ensino (COUNCIL OF EUROPE, 2021c, p. 5). Tais espaços podem incluir, também, locais onde as pessoas estão reunidas e relativamente estáticas (e.g., salas de concertos, estádios, comícios públicos), bem como espaços com pontos de entrada e saída claramente definidos ou por onde as pessoas são "canalizadas" (i.e., conduzidas a passar por um caminho específico) (e.g., entradas de estações ferroviárias, de aeroportos, de centros comerciais, de locais de manifestações políticas) (BFEG, 2019, p. 1).

2.3 Como a FRT Funciona

Como um sistema biométrico que é, a FRT geralmente executa pelo menos uma das seguintes tarefas (LYNCH, 2018, p. 5-6):

1. *Identificação*:
    1.1. Identificar uma pessoa desconhecida (e.g., de uma filmagem de câmera de vigilância).
    1.2. Procurar por vários rostos específicos, previamente identificados (e.g., pessoas procuradas em uma plataforma de metrô, compradores em uma loja, contadores de cartas em um cassino).
2. *Autenticação/verificação*: confirmar a identidade de uma pessoa conhecida (e.g., para desbloquear um *smartphone*, acessar uma conta bancária).
3. *Categorização* (e.g., para fins de segmentação de público para oferecimento de marketing direcionado).

Para identificar um indivíduo, o algoritmo FRT segue as seguintes etapas (WOODWARD Jr *et al.*, 2003, p. 3-4; ADLER e SCHUCKERS, 2007, p. 1248-1249; WP29, 2012a, p. 3; RICANEK e BOEHNEN, 2012 p. 95; GARVIE *et al.*, 2016, p. 9; LYNCH, 2018, p. 4-6):

1. **Obtenção da imagem**: capta o rosto de uma pessoa e o converte em formato digital (a imagem digital).

2. **Detecção facial**: encontra a pessoa dentro do segmento de foto ou vídeo, i.e., detecta a presença de um rosto numa imagem digital e marca essa área da imagem. Segundo Buolamwini *et al*. (2020, p. 2-3), detectar a presença de um rosto e localizá-lo na imagem não é o mesmo que atribuir uma identidade única a um rosto detectado ou tentar determinar atributos como gênero ou idade, i.e., o processo de detecção facial não relata nada sobre quem alguém é ou que tipo de pessoa alguém pode ser.
3. **Normalização**: uma vez detectado, o rosto é dimensionado, girado e alinhado, convertendo-o em uma dimensão-padrão, a fim de ser mais fácil para o algoritmo comparar as imagens na "mesma posição".
4. **Extração de características**: são identificados atributos que podem ser quantificados numericamente (e.g., textura da pele, distância dos olhos, formato do queixo). A FRT registra não a face em si, mas a geometria espacial das características distintivas da face.
5. **Registro**: caso seja a primeira vez que uma pessoa é encontrada pelo sistema de reconhecimento facial, a imagem e/ou padrão de referência (modelo biométrico) pode ser armazenado como registro para ulterior comparação.
6. **Comparação de pares**: processo de medição das semelhanças entre um conjunto de características (a amostra, *probe*) e outro previamente registado no sistema. O algoritmo verifica pares de faces (a imagem é comparada a outras faces previamente coletadas e armazenadas em um repositório) e retorna um valor numérico (uma espécie de pontuação) indicando a similaridade das características.

Como pode ser percebido, a FRT é intrinsecamente probabilística. Seu resultado não é uma resposta binária (sim ou não), mas uma probabilidade de correspondência (um *score*, uma pontuação) entre o rosto pesquisado e os rostos armazenados em um banco de dados. Geralmente, a FRT retornará aquelas fotos que obtiverem uma pontuação acima de um limite de similaridade, classificadas na ordem de probabilidade de identificação correta (LYNCH, 2018, p. 6).

2.4 Usos e Riscos da FRT

Os empregos da FRT são muitos e variados, mas **nem todos eles são éticos**. Seus usos potenciais incluem, mas não estão limitados a (NEC, 2015; AZRIA e WICKERT, 2019, p. 10-11; VAN NOORDEN, 2020, p. 358):

- Detectar intrusos.
- Emissão de documentos de identidade, na maioria das vezes combinado com outras tecnologias biométricas, como impressões digitais (evitando fraude e roubo de identidade), e.g., utilização de FRT para emissão de carteira nacional de habilitação (CNH) – no processo de renovação da CNH, de emissão de 2ª via, de troca de categoria, reabilitação e transferência de unidade da Federação, a foto do condutor é enviada para o Serviço Federal de Processamento de Dados (Serpro), que faz uma conferência para verificar o grau de semelhança com registros

anteriores feitos no Departamento de Trânsito do Estado de emissão e de outros estados (G1 AM, 2019).

- Substituir documentos de identidade (ser usado como meio de identificação).
- Controle de fluxo de passageiros, e.g., sistemas de transporte público verificando a identidade dos viajantes beneficiados com algum tipo de desconto ou isenção (idosos, deficientes, estudantes), para identificar possíveis fraudes (MONTEIRO, 2014; SP TRANS, 2015); aeroportos verificando a identidade dos viajantes (BRASIL, 2021a; G1 SP, 2021; TV BRASIL, 2021) – um estudo de 2018 mostrou que 77% dos aeroportos e 71% das companhias aéreas planejavam investir em biometria, de uma maneira geral, e 59% dos aeroportos e 63% das companhias aéreas, em FRT, de maneira específica, principalmente nos portões de embarque (SITA, 2018, p. 4, 9, 23, 30, 32).
- Controle de fronteiras/alfandegário (RECEITA FEDERAL, 2017a; 2017b; 2017c).
- Controle de imigração e emissão de vistos, e.g., para comparar o retrato em um passaporte biométrico digitalizado com o rosto do titular (MANN e SMITH, 2017, p. 129-130; O'SULLIVAN; THALES GROUP, 2018); na Austrália, o *Migration Act 1958* autoriza a coleta de dados biométricos, incluindo imagem da face de pessoas (cidadãos ou não) entrando ou saindo do país; além disso, os requerentes de visto localizados em certos países são solicitados a fornecer informações biométricas (geralmente suas impressões digitais e imagem facial) durante o processo de solicitação de visto (PETRIE, 2018, p. 5)
- Investigações criminais, ou mesmo para tentar identificar indivíduos que não queiram, ou não possam cooperar (e.g., pessoa inconsciente) (BUOLAMWINI *et al.*, 2020, p. 7).
- Permitir uma pesquisa rápida em banco de dados de fotografia, inclusive a comparação com qualquer imagem ou filmagem CFTV, bem como com fotos tiradas de câmeras de vídeo integradas a vestimentas, drones e imagens de telefone.
- Ajudar a reduzir o tempo de investigação, permitindo que investigadores identifiquem ou excluam rapidamente os suspeitos logo após um crime ter sido cometido.
- Monitorar locais públicos.
- Identificar participantes de manifestações, e.g., manifestantes do movimento *Black Lives Matter* foram identificados com o uso de FRT (COX, 2020; HOLDEN, 2020; VINCENT, 2020); pessoas que participaram da invasão (manifestamente ilegal) do Capitólio em janeiro de 2021, após a derrota do então Presidente Trump nas eleições presidenciais americanas de 2020 também foram identificadas com FRT (GREENBERG, 2021).
- Permitir que pessoas com deficiência visual obtenham informações sobre as pessoas que encontram juntamente com *feedback* de áudio (gênero, idade, emoção) (MICROSOFT, 2021).

- Encontrar pessoas perdidas e/ou desaparecidas (DELHI..., 2018) – incluindo pessoas desorientadas, e.g., com demência, amnésia, epilepsia, doença de Alzheimer ou outros problemas de saúde semelhantes – e impedir o tráfico humano (SIMONITE, 2019).
- Algoritmos de simulação de envelhecimento permitiriam reconhecer pessoas que desapareceram quando eram crianças e agora são adultas (FACEAPP, 2021).
- Diversos filtros no Instagram ou Snapchat usam FRT (KRIEGER, 2020; MARASCIULO, 2020; REID, 2020).
- Acessar *smartphones* e caixas eletrônicos de forma "mais conveniente".
- Instituições financeiras estão usando verificação facial como forma de adicionar segurança a transações bancárias e evitar fraudes (NTECH LAB, 2021).
- Pagar por serviços, e.g., compras em supermercados, lanchonetes etc. (REUTERS, 2017; FAITHFULL, 2021; MARROW, 2021).
- Acessar serviços públicos, programas de governo e benefícios sociais (DOVAL, 2018; BRASIL, 2020b).
- Substituir os bilhetes de entrada convencionais e os *e-tickets* (de shows, teatro, eventos, cinema) por *scanners* faciais para que os espectadores possam entrar de forma "mais rápida e fácil" (KASTRENAKES, 2018).
- Auxiliar no diagnóstico e tratamento médico (VERMA *et al.*, 2020), e.g., detecção de doenças genéticas raras, como a síndrome de DiGeorge[24] (KRUSZKA *et al.*, 2017; MJOSETH, 2017), suporte a medidas de alívio da dor (detectando níveis de dor pela expressão facial em pacientes que não podem falar) (ROY *et al.*, 2016).
- Rastrear e analisar os hábitos dos clientes (HEBER, 2014; INTEL, 2014; FREY, 2016; CASEMIRO, 2019; GILLESPIE, 2019; IDEC, 2019f).
- Fabricantes de carro estão integrando FRT não só para permitir que os motoristas entrem em seus carros sem necessidade de utilização de chave, mas para monitorá-los quanto a sinais de sonolência ou desatenção (AFFECTIVA, 2021)
- Classificar fotos e marcá-las automaticamente em redes sociais (*auto-tagging*), e.g., o algoritmo *DeepFace* do *Facebook*, usado para encontrar as fotos em que um indivíduo está presente, para que ele possa revisar, interagir ou compartilhar o conteúdo (SKY NEWS, 2019; RIDLEY, [2017]).
- Rastrear pessoas que entram e saem de prédios comerciais e de apartamentos (DRAPER, 2018; DURKIN, 2019).
- Algumas igrejas estão usando reconhecimento facial para controlar a frequência à congregação (BRAZILIAN..., 2020).

[24] Distúrbio cromossômico causado por um defeito no cromossomo 22 que resulta em desenvolvimento inadequado de vários sistemas do corpo. Suas características variam amplamente, mesmo entre membros da mesma família. A síndrome é considerada rara e afeta de 1 em 3.000 a 1 em 6.000 crianças. A doença resulta em várias alterações em todo o corpo, que podem incluir fenda palatina, defeitos cardíacos, alterações faciais características (implantação baixa das orelhas, boca em forma de "boca de peixe", má formação nos olhos), problemas de aprendizagem. Entretanto, estas alterações têm um espectro fenotípico bastante amplo, sem nenhum achado patognomônico (característico exclusivamente da doença) ou mesmo obrigatório, de maneira que os profissionais de saúde muitas vezes não conseguem identificar facilmente a doença, especialmente considerando populações com etnias diversas (MJOSETH, 2017; CASA HUNTER, 2021).

- Monitorar a atenção e a frequência de funcionários em empresas (MITREFINCH, 2021).
- Escolas registrando alunos, verificando sua frequência e avaliando o seu comportamento (ANKEL e ASENJO, 2019; ALBA, 2020), e.g., engajamento no ensino remoto.
- Auxiliar departamentos de recursos humanos na seleção de candidatos, e.g., identificando candidatos não-motivados na entrevista de emprego; a HireVue usa gravação de vídeo de candidatos em entrevistas de emprego para "prever", a partir de suas microexpressões, se eles serão bons funcionários (GEE, 2017; HIREVUE, 2021).
- Supervisionar as emoções de indivíduos.
- Detectar emoções durante um filme, um videogame ou um show.
- Ajudar robôs a interagir com humanos, reconhecendo suas identidades e emoções.
- Determinar a orientação sexual a partir das características faciais, e.g., o polêmico e controverso "gaydar" (LEWIS, 2018; WANG e KOSINSKI, 2018; LEUFER, 2021).
- Prever comportamento criminoso (no melhor estilo Lombroso[25]), e.g., determinar se uma pessoa está prestes a cometer um crime por suas características faciais (STANKOVIĆ *et al.*, 2015; WU e ZHANG, 2017; BBC, 2020).
- E muitos outros cenários podem ser imaginados.

Sem embargo, como pode ser percebido de alguns itens listados acima, o uso da FRT apresenta diversos desafios (riscos) para os quais não existem soluções fáceis, mas que precisam ser reconhecidos de forma mais ampla. A seguir, alguns deles são abordados.

2.4.1 Acurácia (grau de confiança)

A FRT é menos precisa do que, por exemplo, a impressão digital, principalmente quando usada em tempo real ou em grandes bancos de dados (GARVIE *et al.*, 2016, p. 3, 46). Vários fatores influenciam a probabilidade/precisão de uma correspondência, como (WP29, 2012b, p. 6; BFEG, 2019, p. 2; HAMANN e SMITH, 2019):

1. A qualidade das imagens (iluminação, fundo, resolução, ângulo, expressão facial etc.)
2. As condições ambientais em que a imagem é capturada (iluminação, posição da câmera etc.)
3. As diferenças entre os equipamentos utilizados (câmeras, dispositivos de escaneamento etc.)

[25] Cesare Lombroso, cientista italiano que ficou conhecido por procurar detectar as causas da criminalidade por meio de pesquisas científico-empíricas das características físicas, fisiológicas e psicológicas do indivíduo criminoso. Sua obra ao mesmo tempo que teve grande repercussão na criminologia mundial, é carregada de críticas e controvérsias, principalmente relacionadas ao determinismo biológico.

4. O tamanho da lista de observação (*watchlist*), i.e., do catálogo de imagens (conjunto de dados).
5. Os limites/parâmetros de correspondência (*match thresholds*).
6. As mudanças que o rosto sofre com o tempo (e.g., peso corporal, pelos faciais, penteado, colocação de *piercings*, procedimentos cirúrgicos/intervenções estéticas, efeitos do envelhecimento).
7. Se a pessoa está usando algum acessório (e.g., óculos, máscara).
8. Uma resposta próxima ao tempo real ou não.
9. Se há ação humana após a identificação biométrica gerada pela máquina (supervisão humana), e se esta pessoa é treinada.

Foi demonstrado que a checagem humana dos resultados da FRT é benéfica (supervisão humana), mas ainda assim, sem treinamento especializado, na metade das vezes, os usuários humanos tomam a decisão errada sobre uma correspondência (WHITE *et al.*, 2015, p. 6).

Estudo da Universidade de Essex aponta que as pessoas são psicologicamente desencorajadas a desafiar as decisões automatizadas devido ao fardo de refutá-las (seja pela percepção que o algoritmo seria neutro e mais acurado, seja pela dificuldade de explicar porque a recomendação não foi seguida) (McGREGOR *et al.*, 2019, p. 317-318). Assim, ainda que a decisão automatizada sirva apenas de recomendação para tomada de decisão, ela pode ser um elemento decisivo, pois para desconsiderá-la, o operador humano teria que fundamentar sua opção por meio de elementos mensuráveis quantitativamente tal como as previsões algorítmicas e o espaço de subjetividade seria eliminado (BIONI e MARTINS, 2020a). Em suma: "é o computador quem tem a palavra final".

Como a FRT varia em sua capacidade de identificar pessoas, ela deve(ria) relatar sua taxa de erros, ou seja, o número de (WP29, 2012b, p. 6; LYNCH, 2018, p. 6):

1. **Falsos positivos**, também conhecido como "taxa de aceitação falsa" (*false accept rate*, FAR): probabilidade de um sistema biométrico identificar incorretamente uma pessoa (dizer que é quem ela não é) ou não rejeitar um impostor.
2. **Falsos negativos**, também conhecido como "taxa de rejeição falsa" (*false reject rate*, FRR): probabilidade de um sistema biométrico não reconhecer a correspondência entre uma pessoa e o seu próprio modelo biométrico existente.

Idealmente, um sistema biométrico teria um valor zero para FAR e FRR, mas o que se observa com frequência é que tais taxas são inversamente proporcionais, i.e., o aumento de falsos positivos reduz o nível de falsos negativos e vice-versa. Quando se avalia a precisão de um sistema biométrico, associados à FAR e à FRR, devem ser considerados fatores relacionados às finalidades do tratamento de dados e à dimensão da população (WP29, 2012b, p. 6).

Falsos positivos ou falsos negativos podem levar a situações de constrangimento, discriminação, prisões arbitrárias, restrição ou violação de direitos. Casos concretos não faltam, e.g., sistema de reconhecimento facial da polícia militar do Rio de Janeiro falha e mulher é detida por engano (falso positivo) (G1, 2019b), para piorar a situação, descobriu-se depois que

a criminosa procurada estava presa há quatro anos, evidenciado, também, grave problema de atualização da base de dados utilizada à época (WERNECK, 2019); sistema de reconhecimento facial instalado em ônibus de São Carlos não logra identificar crianças com deficiência (falso negativo) pois elas não conseguem olhar pelo tempo necessário para câmera que, além de tudo, fica na parte de cima da catraca, afora perder o benefício de utilizar o ônibus de graça, quem tem o cartão bloqueado ainda arca com a despesa de pagar pelo desbloqueio (G1 SÃO CARLOS E ARARAQUARA, 2018).

Durante o carnaval de 2019, nos quatro dias da Micareta de Feira de Santana-BA, o sistema de videovigilância com utilização de FRT capturou a face de mais de 1,3 milhões de pessoas (em princípio cumpridoras da lei, i.e., contra as quais não havia suspeita de ilícito, chamando a atenção, desde logo, a desproporcionalidade dessa rastreabilidade), gerando 903 alertas, o que resultou no cumprimento de 18 mandados e na prisão de 15 pessoas (G1 BA, 2019), i.e., considerando o total de alertas emitidos, mais de 98% não resultaram em nada[26].

No período de 2016 a 2019, a polícia de Londres (*Metropolitan Police Service*, MPS, ou *London Metropolitan Police*, Met) conduziu um total de 10 testes usando FRT durante as operações de policiamento. Um estudo independente da Universidade de Essex (FUSSEY e MURRAY, 2019) que analisou os 6 últimos testes (no período compreendido entre junho de 2018 e 2019) apontou que de 42 correspondências identificadas pela FRT do MPS, apenas 8 foram confirmadas como corretas (i.e., a grande maioria das pessoas "sinalizadas" para a polícia não estava em uma lista de procurados), uma taxa de erro de 81%, extremamente alta, em vista dos efeitos potencialmente prejudiciais para os titulares dos dados[27] (FUSSEY e MURRAY, 2019, p. 5, 10, 70). O MPS, entretanto, reportou medir a precisão comparando correspondências bem-sucedidas e malsucedidas com o número total de rostos processados pelo FRT, segundo essa métrica, a taxa de erro teria sido de apenas 0,1% (JEE, 2019; MANTHORPE e MARTIN, 2019). Percebe-se que a própria definição de como aferir a métrica já é, desde logo, objeto de disputa.

2.4.2 Questões éticas

A preocupação com a eficácia se estende a considerações éticas (INTRONA e NISSENBAUM, 2009, p. 5), que na verdade estão imbricadas em todos os demais desafios relacionados à FRT.

No meio acadêmico, por exemplo, é muito comum que ao publicar os resultados de uma pesquisa, sejam disponibilizados os conjuntos de dados utilizados para validação do modelo proposto. No que diz respeito à FRT, durante as décadas de 1990 e 2000, os cientistas geralmente conseguiam voluntários para posar para fotos, entretanto, atualmente, a maioria coleta imagens faciais sem pedir permissão (VAN NOORDEN, 2020, p. 355), e.g., em 2015,

[26] Isso sob a perspectiva da efetividade pois, para agravar a situação, sob o prisma da pessoa identificada erroneamente, não se pode desconsiderar, para dizer o mínimo, o constrangimento da situação.

[27] Neste trabalho, por titular dos dados, entende-se a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (art. 5º, V, LGPD) (BRASIL, 2019b).

cientistas da Universidade de Stanford, publicaram um conjunto de 12.000 imagens obtidas de uma *webcam* localizada em um café de São Francisco que transmitia as imagens *online* ao vivo (STEWART *et al.*, 2016, p. 2326, 2327, 2331). Em 2016, pesquisadores da *Duke University*, divulgaram mais de 2 milhões de *frames* de imagens, obtidas a partir de vídeos de alunos caminhando no campus da universidade (Projeto DukeMTMC[28]) (RISTANI *et al.*, 2016, p. 11; RISTANI e SOLERA, 2017; SOLERA *et al.*, 2017).

Além disso, o acesso às redes sociais (públicas ou não, autorizado ou não) permite aceder bilhões de fotos que podem ser utilizadas sem o consentimento dos titulares dos dados (AZRIA e WICKERT, 2019, p. 14). De fato, as maiores coleções de imagens foram reunidas *online*. Em 2016, pesquisadores da Universidade de Washington, em Seattle, postaram um banco de dados, chamado *MegaFace* (MF2), com 4,7 milhões de fotos obtidas do site de compartilhamento de imagens *Flickr*[29] (NECH e KEMELMACHER-SHLIZERMAN, 2017). E os cientistas da *Microsoft Research* em Redmond, Washington, divulgaram o maior conjunto de dados do mundo, o MSCeleb, com 10 milhões de imagens, retiradas da internet, de cerca de 100 mil pessoas, incluindo jornalistas, músicos e acadêmicos (GUO *et al.*, 2016). Muitas dessas bases de imagens/fotos foram compartilhadas abertamente e usadas para avaliar e melhorar produtos comerciais de vigilância (VAN NOORDEN, 2020, p. 355). Os cientistas estipulam, às vezes, que os conjuntos de dados devem ser usados apenas para pesquisas não comerciais, entretanto, uma vez que tenham sido compartilhados, é impossível impedir que as empresas os obtenham e utilizem.

A polêmica empresa de tecnologia *Clearview AI* teria montado um banco contendo mais de 3 bilhões de imagens retiradas da internet, e.g., de sites de empregos e de redes sociais (usando uma técnica chamada *scraping*[30] – ainda que isso viole os Termos de Uso de uma série de plataformas, como o *Facebook*, *Linkedin*, *Twitter*, *Instagram*, *YouTube*) (HILL, 2020; O'SULLIVAN, 2020). Cumpre ressaltar que as fotos permanecem na base de dados da *Clearview* mesmo quando os usuários das redes sociais de onde foram retiradas as apagam ou tornam seus perfis privados. Esse banco de fotos estaria acessível a mais de 600 agências governamentais de todo o mundo. Matéria do *The New York Times* relata que o repórter pediu a vários policiais que o procurassem no aplicativo *Clearview*; pouco tempo depois, os policiais receberam telefonemas de representantes da empresa perguntando se eles estavam conversando com a mídia, um indício que a *Clearview* também esteve monitorando quem a polícia estava procurando, i.e., estes dados sugerem que ao checarem imagens no aplicativo, as forças policiais estão enviando-as para os servidores da empresa, cuja capacidade de proteger os dados não foi testada/comprovada (HILL, 2020).

---

[28] Segundo os pesquisadores, o Projeto DukeMTMC visa a acelerar os avanços no rastreamento de múltiplas câmeras de múltiplos alvos. Trata-se de um sistema de rastreamento que funciona dentro e entre câmeras, um conjunto de dados de vídeo de alta definição (*high definition*, HD) gravado por 8 câmeras sincronizadas com mais de 7.000 trajetórias de câmeras únicas, mais de 2.000 identidades exclusivas e um método de avaliação de desempenho que mede a frequência em que o sistema está correto sobre quem está onde.

[29] O *Flickr* é uma espécie de *flog* (*blog* de fotos), um site de hospedagem e compartilhamento de imagens como fotografias, desenhos e ilustrações que pertence desde 2005 à Yahoo! Inc.

[30] Também conhecido pelo termo "coleta de dados" ou "raspagem" é uma forma de extração de dados de sites da *web* convertendo-os em informação estruturada para posterior uso/análise.

Em setembro de 2019, um artigo científico, publicado em 2018, foi denunciado pelo uso controverso da FRT. O estudo mostrava o resultado do treinamento de algoritmos para distinguir os rostos do povo *Uygur* (uma minoria étnica predominantemente muçulmana na China), daqueles de etnia coreana e tibetana (VAN NOORDEN, 2020, p. 354). Importante mencionar que a China já foi condenada internacionalmente por sua forte vigilância e detenções em massa de *Uygur* em campos na província de *Xinjiang* (que o governo diz serem centros de reeducação destinados a reprimir o movimento terrorista) (LE MONDE, 2018).

Relatório de 2019 (AZRIA e WICKERT, 2019, p. 14), apresentado no âmbito da *Convention 108+*, aponta que há especial motivo para preocupação com o **reconhecimento facial de emoções** (*facial emotion recognition*, FER)[31] ou, mais adequadamente, **reconhecimento de expressão facial** (*facial expression recognition*) (BUOLAMWINI *et al.*, 2020, p. 5), uma **subclasse de reconhecimento facial** também referenciada como **reconhecimento afetivo** (*affective computing*) que busca reconhecer e interpretar emoções humanas com base em imagens ou vídeos de rostos, e.g., personalidade, sentimentos, saúde mental, "envolvimento do trabalhador" (VEMOU e HORVATH, 2021). Essa ideia tem se mostrando atraente para corporações e governos, embora as conclusões a que cheguem sejam bastante questionáveis (BARRETT *et al.*, 2019) e tendo em vista o enorme potencial de uso para fins discriminatórios[32].

Não basta denunciar os usos controversos da FRT, é necessário, também, reconhecer os fundamentos moralmente duvidosos de trabalhos acadêmicos, inclusive estudos que coletam enormes conjuntos de dados de imagens de rostos de pessoas sem consentimento, muitos dos quais ajudam a aprimorar algoritmos de vigilância comercial ou militar (VAN NOORDEN, 2020, p. 354-355), como evidenciado pela pesquisadora do *Massachusetts Institute of Technology* (MIT), Chelsea Barabas, "se você projeta um algoritmo de reconhecimento facial para pesquisa médica sem pensar em como ele poderia ser usado pela polícia, por exemplo, você está sendo negligente" (VAN NOORDEN, 2020, p. 358).

É importante destacar que determinadas aplicações de FRT não podem ser corrigidas simplesmente introduzindo dados de treinamento mais diversos, aumentando a precisão ou aplicando métodos técnicos para reduzir vieses. O problema está na origem: o objetivo do emprego da FRT em determinadas situações é, no seu cerne, incompatível com direitos fundamentais (LEUFER, 2021).

2.4.3 Vieses e discriminação

Rodotá (2008, p. 78, 96) destaca que dados pessoais sensíveis, precisamente por seu caráter "estrutural e permanente", integram o "núcleo duro" da privacidade e da proteção de

[31] A FER não é foco deste trabalho, mas colateralmente, será tratada, e.g., no Caso do Metrô de São Paulo (Seção 4.1).

[32] Pesquisadores encontraram apenas uma associação fraca entre emoções e expressões faciais, ressalvando que as expressões faciais variam entre culturas e contextos, tornando o reconhecimento de emoções suscetível a preconceitos e interpretações errôneas (HEAVEN, 2020; UN, 2021, § 28).

dados, devendo ser protegidos de forma mais rígida, pois pelo tipo e natureza de informação que carregam, seu tratamento pode ocasionar a discriminação de seu titular.

Preocupações quanto ao potencial viés racial e de gênero dentro da FRT já foram levantadas (BUOLAMWINI e GEBRU, 2018, p. 2-3). Um relatório do *National Institute of Standards and Technology* (NIST), o Inmetro[33] dos Estados Unidos, informou que a maioria dos algoritmos de reconhecimento facial tem diferentes níveis de precisão entre os grupos demográficos (CAMPBELL, 2018, p. 9-10; GROTHER *et al.*, 2019, p. 6-8).

Pares de fotos da mesma pessoa são apresentados ao algoritmo FRT durante o treinamento; com o tempo, o algoritmo aprende a "se concentrar" nas características mais relevantes. Se um conjunto de dados de treinamento for composto por mais amostras representando um determinado grupo, o algoritmo pode aprender a identificar melhor os membros daquele grupo (BUOLAMWINI e GEBRU, 2018, p. 9).

Inversamente, tem-se o comportamento semelhante ao "efeito de outra raça", um fenômeno no qual as pessoas têm dificuldade em distinguir os indivíduos de uma raça diferente da sua (ANU, 2019; McKONE *et al.*, 2019, p. 1). Estudos demonstraram que a FRT identificou incorretamente "pessoas pretas e minorias étnicas, jovens e mulheres" em taxas mais altas do que "homens brancos adultos" (BUOLAMWINI e GEBRU, 2018, p. 2-3; BFEG, 2019, p. 2). Os primeiros desencadeiam mais reconhecimento falsos positivos, e esse tipo de imprecisão tem impacto sobre a "presunção de inocência", colocando sobre essas pessoas o ônus de mostrar que não são quem a FRT identifica (LYNCH, 2018, p. 10).

A Rede de Observatórios da Segurança[34] monitorou casos de prisões e abordagens com o uso de FRT em cinco estados brasileiros (Bahia, Ceará, Pernambuco, Rio de Janeiro e São Paulo), desde sua implantação em março de 2019 até outubro do mesmo ano e constatou – nos casos para os quais havia informações[35] – que 90,5% das pessoas presas por identificação pela FRT eram negras (NUNES, 2019). Nos dizeres de Nunes (2019), a FRT "tem se mostrado uma atualização *high-tech* para o velho e conhecido racismo que está na base do sistema de justiça criminal e guia o trabalho policial há décadas".

Não se pode ignorar, também, o incidente em 2015 do *Google Photos*, no qual a FRT erroneamente rotulou/identificou pessoas pretas como "gorilas", nem o fato de que as "providências imediatas" para prevenir a repetição do erro foi o serviço de fotos do *Google*,

[33] O Instituto Nacional de Metrologia, Qualidade e Tecnologia (Inmetro) é uma autarquia federal criada pela Lei nº 5.966/1973 e integrante do Sistema Nacional de Metrologia, Normalização e Qualidade Industrial (Sismetro), com a finalidade de formular e executar a política nacional de metrologia, normalização industrial e certificação de qualidade de produtos industriais. No âmbito de sua ampla missão institucional, o Inmetro objetiva fortalecer as empresas nacionais, aumentando sua produtividade por meio da adoção de mecanismos destinados à melhoria da qualidade e da segurança de produtos e serviços (INMETRO, 2021).

[34] Iniciativa de instituições acadêmicas e da sociedade civil da Bahia, Ceará, Pernambuco, Rio de Janeiro e São Paulo dedicada a acompanhar políticas públicas de segurança e a criminalidade nesses Estados (REDE DE OBSERVATÓRIOS DA SEGURANÇA, 2021).

[35] A Rede dá conta que tentou, por meio da Lei de Acesso à Informação, obter dados acerca da quantidade oficial de prisões e do número de pessoas abordadas de forma equivocada (falsos positivos), mas não obteve resposta à solicitação de informação. A Rede teve dificuldades até mesmo para obter informações sobre o perfil das pessoas presas ou abordadas por utilização do FRT, e os motivos da eventual prisão (NUNES, 2019).

censurar por mais de 2 anos os termos de busca "gorila", "macaco" e "chimpanzé" (HERN, 2018; SIMONITE, 2018).

A questão das taxas de erro mais altas em relação a certas categorias de pessoas toca em algo muito mais profundo do que apenas uma questão de enviesamento. É a questão de quem é digno de atenção e distinção, i.e., quem é "digno de ser visto". As questões tecnológicas não podem/devem ser encaradas de maneira desconectada do quadro social mais amplo. Elas não aparecem *ex nihilo*, mas são produtos de uma certa visão do mundo[36].

Cumpre mencionar que, em muitas situações, a FRT é utilizada para categorização, inclusive de gênero, mas essa classificação geralmente parte de modelos cisgênero e binários (na qual geralmente se escolhe entre uma das opções, homem ou mulher). Essa imposição de critérios binários promove situações de transfobia, reforçando a exclusão e o estigma de pessoas transgênero e não-binárias, conflitando, inclusive, com a auto-identificação de gênero (LEUFER, 2021; SILVA e VARON, 2021, p. 29-30, 41; UN, 2021, § 14).

A categorização incluiria uma camada adicional de dano, uma vez que os indivíduos seriam **tanto vigiados quanto descaracterizados** (ACCESS NOW *et al.*, 2021, p. 2). Ademais, a categorização pode também levar ao *profiling* (perfilhamento, perfilação ou definição de perfis[37]) que tem o potencial de criar sérios riscos na medida em que pode diminuir ou aumentar oportunidades sociais em aspectos relevantes da vida da pessoa (e.g., trabalho, habitação, crédito, justiça criminal) conforme a categorização ou o *score* atribuído ao perfil em questão (MENDES e FONSECA, 2021, p. 99). E muitas vezes, não devido a algo que o indivíduo tenha efetivamente feito, mas por causa das inferências ou correlações feitas por algoritmos "sugerindo" que ele pode vir a se comportar de maneiras que o tornam "arriscado" ou "inadequado" (CITRON e PASQUALE, 2014, p. 24; MENDES e MATTIUZZO, 2019, p. 47), i.e., os efeitos se verificam pela inclusão em um grupo e o consequente julgamento desse indivíduo, não por suas características particulares, mas pelas características do grupo no qual foi classificado (trata-se de uma generalização).

Além disso, todos os sistemas de vigilância (no qual a FRT também se inclui) têm um impacto discriminatório nas sociedades em que o racismo, heterossexismo, cis-gênero, capacidade (deficiência ou não), classismo e assim por diante, são sistêmicos e estruturais. Quando se fala em discriminação sistêmica, certas pessoas são impactadas negativamente (e outras positivamente) em sua vida cotidiana, devido à forma como são categorizadas por

[36] Segundo Barocas e Selbst (2016), ainda que se defenda que técnicas algorítmicas eliminam os preconceitos humanos no processo de tomada de decisão, um algoritmo é tão bom quanto os dados com os quais trabalha (conforme o conhecido adágio "*garbage in, garbage out*", literalmente "lixo entra, lixo sai", i.e., dados de entrada falhos produzem saídas falhas). E não raro, os dados frequentemente refletem padrões históricos de preconceito e discriminação contra minorias, i.e., padrões preexistentes de exclusão e desigualdade. Além disso, uma vez que quase sempre a discriminação resultante é uma propriedade emergente não intencional do uso do algoritmo (e não uma escolha intencional/consciente de seus programadores), pode ser particularmente difícil identificar o problema e sua origem.

[37] Segundo o art. 4º(4) do GDPR, entende-se por "definição de perfis", "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações" (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

determinados atributos, não só em nível interpessoal, mas também no nível macro, na busca por moradia, na procura de emprego, na educação, na passagem por fronteiras/imigração, no contato com a polícia etc. Concretamente, significa que a forma como a pessoa é identificada, de acordo com certos critérios (pigmentação da pele, forma de andar, o formato do nariz ou a largura dos ombros) tem impacto direto no seu acesso a recursos (ELIZONDO-URRESTARAZU, 2020). Isso tem sérias consequências quando essas mesmas tecnologias são usadas em sistemas educacionais, nas fronteiras, na aplicação da lei e em todas as áreas onde os problemas causados pela discriminação sistêmica já são fortemente documentados. Neste sentido, cada indivíduo tem o direito a não ser "simplificado, objetivado, e avaliado fora de contexto" (ROSEN *apud* RODOTÁ, 2008, p. 12).

Equipar ruas, supermercados e parques com FRT tem o potencial de ampliar a discriminação existente contra grupos marginalizados. Em vez de serem contestadas, essas práticas tendem a ser escondidas sob um véu de falsa autoridade científica e opacidade deliberada (JAKUBOWSKA, 2021).

2.4.4 Impacto nas liberdades e direitos fundamentais

A maior parte da tecnologia usada para rastrear uma pessoa visa a seus pertences, e.g., telefone celular, carro, computador. A FRT leva o rastreamento a um novo nível, eles "perseguem" o corpo da pessoa. A distinção é significativa: você pode se desfazer de seus pertences, já do seu rosto... (GARVIE *et al.*, 2016, p. 9). Assim, o risco associado à utilização de dados biométricos é significativo, pois eles representam identificadores únicos, praticamente imutáveis, que acompanham os titulares ao longo de toda a vida. Além disso, a FRT pode ser mais invasiva do que outras formas de identificação biométrica (MANN e SMITH, 2017, p, 125): ela pode fazer o rastreamento remotamente, em sigilo e em uma grande quantidade de pessoas (WOODWARD Jr *et al.*, 2003, p. 3-4).

Além do mais, mesmo que as pessoas consigam identificar quem coletou seus dados usando FRT (seja no setor público ou privado), pode ser difícil ou impossível determinar quais dados foram coletados, como foram usados, como e com quem foram compartilhados, muito menos obter acesso a eles para corrigir erros ou remover informações (AZRIA e WICKERT, 2019, p. 19). Como exemplo, em janeiro de 2019, a IBM usou e compartilhou um conjunto de cerca de um milhão de fotos disponibilizadas pelo *Flickr* sob licença *Creative Commons*[38] (que a IBM chamou de *Diversity in Faces*) (SMITH, 2019). Segundo a campanha de comunicação feita pela IBM, essa era a etapa de um projeto maior de treinamento de sua FRT, projetada com o propósito de reduzir vieses (*bias*). No entanto, constatou-se que as fotos foram compartilhadas e divulgadas sem o consentimento ou mesmo o conhecimento dos titulares dos dados. Em resposta, a IBM disse garantir o direito de *opt-out* dos usuários (pedir para serem retirados do banco de dados), entretanto, as restrições eram tamanhas, que na prática, era quase impossível remover fotos do banco de imagens (SOLON, 2019).

[38] As licenças *Creative Commons* são várias licenças públicas que permitem a distribuição (cópia e compartilhamento) gratuita de uma obra protegida por direitos autorais.

Ademais, os agentes que empregam FRT têm como objetivo adicionar "multidões, CFTV, fotografias de carteira de motorista, mídia social" aos seus dados (MANN e SMITH, 2017, p. 121). Nesse caso, qualquer pessoa, mesmo que não seja suspeita de um crime, pode acabar em um banco de dados sem seu conhecimento (STONE *et al.*, 2010, p. 1408; RECTOR e KNEZEVICH, 2016). Um bom exemplo é o *gangs violence matrix* (GVM), um banco de dados desenvolvido pela polícia de Londres. Muitos jovens negros acabaram nesse banco de dados sem nunca terem sido acusados de um crime e, às vezes, até mesmo depois de eles próprios terem sido vítimas (DODD, 2021).

Historicamente, os bancos de dados de impressões digitais e DNA foram compostos de informações de crimes ou investigações criminais. Executando buscas de reconhecimento facial, as delegacias e agências governamentais construíram uma rede biométrica que inclui principalmente pessoas que cumprem a lei; isso não tem precedentes (GARVIE *et al.*, 2016, p. 2). Um estudo de 2016 do *Georgetown Law Center on Privacy and Technology* descobriu que quase metade de todos os adultos americanos estão em algum banco de dados de reconhecimento facial da polícia, em parte por causa de acordos (i.e., sem sequer haver uma base legal de compartilhamento) que fornecem acesso a repositórios de fotos de carteiras de motorista (GARVIE *et al.*, 2016, p. 2; HARWELL, 2019).

Um dos pressupostos fundamentais para o livre desenvolvimento humano é a sensação de existência de espaços livres de observação (BIONI et al., 2020, p. 49). O anonimato pode ser entendido como um valor urbano positivo, até mesmo essencial para a ideia de urbanidade. O anonimato urbano é igual a liberdade. No espaço urbano, as pessoas realmente esperam permanecer anônimas (KOSKELA, 2002, p. 303).

Esse tipo de vigilância imposto pela FRT ameaça a liberdade de ir e vir, a liberdade de expressão e a liberdade de associação (BIG BROTHER WATCH, 2018, p. 41; UN, 2021, § 27), tendo um efeito assustador sobre a disposição de se envolver em um debate público, de divulgar publicamente opiniões políticas, de se associar a outros cuja religião valores ou visões políticas podem ser considerados diferentes da maioria, gerando o que se denomina "espiral do silêncio" (STOYCHEFF, 2016, p. 297-299) e o *chilling effect* ("efeito inibidor" ou resfriamento do engajamento civil-democrático) (COUNCIL OF EUROPE, 2013, p. 1, § 2º e p. 2, § 8º).

Na vanguarda dos métodos de aprendizado de máquina para FRT, os algoritmos estão sendo treinados para reconhecer faces parcialmente ocultas, inclusive em resposta ao uso de máscaras durante a pandemia de Covid-19 (BFEG, 2021, p. 7; GAO, 2021, p. 22, 43, 54).

Quando cada movimento do indivíduo está sujeito à inspeção por entidades cujos procedimentos e pessoal não estão submetidos ao mesmo tratamento, a promessa de democracia e mercados livres soa vazia (PASQUALE, 2015, p. 4).

O problema/dilema é que a FRT pode ser notadamente **prejudicial quando é imprecisa**, mas **assombrosamente opressiva quanto mais precisa fica**.

2.4.5 Riscos de segurança (vazamento de dados)

Como quaisquer outros dados, os dados biométricos também correm o risco de uso indevido e violação por:

1. pessoas de dentro (*insiders*), e.g., em 2013, funcionários da *National Security Agency* (NSA, Agência de Segurança Nacional dos Estados Unidos da América) foram pegos usando registros de vigilância para espionar os cônjuges, namoradas e namorados (GELLMAN, 2013; SELYUKH, 2013).
2. Pessoas de fora (*outsiders*), e.g., *hackers*. Em junho de 2019, o *UK Eurofins Forensics Services* (EFS) sofreu um ataque cibernético. O EFS lida com cerca de 90% dos testes de toxicologia forense da Inglaterra e do País de Gales (mais de 70.000 casos criminais no Reino Unido a cada ano). Foi estabelecido um resgate para desbloquear as contas sequestradas, embora não esteja claro se, ao final, o EFS o pagou (HOUSE OF COMMONS, 2019, p. 9; SHAW, 2019).

Dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[39] dão conta que, apenas durante o ano de 2020, ocorreram mais de 665 mil incidentes de cibersegurança no País (CERT.br, 2021a).

Já são conhecidas histórias de vazamento ilegal de dados sigilosos de beneficiários do Instituto Nacional do Seguro Social (INSS), diretamente atrelado aos abusos na oferta de concessão de empréstimos consignados, com efeitos desastrosos, sobretudo para aposentados que muitas vezes aceitam o crédito consignado sem compreender a situação, comprometendo por vários anos sua renda. O vazamento criminoso persiste há anos, com registro da mídia (RODRIGUES, 2010; G1, 2019a) e inclusive decisão judicial condenando o INSS pois "há repasse de dados pessoais de beneficiários do INSS a empresas que prestam serviço de intermediação de empréstimos consignados entre as instituições bancárias e eventuais interessados" (TJSP, 2019). O próprio INSS teria admitido que apesar dos esforços, as investigações não obtiveram resultados concretos, não tendo identificado o local, nem os responsáveis pelo vazamento (IDEC, 2019d, p. 3). Diante dessa insegurança, mais preocupante é a informação que a Empresa de Tecnologia e Informações da Previdência (DataPrev) – responsável pela gestão da Base de Dados Sociais Brasileira, especialmente a do INSS – começou a coletar e tratar dados biométricos dos beneficiários, inclusive comunicando, recentemente, a expansão da prova de vida por biometria facial para 5,3 milhões de beneficiários (INSS, 2021). Diante desse histórico, é razoável considerar que o vazamento dos dados biométricos dos beneficiários do INSS "deixa de ser um risco eventual, para se tornar um incidente de segurança com alta probabilidade de ocorrer" (IDEC, 2019d, p. 5; 2020).

[39] O CERT.br é um Grupo de Resposta a Incidentes de Segurança (*Computer Security Incident Response Team*, CSIRT) de responsabilidade nacional, mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), do Comitê Gestor da Internet no Brasil (CGI.br). O NIC.br é uma organização privada sem fins lucrativos criada para implementar as decisões e os projetos do CGI.br, que é o responsável por coordenar e integrar as iniciativas e serviços da Internet no país. O CERT.br mantém um conjunto de métricas públicas derivadas dos dados de notificações voluntárias de incidentes de segurança, dos dados capturados nos *honeypots* (do inglês, "pote de mel", i.e., sistema utilizado para atrair um intruso para um ambiente onde há informações falsas que aparentam ser verdadeiras) e de dados recebidos através de parceiros (CERT.br, 2021b).

Outros exemplos de risco de segurança não faltam. Teste realizado com 110 modelos de *smartphones* que usavam FRT para desbloquear o dispositivo mostrou que 42 deles (o que incluía marcas como Samsung, Sony, Nokia, Huawei, Motorola, dentre outras) podiam ser desbloqueados com uma foto de alta qualidade ou um vídeo do proprietário (CIMPANU, 2019b; 2019a).

Fato é que, como boa prática, fortes medidas de segurança, em nível técnico (relacionado à tecnologia) e organizacional (relacionado à entidade), devem ser implementadas contra a perda, o acesso ou uso não autorizado de dados durante todas as etapas do processamento (COUNCIL OF EUROPE, 2021c, p. 13).

As entidades (públicas ou privadas) que utilizam FRT devem tomar medidas para evitar ataques específicos à tecnologia, incluindo **ataques de apresentação** (apresentação de uma falsificação biométrica, e.g., uma foto ou vídeo de uma pessoa ou uma impressão digital falsa de silicone ou gelatina) (ISO e IEC, 2016) e **ataques de metamorfose** (executado pela fusão das imagens de duas faces em uma única imagem de um rosto sintético que contém características de ambas as pessoas, usando esta imagem em um passaporte, as duas pessoas são autenticadas por uma FRT) (FERRARA *et al.*, 2014; PIKOULIS *et al.*, 2021, p. 2).

Isso sem falar no compartilhamento de dados sem uma base legal, e.g., documentos vazados mostram que a Agência Brasileira de Inteligência (Abin), órgão vinculado à Presidência da República, solicitou ao Serpro, fotografias e dados de todas as CNH do País (DIAS e MARTINS, 2020). Trata-se, de um banco de dados enorme: para referência, em maio de 2020, havia 74.268.555 CNH (DENATRAN, 2021), o que correspondia aproximadamente a 35% (mais de um terço!) da população brasileira (estimada em cerca de 211,76 milhões de pessoas) (IBGE, 2021). Destaque-se que, ao lado do cadastro de pessoa física (CPF), a CNH é o único documento de identificação de cidadãos armazenado nacionalmente, com o benefício adicional de incluir a foto do portador. Pouco tempo depois, o Partido Socialista Brasileiro (PSB) ajuizou, no STF, a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 695, com pedido de suspensão do compartilhamento da CNH entre Abin e Serpro, dentre outros motivos, por subverter "a finalidade para a qual os dados pessoais foram inicialmente coletados, destinando-os a um órgão e a um propósito inteiramente incompatíveis com a motivação original" (STF, 2020).

Um exemplo bastante atual do risco de segurança diz respeito à situação no Afeganistão, após a tomada do país pelo Taleban, ocorrida com a saída das tropas americanas do território afegão (em agosto de 2021). O banco de dados biométrico do Ministério do Interior do Afeganistão, chamado de *Afghan Automatic Biometric Identification System* (AABIS, Sistema de Identificação Biométrica Automática Afegão) montado com auxílio do Departamento de Defesa dos Estados Unidos da América (*US Department of Defense*, DoD), pretendia cobrir 80% da população afegã até 2012, o que corresponderia a cerca de 25 milhões de pessoas. Embora não haja informações publicamente disponíveis sobre quantos registros esse banco de dados contém atualmente, há estimativas que situam a quantidade em pelo menos 8,1 milhões de registros. O AABIS foi amplamente usado de várias maneiras pelo governo do Afeganistão anterior à tomada de poder pelo Taleban. As inscrições para empregos e funções governamentais na maioria dos projetos exigiam uma verificação biométrica do sistema para

garantir que os candidatos não tinham antecedentes criminais ou terroristas. Verificações biométricas também foram exigidas para os pedidos de passaporte, identidade nacional e carteira de motorista, bem como registros para o exame de admissão à faculdade do país. Não haveria política de exclusão ou retenção de dados - nem mesmo em situações de contingência, como a tomada pelo Taleban. Para agravar a situação, enquanto o Taleban varria o Afeganistão em agosto de 2021, rapidamente circularam relatórios de que eles também haviam capturado dispositivos biométricos militares dos Estados Unidos da América (EUA) usados para coletar dados como varreduras da íris, impressões digitais e imagens faciais, bem como informações de bancos de dados e não se tem ideia de como esses aparatos serão usados com relação à população (GUO e NOORI, 2021).

De qualquer forma, como mencionado, a biometria é única para a pessoa e não pode ser alterada facilmente, portanto, as consequências de uma violação do reconhecimento facial podem ser mais graves do que de outros dados de identificação (LYNCH, 2018, p. 11).

3. APLICAÇÃO DA LGPD AO RECONHECIMENTO FACIAL

3.1 Videovigilância: a atualização e universalização do Panóptico

Uma câmera é um instrumento óptico que captura uma imagem visual. A obtenção da imagem facial (rosto de um indivíduo) utilizada pela FRT tem uma ligação umbilical com esse dispositivo. Tendo em vista o recorte de espaço público deste estudo e que muitas das imagens utilizadas na FRT têm origem em equipamentos de videovigilância, esta Seção explorará um pouco mais de perto esta "simbiose", aproveitando-se dela para tratar das questões de proteção de dados propriamente ditas.

O monitoramento em espaços abertos não é recente, segundo Vitalis (1998, p. 26), os primeiros sistemas de videovigilância na Europa foram instalados no início da década de 1970, visando a controlar o tráfego, combater assaltos a bancos e a estabelecimentos comerciais de luxo. Durante os anos 1980, tais sistemas se espalharam por transportes coletivos, comércio, locais de trabalho, prédios públicos; prosseguindo sua expansão nos anos 1990 por estádios e vias públicas. Esse cenário se repetiria em diversas outras regiões do mundo. Dados de 2019, mostram que das 10 cidades com mais câmeras de rua por pessoa, 8 estão na China (com *Chongqing*, *Shenzhen*, Xangai, *Tianjin* e *Ji'nan*, liderando o ranking), Londres está em 6º lugar e Atlanta em 10º[40] (KEEGAN, 2019).

As tecnologias de videovigilância podem limitar as possibilidades de movimento anônimo e geralmente limitam a possibilidade de passar despercebido. O espaço urbano não é um espaço de coerção porque estar nele é – pelo menos ostensivamente – voluntário. No entanto, se se quisesse evitar a vigilância, seria impossível viver em uma cidade contemporânea (KOSKELA, 2002, p. 300). Fato é que as câmeras de monitoramento utilizadas em sistemas eletrônicos de segurança estão em todos os lugares – escolas, shoppings, aeroportos, ruas, praças e parques – e há muito se apresentam como um fato cotidiano, não como uma opcionalidade. São um fenômeno cada vez mais recorrente, de tal forma que, hoje em dia, é difícil estar em áreas de circulação pública sem deparar-se com elas (muitos, inclusive, já as consideram como "parte do mobiliário de rua").

Entretanto, a videovigilância deixou de ser epitomizada por uma câmera no topo de um poste, não se trata mais de uma tecnologia passiva que apenas registra e retém imagens. Agora é uma tecnologia pró-ativa que pode ser usada para identificar pessoas e manter registros detalhados de suas atividades. As implicações à proteção de dados são enormes (EDPB, 2019, p. 4). Dessa forma, tem despertado a preocupação pública pois não é mais utilizada exclusivamente para manter as pessoas e suas propriedades seguras, mas cada vez mais para coletar evidências para informar outras decisões, e.g., no Reino Unido pode respaldar a elegibilidade de uma criança para frequentar uma escola em uma determinada área (ICO, 2017, p. 3).

[40] (1º) *Chongqing*, China (168 câmeras por 1.000 habitantes); (2º) *Shenzhen*, China (159 câmeras por 1.000 habitantes); (3º) Xangai, China (113 câmeras por 1.000 habitantes); (4º) *Tianjin*, China (93 câmeras por 1.000 habitantes); (5º) *Ji'nan*, China (74 câmeras por 1.000 habitantes); (6º) Londres, Reino Unido (68 câmeras por 1.000 habitantes); (7º) *Wuhan*, China (60 câmeras por 1.000 habitantes); (8º) *Guanczou*, China (53 câmeras por 1.000 habitantes); (9º) Pequim, China (40 câmeras por 1.000 habitantes); (10º) Atlanta, EUA (16 câmeras por 1.000 habitantes) (KEEGAN, 2019).

De acordo com a *European Data Protection Supervisor* (EDPS, Autoridade Europeia para a Proteção de Dados), videovigilância pode ser definida como (EDPS, 2010, p. 7):

> the monitoring of a specific area, event, activity, or person by means of an electronic device or system for visual monitoring. Typically the Institutions operate CCTV systems, that is, "closed circuit television systems" comprising of a set of cameras monitoring a specific protected area, with additional equipment used for transferring, viewing and/or storing and further processing the CCTV footage. However, using any other electronic device or system, fixed or mobile, also comes under the scope of the Guidelines [on video-surveillance] if it is capable of capturing image data. For example, portable videocameras, cameras taking still images, webcams, infra-red cameras and heat recognition devices[41].

Como corolário dessa definição, tem-se que a videovigilância inclui, também (ICO, 2017, p. 6, 30):

- Reconhecimento automático de número de placa (*Automatic Number Plate Recognition*, ANPR);
- Câmera usada no corpo ou integradas a vestimentas (*body worn video*, BWV);
- Sistemas aéreos não tripulados (*unmanned aerial systems*, UAS): todo sistema sob o qual os *unmanned aerial vehicles* (veículos aéreos não tripulados, UAV) operam, e.g., *Remotely Piloted Aircraft Systems* (RPAS, Sistemas de Aeronaves Pilotadas Remotamente) e drones; e
- Outros sistemas que capturam informações de indivíduos identificáveis ou informações relacionadas a indivíduos.

A maneira como as informações coletadas por essas tecnologias podem ser vinculadas ou combinadas significa que as tecnologias de vigilância estão se tornando mais interconectadas (ICO, 2017, p. 26). E seu uso pode ser bastante intrusivo na medida em que são capazes de colocar um grande número de pessoas que cumprem a lei sob vigilância e registrar seus movimentos enquanto estas pessoas realizam suas atividades diárias (ICO, 2017, p. 9).

Muitos autores que analisam as atuais câmeras de monitoramento aproximam-nas do Panóptico. Descrito pela primeira vez pelo jurista britânico Jeremy Bentham, no século XVIII, o Panóptico é originalmente um projeto de prisão na qual os prisioneiros ficariam encarcerados em celas individuais, ordenadas em círculo, ao redor de uma torre central, onde estaria localizado, estrategicamente, o responsável pela vigilância. Todos os detentos seriam visíveis a quem os vigiasse, mas o contrário não é verdadeiro, cada prisioneiro só teria a certeza da onipresença da torre, mas não veria o vigia, de maneira que sua presença ou ausência seria uma incógnita (FOUCAULT, 2013, p. 155-158). Da mesma forma, os cidadãos no espaço urbano

[41] "o monitoramento de determinada área, evento, atividade ou pessoa por meio de dispositivo eletrônico ou sistema de monitoramento visual. Normalmente as Instituições operam sistemas de CFTV, ou seja, "sistemas de circuito fechado de televisão" compostos por um conjunto de câmeras que monitoram uma área protegida específica, com equipamentos adicionais utilizados para transferência, visualização e/ou armazenamento e posterior processamento das imagens de CFTV. No entanto, a utilização de qualquer outro dispositivo ou sistema eletrônico, fixo ou móvel, também se enquadra no escopo das Diretrizes [de videovigilância] se for capaz de capturar dados de imagem. Por exemplo, videocâmeras portáteis, câmeras tirando fotos, *webcams*, câmeras infravermelhas e dispositivos de reconhecimento de calor" (livre tradução).

verão câmeras de vigilância colocadas em posições visíveis, lembrando-os constantemente sobre sua própria visibilidade.

Este seria o principal efeito do Panóptico: por uma simples ideia de arquitetura, fazer com que os prisioneiros se sentissem vigiados, ainda que não estivessem sendo diretamente observados, ou mesmo, que não houvesse vigia algum na torre central. Em suma, o poder "não teria mais necessidade de se impor efetivamente", o primordial é a ideia de uma permanente visibilidade, de maneira que o resultado de todo dispositivo panóptico é a desindividualização do poder, convertendo-o numa máquina anônima. **E o que seriam os modelos de sistema de vigilância senão a atualização e universalização do Panóptico?** Ficção de policiamento cultivada pela proliferação das "máquinas de vigiar", realizando o mesmo papel da máquina benthamiana, difusa e centralizadora, estabelecendo um sistema abstrato de disciplinamento de toda a sociedade (MACHADO, 1990, p. 25-26; FUCHS, 2011, p. 116-119).

Assim, dispositivos eletrônicos de vigilância generalizam para toda a sociedade métodos de coerção nascidos no interior de presídios ou antes apenas usados na investigação ou repressão policial (MACHADO, 1990, p. 26). Obviamente, o propósito de câmeras de vigilância é exercer poder: para "controlar o comportamento desviante", para "reduzir o crime" e para "manter as cidades seguras". No entanto, com este controle ostensivo vêm outras formas de poder, intencionais ou não. A política de ver e ser visto é complexa (KOSKELA, 2002, p. 295).

A colocação de avisos sobre a presença das câmeras tem como finalidade declarada a proteção da privacidade e intimidade, mas muitas vezes, possui, também, a função não declarada de "inibir a atuação daqueles que pretendem cometer ato ilegal". Desta forma, a já corriqueira mensagem "Sorria, você está sendo filmado", antes do que de fato uma proteção à privacidade, à individualidade humana ou à intimidade, funciona à guisa de um "consentimento informado" coletivo da vigilância permanente nesses locais (KANASHIRO, 2006, p. 59-60).

O olhar de uma câmera de vigilância é "calculado para excluir". Uma câmera representa unidirecionalidade total do olhar, tornando impossível "olhar de volta". O indivíduo pode ver as câmeras, mas a reciprocidade do contato visual é impraticável. Não há "olhar mútuo". A natureza do potencial de visualização é "semelhante a Deus", alguém que está lá e, simultaneamente, não está. Só se pode ser o observado, mas não o observador (KOSKELA, 2002, p. 298). É o "one-way mirror" de Pasquale (2015, p. 9, 17), no qual determinados atores têm conhecimento sem precedente das vidas diárias dos indivíduos, sem que estes saibam nada acerca de como esse conhecimento é utilizado.

Mesmo que alguém veja uma câmera de vigilância, nunca saberá se há alguém por trás dela. A partir da localização da câmera, é impossível inferir a localização do observador, uma vez que é tecnicamente possível colocar a sala de monitoramento em outro andar, prédio, cidade, ou mesmo país (KOSKELA, 2002, p. 299).

A vigilância como experiência emocional evoca uma variedade de sentimentos: os "objetos" observados podem se sentir culpados sem motivo, constrangidos ou inquietos, envergonhados, irritados, com medo; mas também protegidos e seguros. A culpa e o constrangimento garantirão o (auto)controle. A experiência emocional de estar sob vigilância

costuma ser ambivalente (KOSKELA, 2002, p. 300). Estar constantemente consciente de ser observado por supervisores invisíveis leva à internalização do controle. As pessoas internalizam as regras, regulam seu próprio comportamento mesmo quando não é necessário e, assim, exercem poder sobre si mesmas. Consequentemente, a natureza panóptica da videovigilância impõe autovigilância (KOSKELA, 2002, p. 299).

Além disso, a tecnologia de vigilância aparentemente inofensiva é usada em regimes não democráticos e para policiar grupos e movimentos indesejáveis (KOSKELA, 2002, p. 303). E cada vez mais sem exibir seu aspecto ostensivo, i.e., sem que as pessoas saibam que estão submetidas a vigilância.

E justo por este aspecto, de nem sempre exigir a ciência ou cooperação dos indivíduos cujos dados biométricos são processados, a integração de FRT à videovigilância representa um risco adicional para os direitos à privacidade, à proteção de dados pessoais, bem como para outros direitos fundamentais (COUNCIL OF EUROPE, 2018, p. 3) (Seção 2.4.4).

3.1.1 Videovigilância no Brasil

De acordo com Kanashiro (2006, p. 48-49), no Brasil, o registro mais antigo de regulamentação quanto ao uso de videovigilância é a Lei nº 7.102/1983 (ainda em vigor), que "[d]ispõe sobre segurança para estabelecimentos financeiros, estabelece normas para constituição e funcionamento das empresas particulares que exploram serviços de vigilância e de transporte de valores, e dá outras providências" (BRASIL, 1983).

O Projeto de Lei do Senado Federal (PLS) nº 168/2005, que pretendia atualizar a Lei nº 7.102/1983 consigna em sua justificação que o motivo para a proposição da Lei foi que diante da "impossibilidade constitucional, legal e operacional de os órgãos de segurança pública prestarem os serviços de segurança, principalmente de natureza patrimonial, demandados pelos estabelecimentos financeiros privados, **a alternativa viável foi a atribuição, por lei, à iniciativa privada da competência para a organização e prestação desses serviço**" (SENADO FEDERAL, 2005, p. 12, grifo meu).

Por meio da propagação do discurso de aumento da violência, do medo e da ineficiência do Estado justifica-se a narrativa segundo a qual a segurança é transformada em responsabilidade individual e privada (privatização da segurança), adquirindo cunho mercadológico (pode ser vendida e comprada)[42] (KANASHIRO, 2006, p. 52, 65). Assim, a narrativa de utilização dos equipamentos de vigilância se apoia em noções de risco, prevenção e segurança[43].

[42] Trata-se de um mercado que movimenta R$ 36,9 bilhões no Brasil (FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA, 2020, p. 261) e que chega a US$ 132 bilhões no mundo (STATISTA, 2021).

[43] Curioso apontar que o fator econômico entra em diversas facetas, e.g., uma realidade que não se pode ignorar é que, às vezes, a força motivadora da instalação de videovigilância se deve à oferta de melhores condições na contratação de seguro (apólices mais baratas), caso haja este tipo de "mecanismo de segurança" presente (WP29, 2004, p. 3).

A Lei nº 7.102/1983 veda o funcionamento de estabelecimentos financeiros onde haja guarda de valores ou movimentação de numerário, que não possuam sistema de segurança aprovado pelo Ministério da Justiça (art. 1º, Lei 7.102/1983); e determina que esse sistema deve incluir (BRASIL, 1983):

> Art. 2º [...] pelo menos, mais um dos seguintes dispositivos:
> I - **equipamentos elétricos, eletrônicos e de filmagens que possibilitem a identificação dos assaltantes**;
> II - artefatos que retardem a ação dos criminosos, permitindo sua perseguição, identificação ou captura; e
> III - cabina blindada com permanência ininterrupta de vigilante durante o expediente para o público e enquanto houver movimentação de numerário no interior do estabelecimento.

Desta forma, não obstante ser apenas um dos três tipos de dispositivo para segurança propostos, as câmeras são trazidas ao cenário da legislação brasileira a contar dessa Lei, que as conecta ao aumento da segurança e à possibilidade de identificação de criminosos.

Kanashiro (2006, p. 48, 62) aponta, ainda, que os projetos de lei que trataram de câmeras de monitoramento, a partir de 1996, em sua quase totalidade, previram sua obrigatoriedade para vigilância em locais como "instituições financeiras, escolas, hospitais, shoppings centers, estádios de futebol, postos de gasolina, portos, ruas e avenidas, entre outros locais" (espaços públicos). Essa fase é dominada por ideias de "obrigatoriedade, aprimoramento, adjetivação e qualificação" da presença de videovigilância, bem como **seu deslocamento para espaços abertos ou de grande circulação pública**; por fim, aponta uma sinergia com os interesses do empresariado do setor de segurança privada, formulando e intensificando o caráter de mercadoria da segurança.

A título de exemplo, a primeira lei do Estado de São Paulo a tratar da instalação e monitoramento de câmeras de vigilância (Lei nº 9.967/1998), autorizou o Poder Executivo a celebrar convênio "com a Prefeitura do Município de São Paulo, visando à instalação, monitoramento e uso para fins de preservação da ordem pública e investigação policial, de câmeras de vídeo instaladas em pontos de grande circulação de pessoas, cruzamentos de vias públicas consideradas de alta periculosidade, estádios de futebol e outros assim considerados" (art. 1º, Lei nº 9.967/1998 do Estado de São Paulo) (ASSEMBLEIA LEGISLATIVA DE SÃO PAULO, 1998). Curioso pontuar que o Projeto de Lei SP nº 12/1997 que foi convertido na referida Lei, trouxe em sua justificação conteúdos relacionados à identificação do assaltante; promoção da segurança; baixo custo; denúncia; combate ao crime e preservação da ordem pública; ampliando as funções e usos das câmeras para espaços abertos de circulação pública (ASSEMBLEIA LEGISLATIVA DE SÃO PAULO, 1997, p. 2).

Outro exemplo, a Lei nº 10.935/2004 (BRASIL, 2004b) abriu crédito extraordinário para a implantação de novos sistemas de segurança nos portos nacionais exigidos pelo Código de Segurança para Portos e Embarcações (ISPS-Code) e pela Organização Marítima Internacional (OMI), da qual o Brasil é membro com vistas à "realização de obras e implantação de equipamentos de segurança nos portos nacionais, mediante a construção de muros, guaritas, cercas e portões; **instalação de câmeras, computadores, monitores e redes lógicas**" (BRASIL, 2004a, grifo meu), incluindo, assim, o monitoramento e a adequação a um

modelo de segurança para o comércio internacional, associado ao ideário mundial de segurança, que ganhou força após o atentado terrorista de 11 de setembro de 2001, nos Estados Unidos. O período de "combate ao terrorismo" apresenta mecanismos de monitoramento, vigilância e controle de acesso como imprescindíveis para a sobrevivência.

Mas se na década de 1990, Machado (1990, p. 26) dizia que:

> [...] na prática é impossível exercer uma vigilância direta sobre instituições sociais, dada a magnitude estatística dos observados. Imagine-se o aparato que seria necessário para vigiar todas as conversas telefônicas de uma megalópole como São Paulo, ou para censurar todas as cartas que passam pelos seus serviços de correios. A densidade demográfica dos grandes centros urbanos não autoriza mais esquemas de controle direto baseados no poder de uma autoridade central [...]

com o processamento de Big Data[44], com o armazenamento em nuvem, com a Inteligência Artificial, com a Internet das Coisas (*Internet of Things*, IoT) e a emergência constante de novas tecnologias, isso não é mais inteiramente verdade. Além disso, se antes o receio era o *Big Brother* representado pelo Estado[45], a ele se junta o temor das *Little Sisters* (empresas que em seus nichos concentram uma quantidade enorme de informação acerca dos indivíduos) (FUCHS, 2011, p. 119-123; COHEN, 2013, p. 1916, 1921-1923; ZUBOFF, 2019; UN, 2021, §§ 13 e 30).

3.2 Videovigilância e proteção de dados

Não foi encontrado um quadro legislativo primário (específico) ou normativos regendo a videovigilância no Brasil no que diz respeito à proteção de dados, assim, esta Seção (e seguintes) se apoiará na legislação internacional, sobretudo a europeia (da Comunidade Europeia e do Reino Unido), fazendo-se as adaptações à realidade brasileira quando apropriado (em especial no que diz respeito à transposição à aplicação da LGPD).

Em geral, fala-se muito em segurança como um bem maior e desejável (CAIAFA, 2016, p. 7), mas é necessário ir além do senso comum que as câmeras são "facilidades tecnológicas" que auxiliam na prevenção da violência, dos crimes e de depredações, como se fosse uma questão de *tradeoff* entre privacidade e segurança, baseada na concepção que esses elementos seriam intercambiáveis e a troca fosse inevitável (KANASHIRO, 2006, p. 9). Não se trata de uma situação binária, onde só se pode alcançar uma situação renunciando-se à outra.

---

[44] O cenário que está colocado não diz respeito apenas ao tamanho (quantidade, volume) dos dados, mas, sobretudo, à aptidão de converter em dados (informação relevante, utilizável, significativa) aspectos do mundo que até então jamais haviam sido quantificados (MAYER-SCHONBERGER e CUKIER, 2013).

[45] Quanto a isso a reflexão do Ministro Ricardo Lewandowski do STF: "Penso que o maior perigo para a Democracia nos dias atuais não é mais representado por golpes de Estado tradicionais, perpetrados com fuzis, tanques ou canhões, mas pelo progressivo controle da vida privada dos cidadãos, levado a efeito por governos de distintos matizes ideológicos, mediante a coleta maciça e indiscriminada de informações pessoais, incluindo, de maneira crescente, o reconhecimento facial. E esses dados são submetidos ao novo instrumental da tecnologia de informações denominado big data, que consegue armazenar, interligar e manipular uma enorme quantidade de dados, para o bem ou para o mal" (BRASIL, 2020c, p. 79-80).

Como visto na Seção 2.1, o art. 5º, I, da LGPD define "dado pessoal" como informação relacionada a pessoa natural identificada ou identificável, em complementação, traz-se, abaixo a definição de "dado pessoal" segundo o art. 4º(1) do GDPR (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016, grifo meu):

> Artigo 4º Definições
> Para efeitos do presente regulamento, entende-se por:
> 1) «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, **direta ou indiretamente**, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

As implicações dessas definições no contexto de videovigilância são (EDPS, 2010, p. 8-9):

1) As **imagens faciais reconhecíveis sempre constituem dados pessoais**, i.e., mesmo que os indivíduos não sejam conhecidos ou não sejam identificados pelo operador do sistema.
2) Mesmo imagens menos claramente visíveis de um indivíduo podem constituir dados pessoais, desde que os indivíduos sejam direta ou indiretamente (i.e., combinado com outras informações) identificáveis.
3) Além disso, imagens de vídeo contendo objetos que podem estar vinculados a um indivíduo também podem ser consideradas como dados pessoais, dependendo das circunstâncias, e.g., placa de um carro.
4) Por fim, mesmo que não se pretenda capturar imagens que sejam capazes de identificar as pessoas registradas pelas câmeras, **se essas pessoas são identificáveis, tem-se um dado pessoal**.

Em termos práticos, se os indivíduos são capazes de ser identificados (direta ou indiretamente) a partir do sistema de vigilância, trata-se de informação pessoal sobre o indivíduo em questão (ICO, 2017, p. 19; EDPS, 2021c) e deve-se, portanto, seguir os preceitos constantes da LGPD, em especial seus princípios gerais (art. 6º), para que seja reconhecida a licitude da atividade (MULHOLLAND, 2018, p. 163). Estariam excluídas: (i) a utilização para fins domésticos (art. 4º, I, LGPD)[46]; (ii) o uso de câmeras convencionais (não CFTV) para fins exclusivamente jornalísticos (no entanto, a LGPD aplica-se às informações coletadas pelos sistemas de vigilância fornecidas à imprensa), artísticos (e.g., para fazer filmes) ou acadêmicos (art. 4º, II, LGPD)[47]; (iii) as atividades de vigilância realizadas por autoridades públicas porque regidas por normativo específico (art. 4º, III, LGPD).

[46] Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais: I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

[47] Art. 4º [...] II - realizado para fins exclusivamente: a) jornalístico e artísticos; ou b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11 desta Lei;

Ainda que o uso de sistemas de vigilância limitado a fins particulares e não econômicos possa estar livre da incidência da LGPD (art. 4º, I, LGPD), entende-se que essa isenção deve ser interpretada de forma estrita, e.g., uma câmera ao captar imagens fora da propriedade particular do indivíduo não estaria ao abrigo desse dispositivo.

Essa discussão já foi empreendida na Europa, oportunidade em que o Tribunal de Justiça da União Europeia (*Court of Justice of the European Union*, CJEU) no julgamento do caso *František Ryneš v Úřad pro ochranu*, de 11 de dezembro de 2014, concluiu que, quando uma câmera de vigilância voltada para o exterior de uma propriedade privada domiciliar capta imagens de indivíduos além dos limites da propriedade, especialmente quando monitoram um espaço público, a gravação não pode ser considerada para um propósito puramente pessoal ou doméstico (CJEU, 2014, §§ 33 e 35). Isso incluiria qualquer câmera que cobrisse, mesmo que parcialmente, um espaço público, e.g., calçada, rua, ou mesmo áreas como o jardim do vizinho. Esta decisão não significa que o uso de tal câmera não seja possível, mas significa que os indivíduos terão que garantir que seu uso seja legítimo sob a Diretiva nº 95/46/EC (atualmente, o GDPR).

Por sua pertinência, são trazidos abaixo os 12 princípios orientadores para o emprego de videovigilância enunciados pelo ICO (2017, p. 43-44):

1. Deve ter sempre um propósito específico, que vise a um objetivo legítimo e atenda a uma necessidade urgente identificada.
2. Deve levar em consideração seu efeito sobre os indivíduos e sua privacidade, com revisões regulares para garantir que seu uso continue a ser justificado.
3. Deve haver tanta transparência quanto possível, incluindo a informação de um ponto de contato para acesso a informações e reclamações.
4. Deve haver uma clara responsabilidade e responsabilização por todas as atividades, incluindo coleta, manutenção e utilização de imagens e informações.
5. Regras, políticas e procedimentos claros devem estar em vigor antes que a videovigilância seja usada e eles devem ser comunicados a todos que precisam cumpri-los.
6. Não devem ser armazenadas mais imagens e informações do que as estritamente necessárias para o propósito declarado, e tais imagens e informações devem ser descartadas assim que seus propósitos forem atingidos.
7. O acesso às imagens e informações retidas deve ser restrito e deve haver regras claramente definidas sobre quem pode obter acesso e para que finalidade esse acesso é concedido; a divulgação de imagens e informações somente deve ocorrer quando for necessária para tal fim ou para fins de aplicação da lei.
8. Os operadores devem levar em consideração quaisquer padrões operacionais, técnicos e de competência aprovados e relevantes para a videovigilância e trabalhar para atender e manter esses padrões.
9. As imagens e informações devem estar sujeitas a medidas de segurança apropriadas para proteção contra acesso e uso não autorizados.

10. Deve haver mecanismos eficazes de revisão e auditoria para garantir que os requisitos legais, políticas e padrões sejam cumpridos na prática, e relatórios regulares devem ser publicados.
11. Quando o uso da videovigilância visa a um objetivo legítimo e há necessidade premente de seu uso, ela deve ser empregada da maneira mais eficaz para apoiar a segurança pública e a aplicação da lei com o objetivo de processar imagens e informação de valor probatório.
12. Qualquer informação usada para dar suporte à videovigilância que se compare a um banco de dados de referência para fins de correspondência (*matching*) deve ser precisa e mantida atualizada.

Tendo estabelecido que a videovigilância lida com dados pessoais, nas próximas seções buscar-se-á mostrar que quando associada à FRT ela lida com dados pessoais sensíveis.

Esta distinção é importante, pois o contexto do processamento de imagens é relevante para a determinação da natureza sensível dos dados, uma vez que nem todo processamento de imagens envolve o processamento de dados sensíveis (COUNCIL OF EUROPE, 2018, p. 3). Nesse sentido, o Considerando 51, do GDPR enuncia que "[...] [o] tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular [...]" (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

3.3 Um passo adiante: da videovigilância para o reconhecimento facial

O termo "vigilância distribuída" é usada por Bruno (2009, p. 2-3) para caracterizar os regimes de vigilância da atualidade. A autora aponta que nas sociedades contemporâneas, os "propósitos, funções e significações" da vigilância são mais heterogêneos (não se restringindo mais apenas ao aspecto "segurança"), estando implementados em diversos dispositivos, serviços, ambientes, setores (e.g., entretenimento, prestação de serviços, comunicação, consumo e marketing) e focando múltiplos objetos, o que estende a vigilância a consumidores e transeuntes, de tal forma que os que atraem os olhares, os suspeitos e mesmo os perigosos "podem ser todos ou qualquer um". Todos aparentam ser suspeitos, até mesmo o mais comum dos homens parece investido de culpa, como no romance "O Processo" (KAFKA, 2009). A vigilância pode estar associada inclusive a mecanismos e dispositivos que, em princípio, não se destinariam a esse fim, e.g., geolocalização, comunicação, publicidade. Destarte, **gradualmente às câmera de monitoramento, vão sendo agregados mecanismos biométricos, e.g., leitores de íris e de digitais, bem como FRT** (KANASHIRO, 2006, p. 62-63). O fato é que, cada vez mais, os dados biométricos são derivados da videovigilância.

As técnicas de videovigilância podem ser menos intrusivas (e.g., algoritmos de contagem simples) ou mais intrusivas (e.g., tecnologias biométricas complexas). As questões de proteção de dados levantadas em cada situação podem ser diferentes, assim como a análise jurídica ao usar uma ou outra dessas tecnologias (EDPB, 2019, p. 4). Um exemplo ilustrativo

é a utilização de videovigilância para controle de entrada em uma sala com acesso restrito: o grau de intrusividade é completamente diverso se a câmera está direcionada para a porta, de maneira que apenas quem entra ou sai é visto (o que cumpriria a finalidade do monitoramento), ou se seu ângulo está direcionado para as pessoas dentro da sala (o que extrapolaria a finalidade do monitoramento, além de submeter as pessoas à restrição na sua liberdade de ação/comportamento).

Os limites entre o que seria a videovigilância e a videovigilância com FRT é sutil, o *Article 29 Working Party* (2004, p. 4-5) aponta que a videovigilância convencional "se destina sobretudo a documentar acontecimentos específicos e os respectivos autores", ao passo que a nova forma de vigilância (com utilização de "reconhecimento facial ou estudo e previsão do comportamento humano") "baseia-se na **aquisição automatizada das características faciais dos indivíduos**, bem como na sua conduta 'anormal' em associação com a [possibilidade de] disponibilidade de alertas e avisos automatizados, que implicam eventualmente perigos de discriminação" (grifo meu).

Basicamente, a diferença entre a videovigilância pura e simples e a utilização da FRT é a possibilidade desta última de identificação do indivíduo (inclusive em tempo real) por meio do processamento biométrico, esse é o grande giro paradigmático e também o grande risco, que por sua vez é potencializado pela possibilidade de cruzar essa informação com bancos de dados previamente existentes para obter outras informações do titular (o que pode incluir o cruzamento da informação com *watchlists* de identificação policial).

Onde quer que se vá, a FRT associada à videovigilância permite identificar, seguir, destacar e rastrear o indivíduo, reduzindo direitos humanos e liberdades civis.

Além disso, a intrusão do processamento não depende necessariamente de sua finalidade. O uso de FRT para fins, como **segurança privada, representa as mesmas ameaças aos direitos fundamentais** de respeito à vida privada e à proteção dos dados pessoais. Mesmo que previstas limitações, o número potencial de suspeitos ou autores de crimes sempre será "alto o suficiente" para justificar o uso contínuo de FRT para detecção de suspeitos. Muitas vezes se olvida do fato que, ao monitorar áreas abertas, as obrigações sob a lei de proteção de dados devem ser cumpridas não apenas para os suspeitos, mas para todos aqueles que, na prática, estão sendo monitorados (EDPB e EDPS, 2021, p. 11).

Fato é que, alguns empregos da tecnologia têm um alto risco potencial, com tão poucas vantagens associadas, que deveriam ser interrompidos antes de se tornarem grandes. O complicado é que, uma vez que sua utilização se torne comum, ainda que se revelem prejudiciais, é mais difícil retirá-los de uso[48]. Por isso, vale à pena iniciar uma discussão pública sobre o que pode dar errado com essas tecnologias a fim de decidir onde estão os limites coletivos – antes deles serem ultrapassados.

[48] Quanto a isso, Clarissa Long citada pela Ministra Rosa Weber do STF: "a história nos ensina que uma vez estabelecidos, é improvável que poderes governamentais de vigilância e coleta de dados de seus cidadãos e residentes retrocedam voluntariamente. E a história também tem nos ensinado que uma vez que dados são coletados para um propósito, é muito difícil evitar que sejam usados para fins outros não relacionados" (BRASIL, 2020c, p. 30).

O uso de FRT em espaços públicos, diante da intromissão que implica no direito à privacidade, à proteção de dados pessoais e à dignidade dos indivíduos, juntamente com um risco de impacto adverso sobre outros direitos humanos e liberdades fundamentais, deve estar sujeito a um debate democrático sobre a sua utilização e mesmo à possibilidade de moratória enquanto se aguarda uma análise mais profunda (COUNCIL OF EUROPE, 2021c, p. 5).

Diante deste cenário, os principais movimentos de resistência a esses dispositivos de controle estão na defesa da necessidade de construir e consolidar parâmetros legais que limitem e regulem sua utilização.

A *Global Privacy Assembly* (GPA, Assembleia Global de Privacidade)[49] reconheceu que a fim de construir e manter a confiança dos cidadãos, antes que a FRT seja implantada

é necessário identificar e mitigar seus riscos potenciais por meio da adesão a padrões legais, estabelecimento de salvaguardas técnicas e organizacionais, bem como levar em consideração questões éticas e de direitos humanos. Para tanto, devem ser observados princípios de proteção de dados e privacidade, inclusive finalidades claramente definidas, uma base legal clara, necessidade e proporcionalidade, justiça e transparência, direitos individuais, estruturas de governança e de responsabilização (GPA, 2020, p. 3).

3.4 Mais do que dado pessoal, dado pessoal sensível

Konder (2019, p. 460) entende que o fator primordial para se determinar se um dado é sensível ou não diz respeito: (i) ao contexto de sua utilização; (ii) as relações que podem ser estabelecidas com as demais informações disponíveis; e (iii) a potencialidade de seu tratamento servir como instrumento de estigmatização ou discriminação.

O nível de intromissão da FRT e a potencial violação a direitos, à privacidade e à proteção de dados variam de acordo com a situação particular de seus usos. Haverá casos em que a legislação limitará estritamente o emprego da FRT, ou até mesmo o proibirá completamente (COUNCIL OF EUROPE, 2021c, p. 5). O GDPR, em seu art. 9º(1), estabeleceu a proibição da FRT como regra, permitindo sua implementação a título de exceção, em certos casos específicos (art. 9º(2), GDPR) e sujeito a salvaguardas que são adequadas a esses riscos (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016, grifo meu):

> Artigo 9º - **Tratamento de categorias especiais de dados pessoais**
> 1. **É proibido o tratamento de** dados pessoais que revelem a **origem racial ou étnica**, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, **dados biométricos para identificar uma pessoa de forma inequívoca**, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa.
> 2. O disposto no nº 1 não se aplica se se verificar um dos seguintes casos: [...]

[49] Um dos principais fóruns globais para autoridades de proteção de dados e privacidade por mais de quatro décadas, desde quando se reuniu pela primeira vez, em 1979, como a Conferência Internacional de Comissários de Proteção de Dados e Privacidade. A Assembleia conecta os esforços de mais de 130 autoridades de proteção de dados e privacidade de todo o mundo (GPA, 2021).

Como visto na Seção 2.1, quando se fala em FRT, tem-se processamento por meio técnico específico que utiliza como matéria prima, dado biométrico, que no caso da face é inerentemente "vinculado a uma pessoa natural" e, portanto, por definição, é dado pessoal sensível (art. 5º, II, LGPD), assim, cuidados adicionais devem ser tomados.

Podem ser estabelecidas as seguintes premissas (SIMÃO *et al.*, 2020, p. 7-9):

1. Toda tecnologia capaz de detectar uma face humana pode ser considerada FRT.
   Mesmo que o intuito da aplicação da FRT não seja a identificação de uma pessoa determinada, para que ocorra a detecção facial, é preciso coletar e tratar faces humanas (o que envolve a leitura de atributos e pontos de referência de uma face).
2. Dados referentes a faces humanas são dados pessoais.
   Informação relacionada a pessoa natural identificada ou identificável é dado pessoal (art. 5º, I, LGPD), assim, a imagem de um indivíduo e as informações dela decorrentes constituem dado pessoal.
3. Todo reconhecimento facial envolve o tratamento de dados pessoais.
   A FRT implica, necessariamente, o tratamento de imagens de faces humanas, pois sempre envolve a detecção de uma face e o tratamento dessa imagem, ainda que tais dados sejam ulteriormente descartados ou anonimizados. Por importar o tratamento da imagem de uma face (que pela premissa 2, acima, é dado pessoal), não se pode conceber FRT sem presumir tratamento de dados pessoais.
4. Dados de faces humanas tratadas no contexto do reconhecimento facial são dados (biométricos) sensíveis.
   Como a FRT processa pontos de referência de uma face (dados biométricos), extraindo deles inferências sobre características pessoais (i.e., obtenção de um modelo biométrico), há tratamento de dado sensível (art. 5º, II, LGPD e art. 4º(14), GDPR). Outrossim, a partir da extração de atributos de uma face, podem ser inferidas informações outras, que podem ser também sensíveis, e.g., **origem racial ou étnica**, idade, gênero etc.
5. Eventual anonimização dos dados não descaracteriza o tratamento de dados pessoais.
   Ainda que posteriormente à anonimização os dados não possam mais ser individualizados, o processo até que ela ocorra envolve o tratamento da imagem da face de um indivíduo, de maneira que a anonimização ou o descarte da imagem não têm o condão de desobrigar o operador[50] de cumprir exigências e princípios da legislação e salvaguardas aplicáveis.

Entidades/instituições (sejam elas públicas ou privadas) têm de cumprir todos os princípios e disposições de proteção de dados aplicáveis ao processar dados biométricos na sua utilização em FRT (COUNCIL OF EUROPE, 2021c, p. 10). Isso implica que o ciclo de vida dos dados usados para FRT deve ser gerenciado (i.e., os dados devem ser coletados, armazenados, mantidos em segurança, auditados etc.) em conformidade com a LGPD. A esse

[50] Operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, VII, LGPD) (BRASIL, 2019b).

respeito, cumpre destacar que a LGPD estabelece padrões mínimos a serem seguidos, que podem ser suplementados por medidas adicionais de proteção.

As instituições que utilizam FRT têm de ser capazes de demonstrar que esta utilização é prevista em lei, tem um objetivo legítimo específico, é estritamente necessária e proporcional no contexto da sua utilização, respeita a essência dos direitos e liberdade fundamentais dos titulares de dados (COUNCIL OF EUROPE, 2021c, p. 10).

Em janeiro de 2021, a *Convention 108+* emitiu "Diretrizes sobre o Reconhecimento Facial", onde ressaltou que, tendo em vista utilizar uma **categoria especial de dados (i.e., dado sensível)**, deve haver **base legal** aplicável ao processamento dos dados biométricos por meio da FRT, que deve contemplar, pelo menos (COUNCIL OF EUROPE, 2021c, p. 4):

- Explicação detalhada do uso específico e da finalidade;
- Confiabilidade e precisão mínimas do algoritmo utilizado;
- Duração da retenção das imagens utilizadas;
- Possibilidade de auditoria desses critérios (*accountability*);
- Rastreabilidade do processo;
- Salvaguardas (adaptadas aos riscos envolvidos e aos interesses, direitos e liberdades a proteger).

Segundo Mulholland (2018, p. 164), dos princípios previstos no art. 6º da LGPD, dois são especialmente relevantes no que diz respeito ao tratamento de dados sensíveis: o **princípio da finalidade** e o **princípio da não discriminação**.

A seguir, além dos dois princípios elencados por Mulholland, serão abordados os princípios da LGPD que particularmente se mostram relevantes no contexto da FRT, quais sejam: da adequação, da necessidade, da transparência, da segurança, da prevenção, da responsabilização e prestação de contas. Importa mencionar que tais princípios estão intimamente relacionados, de maneira que muitas vezes se mostram justapostos/imbricados, sem contar, necessariamente, com limites nitidamente definidos (e sem que isso represente prejuízo ao titular dos dados).

3.4.1 Finalidade (art. 6º, I, LGPD)

> 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; (BRASIL, 2019b).

O emprego da FRT deve estar associado a uma **finalidade** específica, que cumpra propósitos legítimos, determinados, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essa finalidade (princípio da limitação das finalidades). Neste sentido, legisladores e tomadores de decisão devem garantir que as imagens disponíveis em formato digital não possam ser processadas para extrair modelos biométricos ou integrá-los em sistemas biométricos sem uma base legal específica para o novo processamento, quando essas imagens foram **inicialmente capturadas para outros fins** (e.g.,

para uso em redes sociais) (COUNCIL OF EUROPE, 2021c, p. 5). Conforme a elucidativa analogia de Moraes (2008, p. 9), "[a] coleta não pode ser tomada como uma 'rede jogada ao mar para pescar qualquer peixe'[...] principalmente quando se tratarem de 'dados sensíveis'".

A *Convention 108+* defende que o processamento de dados biométricos por FRT (seja em um ambiente controlado, seja em espaços públicos) deve ser **restrito, em geral, para fins de aplicação da lei** e ser executado exclusivamente pelas autoridades competentes na área da segurança (nessa situação, os normativos aplicáveis devem fornecer **critérios e parâmetros claros** a serem seguidos ao criar bancos de dados – listas de observação). Para **outros interesses públicos**, por parte de autoridades públicas, que não tenham por objetivo a aplicação da lei, argumenta que regras específicas para o processamento biométrico por FRT devem ser estabelecidas. Por fim, sustenta que as **entidades privadas** não devem implantar FRT em espaços públicos, como shoppings, especialmente para identificar pessoas de interesse, para **fins mercadológicos ou de segurança privada** (COUNCIL OF EUROPE, 2021c, p. 6-7).

Especificamente, o uso de imagens digitais carregadas na Internet, incluindo redes sociais, sites de gerenciamento de fotos, capturadas por câmeras de videovigilância, não pode ser considerado legal com base apenas em que os dados pessoais foram manifestamente disponibilizados pelos titulares dos dados (COUNCIL OF EUROPE, 2021c, p. 6). Bancos de dados de imagens digitais inicialmente usados para outros fins só podem ser usados para extrair modelos biométricos e integrá-los em sistemas biométricos quando for para **fins legítimos**, **previstos por lei** e **estritamente necessários e proporcionais para esses fins** (e.g., aplicação da lei ou fins médicos) (COUNCIL OF EUROPE, 2021c, p. 6).

Ainda com relação à finalidade do processamento por FRT, **as expectativas razoáveis do titular dos dados** no momento e no contexto do processamento de seus dados pessoais devem ser respeitadas (art. 44, LGPD[51]). Em relação ao monitoramento sistemático (com ou sem FRT), a relação entre o titular dos dados e o controlador[52] pode variar significativamente e pode afetar as expectativas razoáveis que o titular dos dados possa ter. A interpretação do conceito de expectativas razoáveis não deve se basear apenas nas expectativas subjetivas, um bom critério é se um terceiro poderia esperar e concluir estar sujeito a monitoramento na situação específica em questão, e.g., o monitoramento não é esperado em áreas de convivência, em salas de exame ou de tratamento, em instalações sanitárias, saunas; por outro lado o cliente de um banco pode esperar que seja monitorado dentro do banco ou num caixa eletrônico.

[51] Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou **quando não fornecer a segurança que o titular dele pode esperar**, consideradas as circunstâncias relevantes, entre as quais:
I - o modo pelo qual é realizado;
II - o resultado e os riscos que razoavelmente dele se esperam;
III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano (BRASIL, 2019b, grifo meu).

[52] Neste trabalho, por controlador dos dados, entende-se a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais" (art. 5º, VI, LGPD) (BRASIL, 2019b).

Sinalização informando sobre a videovigilância não é definidor do que o titular dos dados pode esperar objetivamente (EDPB, 2019, p. 10-11).

3.4.2 Adequação (art. 6º, II, LGPD) e necessidade (art. 6º, III, LGPD)

> Art. 6º [...] 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; (BRASIL, 2019b).

Antes de considerar a utilização de FRT, o controlador deve analisar criticamente se a medida é: (i) **adequada para atingir o objetivo pretendido**; e (ii) **necessária aos seus fins**. Além disso, a necessidade da utilização de FRT deve ser avaliada em conjunto com a **proporcionalidade,** a **finalidade** e o **impacto sobre os direitos** dos titulares.

Os indivíduos normalmente têm o direito de conduzir suas vidas sem serem monitorados e examinados:

- Dado que o uso da FRT interfere nesses direitos, tal tecnologia pode ser **usada apenas se outras técnicas menos invasivas não estiverem disponíveis**, i.e., deve se identificado se a FRT é ou não o meio mais apropriado para atender à necessidade.
- Além disso, a FRT deve ser usada de forma a minimizar a interferência na vida das pessoas que adotam comportamentos legais.

Assim, considerando o potencial intrusivo da FRT, principalmente em espaços públicos, deve restar demonstrado, que uma série de fatores, incluindo o local e o momento de implantação dessas tecnologias, justificam a proporcionalidade e a estrita necessidade do seu uso (COUNCIL OF EUROPE, 2021c, p. 6).

Como mencionado acima, a FRT só deve ser escolhida se o objetivo do tratamento não puder ser razoavelmente alcançado por outros meios menos invasivos dos direitos e liberdades fundamentais do titular dos dados, além disso, deve-se levar em consideração, também, a **vulnerabilidade** desses titulares e a **natureza do ambiente** onde essas tecnologias são utilizadas, a segurança em espaços públicos ou controlados, não deve, como regra, ser considerada estritamente necessária e proporcional onde existem mecanismos alternativos menos intrusivos (EDPB, 2019, p. 9; COUNCIL OF EUROPE, 2021c, p. 7), e.g., para prevenir crimes contra a propriedade, em vez de instalar um sistema de videovigilância com FRT, podem ser tomadas medidas alternativas de segurança, como cercar a propriedade; patrulhas regulares que são capazes de reagir e intervir imediatamente; melhor iluminação; instalação de travas de segurança; aplicação de revestimento anti-grafiti nas paredes.

Quanto à **proporcionalidade**, a FRT só pode ser permitida se os benefícios forem proporcionais a qualquer perda de liberdade e privacidade. Os benefícios devem ser suficientemente grandes para justificar a interferência em outros direitos.

Não há normativo prescrevendo um tempo de retenção próprio (mínimo ou máximo) no que diz respeito à FRT. Mas o **período de retenção** não deve ser superior ao necessário para a finalidade específica do processamento, após o que, deve-se garantir a eliminação das informações e/ou modelos biométricos[53]. Assim, é preciso ter um cronograma de retenção e descarte apropriado. Ao determinar esse cronograma, a natureza biométrica dos dados pessoais deve ser levada em consideração, vez que diferentes *outputs* do processamento podem demandar períodos de retenção distintos (COUNCIL OF EUROPE, 2021c, p. 12):

- Se não houver correspondência dos modelos biométricos, o modelo biométrico de indivíduos que passam por um espaço público não pode ser retido e deve ser excluído automaticamente.
- Se houver uma correspondência, os modelos biométricos e os relatórios de correspondência podem ser retidos por um período previamente previsto, limitado ao estritamente necessário, com as salvaguardas aplicáveis.
- Em qualquer caso, a lista de observação e os modelos biométricos devem ser excluídos após a conclusão da finalidade para a qual a FRT foi implantada.

Importante pontuar que o período de retenção não deve ser determinado simplesmente por fatores outros, tais como a capacidade de armazenamento de um sistema (ICO, 2017, p. 20).

Ocasionalmente, pode ser necessário reter informações por um período mais longo, mas isso deve estar fundamentado, e.g., quando um órgão de aplicação da lei está investigando um crime e pede para que a informação seja preservada, para dar-lhes a oportunidade de analisá-la como parte de uma investigação ativa (ICO, 2017, p. 21).

Por fim, como corolário do princípio da necessidade, deriva-se o **princípio da minimização de dados**, que exige que apenas sejam processadas as informações necessárias e não todas as informações disponíveis para a entidade (COUNCIL OF EUROPE, 2021c, p. 12).

3.4.3 Transparência (art. 6º, VI, LGPD)

> Art. 6º [...] 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; (BRASIL, 2019b).

Uma vez que a FRT pode ser utilizada sem qualquer intenção ou cooperação com os titulares dos dados, a **transparência** e **equidade** do tratamento é de extrema importância e deverá ser devidamente considerada pelas entidades que as utilizam (COUNCIL OF EUROPE, 2021c, p. 11).

As pessoas devem ser avisadas quando estiverem em uma área onde um sistema de vigilância esteja em operação (ICO, 2017, p. 37-38). Mais especificamente no que diz respeito

[53] O armazenamento a longo prazo de dados pessoais, sem que haja uma limitação clara de período de retenção, também acarreta riscos específicos, pois os dados poderão ser submetidos a formas futuras de exploração não previstas no momento de sua coleta (UN, 2021, § 14).

ao uso de FRT, é preciso encontrar maneiras apropriadas e **potencialmente inovadoras** de informar os indivíduos (ICO, 2017, p. 33) não só sobre a realização do tratamento, mas sobre os respectivos agentes de tratamento.

A maneira mais comum de se fazer isso é usando placas colocadas de forma ostensiva na entrada da zona do sistema de vigilância e reforçando isso com outras placas dentro da área. Essa mensagem também pode ser corroborada por um anúncio de áudio, onde anúncios públicos já são usados, como em um trem (ICO, 2017, p. 37). Entretanto, a simples passagem por um ambiente onde a FRT é utilizada não pode ser considerada como um consentimento explícito (COUNCIL OF EUROPE, 2021c, p. 7), isso porque, apesar do consentimento não precisar necessariamente ser escrito, não pode ser auferido da omissão do titular, mas apenas de atos positivos que evidenciem sua vontade (VIOLA e TEFFÉ, 2021, p. 138).

Sinalização clara e proeminente é particularmente importante onde os sistemas de vigilância são muito discretos ou em locais onde as pessoas podem não esperar estar sob vigilância (ainda mais com utilização de FRT). Os sinais devem (ICO, 2017, p. 37-38):

- Ser claramente visíveis e legíveis.
- Conter detalhes da organização que opera o sistema, o propósito de usar o sistema de FRT e quem contatar sobre o esquema (quando isso não for óbvio para aqueles que estão sendo monitorados).
- Incluir detalhes de contato básicos, e.g., um endereço de site, número de telefone ou contato de e-mail.
- Ter um tamanho apropriado dependendo do contexto, e.g., se são direcionados para pedestres ou motoristas em automóveis.

O fornecimento destas informações é ratificado em leitura sistemática do princípio da transparência com o art. 9º da LGPD, que dispõe (BRASIL, 2019b):

> 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. [...]

Os fatores relacionados à transparência dizem respeito a fornecer informações aos indivíduos quanto ao contexto da coleta; às expectativas razoáveis de como os dados serão usados; se o reconhecimento facial é apenas uma característica acessória do produto/serviço ou, em vez disso, é parte integrante do próprio serviço; à forma como a coleta, utilização ou partilha de dados é suscetível de os afetar, principalmente quando se tratam de pessoas em

situação de vulnerabilidade; indicar quais direitos e recursos legais podem ser usados pelos titulares dos dados (COUNCIL OF EUROPE, 2021c, p. 11).

Além disso, é uma boa prática que a entidade que utiliza a FRT estabeleça **políticas de proteção de dados sobre reconhecimento facial** ou **material informativo** nos quais constem informações (COUNCIL OF EUROPE, 2021c, p. 11):

- Se e em que medida os dados de reconhecimento facial podem ser transmitidos a terceiros (e, se for o caso, informações sobre a identidade dos terceiros parceiros contratuais que recebem os dados durante o fornecimento do produto ou serviço);
- Retenção, exclusão ou anonimização dos dados de reconhecimento facial;
- Formas de contato disponíveis para os indivíduos fazerem perguntas sobre a coleta, uso e compartilhamento de dados de reconhecimento facial;
- Quando houver mudança das práticas de coleta, uso e compartilhamento, as entidades devem atualizar sua política de privacidade ou divulgá-las, em especial quanto ao contexto da mudança e seu impacto sobre os indivíduos.

Isso é estimulado pela Seção II "Das Boas Práticas e de Governança", do Capítulo VII, da LGPD (art. 50 e ss).

Quando a FRT é implantada em um espaço público, as entidades podem adotar uma **abordagem em camadas** para fornecer as informações necessárias aos titulares dos dados que passam pelo local (COUNCIL OF EUROPE, 2021c, p. 12):

- **Primeira camada**: informações legíveis e inteligíveis sobre a finalidade do processamento, a entidade que usa a tecnologia, a duração do processamento e o perímetro em questão, a serem **afixadas na vizinhança** do local onde a FRT está implantada.
- **Segunda camada**: todas as informações necessárias (exigidas por lei, normativo e/ou política), a serem exibidas **nos pontos de entrada** do local de implantação.

No caso de bases de dados criadas por autoridades responsáveis pela aplicação da lei, a obrigação de transparência pode ser proporcionalmente restringida para não prejudicar os objetivos de aplicação da lei. Entretanto, o uso encoberto de FRT por autoridades policiais pode, no máximo, ser possível se estritamente necessário e proporcional para prevenir riscos iminentes e substanciais para a segurança pública, que devem ser **documentados antes** do uso (COUNCIL OF EUROPE, 2021c, p. 11-12). Quanto a isso, pertinente mencionar estudo realizado pelo Laboratório de Políticas Públicas e Internet (LAPIN)[54] acerca do emprego da FRT no âmbito da Administração Pública, que teve como principal conclusão "que o emprego de tecnologias de vigilância **não tem sido realizado de forma transparente com a população**, o que coloca em risco os direitos e liberdades individuais de cidadãos cujos dados são coletados por esses sistemas" (grifo meu), inclusive diante dos riscos identificados no

[54] Fundado em Brasília, é um "centro independente de pesquisa e ação voltado para os desafios *sociais*, *éticos*, e *jurídicos* que as tecnologias digitais trazem a uma sociedade global conectada. Desde 2016, o Laboratório desenvolve pesquisas científicas, notas técnicas, cursos, campanhas, e ações direcionadas a temas como privacidade, proteção de dados pessoais, liberdade de expressão e inovação" (LAPIN, 2021).

contexto brasileiro, aquele Laboratório recomendou a sua não adoção pelo setor público (REIS *et al.*, 2021, p. 2).

3.4.4 Segurança (art. 6º, VII, LGPD) e prevenção (art. 6º, VIII, LGPD)

> Art. 6º [...] 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; (BRASIL, 2019b).

É necessário escolher cuidadosamente como as informações são mantidas e registradas, bem como garantir que o acesso seja restrito (ICO, 2017, p. 12).

Dados biométricos são únicos para seus titulares, assim, qualquer falha na segurança dos dados pode ter consequências particularmente graves (Seção 2.4.5).

Qualquer violação da segurança dos dados que possa interferir seriamente com os direitos e liberdades fundamentais dos titulares dos dados deve ser notificada à autoridade de supervisão e, se for o caso, aos titulares dos dados (COUNCIL OF EUROPE, 2021c, p. 13), (art. 48, *caput*, LGPD[55]).

As medidas de segurança devem evoluir ao longo do tempo e em resposta às mudanças de ameaças e vulnerabilidades identificadas. Devem também ser proporcionais à sensibilidade dos dados, ao contexto em que a FRT é usada e aos seus objetivos, à probabilidade de danos a indivíduos e a outros fatores relevantes (COUNCIL OF EUROPE, 2021c, p. 13).

Práticas rígidas de retenção e descarte dos dados biométricos faciais – por meio de procedimentos seguros –, com os períodos de retenção mais curtos possíveis, também contribuem para reduzir as exposições de segurança (COUNCIL OF EUROPE, 2021c, p. 13).

"Medidas de segurança e sigilo de dados" estão previstos no art. 46[56] e ss da LGPD e no contexto da FRT devem ser observados com atenção, apesar de certas medidas dependerem em algum grau de definição da Autoridade Nacional de Proteção de Dados (ANPD) (e.g., art. 46, §1º, LGPD[57]).

Deve ser garantido o maior nível de confiabilidade possível, considerando que a utilização de FRT pode resultar em consequências adversas muito significativas para o indivíduo (COUNCIL OF EUROPE, 2021c, p. 10).

---

[55] Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

[56] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito. [...] (BRASIL, 2019b).

[57] Art. 46 [...] § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no *caput* deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no *caput* do art. 6º desta Lei (BRASIL, 2019b).

As entidades devem garantir que os modelos biométricos e as imagens digitais sejam precisos e atualizados (e.g., a qualidade das imagens e modelos biométricos inseridos nos catálogos/em listas de observação deve ser verificada para evitar possíveis correspondências falsas, uma vez que imagens de baixa qualidade podem causar um aumento no número de erros, com sérias consequências para os titulares, *vide* Seção 2.4.1) (COUNCIL OF EUROPE, 2021c, p. 12).

Em caso de falsos positivos, as entidades devem tomar todas as medidas razoáveis para corrigir ocorrências futuras e garantir a precisão das imagens digitais e modelos biométricos (COUNCIL OF EUROPE, 2021c, p. 12).

Além do mais, com o tempo, os dados podem se tornar imprecisos, irrelevantes ou carregar uma identificação histórica incorreta, causando resultados tendenciosos ou errôneos no caso de processamento futuro (UN, 2021, § 14). Com base no princípio da prevenção, medidas devem ser adotadas para evitar a ocorrência de danos nesse contexto.

3.4.5 Não discriminação (art. 6º, IX, LGPD)

> Art. 6º [...] IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; (BRASIL, 2019b).

Segundo Mulholland (2018, p. 166), quando se fala em tratamento de dados sensíveis, o princípio da não discriminação é dos mais relevantes, principalmente quando se está diante do exercício democrático e do acesso a direitos sociais (e.g., direito ao trabalho, à saúde, à moradia, acesso a políticas públicas) (MULHOLLAND, 2018, p. 174).

Para que o uso da tecnologia seja legítimo, ela não deve envolver ou exibir vieses, preconceitos ou injustiças algorítmicas (*vide* Seção 2.4.3). Isso pode ser injusto de, pelo menos, duas maneiras: (i) em primeiro lugar, alguns tipos de reconhecimento incorreto são inerentemente degradantes e insultuosos; (ii) em segundo lugar, a tecnologia com esses preconceitos pode resultar em tratamento desigual e discriminatório de alguns indivíduos ou grupos de indivíduos (e.g., membros de alguns grupos estão muito mais propensos a serem detidos e/ou obrigados a identificar-se).

Nesse sentido, Rodotá (2008, p. 84) lembra que o tratamento de dados pessoais pode gerar discriminação ao ser usada para formação de perfis:

> seja porque dados pessoais, aparentemente não "sensíveis", podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas.

A FRT (incluindo conjuntos de treinamento de dados) que serão usadas em locais públicos deve estar aberta ao escrutínio e supervisão eficaz.

Desenvolvedores ou fabricantes de FRT, mas também entidades que usam FRT, devem tomar medidas para garantir sua acurácia. Em particular, devem ativamente evitar rotulagens incorretas, testar exaustivamente seus sistemas, identificar e eliminar inacurácias, principalmente quanto às variações demográficas na cor da pele, idade e gênero, evitando discriminação não intencional (COUNCIL OF EUROPE, 2021c, p. 9).

Além disso, a fim de garantir a qualidade dos dados e a eficiência dos algoritmos, tanto quanto possível, estes devem ser desenvolvidos usando conjuntos de dados sintéticos, baseados em fotos suficientemente diversas de homens e mulheres, de cores de pele diferentes, morfologia distinta, de todas as idades e de diferentes ângulos de câmera (COUNCIL OF EUROPE, 2021c, p. 9).

Os dados biométricos que revelem inevitavelmente outros dados sensíveis, como informações sobre um tipo de doença ou deficiência física, devem estar sujeitos a salvaguardas complementares adequadas (COUNCIL OF EUROPE, 2021c, p. 9).

3.4.6 Responsabilização e prestação de contas (*accountability*) (art. 6º, X, LGPD)

> Art. 6º [...] 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. (BRASIL, 2019b).

Devem ser usados mecanismos para a responsabilização tanto dos desenvolvedores, como dos fabricantes, dos provedores de serviços e/ou das entidades que usam a FRT (COUNCIL OF EUROPE, 2021c, p. 8).

As empresas que **desenvolvem e comercializam FRT** devem adotar medidas específicas para garantir o cumprimento dos princípios de proteção de dados, tais como (COUNCIL OF EUROPE, 2021c, p. 10):

- Integrar a proteção de dados no projeto e arquitetura de produtos e serviços de reconhecimento facial (**proteção de dados *by design*[58]** – desde o projeto), e.g., programar a exclusão automática de dados brutos após a extração de modelos biométricos.

[58] O termo "privacidade *by design*" (*privacy by design*) geralmente é utilizado para designar o amplo conceito de medidas tecnológicas para garantir a privacidade. Em contraste, os termos "proteção de dados *by design*" é utilizado para designar obrigações legais específicas estabelecidas, na EU, pelo art. 25 do GDPR (por analogia, no Brasil, pelo art. 46, §2º da LGPD). Embora as medidas tomadas de acordo com essas obrigações também contribuam para alcançar o objetivo mais geral de "privacidade *by design*", este último teria um espectro mais amplo que incluiria uma dimensão visionária e ética, consistente com os princípios e valores consagrados na Carta de Direitos Fundamentais da UE (EDPS, 2018, p. 1). Na prática, no âmbito desse trabalho, não se fará distinção entre os termos.

A proteção de dados *by design* está prevista no art. 46, §2º, LGPD[59] (nos Considerando 78[60] e art. 25[61], ambos do GDPR) e, segundo Lemos e Branco (2021, p. 458) pode ser encarada como uma ferramenta de construção de confiança do usuário (por englobar não apenas o tratamento dos dados, mas a própria arquitetura do sistema). Numa sociedade cada vez mais consciente e alerta da importância dos dados, um compromisso com a proteção de dados *by design* pode ser considerado uma vantagem competitiva (EDPS, 2018, p. 19).

- Oferecer um grau de flexibilidade na configuração dessas tecnologias para ajustar as salvaguardas técnicas de acordo com os princípios de limitação da finalidade, minimização de dados e limitação da duração do armazenamento de dados.
- Implementar um processo de revisão interna destinado a identificar e mitigar o impacto potencial sobre os direitos e as liberdades fundamentais (EDPS, 2018, p. 8) antes que as FRT sejam disponibilizadas (*vide* Seção 3.7).
- Integrar uma abordagem de proteção de dados em suas práticas organizacionais, incluindo a atribuição de pessoal dedicado, fornecendo treinamento para funcionários e conduzindo avaliações de impacto de proteção de dados sobre o

[59] Art. 46. [...] § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (BRASIL, 2019b).

[60] (78) A defesa dos direitos e liberdades das pessoas singulares relativamente ao tratamento dos seus dados pessoais exige a adoção de medidas técnicas e organizativas adequadas, a fim de assegurar o cumprimento dos requisitos do presente regulamento. Para poder comprovar a conformidade com o presente regulamento, o responsável pelo tratamento deverá adotar orientações internas e aplicar medidas que respeitem, em especial, os **princípios da proteção de dados desde a conceção e da proteção de dados por defeito**. Tais medidas podem incluir a minimização do tratamento de dados pessoais, a pseudonimização de dados pessoais o mais cedo possível, a transparência no que toca às funções e ao tratamento de dados pessoais, a possibilidade de o titular dos dados controlar o tratamento de dados e a possibilidade de o responsável pelo tratamento criar e melhorar medidas de segurança. No contexto do desenvolvimento, conceção, seleção e utilização de aplicações, serviços e produtos que se baseiam no tratamento de dados pessoais ou recorrem a este tratamento para executarem as suas funções, **haverá que incentivar os fabricantes dos produtos, serviços e aplicações a ter em conta o direito à proteção de dados quando do seu desenvolvimento e conceção e, no devido respeito pelas técnicas mais avançadas, a garantir que os responsáveis pelo tratamento e os subcontratantes estejam em condições de cumprir as suas obrigações em matéria de proteção de dados**. Os princípios de proteção de dados desde a conceção e, por defeito, deverão também ser tomados em consideração no contexto dos contratos públicos (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016, grifo meu).

[61] Artigo 25º - Proteção de dados desde a conceção e por defeito
1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados.
2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.
3. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas nos nº 1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42º (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

desenvolvimento ou modificação de produtos e serviços de reconhecimento facial (**proteção de dados *by default*** – por padrão).

Como padrão de boa prática, quanto à proteção de dados *by design* pode-se elencar um conjunto de técnicas/estratégias (LEMOS e BRANCO, 2021, p. 461):

1. *Minimizar*: reduzir os dados coletados ao mínimo possível.
2. *Esconder*: dados e suas interdependências não devem ser divulgados.
3. *Separar*: o processamento, sempre que possível, deve ocorrer em compartimentos segregados.
4. *Agregar*: o processamento deve se dar com mínimos detalhes (conforme item 1, com o mínimo de dados possível) e com alto nível de agregação/descaracterização (se possível/cabível).
5. *Informar* (transparência): sempre informar o titular dos dados.
6. *Controlar*: o titular dos dados deve ter controle sobre coleta e tratamento de seus dados (autodeterminação informativa).
7. *Fiscalizar e aplicar as leis*: as políticas de proteção de dados devem estar em conformidade com os dispositivos legais pertinentes e devem poder ser fiscalizadas.
8. *Demonstrar*: controladores de dados devem poder/conseguir demonstrar observância às políticas de proteção de dados e requisitos legais (não basta seguir, deve restar demonstrado, ou ser demonstrável o cumprimento/diligência).

Destarte, a proteção de dados *by design* e *by default*[62] deve cobrir toda a cadeia de valor do processamento por FRT[63] (EDPS, 2018, p. iii, 6-7). Deve estar difundida entre os

[62] Em oposição à proteção de dados *by design* e *by default vide* estudo do Conselho de Consumidores da Noruega (FORBRUKARRÅDET, 2018), que apresenta uma análise de como configurações padrão e padrões obscuros (*dark patterns*, i.e., técnicas e recursos de desenho de interface destinados a manipular usuários) são usados para conduzir os usuários para opções intrusivas da privacidade. Os achados incluem não só o emprego de configurações padrão intrusivas, mas também palavras enganosas, que dão aos usuários uma ilusão de controle, ao passo que ocultam escolhas que seriam mais favoráveis à privacidade, a utilização de opções do tipo *take it or leave it* e de arquiteturas de escolha nas quais a alternativa de privacidade amigável requer mais esforço por parte dos usuários.

[63] Um exemplo de *dark pattern* usado especificamente no contexto da FRT diz respeito às configurações de reconhecimento facial do *Facebook*. Para começar, o *Facebook* oculta as configurações pré-selecionadas para que o usuário que simplesmente clicar nos botões "Concordo" ou "Aceitar" nunca veja as configurações e seja difícil saber o que está pré-selecionado (*hidden default*) (FORBRUKARRÅDET, 2018, p. 15). O usuário que desejar desativar o reconhecimento facial deve ir para as configurações e ativamente selecionar "desligado"; para tanto, escolher a opção "mais amigável" à privacidade requer quatro cliques a mais do que a opção "menos amigável" (FORBRUKARRÅDET, 2018, p. 17). No *pop-up* do GDPR do *Facebook*, a interface foi projetada com um botão azul brilhante que induz o usuário a "Concordar e continuar". Por outro lado, o usuário que desejar limitar os dados que o *Facebook* coleta e usa, tem que primeiro clicar em uma caixa cinza chamada "Gerenciar configurações de dados". O contraste dos botões azul para aceitar e cinza fosco para ajustar as configurações fora do padrão é um exemplo de *design* destinado a "manipular" o usuário. Em outras palavras, a opção que o provedor de serviço deseja que o usuário escolha é tornada deliberadamente mais atraente (FORBRUKARRÅDET, 2018, p. 20). Além disso, quando o usuário é questionado se consente com o uso de FRT, a informação apresentada pelo *Facebook* é que a FRT será empregada para "ajudar a proteger o usuário de terceiros usando sua foto" e "dizer às pessoas com deficiência visual quem está em uma foto ou vídeo". A tela seguinte informa ao usuário "se você mantiver o reconhecimento de rosto desativado, não poderemos usar essa tecnologia se um estranho usar sua foto para se passar por você. Se alguém usa um leitor de tela, não será informado quando você estiver em uma foto, a menos que você seja marcado". Ao enquadrar o uso do reconhecimento facial de uma maneira exclusivamente positiva

desenvolvedores a respeito do impacto potencial do uso da FRT sobre os direitos humanos e as medidas que podem ser tomadas *by design* para mitigá-los (COUNCIL OF EUROPE, 2013, p. 2, § 8º). Deve integrar os critérios para aquisição do dispositivo e as decisões sobre implantação e configuração (ICO, 2017, p. 33). As entidades que empregam essa tecnologia devem garantir que os produtos/serviços que estão usando são projetados para processar dados biométricos em conformidade com os princípios de **limitação de finalidade**, **minimização de dados**, **duração limitada do armazenamento**, e integrar à tecnologia **todas as outras salvaguardas** necessárias a fim de minimizar os riscos de interferências com direitos e liberdades (COUNCIL OF EUROPE, 2021c, p. 15). Além disso, importante pensar na produção de sistemas rastreáveis, auditáveis, que possibilitem um monitoramento do fluxo de informações (RUARO e SARLET, 2021, p. 205).

As seguintes medidas organizacionais devem ser levadas em consideração pelas **entidades que usam FRT** (COUNCIL OF EUROPE, 2021c, p. 13):

- Implementar políticas, procedimentos e práticas transparentes para garantir que a proteção dos direitos dos titulares de dados está na base da utilização da FRT;
- Publicar relatórios de transparência sobre o uso concreto da FRT;
- Implementar programas de treinamento e procedimentos de auditoria para os responsáveis pelo processamento de dados de reconhecimento facial;
- Criar comitês de revisão internos para avaliar e aprovar processamento envolvendo dados de reconhecimento facial;
- Estender contratualmente os requisitos aplicáveis a terceiros prestadores de serviços, parceiros comerciais ou outras entidades que utilizem FRT (negar acesso a terceiros que não os cumpram), e.g., se no processamento do dado biométrico for usado um sistema de computação em nuvem, é necessário garantir que este sistema seja seguro e, caso tenha sido contratado um provedor para fornecer esse serviço, é preciso certificar-se que o provedor possa garantir a segurança das informações (ICO, 2017, p. 12).

Conforme já mencionado, a LGPD dedica uma Seção às "boas práticas" e "governança" nos art. 50 e ss. (que abrem espaço, inclusive, para formas alternativas e mais modernas de regulação, como a autorregulação regulada[64]).

Por fim, interessa trazer a ponderação de Zarsky (2013, p. 1533-1534) que a *accountability* está intrinsecamente ligada à concepção que os indivíduos (no caso,

(e.g., utilizar os dados biométricos do usuário para ficar mais seguro, bem como auxiliar deficientes visuais), deixando de lado deliberadamente quaisquer consequências negativas possíveis (e.g., o uso de FRT pode ser empregado para publicidade direcionada com base em estados emocionais ou para identificar usuários em situações em que eles preferem permanecer anônimos), o *Facebook* leva os usuários a habilitar o uso de FRT sem informá-los totalmente. Na verdade, **um apelo para o usuário "ficar mais seguro" e "para ajudar os usuários com deficiência visual" é usado para coletar dados pessoais altamente confidenciais, ocultando fatores importantes que deveriam ser apresentados ao usuário a fim de fazer uma escolha informada** (FORBRUKARRÅDET, 2018, p. 22-23). Por fim, o controle de como o *Facebook* compartilha os dados do usuário com terceiros (inclusive dados resultantes do reconhecimento facial) não está incluído no escopo do *pop-up* do GDPR (FORBRUKARRÅDET, 2018, p. 33).

[64] Para uma visão aprofundada a respeito de autorregulação regulada *vide* Aranha (2019).

principalmente os agentes de tratamento de dados pessoais – controlador, operador e encarregado –, mas também desenvolvedores, empresas que comercializam a tecnologia etc.) são eticamente responsáveis por seus atos, sendo a transparência uma das ferramentas viabilizadoras/facilitadoras dessa responsabilização.

3.5 Hipóteses para tratamento de dados pessoais sensíveis

A LGPD estabeleceu como regra geral, no seu âmbito de aplicação, que todo tratamento de dados "inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado" (art. 1º, LGPD), deverá ter uma base legal para fundamentar o tratamento de dados pessoais que realizar (VIOLA e TEFFÉ, 2021, p. 132). As hipóteses legais para tratamento de dados constam da LGPD em seus art. 7º (dados pessoais) e art. 11 (dados pessoais sensíveis), que trazem rol taxativos, ainda que compostos de algumas hipóteses mais abertas e com algum grau de subjetividade (e.g., o interesse legítimo), cujos detalhes e adequações devem ser promovidos pela ANPD, pelo Legislativo e pelo Judiciário (VIOLA e TEFFÉ, 2021, p. 132-133).

Em geral, a LGPD se apoia fortemente **no consentimento do titular de dados** para o tratamento dos dados pessoais (art. 5º, XII, LGPD)[65] – evidenciando a consideração do legislador com a participação do indivíduo no fluxo de suas informações –, ainda que não seja a única hipótese nem hierarquicamente superior às demais elencadas no art. 7º ou art. 11 da LGPD (MULHOLLAND, 2018, p. 168; VIOLA e TEFFÉ, 2021, p. 134).

Mendes e Fonseca (2021, p. 91-92) destacam que frente aos desafios contemporâneos, **o consentimento não tem sido suficiente para tutelar a privacidade e proteger os dados dos titulares**. Diante desse impasse, apontam três potenciais causas:

1. Limitações cognitivas do titular de dados (FORBRUKARRÅDET, 2018, p. 7).
2. Assimetria de poder entre titulares dos dados e o controlador dos dados (e.g., situações qualificadas como *take it or leave it*; consentimento de empregados frente a empregadores etc.).
   Essa assimetria pode significar que os indivíduos não possam consentir facilmente, se opor ao processamento de seus dados, ou mesmo exercer seus direitos (MARQUES e MUCELIN, 2021, p. 145-146). Tal desequilíbrio, por sua vez, pode levar à violação dos princípios da igualdade e da liberdade. Daí porque Mulholland (2018, p. 177) defende que, proteger os dados pessoais (em especial os sensíveis) de maneira firme é, ao fim e ao cabo, uma maneira de efetivação da igualdade e da liberdade.
3. Menor capacidade de oferecer respostas efetivas aos novos desafios e situações que se apresentam (e.g., novas tecnologias para tratamento de dados e seus empregos, como a FRT).

[65] Art. 5º Para os fins desta Lei, considera-se: [...] XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; (BRASIL, 2019b).

Fazendo um paralelo com o GDPR, no caso da videovigilância, apenas em casos excepcionais o consentimento do titular dos dados servirá de base jurídica nos termos do art. 7º [66], isso porque (EDPB, 2019, p. 12): (i) é da natureza da videovigilância monitorar um número desconhecido de pessoas ao mesmo tempo; (ii) o responsável pelo tratamento dificilmente poderá provar que o titular dos dados deu o consentimento antes do tratamento dos seus dados pessoais (art. 7º(1)), e.g., entrar em uma área monitorada marcada não constitui uma declaração ou uma ação afirmativa clara necessária para consentimento; (iii) caso o titular dos dados retire o seu consentimento, será difícil para o responsável pelo tratamento provar que os dados pessoais deixaram de ser tratados (art. 7º(3)).

De qualquer forma, ainda que se tivesse uma "eventual dispensa da exigência do consentimento" ela não isentaria os agentes de tratamento das demais obrigações previstas na LGPD "especialmente da observância dos princípios gerais e da garantia dos direitos do titular" (art. 7º, § 6º, LGPD[67]) (BRASIL, 2019b).

Este é o momento de lembrar que, como visto na Seção 3.4, **quando falamos de FRT estamos falando de dados pessoais sensíveis**.

O GDPR dispõe sobre o "tratamento de categorias especiais de dados pessoais" (i.e., de dados pessoais sensíveis) em seu art. 9º, no qual estabelece um regime rigoroso, proibindo, geralmente, o processamento desse tipo de dado (art. 9º(1), GDPR). Sem embargo, excetua a proibição em dez circunstâncias (art. 9º(2), GDPR)[68] que incluem, entre outras, a proteção de

---

[66] Artigo 7º - Condições aplicáveis ao consentimento
1. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais.
2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento.
3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar.
4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

[67] Art. 7º [...] § 6º A eventual dispensa da exigência do consentimento não desobriga os agentes de tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular(BRASIL, 2019b).

[68] Artigo 9º [...] 2. O disposto no nº1 não se aplica se se verificar um dos seguintes casos:
a) Se o titular dos dados tiver dado o seu consentimento explícito para o tratamento desses dados pessoais para uma ou mais finalidades específicas, exceto se o direito da União ou de um Estado-Membro previr que a proibição a que se refere o nº 1 não pode ser anulada pelo titular dos dados;
b) Se o tratamento for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos dados em matéria de legislação laboral, de segurança social e de proteção social, na medida em que esse tratamento seja permitido pelo direito da União ou dos Estados-Membros ou ainda por uma convenção coletiva nos termos do direito dos Estados-Membros que preveja garantias adequadas dos direitos fundamentais e dos interesses do titular dos dados;
c) Se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;

interesses vitais do titular e motivos de interesse público importante. Ademais, o Considerando 51, estabelece que "[m]erecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais" (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

A LGPD cuida "Do Tratamento de Dados Pessoais Sensíveis", na Seção II, do Capítulo II (art. 11 e ss.). Pode-se dizer que o art. 11 da LGPD mantém várias das bases legais para tratamento de dados pessoais constantes do art. 7º [69], excluindo do tratamento de dados

---

d) Se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares;
e) Se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;
f) Se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial ou sempre que os tribunais atuem no exercício da sua função jurisdicional;
g) Se o tratamento for necessário por motivos de interesse público importante, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular dos dados;
h) Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas no nº 3;
i) Se o tratamento for necessário por motivos de interesse público no domínio da saúde pública, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos, com base no direito da União ou dos Estados-Membros que preveja medidas adequadas e específicas que salvaguardem os direitos e liberdades do titular dos dados, em particular o sigilo profissional;
j) Se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89º, nº 1, com base no direito da União ou de um Estado-Membro, que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas adequadas e específicas para a defesa dos direitos fundamentais e dos interesses do titular dos dados (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

[69] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2019b).

sensíveis as hipóteses de interesse legítimo do controlador ou terceiro[70] (art. 7º, IX, LGPD), de proteção de crédito (art. 7º, X, LGPD) (PINHEIRO, 2018, p. 40-41; MIRAGEM, 2020, p. 101-102; VIOLA e TEFFÉ, 2021, p. 154) e execução de contrato (art. 7º, V, LGPD)[71].

A LGPD estabelece que, quando se trata de dados sensíveis, além de observar os preceitos do art. 5º, XII (livre, informado, inequívoco), o consentimento deve ser "específico"[72] e "destacado" (art. 11, I, LGPD)[73].

Para garantir que o consentimento foi dado livremente, os titulares dos dados devem receber soluções alternativas ao uso da FRT que sejam fáceis de usar (e.g., utilização de senha ou um crachá de identificação, no caso de autenticação/verificação), se parecer muito complicada em comparação à FRT, a escolha não pode ser considerada genuína (COUNCIL OF EUROPE, 2021c, p. 7). Mas o fato é que o emprego de tecnologias como a FRT estão tornando mais difícil para as pessoas exercerem seu arbítrio para "optar por sair" (*opt-out*) da vigilância, isso porque nem sempre são advertidas e, às vezes, quando são, não se respeita a opção por não participar, e.g., em Stratford, Reino Unido, ao verem cartazes alertando o público que câmeras com FRT as filmavam a partir de uma van da polícia estacionada, pessoas que cobriram o rosto ou puxaram os capuzes para não serem filmadas foram paradas pela polícia, um homem chegou a ser multado (DEARDEN, 2019).

De acordo com a *Convention 108+* (COUNCIL OF EUROPE, 2021c, p. 6-7):

- Quando se fala de autoridades públicas (ou entidades privadas autorizadas a desempenhar funções semelhantes às de autoridades públicas), diante da assimetria de poderes entre os titulares dos dados e essas entidades, como regra geral, **o consentimento não deveria ser o fundamento jurídico para utilização de FRT.**
- Quando se fala em entidades privadas (excetuadas as no exercício de tarefas públicas), para que se use a FRT, exige-se o consentimento explícito, específico, livre e informado das pessoas cujos dados biométricos são processados.

---

[70] "No lugar da hipótese relativa ao legítimo interesse, o Art. 11, II, 'g', trouxe base mais específica, que visa à prevenção de fraudes e garantir a segurança do titular, restando vinculada aos interesses dos titulares e determinadas entidades. Como exemplo de aplicação, aponta-se a seguinte situação: **instituições bancárias e empregadores podem tratar dados biométricos para a prevenção de fraudes, sem o consentimento prévio dos titulares dos dados, a fim de confirmar que é o empregado autorizado que está entrando em área de acesso restrito da empresa ou que é determinado cliente que está realizando uma transação bancária por meio de um caixa eletrônico**, por exemplo. Adicionalmente, pode-se mencionar a exigência para atendimento médico-hospitalar, **com a utilização de seguro ou plano de assistência à saúde, que o segurado/beneficiário coloque seu polegar em um leitor biométrico para confirmar sua identidade**, a fim de evitar que outra pessoa utilize a cobertura securitária em seu lugar" (VIOLA e TEFFÉ, 2021, p. 154-155, grifo meu).

[71] Ainda que haja controvérsia se, em algum grau, esta previsão legal não estaria contida no art. 11, II, d, ao mencionar "inclusive em contrato" na situação específica de "exercício regular de direitos".

[72] Apesar da diferença semântica entre as palavras "expresso" (adotada pelo GDPR) e "específico" (adotada pela LGPD), a doutrina tem entendido que o efeito prático tende a ser o mesmo (BIONI, 2019, p. 202-203).

[73] 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; (BRASIL, 2019b).

Mendes e Fonseca (2021, p. 103-107) apontam que diante das limitações do paradigma do consentimento, é possível lançar mão de conceitos, estratégias e instrumentos complementares, dentre os quais enumeram:

1. A proteção de dados por meio da tecnologia e da arquitetura dos sistemas informacionais (proteção de dados *by design*) como forma de aumentar a confiança do titular na tecnologia (Seção 3.4.6);
2. A análise prévia de riscos e implantação de uma regulação embasada no *accountability*, de maneira que a responsabilidade seja compartilhada entre os atores, com foco no controlador (público ou privado) não ficando o ônus restrito exclusivamente ao gerenciamento do titular pelo seu consentimento. Neste cenário, ganham protagonismo os Relatórios de Impacto de Proteção de Dados Pessoais (RIPD) (Seção 3.7);
3. Estabelecimento de limites materiais ao consentimento, o que envolve ações preventivas combinadas a "considerações éticas", "limites jurídicos" e "salvaguardas" aplicadas ao tratamento dos dados e ao próprio consentimento como forma de materializar a autonomia e o contexto em que foi concedido, e.g., institutos civis como vício de vontade, abuso de poder, boa-fé, tutela da confiança. Isso também implica que quando se trata de dados sensíveis (como os biométricos), a análise ocorre a partir de parâmetros mais rígidos quanto à forma e à finalidade.

Como reiteradamente mencionado neste trabalho, muitas vezes tem-se o emprego amplo da FRT sem que o titular sequer tome conhecimento do seu uso sobre dados pessoais que são sensíveis e que, por suas características e natureza, são marcados pela capacidade de uso discriminatório, seja pelo Estado, seja pelo mercado. A esse cenário, acresça-se a já mencionada assimetria de poderes entre titulares dos dados e entidades que empregam a FRT. Diante disso, **pode-se concluir que o consentimento, geralmente, não se constitui em base legal para a utilização de FRT**.

Há abertura para tratamento de dados sensíveis sem a necessidade de fornecimento de consentimento do titular de dados nas sete hipóteses previstas no art. 11, II, LGPD[74], mormente

[74] Art. 11. [...] II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
a) cumprimento de obrigação legal ou regulatória pelo controlador;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
e) proteção da vida ou da incolumidade física do titular ou de terceiro;
f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou
f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019)
g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL, 2019b).

relacionadas à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos, além de outras hipóteses relacionadas, em grande medida, a interesses públicos. Nestes casos, seria possível prescindir do consentimento do titular dos dados sensíveis por um sopesamento de interesses realizado pela lei, *a priori*, que consideraria prevalecentes os interesses de natureza pública frente aos interesses do titular, ainda que este último tenha atributo de direito fundamental (MULHOLLAND, 2018, p. 168). Entretanto, justamente por ser primordial ao pleno exercício de direitos como os da igualdade, liberdade e privacidade que Mulholland (2018, p. 168) sustenta que este posicionamento legislativo deve ser questionado. Diante disto, a **avaliação do equilíbrio dos interesses e, portanto, da base legal, deveria ser feita caso a caso** (EDPB, 2019, p. 10).

Viola e Teffé (2021, p. 146, 156) entendem que dentre as hipóteses previstas no art. 11 da LGPD não haveria hierarquia, de maneira que nenhuma seria superior às demais. Inclusive, seria possível a utilização de mais de uma base legal para um tratamento de dados, devendo-se buscar aquela mais "adequada e segura para a situação concreta".

3.6 Direito de revisão das decisões automatizadas (art. 20, LGPD)

Conforme visto na Seção 2.1, por sua própria definição, a **FRT é um processo automatizado**. A presença cada vez mais constate de sistemas de decisão automatizada associada a pouca transparência quanto ao seu uso e funcionamento torna mais difícil a tarefa de discernir entre práticas abusivas, discriminatórias ou monopolísticas. Neste cenário, ganham relevância princípios (e.g., da transparência) e direitos (e.g., à informação, de revisão de decisões automatizadas) (MONTEIRO, 2018, p. 1).

Uma vez que o reconhecimento facial **se baseia no tratamento de dados pessoais**, todos os direitos previstos no Capítulo III da LGPD, que trata "Dos direitos do titular", são garantidos aos titulares dos dados, dentre os quais se destacam os direitos: (i) **à autodeterminação informativa** (art. 17)[75]; (ii) **à informação** (art. 18, I)[76]; (iii) **de acesso** (art. 18, II)[77]; (iv) **de retificação** (art. 18, III)[78] (e.g., no caso de falsos positivos, os titulares dos dados podem solicitar retificação para evitar correspondências falsas adicionais/repetitivas); (v) **à oposição** (art. 18, §2º)[79]; (iv) **de revisão de decisões automatizadas** (art. 20). Todos são muito importantes e derivam em maior ou menor grau dos princípios prescritos na própria

[75] Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei (BRASIL, 2019b).

[76] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; (BRASIL, 2019b).

[77] Art. 18. [...] II - acesso aos dados; (BRASIL, 2019b).

[78] Art. 18. [...] III - correção de dados incompletos, inexatos ou desatualizados; (BRASIL, 2019b).

[79] Art. 18. [...] § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei (BRASIL, 2019b).

LGPD, em especial do **livre acesso** (art. 6º, IV)[80], **da qualidade dos dados** (art. 6º, V)[81], **da transparência** (art. 6º, VI), **da prevenção** (art. 6º, VIII), **da não discriminação** (art. 6º, IX), **da responsabilização e prestação de contas** (art. 6º, X).

Erros podem ocorrer e não raro ocorrem, é um risco inerente ao uso da FRT (como visto na Seção 2.4.1). Qualquer uma das taxas de erro (falsos positivos e falsos negativos) são potencialmente problemáticas. E quando erros acontecem, eles devem poder ser desafiados[82].

Dado que a FRT é um processo automatizado, quando seu uso se destina a permitir que seja **tomada uma decisão que afetaria significativamente o titular dos dados**, este último deveria ter o direito de que sua opinião seja levada em consideração (COUNCIL OF EUROPE, 2021c, p. 16). Esse direito é tratado no art. 20, da LGPD, e o restante desta Seção tecerá considerações sobre ele.

Com a crescente automatização de decisões, ainda que a palavra final seja dada por um humano, o processo decisório pode ter sido baseado em uma análise algorítmica, de maneira que nem mesmo o tomador da decisão conseguiria explicá-la. Neste sentido, vêm-se defendendo o **direito ao devido processo informacional**, relacionado à garantia de entender (receber uma explicação) e poder contestar decisões que afetem os interesses do titular de dados (BIONI e MARTINS, 2020b; BRASIL, 2020d, p. 114).

A ideia por trás do "devido processo informacional" encontra analogia com o "devido processo legal": da mesma forma que uma pessoa não pode ser privada de sua vida, liberdade, propriedade, sem o devido processo legal, certos tipos de levantamentos, usos e disseminação de informação podem ser desafiados a fim de permitir que os titulares dos dados possam entender e se posicionar frente a decisões que tenham impacto em seus interesses (CITRON e PASQUALE, 2014, p. 19-20).

Como visto na Seção 3.4.3, a transparência é um dos temas mais críticos e debatidos quando se fala em FRT. A LGPD prevê explicitamente o princípio da transparência no art. 6º, VI, que dá origem ao **direito de acesso** aos dados pessoais (art. 6º, IV, LGPD), este, por sua vez, é robustecido pelo art. 19 (BRASIL, 2019b, grifo meu):

> Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, **mediante requisição do titular**:
> I - **em formato simplificado, imediatamente**; ou
> II - por meio de declaração **clara e completa**, que indique a origem dos dados, a inexistência de registro, **os critérios utilizados e a finalidade do tratamento**, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular.

[80] Art. 6º [...] 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; (BRASIL, 2019b).

[81] Art. 6º [...] 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; (BRASIL, 2019b).

[82] Não se pode perder de vista, como ressaltado em diversas oportunidades neste trabalho, que muitas vezes o titular dos dados sequer tem conhecimento de que seus dados estão sendo tratados por FRT, assim, não raro, apenas quando algum erro acontece o titular dos dados é acionado (ou não).

De uma leitura sistemática da LGPD à luz das discussões e diretrizes internacionais de proteção de dados ter-se-ia a consubstanciação de outros dois direitos (MONTEIRO, 2018, p. 3):

1. **Direito à explicação**: verdadeiro corolário do direito à transparência, diz respeito ao direito a receber informações úteis, suficientes, claras e compreensíveis, capazes de permitir ao titular entender a racionalidade e os critérios utilizados para o tratamento de seus dados pessoais para uma determinada finalidade.
2. **Direito à revisão de decisões automatizadas**: direito do titular requerer a revisão de uma decisão totalmente automatizada que impacte seus interesses, produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente, em especial a análise e previsão de aspectos relacionados com o desempenho profissional, situação econômica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocamentos do titular dos dados, bem como outros aspectos da sua personalidade (art. 20, LGPD; Considerando 71[83] e art. 22[84], GDPR).

[83] (71) O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana. Esse tratamento inclui a definição de perfis mediante qualquer forma de tratamento automatizado de dados pessoais para avaliar aspetos pessoais relativos a uma pessoa singular, em especial a análise e previsão de aspetos relacionados com o desempenho profissional, a situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou deslocações do titular dos dados, quando produza efeitos jurídicos que lhe digam respeito ou a afetem significativamente de forma similar. No entanto, a tomada de decisões com base nesse tratamento, incluindo a definição de perfis, deverá ser permitida se expressamente autorizada pelo direito da União ou dos Estados-Membros aplicável ao responsável pelo tratamento, incluindo para efeitos de controlo e prevenção de fraudes e da evasão fiscal, conduzida nos termos dos regulamentos, normas e recomendações das instituições da União ou das entidades nacionais de controlo, e para garantir a segurança e a fiabilidade do serviço prestado pelo responsável pelo tratamento, ou se for necessária para a celebração ou execução de um contrato entre o titular dos dados e o responsável pelo tratamento, ou mediante o consentimento explícito do titular. Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Essa medida não deverá dizer respeito a uma criança.
A fim de assegurar um tratamento equitativo e transparente no que diz respeito ao titular dos dados, tendo em conta a especificidade das circunstâncias e do contexto em que os dados pessoais são tratados, o responsável pelo tratamento deverá utilizar procedimentos matemáticos e estatísticos adequados à definição de perfis, aplicar medidas técnicas e organizativas que garantam designadamente que os fatores que introduzem imprecisões nos dados pessoais são corrigidos e que o risco de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais riscos para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos. A decisão e definição de perfis automatizada baseada em categorias especiais de dados pessoais só deverá ser permitida em condições específicas (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

[84] Artigo 22º - Decisões individuais automatizadas, incluindo definição de perfis
1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.
2. O nº 1 não se aplica se a decisão:
a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento;

O art. 20 da LGPD determinava o direito de revisão como um direito de revisão humana, i.e., feito por uma pessoa natural, conforme a redação constante do Parecer ao Projeto de Lei (COMISSÃO ESPECIAL, 2018, p. 71, grifo meu):

> Art. 20. O titular dos dados tem direito a solicitar revisão, **por pessoa natural**, de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo, de crédito ou aspectos de sua personalidade.

Contudo, a Lei nº 13.853/2019, que alterou a LGPD para dispor sobre a proteção de dados pessoais e para criar a ANPD (conversão da Medida Provisória nº 869/2018), além de alterar a redação do *caput* do art. 20 (excluindo da redação final a expressão "por pessoa natural"), vetou seu §3º (BRASIL, 2019c), conforme Mensagem nº 288, de 8 de julho de 2019 (BRASIL, 2019d, grifo do original):

> Ouvidos, os Ministérios da Economia, da Ciência, Tecnologia, Inovações e Comunicações, a Controladoria-Geral da União e o Banco Central do Brasil manifestaram-se pelo veto ao seguinte dispositivo:
> **§ 3º do art. 20 da Lei nº 13.709, de 14 de agosto de 2018, alterado pelo art. 2º do projeto de lei de conversão**
> "§ 3º A revisão de que trata o caput deste artigo deverá ser realizada por pessoa natural, conforme previsto em regulamentação da autoridade nacional, que levará em consideração a natureza e o porte da entidade ou o volume de operações de tratamento de dados."
> **Razões do veto**
> "A propositura legislativa, ao dispor que toda e qualquer decisão baseada unicamente no tratamento automatizado seja suscetível de revisão humana, contraria o interesse público, tendo em vista que tal exigência inviabilizará os modelos atuais de planos de negócios de muitas empresas, notadamente das startups, bem como impacta na análise de risco de crédito e de novos modelos de negócios de instituições financeiras, gerando efeito negativo na oferta de crédito aos consumidores, tanto no que diz respeito à qualidade das garantias, ao volume de crédito contratado e à composição de preços, com reflexos, ainda, nos índices de inflação e na condução da política monetária."

Portanto, a redação atual do art. 20 da LGPD dispõe (BRASIL, 2019b, grifo meu):

> Art. 20. O titular dos dados tem **direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses**, incluídas as decisões destinadas a **definir o seu perfil** pessoal, profissional, de consumo e de crédito ou os **aspectos de sua personalidade**. (Redação dada pela Lei nº 13.853, de 2019)

---

b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou

c) For baseada no consentimento explícito do titular dos dados.

3. Nos casos a que se referem o nº 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão.

4. As decisões a que se refere o nº 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9º, nº 1, a não ser que o nº 2, alínea a) [titular dos dados tiver dado seu consentimento] ou g) [o tratamento for necessário por motivos de interesse público relevante], do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

> § 1º O controlador deverá fornecer, sempre que solicitadas, **informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada**, observados os **segredos comercial e industrial**.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, **a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais**.
> § 3º (VETADO). (Incluído pela Lei nº 13.853, de 2019)

Pode-se segmentar o art. 20 em três partes/condições: (i) uma decisão é tomada que é (ii) baseada exclusivamente no tratamento automatizado e (iii) afeta os interesses do titular dos dados.

O primeiro elemento capaz de acionar o art. 20 é a presença de uma "decisão", que pode ser interpretada em sentido amplo, como uma atitude ou posição particular tomada em relação a uma pessoa, se essa posição tiver, pelo menos, probabilidade de ser posta em prática (MENDOZA e BYGRAVE, 2017, p. 10-11; BRKAN, 2019, p. 102).

O segundo elemento diz respeito à decisão ser "baseada exclusivamente no tratamento automatizado". Sua avaliação depende se a intervenção humana é possível de uma perspectiva técnica ou se o processo de tomada de decisão é construído de forma exclusivamente algorítmica, sem espaço para o envolvimento humano. É um ponto que, como será visto adiante, está em discussão/disputa.

As "Diretrizes sobre tomada de decisão individual automatizada e criação de perfil" (WP 251 ver.01) do *Article 29 Working Party* (recepcionadas pelo *European Data Protection Board* – EDPB), apontam que se o processo permitir tecnicamente a intervenção humana, então deve-se avaliar se a ação realizada por pessoa natural é "significativa" ou apenas um "gesto simbólico" procedimental (WP29, 2018, p. 21). Para descaracterizar a decisão como "unicamente com base e tratamento automatizado", a intervenção deveria ser "realizada por quem tenha autoridade e competência para alterar a decisão". Além disso, o ser humano envolvido não deveria apenas ter o poder de mudar a decisão, mas realmente exercer essa competência "considerando todos os dados relevantes" e verificando a substância e a exatidão da decisão gerada pela máquina (WP29, 2018, p. 8), caso contrário, ainda que houvesse intervenção humana, ela não descaracterizaria a decisão como "tomada unicamente com base e tratamento automatizado", i.e., estar-se-ia diante de decisão unicamente automatizada.

Por fim, conforme o terceiro elemento, a decisão deve "afetar" os interesses do titular dos dados, incluído, mas não limitado, à definição de "perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade". Alguns critérios para efeito sobre interesses do titular incluem (WP29, 2018, p. 21): (i) afetar significativamente as circunstâncias, comportamento ou escolhas dos indivíduos em questão; (ii) ter um impacto prolongado ou permanente no titular dos dados; ou (iii) no seu extremo, levar à exclusão ou discriminação de indivíduos.

Em que pesem as alterações no que diz respeito à revisão por pessoa natural, a LGPD trouxe importantes avanços na temática, como a ampliação do dever de transparência e de fornecimento de informações quanto a decisões automatizadas. Contudo, dois importantes pontos esperam por uma melhor definição (BIONI; MARTINS, 2020):

1. Quais os parâmetros do direito de revisão, já que **não há mais a previsão expressa da revisão humana** na LGPD.
2. O que de fato são decisões tomadas **unicamente** com base em tratamento automatizado, i.e., no âmbito da discussão aqui procedida, essencial estabelecer qual será a interpretação dada ao termo "unicamente":
    a. **Literal**, o que praticamente esvaziará o direito de revisão ou;
    b. **Sistemática e ampliativa**, na qual se dará abertura para efetiva aplicação do direito de revisão, considerando-se o grau de automatização dos processos decisórios, ainda que não totalmente automatizados.

Entende-se que esta última seria uma interpretação possível e adequada, capaz de permitir ao cidadão, de maneira mais propícia, o exercício de seus direitos e garantias fundamentais.

Esse é também o entendimento de Enrico Roberto (SAKAI *et al.*, 2020), segundo o qual a proposta que mais coaduna com a intenção trazida pelo legislador seria uma compreensão de decisão "unicamente (ou totalmente) automatizada" como "aquela em que todas as fontes de informação necessária para se chegar à decisão vieram do algoritmo, e não daquela pessoa apontada como responsável para tomar a decisão", i.e., a descaracterização da noção de "unicamente automatizada" só ocorreria caso a atuação humana no processo decisório realmente envolvesse atuação significativa e competência decisória humanas. Um papel apenas formal desempenhado por um humano, envolvendo uma simples validação do resultado do sistema de decisão automatizada, não seria suficiente para descaracterizar a decisão como "unicamente automatizada".

Corrobora esse entendimento o posicionamento do ICO, do Reino Unido, segundo o qual para descaracterizar uma decisão tomada unicamente com base em tratamento automatizado, o envolvimento humano deve ser ativo e não apenas um gesto simbólico, i.e., se um humano revisa a decisão antes de ela ser aplicada e tem discricionariedade para alterá-la, e não simplesmente aplicando a decisão tomada pelo sistema automatizado (ICO, 2021b).

Como mencionado na Seção 2.4.1, a supervisão humana dos resultados da FRT, com treinamento especializado, é benéfica. Sem embargo, também foi visto na Seção 2.4.1 que muitas vezes as pessoas são psicologicamente desencorajadas a desafiar as decisões automatizadas, de maneira que, mesmo que sirva apenas de recomendação para tomada de decisão, o resultado algorítmico pode ser um elemento decisivo. Nesta perspectiva, ainda mais importante o direito à revisão de decisões em que a automatização tenha tido um papel relevante.

Segundo Juliana Sakai, em resposta a levantamento que buscou mapear a maneira como sistemas de decisão automatizada têm sido utilizados no âmbito do Poder Público (Projeto Transparência Algorítmica) todos os órgãos consultados informaram que essas ferramentas têm sido utilizadas somente para dar suporte à tomada de decisão humana, e não elas mesmas como tomadoras de decisão (SAKAI *et al.*, 2020; TRANSPARÊNCIA BRASIL, 2020, p. 19-21). Isso evidencia a disputa entre três eixos: (i) o conceito de "decisão unicamente automatizada"; (ii) a prática corrente no uso de sistemas de decisão; e (iii) a viabilização do

exercício de direito de revisão. Ou seja, para dar alguma efetividade ao art. 20 da LGPD, sua interpretação necessariamente deveria ser ampliativa.

Ademais, as diretrizes internacionais apontam que qualquer uso de tecnologias automatizadas deve envolver algum nível de interação humana e não deve ser feito de forma puramente automatizada (ICO, 2017, p. 32; ACLU *et al.*, 2018). Assim, as entidades que utilizam FRT devem assegurar-se que os operadores humanos desempenhem um papel decisivo nas ações realizadas com os resultados dessas tecnologias, mas, ao mesmo tempo, devem tomar medidas organizacionais para supervisionar os operadores humanos tomando decisões que podem ter um impacto significativo sobre os indivíduos (COUNCIL OF EUROPE, 2021c, p. 14).

Quando a FRT é usada para *autenticação/verificação* (confirmar a identidade de uma pessoa conhecida), do ponto de vista do titular dos dados que tenta acessar um serviço, por exemplo, a maior contrariedade está relacionada a falsos negativos[85] (i.e., não ter seu acesso validado). Isso é particularmente problemático diante da menor acurácia associada a alguns grupos, e.g., pessoas pretas e minorias étnicas, jovens e mulheres (como visto na Seção 2.4.3). O que pode, no mínimo, representar constrangimento diante da negativa de acesso, e.g., a um clube, academia; escola; transporte público; portais de um aeroporto; conjunto habitacional; edifício público ou particular; serviço, benefício ou política pública. Caso não haja um mecanismo alternativo de identificação, a situação se agrava, pois nem sempre é possível acionar o direito de revisão de decisões automatizadas num momento em que se necessita de uma solução rápida/imediata.

Quando se fala do uso de FRT em *identificação* (reconhecer uma pessoa desconhecida, distinguindo-a de um conjunto maior de indivíduos) do ponto de vista do titular de dados, a maior adversidade está associada a falsos positivos (i.e., dizer que é quem ele não é), o que muitas vezes, conforme visto na Seção 2.4.3, tem impacto sobre a "presunção de inocência", colocando sobre essas pessoas o ônus de mostrar que não são quem a FRT identifica, com consequências potencialmente sérias na esfera de liberdade e direitos fundamentais do titular dos dados, e.g., em aplicações de *identificação*, como detecção de fraude de solicitação de visto ou de passaporte, uma falha correspondência positiva com outro indivíduo pode levar a uma acusação, detenção ou deportação (GROTHER *et al.*, 2019, p. 5).

Por fim, quanto ao uso da FRT para *categorização* (processo de extração de características de uma pessoa, a fim de a integrar em uma ou várias categorias amplas), também como visto na Seção 2.4.3, eleva-se o potencial discriminatório a outro patamar, não só no que diz respeito à "descaracterização" do indivíduo, mas também devido à possibilidade de perfilhamento e seu potencial discriminatório, e isso ocorre não devido a algo que a pessoa efetivamente tenha feito, mas por sua "inclusão em um grupo" no qual as inferências ou correlações feitas por algoritmos "sugerem" que ela pode vir a se comportar de maneira que a

[85] No caso de *autenticação/verificação*, um falso positivo (e.g., não rejeitar um impostor) pode também ser problemático, pois pessoas não autorizadas podem ter acesso a locais ou serviços que não deveriam, mas do ponto de vista de direitos e liberdades fundamentais, entende-se que um falso negativo atentaria de maneira mais contundente na esfera de interesses do titular dos dados no que diz respeito à *autenticação/verificação*. Faz-se a ressalva que aqui está-se fazendo uma generalização, sendo possível contraexemplos nos quais um falso positivo seja mais crítico do que um falso negativo, o que depende, obviamente, da situação em concreto.

torna "arriscada" ou "inadequada", e.g., para concessão de crédito ou de seguro, para uma vaga de emprego, para admissão em escolas ou outras instituições (CITRON e PASQUALE, 2014, p. 24). Neste sentido, a seriedade das consequências associadas a dados inexatos e a vieses algorítmicos, capazes de "gerar predições, inferências e interpretações verdadeiramente discriminatórias acerca de um indivíduo ou de um segmento social" (MENDES e FONSECA, 2021, p. 99).

Apesar de poder-se ocultar a lógica do processamento com base no segredo comercial e industrial (art. 20, § 1º, LGPD), o direito à revisão pode ser articulado ao acesso à informação analisada para se chegar à decisão, e.g., no caso de categorização, o direito à revisão pode permitir ao titular promover a correção e/ou atualização dos dados que levaram à definição do perfil, o que lhe possibilitaria obter classificação eventualmente mais vantajosa.

Diante disso, importa destacar que a ideia de explicabilidade quando aplicada ao processo decisório, geralmente se refere às "razões ou justificativas para aquele resultado em particular, e não a uma descrição do processo decisório em geral" (DOSHI-VELEZ e KORTZ, 2017)

Destarte, existem alguns mecanismos indiretos que permitem analisar se decisões automatizadas estão sendo tomadas de forma justa, com respeito aos princípios legais, sem a quebra do segredo de negócio: (i) informação sobre os tipos de dados usados para alimentar a base de dados; (ii) quais decisões são realmente tomadas por sistemas de decisão automatizada; (iii) como tais decisões podem afetar direitos fundamentais; (iv) quais populações são afetadas pela decisão automatizada; (v) quais testes foram feitos com o sistema de decisão automatizada para evitar discriminações (BIONI; MARTINS, 2020).

De todo o exposto, quanto ao emprego de FRT – seja para identificação, verificação ou categorização –, entende-se que a LGPD garante (MONTEIRO, 2018, p. 14):

1. Acesso aos tipos de dados pessoais e aos dados propriamente ditos usados como entrada do sistema responsável pelo processo de decisão automatizada.
2. Se o processo automatizado tiver por finalidade formar um perfil, ou se utilizar de um perfil para tomada de decisão, o direito de acesso aos dados poderá incluir, os dados anonimizados utilizados para enriquecer tais perfis (art. 12, §2º, LGPD)[86].
3. O direito de receber explicações claras acerca dos critérios utilizados para tomar a decisão automatizada, observados os segredos comercial e industrial (art. 20, §1º, LGPD), que devem ser analisados no caso concreto, pois estes conceitos não se encontram definidos na LGPD;
    a. A possibilidade de auditoria pela ANPD para verificação de aspectos discriminatórios (no caso do art. 20, §2º, LGPD).
4. O direito de requerer revisão (contestar a decisão e manifestar o seu ponto de vista) caso a decisão automatizada tenha consequências nos interesses do titular, o que se presume, no caso de perfis comportamentais. E, apesar de não garantida pela legislação brasileira atual, entende-se que essa revisão deva ser promovida por

[86] Art. 12 [...] § 2º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, aqueles utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada.

pessoa natural, em consonância com os debates doutrinários nacionais e internacionais a respeito do assunto[87].

Por fim, independentemente do direito à revisão de decisões automatizadas, em havendo dano em razão do tratamento de dados pessoais, surge a obrigação de reparação. Quanto a isso, cumpre mencionar a Seção III, do Capítulo VI, da LGPD, que trata "Da Responsabilidade e do Ressarcimento de Danos", em especial, o *caput* do art. 42, que dispõe (BRASIL, 2019b):

> 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.

3.7 Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

O monitoramento sistemático por videovigilância (geralmente para fins de proteção patrimonial) traz a coleta e retenção de informações pictóricas ou audiovisuais sobre **todas as pessoas que entram no espaço monitorado** que são identificáveis com base em sua aparência ou outros elementos específicos. A intrusividade se agrava quando à videovigilância é agregada à FRT. O risco potencial de uso indevido desses dados aumenta em relação à dimensão do espaço monitorado, bem como ao número de pessoas que frequentam o espaço.

O responsável pelo tratamento deve avaliar os riscos de intrusão dos direitos do titular dos dados. O critério decisivo para isso é a intensidade da intervenção que, segundo o EDPB (2019, p. 10), pode ser definido pelo: (i) tipo de informação coletada (conteúdo da informação); (ii) escopo (densidade da informação, extensão espacial e geográfica); (iii) quantidade de titulares de dados sob vigilância (seja como um número específico ou como uma proporção de uma população relevante); (iv) situação em questão; (v) os reais interesses do grupo de titulares dos dados; (vi) meios alternativos; (vii) a natureza e âmbito da avaliação dos dados.

Isso é refletido pelo GDPR no art. 35(3)(c)[88], que exige a realização de uma avaliação de impacto sobre a proteção de dados em caso de monitoramento sistemático de uma área acessível ao público em grande escala, bem como no art. 37(1)(b)[89], que exige que o

---

[87] "[...] o caminho a ser trilhado deve sempre guiar-se pelo papel humano no processo de automação. Isso não quer dizer apenas a possibilidade de revisão de decisões automatizadas por pessoas naturais, mas também a centralidade do elemento humano em todo o processo de desenho dos mecanismos [...] a centralidade humana também precisa estar refletida no processo de revisão de decisões automatizadas" (MENDES e MATTIUZZO, 2019, p. 60-61).

[88] Artigo 35º - Avaliação de impacto sobre a proteção de dados
1. Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação.
[...] 3. A realização de uma avaliação de impacto sobre a proteção de dados a que se refere o nº 1 é obrigatória nomeadamente em caso de: [...]
c) Controlo sistemático de zonas acessíveis ao público em grande escala. (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

[89] Artigo 37º - Designação do encarregado da proteção de dados

responsável designe um encarregado da proteção de dados, se a operação de tratamento implicar, pela sua natureza, um acompanhamento regular e sistemático de pessoas (EDPB, 2019, p. 5). Mas também no art. 35(3)(a)[90], o que inclui a FRT para fins de categorização/perfilamento e o art. 35(3)(b)[91] que exige a avaliação de impacto para tratamento em larga escala[92] (o que evidentemente inclui, mas não se restringe a espaços públicos) de categorias especiais de dados a que se refere o art. 9(1)[93], que inclui dados biométricos para identificação. Cumpre mencionar que a lista do art. 35(3) é exemplificativa (i.e., não exaustiva) (WP29, 2017, p. 8-9) sendo que há a possibilidade de a Autoridade de Proteção de Dados elaborar lista de operações para as quais a avaliação de impacto seja obrigatória (art. 35(4), GDPR)[94].

É consenso que a FRT envolve sérios riscos a direitos e liberdades de cidadãos. Para grande parte da população, que não detém a tecnologia nem o conhecimento para reconhecer a extensão do impacto sobre os seus dados pessoais, estes riscos são de difícil mensuração. Tem-se, assim, a associação de dois elementos explosivos: (i) riscos consideráveis, de um lado e; (ii) assimetria informacional e de poder, de outro lado. Diante disso, impõe-se a implantação de processos detalhados de avaliação e mitigação dos riscos, sob responsabilidade de quem controla o uso destas tecnologias de coleta e tratamento de dado, além de prestação de contas e abertura para a participação nesse processo regulatório (BIONI e RIELLI, 2019, p. 5).

Nesse contexto, o Relatório de Impacto de Proteção de Dados Pessoais (RIPD) surge como uma ferramenta fundamental no processo de conformidade com a legislação de proteção de dados, em especial com o princípio da responsabilização e prestação de contas

---

1. O responsável pelo tratamento e o subcontratante designam um encarregado da proteção de dados sempre que:
[…]
b) As atividades principais do responsável pelo tratamento ou do subcontratante consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controlo regular e sistemático dos titulares dos dados em grande escala; (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

[90] Artigo 35º [...] 3. [...] a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, **incluindo a definição de perfis**, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar; (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016, grifo meu)..

[91] Artigo 35º [...] 3. [...] b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere **o artigo 9º, nº 1**, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10º; (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016, grifo meu).

[92] Segundo o *Article 29 Working Party*, apesar de não haver no GDPR uma definição para o que seria "larga escala", critérios que devem ser levados em conta na sua caracterização são: (i) a quantidade de pessoas envolvidas, seja em números absolutos ou como uma proporção da população relevante; (ii) o volume da dados ou a quantidade de itens distintos sendo processados; (iii) a duração ou permanência da atividade de processamento; (iv) a extensão geográfica da atividade de processamento (WP29, 2017, p. 10).

[93] Artigo 9º [...] 1. É proibido o tratamento de dados pessoais que revelem a **origem racial ou étnica**, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, **dados biométricos para identificar uma pessoa de forma inequívoca**, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016, grifo meu).

[94] Artigo 35º [...] 4. A autoridade de controlo elabora e torna pública uma lista dos tipos de operações de tratamento sujeitos ao requisito de avaliação de impacto sobre a proteção de dados por força do nº 1. A autoridade de controlo comunica essas listas ao Comité referido no artigo 68º (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

(*accountability*), mas mais do que isso, o RIPD é uma ferramenta de governança de dados, a ser incorporada à rotina da organização (e não apenas uma peça burocrática) (GOMES, 2019b, p. 14; KLOZA *et al.*, 2020, p. 3). Neste sentido, idealmente, as avaliações de impacto devem ser realizadas em intervalos regulares (WP29, 2017, p. 6, 14, 20; KLOZA *et al.*, 2020, p. 3; COUNCIL OF EUROPE, 2021c, p. 14).

Cumpre referir que o GDPR tornou o RIPD destaque no contexto regulatório de proteção de dados mundial, ao exigir a elaboração dos *Data Protection Impact Assessment* (DPIA) em situações nas quais o processamento de dados é capaz de gerar altos riscos aos direitos e liberdades das pessoas naturais (Considerando 84[95], e art. 35(1)[96], GDPR). Tal posicionamento é ratificado por trabalho do *Article 29 Working Party* (2017, p. 8-12), que estabeleceu orientações a respeito do DPIA e das situações nas quais seria obrigatório.

O RIPD vem de uma lógica de organização sistemática das operações de tratamento de dados, a fim de se identificar, prevenir ou mitigar riscos[97]. O pensamento primordial por trás do RIPD é um diagnóstico de prevenção (e não de reparação) (GOMES, 2019b, p. 8), daí ser um artefato que **deve, via de regra, ser produzido antes do tratamento do dado** (no caso em questão, antes da implantação da FRT) (WP29, 2017, p. 14; KLOZA *et al.*, 2020, p. 3, 5). A LGPD assim define o RIPD (BRASIL, 2019b):

> Art. 5º Para os fins desta Lei, considera-se:[...]
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

A definição do RIPD pode ser segmentada em três partes (GOMES, 2019b, p. 9-11):

---

[95] (84) A fim de promover o cumprimento do presente regulamento **nos casos em que as operações de tratamento de dados sejam suscetíveis de resultar num elevado risco para os direitos e liberdades das pessoas singulares**, o responsável pelo seu tratamento deverá encarregar-se da realização de uma **avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse risco**. Os resultados dessa avaliação deverão ser tidos em conta na determinação das medidas que deverão ser tomadas a fim de comprovar que o tratamento de dados pessoais está em conformidade com o presente regulamento. Sempre que a avaliação de impacto sobre a proteção de dados indicar que o tratamento apresenta um **elevado risco que o responsável pelo tratamento não poderá atenuar através de medidas adequadas**, atendendo à tecnologia disponível e aos custos de aplicação, **será necessário consultar a autoridade de controlo antes de se proceder ao tratamento de dados pessoais** (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016, grifo meu).

[96] Artigo 35º [...] 1. Quando um certo tipo de tratamento, em particular que utilize **novas tecnologias** e tendo em conta a sua natureza, âmbito, contexto e finalidades, for **suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares**, o responsável pelo tratamento procede, antes de iniciar o tratamento, a uma avaliação de impacto das operações de tratamento previstas sobre a proteção de dados pessoais. Se um conjunto de operações de tratamento que apresentar riscos elevados semelhantes, pode ser analisado numa única avaliação (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016, grifo meu)..

[97] Segundo a Associação Brasileira de Normas Técnicas (ABNT), risco é o efeito da incerteza nos objetivos. Ele normalmente é expresso em termos de fontes de risco, eventos, potenciais, suas consequências e suas probabilidades (ABNT, 2018, p. 7).

1. **documentação do controlador**: instrumentaliza a forma como o RIPD deve existir e ser apresentado, i.e., como um documento formal que atenda aos critérios descritos no restante do inciso.
2. **descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais**: consoante Gomes (2019b, p. 10-11), podem ser considerados **direitos fundamentais** os positivados no art. 5º da CF e, como **liberdades civis**, a liberdade de pensamento, liberdade religiosa, liberdade de expressão e liberdade de associação, todos eles inerentemente relacionados aos novos direitos dos titulares de dados, previstos nos arts. 17 a 21 da LGPD. Importa frisar bem que a análise/foco é quanto aos riscos às liberdades civis e aos direitos fundamentais **do titular de dados**, e não os riscos ao negócio do controlador.
3. **medidas, salvaguardas e mecanismos de mitigação desses riscos**: como **medidas**, pode-se entender ações afirmativas do controlador com vistas à redução ou gerenciamento dos riscos existentes, e.g., decidir não realizar operações que envolvam dados sensíveis. Como **salvaguardas**, pode-se considerar medidas preventivas que fomentam a mitigação dos riscos ou a redução dos danos causados por eles, e.g., contratação de um seguro específico contra incidentes de segurança. Já os **mecanismos** são um conjunto de ações positivas ou negativas (fazer ou deixar de fazer) que contribuirão para a mitigação dos riscos de uma determinada operação de tratamento de dados, e.g., desenvolvimento de produtos considerando a proteção de dados *by design* e *by default*.

Importa pontuar que os princípios da segurança (art. 6º, VII, LGPD) e da prevenção (art. 6º, VIII, LGPD) também justificam e densificam avaliações sistemáticas quanto à sensibilidade dos dados tratados, a probabilidade e a gravidade dos danos para os titulares dos dados (art. 50, §2º, LGPD)[98]. Esta pode ser entendida como uma fase que antecede a elaboração do RIPD, já que insta primeiro avaliar o risco e impacto das operações de tratamento da FRT nas liberdades civis e direitos fundamentais do indivíduo titular dos dados (GOMES, 2019b, p. 7).

Segundo as diretrizes que ditam as boas práticas internacionais, um RIPD deve ser baseado em evidências confiáveis, considerar a necessidade que o tratamento pretende atender e se o uso proposto tem uma base legal, é justificado, necessário e proporcional às necessidades identificadas. Assim, numa avaliação de emprego de FRT, deve ser explicitada (COUNCIL OF EUROPE, 2021c, p. 14):

- A legalidade do uso da FRT;
- Os direitos fundamentais em jogo no processamento;
- A vulnerabilidade dos titulares dos dados;

[98] Art. 50. [...] § 2º Na aplicação dos princípios indicados nos incisos VII [princípio da segurança] e VIII [principio da prevenção] do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: [...]

- Como esses riscos podem ser mitigados de forma eficaz.

Especificamente, ao considerar a implantação da FRT em espaços públicos, deve-se considerar (COUNCIL OF EUROPE, 2021c, p. 14):

- Avaliar e justificar a estrita necessidade e proporcionalidade da implantação da FRT;
- Abordar o risco para diferentes direitos fundamentais, incluindo proteção de dados, privacidade, liberdade de expressão, liberdade de reunião, liberdade de movimento, não discriminação, dependendo dos usos potenciais em diferentes lugares.

Durante a preparação do RIPD, as entidades devem envolver as partes interessadas, incluindo indivíduos afetados, para avaliar o impacto potencial sob sua perspectiva (WP29, 2017, p. 15; COUNCIL OF EUROPE, 2021c, p. 14).

É necessário incluir sistematicamente as autoridades de supervisão, em particular, consultá-las previamente à experimentação ou implantação prevista, sobretudo quando o controlador não encontra maneiras de reduzir o risco a um nível aceitável (WP29, 2017, p. 19; COUNCIL OF EUROPE, 2021c, p. 8, 14). Dependendo do dano potencial e da probabilidade de ocorrência do risco identificado pelo RIPD, a opção mais adequada pode ser a não utilização da tecnologia (não processamento do dado pessoal).

As autoridades devem ter acesso às avaliações de impacto realizadas, bem como a todas as auditorias, relatórios e análises realizadas no contexto de tais experiências ou projetos (COUNCIL OF EUROPE, 2021c, p. 8).

Por fim, após a conclusão do RIPD, apesar de não obrigatório e respeitados os segredos comercial e industrial (se aplicáveis), é interessante que a entidade publique o Relatório, ainda que parcialmente (e.g., o sumário ou a conclusão) para receber opiniões do público sobre a potencial implantação da FRT, como forma de construir confiança, bem como demonstrar *accountability* e transparência (WP29, 2017, p. 18; COUNCIL OF EUROPE, 2021c, p. 14).

Bioni e Rielli (2019, p. 4, 6), baseando-se na literatura teórica sobre o princípio da precaução no campo do direito ambiental[99], apresentaram uma avaliação da "força do RIPD" com base no normativo que o exige, pautado por um "princípio da precaução e estratégias regulatórias para FRT":

- **Fraca**: incertezas relacionas ao risco gerado pelo tratamento de dados não justificam inação por parte do controlador; entretanto, não há a atribuição de dever de ação para controlar o risco em si e gerar evidências a esse respeito.
- **Moderada**: incerteza na avaliação do risco justifica ação, mas há a atribuição de deveres para controlar o risco e gerar evidências a esse respeito; o controlador tem discricionariedade para prosseguir ou não com a atividade.

[99] A esse respeito é interessante mencionar que os primeiros *Privacy Impact Assessment* (PIA), previstos na Diretiva nº 95/46/EC, foram originalmente inspirados na legislação ambiental europeia (GOMES, 2019b, p. 8).

- **Forte**: diante da incerteza, inverte-se o ônus da prova para o emprego da FRT, que passa a ser do controlador; havendo ameaça de dano, impõem-se compulsoriamente medidas de precaução.

Preocupantemente, tomando por base a experiência estrangeira na regulação da FRT, Bioni e Rielli (2019, p. 5-11) entendem que a LGPD se enquadra no modelo fraco de aplicação do princípio da precaução no emprego da FRT, na medida em que:

1. Há baixa atribuição de deveres para os desenvolvedores de FRT e para o consumidor final que fará uso da tecnologia.
   1.1. Não há procedimentalização mínima das situações em que o RIPD é obrigatório nem quais elementos compõem o relatório, de maneira que a LGPD abre espaço para a adoção da FRT sem que haja ações correspondentes para mitigar seus riscos (que, como visto nas Seções 2.4.1 a 2.4.5, não são poucos e muito menos insignificantes).
   1.2. Não há previsão do controlador iniciar conversas regulatórias ao se deparar com uma situação de um risco não controlável, situação na qual notificaria a autoridade nacional antes de usar a FRT, a exemplo de mecanismo previsto no GDPR (art. 36(1))[100].
   1.3. Não há um processo de tomada de decisão que alcance atores distintos do controlador e da autoridade nacional, não prevendo um debate público, o que incluiria representantes dos interesses dos cidadãos nos circuitos decisórios.
2. No que diz respeito ao uso da FRT na esfera do setor privado, há espaço para futura regulamentação do RIPD pela ANPD, bem como a possibilidade de validação de códigos de boa conduta e mesmo de entidades certificadoras.
3. No âmbito do setor público, por força do art. 4º, §3º, da LGPD, foi retirado da autoridade nacional o poder de emitir opiniões técnicas, recomendações e de solicitar RIPD quando do emprego de FRT para fins de segurança pública, segurança nacional, defesa do Estado e investigações de natureza penal (situações parcialmente excepcionadas do escopo de aplicação da LGPD).

Entende-se que a análise quanto à necessidade de elaboração de RIPD deve ser feita caso a caso, à luz da situação concreta. Entretanto, no âmbito do objeto de estudo deste trabalho, considera-se que o uso de FRT, diante de aspectos cumulativos relativos à sua criticidade, à utilização de dados (biométricos) sensíveis[101], ao seu potencial invasivo, à utilização em espaços públicos, à assimetria informacional e de poder, seria capaz de gerar altos riscos aos

[100] Artigo 36º - consulta prévia. 1. O responsável pelo tratamento consulta a autoridade de controlo antes de proceder ao tratamento quando a avaliação de impacto sobre a proteção de dados nos termos do artigo 35º indicar que o tratamento resultaria num elevado risco na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o risco (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

[101] Art. 38. A autoridade nacional **poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis**, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados (BRASIL, 2019b, grifo meu).

direitos e liberdades das pessoas naturais, de maneira que deveria implicar na análise de riscos e consequente elaboração de RIPD, entretanto, a palavra final quanto a isso será da ANPD.

A ANPD pode e deve suprir lacunas tais como, indicar em quais situações o RIPD é obrigatório devido aos riscos associados ao tratamento dos dados, quais os elementos mínimos, emitir orientações, sugerir modelos e estruturas de RIPD que auxiliem os agentes de tratamento a compreender sua necessidade e importância (GOMES, 2019b, p. 9; 2019a, p. 13). Nesse intuito, a ANPD realizou entre 21 e 25 de junho de 2021 um conjunto de três reuniões técnicas para discussão do "processo de regulamentação do relatório de impacto à proteção de dados pessoais"[102] (ANPD, 2021c; 2021d; 2021e), tema previsto no item 7 da Agenda Regulatória Bianual da ANPD (ANPD, 2021b). Esse foi um esforço inicial acerca da temática de RIPD que será considerada na elaboração das diretrizes da Política Nacional de Proteção de Dados Pessoais e da Privacidade pela ANPD (art. 55-J, III, LGPD). Neste sentido, muito ainda tem que ser debatido, e as diretrizes específicas para o Brasil, pautadas pela ANPD, ainda estão em discussão/elaboração.

Por fim, cumpre destacar a observação de Gomes (2019a, p. 7-12) que a nossa LGPD traz, em um plano subjacente, a recomendação da adoção de uma abordagem baseada em riscos (*risk-based approach*) para o RIPD, à semelhança da matriz europeia (KLOZA *et al.*, 2020, p. 5). Entretanto, ao se analisar a edição tardia de uma lei geral de proteção de dados no Brasil, pode-se inverter o vetor e enxergar essa demora como uma oportunidade: uma vez que a estrutura metodológica dos RIPD ainda está sendo desenhada no País, é possível pensar sua elaboração por meio de outras metodologias, aproveitando-se de distintos casos de estudo que têm surgido no cenário internacional (e.g., abordagem que mapeia riscos e benefícios – *benefit-risk assessment*).

3.8 Aumentando a conscientização

Conforme mencionado na Introdução (Seção 1), em pesquisa realizada no Reino Unido em 2019 pelo Instituto Ada Lovelace (2019, p. 4-5), ainda que a maioria dos entrevistados informasse estar ciente do uso da FRT no País (90%), apenas 53% afirmaram saber algo sobre ela. Por sua vez, levantamento exploratório (sem relevância estatística)[103] realizado no Brasil pelo *Coding Rights*[104] em 2021, mostrou que 85,7% da pessoas que

[102] De acordo com as competências estabelecidas pelo art. 55-J, XIII, da LGPD, cabe à ANPD "editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais" (BRASIL, 2019b).

[103] As pesquisadoras indicam que o levantamento teve por objetivo apenas uma prospecção inicial ("levantar impressões", portanto, sem relevância estatística) a respeito do emprego da FRT com políticas de gênero dedicadas às pessoas travestis, transexuais e não binárias, neste sentido, criaram um questionário *online* compartilhado em grupos de pessoas trans (um segmento bem específico). Ao todo obtiveram 22 respostas, das quais 45,5% foram de mulheres transexuais; 18,2% de travestis; 18,2% de pessoas não binárias e 13,6% de homens transexuais (SILVA e VARON, 2021).

[104] *Think tank* (laboratório de ideias) focado "em mostrar as assimetrias de poder por trás do uso e implementação de determinadas tecnologias", por meio de "análises feministas e de direitos humanos sobre o uso de tecnologias,

compuseram a amostra informou já ter ouvido falar de FRT, mesmo sem saber exatamente como funciona (SILVA e VARON, 2021, p. 28, 65). Ressalvada a não pretensão estatística do levantamento feito no Brasil, esses *feedbacks* a respeito do conhecimento sobre FRT podem sugerir que a falta de um entendimento um pouco mais qualificado a respeito do assunto poderia estar limitando a capacidade do público para se envolver em um debate informado sobre os benefícios e riscos dessa tecnologia.

O **aumento da consciência entre os usuários**, a **sensibilização dos titulares** dos dados e a **compreensão pelo público em geral** a respeito da FRT e do seu impacto nos direitos fundamentais devem ser ativamente apoiadas através de ações acessíveis e educativas (COUNCIL OF EUROPE, 2021c, p. 8).

A ideia é dar acesso a conceitos simples, capazes de informar os titulares dos dados antes que eles decidam/consintam com o uso da FRT, acerca do que significa usar dados sensíveis, o que são dados biométricos, como a FRT funciona e alertá-los sobre os riscos potenciais, sobretudo em caso de utilização indevida (COUNCIL OF EUROPE, 2021c, p. 8).

Deve-se facilitar o engajamento público no desenvolvimento e uso da FRT e no fornecimento de salvaguardas adequadas para proteger os direitos fundamentais em jogo durante seu uso (COUNCIL OF EUROPE, 2021c, p. 8).

Igualmente, as empresas que desenvolvem e vendem FRT (que se beneficiam de sua utilização) devem tomar medidas razoáveis – como fazer recomendações e fornecer conselhos – para ajudar as entidades que as utilizam a implementar **transparência e respeito pela privacidade e proteção de dados** (e.g., fornecer um modelo para as políticas de privacidade; de sinalização de fácil compreensão que indique que uma FRT está em utilização em um local específico) (COUNCIL OF EUROPE, 2021c, p. 10). Tais iniciativas são incentivadas pela LGPD, no art. 50[105] e ss.

3.9 Questões acerca da proibição

O uso de FRT para aplicação da lei foi proibido no Estado da Califórnia (STATE OF CALIFORNIA, 2019) e o Estado de Illinois tem a única lei nos EUA, o *Biometric Information Privacy Act* (BIPA) que permite que indivíduos entrem com uma ação pelo uso de dados biométricos para fins comerciais sem seu consentimento[106] (ILLINOIS GENERAL

[…] pautadas pela troca em redes de coletivas e defensoras de direitos humanos, particularmente coletivas de ciberfeministas e de mulheres e população LGBTQI+" (SILVA e VARON, 2021, p. 3).

[105] Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão **formular regras de boas práticas e de governança** que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os **padrões técnicos**, as **obrigações específicas** para os diversos envolvidos no tratamento, as **ações educativas**, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2019b, grifo meu).

[106] Ao promulgar o BIPA, criou-se um esquema corretivo para permitir que os titulares de dados processem e exijam tutela pecuniária sem prova de que ocorreram danos reais, bastando mostrar que houve tratamento de dados biométricos sem consentimento. Até então era necessário restar demonstrado que houve dano resultante do tratamento de dados pessoais (e que a empresa era responsável por esse dano, *liability*) para que se cogitasse

ASSEMBLY, 2008). Em 2016, a *L.A. Tan* (uma rede de salões de bronzeamento dos EUA) fez um acordo no valor de US$ 1,5 milhão num caso em que foi acusada de não seguir as diretrizes do BIPA. **Em fevereiro de 2021**, no caso paradigmático *Patel v. Facebook*, o *Facebook* foi condenado a pagar US$ 650 milhões por capturar e armazenar imagens de rosto de 6,5 milhões de residentes de Illinois sem obter consentimento (CST EDITORIAL BOARD, 2021; EPIC, 2021).

Enquanto os protestos do *Black Lives Matter* de 2020 se espalhavam pelos EUA, vários fornecedores de tecnologia – Amazon, IBM, Microsoft – anunciaram uma moratória quanto à venda de FRT para forças policiais em todo o mundo e apelaram para regulamentação dessa poderosa tecnologia (AMAZON, 2020; IBM, 2020; JOWITT, 2020). Entretanto, apesar da importância desse posicionamento, cumpre mencionar que outros fornecedores de FRT disseram pretender manter suas relações com as forças policiais, e.g., *Clearview AI* dos EUA, *NEC* e *Ayonix* do Japão, *Cognitec* da Alemanha e *iOmniscient* da Austrália. Para essas empresas, o reconhecimento facial é uma parte fundamental ou crescente de seus negócios (HOROWITZ, 2020). De acordo com um relatório do *Gartner*[107] de 2019, há mais de 80 fornecedores de FRT em todo o mundo (INGELBRECHT, 2019).

O irônico é que muitas vezes a ameaça parece ser a vigilância governamental, mas em sociedades democráticas há mecanismos para combater a invasão do governo, e.g., muitas informações podem ser obtidas do setor público usando a Lei nº 12.527/2011 (Lei de Acesso à Informação, LAI), ainda que algumas respostas possam ser refratárias e/ou difíceis de obter. Entretanto, não há LAI para empresas de tecnologia ou reconhecimento facial; sem salvaguardas e normas efetivas, não há como controlar essas empresas (COHEN, 2013, p. 1931; FREY, 2016).

A sociedade civil organizada tem se manifestado pela proibição do uso de FRT em determinadas situações, em especial relacionadas à identificação. Como exemplo, tem-se o movimento europeu *ReclaimYourFace* **lançado em novembro de 2020** e coordenado pela *European Digital Rights* (EDRi)[108], que pede a proibição do uso de biometria facial para vigilância em massa em espaços públicos devido ao seu impacto sobre direitos e liberdades (RECLAIM YOUR FACE, 2021). A iniciativa lançou uma *European Citizens' Initiative*[109], **em fevereiro de 2021**, por meio da qual apela à Comissão Europeia para regulamentar de maneira estrita o uso de tecnologias de vigilância biométrica. Outro exemplo é o movimento *Ban*

demandar alguma reparação, e isso muitas vezes era difícil para o titular do dado pois a ocorrência e dimensão do dano poderia muitas vezes ser desconhecida.

[107] Empresa global de pesquisa e consultoria especializada em fornecer informações, conselhos e ferramentas para líderes em tecnologia da informação, finanças, recursos humanos, atendimento e suporte ao cliente, comunicações, direito e conformidade, marketing, vendas e funções da cadeia de suprimentos (GARTNER INC, 2021).

[108] Coletivo europeu de organizações não governamentais (ONGs), especialistas, defensores e acadêmicos de direitos humanos e civis no ambiente digital. Dados de 2021 dão conta que 44 ONGs são membros da EDRi e dezenas de observadores contribuem de perto para o seu trabalho (EDRi, 2021).

[109] A semelhança da "Proposta de Lei por iniciativa popular no Brasil", é um mecanismo da UE que visa a fomentar a democracia direta ao permitir que os cidadãos da UE proponham diretamente à Comissão Europeia um ato jurídico (uma diretiva ou regulamento) numa área onde os Estados-Membros hajam conferido poderes em nível da UE. Para tanto, é necessária a manifestação de pelo menos um milhão de cidadãos da União Europeia, que sejam nacionais de pelo menos um quarto dos Estados-Membros.

Biometric Surveillance (ACCESS NOW, 2021b) que, **em junho de 2021**, lançou uma "carta aberta para banimento global de usos de reconhecimento facial e outros reconhecimentos biométricos remotos que permitam vigilância em massa, discriminatória e enviesada"[110] (ACCESS NOW *et al.*, 2021), que já contava, **em agosto de 2021**, com a assinatura de mais de 200 organizações da sociedade civil, ativistas, tecnólogos e outros especialistas em todo o mundo (ACCESS NOW, 2021b). Nos termos da Carta Aberta (ACCESS NOW *et al.*, 2021, p. 1, grifos do original):

> **We call for a ban because**, even though a moratorium could put a temporary stop to the development and use of these technologies, and buy time to gather evidence and organize democratic discussion, it is already clear that these investigations and discussions will only further demonstrate that **the use of these technologies in publicly accessible spaces is incompatible with our human rights and civil liberties and must be banned outright and for good**.
> […]
> **Our call for a ban specifically focuses on, but is not limited to, the use of these technologies to identify or distinguish a person from a larger set of individuals**, also known as facial or biometric "identification" (i.e. one-to-many matching). We are concerned about the use of these technologies to identify, single out, or track individuals using their face, gait, voice, personal appearance, or any other biometric identifier in a manner that enables mass surveillance or discriminatory targeted surveillance, i.e., surveillance that disproportionately impacts the human rights and civil liberties of religious, ethnic, and racial minorities, political dissidents, and other marginalized groups. We also acknowledge that, in certain cases, facial and other biometric "authentication" systems (i.e. one-to-one matching) can be built and used in a manner that equally enables problematic forms of surveillance, such as by creating large, centralized biometric databases which can be reused for other purposes.[111]

A *Convention 108+* foi a primeira instituição pan-europeia a propor, **em janeiro de 2021**, diretrizes aplicáveis ao desenvolvimento, implantação e uso de FRT. Embora as

[110] A carta aberta foi elaborada pela *Access Now*, *Amnesty International*, *European Digital Rights* (EDRi), *Human Rights Watch*, *Internet Freedom Foundation* (IFF) e pelo Instituto Brasileiro de Defesa do Consumidor (Idec) (ACCESS NOW *et al.*, 2021, p. 7)

[111] "**Pedimos pelo banimento porque**, embora uma moratória pudesse interromper temporariamente o desenvolvimento e uso dessas tecnologias, e ganhar tempo para reunir evidências e organizar a discussão democrática, já está claro que essas investigações e discussões só irão demonstrar ainda mais que **o uso dessas tecnologias em espaços acessíveis ao público é incompatível com nossos direitos humanos e liberdades civis e deve ser banido de vez** [...] **Nosso pedido de banimento se concentra especificamente, mas não está limitado, ao uso dessas tecnologias para identificar ou distinguir uma pessoa de um conjunto maior de indivíduos**, também conhecido como "identificação" facial ou biométrica (ou seja, correspondência um-para-muitos). Estamos preocupados com o uso dessas tecnologias para identificar, destacar individualmente ou rastrear indivíduos usando seu rosto, maneira de andar, voz, aparência ou qualquer outro identificador biométrico que permita a vigilância em massa ou vigilância direcionada discriminatória, ou seja, vigilância que impacta desproporcionalmente os direitos humanos de minorias religiosas, étnicas e raciais, dissidentes políticos e outros grupos marginalizados. Também reconhecemos que, em certos casos, sistemas faciais e outros sistemas de "autenticação" biométrica (ou seja, correspondência um-para-um) podem ser construídos e usados de uma maneira que igualmente permite formas problemáticas de vigilância, por exemplo, criando grandes bases de dados biométricos que podem ser reutilizados para outros fins" (livre tradução, grifo do original).

Diretrizes não sejam vinculativas, elas exortam os Estados-Membros do Conselho da Europa a adotarem regulamentos estritos (JASSERAND *et al.*, 2021, p. 4).

Quanto à proibição de certos usos da FRT, a *Convention 108+* recomenda (COUNCIL OF EUROPE, 2021c; JASSERAND *et al.*, 2021, p. 2):

1. Limitar o uso de FRT para fins de identificação à aplicação da lei;
2. Proibir a confiança no consentimento como base jurídica para o processamento para fins de reconhecimento facial quando o responsável pelo tratamento dos dados for uma autoridade pública ou uma entidade privada autorizada a realizar tarefas semelhantes às de autoridades públicas;
3. Proibir extrair modelos biométricos de imagens digitais disponíveis, bem como integrá-los em sistemas biométricos se eles foram inicialmente processados para outros fins;
4. Proibir o uso de FRT com o único propósito de determinar a cor da pele de uma pessoa, suas crenças religiosas ou outras, sexo, origem racial ou étnica, idade, saúde ou condição social, a menos que salvaguardas adequadas sejam fornecidas;
5. Proibir o reconhecimento de emoções em contextos de recrutamento de pessoal, acesso a seguro e educação; e
6. Proibir o uso de FRT pelo setor privado em um espaço público, como em um shopping center, especialmente para identificar pessoas de interesse, para fins de marketing ou para fins de segurança privada.

Para além do respeito pelas obrigações legais, é também fundamental dar um enquadramento ético à utilização da FRT, nomeadamente com relação aos riscos inerentes à utilização dessa tecnologia em determinados setores (e.g., consulta a comitês de ética independentes, antes e durante implantações mais longas; realização de auditorias; publicação de resultados de pesquisas para complementar ou endossar a responsabilidade de uma entidade). Considerações expressamente éticas podem ajudar a encontrar um equilíbrio adequado entre interesses concorrentes de uma forma um pouco mais justa (COUNCIL OF EUROPE, 2021c, p. 15).

Em abril de 2021, a Comissão Europeia propôs um regulamento geral sobre IA, que também impactará o uso de FRT. Classificando os aplicativos de IA em quatro categorias (aplicativos proibidos; de alto risco; de risco limitado; e de risco mínimo), a proposta proíbe o uso de LFR em espaços públicos pelas autoridades policiais (embora com uma ampla gama de exceções) (JASSERAND *et al.*, 2021, p. 4).

Neste aspecto é importante fazer um *link* entre a discussão aqui empreendida acerca da FRT e a crescente utilização de IA em diferentes aplicações e contextos.

Em junho de 2021, o EDBP e a EDPS adotaram um **Parecer Conjunto (*Joint Opinion* 5/2021) sobre a Proposta de Regulamento da Comissão Europeia que estabelece regras harmonizadas sobre inteligência artificial**. Nessa oportunidade, manifestaram-se pela **proibição do uso de IA para reconhecimento biométrico automatizado em espaços públicos, como o reconhecimento de face (FRT)**, da marcha, de impressões digitais, do DNA, de voz, do padrão de digitação e outros sinais biométricos ou comportamentais, em qualquer

contexto (sejam eles usados em um cenário comercial ou administrativo, ou para fins de aplicação da lei) (EDPB e EDPS, 2021, 2, 11; EDPS, 2021a, p. 1).

Nesse quadro, um exemplo de IA não confiável financiado pela própria Comissão Europeia (no âmbito da iniciativa *Horizon 2020*[112]) é o projeto SEWA (*Automatic Sentiment Estimation in the Wild*). Esse projeto, que funcionou de 2015 a 2018, recebeu cerca de 3,6 milhões de euros para desenvolver tecnologia para análise automática de padrões de comportamento humanos (facial, vocal e verbal), incluindo análise de sentimento, gosto e empatia, com o objetivo final de comercializar produtos de forma mais eficaz para os consumidores, usando um mecanismo de recomendação de anúncios (ICL *et al.*, 2018; EUROPEAN COMISSION, 2019).

Nesse diapasão, um grupo multipartidário de 40 membros do Parlamento Europeu enviou uma carta à **Comissão de Inteligência Artificial e Vigilância Biométrica** para reforçar o pedido de que uma nova proposta legislativa sobre IA **inclua a proibição total do uso de reconhecimento facial e outras formas de vigilância biométrica em locais públicos** (EUROPEAN PARLIAMENT, 2021, p. 1, grifos do original):

> […] Surveillance, distrust and fear risk gradually transforming our society into one of uncritical consumers who believe they have "nothing to hide" and - in a vain attempt to achieve total security - are prepared to give up their liberties. That is not a society worth living in! For these reasons the processing of personal data for indiscriminate surveillance, profiling which threatens personal integrity, the targeted exploitation of vulnerabilities, addictive designs and dark patterns, and methods of influencing political elections that are incompatible with the principle of democracy should be banned. […]
> **Public security is precisely what mass surveillance is being justified with**, it is where it is practically relevant, and it is where the courts have consistently annulled legislation on indiscriminate bulk processing of personal data (e.g. the Data Retention Directive). […]
> Articles 42 and 43 then aim at regulating **biometric mass surveillance** in public spaces, for example to identify citizens or analyse their behaviour and sensitive characteristics (e.g. gender, sexuality, ethnicity, health) without their consent. Biometric mass surveillance technology in publicly accessible spaces is widely being criticised for wrongfully reporting large numbers of innocent citizens, systematically discriminating against under-represented groups and having a chilling effect on a free and diverse society. This is why a ban is needed. The proposed Articles 42 and 43, however, not only fail to ban biometric mass surveillance. They could even be interpreted to create a new legal basis and thus actively enable biometric mass surveillance where it is today unlawful (e.g. under Article 9 GDPR).
> **We urge you to make sure that existing protections are upheld and a clear ban on biometric mass surveillance in public spaces is proposed**. This is what a majority of citizens want.
> Likewise, the automated recognition of people's sensitive characteristics, such as gender, sexuality, race/ethnicity, health status and disability, is not acceptable and needs to be excluded. Such practices reduce the complexity of human existence into a series of clumsy, binary check-boxes, and risk perpetuating many forms of discrimination. Furthermore, such inferences

[112] Programa plurianual de financiamento da UE (na ordem de quase € 80 bilhões) que visou a apoiar e incentivar projetos de pesquisa e inovação durante o período de 2014 a 2020 (EC, 2020).

> often form the basis of both discriminatory predictive policing, and the widescale and indiscriminate monitoring and tracking of populations using their biometric characteristics. This can lead to harms including violating rights to privacy and data protection; suppressing free speech; making it harder to expose corruption; and have a chilling effect on everyone's autonomy, dignity and self-expression – which in particular can seriously harm LGBTQI+ communities, people of colour, and other discriminated-against groups. The AI proposal offers a welcome opportunity to prohibit the automated recognition of gender, sexuality, race/ethnicity, disability and any other sensitive and protected characteristics.
>
> Dear Vice-Presidents, dear Commissioners, if we want AI systems to be worthy of the public's trust, we need to ensure that unethical technologies are banned. Please use this opportunity to **defend our liberty and right to self-determination** – for the sake of our future and that of our children.[113]

Como pôde ser visto, eles também instaram os legisladores da UE a proibir o reconhecimento automatizado de características sensíveis das pessoas (como gênero, sexualidade, raça/etnia, estado de saúde e deficiência) – alertando que tais práticas potencializadas pela IA representam um risco muito grande para os direitos e podem alimentar a discriminação. Essa é uma preocupação interessante à luz do movimento que a Google tem feito, na área de tecnologia de propaganda (*adtech*), de substituir o micromarketing focado no comportamento de indivíduos, por anúncios que têm por alvo grupos de usuários (*Federated*

---

[113] "A vigilância, a desconfiança e o risco do medo gradualmente estão transformando nossa sociedade em uma massa de consumidores acríticos que acreditam que não têm "nada a esconder" e – numa tentativa vã de alcançar a segurança total – estão preparados para desistir de suas liberdades Essa não é uma sociedade na qual valha a pena viver! Por essas razões o processamento de dados pessoais para vigilância indiscriminada, criação de perfis que ameace a integridade pessoal, a exploração direcionada de vulnerabilidades, designs viciantes, padrões obscuros, e métodos para influenciar eleições políticas que são incompatíveis com o princípio da democracia devem ser banidos. [...] **A segurança pública é precisamente o que está sendo usado para justificar a vigilância em massa**, é onde ela é relevante na prática, e é onde os tribunais têm consistentemente anulado a legislação sobre o processamento indiscriminado em massa de dados pessoais (e.g., a Diretiva de Retenção de Dados). [...] Os artigos 42 e 43 visam, então, regulamentar a **vigilância biométrica em massa** em espaços públicos, para, por exemplo, identificar cidadãos ou analisar seu comportamento e caracteres sensíveis (e.g., sexo, sexualidade, etnia, saúde) sem o seu consentimento. A tecnologia de vigilância biométrica em massa em espaços públicos está sendo amplamente criticada por erroneamente reportar grande número de cidadãos inocentes, sistematicamente discriminando grupos sub-representados, bem como tendo um *chilling effect* em uma sociedade livre e diversa. É por isso que uma proibição é necessária. Os artigos 42 e 43 propostos, entretanto, não apenas falham em proibir a vigilância biométrica em massa. Eles poderiam até mesmo ser interpretados para criar uma base jurídica e, assim, permitir ativamente a vigilância em massa com biometria onde hoje ela é ilegal (e.g., sob o art. 9º do GDPR). **Pedimos que vocês se certifiquem de que as proteções existentes sejam mantidas e que seja proposta uma proibição clara da vigilância biométrica em massa em espaços públicos**. Isso é o que a maioria dos cidadãos quer. Igualmente, o reconhecimento automatizado de características sensíveis de pessoas, como gênero, sexualidade, raça/etnia, estado de saúde e deficiência não é aceitável e precisa ser excluído. Essas práticas reduzem a complexidade da existência humana em uma série de caixas de seleção binárias, corre-se o risco de perpetuar muitas formas de discriminação. Além disso, tais inferências muitas vezes formam a base tanto do policiamento preditivo discriminatório, quanto do monitoramento e rastreamento indiscriminados de populações usando suas características biométricas. Isso pode causar danos, incluindo a violação dos direitos à privacidade e à proteção de dados; suprimindo a liberdade de expressão; tornando mais difícil expor a corrupção; e ter um *chilling effect* sobre a autonomia, a dignidade e a auto-expressão de todos – o que em particular pode seriamente prejudicar comunidades LGBTQI +, pessoas de cor e outros grupos discriminados. A proposta de IA oferece uma oportunidade bem-vinda de proibir o reconhecimento automatizado de gênero, sexualidade, raça/etnia, deficiência e quaisquer outras características sensíveis e protegidas. Caros Vice-Presidentes, Caros Comissários, se quisermos que os sistemas de IA sejam dignos do confiança do público, precisamos garantir que as tecnologias antiéticas sejam banidas. Por favor usem esta oportunidade de defender nossa liberdade e direito à autodeterminação – para o bem do nosso futuro e de nossos filhos" (livre tradução, grifo do original).

Learning of Cohorts, ou FLoCs), com base em seus interesses – com esses grupos de usuários definidos conforme os algoritmos de IA da Google. Neste sentido, pode-se questionar se o FLoCs corre o risco de criar discriminação legal – baseado em como os usuários são agrupados para fins de segmentação de anúncios. É interessante ressaltar que a Google "evitou" fazer os primeiros testes na Europa, provavelmente devido ao regime de proteção de dados vigente (LOMAS, 2021).

Em 13 de setembro de 2021, o Alto Comissariado das Nações Unidas para os Direitos Humanos publicou Relatório sobre o "direito à privacidade na era digital", no qual afirmou que o reconhecimento biométrico remoto (incluída a FRT) aumenta drasticamente a capacidade dos Estados de sistematicamente identificar e rastrear indivíduos em espaços públicos, prejudicando a capacidade das pessoas viverem suas vidas sem serem observadas, resultando em um efeito negativo direto sobre o exercício dos direitos, liberdades e garantias fundamentais (UN, 2021, § 27). Nesse contexto, o Alto Comissariado recomendou: (i) banir expressamente os aplicativos de IA que não possam ser operados em conformidade com a legislação internacional de direitos humanos e impor moratória sobre a venda e o uso de sistemas de IA que representem um alto risco para o gozo dos direitos humanos (no qual enquadra a FRT, sobretudo a LFR), pelo menos até que salvaguardas adequadas para proteger os direitos humanos estejam em vigor (UN, 2021, §§ 45, 59c); (ii) impor moratória sobre o uso de tecnologias de reconhecimento biométrico remoto em espaços públicos (o que inclui FRT), pelo menos até que as autoridades responsáveis possam demonstrar conformidade com os padrões de privacidade e proteção de dados, a ausência de problemas de precisão significativos e impactos discriminatórios, bem como até que todas as recomendações definidas no Relatório A/HRC/44/24, §53 (j) (i-v), estejam implementadas[114] (UN, 2021, § 59d).

Pelas datas mencionadas na presente Seção, é possível constatar a atualidade da discussão aqui empreendida e que o debate segue em andamento. Como já mencionado, alguns empregos da tecnologia têm um risco potencial tão alto, com tão poucas vantagens associadas,

[114] "53. Neste contexto, o Alto Comissariado recomenda que os Estados: [...]
(j) Estabeleçam uma moratória sobre o uso de tecnologia de reconhecimento facial no contexto de manifestações pacíficas, pelo menos até que as autoridades responsáveis possam demonstrar conformidade com os padrões de privacidade e proteção de dados, bem como a ausência de questões de precisão significativas e impactos discriminatórios, e até que as seguintes recomendações sejam implementadas:
(i) Conduzir sistematicamente a devida diligência em direitos humanos antes de implantar dispositivos de tecnologia de reconhecimento facial e durante todo o ciclo de vida das ferramentas implantadas;
(ii) Estabelecer mecanismos de supervisão eficazes, independentes e imparciais para o uso de tecnologia de reconhecimento facial, como autoridades independentes de proteção de dados, e considerar a imposição de um requisito de autorização prévia por um organismo independente para o uso de tecnologias de reconhecimento facial no contexto de manifestações;
(iii) Implementar leis rígidas de privacidade e proteção de dados que regulem a coleta, retenção, análise e outro processamento de dados pessoais, incluindo modelos faciais;
(iv) Garantir a transparência sobre o uso de gravações de imagem e tecnologia de reconhecimento facial no contexto de manifestações, inclusive por meio de consultas ao público, especialistas e sociedade civil, e o fornecimento de informações sobre a aquisição de tecnologia de reconhecimento facial, os fornecedores de tal tecnologia e a precisão das ferramentas;
(v) Ao depender de empresas privadas para adquirir ou implantar essas tecnologias de reconhecimento facial, solicitar que as empresas tenham a devida diligência quanto aos direitos humanos para identificar, prevenir, mitigar e abordar impactos adversos potenciais e reais sobre os direitos humanos e, em particular, garantir que a proteção de dados e a não discriminação sejam incluídas no projeto e na implementação dessas tecnologias;" (UN, 2020, livre tradução).

que deveriam ser interrompidos antes de se tornarem relevantes. Daí a importância da discussão pública sobre os limites coletivos, que não devem ser ultrapassados.

4. ESTUDO DE CASO DE APLICAÇÃO DE RECONHECIMENTO FACIAL

4.1 O Caso do Metrô de São Paulo

Em 2012, o reconhecimento facial começou a ser implantado dentro de ônibus das cidades brasileiras, principalmente com o objetivo de checar as imagens captadas por uma câmera instalada na catraca, comparando-as com fotos do banco de cadastros dos usuários beneficiados com algum tipo de desconto ou isenção (idosos, deficientes, estudantes), para identificar possíveis fraudes. Uma das primeiras cidades a testar a tecnologia foi Caruaru-PE já em 2012 (AGÊNCIA TRANSPORTA BRASIL, 2012), seguida por Fortaleza-CE (REDAÇÃO VTEF, 2013) e Vitória-ES (BORGES, 2014), ambas em 2013. Em 2014, foi a vez de Florianópolis-SC (G1 SC, 2014), e Limeira-SP (G1 PIRACICABA, 2014). Em 2015, as cidades de Ribeirão Preto-SP (GOMES e OLIVEIRA, 2018), Manaus-AM (G1 AM, 2015a; 2015b), São Paulo-SP (MONTEIRO, 2014; SP TRANS, 2015), Rio de Janeiro-RJ (VENTURA, 2015), Santa Maria-RS (BITTENCOURT, 2016), Campinas-SP (MIRANDA, 2015). Desde então, esta lista só tem crescido e se diversificado por outros modais.

A Companhia do Metropolitano de São Paulo (METRÔ) foi constituída em 1968. A Linha 4-Amarela, em 2006, foi a primeira linha do metrô paulista concedida ao setor privado para operação em contrato de Parceria Público Privada (PPP) do País. Seu primeiro trecho (Faria Lima-Paulista) foi inaugurado em maio de 2010. Ela incorporou diversas novidades no contexto da rede metroviária paulista, sendo uma das mais expressivas, a operação dos trens sem condutor humano (*Unattended Train Operation*, UTO), tornando-se a primeira linha metroviária totalmente automatizada da América Latina (CAIAFA, 2016, p. 3).

Esta experiência fez-se acompanhar da incorporação de outros automatismos, e.g., automatização da venda de bilhetes, dos bloqueios que controlam o ingresso no sistema, a introdução de esteiras, o emprego de intercomunicadores, e mesmo um projeto de sonorização que permite ao Centro de Controle Operacional (CCO) ouvir o som ambiente durante as viagens. Ao mesmo tempo, a operação se torna mais "refinada e vigilante", e.g., tem-se a multiplicação de câmeras e de sofisticados dispositivos de observação e intervenção. Em nome da gestão de riscos num contexto tecnológico fomenta-se a justificativa da necessidade da vigilância. Na Linha4-Amarela, desde muito cedo, implantou-se câmeras no interior dos trens, quando usualmente apenas as plataformas eram alvo dessa apuração, i.e., a pessoas são vigiadas mais acuradamente em prol da proteção de equipamentos e da reatividade requerida do conjunto de operadores (CAIAFA, 2016, p. 3-5).

Em abril de 2018, a ViaQuatro, concessionária da Linha 4-Amarela do METRÔ, anunciou a instalação do Sistema de Portas Interativas Digitais (Sistema PID), desenvolvido pela empresa americana AdMobilize, nas estações sob sua administração (MOBILIDADE SAMPA, 2018).

Em seu *website*, a AdMobilize informa prover, na análise de pessoas em tempo real por meio de câmeras, as seguintes métricas: (1) quantidade de rostos/pessoas; (2) visualizações; (3) tempo de atenção; (4) velocidade do olhar; (5) gênero; (6) faixa etária; (7) emoção; (8) direção (ADMOBILIZE, 2021a). Ademais, afirma que é a única solução do setor que entrega "métricas 100% anônimas e agregadas" e que "acredita apenas na 'detecção'" e "nunca usará

o reconhecimento", pois a "confiança do consumidor está acima de tudo", por fim, informa que as medições são processadas local e instantaneamente, sendo que nenhuma imagem, vídeo ou informação de identificação pessoal é processada, retida (localmente ou na nuvem), compartilhada ou vendida (ADMOBILIZE, 2021b).

A Linha Amarela transporta por volta de 800 mil passageiros todos os dias (VIAQUATRO, 2021b), dados da época (2018), dão conta que se tratavam de aproximadamente 700 mil viajantes (AMIGO, 2018; VIAQUATRO, 2021a). Cerca da metade deles acessa a linha por meio de uma das três estações onde haviam sido instaladas as novas portas do Sistema PID: Luz, Paulista e Pinheiros (MONTAGNER, 2018). Sendo que, na ação movida contra a ViaQuatro (da qual se falará adiante), aparece informação que o Sistema PID estaria implementado em sete estações da Linha 4-Amarela: Luz, República, Paulista, Fradique Coutinho, Faria Lima, Pinheiros e Butantã (IDEC, 2018; TJSP, 2021a).

O Sistema PID consiste em portas interativas na plataforma metropolitana que exibem anúncios. As portas foram equipadas com câmeras que, segundo a ViaQuatro, permitiriam ao Sistema PID reconhecer rostos humanos dos passageiros do metrô que olhassem os painéis publicitários, contar o número de espectadores únicos (ainda que uma pessoa passasse mais de uma vez diante da câmera, ela seria contabilizada apenas uma vez), estimar sua idade, sexo e classificar suas reações em quatro emoções (feliz, insatisfeito, surpreso ou neutro) e, com isso, adequar os anúncios exibidos ao público, "sem processar dados pessoais", i.e., segundo Harald Zwetkoff, presidente da ViaQuatro, tudo isso seria feito por "detecção facial" e não "reconhecimento facial", sem que houvesse a identificação pessoal dos passageiros, nem a gravação, armazenamento de imagens ou verificação dos dados do indivíduo (AMIGO, 2018).

Ainda segundo o presidente da ViaQuatro, o Sistema PID faria "parte de um projeto experimental", com dois anunciantes exclusivos (pelo período de um ano): a multinacional *LG Corporation*, que forneceu as telas, e a companhia farmacêutica *Hypera Pharma* (AMIGO, 2018). Apesar do caráter mercadológico da inovação, a ViaQuatro teria justificado a implantação alegando que serviria de plataforma para compartilhamento de informações e veiculação de avisos ao público. Segundo notícia do site Mobilidade Sampa (2018) à época:

> As portas interativas digitais **serão estratégicas para a comunicação da ViaQuatro e seus parceiros com os passageiros**. Cada estação receberá quatro portas interativas, na área central da plataforma, sendo a instalação em pares e de forma espelhada. **O conteúdo será focado em campanhas de orientação, mensagens de prestação de serviço e anúncios publicitários** (grifo meu).

Cumpre destacar que ao se valer do reconhecimento facial para explorá-lo com fins eminentemente comerciais, a ViaQuatro abre precedente para a captura desses dados em grande escala contando com o aval do governo do Estado (MONTAGNER, 2018).

4.1.1 Petição inicial

Em agosto de 2018, o Instituto Brasileiro de Defesa do Consumidor (Idec)[115] ajuizou ação civil pública contra a ViaQuatro "para cessar a coleta de dados de forma obrigatória dos consumidores por meio das 'Portas Interativas Digitais', nas estações da ViaQuatro, tutelando-se o direito por tratamento de dado biométrico sem consentimento do consumidor e por imposição de obrigações excessivas ao consumidor do serviço de transporte público" (IDEC, 2018, p. 2).

Segundo o Idec, a conduta da ViaQuatro, violou o CDC e a LGPD (destaque-se que, apesar de já promulgada à época, a LGPD só entraria em vigor em 2020 – e em sua integralidade, em 2021), mais especificamente (IDEC, 2018, p. 2):

1. Violou o direito básico do usuário de serviços públicos à proteção de suas informações pessoais, nos termos da Lei nº 12.527/2011[116] (Lei de Acesso à Informação, LAI) (art. 6º, IV, da Lei nº 13.460/2017[117] – Código de Defesa dos Direitos do Usuário dos Serviços Públicos);
2. Descumpriu os parâmetros definidos pelo art. 10 da Lei nº 13.709/2018[118] (Lei Geral de Proteção de Dados, LGPD);
3. Descumpriu o direito básico do consumidor de proteção contra práticas abusivas nos termos do art. 6º, IV, da Lei nº 8.978/1990[119] (Código de Defesa do Consumidor, CDC);

---

[115] Associação civil de finalidade social, sem fins econômicos e lucrativos, apartidária, fundada em julho de 1987, cuja finalidade precípua é a defesa do consumidor. Para tanto, desenvolve várias atividades, dentre elas atuar "judicial ou extrajudicialmente em defesa do consumidor, associado ou não, nas relações de consumo e qualquer outra espécie de relação correlata, coletiva ou individualmente, também perante os poderes públicos" (IDEC, 2013, p. 1; 2021).

[116] Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.
§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:
I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem. [...] (BRASIL, 2021b).

[117] Art. 6º São direitos básicos do usuário: [...] IV - proteção de suas informações pessoais, nos termos da Lei nº 12.527, de 18 de novembro de 2011; (BRASIL, 2021c).

[118] Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
I - apoio e promoção de atividades do controlador; e
II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial. (BRASIL, 2019b).

[119] Art. 6º São direitos básicos do consumidor: [...] IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços; (BRASIL, 2017).

4. Consistiu em prática abusiva, nos termos do art. 39, V do CDC[120], pois exigiria do consumidor vantagem manifestamente excessiva;
5. Desobedeceu a obrigação dos fornecedores de informar aos consumidores de forma clara sobre os preços de produtos e serviços ofertados (art. 6º, III[121] e art. 31[122], do CDC); e
6. Impôs o cumprimento de obrigações excessivamente onerosas aos consumidores que ensejariam vantagens manifestamente excessivas para os fornecedores (art. 6º, V[123]; art. 39, V[124], e art. 51, §1º, I a III[125], todos do CDC);
7. Descumpriu o direito constitucional de proteção de imagem (art. 5º, da Constituição Federal[126], CF) e violou o art. 20 da Lei nº 10.406/2002[127] (Código Civil, CC) (c/c art. 11 da mesma Lei[128]);

---

[120] Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: (Redação dada pela Lei nº 8.884, de 11.6.1994) [...] V - exigir do consumidor vantagem manifestamente excessiva; (BRASIL, 2017).

[121] Art. 6º São direitos básicos do consumidor: [...] 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; (Redação dada pela Lei nº 12.741, de 2012) (BRASIL, 2017).

[122] Art. 31. A oferta e apresentação de produtos ou serviços devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores (BRASIL, 2017).

[123] Art. 6º São direitos básicos do consumidor: [...] V - a modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas; (BRASIL, 2017).

[124] Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: (Redação dada pela Lei nº 8.884, de 11.6.1994) […] V - exigir do consumidor vantagem manifestamente excessiva; (BRASIL, 2017).

[125] Art. 51. São nulas de pleno direito, entre outras, as cláusulas contratuais relativas ao fornecimento de produtos e serviços que: […]
§ 1º Presume-se exagerada, entre outros casos, a vantagem que:
I - ofende os princípios fundamentais do sistema jurídico a que pertence;
II - restringe direitos ou obrigações fundamentais inerentes à natureza do contrato, de tal modo a ameaçar seu objeto ou equilíbrio contratual;
III - se mostra excessivamente onerosa para o consumidor, considerando-se a natureza e conteúdo do contrato, o interesse das partes e outras circunstâncias peculiares ao caso (BRASIL, 2017).

[126] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]
V - é assegurado o direito de resposta, proporcional ao agravo, além da indenização por dano material, moral ou à imagem; [...]
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; [...]
XXVIII - são assegurados, nos termos da lei:
a) a proteção às participações individuais em obras coletivas e à reprodução da imagem e voz humanas, inclusive nas atividades desportivas; (BRASIL, 2020a).

[127] Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais (BRASIL, 2002).

[128] Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária (BRASIL, 2002).

8. Infringiu o direito de crianças e adolescentes, por conta da coleta de seus dados pessoais[129].

Diante disso, pediu a condenação da ViaQuatro (IDEC, 2018, p. 52-53):

1. A não utilizar dados biométricos ou qualquer outro tipo de identificação dos consumidores e usuários do transporte público, sem consentimento do usuário;
2. Ao pagamento de indenização pela utilização indevida da imagem dos consumidores; e
3. Indenização por danos coletivos em valor não inferior a R$ 100.000.000,00 (cem milhões de reais).

A situação seria agravada pelo fato: (i) da coleta dos dados ocorrer em "local público e de trânsito imprescindível" para muitos passageiros, em especial para qualquer um que quisesse embarcar ou desembarcar nas estações onde o Sistema foi instalado; (ii) não haver qualquer sinalização de que seria realizada uma coleta de dados, o que faria com que o cidadão fosse impedido de buscar formas de reivindicar seus direitos ou alguma fiscalização (IDEC, 2018, p. 9).

Tratar-se-ia de "pesquisa de mercado automatizada", por meio da coleta de **dados sensíveis** dos usuários, sem sua autorização, que também poderia ser entendida como uma "pesquisa de opinião compulsória", com finalidade lucrativa, pois permitiria a obtenção de receita a partir da venda desses dados para terceiros, que poderiam, então, direcionar suas estratégias de publicidade a partir das reações identificadas (IDEC, 2018, p. 3, 10). Não deixaria de ser um "modo de enriquecimento" às custas dos dados pessoais daqueles que dependem do transporte público, o que reforçaria o traço de desigualdade e ilegalidade da conduta (IDEC, 2018, p. 47). Destaque-se, inclusive, que, independentemente da pessoalidade dos dados coletados, a imposição feita a todos os usuário da Linha 4-Amarela já implicaria, de plano, violação básica do direito do consumidor (art. 6º, II[130], IV, CDC) (IDEC, 2018, p. 37).

O Idec articulou a proteção de dados pessoais no caso concreto pela interpretação conjunta da CF, do CC (em especial o Capítulo II – Parte Geral, Livro I, Título I –, que trata dos direitos da personalidade), do CDC (em especial o Capítulo V, Seção VI "Dos Bancos de Dados e Cadastros de Consumidores"), da LAI (em especial do Capítulo IV, Seção V intitulada "Das Informações Pessoais"), do Marco Civil da Internet (Lei nº 12.965/2014) e da Lei do Cadastro Positivo (Lei nº 12.414/2011), demonstrando haver um robusto regime jurídico de proteção de dados pessoais respaldando um "princípio do consentimento" (IDEC, 2018, p. 16, 24).

A LGPD teria agido harmonizando todos estes normativos legais, definindo, dentre outros, o conceito de "dado pessoal", de "dado pessoal sensível", de "tratamento" (art. 5º, I, II

[129] A questão da proteção dos dados pessoais de crianças e adolescentes é de grande importância, mas trata-se de todo um tema específico, que não será o foco da abordagem do caso neste trabalho.

[130] art. 6º São direitos básicos do consumidor: […] II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações; (BRASIL, 2017).

e X, da LGDP, respectivamente, *vide* Seção 2.1) e de "consentimento" (art. 5º, XII, LGPD) (BRASIL, 2019b, grifo meu):

> Art. 5º Para os fins desta Lei, considera-se: [...]
> XII - **consentimento**: **manifestação livre, informada e inequívoca** pela qual o titular **concorda com o tratamento** de seus dados pessoais para uma **finalidade determinada**;

Em sua argumentação o Idec defende que o tratamento de dados pessoais deve cumprir com as exigências constantes do art. 7º da LGPD, do qual destacou o inciso I, e do art. 11, do qual distinguiu, também, o inciso I (ambos tratam do consentimento pelo titular para o tratamento de dados pessoais) (BRASIL, 2019b, grifo meu):

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

Não haveria exigência de que o consentimento fosse por escrito, mas ele deveria ser demonstrado (BRASIL, 2019b, grifo meu):

> 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**.
> [...]
> § 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**.

O art. 43 do CDC[131] possui regramento específico sobre bancos de dados e cadastros de consumidores, desse dispositivo, extrai-se o entendimento que "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,

[131] Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
§ 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
§ 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
§ 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
§ 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor. (Incluído pela Lei nº 13.146, de 2015) (BRASIL, 2017).

devem respeitar os limites legais", de maneira que 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" (MENDES, 2014, p. 143).

Já o Marco Civil da Internet, que "[e]stabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil", dispõe que (BRASIL, 2014, grifo meu):

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> [...]
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, **salvo mediante consentimento livre, expresso e informado** ou nas hipóteses previstas em lei;
> VIII - **informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais**, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - **consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais**, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

É o que a doutrina chama de "autodeterminação informativa" (MENDES, 2016, p. 5):

> A autorização pelo consumidor, como regra geral, é um pressuposto essencial para ao tratamento de dados pessoais nas relações de consumo [...]. Afinal, se os dados pessoais referem-se ao seu titular e o representam, afetando a sua personalidade, somente ele pode decidir a respeito do fluxo desses dados, salvo em casos excepcionais ou expressa previsão legal. [...]. Enquanto o inc. VII [do art. 7º, do Marco Civil da Internet] condiciona o fornecimento a terceiros dos dados pessoais ao consentimento livre, expresso e informado do usuário, salvo em caso de previsão legal, o inc. IX estabelece norma geral acerca do consentimento em caso de coleta, uso, armazenamento e tratamento de dados pessoais, prevendo ainda que o consentimento deve constar de cláusula destacada. [...] Para que o consentimento constitua a real manifestação de vontade do consumidor de submeter os seus dados pessoais a tratamento, ele tem que atender a determinados requisitos. Assim, entende-se que o consentimento somente é válido se for expresso, livre, específico e informado.

Sobre o exposto, a petição inicial do Idec aponta violação de direito por tratamento de dado biométrico sem consentimento (IDEC, 2018, p. 29):

> Como não há consentimento livre, específico, informado e em destaque dos titulares dos dados – nenhum dos 600 mil usuários que utilizam diariamente a Linha Quatro do metrô de São Paulo concordaram ou deram seu consentimento informado –, há uma violação do ordenamento jurídico brasileiro, colocando os consumidores e pessoas 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.

O Idec argumenta que a face é dado biométrico, e como tal, sensível (art. 5º, II, LGPD). Expõe, ainda, que mesmo que se demonstrasse a eliminação de toda e qualquer informação que permitisse a geração de dados biométricos únicos, continuaria havendo tratamento de dados pessoais pela captura de imagens nas câmeras do Sistema PID, independentemente da tratamento subsequente para inferência de emoções (IDEC, 2018).

Menciona que um precedente importante que trata da discussão sobre consentimento e coleta de dados pessoais, é a antecipação de tutela na Ação Civil Pública nº 5009507-78.2018.4.03.6100, da 9ª Vara Cível Federal de São Paulo, na qual, frente à inexistência de consentimento dos usuários do Windows 10 para coleta de dados pessoais, em decisão de antecipação de tutela, a juíza Cristiane Farias dos Santos decidiu pela "plausibilidade parcial do direito invocado, no tocante a determinar-se que a Microsoft adote procedimentos específicos, no prazo de 30 (trinta) dias, de modo a permitir que o usuário do sistema operacional Windows 10, em caso de não autorizar o uso de seus dados, tenha ferramenta operacional que permita o exercício de tal opção de forma tão simples e fácil quanto a que permite a atualização com a autorização dos dados" (TRF3, 2018, p. 12-13), tem-se um clara aplicação e robustecimento do direito de oposição (na forma *opt-out*).

Traz, em sua argumentação o "princípio da finalidade" enunciado no art. 6º da LGPD (BRASIL, 2019b, grifo meu):

> 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**;

O Idec aponta que a ViaQuatro é concessionária do serviço público de transporte e nesta posição, haveria a legítima expectativa dos usuários do serviço que fosse provido um transporte acessível, seguro e de qualidade. Coletar dados sobre quantas pessoas transitam poderia ser considerado útil na prestação do serviço (e.g., cálculo de horários, quantidade de trens, configuração dos vagões). Entretanto, as demais informações captadas pelos dispositivos de detecção facial, não guardariam vínculo com a melhoria da atividade de transporte concedida pelo poder público.

Nesse contexto, não se poderia considerar adequado para os fins de transporte público, muito menos compatível com o legítimo interesse "a coleta e processamento de informações pessoais para obtenção de vantagem econômica e criação de novos tipos de negócios para terceiros (venda de dados agregados de desempenho de propagandas e categorização de reações e emoções de acordo com certas categorias dos consumidores) demonstra um interesse da ViaQuatro em se tornar uma espécie de 'plataforma de publicidade', um mercado de dois lados onde há (i) usuários do transporte gerando informações sem consentimento e (ii) anunciantes que contratam o acesso à 'performance' de seus anúncios publicitários" (IDEC, 2018, p. 38-39), identificando-se o que aponta como claro desvio de finalidade.

Assim, a obtenção de receitas adicionais pela concessionária do serviço público não poderia dar-se com a imposição de exigência, obrigação ou restrição ao usuário não prevista em lei, consoante o disposto no art. 7º, V, da Lei Estadual 10.294/1999[132] e no art. 5º, IV, do Código de Defesa dos Direitos do Usuário dos Serviços Públicos[133], i.e., impor que, para poder locomover-se pela cidade, uma pessoa tenha de colaborar com pesquisas de mercado que em nada se relacionam à prestação do serviço metroviário violaria a adequação entre meios e fins da prestação do serviço.

Por fim, registra que as câmeras são imperceptíveis, praticamente "camufladas", além do que, não haveria qualquer aviso que a pessoa está sendo filmada para fins comerciais e não de segurança (IDEC, 2018, p. 39).

4.1.2 Decisão em tutela de urgência

O juízo decidiu, em tutela de urgência, impor à ViaQuatro obrigação de "cessar a captação de imagens, sons e quaisquer outros dados através de câmeras ou outros dispositivos envolvendo as denominadas portas digitais, promovendo o desligamento das referidas câmeras já instaladas no prazo de 48 (quarenta e oito) horas, sob pena de multa diária de R$ 50.000,00" (TJSP, 2018b, p. 6), incluindo-se a "obrigação de fazer consistente na colocação de adesivos nas câmeras" garantindo o cumprimento da medida judicial (TJSP, 2018a, p. 1). A ViaQuatro acatou a ordem, enquanto o caso prosseguia (TJSP, 2021a).

4.1.3 Contestação

Em outubro de 2018, a ViaQuatro apresentou contestação na qual alegou que (ÓPICE BLUM, 2018, p. 2-3):

1. O funcionamento do Sistema PID não seria capaz de reconhecer pessoas, mas somente detectar a existência de possíveis rostos (não seria feito "reconhecimento facial", mas sim "detecção facial");
2. Não envolveria, portanto, qualquer uso de imagem de pessoas ou de dados pessoais dos usuários da Linha 4 do METRÔ;
3. Os dados coletados seriam anonimizados, inviabilizando a identificação de indivíduos;
4. Haveria expressa aprovação por parte do Poder Concedente em relação à aferição de receitas complementares à prestação de serviço público por meio de publicidade, em especial quanto ao projeto em comento; e

[132] Artigo 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; (ASSEMBLEIA LEGISLATIVA DE SÃO PAULO, 2015).

[133] 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; (BRASIL, 2021c).

5. Não haveria qualquer ilicitude na tecnologia contratada e utilizada, tampouco nexo causal e dano, não havendo provas do alegado, de forma que não se verificaria o dever de indenizar.

Ademais, segundo a contestação da ViaQuatro, o CEO e Fundador da empresa AdMobilize teria explicado que a tecnologia usada no Sistema PID detecta "cerca de 80 (oitenta) pontos no rosto das pessoas" e os converte em números binários sem armazenar qualquer imagem ou identificar o rosto de transeuntes, i.e., a tecnologia embarcada no Sistema PID se limitaria a "contar as pessoas, visualizações, tempo de permanência, tempo de atenção, gênero, faixas etárias, emoções, fator de visão, horas de pico de visualizações e distância de detecção", as informações seriam tratadas de forma anonimizada, gerando apenas dados estatístico, sem coletar, armazenar ou tratar qualquer dado pessoal de pessoa individualizada (ÓPICE BLUM, 2018, p. 6-7, 11, 13).

Argumentou, ainda, que as disposições legais que tutelam dados pessoais não visam a vedar todo e qualquer tipo de tratamento de dados, em especial os "impessoais" (como seria o caso), o que inviabilizaria estudos analítico e estatístico representando verdadeiro retrocesso científico, cultural e tecnológico (ÓPICE BLUM, 2018, p. 20). Inclusive apontou que se fosse cabível qualquer indenização na situação em apreço, também seria o caso em pesquisas estatísticas realizadas em ambientes públicos, ocorridas independentemente do consentimento daqueles que dão origem aos dados anonimizados e estatísticos, como em estudo dos presentes em uma manifestação política; em levantamento dos frequentadores de centros comerciais; na análise do público de um grande evento esportivo ou artístico etc. (ÓPICE BLUM, 2018, p. 39).

Aduziu que os normativos trazidos na petição inicial não seriam aplicáveis à situação, primeiro, por não ser o caso de tratamento de dados pessoais. Segundo, porque a LGPD ainda não estaria em vigor (*vacatio legis*). Ademais, o Idec teria deixado de citar os outros 9 (nove) incisos do art. 7º da LGPD, que mencionam outras hipóteses autorizativas do tratamento de dados pessoais, bem como o art. 11 também da LGPD, que traz outras hipóteses legais para o tratamento de dados pessoais para além do consentimento (ÓPICE BLUM, 2018, p. 21).

Por fim, apontou que o projeto das PID, teria base legal em previsão contratual que autorizaria a aferição de receitas alternativas, complementares, acessórias ou de projetos alternativos (inclusive relativos a publicidade) e teria sido devidamente aprovado pelo próprio Poder Concedente[134] (ÓPICE BLUM, 2018, p. 38).

4.1.4 Caminhar do processo

Em maio de 2019, a Defensoria Pública do Estado de São Paulo (DPSP) foi admitida como assistente litisconsorcial e, em outubro do mesmo ano, o Instituto Alana foi admitido

[134] A ViaQuatro informou que,o em reunião realizada na data de 09/01/2018, apresentou à Administração Pública Estadual o Projeto das PID para fins de esclarecimentos e validação, ao que o Diretor-Presidente do METRÔ (*cf.* Ofício P 221, de 28/05/2021) e o Coordenador da Comissão de Monitoramento das Concessões e Permissões, da Secretaria de Estado dos Transportes Metropolitanos (*cf.* Comunicado CMCP nº 537/2018, de 30/05/2018), manifestaram-se quanto a não haver óbice à implantação do Projeto (ÓPICE BLUM, 2018, p. 36)

como *amicus curiae*, tendo em vista sua missão institucional de promoção, proteção, defesa e controle social de direitos humanos de crianças e adolescentes, além do papel de especialista nas áreas de proteção de dados de crianças e publicidade infantil (ALANA, 2019).

Interessa apontar que a DPSP sustentou que a análise da expressão facial visa a acessar o íntimo da pessoa, sendo que, no caso em apreço, inexistiria qualquer consentimento por parte do indivíduo, tampouco informação a respeito da coleta de dados, ressaltou, que "a invasividade e a perniciosidade inerentes às Portas representam uma verdadeira mercantilização sistemática dos usuários os quais sequer são informados acerca da prática" (TJSP, 2021b, p. 11). Ademais, destacou que a partir do momento em que se diz que um dado foi anonimizado quando do seu tratamento, confessa-se que, em um momento anterior, o dado não o era (MPSP, 2020, p. 6).

Incidentalmente, a ViaQuatro manifestou-se informando que nos equipamentos objeto da lide, além das câmeras, havia telas para veicular material publicitário em absoluta independência do Sistema PID, assim, peticionou para que as telas pudessem ser utilizadas. O juízo constatou que não houve qualquer limitação a esse respeito na decisão que deferiu a liminar, já que a proibição estava relacionada apenas à captação de informação dos usuários pelas câmeras (TJSP, 2021a).

4.1.5 Parecer técnico do IRIS

Parecer técnico do Instituto de Referência em Internet e Sociedade (IRIS)[135] teceu consideração a respeito do tratamento dos dados obtidos no caso em apreço sob duas perspectivas (TEOFILO *et al.*, 2019, p. 8-9):

1. **Da cadeia como um todo**: tem-se a coleta de dados pessoais brutos (imagem do rosto dos transeuntes captada pelas câmeras do Sistema PID) a partir dos quais são extraídas informações de reação às publicidades ofertadas. Estas informações são utilizadas para subsidiar a decisão quanto à apresentação (otimização) de novas publicidades no METRÔ, num processo que se retroalimenta: (i) captura de dados relativos à reação do transeunte à exposição à propaganda; (ii) que são transformados em informação útil; (iii) essa informação é repassada aos anunciantes que produzem propaganda direcionada; (iv) que por sua vez é apresentada ao transeunte que tem sua reação capturada e o processo se reinicia. Esse tratamento de dados não ocorreria de maneira "despretensiosa", uma vez que o consumidor é a origem (fonte das informações), mas também o destinatário final da cadeia de tratamento (que tem por objetivo influenciar seu próprio comportamento de consumo).

[135] Associação civil sem fins lucrativos de cunho científico e formulação de políticas nas áreas de direito e tecnologia, internet e inovação, originada de grupo de estudos na Universidade Federal de Minas Gerais. Tem por missão explorar, investigar e entender os desdobramentos da Internet sobre a sociedade contemporânea: seu desenvolvimento, suas dinâmicas, suas normas e seus padrões (IRIS, 2021).

2. **O que ocorre técnica e juridicamente entre o momento da captura da imagem até a produção das informações extraídas**. Esse enfoque seria dividido em 3 fases:
    a. **Fase 1**: Detecção e captura das imagens do rosto dos usuários do transporte público.
    b. **Fase 2**: Análise da estrutura facial, por meio da elaboração de modelo biométrico do rosto, de forma a detectar gênero, faixa etária, emoção etc.
    c. **Fase 3**: eventual processo de anonimização, que não teria sido comprovado pela ViaQuatro, com agregação dos dados estatístico para o cliente final e possível armazenamento dos dados pessoais identificáveis (modelo biométrico) pela AdMobilize.

O IRIS destaca que já **na Fase 1**, com a captura da imagem (filmagem pelas câmeras de propriedade da ViaQuatro) do rosto do indivíduo (matéria-prima para o algoritmo de IA da AdMobilize) caracteriza-se um tratamento de dado pessoal, ainda que sua duração seja de milésimos de segundo e que ocorra o descarte da imagem em fase posterior do tratamento. Quanto a isso, destaca que nenhum normativo nacional ou internacional apresenta qualquer exigência quanto ao tempo mínimo de processamento entre a captura e a anonimização (TEOFILO *et al.*, 2019, p. 10).

Além disso, ressalta que a foto de um rosto não poderia ser considerada um "dado anônimo *ab initio*, como procuraria argumentar a ViaQuatro, pois <u>é intrínseco da natureza do rosto de uma pessoa ser caracterizado como dado pessoal</u>" (TEOFILO *et al.*, 2019, p. 10, grifo do original).

Na Fase 2, a imagem é analisada pelo algoritmo de IA da AdMobilize que produz um modelo biométrico do rosto da pessoa, que será usado para inferência sobre a emoção no momento da captura da imagem, bem como a identificação do gênero, faixa etária etc. São utilizados pontos de referência do rosto para identificação de características físicas associadas a emoções, e.g., posição da boca (para a detecção de um sorriso), posição das sobrancelhas (para a indicação de surpresa, reprovação etc.). Esse modelo biométrico "configura-se claramente como um dado pessoal sensível, ao representar as **características biométricas únicas** que permitem a identificação de um indivíduo" (TEOFILO *et al.*, 2019, p. 10, grifo do original). Do que se conclui que na Fase 2 também ter-se-ia tratamento de dados pessoais (de natureza ainda mais sensível, por serem dados biométricos).

Associado a isso, é apontado o risco de cruzamento dos dados com outras informações (e.g., data e hora da coleta da imagem, ou com o banco de dados do Bilhete Único – inclusive com alerta para possível venda desses dados a terceiros[136]) o que poderia ser usado para definição de perfis (*profiling*).

[136] Em 2017, o então prefeito da cidade de São Paulo, João Dória (que em 2018 elegeu-se governador do Estado de São Paulo), em viagem a Dubai, anunciou a venda da base de dados dos usuários do Bilhete Único. Com a repercussão negativa, a inciativa foi suspensa. Já em 2018, discutia-se a privatização do Bilhete Único, projeto que também foi suspenso, mas cuja sombra paira sobre o tema. Conforme especialistas manifestaram à época, "esses dados de mobilidade urbana geram um tipo de perfilização muito atrativo para o mercado [...] indicativo de empregabilidade, [...] regularidade habitacional", o que é problemático pois "segue uma tendência em

Apenas na **Fase 3** poder-se-ia falar em dados anonimizados, e isso se restasse comprovado que a AdMobilize não armazena imagem e/ou modelo biométrico dos usuários do METRÔ de forma individualizada (comprovação esta que não teria ocorrido).

Aponta que o *Article 29 Working Party*, no parecer em que analisa a eficácia e os limites das técnicas de anonimização existentes no contexto de proteção de dados, teria estabelecido que (WP29, 2014, p. 7, grifo meu):

> First, anonymisation **is a technique applied to personal data** in order to achieve irreversible de-identification. Therefore, **the starting assumption is that the personal data must have been collected and processed in compliance with the applicable legislation on the retention of data in an identifiable format**.
> In this context, **the anonymisation process**, meaning the processing of such personal data to achieve their anonymisation, **is an instance of "further processing"**[137].

Logo, para que haja anonimização, necessária prévia coleta e processamento em concordância com a legislação vigente. Neste ponto, o IRIS faz uma analogia com a doutrina dos "frutos da árvore envenenada", considerando que se o tratamento inicial dos dados pessoais (nas Fases 1 e 2) viola o direito aplicável (no que diz respeito ao dever de informação sobre o tratamento e quanto ao consentimento sobre o uso de sua imagem), ainda que posteriormente sejam utilizadas técnicas adequadas de anonimização, toda a cadeia de tratamento se torna viciada pela ilicitude inicial que violou o sistema legal (de proteção ao consumidor, dos usuários de transportes públicos e, em especial, os direitos de privacidade, de imagem e de proteção de dados pessoais) (TEOFILO *et al.*, 2019, p. 12):

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

Por fim, enfatizam que conforme o estado atual da técnica, o aprimoramento dos algoritmos de IA para detecção facial é favorecido pelo armazenamento dos dados das análises faciais para verificar sua eficiência e para melhorar sua precisão, pois eles se beneficiam do acesso a grandes conjuntos de dados, através dos quais podem ser "treinados" a detectar padrões e, subsequentemente, aplicar esse conhecimento adquirido na análise de novos conjuntos de dados. Seria, portanto, de interesse da AdMobilize armazenar os dados pessoais considerados no caso concreto (modelo biométrico e as correspondentes emoções detectadas). Segundo o IRIS, da análise do parecer técnico do Instituto Brasileiro de Peritos (IBP),

---

transformar privacidade e proteção de dados em bens de luxo", uma vez que "as pessoas de menor capacidade de renda que usam o transporte público vão ter padrões de deslocamento mapeados" (VICENTE, 2019).

[137] "Em primeiro lugar, a anonimização **é uma técnica aplicada a dados pessoais** para obter uma desidentificação irreversível. Portanto, **parte-se do pressuposto de que os dados pessoais devem ter sido coletados e processados em conformidade com a legislação aplicável sobre a retenção de dados em um formato identificável**. Neste contexto, **o processo de anonimização**, ou seja, o processamento de tais dados pessoais para atingir o seu anonimato, **é uma instância de um 'processamento posterior'**" (livre tradução, grifo meu).

apresentado pela ViaQuatro, não teria restado comprovado que estes dados não são armazenados pela AdMobilize (TEOFILO *et al.*, 2019, p. 12-13).

Prossegue mencionando que a Diretiva 95/46/CE[138], que originalmente teria conceituado anonimização, dispôs ser "técnica de processamento de dados por meio da qual se desvincula uma pessoa natural da titularidade de um dado qualquer". Uma vez que os dados tenham sido anonimizados, não seria mais imperativa a aplicação das normas de proteção de dados pessoais. O IRIS explica que a anonimização não se trata de um processo absoluto, mas que admite gradações, conforme o estado de desenvolvimento da tecnologia e o contexto em que os dados pessoais são tratados, daí a importância do dever de transparência quanto à técnica utilizada por parte do responsável pelo tratamento. Como as Fase 1 e 2 caracterizar-se-iam, necessariamente, como tratamento de dados pessoais, a anonimização dos dados na Fase 3 seria condição necessária para que os dados resultantes não fossem qualificáveis como dados pessoais e não se sujeitassem ao regime jurídico previsto na LGPD (IRIS, 2021, p. 13-16, 30).

Lembra que pelo **princípio da precaução** (proveniente do microssistema de proteção ao consumidor), a empresa que presta o serviço tem a incumbência de conhecer o processamento envolvido e ser capaz de fornecer explanação completa em relação à tecnologia (inclusive em Juízo).

Nesse diapasão, ressalta que nos documentos apresentados pela ViaQuatro não foram informadas quais as eventuais técnicas de anonimização supostamente utilizadas, constituindo verdadeira "caixa preta", o que não permitiria garantir que os usuários do METRÔ expostos à tecnologia não seriam identificados ou identificáveis. Tampouco teria sido apresentado algum dispositivo contratual que: (i) contivesse cláusulas exigindo o emprego adequado de técnicas de anonimização; (ii) que a AdMobilize não tratasse os dados pessoais dos usuários do METRÔ; (iii) que a empresa se comprometesse a não reidentificá-los, caso viesse a tratar os dados que supostamente foram anonimizados na Fase 3; (iv) que exigisse de outras empresas que utilizarão os dados que os mantenham em formato não identificável. Tais medidas não anulariam uma eventual irregularidade que fosse comprovada no decorrer do processo judicial, mas serviriam para demonstrar algum grau de boa-fé (TEOFILO *et al.*, 2019, p. 15-16).

Lembra que a LGPD traz conceitos de anonimização (BRASIL, 2019b):

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

[138] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, "relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", foi revogada em 2018 pelo GDPR.

Ressalta que a identificação de uma pessoa natural pode dar-se por meio de metadados, i.e., dados que fornecem informações sobre outros dados, e.g., dados de geolocalização, registros de acesso a aplicações de internet[139], porta lógica etc.

Quanto ao parecer técnico apresentado pelo IBP, da parte da ViaQuatro, aduziu que (TEOFILO *et al.*, 2019, p. 18-19, 30-31):

> [...] a dashbord e contêiner forense, apesar de serem indicativos, não demonstram tecnicamente a quais dados a AdMobilize tem acesso e armazena no momento posterior à identificação das emoções [...]
> [...] não foram explicitadas quais as medidas de segurança de informação adotadas, o que é grave, considerando-se o perigo de expor dados sensíveis (biométricos) de milhares de usuários da linha amarela do metrô.
> [...] os esclarecimentos técnicos sobre softwares, para serem conclusivos, demandam um processo para descobrir os princípios tecnológicos e o funcionamento de um dispositivo, objeto ou sistema, através da análise de sua estrutura, função e operação. Esses elementos não são encontrados no parecer apresentado pela ViaQuatro, o qual, de forma ampla, apenas analisou o produto final do tratamento de dados que é fornecido à ViaQuatro, sem maiores ponderações quanto ao papel da AdMobilize.
> [...] não ficam evidenciadas quais informações são transmitidas ao software AdMobilize, por quais locais e servidores essas informações transitam e se são armazenadas ou não de maneira individualizada em alguma das etapas, para se verificar se a AdMobilize armazena dados pessoais, e se houve anonimização adequada dos dados encaminhados à ViaQuatro.
> [...] os documentos juntados pela ViaQuatro não são suficientes para excluir a possibilidade de dano causado caso existam dados pessoais armazenados de forma insuficientemente anonimizada ou não anonimizada, que é ainda mais grave.

Quanto aos efeitos derivados da assimetria de informação entre a empresa concessionária e os consumidores, lembra que (TEOFILO *et al.*, 2019, p. 24-28):

1. O METRÔ é um serviço público com usuários que esperam deste serviço a capacidade de locomoção entre um ponto e outro da estrutura urbana, sendo que pesquisas demográficas com fins mercadológicos não fariam parte de sua atividade-fim.
2. A coleta de dados com a participação compulsória dos usuários da rede metroviária não poderia ser considerada essencial à adequada prestação dos serviços, nem guardaria vínculo com a melhoria da atividade de transporte, na verdade, violaria a adequação entre meios e fins da prestação do serviço.
3. Devido a seu valor econômico, a atividade de detecção facial promovida pela ViaQuatro integraria prática comercial.
4. Uma pessoa, ao utilizar o serviço de transporte público, contribuiria obrigatoriamente com uma atividade de pesquisa mercadológica sem a possibilidade de não o fazer (não poderia manifestar consentimento, nem teria

[139] Art. 5º Para os efeitos desta Lei, considera-se: [...] VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP (BRASIL, 2014).

possibilidade de *opt out*, i.e., recusar-se a participar), o que feriria a liberdade de escolha dos cidadãos.

5. Além de obrigar seus usuários a integrar pesquisa demográfica compulsória, a ViaQuatro o faz com exclusividade, sendo a única empresa que teria esse poder naqueles espaços, o que tornaria essa coleta de informações vantajosa economicamente à concessionária.
6. Na condição de fornecedora de serviços na modalidade de adesão, em que os usuários do METRÔ não teriam o poder de negociar os termos da contratação do serviço de transporte, haveria o dever de informar ostensivamente de maneira compreensível ao usuário todos os termos de uso do serviço (art. 4º, *caput*[140], 6º, III, 46[141] e 54[142], todos do CDC). O fato de os usuários da linha de METRÔ sob concessão da ViaQuatro não saberem que, ao adquirirem um bilhete e usarem o trecho, também estariam participando de pesquisa com fins comerciais, infringiria o dever de informar.
7. Ocultar que uma pessoa participa de determinada situação, que em especial gerará lucro a terceiro, seria ferir a autodeterminação dela enquanto sujeito.
8. A situação em apreço não se equipararia à oferta de espaço para anúncios publicitários, pois o que se estaria oferecendo como contrapartida lucrativa não seria de propriedade da concessionária, mas de seus usuários.
9. O usuário de METRÔ ao ser obrigado a gerar lucro para a concessionária com a captação de seus dados, não apenas pagaria em dinheiro para usar o serviço de transporte, mas pagaria à concessionária com seus dados, de maneira oculta e sem qualquer possibilidade de escolha, i.e., ter-se-ia caracterizado não só o preço oculto do serviço fornecido, mas vantagem manifestamente excessiva.

Conclui afirmando não restar dúvida que houve dano diante de toda exposição acerca da violação aos direitos coletivos relacionados ao consentimento, à informação e à autodeterminação dos usuários do METRÔ. Destaca, entretanto, que o dano pode ser ainda

---

[140] Art. 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: (Redação dada pela Lei nº 9.008, de 21.3.1995) (BRASIL, 2017).

[141] Art. 46. Os contratos que regulam as relações de consumo não obrigarão os consumidores, se não lhes for dada a oportunidade de tomar conhecimento prévio de seu conteúdo, ou se os respectivos instrumentos forem redigidos de modo a dificultar a compreensão de seu sentido e alcance (BRASIL, 2017).

[142] Art. 54. Contrato de adesão é aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo.
§ 1° A inserção de cláusula no formulário não desfigura a natureza de adesão do contrato.
§ 2° Nos contratos de adesão admite-se cláusula resolutória, desde que a alternativa, cabendo a escolha ao consumidor, ressalvando-se o disposto no § 2° do artigo anterior.
§ 3º Os contratos de adesão escritos serão redigidos em termos claros e com caracteres ostensivos e legíveis, cujo tamanho da fonte não será inferior ao corpo doze, de modo a facilitar sua compreensão pelo consumidor. (Redação dada pela nº 11.785, de 2008)
§ 4° As cláusulas que implicarem limitação de direito do consumidor deverão ser redigidas com destaque, permitindo sua imediata e fácil compreensão.
§ 5° (Vetado) (BRASIL, 2017).

maior, pois os documentos juntados pela ViaQuatro não são suficientes para excluir a grave possibilidade de que existam dados pessoais (que, por serem biométricos, seriam sensíveis) armazenados de forma insuficientemente anonimizada ou mesmo não-anonimizada (TEOFILO *et al.*, 2019, p. 31).

4.1.6 Parecer Técnico da Access Now

A Access Now[143] apresentou parecer complementar ao do IRIS, focando, em particular (ARROYO e LEUFER, 2020a, p. 2):

1. Nas atividades de tratamento de dados pessoais envolvidas no Sistema PID, incluindo as afirmações feitas sobre anonimização de dados;
2. No *status* científico da chamada tecnologia de detecção de emoções; e
3. No potencial de discriminação devido à classificação do gênero como binário masculino-feminino no funcionamento do Sistema PID.

Aquela Organização entende que (ARROYO e LEUFER, 2020a, p. 2, 19):

1. Não foram fornecidas informações claras e adequadas aos consumidores quanto ao funcionamento do Sistema PID;
2. O direito dos passageiros de optar ou não pela coleta de seus dados pessoais sensíveis não foi respeitado pelo Sistema – o que teria sido restringido/agravado pelo fato do transporte público ser essencial na vida cotidiana de muitos passageiros que não teriam um alternativa viável (ARROYO e LEUFER, 2020b); e
3. As informações sobre a anonimização dos dados pessoais e as possibilidades de identificação dos transeuntes não foram suficientes.

E esses pontos combinados, demonstrariam claramente que o Sistema PID violaria os direitos dos usuários da linha do METRÔ.

A Access Now argumenta no sentido que o Sistema PID (ARROYO e LEUFER, 2020a, p. 3):

1. Utiliza, de fato, uma forma de reconhecimento facial, denominada categorização/classificação facial.
2. Coleta, armazena (ainda que) temporariamente e processa os dados biométricos de transeuntes, sem dar-lhes a possibilidade de recusar ou consentir que seus dados sejam processados.
3. Coleta dados que podem ser usados para identificar os indivíduos.

Por fim, ressalta duas questões relevantes, relacionadas à alegação de que as informações demográficas podem ser derivadas das *views* (i.e., uma face captada pela câmera

[143] Organização sem fins lucrativos fundada em 2009 com a missão de defender e estender os direitos civis digitais dos usuários em todo o mundo em áreas como proteção de dados/privacidade, liberdade de expressão, segurança digital, discriminação na rede, direitos humanos e dos negócios (ACCESS NOW, 2021a).

que pareça estar "de fato olhando/interagindo" para/com o anúncio) (ARROYO e LEUFER, 2020a, p. 3, 11):

1. Não há base científica clara para derivar informações sobre emoções a partir de expressões faciais e, portanto, tais inferências sobre emoção seriam inválidas.
2. A tecnologia automatizada de reconhecimento de gênero usada para prever o gênero dos transeuntes discriminaria sistematicamente indivíduos trans e não binários.

Segundo o parecer técnico da Access Now, o software da AdMobilize primeiro realiza a detecção facial e, em seguida, processa os dados biométricos (no caso, dados faciais) em um processo tecnicamente denominado "análise facial, classificação ou categorização" (ARROYO e LEUFER, 2020a, p. 3).

Apontam que há uma deturpação na utilização de uma série de termos pela AdMobilize, ViaQuatro, IBP e Raul Spiguel (estes dois últimos trazidos aos autos como peritos pela ViaQuatro). Salientam que na definição padrão, tecnologia de reconhecimento facial é normalmente usada como um termo genérico (guarda-chuva) que abrange uma variedade de processos tecnológicos, incluindo *detecção facial*, *identificação* (correspondência 1-muitos), *autenticação/verificação* (correspondência 1-1), e *classificação/categorização/análise* (fazer inferências sobre que tipo de rosto é visto) (ARROYO e LEUFER, 2020b).

O sistema da ViaQuatro não usaria "apenas detecção facial", mas dois tipos de reconhecimento facial: (i) primeiro, detecção facial para descobrir se há rostos humanos nas imagens capturadas pela câmera e; (ii) segundo, análise/categorização/classificação facial para fazer inferências sobre a idade, sexo e emoção desses rostos. E não é possível fazer esses dois tipos de reconhecimento facial usando apenas dados anonimizados, i.e., sem usar dados pessoais (ARROYO e LEUFER, 2020b).

A Access Now usa em sua argumentação o GDPR tanto por ter sido diversas vezes referenciada no âmbito do processo (inclusive nas alegações da ViaQuatro de que a tecnologia usada no Sistema PID é compatível com ele), mas também por ter servido de inspiração para a elaboração da LGPD.

Trazem a definição de "dados biométricos" enunciada pelo *Article 29 Working Party* (*vide* Seção 2.1) para demonstrar que o Sistema PID captura e processa dados biométricos relativos às características fisiológicas dos indivíduos (pois captura e processa imagens dos rostos dos transeuntes), além disso, torna as características faciais dos transeuntes "legíveis e sujeitas a uso posterior" categorizando-as de acordo com a idade, sexo e emoção, o que só reforçaria as características enunciadas de dados biométricos (ARROYO e LEUFER, 2020a, p. 4).

Em seguida, apresenta a definição do *Article 29 Working Party* (*vide* Seção 2.1) para "sistema biométrico", destacando que podem ser usados para propósitos de categorização/segregação, e neste ponto, ainda que a AdMobilize afirme que seu Sistema PID não identifica indivíduos, ao categorizar/separar claramente os indivíduos de acordo com a idade, sexo e emoção, se enquadraria de maneira inequívoca na definição de um sistema biométrico (ARROYO e LEUFER, 2020a, p. 4-5).

Ainda a partir das definições do *Article 29 Working Party* quanto às etapas do processamento de dados biométricos, ressalta que a etapa de "cadastramento biométrico" nem sempre é feita com o conhecimento ou consentimento dos indivíduos. Situação em que se enquadraria o Sistema PID, que coletaria informações biométricas dos clientes do METRÔ sem seu conhecimento e sem dar-lhes a oportunidade de recusar ou consentir com o processamento (ARROYO e LEUFER, 2020a, p. 5).

Destacam, assim como o IRIS, que a ViaQuatro e seus especialistas fornecem informações insuficientes sobre como qualquer modelo usado pelo Sistema PID é construído de modo a evitar o risco de reidentificação em uma fase posterior, especialmente se combinado com outras fontes de dados, como a data e hora em que a imagem foi capturada, ou outras informações contidas no sistema de METRÔ, incluindo o banco de dados do Bilhete Único (ARROYO e LEUFER, 2020a, p. 6).

Quanto à etapa de "correspondência biométrica", em que pese a AdMobilize afirmar que não faz identificação ela teria "esquecido" de mencionar que faz categorização, o que nada mais é do que uma das formas de reconhecimento facial, i.e., ao fazer inferências sobre a idade, sexo e emoção dos clientes do METRÔ, o Sistema PID faz categorização biométrica de transeuntes, que se qualifica como processamento de informações pessoais (ARROYO e LEUFER, 2020a, p. 6).

Ressalva que a tecnologia em questão não é validada cientificamente e não é capaz de "perceber" ou "detectar" emoções. Em vez disso, ela primeiro detecta se há um rosto na imagem. A seguir, armazena os dados biométricos sobre aquele rosto. A tecnologia então detecta movimentos faciais ou configurações faciais a partir dos dados biométricos para, em seguida, fazer uma inferência reversa com base nessa informação sobre qual seria a "emoção" que a pessoa estava sentindo. Apontou estudo de Barrett *et al*. (2019) que investigou se as emoções podem ser previstas com segurança a partir da análise facial. No estudo, foram analisados sistemas como o PID, de "[t]echnology companies [that] are investing tremendous resources to figure out how to objectively 'read' emotions in people by detecting their presumed facial expressions, such as scowling faces, frowning faces, and smiling faces, in an automated fashion"[144] (BARRETT *et al.*, 2019, p. 2). No entanto, a conclusão do estudo foi que "the science of emotion is ill-equipped to support any of these initiatives"[145] (BARRETT *et al.*, 2019, p. 48). Não haveria base científica para afirmar que sistemas como o PID podem "perceber" ou "detectar" as emoções de uma pessoa a partir de imagens de seu rosto. Em um nível básico, não existiria uma correlação direta simples entre configurações faciais (como sorrisos ou caretas) e emoções; as pessoas geralmente sorriem por outras razões que não sejam porque estão felizes, ou expressam felicidade por outras configurações faciais que não um sorriso.

[144] "empresas de tecnologia [que] estão investindo enormes recursos para descobrir como objetivamente 'ler' as emoções das pessoas, detectando suas supostas expressões faciais, como rostos entediados, carrancudos e sorridentes, de forma automatizada" (livre tradução).

[145] "a ciência da emoção está mal equipada para apoiar qualquer uma dessas iniciativas" (livre tradução).

Assim, em vez de "detectar emoções", o que a AdMobilize realmente estaria fazendo são inferências inválidas com base em crenças super-simplificadas. Os proponentes dessa visão das emoções básicas afirmam que essas configurações/movimentos faciais básicos são protótipos de expressão emocional com validade universal. Em contraste, Barrett *et al.* (2019, p. 46) teriam demonstrado que essas configurações "are best thought of as Western gestures, symbols or stereotypes that fail to capture the rich variety with which people spontaneously move their faces to express emotions in everyday life"[146]. Nesse ponto em especial, a Access Now destacou que o Brasil é um país cujo contexto e cultura podem diferir significativamente daqueles países onde essa tecnologia foi desenvolvida e, portanto, as informações usadas para inferências não seriam necessariamente precisas para categorizar as emoções dos indivíduos no Brasil. Acresça-se a isso, o fato que, não é por serem inválidas que tais inferências seriam menos invasivas dada a forma como são obtidas (ARROYO e LEUFER, 2020a, p. 12-14). Os usuários não só não puderam recusar-se a participar, mas também foram mal-informados quanto a um experimento que não teria uma base científica clara.

Em suma: as inferências feitas sobre as emoções dos usuários do METRÔ não seriam cientificamente válidas; seus dados biométricos estariam sendo coletados, armazenados e processados a fim de fazer inferências não científicas sobre sua vida emocional privada.

Ademais, apontam que a AdMobilize afirma que o Sistema PID é capaz de detectar o gênero dos transeuntes entre homem e mulher com uma precisão de 80-90%. Como a detecção se baseia na análise dos rostos dos transeuntes, supõe-se que o gênero seria determinado a partir das características fisiológicas do rosto de uma pessoa. Mas esta seria uma suposição equivocada, que não só falharia em explicar a existência de pessoas não binárias e pessoas trans, mas que perpetuaria a discriminação e prejudicaria os indivíduos que não se enquadram nessa concepção de gênero binária e fisiologicamente baseada (ARROYO e LEUFER, 2020a, p. 15). O Sistema PID da AdMobilize negaria essa diversidade e dignidade aos transeuntes que teriam o direito à auto-declaração e a não serem erroneamente classificados. Tratar-se-ia de um risco desproporcional considerado o propósito mercadológico do Sistema PID (ARROYO e LEUFER, 2020a, p. 20).

4.1.7 Manifestação do Ministério Público

Em janeiro de 2020, o Ministério Público do Estado de São Paulo (MPSP) posicionou-se favoravelmente à concessão dos pedidos formulados pelo Idec. Dentre outras colocações, manifestou-se quanto ao grave abuso relacionado à compulsoriedade da pesquisa demográfica, manifestamente ilegal e contrária aos "termos contratuais da concessão, desvirtuando o seu objeto, que deveria ser restrito a prestação de serviço de transporte público", neste sentido, o ato permaneceria ilegal, independente da anuência do Concedente, "porque o Estado não pode dispor dos direitos fundamentais dos cidadãos", ao que acresceu que a "pesquisa é inteiramente inútil para a atividade fim, uma vez que os dados não são empregados para melhorar a

[146] "são melhor concebidos como gestos, símbolos ou estereótipos ocidentais que não conseguem capturar a rica variedade com que as pessoas movem espontaneamente seus rostos para expressar emoções na vida cotidiana" (livre tradução).

qualidade do serviço público de transporte, mas para atender propósitos mercadológicos". Concordou com a afronta ao art. 5º, X, CF, o que no seu entender já seria suficiente para remoção de todas as câmeras e para o pagamento de indenização/sanção. Posicionou-se quanto à flagrante violação dos direitos das crianças e adolescentes (MPSP, 2020, p. 18-22).

4.1.8 Sentença

Em maio de 2021, a juíza Patrícia Martins Conceição, da 37ª Vara Cível do Foro Central de São Paulo proferiu sentença dando parcial procedência à ação, na qual (TJSP, 2021a; 2021b, p. 17):

1. Determinou que a ViaQuatro se abstenha de captar as imagens, sons e quaisquer outros dados pessoais dos consumidores usuários, através das câmeras ou outros dispositivos envolvendo os equipamentos instalados na Linha 4-Amarela do METRÔ, sem consentimento prévio do consumidor, confirmando a liminar anteriormente concedida.
2. Determinou à ViaQuatro que, caso deseje readotar as práticas tratadas nos autos, deverá obter o consentimento prévio dos usuários mediante informação clara e específica sobre a captação e tratamento dos dados, com adoção das ferramentas pertinentes.
3. Condenou a ViaQuatro ao pagamento de indenização por danos morais coletivos no valor de R$100.000,00 (cem mil reais), corrigida segundo a tabela do Tribunal de Justiça de São Paulo (TJSP), desde a data da publicação da sentença, e com juros de mora de 1% ao mês, incidentes a partir da citação, a ser revertido para o Fundo de Defesa de Direitos Difusos (FDD).

Na sentença, consignou que (TJSP, 2021b, p. 7-17, grifos do original):

> [...] [A] **limitação do sistema de apenas se utilizar das imagens dos usuários para fins estatísticos, sem efetiva captação, gravação ou identificação não está demonstrada nos autos**, ônus que incumbia à ré, na forma do artigo 373, II do Código de Processo Civil.
> **Diante do fato incontroverso de que havia equipamentos de gravação de imagens dos usuários para fins publicitários e estatísticos nas estações administradas pela ré, cabia a essa na qualidade de concessionária de serviço público, demonstrar cabalmente que o sistema não armazena dados pessoais dos usuários da plataforma, tampouco realiza o reconhecimento facial pelo equipamento instalado, a ausência de gravação ou filmagem dos usuários e a real destinação dada ao material obtido, se o caso, o que não ocorreu.**
> [...]
> E ainda que se constatasse concretamente a ausência de efetivo reconhecimento facial pelo equipamento instalado, **não há dúvidas de que há captação da imagem de usuários, sem o seu conhecimento ou consentimento para fins comerciais que beneficiam a ré e a empresa por ela contratada**.
> A ré confessa que há detecção da imagem dos usuários e que tal dado é utilizado para fins estatísticos [...].

Portanto, inexiste controvérsia acerca da detecção da imagem dos usuários, bem como captação e reconhecimento de informações como gênero, faixa etária, reação à publicidade veiculada no mesmo equipamento, entre outros.

[...]

Desta forma, **o reconhecimento facial ou mesmo a mera detecção facial, sem que seja possível a identificação concreta do indivíduo, mas com acesso à sua imagem e face, parece já esbarrar no conceito de dado biométrico, legalmente considerado como dado pessoal sensível, daí porque merece tratamento especial à luz da Lei nº 13.709/2018**.

Anote-se que a LGPD estabeleceu proteção especial aos dados pessoais sensíveis, autorizando o seu **tratamento somente na hipótese de consentimento claro e específico pelo titular do dado**, ou, sem o consentimento do titular, nas situações elencadas no rol do inciso II do artigo 11 da LGPD, não se vislumbrando nenhuma das hipóteses no caso em tela.

[...]

A situação exposta no caso concreto é muito diferente da captação de imagens por sistemas de segurança com objetivo de melhoria na prestação do serviço, segurança dos usuários ou manutenção da ordem, o que seria não só aceitável, mas necessário diante da obrigação da fornecedora de serviço público zelar pela segurança de seus usuários dentro de suas dependências. É **evidente que a captação da imagem ora discutida é utilizada para fins publicitários e consequente cunho comercial, já que, em linhas gerais, se busca detectar as principais características dos indivíduos que circulam em determinados locais e horários, bem como emoções e reações apresentadas à publicidade veiculada no equipamento**.

Ademais**, restou incontroverso que os usuários não foram advertidos ou comunicados previa ou posteriormente acerca da utilização ou captação de sua imagem pelos totens instalado nas plataformas, ou seja, os usuários nem mesmo têm conhecimento da prática realizada pela requerida**, o que viola patentemente o seu direito à informação clara e adequada sobre os produtos e serviços, bem como à proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, ambos elencados no artigo 6º, III e IV do Código de Defesa do Consumidor.

[...]

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**.

[...]

No caso, **a possibilidade de reconhecimento facial, a detecção facial, a utilização das imagens captadas dos usuários do metrô, com evidente finalidade comercial, assim como a ausência de prévia autorização ou mera cientificação para captação das imagens, revela conduta bastante reprovável capaz de atingir a moral e os valores coletivos, principalmente considerando o incalculável número de indivíduos que transitam pela plataforma da requerida diariamente, inclusive crianças e adolescentes, cuja imagem goza de maior e notória proteção, nos termos do artigo 17 do ECA**.

> Note-se que não houve prática de mero ato ilícito pela requerida, mas real conduta violadora de imagem dos usuários consumidores do metrô, que ultrapassa os limites da tolerabilidade.

Ainda em maio de 2021, ambas as partes apresentaram embargos de declaração que foram conhecidos e rejeitados.

Em junho de 2021, a ViaQuatro apresentou apelação. Em julho de 2021, foram apresentadas contrarrazões ao recurso de apelação. Em agosto de 2021, os autos foram remetidos ao Colégio Recursal do TJSP onde, até o momento da escrita desta Seção, setembro de 2021, aguardavam julgamento.

Se o caso, desde logo, já se mostra importante do ponto de vista da proteção de dados por seu pioneirismo, o desenrolar da ação promete ser de grande interesse, sobretudo pela entrada em vigor da LGPD, uma vez que o questionamento feito à luz do microssistema de proteção de dados ganha força diante da incompatibilidade do tratamento dos dados frente ao arcabouço jurídico de proteção de dados, agora fortalecido por uma lei geral que lhe dá maior envergadura.

4.1.9 Importância do Caso

O uso de tecnologias como a FRT, capazes de um grande grau de intrusividade a respeito da vida de seus titulares é cada vez mais significativa. Neste diapasão, não só o ordenamento brasileiro tem sido cada vez mais instado a disciplinar atividades que envolvem dados pessoais, tratamento automatizado e aplicação de algoritmos; mas o judiciário também tem sido progressivamente mais acionado para definir os limites, requisitos e bases legais de determinadas ferramentas.

As particularidades concernentes a esta Ação Civil Pública mostram-se importantes para a definição de precedentes relativos à utilização de novas tecnologias no Brasil, o que assevera, também, a importância de litígios estratégicos relativos ao ambiente digital. Isso sem falar que se trata de um assunto de fronteira entre Direito e tecnologia, portanto multidisciplinar, mas com forte componente de consolidação de direitos na atualidade.

A Ação lida com temáticas como proteção de dados pessoais no Brasil; processamento automatizado de larga escala; coleta de dados em local público; utilização de tecnologia de inteligência artificial; obrigações relativas à transparência, informação, segurança e cautela dos transeuntes.

Além do mais, como visto, o Idec articulou a proteção de dados pessoais no caso concreto pela interpretação conjunta da CF, do CC, do CDC[147], da LAI, do Marco Civil da Internet, da Lei do Cadastro Positivo, demonstrando haver todo um microssistema de proteção

[147] A esse propósito, para uma discussão dos riscos criados pela coleta e tratamento massivo de dados dos consumidores para a hiperpersonalização de produtos, serviços e conteúdos no que se tem chamado de "novo mercado de consumo simbiótico ou omnipresente" e, diante dessa prática o "diálogo das fontes" entre a LGPD e o CDC (o que inclusive encontra suporte principalmente no art. 22 da LGPD, mas também nos art. 2º, VI, art. 18, §8º, art. 45, art. 55-k, art. 64, todos da LGPD) *vide* Marques e Mucelin (2021).

de dados pessoais, ao qual a LGPD teria se integrado, harmonizando todos estes normativos legais. Essa constatação também traz à tona que, um mesmo fato pode ter consequências jurídicas distintas (punitivas e/ou reparadoras) em esferas diferentes, dado que se tem subsistemas sancionadores autônomos, sem que isso implique em *bis in idem* (i.e., na repetição de uma sanção sobre mesmo fato). Isso apenas indica que uma realidade infracional única pode ter repercussão em diferentes esferas, uma vez que a importância e consequência sobre o direito afetado merece proteção em distintas dimensões/categorias, o que encontra amparo no art. 52, §2º, da LGPD[148].

Essa foi a primeira condenação judicial do tipo em ação coletiva no Brasil (HIGÍDIO, 2021; REDAÇÃO DO MIGALHAS, 2021; SOPRANA e AMÂNCIO, 2021). Michel Roberto de Souza, advogado do Idec, destacou a importância da decisão, que mostra que "as pessoas não são obrigadas a dar sua imagem para que as empresas faturem em cima disso. Indica que fazer esse tipo de abordagem é ilegal", o advogado ressaltou que futuros contratos de concessão provavelmente trarão menção expressa quanto ao que as empresas podem ou não fazer com reconhecimento facial (SOPRANA e AMÂNCIO, 2021).

Segundo o Instituto Alana, em sua participação na ação, "o caso em tela é paradigmático em diversos segmentos relacionados ao contexto atual da tecnologia no Brasil e em âmbito internacional [...]. No campo da proteção de dados pessoais, é a oportunidade que o judiciário tem, diante do caso em tela, de assegurar a responsabilização de empresas e do Estado pela ofensa contra o direito de seus cidadãos. Ao mesmo tempo, também apresenta a chance de conformar o direito consumerista à utilização de novas tecnologias" (MPSP, 2020, p. 16).

Ao longo de 2019, em diversas outras situações de emprego de FRT, ao pedir esclarecimento aos envolvido, o Idec citou explicitamente a liminar obtida no âmbito dessa Ação Civil Pública movida em face da ViaQuatro, foi o caso:

- Da *Hering Experience*, uma loja conceito da marca de vestuário brasileira, inaugurada em 2018 no Morumbi Shopping, em São Paulo, equipada com um sistema de reconhecimento facial por meio do qual câmeras captavam as reações do consumidor às peças dispostas no local (MERCADO & CONSUMO, 2018). Após tomar ciência da notificação do Idec solicitando esclarecimentos sobre o uso da FRT sem consentimento dos consumidores (IDEC, 2019b), a Secretaria Nacional do Consumidor (Senacon) instaurou processo administrativo contra a empresa, que resultou em condenação por violação do direito à informação e aos direitos da personalidade dos cidadãos, determinando o pagamento de multa de aproximadamente R$ 58 mil destinada ao FDD (IDEC, 2019e). Esta foi a primeira condenação pela Senacon relativa a violações decorrentes da utilização de FRT (IDEC, 2019a).

[148] Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: […] § 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica. (Redação dada pela Lei nº 13.853, de 2019) (BRASIL, 2019b).

- Da loja conceito do *Carrefour* Brasil em parceria com a *Zaitt*[149], inaugurada em São Paulo, onde para entrar na loja, os clientes deveriam escolher entre ser submetidos a reconhecimento facial ou à leitura de *QR Code*; na saída, o cliente ficava entre duas portas de vidro enquanto os itens comprados eram identificados por radiofrequência (RFID), concluída a leitura, o cliente confirmava a compra para deixar a loja; o valor era debitado no cartão de crédito cadastrado pelo cliente (IDEC, 2019c; 2019f; NOVAREJO, 2019).

Cumpre mencionar que com a operacionalização e fortalecimento da ANPD, espera-se que haja, na esfera administrativa, progressiva manifestação quanto a questões paradigma e à uniformização de entendimentos na interpretação e aplicação da LGPD[150], e que cheguem ao judiciário apenas questões realmente controversas, não pacificadas administrativamente. Mas até lá, dado o descompasso entre o contínuo desenvolvimento de novas tecnologias (dentre elas a FRT) e a regulamentação (COUNCIL OF EUROPE, 2013, p. 1, § 1; MANN e SMITH, 2017, p. 121-122), é possível que se veja um movimento de aumento das demandas judiciais antes que se observe um arrefecimento[151].

Um aspecto que merece destaque na Ação é que a argumentação se encaminhou no rumo que havia de fato **tratamento de dados sensíveis** (portanto, necessidade de enquadramento em um dos incisos do *caput* do art. 11 da LGPD, como base legal para o tratamento), entretanto, também houve a sagacidade de se articular a exposição exigindo-se a incidência do art. 7º, caso se entendesse que, porventura, o tratamento tivesse envolvido tão somente dado pessoal, e não dado pessoal sensível. Depreende-se da decisão em primeira instância, que o entendimento de que houve tratamento de dado pessoal sensível foi aceito. Convém mencionar que se entende acertada tal compreensão, sobretudo: (i) pelo processamento de pontos da face; (ii) geração de modelos biométricos para se tentar inferir as "emoções" dos transeuntes; (iii) a afirmação de que uma pessoa "não seria" contabilizada mais de uma vez o que envolveria alguma forma de reter sua informação e compará-la posteriormente; (iv) a possibilidade de associação a informação de utilização do Bilhete Único etc. Tudo levando à constatação de que foram tratados dados biométricos vinculados a pessoa natural identificável, portanto, dado pessoal sensível (ainda mais por não ter restado comprovado que, de fato, houve anonimização e que aqueles dados teriam sido descartados).

---

[149] Primeiro supermercado 100% autônomo da América Latina. Na loja não há funcionários; os fornecedores são os responsáveis pela reposição dos produtos diretamente nas prateleiras ao serem avisados sobre o fluxo de vendas e quando devem entregar nova remessa de produtos na loja; o cliente realiza as compras usando um aplicativo (GS1 BRASIL, 2019).

[150] Art. 55-J. Compete à ANPD: [...]
XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019) [...]
XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei nº 13.853, de 2019) (BRASIL, 2019b).

[151] Levantamento feito pela Juit, *startup* de pesquisa de jurisprudência e jurimetria, identificou que até 18/09/2021, data em que completou um ano de vigência, a LGPD já teria embasado 1.102 sentenças judiciais de cidadãos que questionaram o uso de seus dados por empresas (até julho de 2021, eram apenas 600 decisões) (LAURINO, 2021).

Outro ponto a salientar foi a consistente argumentação quanto ao potencial discriminatório desse tipo de tecnologia (FRT), sobretudo quando empregada em espaços públicos e sobre grupos vulneráveis.

Por fim, em que pese a grande importância paradigmática da Ação, parece importante fazer uma pequena crítica quanto a um dos pontos da argumentação, que se embasou fortemente na falta de consentimento dos titulares de dados (usuários da Linha 4-Amarela do METRÔ). Como visto na Seção 3.5, quando se trata de videovigilância, em geral (e no caso específico de videovigilância com FRT), apenas em casos excepcionais o consentimento do titular dos dados servirá de base jurídica (o que não significa que não se tenha o dever de transparência e informação). De fato, há abertura para tratamento de dados em determinadas hipóteses (trazidas pelos art. 7º, II a X e art. 11, II, LGPD) sem a necessidade de fornecimento de consentimento do titular de dados e, ainda que o ônus da comprovação de que a base legal de tratamento se enquadra em uma dessas hipóteses recaia sobre o controlador, a argumentação do Idec foi débil neste sentido. Afortunadamente, a Juíza reconheceu não se verificar, no caso concreto, nenhuma das hipóteses distintas do consentimento que permitiriam tratamento. Ademais, parece ter aceitado a necessidade de comprovação da hipótese de consentimento, conforme itens 1 e 2 da Sentença citada à Seção 4.1.8.

5. CONCLUSÃO

De todas as tecnologias biométricas, a FRT é a que imita mais de perto como as pessoas identificam os outros: examinando seus rostos.

Ao mesmo tempo que o emprego de FRT vem acompanhado do discurso de benefícios, eficiência, facilidade, rapidez, comodidade e conveniência, ele carrega consigo, também, muitas dúvidas e controvérsias.

A face tem um significado que vai além da aparência – é um marcador de identidade e individualidade únicas. Mas com a disseminação da FRT, a face torna-se uma coleção de pontos que podem ser literalmente transformados em *commodities* e comercializados. Isso tem sérias repercussões em questões de privacidade, liberdade, dignidade, integridade humana e mesmo democracia e não discriminação.

Quando se fala em espaços públicos, o uso de FRT pode envolver o processamento de dados de forma indiscriminada, sobre um número desproporcional de pessoas, ainda que o foco seja a identificação de apenas alguns indivíduos (e.g., passageiros em aeroportos, estações ferroviárias e de metrô). O fato da **identificação por FRT poder ser feita à distância** também apresenta problemas de transparência e questões relacionadas à base legal para o processamento sob a legislação (principalmente a LGPD, mas também outras leis possivelmente aplicáveis ao caso concreto). O problema em relação à maneira adequada de informar as pessoas sobre esse processamento **ainda se encontra sem solução**, o mesmo pode ser dito sobre o exercício efetivo e oportuno dos direitos das pessoas. Prudente mencionar o efeito irreversível e severo sobre a **expectativa (razoável) das pessoas de serem anônimas em espaços públicos**, resultando em um efeito negativo inibidor (*chilling effect*) sobre o exercício de direitos, de liberdades fundamentais (e.g., liberdade de expressão, de reunião, de associação, de ir e vir) e, de uma maneira geral, dos princípios democráticos.

Tendo em vista o recorte de espaço público, muitas das imagens utilizadas na FRT têm origem em equipamentos de videovigilância.

No contexto de videovigilância: (i) **as imagens faciais reconhecíveis sempre constituem dados pessoais**; (ii) mesmo imagens menos claramente visíveis de um indivíduo podem constituir dados pessoais, desde que os indivíduos sejam direta ou indiretamente identificáveis; (iii) imagens de vídeo contendo objetos que podem estar vinculados a um indivíduo também podem ser consideradas como dados pessoais, dependendo das circunstâncias; (iv) mesmo que não se pretenda capturar imagens que sejam capazes de identificar as pessoas registradas pelas câmeras, se essas pessoas são identificáveis, tem-se um dado pessoal. Como consequência, deve-se seguir os preceitos constantes da LGPD (à exceção, apenas, dos casos trazido pelo art. 4º) para que seja reconhecida a licitude da atividade.

No que diz respeito à utilização de videovigilância associada a FRT, o giro paradigmático diz respeito à **identificação do indivíduo por meio do processamento biométrico**, neste sentido, podem ser estabelecidas as premissas que: (i) toda tecnologia capaz de detectar uma face humana pode ser considerada FRT; (ii) **dados referentes a faces humanas são dados pessoais**; (iii) todo reconhecimento facial envolve o tratamento de dados pessoais; (iv) **dados de faces humanas tratadas no contexto do reconhecimento facial são**

dados (biométricos) sensíveis; (v) eventual anonimização dos dados não descaracteriza o tratamento de dados pessoais. Desta forma, a FRT não só lida com dados pessoais, mas dados pessoais sensíveis que, neste sentido, gozam de proteção especial, conforme a LGPD.

Em geral, a LGPD se apoia fortemente no consentimento do titular de dados para o tratamento dos dados pessoais, ainda que não seja a única hipótese nem hierarquicamente superior às demais elencadas no art. 7º ou no art. 11. Cumpre lembra que, frente aos desafios contemporâneos, o consentimento não tem sido suficiente para tutelar a privacidade e proteger os dados dos titulares. No que diz respeito à FRT, acresça-se o fato que muitas vezes a tecnologia é utilizada sem que o titular sequer tome conhecimento do seu emprego sobre dados pessoais que são sensíveis e que, por suas características e natureza, são marcados pela capacidade de uso discriminatório. A esse cenário, adicione-se a assimetria de poderes entre titulares dos dados e entidades que empregam a FRT. Diante disso, **pode-se concluir que o consentimento, geralmente, não se constitui em base legal para a utilização de FRT,** principalmente em espaços públicos. Assim, para que haja tratamento válido, não havendo o consentimento do titular de dados, é **necessário o enquadramento em uma das sete hipóteses previstas no art. 11, II da LGPD**.

Por sua própria definição, a **FRT é um processo automatizado**. Quando a utilização de FRT se destina a permitir que seja tomada decisão que afeta significativamente o titular dos dados, este último deveria ter o direito de que sua opinião seja levada em consideração, esse direito é tratado no art. 20 da LGPD, que em leitura sistemática garante: (i) acesso aos tipos de dados pessoais e aos dados propriamente ditos usados como entrada do sistema responsável pelo processo de decisão automatizada; (ii) se o processo automatizado tiver por finalidade formar um perfil comportamental, ou se utilizar de um perfil comportamental para tomada de decisão, o direito de acesso aos dados poderá incluir os dados anonimizados utilizados para enriquecer tais perfis; (iii) o direito de receber explicações claras acerca dos critérios utilizados para tomar a decisão automatizada, observados os segredos comercial e industrial, que devem ser analisados no caso concreto, pois estes conceitos não se encontram definidos na LGPD; (iv) a possibilidade de auditoria pela ANPD para verificação de aspectos discriminatórios; (v) o direito de requerer revisão, caso a decisão automatizada tenha consequências nos interesses do titular, o que se presume, no caso de perfis comportamentais.

Quanto à elaboração de RIPD, entende-se que o uso de FRT, diante de aspectos cumulativos relativos à sua criticidade, à utilização de dados (biométricos) sensíveis, ao seu potencial invasivo, à utilização em espaços públicos, à assimetria informacional e de poder, seria capaz de gerar altos riscos aos direitos e liberdades das pessoas naturais, de maneira que deveria implicar, necessariamente, a análise de riscos e consequente elaboração de RIPD (ainda que se reconheça que a palavra final quanto a essa necessidade será da ANPD).

É sabido que a FRT envolve *tradeoffs*, mas ainda se está descobrindo o alcance que essa tecnologia tem em diferentes aspectos da vida. Embora esta análise indique que, em determinados contextos, o uso da FRT deva ser restringido, não se trata de um movimento "anti-inovação", mas de um mecanismo de pesos e contrapesos para garantir que essa tecnologia contribua para a sociedade, ao mesmo tempo que esta mesma sociedade é protegida contra riscos.

A busca pelo equilíbrio entre a promoção da inovação e a garantia que a tecnologia é "confiável" e "centrada no ser humano", pode sugerir uma série de técnicas reguladoras para a área. Nesse sentido, este trabalho buscou destacar a importância:

1. Dos princípios de proteção de dados e privacidade *by design* e *by default* no desenvolvimento e uso de FRT;
2. Dos princípios da necessidade e da proporcionalidade, garantindo que a FRT não seja usada onde o propósito pode ser razoavelmente alcançado por outros meios menos intrusivos;
3. Da transparência e da responsabilidade sobre o uso de dados pessoais, sua governança e direitos aplicáveis aos indivíduos;
4. Dos requisitos de lealdade e boa fé no processamento de dados pessoais;
5. De uma abordagem ética para o uso de dados biométricos; e
6. De estruturas legais adequadas ao propósito de regulamentar tecnologias em evolução, como a FRT.

Cumpre mencionar que alguns usos são controversos na sua origem (carregam problemas éticos na base), ou seja, independente de uma melhora na técnica (e.g., diminuição de vieses, melhora da acurácia) há situações em que a FRT não deveria ser utilizada. Determinados usos de FRT minam ativamente anos de trabalho na luta por justiça e direitos. Nesses casos, é necessário não só que legisladores tomem medidas para salvaguardar direitos, mas empresas, programadores e desenvolvedores também têm um papel a desempenhar. Ao criar sistemas de FRT e interfaces de usuário, eles podem tomar decisões importantes sobre quais recursos construir e como melhor incluir e capacitar pessoas a exercerem seus direitos. **Caso contrário, o futuro apenas reproduzirá, sedimentará e agravará injustiças**.

Este processo carece de envolvimento crítico de partes imparciais, como a sociedade civil, grupos de interesse público ou comunidades que seriam afetadas por esses projetos "inovadores". É necessário um debate público honesto, crítico e informado sobre essa tecnologia emergente que tem potencial de moldar a vida pública futura.

Por fim, como possíveis trabalhos futuros, mapeados durante a execução desta pesquisa e que representam, por si só, temas ainda pouco explorados, aponta-se a interseção do emprego da FRT com os seguintes domínios: (i) a proteção de dados de crianças e adolescentes; (ii) a anonimização dos dados; (iii) a evolução da temática relativa ao RIPD; (iv) a questão de responsabilização e ressarcimento de danos resultantes da atividade de tratamento de dados pessoais (no âmbito individual e/ou coletivo).

6. REFERÊNCIAS

ABNT, Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31000:2018**. Gestão de riscos - Diretrizes. Risk management - Guidelines. 2 ed. 28 mar. 2018. Disponível em: https://www.apostilasopcao.com.br/arquivos-opcao/erratas/10677/66973/abnt-nbr-iso-31000-2018.pdf. Acesso em: 5 ago. 2021.

ACCESS NOW. **About us**. 2021a. Disponível em: https://www.accessnow.org/about-us/. Acesso em: 4 jul. 2021.

ACCESS NOW. **Ban Biometric Surveillance**. 2021b. Disponível em: https://www.accessnow.org/ban-biometric-surveillance/. Acesso em: 28 ago. 2021.

ACCESS NOW; AMNESTY INTERNATIONAL; EDRi, European Digital Rights; WATCH, HUMAN RIGHTS; IFF, Internet Freedom Foundation; IDEC, Instituto Brasileiro de Defesa do Consumidor. **Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance** [Carta aberta para banimento global de usos de reconhecimento facial e outros reconhecimentos biométricos remotos que permitam vigilância em massa, discriminatória e enviesada]. **Access Now**, 7 jun. 2021. Disponível em: https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf. Acesso em: 9 jun.

ACLU, American Civil Liberties Union; CENTER FOR DEMOCRACY & TECHNOLOGY; ELECTRONIC FRONTIER FOUNDATION; NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE; RAICU, Irina; SUZOR, Nicolas; WEST, Sarah Myers; ROBERTS, Sarah T. **Santa Clara Principles on transparency and accountability in content moderation**. 7 mai. 2018. Disponível em: https://santaclaraprinciples.org/. Acesso em: 28 ago. 2021.

ADA, Ada Lovelace Institute. **Beyond face value: public attitudes to facial recognition technology**. London: Ada Lovelace Institute, 2019. Disponível em: https://www.adalovelaceinstitute.org/wp-content/uploads/2019/09/Public-attitudes-to-facial-recognition-technology_v.FINAL_.pdf. Acesso em: 23 jul. 2021.

ADA, Ada Lovelace Institute. **About**. 2021. Disponível em: https://www.adalovelaceinstitute.org/about/. Acesso em: 24 jul. 2021.

ADLER, Andy; SCHUCKERS, Michael E. Comparing Human and Automatic Face Recognition Performance. **IEEE Trans Syst Man Cybern B Cybern,** v. 37, n. 5, p. 1248-1255, 24 set. 2007. Disponível em: https://doi.org/10.1109/TSMCB.2007.907036. Acesso em: 10 jul. 2021.

ADMOBILIZE. **Audience Intelligence**. 2021a. Disponível em: https://www.admobilize.com/audience-intelligence/#crowd. Acesso em: 1 jul. 2021.

ADMOBILIZE. **Privacy By Design**. 2021b. Disponível em: https://www.admobilize.com/privacy-by-design/. Acesso em: 1 jul. 2021.

AFFECTIVA. **Affectiva Automotive AI for Driver Monitoring Systems**. 2021. Disponível em: https://www.affectiva.com/product/affectiva-automotive-ai-for-driver-monitoring-solutions/. Acesso em: 15 ago. 2021.

AGÊNCIA CÂMARA DE NOTÍCIAS. Rodrigo Maia recebe anteprojeto para controle de dados de investigações criminais. **Agência Câmara de Notícias**, 5 nov. 2020. Disponível em: https://www.camara.leg.br/noticias/705293-rodrigo-maia-recebe-anteprojeto-para-controle-de-dados-de-investigacoes-criminais/. Acesso em: 22 jun. 2021.

AGÊNCIA TRANSPORTA BRASIL. Caruaru (PE) terá ônibus com reconhecimento facial e controle por GPS. **Agência Transporta Brasil**, 21 set. 2012. Disponível em: https://www.transportabrasil.com.br/2012/09/caruaru-pe-tera-onibus-com-reconhecimento-facial-e-controle-por-gps/. Acesso em: 2 jul. 2021.

ALANA, Instituto. **Pedido de *Amicus Curiae* do Instituto Alana**. 30 abr. 2019. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2020/12/30.4.2019-Amicus-Curiae-Alana.pdf. Acesso em: 4 jul. 2021.

ALBA, Davey. Facial Recognition Moves Into a New Front: Schools. **The New York Times**, 6 fev. 2020. Disponível em: https://www.nytimes.com/2020/02/06/business/facial-recognition-schools.html. Acesso em: 15 ago. 2021.

AMAZON. **We are implementing a one-year moratorium on police use of Rekognition**. 10 jun. 2020. Disponível em: https://www.aboutamazon.com/news/policy-news-views/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition. Acesso em: 2 ago. 2021.

AMIGO, Ignacio. The Metro Stations of São Paulo That Read Your Face. **Bloomberg CityLab**, 18 mai. 2018. Disponível em: https://www.bloomberg.com/news/articles/2018-05-08/s-o-paulo-metro-s-newest-platform-doors-can-read-your-face. Acesso em: 01 jul. 2021.

AMOORE, Louise; BALL, Kirstie; GRAHAM, Steve; GREEN, Nicola; LYON, David; WOOD, David Murakami; NORRIS, Clive; PRIDMORE, Jason; RAAB, Charles; SAETNAN, Ann Rudinow. **A Report on the Surveillance Society**. London: ICO, Information Comissioner's Office, 2006. Disponível em: https://ico.org.uk/media/1042388/surveillance-society-public-discussion-document-06.pdf. Acesso em: 13 jul. 2021.

ANKEL, Sophia; ASENJO, Alba. A school in Sweden has been fined over $20,000 for using facial recognition software to control student attendance. **Insider**, 29 ago. 2019. Disponível em: https://www.businessinsider.com/a-school-used-facial-recognition-to-illegally-record-class-attendance-2019-8. Acesso em: 15 ago. 2021.

ANPD, Autoridade Nacional de Proteção de Dados. ANPD participa da 41ª Reunião Plenária da Convenção 108. **gov.br**, 1 jul. 2021a. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-da-41a-reuniao-plenaria-da-convencao-108. Acesso em: 2 jul. 2021.

ANPD, Autoridade Nacional de Proteção de Dados. Portaria nº 11, de 27 de janeiro de 2021. Torna pública a agenda regulatória para o biênio 2021-2022. **Diário Oficial da União (DOU),** v. 19, n. Seção 1, p. 3, 28 jan. 2021b. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313. Acesso em: 5 ago. 2021.

ANPD, Autoridade Nacional de Proteção de Dados. **Reunião Técnica sobre Relatório de Impacto de Proteção de Dados Pessoais - BLOCO 1**: Metodologias e Critérios para

Elaboração e Análise do Relatório de Impacto. 21 jun. 2021c. Disponível em: https://www.youtube.com/watch?v=lOUyGsVIKOI. Acesso em: 5 ago. 2021.

ANPD, Autoridade Nacional de Proteção de Dados. **Reunião Técnica sobre Relatório de Impacto de Proteção de Dados Pessoais - BLOCO 2**: Situações/circunstâncias que ensejam a necessidade ou dispensa de elaboração de Relatório de Impacto. 23 jun. 2021d. Disponível em: https://www.youtube.com/watch?v=ClB-gXhhoE4. Acesso em: 5 ago. 2021.

ANPD, Autoridade Nacional de Proteção de Dados. **Reunião Técnica sobre Relatório de Impacto de Proteção de Dados Pessoais - BLOCO 3**: Transparência e publicidade dos Relatórios de Impacto para o setor público e o setor privado. 25 jun. 2021e. Disponível em: https://www.youtube.com/watch?v=DZH8Vgk6jJU.

ANU, Australian National University. Early Exposure Key to Recognising 'Other-race' Faces. **ANU, Newsroom**, 13 set. 2019. Disponível em: https://www.anu.edu.au/news/all-news/early-exposure-key-to-recognising-%E2%80%98other-race%E2%80%99-faces. Acesso em: 9 jul. 2021.

ARANHA, Márcio Iorio. **Manual de Direito Regulatório: Fundamentos de Direito Regulatório**. 5. ed. rev. ampl. London: Laccademia Publishing, 2019.

ARROYO, Verónica; LEUFER, Daniel. Brazil Expert Opinion Facial Categorization (manifestação nos Autos nº 1090663-42.2018.8.26.0100, ação civil pública). **Access Now**, 2020a. Disponível em: https://www.accessnow.org/Brazil-Expert-Opinion-Facial-Categorization. Acesso em: 30 jun. 2021.

ARROYO, Verónica; LEUFER, Daniel. Facial recognition on trial: emotion and gender "detection" under scrutiny in a court case in Brazil. **Access Now**, 29 jun. 2020b. Disponível em: https://www.accessnow.org/facial-recognition-on-trial-emotion-and-gender-detection-under-scrutiny-in-a-court-case-in-brazil/. Acesso em: 28 jun. 2021.

AZRIA, Sandra; WICKERT, Frédéric. **Facial recognition: current situation and challenges**. T-PD(2019)05rev. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Convention 108. 13 nov. 2019. Disponível em: https://rm.coe.int/t-pd-2019-05rev-facial-recognition-report-003-/16809eadf1. Acesso em: 27 jul. 2021.

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. **California Law Review,** v. 104, n. 3, p. 671-732, jun. 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.#. Acesso em: 30 ago. 2021.

BARRETT, Lisa Feldman; ADOLPHS, Ralph; MARSELLA, Stacy; MARTINEZ, Aleix M.; POLLAK, Seth D. Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements **Psychological Science in the Public Interest,** v. 20, n. 1, p. 1-68, 17 jul. 2019. Disponível em: https://doi.org/10.1177/1529100619832930. Acesso em: 30 jun. 2021.

BBC. Facial recognition to 'predict criminals' sparks row over AI bias. **BBC News**, 24 jun. 2020. Disponível em: https://www.bbc.com/news/technology-53165286. Acesso em: 27 jul. 2021.

BFEG, The Biometrics and Forensics Ethics Group. **Ethical issues arising from the police use of live facial recognition technology** (Interim report). fev. 2019. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/781745/Facial_Recognition_Briefing_BFEG_February_2019.pdf. Acesso em: 2 ago. 2021.

BFEG, The Biometrics and Forensics Ethics Group. **Briefing note on the ethical issues arising from public–private collaboration in the use of live facial recognition technology**. 21 jan. 2021. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/953359/LFR_briefing_note_18.1.21.final.pdf. Acesso em: 2 ago. 2021.

BIG BROTHER WATCH. **Face Off: the lawless growth of facial recognition in UK policing**. London: BBW, 2018. Disponível em: https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf. Acesso em: 9 jul. 2021.

BIONI, Bruno; MARTINS, Pedro. **Devido processo informacional**: um salto teórico-dogmático necessário? . 2020a. Disponível em: https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F108127%2F1599509820Ensaio_Devido_Processo_Informacional_-_V2.pdf. Acesso em: 10 jun. 2021.

BIONI, Bruno; MARTINS, Pedro. O que você precisa ler para entender sobre devido processo informacional. **Data Privacy Brasil**, 2020b. Disponível em: https://conteudo.dataprivacy.com.br/devido-processo-informacional. Acesso em: 29 jun. 2021.

BIONI, Bruno Ricardo. **Proteção de dados pessoais : a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo; RIELLI, Mariana. **Uso de ferramentas de reconhecimento facial por parte de empresas e governos**. Audiência Pública. Ref. Inquérito Civil Público n. 08190.052289/18-94. 2019. Disponível em: https://dataprivacy.com.br/wp-content/uploads/2019/05/Bioni-Data-Privacy-AP-Reconhecimento-facial.pdf. Acesso em: 5 ago. 2021.

BITTENCOURT, Ana. Sistema biométrico registra mais de 400 casos de uso irregular de cartões no transporte público. **Prefeitura Municipal de Santa Maria, Secretaria de Comunicação e Programação Institucional**, 9 jun. 2016. Disponível em: https://www.santamaria.rs.gov.br/noticias/13119-sistema-biometrico-registra-mais-de-400-casos-de-uso-irregular-de-cartoes-no-transporte-publico. Acesso em: 2 jul. 2021.

BORGES, Juliana. Ônibus de Vitória têm sistema de biometria para evitar fraudes. **Portal G1**, 2014. Disponível em: http://g1.globo.com/espirito-santo/noticia/2014/01/onibus-de-vitoria-tem-sistema-de-biometria-para-evitar-fraudes.html. Acesso em: 2 jul. 2021.

BRASIL. Brasil testa primeira ponte aérea com reconhecimento facial do mundo. **gov.br, Notícias**, 15 jun. 2021a. Disponível em: https://www.gov.br/pt-br/noticias/transito-e-transportes/2021/06/brasil-testa-primeira-ponte-aerea-com-reconhecimento-facial-do-mundo. Acesso em: 13 jul. 2021.

BRASIL, Ministério da Economia. Reconhecimento facial pelo aplicativo "Meu gov.br" é a primeira etapa da prova de vida dos aposentados. **gov.br**, 24 ago. 2020b. Disponível em: https://www.gov.br/economia/pt-br/assuntos/noticias/2020/agosto/reconhecimento-facial-pelo-aplicativo-meu-gov-br-e-a-primeira-etapa-da-prova-de-vida-dos-aposentados. Acesso em: 13 jul. 2021.

BRASIL, Supremo Tribunal Federal (Plenário). **Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal**. Ementa: medida cautelar em ação direta de inconstitucionalidade. referendo. medida provisória nº 954/2020. emergência de saúde pública de importância internacional decorrente do novo coronavírus (covid-19). compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o instituto brasileiro de geografia e estatística. *fumus boni juris*. *periculum in mora*. deferimento. ADI 6387 MC-Ref, Relator(a): Min. Rosa Weber, Tribunal Pleno, julgado em 07/05/2020, Processo Eletrônico DJe-270 Divulg. 11-11-2020 Public. 12-11-2020. 2020c. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754357629. Acesso em: 31 ago. 2021.

BRASIL, Supremo Tribunal Federal (Plenário). **Referendo na Medida Cautelar na Ação Direta de inconstitucionalidade (ADI) nº 6.389/DF**. Ementa medida cautelar em ação direta de inconstitucionalidade. Referendo. Medida provisória nº 954/2020. Emergência de saúde pública de importância internacional decorrente do novo coronavírus (covid-19). Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o instituto brasileiro de geografia e estatística. Fumus boni juris. Periculum in mora. Deferimento. Relatora: Min. Rosa Weber, julgado em 07/05/2020, processo eletrônico dje-270, divulg 11-11-2020, public 12-11-2020. 12 nov. 2020d. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344950131&ext=.pdf. Acesso em: 29 jun. 2021.

BRAZILIAN churches start to introduce facial recognition in their worship services. **Evangelical Focus**, 5 fev. 2020. Disponível em: https://evangelicalfocus.com/science/5088/brazilian-churches-start-to-introduce-facial-recognition-in-their-services. Acesso em: 15 ago. 2021.

BRKAN, Maja. Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond **International Journal of Law and Information Technology,** v. 27, n. 2, p. 91–121, Summer 2019. Disponível em: https://doi.org/10.1093/ijlit/eay017. Acesso em: 1 set. 2021.

BRUNO, Fernanda. Mapas de crime: vigiância distribuída e participação na cibercultura. **Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação,** v. 12, n. 2, p. 1-16, mai./ago. 2009. Disponível em: https://www.e-compos.org.br/e-compos/article/download/409/352/0. Acesso em: 3 jul. 2021.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification **Proceedings of Machine Learning Research. Conference on Fairness, Accountability, and Transparency,** v. 18, p. 1-15, 2018. Disponível em: proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 30 jun. 2021.

BUOLAMWINI, Joy; ORDÓÑEZ, Vicente; MORGENSTERN, Jamie; LEARNED-MILLER, Erik. **Facial recognition technologies: a primer**. 2020. Disponível em: https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf. Acesso em: 15 ago. 2021.

CAIAFA, Janice. Automação e vigilância no metrô de São Paulo. **IV Simposio Internacional LAVITS: Nuevos paradigmas de la Vigilancia? Buenos Aires**, 2016. Disponível em: https://lavits.org/wp-content/uploads/2017/08/P2_Caiafa.pdf. Acesso em: 2 jul. 2021.

CAMPBELL, John W. M. Differential Impacts of Demographics in Biometric Systems. **NIST IFPC Conference**, 27 nov. 2018. Disponível em: file:///Users/sss/Downloads/13_campbell_NIST_IFPC_Conference_2018.pdf. Acesso em: 21 jul. 2021.

CASA HUNTER. **Síndrome de DiGeorge**. 2021. Disponível em: https://casahunter.org.br/doencas-raras/sindrome-digeorge.php. Acesso em: 20 ago. 2021.

CASEMIRO, Luciana. **Hering terá que explicar o que faz com dados de reconhecimento facial**. **O Globo**, 26 fev. 2019. Disponível em: https://oglobo.globo.com/economia/defesa-do-consumidor/hering-tera-que-explicar-que-faz-com-dados-de-reconhecimento-facial-de-clientes-23482114. Acesso em: 19 jul. 2021.

CERT.br, Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil. **Estatísticas dos Incidentes Reportados ao CERT.br**. 3 ago. 2021a. Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 31 ago. 2021.

CERT.br, Centro de Estudos Resposta e Tratamento de Incidentes de Segurança no Brasil. **Sobre o CERT.br** 2021b. Disponível em: https://www.cert.br/sobre/. Acesso em: 31 ago. 2021.

CIMPANU, Catalin. Facial recognition doesn't work as intended on 42 of 110 tested smartphones. 5 jan. 2019a. Disponível em: https://www.zdnet.com/article/facial-recognition-doesnt-work-as-intended-on-42-of-110-tested-smartphones/. Acesso em: 28 jul. 2021.

CIMPANU, Catalin. Samsung Galaxy S10 facial recognition fooled by a video of the phone owner. **ZDNet**, 11 mar. 2019b. Disponível em: https://www.zdnet.com/article/samsung-galaxy-s10-facial-recognition-fooled-by-a-video-of-the-phone-owner/. Acesso em: 28 jul. 2021.

CITRON, Danielle Keats; PASQUALE, Frank A. The Scored Society: Due Process for Automated Predictions. **Washington Law Review,** v. 89, p. 1-31, 2014. Disponível em: https://ssrn.com/abstract=2376209. Acesso em: 29 jun. 2021.

CJEU, Court of Justice of the European Union. **Case František Ryneš v Úřad pro ochranu**. Case C-212/13. Judgment of the Court (Fourth Chamber). REQUEST for a preliminary ruling under Article 267 TFEU from the Nejvyšší správní soud (Czech Republic), made by decision of 20 March 2013, received at the Court on 19 April 2013, in the proceedings. (Reference for a preliminary ruling — Directive 95/46/EC — Protection of individuals — Processing of personal data — Concept of 'in the course of a purely personal or household activity'). 11 dez. 2014. Disponível em:

https://curia.europa.eu/juris/document/document_print.jsf;jsessionid=7669E32758B7C95134342645F7D25B26?docid=160561&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=727415. Acesso em: 21 jul. 2021.

COHEN, Julie E. What privacy is for. **Harv. L. Rev. ,** v. 126, n. 7, p. 1904-1933, 20 mai. 2013. Disponível em: https://harvardlawreview.org/2013/05/what-privacy-is-for/ https://harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf. Acesso em: 10 jun. 2021.

COMISSÃO DE JURISTAS, sobre Segurança Pública. **Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal**. nov. 2020. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos. Acesso em: 22 jun. 2021.

COMISSÃO ESPECIAL, destinada a proferir parecer ao Projeto de Lei nº 4.060, de 2012,. **Parecer ao Projeto de Lei nº 4.060, de 2012** (Tratamento e Proteção de Dados Pessoais) (Apenso PLs nº 5.276/16 e 6.291/16). Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Autor: Deputado Milto Monti. Relator: Deputado Orlando Silva., 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305

http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1664206. Acesso em: 22 jun. 2021.

CORMEN, Thomas H.; LEISERSON, Charles E.; RIVEST, Ronald L.; STEIN, Clifford. **Introduction to Algorithms**. 2nd ed. Massachusetts: MIT Press, 2001.

COUNCIL OF EUROPE. **Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies.** Adopted by the Committee of Ministers on 11 June 2013 at the 1173rd meeting of the Ministers' Deputies. 11 jun. 2013. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168068460d. Acesso em: 27 jul. 2021.

COUNCIL OF EUROPE. **128th Session of the Committee of Ministers. Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data**. CM/Inf(2018)15-final. Elsinore, Denmark. 17-18 mai. 2018. Disponível em: https://ccdcoe.org/uploads/2019/09/CoE-180518-Modernised-Convention-for-the-Protection-of-Individuals-with-Regard-to-the-Processing-of-Personal-Data.pdf. Acesso em: 27 jul. 2021.

COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty 108**. 27 jul. 2021a. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108?module=signatures-by-treaty&treatynum=108. Acesso em: 27 jul. 2021.

COUNCIL OF EUROPE. **Convention 108 and Protocols**. 2021b. Disponível em: https://www.coe.int/en/web/data-protection/convention108-and-protocol. Acesso em: 27 jul. 2021.

COUNCIL OF EUROPE. **Guidelines on Facial Recognition**. T-PD(2020)03rev4. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data Convention 108.40ª Convention 108 on Data Protection. 28 jan. 2021c. Disponível em: https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3. Acesso em: 20 jul. 2021.

COX, Kate. Cops in Miami, NYC arrest protesters from facial recognition matches. **ArsTechnica**, 18 ago. 2020. Disponível em: https://arstechnica.com/tech-policy/2020/08/cops-in-miami-nyc-arrest-protesters-from-facial-recognition-matches/. Acesso em: 27 jul. 201.

CST EDITORIAL BOARD. Don't gut Illinois law that prohibits the secret sale of our fingerprints and other biometric information. **Chicago Sun-Times**, 16 mar. 2021. Disponível em: https://chicago.suntimes.com/2021/3/16/22334405/biometric-protection-bipa-illinois-law-legislation-editorial. Acesso em: 2 ago. 2021.

DEARDEN, Lizzie. Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested. **Independent**, 31 jan. 2019. Disponível em: https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html. Acesso em: 2 ago. 2021.

DELHI: Facial recognition system helps trace 3,000 missing children in 4 days. **The Times of India**, 22 abr. 2018. Disponível em: https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms. Acesso em: 27 jul. 2021.

DENATRAN, Departamento Nacional de Trânsito. Quantidade de Habilitados - DENATRAN. **gov.br**, 2021. Disponível em: https://www.gov.br/infraestrutura/pt-br/assuntos/transito/conteudo-denatran/estatisticas-quantidade-de-habilitados-denatran1790. Acesso em: 29 jul. 2021.

DIAS, Tatiana; MARTINS, Rafael Moro. Documentos vazados mostram que Abin pediu ao Serpro dados e fotos de todas as CNHs do país. **The Intercept Brasil**, 2020. Disponível em: https://theintercept.com/2020/06/06/abin-carteira-motorista-serpro-vigilancia/. Acesso em: 29 jul. 2021.

DODD, Vikram. A thousand young, black men removed from Met gang violence prediction database. **The Guardian**, 3 fev. 2021. Disponível em: https://www.theguardian.com/uk-news/2021/feb/03/a-thousand-young-black-men-removed-from-met-gang-violence-prediction-database. Acesso em: 21 jul. 2021.

DOSHI-VELEZ, Finale; KORTZ, Mason A. Accountability of AI Under the Law: The Role of Explanation. **Berkman Klein Center Working Group on Explanation and the Law, Berkman Klein Center for Internet & Society working paper.**, p. 1-15, 2017. Disponível em: http://nrs.harvard.edu/urn-3:HUL.InstRepos:34372584. Acesso em: 30 ago. 2021.

DOVAL, Pankaj. Face recognition to be must for all Aadhaar authentications. **The Times of India**, 24 ago. 2018. Disponível em: https://timesofindia.indiatimes.com/india/face-recognition-to-be-must-for-all-aadhaar-authentications/articleshow/65522828.cms. Acesso em: 27 jul. 2021.

DRAPER, Kevin. Madison Square Garden Has Used Face-Scanning Technology on Customers. **The New York Times**, 13 mar. 2018. Disponível em: https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html. Acesso em: 15 ago. 2021.

DURKIN, Erin. New York tenants fight as landlords embrace facial recognition cameras. **The Guardian**, 30 mai. 2019. Disponível em: https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex. Acesso em: 27 jul. 2021.

EC, European Commission. **What is Horizon 2020?** . 2020. Disponível em: https://ec.europa.eu/programmes/horizon2020/en/what-horizon-2020. Acesso em: 10 set. 2021.

EDPB, European Data Protection Board. **Guidelines 3/2019 on processing of personal data through videodevices**. 10 jul. 2019. Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_201903_videosurveillance.pdf. Acesso em: 22 jul. 2021.

EDPB, European Data Protection Board. **Article 29 Working Party**. 2021a. Disponível em: https://edpb.europa.eu/about-edpb/more-about-edpb/article-29-working-party_en. Acesso em: 10 jul. 2021.

EDPB, European Data Protection Board. **Who we are**. 2021b. Disponível em: https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_en. Acesso em: 10 jul. 2021.

EDPB, European Data Protection Board; EDPS, European Data Protection Supervisor. **EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence** (Artificial Intelligence Act). 18 jun. 2021. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en. Acesso em: 26 jun. 2021.

EDPS, European Data Protection Supervisor. **The EDPS Video-Surveillance Guidelines**. 17 mar. 2010. Disponível em: https://edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf. Acesso em: 22 jul. 2021.

EDPS, European Data Protection Supervisor. Preliminary Opinion on privacy by design (Opinion 5/2018). 31 mai. 2018. Disponível em: https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf. Acesso em: 4 set. 2021.

EDPS, European Data Protection Supervisor. **Artificial Intelligence Act**: a welcomed initiative, but ban on remote biometric identification in public space is necessary. Presse Release EDPS/2021/09. Brussels, 23 April 2021., 2021a. Disponível em: https://edps.europa.eu/press-publications/press-news/press-releases/2021/artificial-intelligence-act-welcomed-initiative_en. Acesso em: 26 jun. 2021.

EDPS, European Data Protection Supervisor. **Glossary**. 2021b. Disponível em: https://edps.europa.eu/data-protection/data-protection/glossary_en. Acesso em: 22 jul. 2021.

EDPS, European Data Protection Supervisor. **Video-surveillance**. 2021c. Disponível em: https://edps.europa.eu/data-protection/data-protection/reference-library/video-surveillance_en. Acesso em: 22 jul. 2021.

EDRi, European Digital Rights. Who we are. 2021. Disponível em: https://edri.org/about-us/. Acesso em: 26 ago. 2021.

ELIZONDO-URRESTARAZU, Jone. The other pandemic: Systemic racism and its consequences. **Equinet [European Network of Equality Bodies]**, 8 jun. 2020. Disponível em: https://equineteurope.org/2020/the-other-pandemic-systemic-racism-and-its-consequences/. Acesso em: 30 jun. 2021.

EPIC, Electronic Privacy Informaiton Center. Patel v. Facebook. Whether collection of an individual's biometric data in violation of the Illinois Biometric Information Privacy Act is sufficient to establish Article III standing. **epic.org**, 2021. Disponível em: https://epic.org/amicus/bipa/patel-v-facebook/. Acesso em: 21 ago. 2021.

EUROPEAN COMISSION. **Automatic Sentiment Estimation in the Wild (SEWA)**. 13 jun. 2019. Disponível em: https://cordis.europa.eu/project/id/645094. Acesso em: 29 jun. 2021.

EUROPEAN PARLIAMENT. **Letter to the Commission on Artificial Intelligence and Biometric Surveillance. Brussel**. 15 abr. 2021. Disponível em: https://www.patrick-breyer.de/wp-content/uploads/2021/04/MEP-Letter-to-the-Commission-on-Artificial-Intelligence-and-Biometric-Surveillance.pdf. Acesso em: 26 jun. 2021.

FACEAPP, Technology Limited. **FaceApp**. 2021. Disponível em: https://www.faceapp.com/. Acesso em: 27 jul. 2021.

FAITHFULL, Mark. Forget Apps, Russia's X5 And Visa Have Launched Pay With Your Face. **Forbes**, 10 mar. 2021. Disponível em: https://www.forbes.com/sites/markfaithfull/2021/03/10/forget-apps-russias-x5-and-visa-have-launched-pay-with-your-face/?sh=6bb54161787d. Acesso em: 13 jul. 2021.

FERRARA, Matteo; FRANCO, Annalisa; MALTONI, Davide. The magic passport. **EEE International Joint Conference on Biometrics**, p. 1-7, 2014. Disponível em: http://dx.doi.org/10.1109/BTAS.2014.6996240. Acesso em: 29 jul. 2021.

FIRST INSIGHT. **The evolving in-store experience: inside the mind of today's consumer**. Consumer Survey Report. ago. 2015. Disponível em: https://cdn2.hubspot.net/hubfs/160569/First_Insight-In_Store_Experience_Report.pdf. Acesso em: 13 jul. 2021.

FORBRUKARRÅDET, [Conselho de Consumidores da Noruega]. Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy. 27 jun. 2018. Disponível em: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf. Acesso em: 4 set. 2021.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2020**. 2020. Disponível em: https://forumseguranca.org.br/wp-content/uploads/2020/10/anuario-14-2020-v1-interativo.pdf. Acesso em: 18 jul. 2021.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Lisboa: Edições 70, 2013.

FREY, Chris. Revealed: how facial recognition has invaded shops – and your privacy. **The Guardian**, 3 mar. 2016. Disponível em: https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto. Acesso em: 27 jul. 2021.

FUCHS, Christian. Como podemos definir vigilância? **MATRIZes,** v. 5, n. 1, p. 109-136, jul./dez. 2011. Disponível em: https://www.revistas.usp.br/matrizes/article/download/38311/41154. Acesso em: 7 set. 2021.

FUSSEY, Pete; MURRAY, Daragh. **Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology**. Essex: The Human Rights, Big Data and Technology Project (Human Rights Centre - University of Essex), 2019. Disponível em: https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf. Acesso em: 28 jul. 2021.

G1. Recém-aposentados sofrem com assédio abusivo de oferta de empréstimo consignado. **Portal G1, Fantático**, 17 fev. 2019a. Disponível em: https://g1.globo.com/fantastico/noticia/2019/02/17/recem-aposentados-sofrem-com-assedio-abusivo-de-oferta-de-emprestimo-consignado.ghtml. Acesso em: 10 ago. 2021.

G1. Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano. **Portal G1**, 11 jul. 2019b. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em: 1 jul. 2021.

G1 AM. Mais de 3 mil têm cartão bloqueado com biometria facial em ônibus no AM. **Portal G1**, 25 nov. 2015a. Disponível em: http://g1.globo.com/am/amazonas/noticia/2015/11/mais-de-3-mil-tem-cartao-bloqueado-com-biometria-facial-em-onibus-no-am.html. Acesso em: 2 jul. 2021.

G1 AM. Ônibus terão biometria facial após fraudes de R$ 230 mil por mês, no AM. **Portal G1**, 23 nov. 2015b. Disponível em: http://g1.globo.com/am/amazonas/noticia/2015/11/onibus-terao-biometria-facial-apos-fraudes-de-r-230-mil-por-mes-no-am.html. Acesso em: 2 jul. 2021.

G1 AM. Sistema de reconhecimento facial para emissão da CNH é implantado no AM. **Portal G1**, 23 out. 2019. Disponível em: https://g1.globo.com/am/amazonas/noticia/2019/10/23/sistema-de-reconhecimento-facial-para-emissao-da-cnh-e-implantado-no-am.ghtml. Acesso em: 30 jul. 2021.

G1 BA. Feira de Santana registra 33 prisões por reconhecimento facial durante micareta **Portal G1**, 29 abr. 2019. Disponível em: https://g1.globo.com/ba/bahia/noticia/2019/04/29/feira-de-

santana-registra-33-prisoes-por-reconhecimento-facial-durante-micareta.ghtml. Acesso em: 26 ago. 2021.

G1 PIRACICABA. Reconhecimento facial em ônibus começa a funcionar em Limeira, SP. **Portal G1**, 10 jun. 2014. Disponível em: http://g1.globo.com/sp/piracicaba-regiao/noticia/2014/06/reconhecimento-facial-em-onibus-comeca-funcionar-em-limeira-sp.html. Acesso em: 2 jul. 2021.

G1 SÃO CARLOS E ARARAQUARA. Após instalação de biometria facial, crianças portadoras de deficiência não conseguem andar de graça nos ônibus. **Portal G1**, 26 jul. 2018. Disponível em: https://g1.globo.com/sp/sao-carlos-regiao/noticia/2018/07/26/apos-instalacao-de-biometria-facial-criancas-portadoras-de-deficiencia-nao-conseguem-andar-de-graca-nos-onibus.ghtml. Acesso em: 29 jul. 2021.

G1 SC. Reconhecimento facial começa a funcionar em terminais de ônibus. **Portal G1**, 21 jul. 2014. Disponível em: http://g1.globo.com/sc/santa-catarina/noticia/2014/07/reconhecimento-facial-comeca-funcionar-em-terminais-de-onibus.html. Acesso em: 2 jul. 2021.

G1 SP. Aeroporto de Congonhas testa câmeras de reconhecimento facial. **Portal G1**, 15 jun. 2021. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2021/06/15/aeroporto-de-congonhas-testa-cameras-de-reconhecimento-facial.ghtml. Acesso em: 13 jun. 2021.

GAO, United States Government Accountability Office. Facial Recognition Technology: Current and Planned Uses by Federal Agencies (GAO-21-526). ago. 2021. Disponível em: https://internetlab.us13.list-manage.com/track/click?u=90e39079bb4e0e61df967d918&id=3a1f8b5f94&e=0975f2d982. Acesso em: 2 ago. 2021.

GARTNER INC. **About us**. 2021. Disponível em: https://www.gartner.com/en/about. Acesso em: 21 ago. 2021.

GARVIE, Clare; BEDOYA, Alvaro M; FRANKLE, Jonathan. **The Perpetual Line-up: Unregulated Police Face Recognition in America**. Law Center Center on Privacy & Technology, Georgetown University, 2016. Disponível em: https://www.perpetuallineup.org/. Acesso em: 30 jun. 2021.

GEE, Kelsey. In Unilever's Radical Hiring Experiment, Resumes Are Out, Algorithms Are In **The Wall Street Journal**, 26 jun. 2017. Disponível em: https://www.wsj.com/articles/in-unilevers-radical-hiring-experiment-resumes-are-out-algorithms-are-in-1498478400. Acesso em: 30 ago. 2021.

GELLMAN, Barton. NSA broke privacy rules thousands of times per year, audit finds. **The Washington Post**, 15 ago. 2013. Disponível em: https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html. Acesso em: 9 jul. 2021.

GILLESPIE, Eden. Are you being scanned? How facial recognition technology follows you, even as you shop. **The Guardian**, 24 fev. 2019. Disponível em:

https://www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop. Acesso em: 27 jul. 2021.

GOMES, Amur Castanheira; OLIVEIRA, Davi. Em menos de três anos, biometria facial bloqueia 12 mil cartões de ônibus em Ribeirão Preto. **Diário do Transporte**, 21 mar. 2018. Disponível em: https://diariodotransporte.com.br/2018/03/21/em-menos-de-tres-anos-biometria-facial-bloqueia-12-mil-cartoes-de-onibus-em-ribeirao-preto-27/. Acesso em: 2 jul. 2021.

GOMES, Maria Cecília Oliveira. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. In: LIMA, A. P.;HISSA, C.*, et al* (Ed.). **Direito Digital: Debates Contemporâneos**. São Paulo: Revista dos Tribunais, 2019a. p.141-153.

GOMES, Maria Cecília Oliveira. Relatório de impacto à proteção de dados. Uma breve análise da sua definição e papel na LGPD. **Revista da AASP,** v. 144, p. 6-15, 2019b. Disponível em: https://direito.academia.edu/MariaCec%C3%ADliaOliveiraGomes. Acesso em: 5 ago. 2021.

GPA, Global Privacy Assembly. Adopted Resolution on Facial Recognition Technology. **42nd Closed Session of the Global Privacy Assembly**, out. 2020. Disponível em: https://edps.europa.eu/sites/edp/files/publication/final_gpa_resolution_on_facial_recognition_technology_en.pdf. Acesso em: 23 jul. 2021.

GPA, Global Privacy Assembly. **GPA Home**. 2021. Disponível em: https://globalprivacyassembly.org/. Acesso em: 24 jul. 2021.

GREENBERG, Andy. This Site Published Every Face From Parler's Capitol Riot Videos. **Wired**, 20 jan. 2021. Disponível em: https://www.wired.com/story/faces-of-the-riot-capitol-insurrection-facial-recognition/. Acesso em: 27 jul. 2021.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. **National Institute of Standards and Technology, U.S. Department of Commerce**, dez. 2019. Disponível em: https://doi.org/10.6028/NIST.IR.8280. Acesso em: 30 jun. 2021.

GS1 BRASIL. Supermercado de experiência autônoma Zaitt prevê novas lojas. **GS1 Brasil**, 30 ago. 2019. Disponível em: https://noticias.gs1br.org/supermercado-de-experiencia-autonoma-zaitt-preve-novas-lojas/. Acesso em: 10 ago. 2021.

GUO, Eileen; NOORI, Hikmat. This is the real story of the Afghan biometric databases abandoned to the Taliban. **MIT Technology Review**, 30 ago. 2021. Disponível em: https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/. Acesso em: 2 set. 2021.

GUO, Yandong; ZHANG, Lei; HU, Yuxiao; HE, Xiaodong; GAO, Jianfeng. **MS-Celeb-1M: A Dataset and Benchmark for Large-Scale Face Recognition**. Lecture Notes in Computer Science. Computer Vision – ECCV 2016. B., L.;J., M.*, et al*: Springer, Cham. vol 9907 2016.

HAMANN, Kristine; SMITH, Rachel. Facial Recognition Technology: Where Will it Take Us? **American Bar Association Criminal Justice Magazine**, Spring 2019. Disponível em:

https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/. Acesso em: 9 jul. 2021.

HARWELL, Drew. FBI, ICE Find State Driver's License Photos a Gold Mine for Facial-Recognition Searches. **The Washington Post**, 7 jul. 2019. Disponível em: https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/. Acesso em: 30 jun. 2021.

HEAVEN, Douglas. Why faces don't always tell the truth about feelings. **Nature, News Feature**, 26 fev. 2020. Disponível em: https://www.nature.com/articles/d41586-020-00507-5. Acesso em: 17 set. 2021.

HEBER, Alex. Coca-Cola Is Using Facial Recognition Technology On Fridges In Australia To Sell More Drinks. **Business Insider Australia**, 1 mai. 2014. Disponível em: https://www.businessinsider.com.au/coca-cola-is-using-facial-recognition-technology-on-fridges-in-australia-to-sell-more-drinks-2014-5. Acesso em: 27 jul. 2021.

HERN, Alex. Google's solution to accidental algorithmic racism: ban gorillas. **The Guardian**, 12 jan. 2018. Disponível em: https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people. Acesso em: 28 jul. 2021.

HIGÍDIO, José. ViaQuatro deve indenizar por implantar sistema de detecção facial nas estações. **Revista Consultor Jurídico**, p. 10 mai., 2021. Disponível em: https://www.conjur.com.br/2021-mai-10/viaquatro-indenizar-implantar-sistema-deteccao-facial. Acesso em: 1 jul. 2021.

HILL, Kashmir. The Secretive Company That Might End Privacy as We Know It. **The New York Times**, 18 jan. 2020. Disponível em: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. Acesso em: 30 jun. 2021.

HIREVUE. HireVue hiring assessment software. **HireVue, Inc.**, 2021. Disponível em: https://www.hirevue.com/platform/assessment-software. Acesso em: 28 jul. 2021.

HOLDEN, Mike. Pittsburgh police used facial recognition technology during Black Lives Matter protests. **WPXI-TV**, 21 mai. 2020. Disponível em: https://www.wpxi.com/news/top-stories/pittsburgh-police-used-facial-recognition-technology-during-black-lives-matter-protests/VT52MGWM3VCDJINJSZPOO5NHKU/. Acesso em: 27 jul. 2021.

HOROWITZ, Julia. Tech companies are still helping police scan your face. **CNN Business**, 3 jul. 2020. Disponível em: https://edition.cnn.com/2020/07/03/tech/facial-recognition-police/index.html. Acesso em: 30 jun. 2021.

HOUSE OF COMMONS, Science and Technology Committee. **The work of the Biometrics Commissioner and the Forensic Science Regulator. Nineteenth Report of Session 2017–19**. London: House Of Commons, Science and Technology Committee, 2019.

IBGE, Instituto Brasileiro de Geografia e Estatística. **Estimativas de População**. Tabela 6579. População residente estimada. 2021. Disponível em: https://sidra.ibge.gov.br/tabela/6579. Acesso em: 29 jul. 2021.

IBM. **IBM CEO's Letter to Congress on Racial Justice Reform**. 8 jun. 2020. Disponível em: https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/. Acesso em: 2 ago. 2021.

ICL, Imperial College London; UAU, University of Augsburg; UO, University of Passau; RealEyes; PlayGen. **SEWA Project**. 2018. Disponível em: https://www.sewaproject.eu/. Acesso em: 29 jun. 2021.

ICO, Information Comissioner's Office. **In the picture: A data protection code of practice for surveillance cameras and personal**. Version 1.2. London: ICO, Information Comissioner's Office, 2017. Disponível em: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf. Acesso em: 13 jul. 2021.

ICO, Information Comissioner's Office. **About the ICO**. 2021a. Disponível em: https://ico.org.uk/about-the-ico/. Acesso em: 15 jul. 2021.

ICO, Information Comissioner's Office. What does the UK GDPR say about automated decision-making and profiling? , 2021b. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/. Acesso em: 9 set. 2021.

IDEC, Instituto Brasileiro de Defesa do Consumidor. Estatuto Idec-Instituto Brasileiro de Defesa do Consumidor. Aprovado pela Assembleia Geral Ordinária de associados em 20 de julho de 2013. **Idec**, 2013. Disponível em: https://idec.org.br/uploads/pages/pdfs/estatuto-20131.pdf. Acesso em: 3 jul. 2021.

IDEC, Instituto Brasileiro de Defesa do Consumidor. **Petição inicial de ação civil pública com pedido de tutela de urgência do Instituto Brasileiro de Defesa do Consumidor (Idec) contra a Concessionária da Linha-Amarela 4 do metrô de São Paulo (ViaQuatro)**. 30 ago. 2018. Disponível em: https://idec.org.br/sites/default/files/acp_viaquatro.pdf. Acesso em: 30 jun. 2021.

IDEC, Instituto Brasileiro de Defesa do Consumidor. Após denúncia do Idec, Hering é condenada por uso de reconhecimento facial **Idec**, 31 ago. 2019a. Disponível em: https://idec.org.br/noticia/apos-denuncia-do-idec-hering-e-condenada-por-uso-de-reconhecimento-facial. Acesso em: 19 jul. 2021.

IDEC, Instituto Brasileiro de Defesa do Consumidor. **Carta Idec nº 51/2019/Coex, de 22 de fevereiro de 2019, à Cia Hering**. Questionamento sobre reconhecimento facial e compartilhamento de dados. 22 fev. 2019b. Disponível em: https://idec.org.br/sites/default/files/carta_idec_hering_.pdf. Acesso em: 19 jul. 2021.

IDEC, Instituto Brasileiro de Defesa do Consumidor. **Carta Idec nº 178/2019/Coex, de 18 de abril de 2019**. Ao Carrefour Comércio e Indústria Ltda. 2019c. Disponível em: https://idec.org.br/sites/default/files/carta_idec_178_2019_coex_.pdf. Acesso em: 19 jul. 2021.

IDEC, Instituto Brasileiro de Defesa do Consumidor. **Carta Idec nº 647/2019/Coex, de 30 de agosto de 2019**. À Empresa de Tecnologia e Informações da Previdência - DATAPREV. 2019d. Disponível em: https://idec.org.br/sites/default/files/carta_idec_647_2019_coex.pdf. Acesso em: 19 jul. 2021.

IDEC, Instituto Brasileiro de Defesa do Consumidor. Idec notifica Hering por coleta de dados faciais para publicidade **Idec**, 23 abr. 2019e. Disponível em: https://idec.org.br/noticia/idec-notifica-hering-por-coleta-de-dados-faciais-para-publicidade. Acesso em: 19 jul. 2021.

IDEC, Instituto Brasileiro de Defesa do Consumidor. Idec pede esclarecimento sobre coleta de dado facial em loja do Carrefour. **Idec**, 1 out. 2019f. Disponível em: https://idec.org.br/noticia/idec-pede-esclarecimento-sobre-coleta-de-dado-facial-em-loja-do-carrefour. Acesso em: 19 jul. 2021.

IDEC, Instituto Brasileiro de Defesa do Consumidor. Idec notifica Dataprev por licitação para uso de reconhecimento facial. **Idec**, 27 abr. 2020. Disponível em: https://idec.org.br/noticia/idec-notifica-dataprev-por-licitacao-para-uso-de-reconhecimento-facial. Acesso em: 19 jul. 2021.

IDEC, Instituto Brasileiro de Defesa do Consumidor. Quem Somos. **Idec**, 2021. Disponível em: https://idec.org.br/quem-somos. Acesso em: 3 jul. 2021.

ILLINOIS GENERAL ASSEMBLY. **Biometric Information Privacy Act (BIPA)**. (740 ILCS 14/). 3 out. 2008. Disponível em: https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57. Acesso em: 2 ago. 2021.

INGELBRECHT, Nick. Market Trends: Facial Recognition for Enhanced Physical Security - Differentiating the Good, the Bad and the Ugly. **Gartner Research**, 5 abr. 2019. Disponível em: https://www.gartner.com/en/documents/3906385/market-trends-facial-recognition-for-enhanced-physical-s. Acesso em: 30 jun. 2021.

INMETRO, Instituto Nacional de Metrologia, Qualidade e Tecnologia. **Institucional**. 31 mar. 2021. Disponível em: https://www.gov.br/inmetro/pt-br/acesso-a-informacao/institucional/institucional-index. Acesso em: 24 jul. 2021.

INSS, Instituto Nacional do Seguro Social. INSS amplia e simplifica prova de vida digital. **gov.br**, 23 fev. 2021. Disponível em: https://www.gov.br/inss/pt-br/assuntos/prova-de-vida/inss-amplia-e-simplifica-prova-de-vida-digital. Acesso em: 20 ago. 2021.

INSTITUTO IGARAPÉ. **Reconhecimento Facial no Brasil**. 2019. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/. Acesso em: 30 jun. 2021.

INTEL. Ford and Intel Research Demonstrates the Future of In-Car Personalization and Mobile Interior Imaging Technology. **Intel Newsroom**, 25 jun. 2014. Disponível em: https://newsroom.intel.com/news-releases/ford-and-intel-research-demonstrates-the-future-of-in-car-personalization-and-mobile-interior-imaging-technology/#gs.7io55a. Acesso em: 27 jun. 2021.

INTRONA, Lucas D; NISSENBAUM, Helen. **Facial Recognition Technology: a Survey of Policy and Implementation Issues**. New York: The Center for Catastrophe Preparedness & Response, New York University, 2009.

IRIS, Instituto de Referência em Internet e Sociedade. **Sobre o IRIS**. 2021. Disponível em: https://irisbh.com.br/sobre-o-iris/. Acesso em: 4 jul. 2021.

ISO, International Organization for Standardization; IEC, International Electrotechnical Commission. **ISO/IEC 30107-1:2016(E): Information technology - Biometric presentation attack detection - Part 1: Framework**. 15 jan. 2016. Disponível em: https://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip. Acesso em: 29 jul. 2021.

ISO, International Organization for Standardization; IEC, International Electrotechnical Commission. **ISO/IEC 2382-37:2017(E): Information technology - Vocabulary - Part 37: Biometrics**. 2 ed. Switzerland: ISO/IEC, 2017. Disponível em: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

JAKUBOWSKA, Ella. Mass facial recognition is the apparatus of police states and must be regulated. **EuroNews**, 17 fev. 2021. Disponível em: https://www.euronews.com/2021/02/17/mass-facial-recognition-is-the-apparatus-of-police-states-and-must-be-regulated. Acesso em: 28 jun. 2021.

JASSERAND, Catherine; FONTANILLO-LÓPEZ, César; BELKADI, Lydia; CZARNOCKI, Jan; ÖZAL, Mert; SUMER, Bilgesu; KINDT, Els. **New Extensive Guidelines on the Use of Facial Recognition by the Council of Europe**. mai. 2021. Disponível em: https://lirias.kuleuven.be/retrieve/621497. Acesso em: 25 jul. 2021.

JEE, Charlotte. London police's face recognition system gets it wrong 81% of the time. **MIT Technology Review**, 4 jul. 2019. Disponível em: https://www.technologyreview.com/2019/07/04/134296/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time/. Acesso em: 28 jul. 2021.

JOWITT, Tom. Microsoft Bans Facial Recognition Sales To Police. **Silicon.co.uk**, 12 jun. 2020. Disponível em: https://www.silicon.co.uk/e-innovation/artificial-intelligence/microsoft-bans-facial-recognition-police-345703. Acesso em: 2 ago. 2021.

KAFKA, Franz. **O Processo**. Alfragide: LeYa, 2009.

KANASHIRO, Marta Mourão. **Sorria, você está sendo filmado: as câmeras de monitoramento para segurança em São Paulo**. 2006. (Mestrado). Departamento de Sociologia do Instituto de Filosofia e Ciências Humanas, Universidade Estadual de Campinas, Campinas.

KASTRENAKES, Jacob. Ticketmaster could replace tickets with facial recognition. **The Verge**, 7 mar. 2018. Disponível em: https://www.theverge.com/2018/5/7/17329196/ticketmaster-facial-recognition-tickets-investment-blink-identity. Acesso em: 28 jul. 2021.

KEEGAN, Matthew. Big Brother is watching: Chinese city with 2.6m cameras is world's most heavily surveilled. **The Guardian**, 2 dez. 2019. Disponível em: https://www.theguardian.com/cities/2019/dec/02/big-brother-is-watching-chinese-city-with-26m-cameras-is-worlds-most-heavily-surveilled. Acesso em: 27 jul. 2021.

KLOZA, Dariusz; VAN DIJK, Niels; GELLERT, Raphaël Maurice; BOROCZ, Istvan Mate; TANAS, Alessia; MANTOVANI, Eugenio; QUINN, Paul; RIELLI, Mariana. Avaliações de impacto sobre a proteção de dados na União Europeia: complementando o novo regime jurídico em direção a uma proteção mais robusta dos indivíduos. **d.pia.lab Policy Brief, 1/2017**, p. 1-8, 2020.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei nº 13.709/2018 (Cap. 1). In: FRAZÃO, A.;TEPEDINO, G., *et al* (Ed.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p.445-463.

KOSKELA, Hille. 'Cam Era': the contemporary urban Panopticon. **Surveillance & Society,** v. 1, n. 3, p. 292-313, 2002. Disponível em: https://doi.org/10.24908/ss.v1i3.3342. Acesso em: 27 jun. 2021.

KRIEGER, Mitchell. How to make your own Instagram filter with facial recognition using python. **Towards Data Science**, 27 out. 2020. Disponível em: https://towardsdatascience.com/how-to-make-your-own-instagram-filter-with-facial-recognition-from-scratch-using-python-d3a42029e65b. Acesso em: 16 ago. 2021.

KRUSZKA, Paul; ADDISSIE, Yonit A.; McGINN, Daniel E.; PORRAS, Antonio R.; BIGGS, Elijah; SHARE, Matthew; CROWLEY, T. Blaine; CHUNG, Brian H. Y.; MOK, Gary T. K.; MAK, Christopher C. Y.; MUTHUKUMARASAMY, Premala; THONG, Meow-Keong; SIRISENA, Nirmala D.; DISSANAYAKE, Vajira H. W.; PATHTHINIGE, C. Sampath; PRABODHA, L. B. Lahiru; MISHRA, Rupesh; SHOTELERSUK, Vorasuk; EKURE, Ekanem Nsikak; SOKUNBI, Ogochukwu Jidechukwu; KALU, Nnenna; FERREIRA, Carlos R.; DUNCAN, Jordann-Mishael; PATIL, Siddaramappa Jagdish; JONES, Kelly L.; KAPLAN, Julie D.; ABDUL-RAHMAN, Omar A.; UWINEZA, Annette; MUTESA, Leon; MORESCO, Angélica; OBREGON, María Gabriela; RICHIERI-COSTA, Antonio; GIL-DA-SILVA-LOPES, Vera L.; ADEYEMO, Adebowale A.; SUMMAR, Marshall; ZACKAI, Elaine H.; McDONALD-McGINN, Donna M.; LINGURARU, Marius George; MUENKE, Maximilian. 22q11.2 deletion syndrome in diverse populations. **American Journal of Medical Genetics,** v. 173, n. 4, p. 879-888, 22 mar. 2017. Disponível em: https://doi.org/10.1002/ajmg.a.38199. Acesso em: 27 jul. 2021.

KUTTERER, Cornelia; HOUWING, Lotte; LE GRAND, Gwendal. Facial recognition, a 'convenient' and 'efficient' solution looking for a problem? [1h04min40seg]. Moderator: VELD, Sophie in 't; KORNER, Moritz **13th Computers, Privacy and Data Protection (CPDP) International Conference**, 20 jan. 2020. Disponível em: https://www.youtube.com/watch?v=zVXgB28Qrf0. Acesso em: 28 jun. 2021.

LAPIN, Laboratório de Políticas Públicas e Internet. **Sobre nós**. 2021. Disponível em: https://lapin.org.br/sobre-nos/. Acesso em: 21 ago. 2021.

LAURINO, Talita. Após um ano em vigor, LGPD já embasou mais de mil sentenças na Justiça. **Metrópoles**, 18 set. 2021. Disponível em: https://www.metropoles.com/brasil/economia-br/apos-um-ano-em-vigor-lgpd-ja-embasou-mais-de-mil-sentencas-na-justica. Acesso em: 20 set. 2021.

LE MONDE. La Chine détiendrait un million de Ouïgours dans « des camps d'internement ». **Le Monde**, 31 ago. 2018. Disponível em: https://www.lemonde.fr/asie-pacifique/article/2018/08/31/la-chine-detiendrait-un-million-d-ouigours-dans-des-camps-d-internement_5348573_3216.html. Acesso em: 28 jul. 2021.

LEMOS, Ronaldo; BRANCO, Sérgio. *Privacy by design*: conceito, fundamentos e aplicabilidade na LGPD. In: DONEDA, D.;SARLET, I. W.*, et al* (Ed.). **Tratado de Proteção de Dados**. Rio de Janeiro: Forense, 2021.

LEUFER, Daniel. Computers are binary, people are not: how AI systems undermine LGBTQ identity. **Access Now**, 6 abr. 2021. Disponível em: https://www.accessnow.org/how-ai-systems-undermine-lgbtq-identity/. Acesso em: 15 ago. 2021.

LEWIS, Paul. 'I was shocked it was so easy': meet the professor who says facial recognition can tell if you're gay. **The Guardian, Artificial Intelligence (AI)**, 7 Jul. 2018. Disponível em: https://www.theguardian.com/technology/2018/jul/07/artificial-intelligence-can-tell-your-sexuality-politics-surveillance-paul-lewis. Acesso em: 26 jun. 2021.

LOMAS, Natasha. **Google isn't testing FLoCs in Europe yet**. 24 mar. 2021. Disponível em: https://techcrunch.com/2021/03/24/google-isnt-testing-flocs-in-europe-yet/. Acesso em: 26 jun. 2021.

LYNCH, Jennifer. **Face Off: Law Enforcement Use of Face Recognition Technology**. Electronic Frontier Foundation, 2018. Disponível em: https://www.eff.org/wp/face-off.

LYON, David. Biometrics, Identification and Surveillance. **Bioethics,** v. 22, n. 9, p. 499, 2008. Disponível em: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1467-8519.2008.00697.x. Acesso em: 6 jul. 2021.

MACHADO, Arlindo. Máquinas de vigiar. **Revista USP**, n. 7, p. 23-32, 1990. Disponível em: https://doi.org/10.11606/issn.2316-9036.v0i7p23-32. Acesso em: 27 jun. 2021.

MANN, Monique; SMITH, Marcus. Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight. **UNSW Law Journal,** v. 40, n. 1, p. 121, 2017.

MANTHORPE, Rowland; MARTIN, Alexander J. 81% of 'suspects' flagged by Met's police facial recognition technology innocent, independent report says. **Sky News**, 4 jul. 2019. Disponível em: https://news.sky.com/story/met-polices-facial-recognition-tech-has-81-error-rate-independent-report-says-11755941. Acesso em: 28 jul. 2021.

MARASCIULO, Marilia. Reconhecimento facial: prós e contras da tecnologia que veio para ficar. **Revista Galileu**, 22 jun. 2020. Disponível em: https://revistagalileu.globo.com/Tecnologia/noticia/2020/06/reconhecimento-facial-pros-e-contras-da-tecnologia-que-veio-para-ficar.html. Acesso em: 16 ago. 2021.

MARQUES, Claudia Lima; MUCELIN, Guilherme. Novo Mercado de Consumo 'Simbiótico' e a Necessidade de Proteção de Dados dos Consumidores. In: SARLET, G. B. S.;TRINDADE, M. G. N., *et al* (Ed.). **Proteção de dados: temas controvertidos**. Indaiatuba: Foco, 2021. p.133-183.

MARROW, Alexander. 'Pay with a glance': Russia's Sberbank rolling out face-recognition payments. **Reuters**, 22 abr. 2021. Disponível em: https://www.reuters.com/article/russia-technology-sberbank-face-idUSL8N2MF4BF. Acesso em: 13 jul. 2021.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. **Big Data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana**. Rio de Janeiro: Elsevier, 2013.

McGREGOR, Lorna; MURRAY, Daragh; NG, Vivian. International Human Rights Law as a Framework for Algorithmic Accountability. **International & Comparative Law Quarterly,** v. 68, n. 2, p. 309 - 343 2019. Disponível em: https://doi.org/10.1017/S0020589319000046. Acesso em: 29 jun. 2021.

McKONE, Elinor; WAN, Lulu; PIDCOCK, Madeleine; CROOKES, Kate; REYNOLDS, Katherine; DAWEL, Amy; KIDD, Evan; FIORENTINI, chiara. A Critical Period for Faces: Other-race Face Recognition is Improved by Childhood but not Adult Social Contact. **Scientific Reports,** v. 9, n. 12820, p. 1-13, 6 set. 2019. Disponível em: https://www.nature.com/articles/s41598-019-49202-0. Acesso em: 9 jul. 2021.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. O diálogo entre o marco civil da Internet e o Código de defesa do consumidor. **Revista de Direito do Consumidor,** v. 25, n. 106, p. 37-69, 2016. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RDCons_n.106.02.PDF.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. **Jota**, 10 mai. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 22 jun. 2021.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais e Justiça,** v. 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel; FONSECA, Gabriel ampos Soares da. Proteção de dados para além do consentimento: tendências de materialização. (cap. 4). In: DONEDA, D.;SARLET, I. W., *et al* (Ed.). **Tratado de Proteção de Dados**. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados. **Revista de Direito do Consumidor,** v. 130, p. 471-478, jul./ago. 2020.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. **RDU,** v. 16, n. 90, p. 39-64, nov.-dez. 2019.

MENDOZA, Isak; BYGRAVE, Lee A. The Right Not to Be Subject to Automated Decisions Based on Profiling. **University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20**, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855. Acesso em: 1 set. 2021.

MERCADO & CONSUMO. Hering inaugura loja conceito no Shopping Morumbi, em São Paulo. **Mercado & Consumo**, 12 out. 2018. Disponível em: https://mercadoeconsumo.com.br/2018/10/12/hering-inaugura-loja-conceito-no-shopping-morumbi-em-sao-paulo/. Acesso em: 19 jul. 2021.

MICROSOFT. **Seeing AI App**. 2021. Disponível em: https://www.microsoft.com/en-us/ai/seeing-ai. Acesso em: 27 jul. 2021.

MIRAGEM, Bruno. **Curso de Direito do Consumidor [livro eletrônico]**. 6. ed. em e-book baseada na 8. ed. impressa. São Paulo: Thomson Reuters Brasil, 2020.

MIRANDA, Inaê. Ônibus tenta evitar fraude com biometria facial. **Correio Popular**, 12 nov. 2015. Disponível em: https://correio.rac.com.br/_conteudo/2015/11/campinas_e_rmc/399614-nibus-tenta-evitar-fraude-com-biometria-facial.html. Acesso em: 2 jul. 2021.

MITREFINCH. **Facial Recognition for Employee Time Tracking**. 2021. Disponível em: https://mitrefinch.com/blog/facial-recognition-for-employee-time-tracking/. Acesso em: 15 ago. 2021.

MJOSETH, Jeannine. Facial recognition software helps diagnose rare genetic disease. **NHGRI, National Human Genome Research Institute**, 23 mar. 2017. Disponível em: https://www.genome.gov/news/news-release/Facial-recognition-software-helps-diagnose-rare-genetic-disease. Acesso em: 27 jul. 2021.

MOBILIDADE SAMPA. **ViaQuatro lança portas interativas digitais nas plataformas da Linha 4-Amarela**. 2018. Disponível em: https://mobilidadesampa.com.br/2018/04/viaquatro-lanca-portas-interativas-digitais-nas-plataformas-da-linha-4-amarela/. Acesso em: 30 jun. 2021.

MONTAG, Luca; McIEOD, Rory; METS, Lara De; GAULD, Meghan; RODGER, Fraser; PEŁKA, Mateusz. **The rise and rise of biometric mass surveillance in the EU: a legal analysis of biometric mass surveillance practices in Germany, The Netherlands, and Poland**. Brussels: EDRi, European Digital Rights, 2021. Acesso em: 10 jul. 2021.

MONTAGNER, Camila. Dados biométricos dos paulistanos são coletados no metrô sem consentimento nem debate das implicações. **Rede Latino-Americana de Estudos sobre Vigilância, Tecnologia e Sociedade (Lavits)**, 2 mai. 2018. Disponível em: https://lavits.org/dados-biometricos-dos-passageiros-do-metro-de-sp-sao-tratados-sem-consentimento-nem-discussao-das-implicacoes/?lang=pt. Acesso em: 2 jul. 2021.

MONTEIRO, André. Ônibus de SP terão catraca com câmera para flagrar fraude no transporte. **Folha de S.Paulo**, 31 jul. 2014. Disponível em:

https://www1.folha.uol.com.br/cotidiano/2014/07/1493653-onibus-de-sp-terao-catraca-com-camera-para-flagrar-fraude-no-transporte.shtml. Acesso em: 2 jul. 2021.

MONTEIRO, Renato Leite. Proteção de dados: a legislação vigente no Brasil (white-paper). **Baptista Luz Advogados**, 27 nov. 2017. Disponível em: http://baptistaluz.com.br/wp-content/uploads/2017/11/Privacy-Hub-Leis-Setoriais.pdf. Acesso em: 15 jun. 2021.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? **Instituto Igarapé - Artigo Estratégico,** v. 39, dez. 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf.

MORAES, Maria Celina Bodin de. Apresentação do autor e da obra. In: RODOTÁ, S. (Ed.). **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

MPSP, Ministério Público do Estado de São Paulo. **Manifestação do MPSP no Processo nº 1090663-42.2018.8.26.0100, da 37ª Vara Cível – Foro Central**. 27 jan. 2020. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2020/12/27.01.2020-Manifesta%C3%A7%C3%A3o-do-MP-concordando-com-o-deferimento-dos-pedidos.pdf. Acesso em: 4 jul. 2021.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (lei 13.709/18). **R. Dir. Gar. Fund,** v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: http://dx.doi.org/10.18759/rdgf.v19i3.1603. Acesso em: 15 ago. 2021.

NEC. NEC Facial Recognition Helps NT Police Solve Cold Cases and Increase Public Safety in Australia. **NEC**, 1 set. 2015. Disponível em: https://www.nec.com/en/press/201509/global_20150901_02.html. Acesso em: 9 jul. 2021.

NECH, Aaron; KEMELMACHER-SHLIZERMAN, Ira. Level Playing Field for Million Scale Face Recognition. **Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)**, p. 7044-7053, 2017. Disponível em: https://openaccess.thecvf.com/content_cvpr_2017/papers/Nech_Level_Playing_Field_CVPR_2017_paper.pdf. Acesso em: 25 jul. 2021.

NOVAREJO. **Zaitt - como funciona o primeiro supermercado 100% autônomo?** [4min10seg]. 16 abr. 2019. Disponível em: https://www.youtube.com/watch?v=3sePipUMMZU. Acesso em: 10 ago. 2021.

NTECH LAB. **Face Recognition for Financial Institutions**. 2021. Disponível em: https://ntechlab.com/solution/finance/. Acesso em: 15 ago. 2021.

NUNES, Pablo. Levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros. **The Intercept Brasil**, 21 nov. 2019. Disponível em: https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/. Acesso em: 26 ago. 2021.

O'SULLIVAN, Donie. This man says he's stockpiling billions of our photos. **CNN Business**, 10 fev. 2020. Disponível em: https://edition.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html. Acesso em: 30 jun. 2021.

O'SULLIVAN, Matthew. "Your Face Will be Your Passport" Sydney Airport to Trial Biometrics. **Sidney Morning Herald**, 22 fev. 2018. Disponível em: https://www.smh.com.au/business/companies/your-face-will-be-your-passport-sydney-airport-to-trial-biometrics-20180221-p4z14p.html. Acesso em: 28 jul. 2021.

ÓPICE BLUM. **Contestação da ViaQuatro na ação civil pública com pedido de tutela de urgência do Instituto Brasileiro de Defesa do Consumidor (Idec) contra a Concessionária da Linha 4-Amarela do metrô de São Paulo (ViaQuatro)**. Processo nº 1090663-42.2018.8.26.0100. 22 out. 2018. Disponível em: https://criancaeconsumo.org.br/wp-content/uploads/2020/12/22.10.2018-Contesta%C3%A7%C3%A3o-ViaQuatro.pdf. Acesso em: 1 jul. 2021.

ORWELL, George. **1984**. ed. Especial. São Paulo: Companhia das Letras, 2019.

PASQUALE, Frank. **The Black Box Society: The Secret Algorithms That Control Money and Information**. Cambridge (Massachusetts), London: Harvard University Press, 2015.

PETRIE, Claire. Identity-matching Services Bill 2018 and Australian Passports Amendment (Identity-matching Services) Bill 2018. **Parliamentary Library information Analysis Advice. Bills Digest.**, n. 110, 2017–18, 22 mai. 2018. Disponível em: https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/bd/bd1718a/18bd110. Acesso em: 9 jul. 2021.

PEW RESEARCH CENTER. More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly. **Pew Research Center**, 5 set. 2019. Disponível em: https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2019/09/09.05.19.facial_recognition_FULLREPORT_update.pdf. Acesso em: 30 jun. 2021.

PIKOULIS, Erion-Vasilis; IOANNOU, Zafeiria-Marina; PASCHOU, Mersini; SAKKOPOULOS, Evangelos. Face Morphing, a Modern Threat to Border Security: Recent Advances and Open Challenges. **Appl. Sci.,** v. 11, p. 1-15, 2021. Disponível em: https://doi.org/10.3390/app11073207. Acesso em: 29 jul. 2021.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD)**. São Paulo: Saraiva Educação, 2018.

PIOVESAN, Eduardo; MACHADO, Ralph. Câmara aprova em 2º turno PEC que inclui a proteção de dados pessoais na Constituição. **Agência Câmara de Notícias**, 2021. Disponível em: https://www.camara.leg.br/noticias/801696-camara-aprova-em-2o-turno-pec-que-inclui-a-protecao-de-dados-pessoais-na-constituicao/. Acesso em: 2 set. 2021.

RECEITA FEDERAL, Ministério da Economia. **Coletiva - Reconhecimento Facial**. 2017a. Disponível em: https://receita.economia.gov.br/videos/coletivas/coletiva-reconhecimento-facial. Acesso em: 13 jul. 2021.

RECEITA FEDERAL, Ministério da Economia. **Entrevista - Reconhecimento Facial**. [4min8seg]. 2017b. Disponível em: https://www.youtube.com/watch?v=XPCzxr2KrQ0. Acesso em: 13 jul. 2021.

RECEITA FEDERAL, Ministério da Economia. **Sistema de Reconhecimento Facial do Projeto IRIS**. [2min38seg]. 2017c. Disponível em: https://www.youtube.com/watch?v=6eJVpxe0pxY. Acesso em: 13 jul. 2021.

RECLAIM YOUR FACE. **Evidence shows why we need a law against biometric mass surveillance**. 30 mar. 2021. Disponível em: https://reclaimyourface.eu/evidence-in-eu-countries/. Acesso em: 30 jun. 2021.

RECTOR, Kevin; KNEZEVICH, Alison. Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates. **The Baltimore Sun**, 18 oct. 2016. Disponível em: https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html.

REDAÇÃO DO MIGALHAS. Linha de metrô é condenada por instalar câmeras com captura facial. **Migalhas**, 11 mai. 2021. Disponível em: https://www.migalhas.com.br/quentes/345285/linha-de-metro-e-condenada-por-instalar-cameras-com-captura-facial. Acesso em: 1 jul. 2021.

REDAÇÃO VTEF. Bilhete Único – Fortaleza será pioneira em biometria facial. **Vale Transporte Eletrônico Fortaleza**, 22 abr. 2013. Disponível em: https://www.vtefortaleza.com.br/2013/04/22/bilhete-unico-fortaleza-sera-pioneira-em-biometria-facial/. Acesso em: 2 jul. 2021.

REDE DE OBSERVATÓRIOS DA SEGURANÇA. **O que é**. 2021. Disponível em: http://observatorioseguranca.com.br/a-rede/o-que-e/. Acesso em: 26 ago. 2021.

REID, Alana. Are Filters on Social Media Being Used to Collect your Identity? **8 Million Stories**, 6 abr. 2020. Disponível em: https://8ms.com/blog/are-filters-on-social-media-being-used-to-collect-your-identity/. Acesso em: 16 ago. 2021.

REIS, Carolina; ALMEIDA, Eduarda; SILVA, Felipe da; DOURADO, Fernando. **Relatório sobre o uso de tecnologias de reconhecimento facial e câmeras de vigilância pela administração pública no Brasil**. Brasília: Laboratório de Políticas Públicas e Internet, 2021. Disponível em: https://lapin.org.br/download/4136/. Acesso em: 8 jul. 2021.

REUTERS. Just smile: In KFC China store, diners have new way to pay. **Reuters**, 1 set. 2017. Disponível em: https://www.reuters.com/article/us-alibaba-payments-facialrecognition/just-smile-in-kfc-china-store-diners-have-new-way-to-pay-idUSKCN1BC4EL. Acesso em: 27 jul. 2021.

RICANEK, Karl; BOEHNEN, Chris. Facial Analytics: From Big Data to Law Enforcement. **IEEE Computer,** v. 45, n. 9, p. 95-97, set. 2012

RIDLEY, Doug. Facebook's New Facial Recognition Photo Tagging: How to Use (Or Not Use) **Vital**, [2017]. Disponível em: https://vtldesign.com/digital-marketing/social-media/nh-

facebook-marketing/how-to-disable-facebook-facial-recognition-photo-tagging-nhmarketing/. Acesso em: 27 jul. 2021.

RISTANI, Ergys; SOLERA, Francesco. Duke Imagelab Multi-Target, Multi-Camera Tracking Project. **AlmageLab Laboratory, Università degli Studi di Modena e Reggio Emilia**, 2017. Disponível em: https://aimagelab.ing.unimore.it/imagelab/researchActivity.asp?idActivity=044. Acesso em: 25 jul. 2021.

RISTANI, Ergys; SOLERA, Francesco; ZOU, Roger S.; CUCCHIARA, Rita; TOMASI, Carlo. Performance Measures and a Data Set for Multi-Target, Multi-Camera Tracking. **ECCV 2016 Workshop on Benchmarking Multi-Target Tracking**, 2016. Disponível em: https://arxiv.org/abs/1609.01775. Acesso em: 25 jul. 2021.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

RODRIGUES, Lino. Sigilo vazado por R$ 200: CDs com dados de aposentados e donos de carros são vendidos livremente em São Paulo. **O Globo**, 24 out. 2010. Disponível em: https://oglobo.globo.com/economia/sigilo-vazado-por-200-cds-com-dados-de-aposentados-donos-de-carros-sao-vendidos-2961335. Acesso em: 20 ago. 2021.

ROY, Sourav Dey; BHOWMIK, Mrinal Kanti; ANJAN, Priya Saha; GHOSH, Kumar. An Approach for Automatic Pain Detection through Facial Expression. **Procedia Computer Science,** v. 84, p. 99-106, 2016. Disponível em: https://doi.org/10.1016/j.procs.2016.04.072. Acesso em: 27 jul. 2021.

ROYAL COURTS OF JUSTICE RULING. **R. (Bridges) v. Chief Constable [CC] SWP and the Secretary of State for the Home Department [SSHD]**. (R (Bridges) v CCSWP and SSHD). Case No: CO/4085/2018. Neutral Citation Number: [2019] EWHC 2341 (Admin). 4 set. 2019. Disponível em: https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf. Acesso em: 5 ago. 2021.

RUARO, Regina Linden; SARLET, Gabriele Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) - Lei 13. 709/2018. In: DONEDA, D.;SARLET, I. W., *et al* (Ed.). **Tratado de Proteção de Dados**. Rio de Janeiro: Forense, 2021.

SAKAI, Juliana; BUTALLA, Vanessa; ROBERTO, Enrico; BIONI, Bruno; MARTINS, Pedro. LGPD e decisões automatizadas. [1h53min26seg]. **Data Privacy Brasil, LGPD em Movimento**, 3 dez. 2020. Disponível em: https://www.youtube.com/watch?v=SNg8N7eCU6k. Acesso em: 17 jul. 2021.

SELYUKH, Alina. NSA Staff Used Spy Tools on Spouses, Ex-lovers: Watchdog. **Reuters**, 28 set. 2013. Disponível em: https://www.reuters.com/article/us-usa-surveil-lance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927. Acesso em: 9 jul. 2021.

SHAW, Danny. Eurofins Scientific: Forensic services firm paid ransom after cyber-attack. **BBC News**, 5 jul. 2019. Disponível em: https://www.bbc.co.uk/news/uk-48881959. Acesso em: 9 jul. 2021.

SILVA, Mariah Rafaela; VARON, Joana. **Reconhecimento Facial no Setor Público e Identidades Trans: tecnopolíticas de controle e ameaça à diversidade de gênero em suas interseccionalidades de raça, classe e território**. Rio de Janeiro: Coding Rights, 2021. Disponível em: https://codingrights.org/docs/rec-facial-id-trans.pdf. Acesso em: 29 jul. 2021.

SIMÃO, Bárbara; FRAGOSO, Nathalie; ROBERTO, Enrico. **Reconhecimento Facial e o Setor Privado: Guia para a adoção de boas práticas**. São Paulo: InternetLab/IDEC, 2020. Disponível em: https://idec.org.br/sites/default/files/reconhecimento_facial_diagramacao_digital_2.pdf. Acesso em: 19 jul. 2021.

SIMONITE, Tom. When It Comes to Gorillas, Google Photos Remains Blind. **Wired**, 11 jan. 2018. Disponível em: https://www.wired.com/story/when-it-comes-to-gorillas-google-photos-remains-blind/. Acesso em: 28 jul. 2021.

SIMONITE, Tom. How Facial Recognition Is Fighting Child Sex Trafficking. **Wired**, 19 jun. 2019. Disponível em: https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/. Acesso em: 27 jul. 2021.

SITA, Société Internationale de Télécommunication Aéronautique. **Air Transport IT Insights**. 2018. Disponível em: https://www.sita.aero/globalassets/docs/surveys--reports/it-insights-2018.pdf. Acesso em: 27 jul. 2021.

SKY NEWS. **Facebook stops automatic facial recognition to tag photos**. 4 set. 2019. Disponível em: https://news.sky.com/story/facebook-allows-users-to-opt-out-of-facial-recognition-in-photos-11801900. Acesso em: 27 jul. 2021.

SMITH, John R. IBM Research Releases 'Diversity in Faces' Dataset to Advance Study of Fairness in Facial Recognition Systems. **IBM**, 15 fev. 2019. Disponível em: https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/. Acesso em: 18 ago. 2021.

SOLERA, Francesco; CALDERARA, Simone; RISTANI, Ergys; TOMASI, Carlo; CUCCHIARA, Rita Tracking social groups within and across cameras, vol. 27, pp. , 2017 | DOI: 10.1109/TCSVT.2016.2607378. **IEEE Transactions on Circuits and Systems for Video Technology,** v. 27, p. 441-453, 2017. Disponível em: https://doi.10.1109/TCSVT.2016.2607378. Acesso em: 25 jul. 2021.

SOLON, Olivia. Facial recognition's 'dirty little secret': Millions of online photos scraped without consent. **NBC Newa**, 12 mar. 2019. Disponível em: https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921. Acesso em: 28 jul. 2021.

SOPRANA, Paula; AMÂNCIO, Thiago. ViaQuatro é condenada por reconhecimento facial sem autorização no Metrô de SP **Folha de S.Paulo**, 11 mai. 2021. Disponível em: https://www1.folha.uol.com.br/cotidiano/2021/05/viaquatro-e-condenada-por-reconhecimento-facil-sem-autorizacao-no-metro-de-sp.shtml. Acesso em: 1 jul. 2021.

SP TRANS. Idosos e portadores de deficiências terão acesso mais fácil nos ônibus a partir de domingo, dia 6. **Cidade de São Paulo, Secretaria Municipal de Mobilidade e Transportes**, 30 nov. 2015. Disponível em: https://www.prefeitura.sp.gov.br/cidade/secretarias/transportes/noticias/?p=207626. Acesso em: 2 jul. 2021.

STANKOVIĆ, Miloš; NEŠIĆ, Milkica; OBRENOVIĆ, Joviša; STOJANOVIĆ, Dunja; MILOŠEVIĆ, Vuk. Recognition of facial expressions of emotions in criminal and non-criminal psychopaths: Valence-specific hypothesis. **Personality and Individual Differences,** v. 82, p. 242-247, ago. 2015. Disponível em: https://doi.org/10.1016/j.paid.2015.03.002. Acesso em: 27 jul. 2021.

STATISTA. **Size of the security services market worldwide from 2011 to 2020**. mar. 2021. Disponível em: https://www.statista.com/statistics/323113/distribution-of-the-security-services-market-worldwide/. Acesso em: 18 jul. 2021.

STEWART, Russell; ANDRILUKA, Mykhaylo; NG, Andrew Y. End-To-End People Detection in Crowded Scenes. **Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)**, p. 2325-2333, 2016. Disponível em: https://openaccess.thecvf.com/content_cvpr_2016/papers/Stewart_End-To-End_People_Detection_CVPR_2016_paper.pdf. Acesso em: 25 jul. 2021.

STF, Supremo Tribunal Federal. **PSB pede suspensão de compartilhamento de dados da CNH entre Serpro e Abin**. 18 jun. 2020. Disponível em: http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=445873&ori=1. Acesso em: 29 jul. 2021.

STF, Supremo Tribunal Federal. **OAB questiona decreto presidencial sobre compartilhamento de dados dos cidadãos**. 25 jan. 2021. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=459125&ori=1. Acesso em: 21 jul. 2021.

STOLTON, Samuel. **LEAK: Commission considers facial recognition ban in AI 'white paper'**. 17 jan. 2020. Disponível em: https://www.euractiv.com/section/digital/news/leak-commission-considers-facial-recognition-ban-in-ai-white-paper/. Acesso em: 29 jun. 2021.

STONE, Zak; ZICKLER, Todd; DARRELL, Trevor. Toward Large-Scale Face Recognition Using Social Network Context. **Proceedings of the IEEE,** v. 98, n. 8, p. 1408-1415, 2010.

STOYCHEFF, Elizabeth. Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. **Journalism & Mass Communication Quarterly,** v. 93, n. 2, p. 296-311, 8 mar. 2016.

STRUCTURE for the white paper on artificial intelligence: a European approach (draft). 2020. Disponível em: https://www.euractiv.com/wp-content/uploads/sites/2/2020/01/AI-white-paper-EURACTIV.pdf. Acesso em: 29 jun. 2021.

SURFSHARK. The facial recognition world map: smile you're on camera. **SurfShark**, 2020. Disponível em: https://surfshark.com/facial-recognition-map. Acesso em: 2 jul. 2021.

TEOFILO, Davi; KURTZ, Lahis; PORTO JR, Odílio; VIEIRA, Victor Barbieri Rodrigues. **Parecer do IRIS na Ação civil Pública IDEC vs. Via Quatro. Parecer sobre a atividade de detecção facial de usuários da Linha Quatro Amarela de metrô de São Paulo, objeto do Processo nº 1090663-42.2018.8.26.0100 da 37ª Vara Cível do Foro Central Cível da Comarca de São Paulo, ação interposta pelo Instituto Brasileiro de Defesa do Consumidor (IDEC) contra a Concessionária da linha 4 do metrô de São Paulo S.A. (ViaQuatro)**. Belo Horizonte: IRIS, 2019. Disponível em: https://irisbh.com.br/wp-content/uploads/2019/09/Acao-Civil-Publica-IDEC-vs.-ViaQuatro-Parecer-do-IRIS-1.pdf. Acesso em: 4 jul. 2021.

THALES GROUP. PARAFE: a new generation of smart gates for the ADP Group. **Thales Group**, 2018. Disponível em: https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/smart-gates-paris. Acesso em: 27 jul. 2021.

TJSP, Tribunal de Justiça de São Paulo. **Complemento à decisão de deferimento da Tutela Provisória de Urgência**. Processo nº 1090663-42.2018.8.26.0100. 27 set. 2018a. Disponível em: https://esaj.tjsp.jus.br/cpopg/abrirDocumentoVinculadoMovimentacao.do?processo.codigo=2S000WSPS0000&cdDocumento=64600509&nmRecursoAcessado=Decis%C3%A3o. Acesso em: 4 jul. 2021.

TJSP, Tribunal de Justiça de São Paulo. **Decisão de deferimento da Tutela Provisória de Urgência**. Processo nº 1090663-42.2018.8.26.0100. p. 14 set., 2018b. Disponível em: https://esaj.tjsp.jus.br/cpopg/abrirDocumentoVinculadoMovimentacao.do?processo.codigo=2S000WSPS0000&cdDocumento=64278352&nmRecursoAcessado=Concedida+a+Antecipa%C3%A7%C3%A3o+de+tutela. Acesso em: 1 jul. 2021.

TJSP, Tribunal de Justiça de São Paulo. Expediente Nº 5803. Ação Civil Pública 0017291-65.2016.403.6100 - Ministério Público Federal X Instituto Nacional do Seguro Social X Tifim Recuperadora de Créditos e Cobranças LTDA - ME. **Jusbrasil**, 28 mai. 2019. Disponível em: https://www.jusbrasil.com.br/processos/122351392/processo-n-0017291-6520164036100-do-trf-3. Acesso em: 10 ago. 2021.

TJSP, Tribunal de Justiça de São Paulo. Processo nº 1090663-42.2018.8.26.0100. Ação Civil Pública Cível - Transporte Ferroviário - Idec - Instituto Brasileiro de Defesa do Consumidor - Concessionaria da Linha 4 do Metro de Sao Paulo SA (Via Quatro) - Instituto Alana - Defensoria Publica Estado de São Paulo. O processo teve origem no Tribunal de Justiça de São Paulo, no Foro Central Cível, em 30 de agosto de 2018. **Jusbrasil**, 2021a. Disponível em: https://esaj.tjsp.jus.br/cpopg/show.do?processo.codigo=2S000WSPS0000&processo.foro=100&processo.numero=1090663-42.2018.8.26.0100&uuidCaptcha=sajcaptcha_8bac151303ea47a3842ba40e69f434f7. Acesso em: 1 jul. 2021.

TJSP, Tribunal de Justiça de São Paulo. **Sentença no Processo nº 1090663-42.2018.8.26.0100**. 7 mai. 2021b. Disponível em: https://esaj.tjsp.jus.br/cpopg/abrirDocumentoVinculadoMovimentacao.do?processo.codigo=2S000WSPS0000&cdDocumento=87156787&nmRecursoAcessado=Julgada+Procedente+em+Parte+a+A%C3%A7%C3%A3o. Acesso em: 4 jul. 2021.

TRANSPARÊNCIA BRASIL. **Recomendações de governança**: uso de inteligência artificial pelo poder público. fev. 2020. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 28 ago. 2021.

TRF3, Tribunal Regional Federal da 3ª Região. **Decisão na Ação Civil Pública (65) nº 5009507-78.2018.4.03.6100**. 9ª Vara Cível Federal de São Paulo. Autor: Ministério Público Federal - PR/SP. Réu: Microsoft Informatica Ltda e Uniao Federal. 27 abr. 2018. Disponível em: http://www.omci.org.br/m/jurisprudencias/arquivos/2018/jfsp_50095077820184036100_27042018.pdf. Acesso em: 3 jul. 2021.

TV BRASIL, Programa Brasil em dia. **Reconhecimento facial começa a ser testado nos aeroportos do país**. [1min31seg]. 15 jun. 2021. Disponível em: https://www.youtube.com/watch?v=A0LMC24adOM. Acesso em: 13 jul. 2021.

UN, United Nations (Human Rights Council). **Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests**. Report of the United Nations High Commissioner for Human Rights. Human Rights Council. Forty-fourth session, 15 June–3 July 2020. Agenda items 2 and 3. Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. 24 jun. 2020. Disponível em: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session44/Documents/A_HRC_44_24_AEV.docx. Acesso em: 17 set. 2021.

UN, United Nations (Human Rights Council). **The right to privacy in the digital age**. Report of the United Nations High Commissioner for Human Rights. Forty-eighth session, 13 September–1 October 2021. Agenda items 2 and 3. Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. A/HRC/48/31. 13 set. 2021.

UNESCO, United Nations Educational, Scientific and Cultural Organization. **Inclusion Through Access to Public Space**. 2017. Disponível em: http://www.unesco.org/new/en/social-and-human-sciences/themes/urban-development/migrants-inclusion-in-cities/good-practices/inclusion-through-access-to-public-space/. Acesso em: 10 jul. 2021.

VAN NOORDEN, Richard. The ethical questions that haunt facial-recognition research. **Nature,** v. 587, p. 354-358, 18 nov. 2020. Disponível em: https://doi.org/10.1038/d41586-020-03187-3. Acesso em: 20 jul. 2021.

VEMOU, Konstantina; HORVATH, Anna. Facial Emotion Recognition. **TechDispatch, EDPS (European Data Protection Supervisor)**, n. 1, 2021. Disponível em: file:///Users/sss/Downloads/21-05-26_techdispatch-facial-emotion-recognition_ref_en.pdf. Acesso em: 27 jul. 2021.

VENTURA, Felipe. Ônibus adotam biometria facial em todo o Brasil para evitar fraudes. **UOL, Guizmodo Brasil**, 2015. Disponível em: https://gizmodo.uol.com.br/onibus-e-biometria-facial/. Acesso em: 2 jul. 2021.

VERMA, Vinay Kumar; KANSAL, Vanika; BHATNAGAR, Pankhuri. Patient Identification using Facial Recognition. **International Conference on Futuristic Technologies in Control Systems & Renewable Energy (ICFCR)**, p. 1-7, 2020. Disponível em: https://doi/10.1109/ICFCR50903.2020.9250002. Acesso em: 27 jul. 2021.

VIAQUATRO. Passageiros Transportados. Informações sobre demanda de passageiros por estação - média dias úteis (em milhares). Relatórios disponíveis de 2010 a mai./2021. **ViaQuatro**, 2021a. Disponível em: https://www.viaquatro.com.br/linha-4-amarela/passageiros-transportados. Acesso em: 3 jul. 2021.

VIAQUATRO. **Sobre a ViaQuatro**. 2021b. Disponível em: http://www.viaquatro.com.br/a-via-quatro. Acesso em: 01 jul. 2021.

VICENTE, João Paulo. Mudanças no Bilhete Único acendem alerta sobre coleta indevida de dados. **Motherboard Tech by Vice**, 25 fev. 2019. Disponível em: https://www.vice.com/pt/article/panq7n/mudancas-no-bilhete-unico-acendem-alerta-sobre-coleta-indevida-de-dados. Acesso em: 11 jul. 2021.

VINCENT, James. NYPD used facial recognition to track down Black Lives Matter activist. **The Verge**, 18 ago. 2020. Disponível em: https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram. Acesso em: 27 jul. 2021.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.º e 11. In: DONEDA, D.;SARLET, I. W., *et al* (Ed.). **Tratado de Proteção de Dados**. Rio de Janeiro: Forense, 2021.

VITALIS, André. Le regard omniprésent de la vidéosurveillance. **Le Monde Diplomatique**, p. 26-27, mar. 1998. Disponível em: https://www.monde-diplomatique.fr/1998/03/VITALIS/3586. Acesso em: 24 jun. 2021.

WANG, Yilun; KOSINSKI, Michal. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. **Journal of Personality and Social Psychology,** v. 114, n. 2, p. 246-257, 2018. Disponível em: https://doi.org/10.1037/pspa0000098.

WERNECK, Antônio. Reconhecimento facial falha em segundo dia, e mulher inocente é confundida com criminosa já presa. **O Globo**, 11 jul. 2019. Disponível em: https://oglobo.globo.com/rio/reconhecimento-facial-falha-em-segundo-dia-mulher-inocente-confundida-com-criminosa-ja-presa-23798913. Acesso em: 26 ago. 2021.

WHITE, David; DUNN, James D.; SCHMID, Alexandra C.; KEMP, Richard I. Error Rates in Users of Automatic Face Recognition Software. **PLoS ONE,** v. 10, n. 10, p. 1-14, 2015. Disponível em: https://doi.org/10.1371/journal.pone.0139827. Acesso em: 9 jul. 2021.

WOODWARD Jr, John D; HORN, Christopher; GATUNE, Julius; THOMAS, Aryn. **Biometrics: a Look at Facial Recognition. Documented Briefing**. Santa Monica: RAND, 2003.

WP29, Article 29 Data Protection Working Party. **Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance** (adopted on 11th February 2004). 2004. Disponível em: https://www.gpdp.gov.mo/uploadfile/2014/0505/20140505071008284.pdf. Acesso em: 10 jul. 2021.

WP29, Article 29 Data Protection Working Party. **Opinion 2/2012 on facial recognition in online and mobile services** (WP192, adopted on 22 March 2012) 2012a. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf. Acesso em: 10 jul. 2021.

WP29, Article 29 Data Protection Working Party. **Opinion 3/2012 on developments in biometric technologies**. 2012b. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf. Acesso em: 30 jun. 2021.

WP29, Article 29 Data Protection Working Party. **Opinion 5/2014 on Anonymisation Techniques** (adopted on 10 April 2014) 0829/14/ENWP216. 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Acesso em: 11 jul. 2021.

WP29, Article 29 Data Protection Working Party. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679**. WP 248 rev.01. 4 out. 2017. Disponível em: https://ec.europa.eu/newsroom/just/redirection/document/47711. Acesso em: 10 ago. 2021.

WP29, Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. WP251rev.01. 6 fev. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/redirection/document/49826. Acesso em: 15 ago. 2021.

WU, Xiaolin; ZHANG, Xi. **Automated Inference on Criminality using Face Images**. 26 mai. 2017. Disponível em: https://arxiv.org/pdf/1611.04135v1.pdf. Acesso em: 28 jul. 2021.

ZARSKY, T. Transparent Predictions. **University Of Illinois Law Review,** v. 2013, n. 4, p. 1503-1570, 2013. Disponível em: https://www.illinoislawreview.org/wp-content/ilr-content/articles/2013/4/Zarsky.pdf. Acesso em: 30 ago. 2021.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power**. New York: PublicAffairs, 2019.

6.1 Leis, Projetos de Lei e Correlatos

ASSEMBLEIA LEGISLATIVA DE SÃO PAULO. **Projeto de Lei nº 12/1997**. Autoriza o Poder Executivo a firmar convênio com a Prefeitura do Município de São Paulo, para instalação de câmeras de vídeo com a finalidade de auxiliar as polícias, Civil e Militar, no combate ao

crime e à violência. Convertido na Lei nº 9.967/1998., 1997. Disponível em: https://www.al.sp.gov.br/propositura/?id=5046. Acesso em: 27 jun. 2021.

ASSEMBLEIA LEGISLATIVA DE SÃO PAULO. **Lei nº 9.967, de 07 de maio de 1998**. Autoriza o Poder Executivo a celebrar convênio na forma que especifica [Fica o Poder Executivo, através da Secretaria da Segurança Pública, autorizado a celebrar convênio com a Prefeitura do Município de São Paulo, visando à instalação, monitoramento e uso para fins de preservação da ordem pública e investigação policial, de câmeras de vídeo instaladas em pontos de grande circulação de pessoas, cruzamentos de vias públicas consideradas de alta periculosidade, estádios de futebol e outros assim considerados para as finalidades desta lei]. 1998. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/lei/1998/lei-9967-07.05.1998.html. Acesso em: 27 jun. 2021.

ASSEMBLEIA LEGISLATIVA DE SÃO PAULO. **Lei nº 10.294, de 20 de abril de 1999**. (Atualizada até o julgamento do Recurso Extraordinário pelo STF). Dispõe sobre a proteção e defesa do usuário do serviço público do Estado. 2015. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/lei/1999/lei-10294-20.04.1999.html. Acesso em: 18 jul. 2021.

BRASIL. **Lei nº 7.102, de 20 de junho de 1983**. Dispõe sobre segurança para estabelecimentos financeiros, estabelece normas para constituição e funcionamento das empresas particulares que exploram serviços de vigilância e de transporte de valores, e dá outras providências. 1983. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L7102compilado.htm. Acesso em: 27 jun. 2021.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Código Civil (CC). 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 21 ago. 2021.

BRASIL. **EM nº 084/2004 - MP**. Apresentar proposta de Medida Provisória (MPv nº 184, de 2004) que abre ao Orçamento Fiscal da União (Lei nº 10.837, de 16 de janeiro de 2004), em favor dos Ministérios da Justiça, dos Transportes e da Defesa, crédito extraordinário no valor global de R$ 100.000.000,00 (cem milhões de reais). 5 mai. 2004a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2004/Exm/EM-084-MP-04.htm. Acesso em: 21 ago. 2021.

BRASIL. **Lei nº 10.935, de 12 de agosto de 2004**. Abre crédito extraordinário aos Orçamentos Fiscal e de Investimento da União, em favor dos Ministérios da Justiça, dos Transportes e da Defesa, para os fins que especifica., 2004b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/L10.935.htm. Acesso em: 18 jul. 2021.

BRASIL. **Lei nº 12.414, de 9 de junho de 2011** (Lei do Cadatro Positivo). Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito., 2011. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 19 ago. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). 2014. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 jul. 2021.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor (CDC). Dispõe sobre a proteção do consumidor e dá outras providências., 2017. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 21 ago. 2021.

BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados". 2019a. Disponível em: www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 4 jul. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). 2019b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 jun. 2021.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. (Conversão da Medida Provisória nº 869, de 2018). 2019c. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 22 jun. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. 2020a. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm. Acesso em: 21 ago. 2021.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação (LAI).Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências., 2021b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 21 ago. 2021.

BRASIL. **Lei nº 13.460, de 26 de junho de 2017**. Código de Defesa dos Direitos do Usuário dos Serviços Públicos. Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública., 2021c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm. Acesso em: 21 ago. 2021.

BRASIL, Presidência da República. **Mensagem nº 288, de 8 de julho de 2019**. Comunica veto parcial ao Projeto de Lei de Conversão nº 7, de 2019 (MP nº 869/2018), que "Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências". 2019d. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm. Acesso em: 22 jun. 2021.

CÂMARA DOS DEPUTADOS. **Ficha de tramitação da Proposta de Emenda à Constituição nº 17/2019**. "Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais". 2021a. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 2 set. 2021.

CÂMARA DOS DEPUTADOS. **Proposta de Emenda à Constituição nº 17/2019**. "Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais". 2021b. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01bntm80gpb1sz1why3y1k27ok04099321.node0?codteor=2067091&filename=Tramitacao-PEC+17/2019. Acesso em: 2 set. 2021.

CÂMARA DOS DEPUTADOS. **Ato do Presidente da Câmara dos Deputados, de 26 de novembro de 2019**. Institui Comissão de Juristas destinada a elaborar anteprojeto de legislação específica para o tratamento de dados pessoais no âmbito de segurança pública, investigações penais e repressão de infrações penais, conforme o disposto no artigo 4°, inciso III, alíneas "a" e "d" da Lei n. 13.709, de 14 de agosto de 2018., 26 nov. 2021. Disponível em: https://www2.camara.leg.br/legin/int/atoprt_sn/2019/atodopresidente-58133-26-novembro-2019-789470-publicacaooriginal-159494-cd-presi.html. Acesso em: 21 jun. 2021.

PARLAMENTO EUROPEU; CONSELHO EUROPEU. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE** (Regulamento Geral sobre a Proteção de Dados, RGPD, ou General Data Protection Regulation, GDPR). **EUR-Lex, Access to European Union Law**, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 10 jul. 2021.

SENADO FEDERAL. **Projeto de Lei do Senado nº 168/2005**. Dispõe sobre o sistema de segurança privada, estabelece normas para constituição e funcionamento das empresas privadas que exploram os serviços de segurança, e dá outras providências. Autor: Senador Tasso Jereissati (PSDB/CE). Arquivada ao final da 55ª Legislatura., 2005. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=2988035&ts=1594038401103&disposition=inline. Acesso em: 27 jun. 2021.

STATE OF CALIFORNIA. **Assembly Bill No. 1215, Ting**. Law enforcement: facial recognition and other biometric surveillance. An act to add and repeal Section 832.19 of the State of California Penal Code, relating to law enforcement [Approved by Governor October 08, 2019. Filed with Secretary of State October 08, 2019.]. 8 out. 2019. Disponível em: https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB1215. Acesso em: 2 ago. 2021.

7. ARTIGOS PRODUZIDOS AO LONGO DO CURSO DE BACHARELADO EM DIREITO NA UNIVERSIDADE DE BRASÍLIA

Este apartado é composto pelos artigos produzido e publicados ao longo do curso de Bacharelado em Direito na Universidade de Brasília (UnB), representando o percurso da autora desta Monografia como acadêmica de Direito. Os artigos foram elaborados no âmbito de disciplinas cursada no período de graduação, submetidos e aceitos para publicação em periódicos e/ou livros na área do Direito.

O artigo "*Facial Recognition, Law Enforcement and the Identity-Australian Matching Services (IMS) Bill*", trata de temática relacionada à proteção de dados, resultado dos estudos procedidos na disciplina *Information Law*, durante intercâmbio acadêmico na *Australian National University* (ANU). Ele foi o embrião da presente Monografia de final de curso. À exceção dele, e do artigo "*Revisão de decisão tomada com base em tratamento automatizado*", escrito especialmente para integrar o Primeiro Anuário do Observatório da LGPD-UnB, os demais artigos constantes deste apartado não tratam da temática da Monografia, entretanto, são aqui trazidos com objetivo duplo:

1. Manter o registro, em um único local, da produção na temática de Direito, elaborada ao longo do percurso acadêmico de graduação (registro de uma jornada).
2. Disponibilizar, divulgar e publicizar, para uso acadêmico, tais textos, pois nem todos estão facilmente acessíveis/disponíveis para consulta.

A monografia não está dissociada desse caminho percorrido, antes disso, é um epílogo dessa etapa da graduação, da qual cada um dos artigos aqui apresentados, representa um marco (*milestone*).

Segue a listagem dos artigos (associados ao nome da disciplina para a qual foram originalmente escritos) em ordem de data de publicação:

1) Teoria Geral do Estado (UnB): SCHLOTTFELDT, Shana; COSTA, Alexandre A. Em busca do poder: a evolução da participação política da mulher na Câmara dos Deputados brasileira. *Revista Eletrônica do Programa de Pós-Graduação da Câmara dos Deputados (E-Legis)*, v. 9, 2016, p. 100-126. Disponível em: https://doi.org/10.51206/e-legis.v9i21.276. ISSN 2175-0688.
2) Direito Penal 1 (UnB): SCHLOTTFELDT, Shana. Femicídio, feminicídio e o entendimento dos operadores do Direito brasileiro ao tratar a morte de mulheres em razão do gênero. *Boletim IBCCRIM*, v. 291, 2017, p. 9-11. Disponível em: https://www.ibccrim.org.br/noticias/exibir/6628/. ISSN 1676-3661.
3) Teoria Geral do Direito Penal (UnB): SCHLOTTFELDT, Shana; ROCHA, Fernanda: ROCHA, Luana. Crimes sexuais e violência de gênero contra mulheres na ditadura militar no Brasil. In: TEIXEIRA, Érica Fernandes *et al*. (Org.). *Direitos Sociais*: reflexões e desdobramentos. 1. ed. Curitiba: Appris, 2019, p. 307-325. ISBN 978-85-473-2972-3
4) Information Law (ANU): SCHLOTTFELDT, Shana. Facial Recognition, Law Enforcement and the Identity-Australian Matching Services (IMS) Bill. *Revista dos Estudantes de Direito da Universidade de Brasília*, v. 1, p. 343-357, 2020.

Disponível em: https://periodicos.unb.br/index.php/redunb/article/view/30375/27955. ISSN impresso: 1981-9684 / ISSN eletrônico: 2177-6458.

5) Direito Econômico/Direito Administrativo 3 (UnB): SCHLOTTFELDT, Shana. Autorregulação e corregulação: duas ferramentas no canivete do regulador. *Revista Consultor Jurídico (ConJur)*. 11 jun. 2021. Disponível em: https://www.conjur.com.br/2021-jun-11/opiniao-autorregulacao-corregulacao-ferramentas-canivete-regulador. ISSN 1809-2829.
6) Direito Processual Penal 2 (UnB): FONSECA, Reynaldo Soares da; SCHLOTTFELDT, Shana. A (Ir)Retroatividade da Alteração da Natureza da Ação Penal no Crime de Estelionato pela Lei Anticrime: como ficam as ações penais em curso? *Revista Magister de Direito Penal e Processual Penal*. v. 102, jun./jul. 2021, p. 26-42. ISSN 1807-3395.
7) Direito do Trabalho (UnB): SCHLOTTFELDT, Shana; BARROS, Elaine Sampaio. Breve panorama da trajetória histórica do reconhecimento dos direitos das empregadas domésticas no Brasil. In: TEIXEIRA, Érica Fernandes, *et al*. (Org.). *Direitos Sociais*: reflexões e desdobramentos. v. 2. 1. ed. Curitiba: Appris, 2021. Aceito em jun. 2020. No prelo.
8) Direito Internacional Público (UnB): SCHLOTTFELDT, Shana; RESENDE, Otávio Henrique Mayrink. Violência sexual contra mulheres: a incorporação da perspectiva de gênero no Direito Internacional Público. *Revista Eletrônica do Programa de Pós-Graduação da Câmara dos Deputados (E-Legis)*. ISSN 2175-0688. Aceito em mai. 2021. No prelo. Previsão de publicação no v. 15, n. 37, jan./abr. 2022.
9) Anuário do Observatório da LGPD (UnB): SCHLOTTFELDT, Shana. *Revisão de decisão tomada com base em tratamento automatizado*. Selecionada em jun. 2021 para compor o Primeiro Anuário da LGPD-UnB.

Por fim, relaciona-se a seguir, artigos que foram submetidos para publicação e aguardam avaliação:

10) Direito Coletivo do Trabalho (UnB): SCHLOTTFELDT, Shana; DUTRA, Renata Queiroz. *A greve dos servidores públicos civis em face das reformas de austeridade*: um direito constitucional em disputa. Em avaliação.
11) Direito Administrativo 2 (UnB): SCHLOTTFELDT, Shana. *Acordo de leniência e o Acordo de Cooperação Técnica de ago./2020*: porque o Ministério Público não é (e não deveria ser) signatário. Em avaliação.

ANEXO 1 - Em busca do poder: a evolução da participação política da mulher na Câmara dos Deputados brasileira

Teoria Geral do Estado (UnB): SCHLOTTFELDT, Shana; COSTA, Alexandre A. Em busca do poder: a evolução da participação política da mulher na Câmara dos Deputados brasileira. *Revista Eletrônica do Programa de Pós-Graduação da Câmara dos Deputados (E-Legis)*, v. 9, 2016, p. 100-126. Disponível em: https://doi.org/10.51206/e-legis.v9i21.276. ISSN 2175-0688.

EM BUSCA DO PODER: A EVOLUÇÃO DA PARTICIPAÇÃO POLÍTICA DA MULHER NA CÂMARA DOS DEPUTADOS BRASILEIRA

SEEKING THE POWER: THE EVOLUTION OF WOMEN'S POLITICAL PARTICIPATION IN THE BRAZILIAN CHAMBER OF DEPUTIES

Shana Schlottfeldt
Alexandre Araújo Costa*

Resumo: O presente estudo analisa a evolução da participação política da mulher na Câmara dos Deputados brasileira para corroborar o diagnóstico de sub-representação feminina nas esferas de poder e decisão. A metodologia empregada utilizou levantamento bibliográfico e de informações junto a bancos de dados nacionais e internacionais. Os resultados apontam que a democracia no Brasil, desde os seus primórdios, foi excludente, limitando a participação das brasileiras por meio de vários artifícios. Constatou-se também que a adoção da política de cotas não conseguiu alterar esse quadro: houve aumento nas candidaturas, mas não se notam impactos na evolução do percentual de eleitas.

Palavras-chaves: Mulher; Gênero; Política; Democracia; Câmara dos Deputados.

Abstract: We studied the evolution of women's political participation in the Brazilian Chamber of Deputies as a way to put in evidence the women's under-representation in decision-making spheres. Methodology included literature research and analysis of data from national and international databases. Results showed that democracy in Brazil, since its beginning, was exclusionary, limiting the participation of women. We also found that the quota policy was unable to change this situation: there was an increase in candidacy, but we did not notice impacts on the percentage of elected women.

Keywords: Women; Gender; Politics; Democracy; Chamber of Deputies.

* Shana Schlottfeldt é Analista Legislativo da Câmara dos Deputados. Doutora em Informática pela Universidade de Brasília, Mestre em Informática pela Universidade Carlos III de Madrid (shana.santos@camara.leg.br). Alexandre Araújo Costa é Professor da Faculdade de Direito da Universidade de Brasília. Doutor em Direito, Estado e Constituição, Mestre e Graduado em Direito pela Universidade de Brasília (alexandrearcos@unb.br).

1 Introdução

Nas eleições de 2014, as mulheres, que formaram 52,13% do eleitorado nacional, participaram com apenas 29,38% das candidaturas à Câmara dos Deputados[1] e contaram com apenas 51 deputadas eleitas para a Legislatura 2015-2019, ou seja, 9,94% do total de parlamentares (TRIBUNAL SUPERIOR ELEITORAL, 2014, 2015).

Os números citados indicam que, no Brasil, a extensão às mulheres do direito de votar e ser votada não alterou significativamente a composição de gênero do Parlamento nas legislaturas subsequentes, que continuou a ser predominantemente masculina. Por isso, o resultado prático da conquista do voto feminino deve ser interpretado criticamente, pois, no que diz respeito à presença feminina nos espaços de representação política e de poder, as mudanças foram muito pequenas quando o que está em análise é a equidade entre os gêneros.

A relevância do tema é evidente: a exclusão de grupos das esferas decisórias do poder não é compatível com a democracia. Além de dar visibilidade ao fato da sub-representação feminina, o debate ora proposto é importante para fornecer subsídios ao aprimoramento das estratégias na busca da igualdade de fato entre homens e mulheres no que diz respeito à representação política.

O escopo deste trabalho é a participação política feminina na Câmara dos Deputados brasileira, de sorte que, na maioria das vezes, os dados farão referência à participação de parlamentares mulheres naquela Casa, ainda que em alguns momentos se faça alusão a dados relativos ao Senado ou mesmo a outras esferas do poder, além da Legislativa.

Ressalte-se que a expressão "participação política", neste estudo, se refere à participação formal, ou seja, ao sufrágio – o direito de eleger e ser eleito.

Na realização deste trabalho, foram utilizados métodos de sistematização de dados, bem como de revisão bibliográfica. Trata-se de uma pesquisa exploratória e descritiva. Fez-se um levantamento bibliográfico da literatura especializada e levantamento de dados junto a bancos de dados nacionais e internacionais, sobretudo dados brutos sobre eleições, disponíveis no site do Tribunal Superior Eleitoral (TRIBUNAL SUPERIOR ELEITORAL, 2015) e dados da União Interparlamentar (INTER-PARLIAMENTARY UNION, 2015a).

Este trabalho foi estruturado em cinco seções, incluindo esta Introdução e a Conclusão. A Seção 2 apresenta a dicotomia entre espaço público e privado, bem como seu reflexo na desigualdade de representação das mulheres nos espaços de decisão e poder. A Seção 3 traça um breve panorama histórico dos direitos políticos das mulheres brasileiras e da trajetória política feminina nas esferas formais de participação. As Seções 2 e 3 fornecem os subsídios para a Seção 4, em que é feita a exposição da situação atual da participação política da mulher na Câmara dos Deputados brasileira, abordando aspectos tais como a participação nos partidos

[1] Consideradas apenas as candidaturas com situação DEFERIDA (5.864). Não foram computadas candidaturas com situação CANCELADA (14), FALECIDA (3), INDEFERIDA (864), NÃO CONHECIDA (24), RENÚCIA (371).

políticos, as cotas de gênero, as propostas para o aumento da participação das mulheres nos espaços de poder, além do questionamento quanto à correlação entre maior presença no espaço político e a efetiva representação dos interesses da mulher.

2 Dicotomia entre espaço público e privado: raízes da desigualdade de representação entre homens e mulheres nos espaços de decisão e poder

A palavra cidadania (do latim *civitas*, cidade) corresponde ao complexo de direitos e deveres a que o indivíduo está sujeito em relação à sociedade em que vive. Seu conceito surgiu na Grécia Antiga onde era utilizada para expressar o conjunto de direitos do cidadão junto à comunidade dentro da *polis*, cidade grega. A cidadania era entendida como o atributo do indivíduo que pertencia a uma comunidade, com todas as consequências resultantes da convivência em grupo (SOW, 2010). Entretanto, do conceito de cidadania estavam excluídos *mulheres*, escravos, estrangeiros, crianças e cidadãos privados de direitos políticos (MENEZES, 2010). De fato, pode-se afirmar que desde a *polis* grega e a *civitas* romana (e até mesmo antes disso), a história dos espaços de decisão e poder tem sido contada com a exclusão da mulher.

No que tange às identidades femininas, a história mostra que elas têm sido formadas em oposição às identidades masculinas, de maneira que o gênero tem sido um princípio ordenador e normatizador das práticas sociais (COUTO, SCHRAIBER, 2013; ABRÃO, 2009).

Dussel (1993) nos mostra a imposição, desde o descobrimento do novo continente, da sexualidade puramente masculina, opressora, alienante, injusta que coloniza a sexualidade índia, instaurando a moral dupla do machismo: dominação sexual da índia e respeito puramente aparente pela mulher europeia.

Ao homem sempre foi franqueado o acesso ao espaço público e à mulher, por sua vez, atribuído o espaço privado, nos limites da família e do lar, no que se caracteriza pela formação de dois mundos: "um de dominação, produtor (mundo externo) e o outro de submissão e reprodutor (mundo interno)" (RITT; RITT, 2014).

Essa distribuição de papéis sociais entre os gêneros reforça conceitos que contemplam o homem como o ser portador da cultura/mente/razão e a mulher como portadora da natureza/corpo/emoção (SEIDLER, 1987).

A partir desses espaços (público *versus* privado), é possível perceber como são sutis as distinções entre o permitido e o negado, fazendo com que as mulheres encontrem resistência em transpor a barreira invisível que as exclui de participar da vida pública (FERREIRA, 2004b).

A aceitação e a vivência em si dos papéis e das normatizações desiguais entre os gêneros, como se naturais fossem, reforça a violência simbólica (BOURDIEU, 2005). As normas sociais que regem a convivência entre homens e mulheres contêm violência e a simples obediência a tais regras é uma forma de violência simbólica.

Ainda que a dicotomia entre espaço público e privado esteja esvanecendo, tendo como

marco a organização dos sujeitos historicamente excluídos (negros, mulheres, indígenas), a maneira como estes sujeitos foram privados do trânsito em espaços pensados pelos e para os homens (brancos) ainda faz parte das construções sociais (FERREIRA, 2004b).

Conforme pontua Perrot (1997), há setores – o religioso, o militar e o político, por exemplo – que, como as três ordens da Idade Média, permanecem verdadeiros "santuários que fogem às mulheres", baluartes da dominação masculina, espaços quase inacessíveis às mulheres tamanha a resistência em integrá-las.

Historicamente, o campo político pressupõe o desenvolvimento de competências específicas dos partícipes, a separação entre profissionais e profanos, entre incluídos e excluídos do jogo do poder (BOURDIEU, 2000). Sendo assim, deve-se pensar nas condições sociais de acesso ao campo político, sopesando: (1) a divisão social do trabalho entre os sexos; (2) as condições de acesso à educação; e (3) o tempo livre necessário para se ocupar de política e para falar de política.

Cada ampliação (ou retrocesso) dos direitos políticos aumenta (ou diminui) a definição institucional de um determinado governo, movendo literalmente as fronteiras da sociedade para frente (ou para trás). A ideia de uma entidade política ou mesmo de um espaço social incorporado, é modificada toda vez que um grupo é admitido a novos direitos e procedimentos participatórios (DOUZINAS, 2009).

Pela determinação de lugares reservados aos homens e vedados às mulheres, são criadas formas de exclusão que se institucionalizam e se refletem na "desigualdade de representação legislativa e em praticamente todos os espaços de decisão e poder que vão do Judiciário ao Executivo, das direções sindicais e partidárias aos cargos nas universidades" (FERREIRA, 2004b, p. 3).

Nas áreas da política e do poder, têm-se com maior veemência a expressão do processo de exclusão da mulher. Historicamente observa-se uma sub-representação feminina, que orbitou entre a ausência total de representação e os resultados atuais, o que situa o Brasil no grupo de países com pior desempenho relativo à presença das mulheres nas esferas de poder, e.g., na Câmara dos Deputados elas são menos de 10%.

Em que pesem os baixos níveis de participação feminina no Congresso Nacional, essa presença representa uma conquista da democracia recente (PINHEIRO, 2007) e tem gerado, sobretudo a partir da década de 1990, cada vez mais estudos, diagnósticos e pesquisas que se dedicam a analisar a questão e a fornecer elementos para a atuação do Estado.

Segundo Pinheiro (2007, p. 31), o interesse no tema pode ser atribuído a dois motivos correlatos: (1) o contraste entre o grau de inserção feminina em esferas da vida social – como na educação e no mercado de trabalho – e a sua exígua presença em instâncias – formais ou informais – de exercício do poder; (2) o surgimento, em todo o mundo, mas em especial na América Latina, de ações afirmativas no campo político, com destaque para o surgimento das

cotas para a candidatura de mulheres.

3 Panorama histórico dos direitos políticos das mulheres brasileiras: evolução do eleitorado brasileiro e da participação política feminina

Entre princípios dos séculos XIX e XX, as alterações sociais, culturais, políticas e econômicas que repercutiram no interior das famílias e redundaram nos movimentos organizados femininos ocorreram de maneira mais ou menos homogênea e concertada cronologicamente. Quanto aos níveis de atividade laboral, o histórico das mulheres até a atualidade segue uma evolução similar entre os países. Entrementes, quando se fala em participação política, principalmente a partir das primeiras décadas do século XX, é possível observar de maneira clara cisões no desenvolvimento histórico feminino (CAMPOS; PASCUAL, 2010).

Entre 1500 e 1932 as mulheres brasileiras estavam formalmente excluídas da política institucional. O movimento sufragista feminino, iniciado no Brasil em 1919 – com as *suffragettes* brasileiras, que mantinham ligações com as líderes do movimento internacional –, resultou na conquista do direito ao voto pelas mulheres em 1932[2], inaugurando a história da participação feminina no Parlamento brasileiro[3] (FERREIRA, 2004a).

Entretanto, num primeiro momento, apenas mulheres casadas, com autorização de seus maridos, ou mulheres viúvas e solteiras com renda própria podiam votar (SOARES, 2013, p. 347).

O que efetivamente se observou foi que, durante 33 anos (de 1932 a 1965), diferentes versões do Código Eleitoral estabeleceram regras consideradas adequadas à participação das mulheres, colocadas em posição de dependência, com escassas possibilidades de acumular capital social, cultural e político (VOGEL, 2012), e.g., até 1965, quando foi promulgado o Código Eleitoral vigente (Lei nº 4.737/1965) , o voto feminino só era obrigatório para as mulheres que exerciam "profissão lucrativa" ou "função pública remunerada" (SOW, 2010, p. 85).

A manifestação do indivíduo no sentido de reconhecer-se como habilitado a envolver-se nas questões políticas, a expressar opinião a respeito delas e a modificar o seu curso, passa pela relação entre: (1) a posição ocupada na estrutura social e na divisão do trabalho; e (2) o capital cultural e social de que dispõe. Assim, ao facultar o voto às mulheres que não exerciam "profissão lucrativa" ou "função pública remunerada" ao mesmo tempo em que o obrigava a todos os homens maiores de 21 anos (independentemente da posição ocupada na estrutura

[2] Na década de 1880, cerca de 50 anos antes da conquista do direito de voto pelas mulheres, baseando-se no Decreto nº 3.029/1881 (Lei Saraiva), que garantia o direito de voto aos portadores de títulos científicos, a dentista Isabel de Mattos Dillon, requereu e conquistou, em segunda instância, seu alistamento eleitoral e o reconhecimento de seu direito de votar (AZEVEDO; RABAT, 2012).

[3] Para a Assembleia Constituinte de 1933, Carlota Pereira de Queirós foi eleita a primeira deputada federal do Brasil, tornando-se também a primeira deputada eleita na América Latina.

social), a legislação eleitoral absorvia a representação dominante a respeito das mulheres, de que não se deveria exigir seu comprometimento com questões públicas coletivas (ainda que tais questões afetassem indistintamente a vida de homens e mulheres), uma vez que sua esfera de atuação estava ligada ao mundo privado, ao lar (VOGEL, 2012).

Assim, no decorrer do século XX, até a década de 1970, o quadro de exclusão não sofreu muitas modificações. A presença feminina no Parlamento federal ocorreu em ocasiões esporádicas, em que algumas poucas mulheres conseguiram converter capital cultural ou social em capital político.

Em finais da década de 1980, a situação começou a modificar-se como reflexo do crescimento industrial – que colaborou para um aumento expressivo da participação feminina no mercado de trabalho, com impacto sobre as relações sociais –, bem como da ampliação da escolarização e da crescente inserção das mulheres no ensino superior. Destacam-se também o surgimento de novos tipos de famílias e a ruptura dos padrões familiares patriarcais (AVELAR, 2001). Some-se a este contexto o processo de redemocratização do país. Todos estes fatores contribuíram para ampliar a participação da mulher nas esferas de poder, incentivando-as a organizarem-se politicamente (FERREIRA, 2004a).

As mulheres, ao emergirem da esfera privada para reivindicarem na esfera pública, tornam-se visíveis, também, na esfera social (SOARES, 2013), neste sentido, o período Constituinte de 1988 foi fundamental para que as mulheres, a partir de sua atuação, conquistassem direitos legais e obtivessem legitimidade para suas demandas, inclusive na esfera da política institucional. Nesse período, estima-se que as mulheres conseguiram que 80% de suas reivindicações fossem incorporadas ao texto constitucional (AVELAR, 2013) e foram criados os Conselhos Nacional, Estaduais e Municipais da Condição Feminina, as delegacias da mulher e os coletivos de mulheres nos partidos e sindicatos (FERREIRA, 2004a). Entretanto, em termos de representação no Legislativo, à época com apenas 5,3% do total de deputadas, aquela instância de representação e reconhecimento político não determinou um equilíbrio entre homens e mulheres.

Paralelamente, cada uma das conferências – Conferência Mundial de Mulheres no México, em 1975; Convenção sobre Eliminação de Todas as Formas de Discriminação contra a Mulher (CEDAW) em 1979; conferências de Copenhague, em 1980, de Nairóbi, em 1982, de Viena, em 1993, de Belém do Pará, em 1994; Conferência sobre População do Cairo, em 1994; de Pequim, em 1995; Conferência contra o Racismo, em 2001 –, demarcou uma ação política que contribuiu para fortalecer as articulações dos movimentos de mulheres nas diversas instâncias do poder no país e a discussão de propostas de ampliação dos direitos da mulher, entre os quais os direitos políticos. Toda essa movimentação forneceu elementos para se pensar medidas de inclusão das mulheres nos espaços decisórios, culminando com a Lei das Cotas (FERREIRA, 2004b).

Analisando-se a evolução do eleitorado brasileiro, desde a República Velha (1889-1930)[4] até a Segunda Guerra Mundial, o percentual de eleitores no Brasil não ultrapassou os 5% da população. Em 1945, com o primeiro processo de redemocratização (pós-Estado Novo), o eleitorado brasileiro chegou a 7,4 milhões de eleitores, o que correspondia, à época, a 16,13% da população (VOGEL, 2012). Com o processo de redemocratização pós-ditadura militar, houve um salto nos números absoluto e relativo de votantes, sendo que, pela primeira vez, as pessoas aptas a votar ultrapassaram 50% da população. Estes números cresceram de maneira contínua e o eleitorado brasileiro, atualmente de 142.822.046 de eleitores, corresponde a 71,04% de uma população de 201.032.714 de habitantes (TRIBUNAL SUPERIOR ELEITORAL, 2014).

Em termos da evolução percentual do eleitorado feminino, tomando-se dados a partir da redemocratização (1988), observa-se que nas últimas eleições do século XX as mulheres foram chegando perto da paridade. A partir do ano 2000, gradualmente ampliaram a presença, aumentando seu percentual em relação ao sexo masculino (Figura 1). Segundo dados do Tribunal Superior Eleitoral (TRIBUNAL SUPERIOR ELEITORAL, 2014), nas eleições de 2014, as mulheres brasileiras formaram 52,13% do eleitorado nacional.

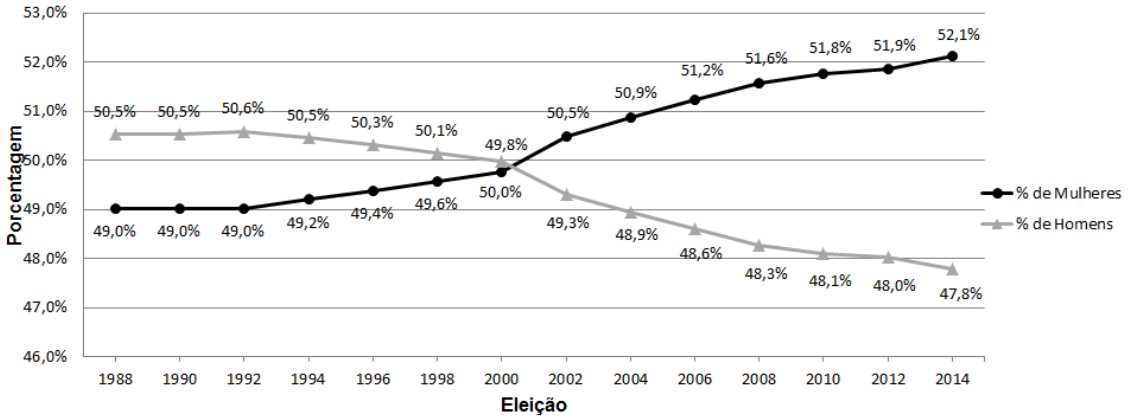


Figura 1 - Evolução do eleitorado brasileiro por sexo de 1988 a 2014.
Fonte: Tribunal Superior Eleitoral (2015).

No entanto, quando se observam as estatísticas referentes à presença e participação das mulheres nos espaços de atuação político-partidária, constata-se que as mesmas encontram-se sub-representadas (SOARES, 2013). O Brasil ainda vivencia a desigualdade de gênero, a qual se reflete fortemente na política.

Entre 1932 e 1963, apenas quatro mulheres obtiveram assento na Câmara dos Deputados[5], num total de sete mandatos, sendo que nas eleições de 1945 nenhuma mulher foi eleita. Até 1982, praticamente uma ou duas mulheres se revezavam na Câmara dos Deputados.

[4] Nesse período, considerados apenas os homens, dado que as mulheres ainda não tinham direito ao voto.
[5] Carlota de Queirós - PC/SP (dois mandatos); Bertha Lutz (um mandato), Ivette Vargas - PTB/SP (três mandatos) e Nita Costa - PTB/BA (um mandato) (CÂMARA DOS DEPUTADOS, 2015).

A representação feminina na Câmara Federal ficou abaixo de 2% até 1986. Na eleição para a Assembleia Constituinte de 1988, foram eleitas 26 mulheres (5,34% do total de deputados). Este quantitativo permaneceu praticamente estável até 2002, quando o número de mulheres eleitas chegou a 42 (8,19%). Em 2006, alcançou o número de 45 deputadas eleitas (8,77%), voltou a cair em 2010 para 44 deputadas (8,60%), e atingiu, por fim, em 2014, o pico de 51 deputadas (9,94%) (TRIBUNAL SUPERIOR ELEITORAL, 2015).

Cabe destacar que as candidatas eleitas foram aquelas capazes de converter em votos o capital (cultural, social ou político) acumulados em suas áreas de atuação:

> [...] diplomadas em cursos superiores, parentes de políticos influentes, dirigentes de instituições que prestam assistência social à população excluída, jornalistas ou apresentadoras de programas de rádio ou TV, defensoras das liberdades democráticas ou da representação política de seus maridos com direitos políticos cassados pela ditadura militar, essas raras mulheres bem sucedidas eleitoralmente (...) souberam vencer os preconceitos e se utilizar do tipo de capital de que dispunham para adentrar no terreno predominantemente masculino e elitista que caracteriza a política brasileira (VOGUEL, 2012, p. 27).

Em que pese o grande avanço ocorrido nos últimos 30 anos, a participação feminina na Câmara Federal ainda é muito baixa (Figura 2). É importante destacar que somente em 1990 foi eleita a primeira senadora; em 1994, a primeira governadora; em 2010, a primeira presidente do Brasil; e em 2011, a primeira mulher titular de um cargo na Mesa Diretora da Câmara dos Deputados, a Deputada Rose de Freitas, 1ª Vice-Presidente. Atualmente, a Mesa Diretora da Câmara, eleita para o período de 2015-2017 conta também com apenas uma mulher, a Deputada Mara Gabrilli, 3ª Secretária. Dessa forma, as mulheres brasileiras continuam sub-representadas em todos os níveis do poder político.

Com base nos dados apresentados é perfeitamente legítimo falar-se na existência de um verdadeiro déficit democrático na história de participação da mulher na política brasileira.

Além da baixa representação, aquelas parlamentares que conseguem vencer as barreiras iniciais para entrada no Parlamento sofrem com uma série de limitações no desempenho pleno de seus mandatos: desde as oriundas da pouca experiência para disputar, se impor e se manter nos espaços de poder até as manifestações sexistas e discriminatórias de muitos de seus pares (PINHEIRO, 2007).

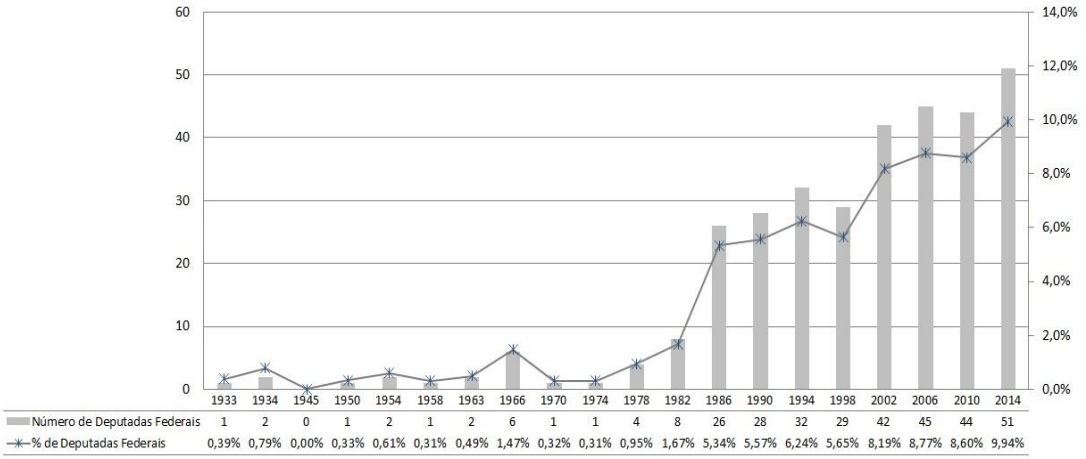


Figura 2 - Número absoluto e porcentagem de mulheres deputadas federais eleitas no Brasil no período de 1933-2014
Fonte: Azevedo; Rabat (2012), Câmara dos Deputados (2015) e Tribunal Superior Eleitoral (2015).

Em termos da implantação de mecanismos institucionais especiais de promoção da igualdade de gênero, destacam-se algumas iniciativas como a criação, no âmbito do Poder Executivo Federal, da Secretaria Especial de Políticas para as Mulheres (Lei nº 10.683/2003), atualmente Secretaria de Políticas para as Mulheres (SPM) (Lei nº 12.314/2010) a quem compete assessorar direta e imediatamente o Presidente da República na formulação, coordenação e articulação de políticas para as mulheres; elaborar e implementar campanhas educativas e antidiscriminatórias de caráter nacional; elaborar o planejamento de gênero que contribua na ação do governo federal e demais esferas de governo com vistas à promoção da igualdade; articular, promover e executar programas de cooperação com organismos nacionais e internacionais, públicos e privados, voltados à implementação de políticas para as mulheres; promover o acompanhamento da implementação de legislação de ação afirmativa e definição de ações públicas que visem ao cumprimento dos acordos, convenções e planos de ação assinados pelo Brasil, nos aspectos relativos à igualdade entre mulheres e homens e de combate à discriminação.

Sobre a afirmação dos direitos e das políticas para as mulheres, cabe destacar a lei que estabeleceu 2004 como o Ano da Mulher no Brasil (Lei nº 10.745/2003). Nesse mesmo ano, foi desencadeado o processo de instalação da 1ª Conferência de Políticas Públicas para Mulheres (CENTRO FEMINISTA DE ESTUDOS E ASSESSORIA, 2006). A partir dessa iniciativa, a SPM apresentou o Plano Nacional de Políticas para Mulheres (PNPM), em fins de 2004, destacando objetivos, metas, prioridades e plano de ação nas áreas de trabalho e cidadania; educação; saúde, direitos sexuais e direitos reprodutivos; violência contra as mulheres; e gestão e monitoramento do próprio PNPM (BRASIL, 2004).

No que respeita à participação política feminina, a constituição do Fórum Nacional de Instâncias de Mulheres de Partidos Políticos, em 2006, foi outro passo importante, possibilitando a discussão política sobre assuntos de comum interesse na atuação pluripartidária

e suprapartidária, sobretudo no que diz respeito à temática de gênero nos partidos políticos, com a finalidade de debater a participação, as limitações e os desafios para a transformação da sub-representação das mulheres (MATOS; CORTÊS, 2010).

Em 2007 ocorreu a 2ª Conferência de Políticas Públicas para Mulheres, em que mulheres brasileiras se reuniram para avaliar a implementação do I PNPM, para discutir sua participação nos espaços de poder e aprovar o II PNPM.

Com o objetivo de ampliar a participação política das mulheres, o II PNPM procurava tratar a questão considerando as mais diferentes dimensões e espaços de exercício de poder e decisão, como a participação em organizações da sociedade e nos partidos políticos, a ocupação de cargos e de mandatos eletivos no Estado, especialmente nos Poderes Legislativo e Executivo e nas instâncias federal, estadual e municipal. Nesse sentido, as iniciativas pretendiam atingir a própria formação cultural da sociedade no que tange às representações consagradas de homens e mulheres e aos lugares ocupados por ambos. Trabalhou-se, assim, na criação de procedimentos e mecanismos que estimulassem novas percepções e atitudes, desconstruindo mitos e preconceitos que alimentam as desigualdades, também no âmbito das famílias e dos espaços privados, nos quais as relações de poder entre os sexos começam a ser engendradas (BRASIL, 2009).

Tem destaque no II PNPM, o eixo V - Participação das Mulheres nos Espaços de Poder e Decisão, cujo objetivo geral é "promover e fortalecer a participação igualitária, plural e multirracial das mulheres nos espaços de poder e decisão", tendo como objetivos específicos:

> I. Promover a mudança cultural na sociedade, com vistas à formação de novos valores e atitudes em relação à autonomia e empoderamento das mulheres;
> II. Estimular a ampliação da participação das mulheres nos partidos políticos e nos Parlamentos federal, estadual e municipal e nas suas instâncias de poder e decisão;
> III. Estimular a ampliação da participação das mulheres nos cargos de decisão dos poderes constituídos (Executivo, Legislativo e Judiciário) em todos os níveis, respeitando-se os recortes de raça/etnia;
> IV. Estimular a ampliação da participação de mulheres nos cargos de liderança política e de decisão no âmbito das entidades representativas de movimentos sociais, sindicatos, conselhos de naturezas diversas, e todos os tipos de associação onde mudanças nesse sentido se façam necessárias;
> V. Estimular a ampliação da participação das mulheres indígenas e negras nas instâncias de poder e decisão;
> VI. Estimular a participação e o controle social nas políticas públicas;
> VII. Inserir no debate da reforma política o tema da paridade na representação parlamentar. (BRASIL, 2008, p. 20)

A 3ª Conferência de Políticas Públicas para Mulheres, realizada em 2011, teve por objetivo discutir e elaborar propostas de políticas que contemplassem a construção da igualdade de gênero, na perspectiva do fortalecimento da autonomia econômica, social, cultural e política das mulheres, e contribuíssem para a erradicação da pobreza extrema e para o exercício pleno da cidadania pelas mulheres brasileiras (CONFERÊNCIA NACIONAL..., 2013).

A 4ª Conferência de Políticas Públicas para Mulheres realizada em Brasília, no período de 10 a 13 de março de 2016, propôs-se a discutir as estratégias de fortalecimento das políticas para as mulheres e a democratização da participação das mulheres nas diversas esferas institucionais e federativas (CONFERÊNCIA NACIONAL..., 2015).

Em que pesem as iniciativas referidas, é possível afirmar que a democracia no Brasil, desde os seus primórdios, foi excludente, limitando a participação das brasileiras por meio de vários artifícios – o acesso desigual à educação e aos direitos sociais; a divisão sexual do trabalho e das responsabilidades, como a sobrecarga de tarefas domésticas, a dupla e tripla jornadas de trabalho – que se constituem em verdadeiras "formas invisíveis" de cercear essa participação dificultando ou mesmo impedindo as mulheres de integrar/interagir com o mundo público (SOARES, 2013; FERREIRA, 2004b).

4 Situação atual da participação política da mulher no Brasil

Dados da União Interparlamentar (IPU) compreendendo o período de 1995 a 2015 (INTER-PARLIAMENTARY UNION, 2015b), mostram que, nos últimos 20 anos, a média de participação feminina em parlamentos ao redor do mundo praticamente dobrou, passando de 11,3% para 22,1%. No mesmo período, o número de câmaras baixas ou únicas com mais de 30% de mulheres cresceu de cinco para 45; aquelas com mais de 40% de mulheres foram de um para 14; duas câmaras ultrapassaram os 50% de participação feminina (Ruanda e Bolívia), sendo que uma delas ultrapassou os 60% de mulheres parlamentares (Ruanda).

Em 1995, cerca de dois terços dos países (61,6%) tinham menos de 10% mulheres nas câmaras baixas ou únicas. Quase todos (88,1%) tinham menos de 20%. Apenas 2,8% tinham 30% ou mais. Já em 2015, apenas 20% dos países tinham menos de 10% de mulheres em suas câmaras baixas ou únicas (incluído aqui o Brasil), entretanto, a maioria (53,2%) ainda têm menos de 20%.

As Américas foram, entre todas as regiões, as que registraram o maior progresso, com a participação de mulheres em parlamentos saindo de 12,7%, em 1995, e atingindo média de 26,4%, em 2015, mais que o dobro do ponto de partida.

Entretanto, a porcentagem de mulheres no Parlamento brasileiro está muito abaixo da média mundial. Segundo dados da IPU de setembro de 2015 (INTER-PARLIAMENTARY UNION, 2015a), o Brasil ocupa a 118ª posição na classificação de quantitativo de mulheres em parlamentos (num *ranking* composto por 190 países), com apenas 10,8% de representantes mulheres (9,9% na Câmara dos Deputados e 16,0% no Senado), enquanto em Ruanda são 57,55% ; na Bolívia são 51,81% (dois únicos países onde as deputadas são maioria, contando com 63,8% e 53,1% dos assentos, respectivamente); e em Cuba são 43,20% . O Brasil ocupa o último lugar na América do Sul e penúltimo da América Latina, estando mais bem posicionado apenas em relação ao Haiti (136ª). Tal situação coloca o Brasil inclusive em pior posição que

estados árabes muçulmanos, como Argélia (31,6%), Tunísia (31,3%), Iraque e Sudão do Sul (ambos com 26,5%) e Emirados Árabes Unidos (17,7%).

Esses dados, quando analisados frente à participação de mulheres em parlamentos por regiões do Mundo (ainda que o Brasil participe dos dados que compõem a estatística das Américas puxando os valores percentuais para baixo), evidenciam não só a sub-representação feminina no Brasil, mas sua defasagem em termos mundiais (Tabela 1 e Figura 3).

Tabela 1 - Participação de mulheres em parlamentos por Regiões do Mundo.

Região do Mundo	Câmara Baixa ou Câmara dos Deputados	Câmara Alta ou Senado	As duas Casas combinadas
Países Nórdicos	41,1%	---	---
Américas	27,4%	26,3%	27,2%
Europa – Países membros da Organização para Segurança e Cooperação da Europa (OSCE), incluindo países nórdicos	25,8%	24,3%	25,5%
Europa - Países membros da Organização para Segurança e Cooperação da Europa (OSCE), excluindo países nórdicos	24,4%	24,3%	24,4%
África Subsaariana	23,4%	20,1%	23,0%
Ásia	19,0%	13,2%	18,4%
Estados Árabes	19,0%	8,9%	17,1%
Pacífico	13,1%	36,0%	15,7%

Fonte: Inter-Parliamentary Union (2015a), dados atualizados até 1/9/2015 (consulta em 12/10/2015).

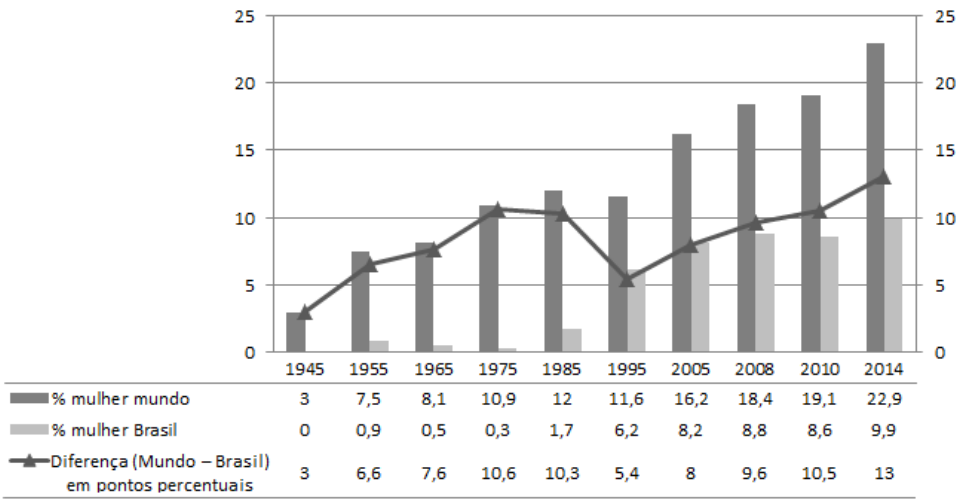


Figura 3 - Porcentagem de mulheres na câmara baixa ou na câmara única (quando não há separação entre câmara baixa e alta) no Mundo e no Brasil no período de 1945-2014.
Fonte: Tribunal Superior Eleitoral (2015), Inter-parliamentary Union (2015a), International Institute for Democracy and Electoral Assistance (2011).

4.1 A participação nos partidos políticos

Em geral, o nível de identificação dos brasileiros com os partidos políticos é reduzido e as raízes dessas instituições na sociedade tendem a ser frágeis. Mas, de qualquer forma, são os partidos que controlam o acesso e o avanço das mulheres nas estruturas de poder. Para alcançar posições de liderança, a mulher deve ascender dentro dos partidos, que têm atribuição exclusiva

de nomear os candidatos a cargos públicos.

Os partidos políticos historicamente têm se caracterizado por serem estruturas sexistas que não incorporam as mulheres em igualdade de condições com os homens. Entretanto, tal situação começa a mudar, ainda que o ritmo seja lento e as oportunidades variem dependendo do partido (INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE, 2002). Dados das eleições de 2014 (Tabela 2), referentes às estatísticas de candidaturas aptas à Câmara dos Deputados, por sexo e por partido, dão conta das diferenças de oportunidades entre homens e mulheres dentro dos partidos.

Tabela 2 - Estatísticas de candidaturas registradas para a Câmara dos Deputados nas Eleições 2014 – Partido/Sexo.

Partido	Número de Candidatas Mulheres	Número de Candidatos Homens	% Mulheres	% Homens
PSTU	40	45	47,06%	52,94%
PC do B	27	46	36,99%	63,01%
PCB	16	29	35,56%	64,44%
PSDB	99	189	34,38%	65,63%
PSL	55	108	33,74%	66,26%
PMN	46	93	33,09%	66,91%
PRB	72	151	32,29%	67,71%
PSOL	115	257	30,91%	69,09%
PTN	32	72	30,77%	69,23%
PSB	108	249	30,25%	69,75%
PSC	46	108	29,87%	70,13%
PMDB	97	230	29,66%	70,34%
PTB	67	162	29,26%	70,74%
PPL	16	39	29,09%	70,91%
PP	46	113	28,93%	71,07%
PT do B	57	141	28,79%	71,21%
PT	102	253	28,73%	71,27%
PRP	61	152	28,64%	71,36%
SD	40	100	28,57%	71,43%
PHS	62	158	28,18%	71,82%
PV	72	184	28,13%	71,88%
PDT	77	200	27,80%	72,20%
PR	48	125	27,75%	72,25%
PPS	32	84	27,59%	72,41%
PROS	24	66	26,67%	73,33%
PTC	44	125	26,04%	73,96%
DEM	36	103	25,90%	74,10%
PSD	40	115	25,81%	74,19%
PSDC	45	131	25,57%	74,43%
PEN	54	158	25,47%	74,53%
PRTB	45	148	23,32%	76,68%
PCO	2	7	22,22%	77,78%
Total	**1.723**	**4.141**	**29,38%**	**70,62%**

Fonte: Tribunal Superior Eleitoral (2015). Acesso em: 4 set. 2015.

A Constituição Federal de 1988 define três sistemas eleitorais distintos, que são detalhados no código eleitoral: (1) eleições proporcionais para a Câmara dos Deputados, câmaras estaduais e câmaras municipais; (2) eleições majoritárias para o Senado Federal (com renovação de 1/3 e 2/3 da Casa alternadamente); e (3) eleições majoritárias em dois turnos para

Presidente da República e chefes dos executivos das demais esferas.

Estudos demonstram que o sistema eleitoral tem importância crítica quanto às possibilidades das mulheres de serem eleitas. Países com sistemas de representação proporcional (RP) tendem a eleger mais mulheres do que aqueles cujo sistema é majoritário. Tal observação estaria relacionada ao fato que, nos sistemas RP – em que os postos são distribuídos com base na porcentagem total de votos obtidos –, os partidos têm um incentivo para equilibrar suas listas, incluindo aspirantes que tenham nexos com uma gama variada de grupos sociais (por exemplo, as mulheres) apresentando candidatos que representem diferentes setores do eleitorado. Nos sistemas majoritários, os incentivos são diferentes: os partidos têm que nomear candidatos que tenham reais oportunidades de ganhar mais votos do que seus oponentes e, na maioria dos casos, os dirigentes dos partidos tendem a escolher candidatos homens. Dados de 53 países, obtidos em 1999, mostravam que as mulheres correspondiam a 20% do total de congressistas nos sistemas de RP, 15% em sistemas mistos e 11% nos sistemas majoritários (INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE, 2002), entretanto, tal tendência não tem sido a observada no Brasil, tendo em vista que na Casa onde as eleições são essencialmente por RP – a Câmara dos Deputados –, constata-se a menor porcentagem de representação feminina.

O Centro Feminista de Estudos e Assessoria (CFEMEA) apontou duas tendências que se manifestam no Congresso Nacional e que, em tese, favorecem o apoio à luta pelos direitos das mulheres: (1) a ampliação da bancada feminina; e, (2) a ampliação do número de parlamentares vinculados ao campo de centro-esquerda e esquerda em relação aos de direita (aqui considerados PDT, PMN, PPS, PROS, PSDB, PV, REDE, PPL, PSB, PT, PSOL, PC do B, PCB, PCO, PSTU). Segundo o CFEMEA, em pesquisas de opinião com parlamentares federais sobre os direitos das mulheres, constatou-se uma correlação positiva entre esses dois itens (parlamentares mulheres e parlamentares de centro-esquerda e esquerda) e opiniões favoráveis à consolidação e ampliação dos direitos das mulheres (CENTRO FEMINISTA DE ESTUDOS E ASSESSORIA, 2006).

O quantitativo de parlamentares (mulheres e homens) que integram os partidos vinculados ao campo da centro-esquerda e esquerda nas legislaturas compreendidas entre os anos de 1999 a 2007 e 2011 a 2019 consta da Tabela 3.

Tabela 3 – Parlamentares que integram partidos vinculados à centro-esquerda, esquerda nas Legislaturas compreendidas entre os anos de 1999-2007 e 2011-2019.

Legislatura	Candidatos eleitos	% de representação no Congresso Nacional	Vagas na Câmara dos Deputados	Vagas no Senado Federal
51ª (1999-2003)	125	23%	513	27
52ª (2003-2007)	241	43%	513	54
54ª (2011-2015)	274	48%	513	54
55ª (2015-2019)	235	44%	513	27

Fonte: Dados para a 51ª e 52ª Legislaturas (CENTRO FEMINISTA DE ESTUDOS E ASSESSORIA, 2006, p. 40), dados para a 54ª e 55ª Legislaturas (TRIBUNAL SUPERIOR ELEITORAL, 2015).

Sem embargo, pesquisa de opinião realizada pelo Instituto Nacional de Estudos Socioeconômicos (Inesc), juntamente com o Departamento Intersindical de Assessoria Parlamentar (Diap), com 150 parlamentares (homens), entre março e maio de 2009, revelou que a maioria dos deputados e senadores não queria mudanças nas regras de eleição que garantissem vagas para grupos com baixa representação no Congresso Nacional. Os parlamentares se manifestaram contra a criação de medidas que favoreçam a eleição de candidatas mulheres (60%), candidatos negros (86%) e candidatos indígenas (76%) (AVELAR, 2013; BRASIL, 2010).

Quanto à população em geral, segundo a Pesquisa Mulheres na Política, realizada pelo IBOPE-Instituto Patrícia Galvão, em 2009, oito em cada dez entrevistados defendiam a adoção de leis que reduzissem as desigualdades entre os sexos no cenário político. Nesse aspecto, 55% defenderam número igual de candidaturas femininas e masculinas, possibilitando assim que as câmaras de vereadores, as assembleias estaduais e o Congresso Nacional tivessem uma representação política igualitária (BRASIL, 2010). As mulheres entrevistadas foram mais favoráveis a esse recurso, 83%, contra 76% dos homens (BRASIL, 2010).

Sem a inclusão da mulher nos processos de partilha do poder decisório interno ou externo aos partidos, perpetua-se, inevitavelmente, a diferenciação hierárquica dos espaços destinados a homens e mulheres, asseverando a invisibilidade da mulher como sujeito político, em especial, perante o Estado (ABRÃO, 2009).

4.2 As cotas de gênero: política de ação afirmativa para aumento da participação política feminina

A 4ª Conferência Mundial das Mulheres, realizada em Pequim, em 1995, recomendou aos países a adoção de ações afirmativas para o empoderamento das mulheres com vistas à reversão do déficit democrático mundial de representação, estabelecendo a meta de 30% de representação feminina em posições de decisão e poder (WORLD CONFERENCE..., 1996).

Um caminho para a mudança tem sido trilhado através de transformações sociais, econômicas e políticas, que lentamente têm atuado sobre os valores patriarcais, oferecendo mais oportunidades para mulheres assumirem diferentes papéis na sociedade. Um segundo caminho mais proativo tem sido desafiar os pontos de estrangulamento, inclusive a resistência tradicional dos partidos em recrutar mulheres por meio da adoção de medidas especiais temporárias (ações afirmativas) – em particular as cotas de gênero eleitoral –, como forma de obter ganhos em um curto período de tempo. Antes de 1995, apenas um pequeno número de países tinha cotas para mulheres, na maioria dos casos, adotadas voluntariamente por partidos políticos individualmente. Em 2015, as cotas se espalharam pelos quatro cantos do mundo, por mais de 120 países (INTER-PARLIAMENTARY UNION, 2015b).

A primeira experiência no Brasil aconteceu logo após a Conferência de Pequim, com a

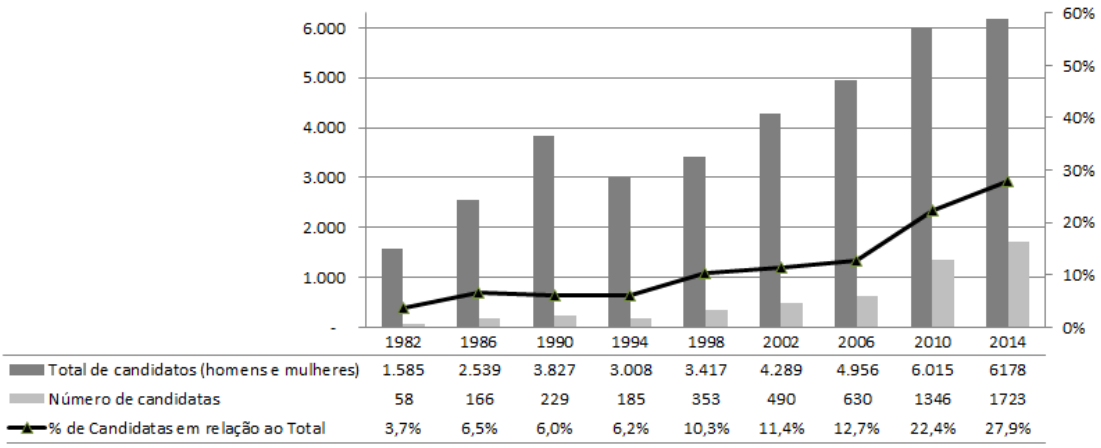
aprovação da Lei nº 9.100/1995, que estabelecia normas para a realização das eleições municipais de 3 de outubro de 1996 e dispunha em seu art. 11, §3º, que "Vinte por cento, no mínimo, das vagas de cada partido ou coligação deverão ser preenchidas por candidaturas de mulheres". Segundo Ferreira (2004a), a aprovação dessa lei traduziu o reconhecimento da luta política dos grupos envolvidos, possibilitou uma maior conscientização da sociedade a respeito da igualdade de direitos, bem como ampliou as discussões em torno da mulher e sua participação política.

Entretanto, ao mesmo tempo em que estabelecia uma cota mínima de 20% de mulheres nas listas dos partidos ou coligações, a Lei nº 9.100/1995 dispôs que o número total de candidaturas fosse também ampliado em 20%, o que diluiu o efeito da política de cotas, dificultando sua efetividade. Desta forma, a abertura de espaço para as mulheres foi acompanhada por uma expansão dos espaços disponíveis, o que possibilitou incluir mais candidatas sem excluir nenhum dos candidatos típicos. Uma cota que não transferiu de fato espaço para as mulheres.

A Lei nº 9.504/1997 assumiu em seu art. 10, § 3º, um caráter universal ao propor que "Do número de vagas resultante das regras previstas neste artigo, cada partido ou coligação deverá reservar o mínimo de trinta por cento e o máximo de setenta por cento para candidaturas de cada sexo". Também ampliou para 150%, a possibilidade de candidaturas em relação ao total das vagas, comprometendo a eficácia do dispositivo anterior.

O grande problema do art. 10, § 3o, da Lei nº 9.504/1997 foi sua aplicação sobre a reserva das vagas e não sobre as candidaturas das listas partidárias, pois os partidos seriam obrigados a reservar as vagas, mas não preenchê-las.

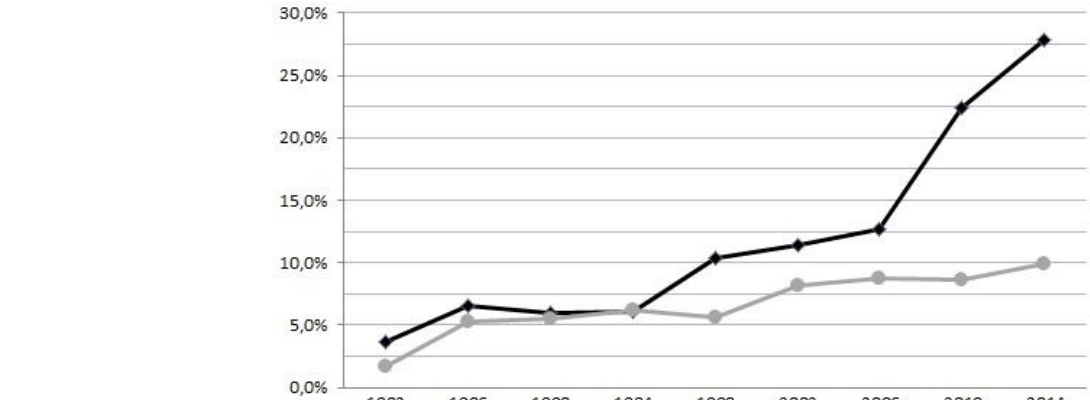
As primeiras eleições federais sob vigência das cotas produziram resultados contraditórios quanto ao desempenho das mulheres. Com relação à quantidade de candidatas, em 1998 não se atingiu metade do percentual mínimo. Os partidos aproveitaram a brecha da legislação que determinava apenas a reserva, mas não o preenchimento, e não completaram as vagas, deixando-as no todo ou em parte vazias. A porcentagem não incidiu sobre a lista efetiva, mas sobre a lista potencial. A cota recaiu sobre o número total de candidatos que o partido poderia lançar e não sobre o número de candidatos que o partido realmente lançou. Contudo, registrou-se uma elevação do número absoluto e do percentual de candidatas em comparação com as eleições anteriores (Figura 4), o que pode ser atribuído à adoção das cotas, que, parece ter estimulado mais mulheres a se candidatar ou partidos a preencherem suas cotas (MARTINS, 2007).



	1982	1986	1990	1994	1998	2002	2006	2010	2014
Total de candidatos (homens e mulheres)	1.585	2.539	3.827	3.008	3.417	4.289	4.956	6.015	6178
Número de candidatas	58	166	229	185	353	490	630	1346	1723
% de Candidatas em relação ao Total	3,7%	6,5%	6,0%	6,2%	10,3%	11,4%	12,7%	22,4%	27,9%

Figura 4 - Percentual de candidatas à eleição para a Câmara dos Deputados no período de 1982[6]-2014.
Fonte: Para 1982 a 2006, Martins (2007, p. 26) para 2010 a 2014 Tribunal Superior Eleitoral (2015).

Por outro lado, em termos de representantes eleitas, os números foram desalentadores, com queda de 6,24% de deputadas eleitas (32 parlamentares) em 1994 para 5,65% (29 deputadas) em 1998, ou seja, o aumento das candidaturas não se traduziu em resultados eleitorais (Figura 5).



	1982	1986	1990	1994	1998	2002	2006	2010	2014
% de Candidatas em relação ao Total	3,7%	6,5%	6,0%	6,2%	10,3%	11,4%	12,7%	22,4%	27,9%
% de Deputadas Federais Eleitas	1,67%	5,34%	5,57%	6,24%	5,65%	8,19%	8,77%	8,60%	9,94%

Figura 5 - Evolução do número absoluto de candidatas à Câmara dos Deputados e deputadas federais eleitas no período de 1982 a 2014.
Fonte: Para candidatas de 1982 a 2006, Martins (2007, p. 26) para 2010 e 2014, Tribunal Superior Eleitoral (2015). Para *eleitas* de 1982 a 2014, Tribunal Superior Eleitoral (2015).

Martins (2007) ressalta que naquele primeiro momento, as mulheres não teriam concorrido com os homens, mas com elas mesmas, de maneira que o aumento da concorrência feminina parece ter provocado a diluição dos votos entre as próprias candidatas, diminuindo suas chances eleitorais. Outro fator a se destacar foi a ampliação do número total de candidatos que o partido ou coligação poderiam lançar para concorrer ao pleito. O aumento permitido pela lei foi suficiente para que os partidos rearranjassem todos os candidatos homens, acomodando-os sem a necessidade de deslocamentos, uma vez que o universo foi suficientemente amplo para que não fosse necessária a retirada de nomes masculinos em favor da inclusão de candidatas

[6] 1982 coincide com o início da abertura política do país.

mulheres, que tiveram que concorrer com todo o contingente masculino anterior.

Nas eleições de 2002, a porcentagem de mulheres eleitas aumentou para 8,19%. Entretanto, não se pode afirmar que esse incremento é devido apenas às cotas, pois pode estar associado à retomada do ritmo de crescimento observado desde 1982 (Figura 2). Ao mesmo tempo, não é possível assegurar que os resultados seriam os mesmos na ausência da ação afirmativa.

Da análise da Figura 5, é possível inferir que a eleição das mulheres não está condicionada ao volume de candidatas. Em que pese o aumento significativo de candidaturas femininas, não se verificaram ganhos em termos eleitorais, o que indica que a capacidade de concorrer com chances de vencer deve envolver outros fatores que não a política de cotas. Os dados parecem indicar, para o caso brasileiro, que não há uma correlação positiva clara entre a adoção da política de cotas e a eleição de mulheres.

A Lei nº 12.034/2009 deu nova redação ao art. 10, § 3º, da Lei nº 9.504/1997: "do número de vagas resultante das regras previstas neste artigo, cada partido ou coligação preencherá o mínimo de 30% (trinta por cento) e o máximo de 70% (setenta por cento) para candidaturas de cada sexo".

A alteração parece pequena, mas a mudança do verbo "reservar" para "preencher" significou uma mudança radical na política de cotas. Com a nova redação, os partidos foram obrigados – ao registrarem a lista de candidaturas no Tribunal Superior Eleitoral – a apresentar no mínimo 30% de candidaturas de cada sexo, podendo deixar vazios os outros 40%.

Além disso, a Lei nº 12.034/2009 determinou a obrigatoriedade de utilização de no mínimo 5% dos recursos do Fundo Partidário para a promoção da participação política das mulheres, bem como reservou pelo menos 10% da propaganda partidária gratuita para as mulheres dos partidos políticos.

A lei, no entanto, não estabelece punição ao partido que não a cumpre. Dados relativos às eleições de 2014 (TRIBUNAL SUPERIOR ELEITORAL, 2015), mostram que a porcentagem de candidatura de mulheres à Câmara dos Deputados foi de 29,38% (Tabela 2), observando-se partidos com apresentação de tão somente 22-23% de candidaturas femininas. De 32 partidos, apenas 10 apresentaram pelo menos um mínimo de 30% de mulheres candidatas (Tabela 2). Além disso, observou-se a proliferação de candidatas aparentes ou laranjas, aquelas candidaturas registradas apenas para cumprir a Lei Eleitoral, sem financiamento, apoio ou tempo de televisão e, em alguns casos, sem nenhum voto (EMPRESA BRASIL DE COMUNICAÇÃO, 2014).

As cotas podem até ter estimulado as mulheres a se candidatarem, mas aparentemente não interferiram na tarefa de elegê-las. Em eleição de voto unipessoal a candidatura não garante a eleição. Nesse sentido, o número de candidatas definitivamente não é o fator preponderante no exame das chances de êxito eleitoral das mulheres, mas sim a sua inserção social em posições

que permitam converter capital social, econômico e cultural em capital político, sendo esse o fator primordial para o recrutamento das mulheres pelos partidos e conversão desse capital precedente em votos para suas candidaturas (e para as listas dos partidos) (VOGEL, 2012).

Embora se busque a paridade, um percentual de 30% já representa um ganho político, considerando-se a estrutura da sociedade e as relações patriarcais que a perpassam. A lei vem responder às reivindicações dos movimentos de mulheres, entretanto, é sabido que, somente com uma ação conjunta das diversas organizações de mulheres com os partidos políticos, e a partir de um projeto de educação política que tenha o gênero como recorte metodológico, será possível diminuir as disparidades.

4.3 A política de cotas não tem sido suficiente

Os avanços na legislação são resultado de muitas lutas dos sujeitos políticos, buscando aprofundar a democracia e a cidadania, e o simples fato de ser aprovada pelo Parlamento não significa que a legislação será cumprida sem questionamentos por atores sociais situados em posições estruturalmente antagônicas na sociedade. Neste contexto, reitera-se a existência de um verdadeiro hiato entre a conquista formal dos direitos e a possibilidade real de seu desfrute.

De maior expressividade do que os resultados alcançados – ainda bastante tímidos – pela política de cotas é a discussão que ela vem gerando no sentido de dar maior visibilidade à exclusão da mulher nos espaços políticos e às disparidades existentes no âmbito político (FERREIRA, 2004a).

A Lei das Cotas não garante que a mulher tenha real acesso ao poder: as cotas não irão mudar as relações de poder em curto prazo, mas elas representam um elemento que modifica a composição dos órgãos diretivos, que trazem novas ideias para o debate e propiciam uma nova forma de aprendizagem do exercício do poder. As mudanças na política se dão gradativamente. O debate que se estabeleceu na sociedade cria condições mais favoráveis à ampliação do número de mulheres nas direções de sindicatos, partidos, assembleias, câmaras, etc., tem efeito multiplicador e contribui para tornar mais visível o cotidiano das mulheres e os obstáculos à sua integração à vida política (FERREIRA, 2004b).

Em que pesem os aspectos apontados, é importante destacar que mesmo considerados certos limites de influência e de poder da mídia, ela pode contribuir tanto para levantar temas para debate como para suprimir temas que, por não serem considerados de interesse ou por não comportarem novidades, ficam fora da cobertura e, portanto, da agenda do debate público. É o que ocorre com a pauta sobre mulher e política, que tem recebido um olhar jornalístico pontual e sem o necessário aprofundamento.

Apesar da demanda por maior participação das mulheres na esfera política, a legislação de cotas é conhecida por apenas 24% dos brasileiros. As mulheres a conhecem ainda menos (20%) do que os homens (28%) (BRASIL, 2010).

Esses dados evidenciam a necessidade de uma maior divulgação da lei, como uma forma de garantir sua efetiva aplicação pelos partidos políticos. Tal fato é confirmado por dados de pesquisa que mostraram que os entrevistados que tinham conhecimento prévio da política de cotas eram mais favoráveis (83%) a ela do que aqueles que tomaram conhecimento sobre a lei no momento da entrevista (75%) (BRASIL, 2010).

A inserção das candidaturas femininas não ameaçou o *status quo*, não destituiu ninguém de seu lugar e ainda colaborou no somatório final de votos (dado o coeficiente eleitoral). Nesse sentido, Abrão (2009) aponta o sistema de cotas na política como uma estratégia de efeitos demagógicos, aparentando democratização e abertura de espaços para a participação da mulher, mas não se comprometendo com sua efetiva eleição.

A política de cotas vigente no Brasil não conseguiu alterar o quadro de sub-representação política da mulher. A necessidade de mudança dessa realidade urge. Fazendo-se uma projeção para o futuro, se a tendência observada não se alterar, considerando-se o quantitativo atual de 513 deputados, para que a representação seja paritária, ou seja, tenhamos mulheres ocupando 50% das vagas na Câmara (pelo menos 256 deputadas eleitas), imaginando-se um quadro exclusivamente progressivo (a cada eleição o número de eleitas sempre aumenta), se for considerada a tendência observada entre 1982-2014 (média de aumento de cinco deputadas por eleição), a paridade seria observada em 176 anos. Caso fosse considerada a tendência observada entre 1988-2014 (média de aumento de três deputadas por eleição), a paridade seria alcançada somente em 288 anos (Figura 6). Torna-se claro que incentivos outros que a política de cotas devem fazer parte da ação conjunta necessária para que se possa reverter esta situação em um futuro menos distante.

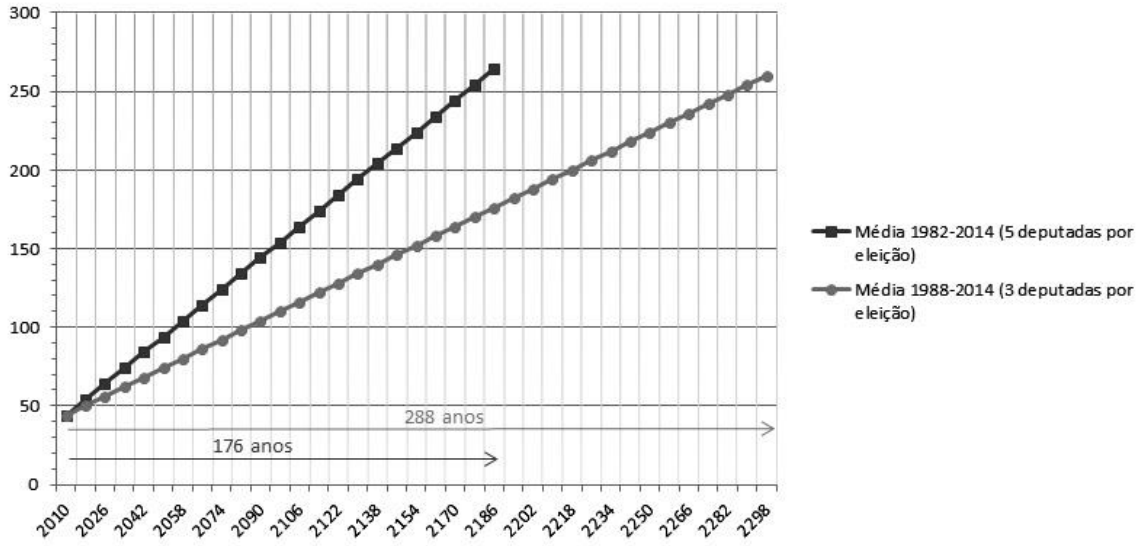


Figura 6 - Cenário projetado para a paridade (256 deputadas) com base em crescimento linear.
Fonte: Elaborado pelos autores

4.4 Propostas para aumentar a participação das mulheres nos espaços de poder

Vogel (2012) destaca alguns aspectos que devem ser levados em consideração nas análises sobre o exercício do direito de voto e a representação feminina no Parlamento:

> a) condições socioeconômicas desfavoráveis, em especial, a "feminização" da pobreza, do desemprego e as discriminações no mercado de trabalho em questões salariais, de recrutamento, promoção e demissão;
> b) escasso acesso às redes políticas estruturadas na sociedade e incipiente relacionamento cooperativo com sindicatos e grupos específicos envolvidos com a militância feminista;
> c) reduzido apoio dos partidos, seja no que se refere ao interesse no recrutamento de candidatas do sexo feminino[7] como também no montante destinado ao financiamento das campanhas das mulheres, insensibilidade dos partidos para a superação do problema e falta de apoio político-eleitoral;
> d) menor capital político e cultural decorrente da baixa experiência em situações de liderança na vida social, organização incipiente das mulheres e falta de experiência política (prática específica desse "agir");
> e) discriminação contra a mulher candidata e indiferença do eleitorado à contribuição da mulher no legislativo (VOGEL, 2012, p. 16).

A proposta de Reforma Política que se encontra em tramitação no Congresso Nacional aborda a temática das mulheres em espaços de poder e de decisão: (1) com destaque para a adoção do financiamento público exclusivo de campanhas eleitorais, meio de combater a excessiva influência do poder econômico no processo político; (2) a introdução do sistema proporcional com listas flexíveis, como forma de fortalecer os partidos e ampliar o conteúdo programático das propostas políticas defendidas nas eleições proporcionais, sem retirar a prerrogativa do eleitor de escolher os candidatos de sua preferência.

No sistema eleitoral de lista aberta vigente no Brasil, o êxito eleitoral está estreitamente relacionado à sustentação financeira das campanhas: os gastos de campanha têm fundamental importância na visibilidade das propostas políticas dos candidatos.

Os defensores do financiamento público manifestam preocupação com os crescentes custos das campanhas eleitorais no país, as implicações de financiamento por empresas privadas – com possível influência sobre a gestão do erário e dos assuntos públicos –, a competição e o personalismo decorrentes do sistema eleitoral de lista aberta e do modelo de financiamento centrado no candidato (VOGUEL, 2012).

No sistema de lista flexível, assim como na representação proporcional de lista fechada, o partido registra seus candidatos por meio de lista partidária preordenada. Entretanto, o modelo de lista flexível permite ao eleitor alterar o ordenamento dos candidatos feito pelos partidos antes das eleições. Havendo concordância com o ordenamento da lista, o eleitor vota no partido. Caso não concorde, o eleitor poderia intervir no ordenamento da lista de duas formas: (1) votando nominalmente em candidatos, assinalando seu nome na lista (modelo adotada na

[7] É importante aqui lançar luz sobre um argumento recorrente de que os partidos simplesmente não conseguem número suficiente de mulheres interessadas para preencherem a porcentagem mínima legal (30%) da lista de candidatos. O recrutamento poderia ocorrer entre as próprias filiadas aos partidos, uma vez que, em nível nacional, do total de filiados de todos os partidos, cerca 40% são mulheres. Segundo Maria Luzia Álvarez (*apud* VOGEL, 2012, p. 16) o problema "está na passagem de filiadas para a lista partidária de candidaturas".

Áustria, Bélgica, Dinamarca, Holanda, Grécia e Suécia); (2) reordenando a lista segundo suas preferências (modelo adotado na Noruega) (VOGUEL, 2012).

Os movimentos de mulheres vêm colocando que a alternância dos sexos na composição da lista preordenada dos partidos e federações é essencial, devendo ser obrigatória por lei, caso contrário, as mulheres podem ser colocadas ao final da lista e não serem eleitas (CENTRO FEMINISTA DE ESTUDOS E ASSESSORIA, 2006).

Importante comentar que existem projetos de lei em tramitação no Congresso Nacional dispondo também sobre cotas por sexo no Poder Executivo e no Poder Judiciário, no sentido de estender as ações afirmativas para esses poderes.

A Proposta de Emenda à Constituição (PEC) nº 590/2006 propõe a representação proporcional de cada sexo na composição das mesas diretoras da Câmara, do Senado e das comissões, garantindo pelo menos uma vaga para cada sexo (PIETÁ, 2010). A PEC já está pronta para ser votada há oito anos, mas até agora os líderes não a colocaram em pauta[8].

Ainda não apresentadas no Congresso, mas já em discussão em fóruns relativos à equidade representativa, há propostas de nomear mulheres nas primeiras posições das listas de candidatos a eleições; exigir de que para cargos em que o candidato oficial seja um homem, a alternativa seja uma mulher e vice-versa; adotar cotas tanto para eleição de candidatos a postos de eleição popular como para eleições internas dos partidos. Além disso, no que diz respeito à política de cotas, propõe-se que a lei deve prever sanções ao seu descumprimento.

4.5 Atuação feminina na Câmara dos Deputados: maior representação formal não necessariamente significa maior representação dos interesses da mulher

A ausência de mulheres nas casas legislativas remete ao silêncio e é associada à ausência de representação de seus interesses. A presença de mulheres nos parlamentos estabeleceria as vias capazes de permitir conhecer as necessidades e os interesses da população feminina. Ganha espaço, nessa argumentação, a concepção de que a participação feminina representa um rompimento com a política tradicional desenvolvida pelos homens, de maneira que a maior presença de mulheres levaria: (1) à (re)construção de um espaço mais honesto e ético, características estereotipicamente atribuídas a elas; (2) à inclusão, na agenda política, de temas até então negligenciados e suplantados, em geral, pelas discussões econômicas (PINHEIRO, 2007).

À ideia de que homens e mulheres atuam de forma diferenciada na política por trazerem experiências de socialização diferenciadas, somam-se outros fatores relacionados a dimensões

[8] A escolha das matérias a serem analisadas pelo Plenário é feita pelo Colégio de Líderes. Claro está que nem todos os agentes possuem a mesma faculdade de determinar a agenda a ser seguida. De fato, grupos sociais com menor representação (aqui incluídas as mulheres) terão maior dificuldade em colocar seus interesses em pauta no processo de construção da agenda de prioridades da ação estatal.

como: capital político, bases políticas e dominação masculina/patriarcalismo que são determinantes para moldar uma prática política dita feminina (PINHEIRO, 2007).

A partir desse discurso, é estabelecida a ideia de uma divisão sexual dos trabalhos parlamentares que

> [...] pela própria natureza de exclusão vivenciada historicamente pelas mulheres, as colocaria em condição de melhor falar pelos grupos sociais mais vulneráveis, pelas temáticas mais esquecidas e, na lógica da política de presença, pelas mulheres de modo geral, visando a um aumento da pressão e ampliação dos espaços de legitimidade (PINHEIRO, 2007, p. 20).

Entretanto, não se deve construir um julgamento quanto aos interesses de gênero. As mulheres constituem um grupo social heterogêneo em termos dos valores políticos que orientam sua prática e seu discurso. Elas podem estar comprometidas com "interesses divergentes, ou objetivos específicos desvinculados da elaboração de políticas públicas para as necessidades sociais vinculadas ao seu gênero" (VOGEL, 2012, p. 13).

Andrade (2008) aponta que há uma diferença entre representação política e participação política. A ausência sistemática de determinados grupos sociais nos fóruns de decisão constituiria uma flagrante falha da democracia. Para a autora, a igualdade de presença já estaria implícita na noção de participação, ainda que não tão claramente na de representação política.

Entretanto, parece mais coerente o fato de que não há nada que garanta que uma maior presença feminina no Parlamento signifique, automaticamente, uma maior defesa dos interesses femininos e a inclusão de temas prioritários a esse segmento na pauta política. A atuação exitosa das mulheres na política depende muito mais de suas ideias do que de seu sexo.

Ademais, o condicionamento da atuação política da mulher à defesa de determinados assuntos, reforça os tradicionais papéis de gênero.

Ao impor uma divisão sexual dos trabalhos parlamentares, os homens são exonerados de lidar com questões essenciais relacionadas às esferas privada e social ao passo que as mulheres são oneradas ao serem responsabilizadas exclusivamente pela transformação de sua condição social (PINHEIRO, 2007).

Segundo Ferreira (2006), os projetos que diziam respeito aos direitos da mulher representavam 1,68% do total dos projetos que tramitavam no Legislativo em 2006 e correspondiam a 7,32 % dos projetos apresentados pelas deputadas. Eram dez projetos, nenhum deles apresentado por deputados. Isso pode tanto indicar um claro desinteresse dos deputados em propor leis que possam alterar as relações de gênero, ou o reflexo da suposta "seara feminina".

Para que os temas de interesse feminino ganhem maior visibilidade e efetividade na agenda política, é necessário que haja a desconstrução da divisão sexual dos trabalhos parlamentares e que a questão feminina torne-se, de fato, responsabilidade de toda a sociedade. Isso exige não só alterações profundas nos modelos existentes de socialização diferenciada, mas

também mudanças significativas nas relações entre o eleitorado e seus representantes, nos padrões culturais de construção de carreiras políticas e no sexismo institucional ainda vigente (PINHEIRO, 2007).

A questão que se coloca é a da cultura política. É necessário desconstruir a leitura conservadora da mulher, desfazer a visão social da figura da mulher ligada ao ambiente privado. Muitas das mulheres que são eleitas estão a serviço dos interesses políticos dos seus maridos. Ou os maridos que não puderam ser candidatos colocam suas mulheres na política (a exemplo da candidatura de Weslian Roriz, mulher de Joaquim Roriz, para Governadora do Distrito Federal, nas eleições de 2010). Então, há que se pensar sobre mais mulheres no poder, mas também sobre mais poder para as mulheres. Caso contrário, não se conseguirá romper a desigualdade nos processos de decisão.

5 Conclusão

Os direitos, no caso das mulheres, foram sendo conquistados e ampliados ao longo dos anos, especialmente no período pós-Constituinte de 1988. No entanto, esse caminho não é linear e, assim como se observam progressos, tem-se que lutar diuturnamente contra retrocessos. O contexto atual alude à necessidade de organização e constante mobilização social para fazer frente também à possibilidade de perda e restrição de direitos conquistados.

A avaliação dos resultados eleitorais indica que as cotas brasileiras não são instrumentos suficientes para aumentar a representação política da mulher. Vale destacar os pontos negativos da legislação que instituiu as cotas, como a inexistência de punição em caso de descumprimento e a ampliação do número de candidatos que podem ser lançados, o que aumentou substancialmente o número de concorrentes. A despeito disso, as análises apontam que houve aumento nas candidaturas de mulheres após as cotas. O mesmo não pode ser dito com relação aos ganhos eleitorais. Não se notam impactos na evolução do percentual de eleitas.

Reverter o quadro de desigualdade é um desafio que se apresenta para toda a sociedade: homens e mulheres, partidos políticos e instituições de Estado – Legislativo, Executivo ou Judiciário. Trata-se de aperfeiçoar a democracia: o déficit de representatividade – as mulheres, que correspondem a 52% do eleitorado brasileiro ocupam menos de 10% das vagas do Parlamento –, significa um déficit para a democracia brasileira. E só se pode falar em democracia de fato e de direito quando os direitos de cidadania (incluídos os políticos, como o de votar e ser votado) são extensivos a todos os segmentos sem discriminação de nenhum tipo (territorial, socioeconômica, de raça, de gênero).

Por oportuno, cabe citar Michelle Bachelet, presidente do Chile de 2006 a 2010, reeleita para o período de 2014 a 2018, primeira mulher eleita presidente na América do Sul, em discurso proferido no ano de 2007: “Cuando una mujer llega sola a la política, cambia la mujer. Cuando muchas mujeres llegan a la política, cambia la política”.

Referências

ABRÃO, L. G. M. **A participação política da mulher**: uma análise do ponto de vista psicológico. 2009. Tese (Doutorado) – Instituto de Psicologia, Universidade de Brasília, Brasília, 2009.

ANDRADE, G. O. **Presença da Diferença**. 2008. 287 fl. Dissertação (Mestrado em Ciência Política) – Instituto de Ciência Política, Universidade de Brasília, Brasília, 2008.

AVELAR, L. **Mulheres na elite política brasileira**. 2. ed. São Paulo: Fundação Konrad Adenauer, 2001.

_____. Mulher e política em perspectiva. In: VENTURI, G.; GODINHO, T. (Ed.). **Mulheres brasileiras e gênero nos espaços público e privado**: uma década de mudanças na opinião pública. São Paulo: Fundação Perseu Abramo, 2013.

AZEVEDO, D. B. D.; RABAT, M. N. **Palavra de mulher**: oito décadas do direito de voto. 2. ed. Brasília: Edições Câmara, 2012.

BOURDIEU, P. **Propos sur le champ politique**. Lyon: Presses Universitaires de Lyon, 2000.

_____. Sobre o poder simbólico. In: _____. **O poder simbólico**. 8. ed. Rio de Janeiro: Bertrand Brasil, 2005.

BRASIL. **Plano Nacional de Políticas para as Mulheres**. Brasília: Presidência da República, Secretaria Especial de Políticas para as Mulheres, 2004.

_____. **II Plano Nacional de Políticas para as Mulheres (versão compacta)**. Brasília: Presidência da República; Secretaria Especial de Políticas para as Mulheres, 2008.

_____. **Relatório final de implementação**: I Plano Nacional de Políticas para as Mulheres. Brasília: Secretaria Especial de Políticas para as Mulheres, 2009.

_____. **Mais mulheres no poder**: uma questão de democracia. Secretaria de Políticas para as Mulheres. Brasília, 2010.

CAMPOS, M. R.; PASCUAL, A. L. **Mulheres e desigualdade de gênero**: a evolução das políticas de ação afirmativa na América Latina. Projeto (Iniciação Científica em Direito e Ações Afirmativas) – Faculdade de Direito, Universidade de Brasília. Brasília. 2010.

CÂMARA DOS DEPUTADOS. **Bancada Feminina**: bancadas anteriores. Brasília, 2015. Disponível em: <http://www2.camara.leg.br/documentos-e-pesquisa/fiquePorDentro/temas/temas-anteriores-desativados-sem-texto-da-consultoria/mulheresnoparlamento/bancada-feminina/bancadas-anteriores>. Acesso em: 20 out. 2015.

CENTRO FEMINISTA DE ESTUDOS E ASSESSORIA. **Os direitos das mulheres na legislação brasileira pós-constituinte**. Brasília: Letras Livres, 2006.

CONFERÊNCIA NACIONAL DE POLÍTICAS PARA AS MULHERES, 3., 2013. Brasília, **Anais...** Brasília: Secretaria de Políticas para as Mulheres, 2013.

_____. 4., 2015, Brasília. **Texto Base**. Brasília: Secretaria de Políticas para as Mulheres, 2015.

COUTO, M. T.; SCHRAIBER, L. B. Machismo hoje no Brasil: uma análise de gênero das percepções dos homens e das mulheres. In: VENTURI, G.; GODINHO, T. (Ed.). **Mulheres brasileiras e gênero nos espaços público e privado**: uma década de mudanças na opinião pública. São Paulo: Fundação Perseu Abramo, 2013.

DOUZINAS, C. **O fim dos direitos humanos**. São Leopoldo: Unisinos, 2009.

DUSSEL, E. D. **1492 O encobrimento do outro**: a origem do "mito da modernidade". Petrópolis: Editora Vozes, 1993.

EMPRESA BRASIL DE COMUNICAÇÃO. **Mulheres não querem ser candidatas a "laranja"**. 2014. Disponível em: <http://www.ebc.com.br/noticias/politica/galeria/audios/2014/10/mulheres-nao-querem-ser-candidatas-a-laranja>. Acesso em: 30 out. 2015.

FERREIRA, M. M. Do voto feminino à Lei das Cotas: a difícil inserção das mulheres nas

democracias representativas. **Revista Espaço Acadêmico**, v. 4, n. 37, 2004a.

_____. Representação feminina e construção da democracia no Brasil. In: SCAVONE, L. (Ed.). **Questões feministas nas Ciências Sociais**: em busca do tempo presente. Coimbra: Centro de Estudos Sociais da Universidade de Coimbra, 2004b.

_____. Mulheres no Legislativo: demandas e ação política das deputadas. In: SEMINÁRIO INTERNACIONAL FAZENDO GÊNERO, 7., 2006, Santa Catarina, **Anais...** Santa Catarina: UFSC, 2006. Disponível em: <http://www.fazendogenero.ufsc.br/7/artigos/M/Mary_Ferreira_38_B.pdf>. Acesso em: 18 out. 2015.

INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE. **Mujeres en el parlamento**: más allá de los números. Estocolmo, 2002. Disponível em: <http://www.idea.int/publications/wip/es.cfm>. Acesso em: 18 out. 2015.

_____. **Democracy and gender**. Estocolmo, 2011. Disponível em: <http://www.idea.int/gender/index.cfm>. Acesso em: 9 set. 2015.

INTER-PARLIAMENTARY UNION. **Women in national parliaments**. Geneva, 2015a. Disponível em: <http://www.ipu.org/wmn-e/classif.htm>. Acesso em: 10 de out. 2015.

_____. **Women in Parliament**: 20 years in review. Geneva, 2015b. Disponível em: <http://www.ipu.org/pdf/publications/WIP20Y-en.pdf >. Acesso em: 10 de out. 2015.

MARTINS, E. V. **A política de cotas e a representação feminina na Câmara dos Deputados**. 2007. Monografia (Especialização em Instituições e Processos Políticos do Legislativo) – Centro de Formação, Treinamento e Aperfeiçoamento, Câmara dos Deputados, Brasília.

MATOS, M.; CORTÊS, I. R. **Mais mulheres no poder**: contribuição à formação política das mulheres. Brasília: Presidência da República, Secretaria de Políticas para as Mulheres, 2010.

MENEZES, M. L. D. Democracia de assembleia e democracia de parlamento: uma breve história das instituições democráticas. **Sociologias,** v. 12, n. 23, p. 20-45, jan./abr., 2010.

PERROT, M. **Femmes publiques**. Paris: Textuel, 1997.

PIETÁ, J. **Carta à Bancada Feminina**. Brasília: Câmara dos Deputados, 2010. Disponível em: <http://www2.camara.gov.br/a-camara/conheca/camara-destaca/mulheres-no-parlamento/bancada-feminina/carta-as-deputadas>. Acesso em: 10 set. 2015.

PINHEIRO, L. S. **Vozes femininas na política**: uma análise sobre mulheres parlamentares no pós-Constituinte. Brasília: Secretaria Especial de Políticas para as Mulheres, 2007.

RITT, C. F.; RITT, E. A (des) necessidade da representação da vítima para a punição do agressor da violência de gênero compreendida como garantia fundamental contra a violência doméstica praticada contra a mulher. In: SEMINÁRIO INTERNACIONAL DE DEMANDAS SOCIAIS E POLÍTICAS PÚBLICAS NA SOCIEDADE CONTEMPORÂNEA, 11., 2014, Santa Cruz do Sul. **Anais...** Santa Cruz do Sul: UNISC, 2014.

SEIDLER, V. Reason, desire, and male sexuality. In: CAPLAN, P. (Ed.). **The cultural construction of sexuality**. London; New York: Taylor & Francis, 1987.

SOARES, V. Percepções e atitudes: ser mulher e participação política. In: VENTURI, G.; GODINHO, T. (Ed.). **Mulheres brasileiras e gênero nos espaços público e privado**: uma década de mudanças na opinião pública. São Paulo: Fundação Perseu Abramo, 2013.

SOW, M. M. A participação feminina na construção de um parlamento democrático. **E-legis,** v. 5, n. 2, p. 79-94, 2010.

TRIBUNAL SUPERIOR ELEITORAL. **Dados estatísticos**: eleições 2014. Brasília, 2014. Disponível em: <http://www.tse.jus.br/hotSites/CatalogoPublicacoes/pdf/informacoes_dados_estatisticos_eleicoes_2014_web.pdf>. Acesso em: 9 de set. 2015.

_____. **Repositório de dados eleitorais**. 2015. Disponível em: <http://www.tse.jus.br/eleicoes/estatisticas/repositorio-de-dados-eleitorais>. Acesso em: 4 set. 2015.

VOGEL, L. H. **A difícil inserção**: voto feminino e as condições sociais de acesso ao campo político no Brasil (1932-2012). Brasília: Câmara dos Deputados, Consultoria Legislativa, 2012.

WORLD CONFERENCE ON WOMEN, 4. Beijing, 1995. **Report of the...** New York: United Nations, 1996.

Artigo recebido em: 19/01/2016

Artigo aceito para publicação em: 28/09/2016

ANEXO 2 - Femicídio, feminicídio e o entendimento dos operadores do Direito brasileiro ao tratar a morte de mulheres em razão do gênero

Direito Penal 1 (UnB): SCHLOTTFELDT, Shana. Femicídio, feminicídio e o entendimento dos operadores do Direito brasileiro ao tratar a morte de mulheres em razão do gênero. *Boletim IBCCRIM*, v. 291, 2017, p. 9-11. Disponível em: https://www.ibccrim.org.br/noticias/exibir/6628/. ISSN 1676-3661.

Há caminhos de mudanças já construídos pela lei, por normativos internacionais, mas esses caminhos precisam ser desbravados e corajosamente percorridos.

Nota

(1) Depen. Levantamento Nacional de Informações Penitenciarias – *Infopen Mulheres*, jun. 2014.

Paola Hakenhaar
Especialista em Direito Penal e Processual Penal Empresarial pelo Centro Universitário - Católica de Santa Catarina.
Professora de Processo Penal na Faculdade Cenecista de Joinville – CNEC.
Professora de Processo Penal e Criminologia na Faculdade Guilherme Guimbala – ACE.

Femicídio, feminicídio e o entendimento dos operadores do Direito brasileiro ao tratar a morte de mulheres em razão do gênero

Shana Schlottfeldt

A violência contra a mulher não é algo novo. Tem raízes nas desigualdades de gênero, fundadas no machismo e patriarcalismo que criaram um sistema de sujeição, subordinação e dominação da mulher, capaz de considerar natural a desigualdade produzida socioculturalmente (MELLO, 2016, p. 97). Novidade é a judicialização do problema, seja pela elaboração de leis, seja pelo estabelecimento de meios pelos quais a estrutura policial e/ou jurídica possa ser acionada para proteger vítimas e/ou punir agressores (WAISELFISZ, 2015, p. 7).

Há dez anos, foi sancionada a Lei 11.340/2006 (Lei Maria da Penha), que criou mecanismos para coibir a violência doméstica e familiar contra a mulher; e há um ano, foi sancionada a Lei 13.104/2015 (Lei do Feminicídio), que previu o feminicídio como circunstância qualificadora do crime de homicídio e incluiu-o no rol dos crimes hediondos.

Mas o que vem a ser feminicídio? E qual tem sido o entendimento dos operadores do Direito no que diz respeito a ele?

Antes de qualquer coisa, cumpre tecer algumas considerações a respeito dos termos *femicídio* e *feminicídio*.

A expressão *femicide* (do inglês) foi usada pela primeira vez em 1976, no Tribunal Internacional de Crimes contra Mulheres, em Bruxelas, pela socióloga **Diana Russell**, significando a morte intencional de mulheres, por homens, em razão de serem mulheres (motivadas por razão do gênero). O vocábulo foi proposto como uma alternativa ao termo neutro homicídio – que contribuiria para manter invisível a realidade de desigualdade, opressão e violência sistemática contra a mulher (ONU MULHERES; SPM; SENASP, 2016, p. 20). Segundo **Russell**, a definição de um nome que significa a "morte de mulheres" é um passo importante na evidenciação dessa forma de violência, uma vez que poder nomear um crime provê meios de se problematizar a questão, o que comumente precede o enfrentamento do tema (RADFORD; RUSSELL, 1992, p. XIV).

Há um grande debate em torno do termo a ser adotado, se femicídio ou feminicídio, o que tem gerado grande discussão entre feministas da América do Norte e da América Latina. **Russell** propõe "femicídio", por considerá-lo um termo unificado (tradução direta da palavra *femicide*); além disso, manifesta aversão ao vocábulo "feminicídio", por julgá-lo assemelhado ao conceito opressivo de "feminilidade". Por outro lado, há uma corrente, da qual faz parte a socióloga **Julia Monárrez**, que sustenta que a palavra adequada seria feminicídio, dado que as duas raízes latinas da palavra são *femina* (mulher) e *caedo*, *caesun* (matar), de maneira que a morte de uma mulher seria *feminicidium*, de onde se chegaria à palavra feminicídio. Por fim, na opinião da antropóloga **Marcela Lagarde**, a palavra proposta por **Radford** e **Russell** (*femicide*) perderia força ao ser traduzida para o espanhol (e, em nosso caso, para o português), sugerindo o uso da palavra feminicídio (MELLO, 2016, p. 20-24).

No Brasil, a escolha da nomenclatura se deu pelo legislador, que optou pelo termo feminicídio.

A partir de uma perspectiva jurídico-penal, femicídio corresponderia à morte de uma mulher, não necessariamente relacionada à condição do sexo feminino (BIANCHINI; GOMES, 2015). Englobaria todas as mortes evitáveis de mulheres – violentas ou não, criminais ou não –, *e.g.*, a morte de uma mulher por bala perdida (violência urbana); como fruto de uma esterilização forçada; em decorrência de partos e abortos inseguros (LAURENZO-COPELLO, 2012, p. 125-126). Assim, um traço do termo femicídio é a ligação que ele faz entre as diversas formas de violência contra as mulheres, de sorte que, se uma delas termina em morte, constitui um femicídio (MELLO, 2016, p. 28).

Uma definição de feminicídio adequada e útil para a análise jurídico-penal brasileira seria "*o assassinato de mulheres baseado no gênero, incluindo não apenas o assassinato por parceiros íntimos, mas também a morte intencional por parceiros não íntimos, que tenha sido motivado em razão de gênero*" (MELLO, 2016, p. 33).(1)

A lei dispõe que houve feminicídio quando a morte resulta de violência doméstica e familiar, ou quando evidencia menosprezo ou discriminação à condição de mulher, caracterizando crime por razões de condição do sexo feminino (art. 121, § 2º, VI; § 2º-A, I e II, do Decreto-lei 2.848/1940 – Código Penal (CP), redação dada pela Lei 13.104/2015).

Entre os principais obstáculos para análise do feminicídio encontra-se a ausência de dados estatísticos confiáveis e comparáveis sobre o assunto em todos os Poderes constituídos e em todas as esferas de governo (SENADO, 2013, p. 9). Há dificuldade no acesso e compreensão das estatísticas oficiais, em especial as produzidas no âmbito da segurança pública; disparidade dos dados apresentados pelos serviços de segurança e justiça e aqueles apresentados pelos serviços de saúde, decorrentes das diferenças entre as unidades de registro oficial e sua finalidade (CERQUEIRA et al., 2015, p. 9; MELLO, 2016, p. 125; WAISELFISZ, 2015, p. 8 e 67).

Quando se fala em homicídio, a desproporção entre as taxas de

vitimização de homens e mulheres é irrefutável: no Brasil, no período de 2000 a 2011, a taxa de mortes de mulheres foi de 4-5 por 100 mil mulheres,[2] ao passo que de homens foi da ordem de mais de 50 por 100 mil homens (CERQUEIRA et al., 2015, p. 16-17). Diante desse quadro, as mortes de mulheres permanecem encobertas por sua pequena expressão numérica e, consequentemente, seu pequeno impacto nas políticas públicas.

Em 2013, o número de mortes de mulheres, no Brasil, por causas violentas foi de 4.762, representando 13 homicídios femininos diários. Do total de mortes de mulheres registradas, 50,3% foram perpetradas por um familiar da vítima; sendo que 33,2% dos homicidas eram parceiros ou ex-parceiros da vítima (feminicídio íntimo) (WAISELFISZ, 2015, p. 70).

O meio ou forma com que foi praticada a agressão contra as mulheres – estrangulamento/sufocação (uso das mãos, cinto, fio elétrico), arma cortante/penetrante (faca, peixeira, canivete, garrafa de vidro), objeto contundente (martelo, pedra, cabo de vassoura, botas, vara de pescar), espancamento, empalamento, desfiguração – demonstra maior presença de crimes de ódio ou por motivos fúteis/banais, muitas vezes com imposição de sofrimento às vítimas previamente à execução (SRJ, 2015, p. 39; WAISELFISZ, 2015, p. 39).

Ainda que longe do ideal, os dados disponíveis permitem inferir que a violência doméstica e familiar é central para a caracterização do feminicídio, no qual a morte é, frequentemente, o epílogo de histórias marcadas por um contínuo de violência (ONU MULHERES; SPM; SENASP, 2016, p. 21; SRJ, 2015, p. 11; SENADO, 2013, p. 1.003).

As Diretrizes Nacionais para investigar, processar e julgar com perspectiva de gênero as mortes violentas de mulheres explicitam as motivações embasadas em gênero que podem estar por trás de episódios violentos: inconformismo com o término do relacionamento; sentimento de posse sobre a mulher; controle sobre seu corpo, desejo e autonomia; limitação da sua emancipação profissional, econômica, social ou intelectual; tratamento da mulher como objeto sexual; e manifestações de desprezo e ódio pela mulher e por sua condição de gênero (ONU MULHERES; SPM; SENASP, 2016, p. 43).

Também chamam a atenção as falhas e dificuldades na investigação de mortes violentas de mulheres: a persistência de preconceitos e estereótipos na prática dos operadores judiciais; a demora no início das investigações; a inatividade dos expedientes; as negligências e irregularidades na coleta e prática das provas, bem como na identificação das vítimas e responsáveis; a insuficiente participação dos representantes das vítimas (MELLO, 2016, p. 131).

Pesquisa efetuada pelo Instituto de Bioética, Direitos Humanos e Gênero (ANIS, 2013, p. 175-183), sobre o homicídio de mulheres no Distrito Federal entre os anos de 2006 e 2011, apontou os seguintes achados:[3] em 45% dos casos, as mulheres foram mortas com violência doméstica ou familiar; em 96% dos casos de violência doméstica ou familiar, a mulher foi morta por seu companheiro ou ex-companheiro; a agravante de violência contra a mulher (art. 61, II, *f*, do CP) só foi mencionada por qualquer um dos atores do processo em 31% dos processos e só constou de 22% das condenações. Três qualificadoras foram observadas: motivo torpe (art. 121, § 2º, I, do CP); motivo fútil (art. 121, § 2º, II, do CP) e dificuldade de defesa da vítima (art. 121, § 2º, IV, do CP). A maioria dos réus foi condenada por homicídio duplamente qualificado com base no art. 121, § 2º, II e IV. Em poucos casos os magistrados reconheceram a agravante de violência contra a mulher e a aplicação da Lei Maria da Penha. Em 86% dos casos houve condenação do réu por homicídio doloso. As penas aplicadas situaram-se entre 22 anos e oito meses e 7 anos, com pena média de 15 anos de reclusão. Conforme **Belloque** (2015), o estudo mostra que se trata de uma área do sistema de justiça criminal em que "não há impunidade e as penas já costumam ser altas".

Estudo qualitativo[4] de processos judiciais relativos a crimes de homicídio tentado e consumado de mulheres realizado pela Secretaria de Reforma do Judiciário (SRJ, 2015, p. 38-63) mostrou a recorrência e a relevância de elementos factuais no feminicídio, bem como o tratamento judicial que lhe é conferido.

O estudo mostrou que as narrativas produzidas no sistema de justiça criminal tendem a acentuar os estereótipos dos papéis que homens e mulheres desempenham na sociedade, reafirmando discursos de culpabilização da vítima. Associado a isso, apontou que os atores do sistema de justiça têm dificuldade em enxergar a violência doméstica como estruturante das relações sociais, explicando o conflito a partir de uma lógica individual e tradicional, em que a violência final contra a mulher é episódica. A legítima defesa da honra não foi utilizada expressamente, mas a lógica dessa argumentação esteve presente. Os representantes do Ministério Público foram os atores que apresentaram teses mais situadas em um contexto de gênero; já o discurso dos(as) magistrados(as) tendeu a não considerar a variável da violência de gênero no momento da dosimetria.

Quanto ao processamento dos casos pelo Tribunal do Júri, para os homicídios consumados, houve quatro formas de enquadramento: (1º) ausência do dolo de matar, com pedido de absolvição do réu; (2º) conduta multiqualificada, com pedido de condenação do réu a uma pena de longa duração; (3º) entre os dois extremos, a caracterização da conduta como homicídio privilegiado, com diminuição da pena (art. 121, § 1º, do CP); ou (4º) homicídio simples (art. 121, *caput*, do CP). Mas os fatos entendidos como feminicídios íntimos foram enquadrados, desde a denúncia até a sentença de mérito, majoritariamente como homicídios qualificados, tentados ou consumados. As qualificadoras foram: motivo torpe (art. 121, § 2º, I, do CP); motivo fútil (art. 121, § 2º, II, do CP) (segunda mais frequente); meio cruel (art. 121, § 2º, III, do CP) e dificuldade de defesa da vítima (art. 121, § 2º, IV, do CP) (qualificadora mais frequente). Em cerca de um terço dos casos a sentença condenatória trazia mais de uma qualificadora (geralmente uma combinação dos incisos II e IV). Houve condenação em 79% dos casos de homicídio. As maiores penas aplicadas (26%) estiveram compreendidas entre 32 anos e oito meses e 22 anos de reclusão. Ainda sobre os homicídios qualificados consumados, em 53% dos processos houve condenação em primeira instância a penas de prisão no intervalo de 12 a 20 anos de reclusão. Quando houve interposição de recurso para rever a pena, a tendência foi de manutenção do *quantum* definido em primeira instância. As manifestações dos Tribunais de Justiça em geral demonstraram pouca permeabilidade à discussão sobre violência de gênero, embora se tenha verificado uma tendência à expansão da aplicação da Lei Maria da Penha.

Mas o que dizer diante do fato, acima apontado, de o recorte do feminicídio ser uma área do sistema de justiça criminal em que se verifica condenação e no qual as penas já costumavam ser altas antes mesmo da Lei do Feminicídio?

Quanto a isso, destacam-se três aspectos fundamentais:

Primeiro, conforme apontado por **Mello** (2016, p. 140), um dos pontos cegos deixados pela Lei Maria da Penha – em que pese sua importância para a luta das mulheres – foi o fato de prever apenas a lesão corporal relacionada à violência doméstica, não abrangendo o mais grave desdobramento dessa mesma violência: a morte, de maneira que os crimes de homicídio escapavam ao seu escopo. Daí, segundo a pesquisadora e magistrada, a importância da Lei do Feminicídio.

Segundo, apesar da crítica a respeito da asseveração da pena, importa deixar claro que "há um exagero na leitura sobre o agravamento punitivo", pois o feminicídio, antes da Lei 13.104/2015, já vinha sendo considerado homicídio qualificado (como referido acima, com enquadramento no art. 121, § 2º, I-IV, do CP); além disso, as hipóteses de homicídio qualificado já eram consideradas crime hediondo[5] (CASTILHO, 2015), não havendo,

portanto, que se falar em expansionismo penal nesse caso (MELLO, 2016, p.3). Dessa forma, a proposta, ao não trazer aumento de pena, colocou mais "*ênfase na adequação da resposta do sistema de justiça criminal (com atenção para a desigualdade de gênero) do que na maior punição para os autores do crime de feminicídio*" (MACHADO; MATSUDA; 2015).

Por fim, cumpre ressaltar que aquilo que não se nomeia não existe. A criação de um crime sob o nome de feminicídio serve a razões muito mais fundamentais do que a mera possibilidade de uma punição. Representa o reconhecimento pelo Direito, como instituição, de uma realidade que muitas vezes não é reconhecida no próprio seio social. Conceituar como crime o assassinato de mulheres pelo fato de serem mulheres constitui um avanço na compreensão política do fenômeno de subordinação da mulher, da negação da sua autonomia, do fator discriminação, da violência estrutural e sistemática, bem como da ausência de políticas públicas visando à prevenção e à erradicação desse tipo de violência contra as mulheres. Pode representar um divisor de águas no que diz respeito à produção de estatísticas e à criação de políticas de enfrentamento.

Os dados e estudos apresentados nos dão conta do tratamento do feminicídio (homicídio de mulheres em razão do gênero) previamente à própria Lei do Feminicídio. Passado um ano de sua sanção, ainda carecemos de estudos que mostrem o impacto específico da nova Lei para avaliar se a discussão proposta está tendo resultado.(6)

Sabe-se, empiricamente, que a qualificação de um crime não tem o condão de prevenir o próprio crime ou a violência. Quando o Poder Judiciário é provocado na seara penal, já houve lesão ao bem jurídico, o que é, em si mesmo, inaceitável.(7) Assim, mais importante é prevenir, orientar, educar ou, em outros termos, impedir que se chegue a um trágico desfecho, não apenas mudando nossa herança histórico-cultural machista, mas instruindo novos cidadãos e cidadãs em busca de uma convivência harmônica.

Referências Bibliográficas

Anis. O impacto dos laudos periciais no julgamento de homicídio de mulheres em contexto de violência doméstica ou familiar no distrito federal. In: Figueiredo, I. S. de; Neme, C.; Lima, C. do S. L. (org.). *Homicídios no Brasil*: registro e fluxo de informações. Brasília: SENASP, 2013. v. 1, p. 143-193. (Coleção Pensando a Segurança Pública)

Belloque, J. G. Feminicídio: o equívoco do pretenso direito penal emancipador. *Boletim IBCCRIM*, São Paulo, n. 270, maio 2015.

Bianchini, A.; Gomes, L. F. *Feminicídio*: entenda as questões controvertidas da Lei 13.104/2015. Disponível em: <http://professorlfg.jusbrasil.com.br/artigos/173139525/feminicidio-entenda-as-questoes-controvertidas-da-lei-13104-2015>. Acesso em: 4 out. 2016.

Castilho, E. W. V. de. Sobre o feminicídio. *Boletim IBCCRIM*, São Paulo, n. 270, maio 2015.

Cerqueira, D.; Matos, M. V. M.; Martins, A. P. A.; Pinto Jr., J. *Avaliando a efetividade da Lei Maria da Penha*. Brasília: IPEA, 2015.

D'Elia, F. S. Feminicídio: uma via legal de proteção de gênero e de determinadas situações de vulnerabilidade. *Boletim IBCCRIM*, São Paulo, n. 272, jun. 2015.

Laurenzo-Copello, P. Apuntes sobre el feminicídio. *Revista de Derecho Penal y Criminologia*, 3ª Época, n. 8, p. 119-143, jul. 2012.

Machado, M.; Matsuda, F. Um copo meio cheio. *Boletim IBCCRIM*, São Paulo, n. 270, maio 2015.

Mello, A. R. de. *Feminicídio*: uma análise sociojurídica da violência contra a mulher no Brasil. Rio de Janeiro: LMJ Mundo Jurídico, 2016.

Nowak, M. Femicide: a global problem. *Small Arms Survey Research Notes*, Genebra, n. 14, p. 1-4, feb. 2012.

OACNUDH; ONU Mulheres. *Modelo de protocolo latino-americano de investigação das mortes violentas de mulheres por razões de gênero (femicídio/feminicídio)*. Brasília: OACNUDH e ONU Mulheres, 2014.

ONU Mulheres; SPM; SENASP. *Feminicídios*: diretrizes nacionais para investigar, processar e julgar com perspectiva de gênero as mortes violentas de mulheres. Brasília: ONU Mulheres, SPM e SENASP, 2016.

Radford, J.; Russell, D. E. H. *Feminicide*: the Politics of woman killing. New York: Twayne, 1992.

Senado Federal. *Relatório Final da Comissão Parlamentar Mista de Inquérito da Violência Contra a Mulher*. Brasília: Senado Federal, 2013.

Spinelli, B. Femicide in Europe. In: Academic Council on The United Nations System. *Femicide*: a global issue that demands action. 2. ed. Viena: ACUNS, 2013.

SRJ. *A violência doméstica fatal*: o problema do feminicídio íntimo no Brasil. Secretaria de Reforma do Judiciário (SRJ). Brasília: SRJ, 2015.

Waiselfisz, J. J. *Mapa da Violência 2015*: Homicídio de mulheres no Brasil. Brasília: SPM, ONU Mulheres e OPAS/OMS, 2015.

Notas

(1) Na doutrina, a classificação dos feminicídios inclui: íntimo, não íntimo, infantil, familiar, por conexão, sexual sistêmico, por prostituição ou ocupações estigmatizadas, por tráfico de pessoas, por contrabando de pessoas, transfóbico, lesbofóbico, racista, por mutilação genital feminina. Para a descrição destes, vide OACNUDH; ONU Mulheres, 2014, p. 20-22.

(2) A partir de 3 por 100 mil mulheres, a taxa pode ser considerada muito alta (Nowak, 2012, p. 1).

(3) Os achados referem-se à parte qualitativa da pesquisa em que foram analisadas 36 ações penais com trânsito em julgado, nas quais o crime foi cometido com violência doméstica ou familiar (Anis, 2013, p. 175). Lembrando que os dados do estudo são prévios à Lei do Feminicídio.

(4) Foram analisados 34 processos judiciais contemplando casos com data do fato anterior e posterior à Lei Maria da Penha (mas anteriores à Lei do Feminicídio). Por ser uma pesquisa qualitativa, os autores advertem que a análise deve ser considerada dentro do universo analisado, o que não impede que se apontem tendências gerais a partir do material empírico estudado (SRJ, 2015, p. 38-39).

(5) A maior inovação da Lei 13.104/2015 parece ter ocorrido na questão da vulnerabilidade, com a criação de uma nova situação de vulnerável: familiares das mulheres vítimas de homicídio que presenciam o crime (D'Elia, 2015) e não na criação da qualificadora de feminicídio e sua inclusão no rol de crimes hediondos.

(6) Em consulta à jurisprudência do Tribunal de Justiça do Distrito Federal e Territórios (TJDFT) – <http://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj> Termo da consulta: "feminicídio" –, verificou-se a ocorrência da expressão feminicídio em 23 acórdãos julgados desde julho de 2015 a setembro de 2016, o que, cotejado com os estudos do Anis (36 processos) e da SRJ (34 processos) aqui apresentados, poderia sinalizar uma maior visibilidade do fenômeno.

(7) É importante manter a crítica ao modelo punitivo, pois há que se considerar o conjunto dos problemas sociais trazidos pela prisão, os déficits de funcionamento desse sistema já tão inflado e as limitações das respostas por ele oferecidas (Machado; Matsuda, 2015).

Shana Schlottfeldt
Analista Legislativo da Câmara dos Deputados.
Membro do Comitê Gestor Pró-Equidade de Gênero e Raça da Câmara dos Deputados.
Doutora em Informática pela Universidade de Brasília.

ANEXO 3 - Crimes sexuais e violência de gênero contra mulheres na ditadura militar no Brasil

Teoria Geral do Direito Penal (UnB): SCHLOTTFELDT, Shana; ROCHA, Fernanda: ROCHA, Luana. Crimes sexuais e violência de gênero contra mulheres na ditadura militar no Brasil. In: TEIXEIRA, Érica Fernandes *et al*. (Org.). *Direitos Sociais*: reflexões e desdobramentos. 1. ed. Curitiba: Appris, 2019, p. 307-325. ISBN 978-85-473-2972-3

SCHLOTTFELDT, Shana; ROCHA, Fernanda; ROCHA, Luana. Crimes sexuais e violência de gênero contra mulheres na ditadura militar no Brasil. In: TEIXEIRA, Érica Fernandes *et al*. (Org.). *Direitos Sociais*: reflexões e desdobramentos. 1. ed. Curitiba: Appris, 2019, p. 307-325. ISBN 978-85-473-2972-3.

Crimes Sexuais e Violência de Gênero contra Mulheres na Ditadura Militar no Brasil

Shana Schlottfeldt[1]
Fernanda Rocha[2]
Luana Rocha[3]

RESUMO
O artigo trata a violência cometida contra mulheres na ditadura militar do Brasil sob uma perspectiva de gênero, em especial a violência sexual, uma vez que o modo de atuação do sistema repressivo buscava atingir as mulheres na essência de sua identidade feminina, explorando seu corpo, sua sexualidade, sua maternidade. A metodologia empregada utilizou levantamento bibliográfico. São abordadas a Lei de Abuso de Autoridade e a Lei de Tortura, evidenciando a dificuldade da mulher em acionar a justiça quando é vítima de violência como consequência da discriminação histórica, mas destacando a importância de investigar os crimes sexuais cometidos, pois se revestem das características de crimes de lesa-humanidade.
Palavras-chave: ditadura. violência de gênero. tortura. mulheres. crimes sexuais.

Introdução

A ditadura militar no Brasil (1964-1985) valeu-se do aparato estatal para impor seu plano de terror. A disputa era assimétrica, e a repressão governamental recorreu a métodos inclusive ilegais para aniquilar a oposição política, tais como restrição às mais diversas dimensões de liberdade (e.g., de expressão, de imprensa, de ir e vir), à violência e mesmo à tortura. Um dos recursos utilizados com o objetivo implícito e explícito de degradar, minar e destruir as vítimas foi a violência sexual[4].

---

[1] Analista Legislativo da Câmara dos Deputados. Membro do Comitê Gestor Pró-Equidade de Gênero e Raça da Câmara dos Deputados. Doutora em Informática pela Universidade de Brasília. Mestre em Informática pela Universidade Carlos III de Madrid. Graduanda em Direito pela Universidade de Brasília. shanass@unb.br.

[2] Graduanda em Direito pela Universidade de Brasília. fernandasiro@hotmail.com.

[3] Graduanda em Direito pela Universidade de Brasília. luanasiro@hotmail.com.

[4] BARRERA, F. El crimen de violación y violencia sexual en el derecho nacional e internacional. In: VASALLO, M. (Org.). *Grietas en el silencio*: una investigación sobre la violencia sexual en el marco del terrorismo de Estado. 1 ed. Rosario: Cladem, 2011, p. 141.

Em que pese o fato de ambos, mulheres e homens, terem sido vítimas de crimes sexuais durante o regime de exceção, o foco do presente artigo são os crimes sexuais contra mulheres cometidos por membros estatais (forças armadas, polícia civil, militar) durante a última ditadura militar no Brasil, uma vez que esse tipo de violência teve um impacto distinto sobre as mulheres quando comparadas aos homens.

A violência dirigida à mulher teve aspectos de tecnologia de gênero entendido como mecanismo capaz de selecionar, estigmatizar, construir e conformar corpos sexuados como femininos ou masculinos dentro de padrões e expectativas performáticas de gênero. Desta forma, como aponta Duque[5], o gênero aqui é entendido como "uma categoria analítica, construída discursivamente e capaz de criar, no plano fático, comportamentos e estigmas a mulheres".

O presente estudo está dividido em quatro seções. A primeira trata do contexto das mulheres à época da ditadura. Na segunda, é tratado o abuso de autoridade e de que forma o tema se relaciona aos crimes de gênero ocorridos no período da ditadura militar no Brasil. A terceira trata da Lei de Tortura, tecendo comentários de como seus resultados refletiram na dinâmica do enfrentamento da violência de gênero cometida na ditadura. Por fim, são apresentadas a conclusão e considerações finais acerca do tema.

1. Contexto das Mulheres na época da Ditadura

O período entre 1964 e 1985 no qual o Brasil esteve sob regime ditatorial foi uma fase nebulosa, cruel, covarde e injusta. Nebulosa porque todo o aparato estatal, principalmente o de repressão, encarnado nas polícias e forças armadas, regia um Estado "Democrático de Direito" de acordo com seus parâmetros próprios. Cruel, pois todos aqueles que não se encaixassem nesse Estado ou em qualquer medida não concordassem com ele, eram brutalmente rechaçados aos porões e celas das delegacias ou quarteis. Covarde por não haver equiparação/equidade de forças, sendo o abuso de autoridade e o excesso de força aplicados constantemente. Injusta porque não eram combatidas apenas as contestações políticas, mas também outras diferenças, como as ligadas ao gênero.

O cenário de inserção das mulheres no Brasil passou por inúmeras transformações entre as décadas de 60 e 70. Com a expansão do capitalismo, as mulheres passaram a ser

[5] DUQUE, A. P. del V. *Direito como tecnologia de gênero*: uma análise a partir dos relatos de tortura a mulheres pela ditadura civil-militar nos processos do Superior Tribunal Militar (1964-1979). 2015, 63 f. Monografia (Graduação em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília, 2015, p. 12.

requisitadas pelo mercado de trabalho, tendo que rapidamente se profissionalizar para atender às demandas da sociedade. A pílula anticoncepcional foi descoberta em 1960, causando enorme queda das taxas de natalidade. Ainda, neste mesmo período, as ondas libertárias introduziram o feminismo no mundo, que, àquela época, reivindicava, dentre outras demandas, a liberdade sexual, o direito ao próprio corpo, a politização do espaço privado[6].

Na década de 60, as feministas norte-americanas começam a criticar a separação entre as esferas (privada para as mulheres e a pública reservada aos homens), passando a denunciar o que acontecia no âmbito privado. O questionamento, denúncia e visualização das diferenças de tratamento e análise do público e do privado, representou uma mudança dos papéis designados aos sexos, numa tentativa de derrubar a barreira que separava a mulher da denúncia, da discussão e do diálogo político[7].

Em meio a mudanças significativas no processo de libertação da mulher, implantou-se a Ditadura no Brasil. Como explica a ex-militante Maria Amélia de Almeida Teles[8]:

> A censura foi adotada desde os primeiros dias da ditadura e se manteve durante todo o período ditatorial. Aliás, *a misoginia da ditadura andava de mãos dadas com a censura. Houve, de maneira especial, a censura aos assuntos referentes às mulheres, sob alegação da defesa da família, da moral e dos bons costumes*. (grifo nosso).

A conjuntura social do momento, na qual as mulheres eram cada vez mais independentes, desencadeou/evidenciou um sistema institucional misógino que era contra as conquistas das mulheres. Existia uma forte aversão às mulheres militantes, como se a mulher pertencesse ao ambiente doméstico, e somente a este, o que evidencia o relato de Ana Maria Gomes[9]:

> O sindicato foi invadido, nós fomos levadas para uma delegacia no bairro e depois para o DOPS. [...] No final do dia, fomos chamadas à sala do delegado. [...] eu não podia, evidentemente, dizer o que eu estava fazendo lá [no sindicato]. Então, eu disse que o meu irmão [...] começou a demorar muito para chegar em casa [...] e a gente supôs que ele estivesse no sindicato. [...] Nós recebemos um sermão. Ele [delegado] disse: *'vocês são moças, jovens, que provavelmente pretendem casar, constituir uma família, e fica muito mal, moças como vocês estarem frequentando sindicato, estarem metidas nesse tipo de coisa, então vocês vão para casa, tenham juízo e nunca mais se metam nessa' [...] É interessante ver em como você se coloca na tua condição de mulher e você consegue resistir a partir dessa condição que a sociedade te dá. Aí foi perfeito: nos enquadramos e pronto. E [é interessante ver] como ele também nos ameaçava com o perigo de não casar, com o perigo de não cumprir com aquilo que toda mulher sonha* (grifo nosso).

É perceptível, nessa época, que a mulher militante não era vista como "mulher honesta", digna de proteção. Os valores tradicionais, a ideia do papel da mulher como dona de

---

[6] TELES, M. A. de A. Violações dos direitos humanos das mulheres na ditadura. *Revista Estudos Feministas*, Florianópolis, v. 23, n. 3, p. 1001-1022, dez. 2015, p. 1005.

[7] CÁNAVES, V. Como la cigarra: notas sobre violencia sexual, jurisprudencia, y Derechos Humanos. *Revista Jurídica de la Universidad de Palermo*. v.12, n.1, p. 88-110, Oct. 2011, p. 89-90.

[8] Teles, 2015, p. 1006.

[9] COMISSÃO NACIONAL DA VERDADE. Capítulo 10: Violência sexual, violência de gênero e violência contra crianças e adolescentes. In: *Relatório da Comissão Nacional da Verdade*. v.1, Brasília: CNV, 2014, p. 405.

casa, que cuida do marido e dos filhos, estava muito presente naquela sociedade. Submissão, fraqueza, dependência, emoção, castidade, pudor, honra feminina, manutenção de valores e tradições familiares são exemplos desses estereótipos[10]. O papel social dos gêneros e suas expectativas sociais tiveram influência fundamental no tratamento dos supostos militantes. A mulher, que deveria permanecer virgem até casar-se, era condenada socialmente se praticasse relações sexuais fora do matrimônio. Paralelamente, o homem era incentivado a ter variadas relações sexuais para adquirir experiência[11].

Ainda que os homens também tenham sido vítimas de crimes sexuais no regime ditatorial, é perceptível diante dos relatos que as consequências, principalmente psicológicas, desta mesma prática nas vítimas do gênero feminino foram diferentes. A mulher, ensinada a praticamente inibir sua sexualidade, sentia enorme vergonha e humilhação por ter seu corpo violado[12].

Em meio a tudo isso, o feminismo brasileiro ganhou força e eclodiu nos anos 70, surgiu, sobretudo, como consequência da resistência das mulheres à ditadura. Implicava não apenas ser contra a ordem política vigente, mas uma transgressão ao que era designado na época como próprio das mulheres. As militantes negavam o lugar atribuído a elas, colocando em questão a virgindade, o casamento, se comportando "como homens", e contribuindo, dessa maneira, para a emancipação no reconhecimento da igualdade, pelo menos retoricamente[13].

As agressões sofridas pelas mulheres naquele período buscavam de alguma forma atingir aquilo que é identificado como mulher em nossa sociedade, como explica Sarti[14]:

> [...] em 1996, o espaço acadêmico se abriu para um evento eminentemente político que debatia a tortura durante a ditadura militar no Brasil. Nesse seminário, foi *discutida a presença da mulher como protagonista na resistência à ditadura e, pela primeira vez, como vítima de uma violência específica. Os depoimentos femininos foram contundentes em revelar um corpo ferido e torturado com base naquilo que identifica o ser mulher em nossa sociedade, dada a forma específica de violência a que a repressão submeteu as mulheres militantes. Elas foram atingidas não apenas sexualmente, mas também por uma manipulação do vínculo entre mãe e filhos*, uma vez que esse vínculo torna a mulher particularmente vulnerável e suscetível à dor (grifo nosso).

Foram estabelecidos dois estereótipos: o da mulher cuidadora e o da mulher honesta. No estereótipo da mulher cuidadora a ação dos agentes da ditadura se fundamentou na menção expressa a maus tratos a pessoas próximas, a partir da construção que se tem da mulher enquanto

---

[10] Idem, p. 401.

[11] ZURUTUZA, C. Crímenes sexuales en contextos concentracionarios: violencia, género, subjetividad. In: VASALLO, M. (Org.). *Grietas en el silencio*: una investigación sobre la violencia sexual en el marco del terrorismo de Estado. 1 ed. Rosario: Cladem, 2011, p. 82.

[12] COMISSÃO NACIONAL DA VERDADE, 2014, p. 415.

[13] SARTI, C. A. O feminismo brasileiro desde os anos 1970: revisitando uma trajetória. *Revista Estudos Feministas*, v. 12, n. 2, 2004, p. 37.

[14] Idem, p. 38.

alguém que deve zelar pelo cuidado com a família. O estereótipo da mulher honesta se baseou na construção da mulher respeitável, que tem sua sexualidade colocada sob ameaça, justamente pelo fato do valor da mulher, no mais das vezes, estar fundado em sua não sexualidade ou sexualidade contida, invisibilizada[15].

Percebe-se nitidamente a diferença e peculiaridade do tratamento dispensado pelos agentes do Estado às mulheres, e isso se reflete no tipo de violência utilizado contra elas. As agressões físicas e psicológicas aplicadas às mulheres eram, em sua maioria, de ordem sexual. Eram atos que transpareciam superioridade, poder, dominação, desprezo e discriminação. O objetivo não era "apenas" puni-las pelos supostos delitos cometidos, nem tentar conseguir informações, mas atribuir a elas um papel de submissão, ou seja, colocá-las no "seu lugar". As mulheres, principalmente as militantes, eram subjugadas por serem mulheres.

Os métodos de tortura, quando realizados em mulheres, visavam atingir o gênero feminino de forma singular ao explorarem: a maternidade, a tortura sexual científica, o aborto forçado, a separação dos filhos, a ameaça de tortura aos filhos, o corte de leite materno, além dos estupros (propriamente ditos) e atos libidinosos. Quanto a isso cabe esclarecer que a violência sexual ultrapassa o que se chamaria de estupro, pois além da penetração vaginal, anal e oral, também constituem violência sexual:

> [...] golpes nos seios; golpes no estômago para provocar aborto ou afetar a capacidade reprodutiva; introdução de objetos e/ou animais na vagina, pênis e/ou ânus; choque elétrico nos genitais; sexo oral; atos físicos humilhantes; andar ou desfilar nu ou seminu diante de homens e/ou mulheres; realizar tarefas nu ou seminu; maus-tratos verbais e xingamentos de cunho sexual; obrigar as pessoas a permanecer nuas ou seminuas e expô-las a amigos, familiares e/ou estranhos; ausência de intimidade ou privacidade no uso de banheiros; negar às mulheres artigos de higiene, especialmente durante o período menstrual e ameaças de violação sexual como as anteriormente mencionadas[16].

Por sua força e relevância, reproduzem-se, a seguir, alguns relatos de mulheres vítimas de violência na Ditadura militar conforme apresentados à Comissão Nacional da Verdade (CNV), o que exemplifica os variados tipos de violência praticados, tão particulares ao gênero mulher[17]:

> [...] Hoje, na minha compreensão feminista, eu entendo que *eles torturavam as crianças na frente das mulheres achando que nos desmontaríamos por causa da maternidade*. (Eliana Bellini Rolemberg).
> *Na questão da mulher, a coisa ficava pior* porque... quer dizer pior, era pior para todo mundo, não tinha melhor para ninguém, né? Mas [...] *existia uma intenção da humilhação enquanto mulher*. Então, o *choque na vagina, no ânus, nos mamilos, alicate no mamilo,* então... eram as coisas que eles faziam. *Muitas vezes, eu fui torturada junto com Celso Brambilla porque a gente sustentou a questão de ser noivo. Eles usaram*, obviamente, essa situação, *esse vínculo*, suposto vínculo, além da militância, *que seria um vínculo afetivo também, para tortura* [...] *Uma das coisas mais humilhantes, além dessas de choques na vagina, no ânus, no seio, foi que eu fui colocada em cima de uma mesa e fui obrigada a dançar para alguns policiais, nua.*

[15] DUQUE, 2015, p.13.

[16] COMISSÃO NACIONAL DA VERDADE, 2014, p. 419-420.

[17] Idem, p. 406-421.

> Enquanto isso, eles me davam choque. [...] Celso estava sendo torturado ao lado, também com choque elétrico, me vendo nessa situação (Márcia Bassetto Paes).
> Veio um enfermeiro logo depois, pra me dar uma *injeção pra cortar o leite*. [...] Então, *essa foi também uma das coisas horríveis, porque enquanto você tem o leite, você está ligada com o seu filho, né? Me deram uma injeção à força*, eu não quis tomar, briguei e tal, empurrei, aquela coisa [...] Ele me pegou à força e deu injeção aqui na frente, na frente da coxa [...]. Realmente, acabou o leite (Rose Nogueira).
> E a *ameaça maior* na Operação Bandeirantes e, depois, também no DOPS, *era de pegar minha filha. Eles [os agentes da repressão] usavam muito [esse tipo de ameaça]* [...] *Eu tinha pavor*. (Eliana Bellini Rolemberg).
> *Tive os meus filhos sequestrados e levados para sala de tortura*, na Operação Bandeirante. A Janaina com cinco anos e o Edson, com quatro anos de idade. [...] Inclusive, eu *sofri uma violência, ou várias violências sexuais. Toda nossa tortura era feita [com] as mulheres nuas [...] levando choques pelo corpo todo. Inclusive na vagina, no ânus, nos mamilos, nos ouvidos. E os meus filhos me viram dessa forma. Eu urinada, com fezes*. Enfim, o *meu filho chegou para mim e disse: "Mãe, por que você ficou azul e o pai ficou verde?". O pai estava saindo do estado de coma e eu estava azul de tanto... Aí que eu me dei conta: de tantos hematomas no corpo*. (Maria Amélia de Almeida Teles).
> Levaram a gente para aquela solitária, e aí eu comecei a sentir umas dores, umas dores absurdas [...] *Eu falei que estava com muita dor, cólica, não sabia o que estava acontecendo comigo, aí eles trouxeram dois comprimidos de AAS, que é absolutamente contraindicado para uma pessoa que está abortando*. O AAS, ele é facilitador do aborto, entendeu? *Aí, eu abortei completamente mesmo*. De qualquer forma, naquela situação, foi uma sorte. [...] não centrei nisso, de jeito nenhum [...] *Parece que eu tava assim, obnubilada*. (Rosa Maria Barros dos Santos). (grifo nosso)

As consequências foram muitas. Aos exílios, às cicatrizes (no corpo e na alma), à perda de pessoas queridas, à separação de filhos, associou-se a dor psicológica, os traumas e a certeza de que suas vidas nunca mais seriam as mesmas. Vejam-se os seguintes relatos[18]:

> Depois que eu saí, eu fiquei fechada, encerrada. Não queria saber de nada e nem de ninguém [...] Eu tinha perdido a linguagem verbal. Fiquei fechada [...]. Acabam com a sua vida e aí você tem que ver como é que você vai refazer o seu eu, para você ver que vida você quer ter, para onde você vai. Então, a primeira coisa foi que acabou tudo até recomeçar outra vez, mas nunca mais do [mesmo] jeito. A violência acaba com o ser humano. [...] A violência, ela impede, ela [...] interdita o movimento de crescer, então você regride, você fica todo encapsulado. (Roseli Lacerda).
> Como você lida com este ser que você sai depois que você é preso e torturado? Em que você fala mais ou menos, que você não morre, que você está aí e que você não aguenta enfrentar a morte. Como é que fica? Como você recompõe este ser humano? Como você volta a se respeitar? Como você acha que vale alguma coisa? Então este é um ponto muito complicado, difícil [...]. Não é algo que você resolve fácil. (Maria Aparecida Costa).

No que diz respeito às mulheres, as torturas que sofreram nesse período está ligada diretamente à questão de gênero. Aucía, Berterame e Zurutuza[19] citam decisão da Corte Interamericana de Direitos Humanos (CIDH) que defende não haver tortura neutra, dado que toda violência dirigida às mulheres constitui violência de gênero, pois ataca a mulher em sua identidade:

> […] não existe tortura que não leve em conta o gênero da vítima. Não existe […] tortura "neutra" […]. Mesmo quando uma forma de tortura não seja "específica" para a mulher […] seus efeitos terão, sim, especificidades próprias na mulher […] ainda que nem toda forma de violência nesse caso tenha sido específica das mulheres, […] constituiu violência de gênero, pois estava dirigida […] a atacar a identidade feminina (tradução livre).

Assim, partindo do pressuposto que a violência contra as mulheres compreende por si só um crime de gênero e, tendo em vista as torturas praticadas pelos agentes estatais na Ditadura

[18] Ibidem, p. 428.

[19] AUCÍA, A.; BERTERAME, M. C.; ZURUTUZA, M. C. Te volvieron a violar: terrorismo violencia sexual y justicia. *IV Seminario de Políticas de la Memoria, Centro Cultural de la Memoria Haroldo Conti*. Buenos Aires, 2011, p. 4.

militar brasileira, pode-se afirmar que os abusos cometidos, físicos, psicológicos, sexuais ou não, constituem violência de gênero.

A violência sexual é uma manifestação extrema de discriminação contra as mulheres, e sua utilização por parte do poder estatal é consequência da percepção no que diz respeito às mulheres e seus papéis no contexto sociocultural da época.

2. Abuso de Autoridade (Lei nº 4.898/65) e os crimes de gênero na ditadura

A análise do ordenamento jurídico à época da Ditadura Militar no Brasil e sua relação com o gênero – mais especificamente, no caso deste estudo, com a mulher –, faz-se importante devido ao número significativo e o valor substancial do papel feminino no combate ao regime: do total de presos, 20% eram mulheres[20,21].

Com a promulgação do Ato Institucional nº 2 (AI-2), em 1965, são criados os Inquéritos Policiais Militares (IPM), base fundamental das investigações e processos apresentados pela polícia, pois tinham como princípio norteador indicar todos aqueles ligados a atividades consideradas subversivas[22]. Nesses inquéritos era patente a falta de observância dos direitos e garantias fundamentais, ademais, eram carregados de lacunas fáticas – muitas vezes, "contrárias às leis da Física" ou ao "bom senso":

> O IPM [inquérito policial militar] concluiu, de forma absurda, que o morto teria disparado alguns tiros antes de embrulhar uma das armas na colcha que o cobria para abafar o tiro que daria em sua própria cabeça. O laudo necroscópico, assinado por Octávio D'Andréa e Orlando Brandão, confirma o suicídio[23].

Em 1965 é promulgada a Lei nº 4.898/1965, que "regula o Direito de Representação e o processo de Responsabilidade Administrativa Civil e Penal, nos casos de abuso de autoridade" (Lei de Abuso de Autoridade).

Um momento de partida ideal é a promulgação do AI-5, em 1968, um marco legal que representou um grande retrocesso em matéria de direitos e aumento feroz da repressão, como se depreende da fala de Adriano Codato[24]: "O ano de 1964 só se consuma politicamente em 1968". Já no ano seguinte, são criados os Destacamentos de Operações de Informações - Centro

[20] ABREU, A. A. Quando eles eram jovens revolucionários. In: VIANNA, Hermano. (Org.). *Galeras Cariocas*: territórios de conflitos e encontros culturais. Rio de Janeiro: UFRJ, 1997, p. 192.

[21] TELES, A. Introdução: Mulheres e crianças inimigas do Estado. In: *Relatório da Comissão Nacional da Verdade*. v.1, Brasília: CNV, 2014, p. 14.

[22] ALVES, M. H. M. *Estado e Oposição no Brasil*: 164-1984. Bauru: Edusc, 2005, p. 69.

[23] COMISSÃO NACIONAL DA VERDADE, 2014, p. 473.

[24] CODATO, A. N. O Golpe de 1964 e o Regime de 1968: aspectos conjunturais e variáveis históricas. *História. Questões & Debates*, Curitiba, v. 40, 2004, p. 12

de Operações de Defesa Interna (DOI-CODIs), instrumentos dedicados ao estabelecimento de uma inteligência na busca de informações e repressão aos contrários ao Regime[25].

Intrinsecamente relacionada à questão estava a utilização, desde o início do regime militar, de instrumentos excepcionais que reduziam ou suprimiam o direito de defesa dos acusados de crimes cometidos contra a "segurança nacional". Com vistas à eliminação da subversão interna de esquerda e ao restabelecimento da "ordem" no país, o regime instalado em 1964 classificava de inimigos do Estado todos os que se opunham às suas ideias. No processo repressivo, não economizou punições e extrapolou na violência. A pena de morte, estabelecida pelo AI-14, oficialmente nunca foi utilizada, pois na eliminação de seus adversários, o governo optou por execuções sumárias ou no decorrer de sessões de torturas, sempre às escuras.

Mediante esse aparelho repressivo, os "inimigos" do regime eram submetidos a torturas de forma dual: física, com viés momentâneo; e psicológica, tendo em vista a desestruturação psíquica total da vítima [26]. O regime Ditatorial Militar no Brasil institucionalizou sistemas capazes de produzir e disseminar, deliberadamente, o terror, o que fazia a população refém de um estado de medo permanente.

Há vários relatos que demonstram que a Lei de Abuso de Autoridade não se aplicava aos casos concretos:

> [...] o delegado de plantão [...] afirmou, na presença [do] presidente da Ordem dos Advogados do Brasil, seccional de São Paulo (OAB/SP), não saber o motivo das prisões de Dallari e Dias, nem de quem partiram as ordens. Dallari exigiu ser solto e acusou o delegado de cometer crime de abuso de autoridade. [O delegado] respondeu que 'a polícia prendia quem e quando quisesse', e mandou o presidente da OAB/SP se retirar[27].
> Morava em São Paulo quando os policiais federais chegaram e disseram que eu deveria acompanhá-los até o 3º Batalhão de Caçadores para prestar depoimento. O depoimento durou dois meses[28].

O abuso de autoridade, particularmente no que diz respeito às mulheres, tinha um caráter simbólico, carregado de rótulos patriarcais e machistas, reprodutor do "estereótipo da mulher restrita ao espaço privado e doméstico, enquanto mãe, esposa, irmã e dona de casa, que vive em função do mundo masculino"[29].

[25] GASPARI, E. *A ditadura escancarada*. São Paulo: Companhia das Letras, 2002.

[26] ARNS, P. E. *Brasil*: nunca mais. Petrópolis: Vozes, 1985.

[27] COMISSÃO NACIONAL DA VERDADE, 2014, p. 312.

[28] VALFRÉ, V. Violência sexual ao interrogar mulheres durante Ditadura Militar. *Gazeta Online*. Vitória. 24 mar. 2014. Disponível em: <http://www.gazetaonline.com.br/_conteudo/2014/03/noticias/cidades/1482632-violencia-sexual-ao-interrogar-mulheres-durante-ditadura-militar.html>. Acesso em: 23 mai. 2017.

[29] RIDENTI, M. S. As mulheres na política brasileira: os anos de chumbo. *Tempo Social*, Brasil, v. 2, n. 2, dez. 1990. Disponível em: <http://www.revistas.usp.br/ts/article/view/84806>. Acesso em: 22 mai. 2017. p. 114.

Essa carga fomentava o abuso, no sentido que considerava que a mulher militante estava cometendo delito em duas instâncias: política, por ir contra o ordenamento político; e social, por lutar contra sua condição de dona do lar.

> Uma das vítimas entrevistada lembrou-se que "o diretor da prisão [...] gritava: '*Assassinas, guerrilheiras, putas'* " […]. Nesta expressão percebe-se claramente a *referência a conotações políticas – guerrillera – e à transgressão de estereótipos femininos – mulher decente ou sexualmente casta -, com a expressão putas*[30]. (tradução livre, grifo nosso).
> *O simples fato, eu acho, de você estar no meio de homens, só homens. Só homens que têm sobre você um olhar*, como eu diria? É o olhar que te... *Pelo fato de você ser mulher, também você percebe que há talvez, às vezes, uma raiva muito maior, eu não sei se é pela questão de achar "por que uma mulher está fazendo isso? Por que uma moça está fazendo isso?" E é uma forma, talvez, muito de querer te desqualificar de todas as maneiras*. Inclusive, *o mínimo que você ouve é que você é uma "vaca"***.** [...] você enfim, se encontra diante deles de uma dupla maneira: *você está inteiramente nas mãos enquanto ser humano e na tua condição feminina você está nu*, você está à mercê, não é? Disso tudo. [...] Como os homens também foram, mas talvez, *por ser uma mulher, eu acho que isso tem um peso terrível*. Pela tua formação, pela formação social, ideológica. Por si já é uma exposição e aumenta ainda mais a tua exposição [...] *Normalmente você é educado e visto para proteger a sua feminilidade para que ela se exponha em outras situações* [...] de escolha[31] (grifo nosso).

Essa violência, carregada do simbolismo inerente à violência e identidade de gênero, são destacadas no Relatório da CNV[32]:

> Inserida na lógica da tortura e estruturada na hierarquia de gênero e sexualidade, a violência sexual relatada por sobreviventes da ditadura militar *constitui abuso de poder não apenas se considerarmos poder como a faculdade ou a possibilidade do agente estatal infligir sofrimento, mas também a permissão (explícita ou não) para fazê-lo*. Foi assim que rotineiramente, nos espaços em que a *tortura tornou-se um meio de exercício de poder e dominação total, a feminilidade e a masculinidade foram mobilizadas para perpetrar a violência, rompendo todos os limites da dignidade humana*. Nesse espaço desempoderado, os perseguidos políticos tiveram seus corpos encaixados na condição de prisioneiras e prisioneiros. *No exercício da violência, mulheres foram instaladas em loci de identidades femininas tidas como ilegítimas (prostituta, adúltera, esposa desviante de seu papel, mãe desvirtuada etc.), ao mesmo tempo que foram tratadas a partir de categorias construídas como masculinas: força e resistência físicas*. Nesses mesmos espaços de violência absoluta, também foi possível feminilizar ou emascular homem (grifo nosso).

Nesse contexto, observa-se que o abuso de autoridade dos agentes do Estado para com as mulheres tinha um viés bem diferente do simplesmente agir com maior ênfase no cumprimento de seus deveres de polícia. O abuso de autoridade foi uma ferramenta utilizada para dominar as almas e os corpos das mulheres que se revoltaram contra o sistema repressor. Essa prática, ao mesmo tempo em que provocava maior confiança de superioridade aos agentes repressores, era usada (conscientemente ou não) para reprimir as vítimas fazendo-as se sentirem insignificantes, confusas e frágeis.

3. Lei de Tortura

[30] AUCÍA, BERTERAME, ZURUTUZA, 2011, p. 3.

[31] COMISSÃO NACIONAL DA VERDADE, 2014, p. 404.

[32] Idem, 2014, p. 402.

Historicamente, a tortura aplicada de maneira sistemática é uma prática de punição que envolve castigos físicos e/ou psicológicos. Apesar de ser utilizada desde tempos antigos, por povos como os romanos, seu emprego foi disseminado de forma sistemática durante a Inquisição, na Idade Média, período em que a Igreja estabeleceu inúmeras punições aos "hereges" associadas a julgamentos totalmente arbitrários, não havendo praticamente nenhuma garantia para os presos.

Com a ascensão de movimentos libertários no século XVIII, estas práticas começaram a ser de fato proibidas. No entanto, a tortura voltou de maneira contundente durante as Guerras Mundiais do século XX. Como reação a tais acontecimentos, no período pós Segunda Guerra Mundial, foram criados os tratados internacionais de direitos humanos na tentativa de evitar que estas atrocidades se repetissem. Porém, mesmo assim, a tortura voltou a ser utilizada sistematicamente durante os períodos autoritários ditatoriais que se espalharam pela América Latina (e mesmo outras partes do mundo, como Portugal de Salazar e a Espanha do General Franco).

A Constituição Federal de 1998 (CF/88), em seus incisos III e XLIII, do art. 5º, assim trata a tortura:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País *a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes*:
> [...]
> III - *ninguém será submetido a tortura nem a tratamento desumano ou degradante*;
> [...]
> XLIII - *a lei considerará crimes inafiançáveis e insuscetíveis de graça ou anistia a prática da tortura*, o tráfico ilícito de entorpecentes e drogas afins, o terrorismo e os definidos como crimes hediondos, por eles respondendo os mandantes, os executores e os que, podendo evitá-los, se omitirem; (grifo nosso)

A Lei nº 8.072/1990, que "dispõe sobre os crimes hediondos, nos termos do art. 5º, inciso XLIII, da Constituição Federal, e determina outras providências", dá tratamento à tortura semelhante ao de crimes hediondos no que diz respeito à vedação de extinção da punibilidade (anistia, graça e indulto) e quanto ao regime prisional, sem, contudo, incluí-la no rol de crimes hediondos.

Nove anos após a promulgação da CF/88, entra em vigor a Lei nº 9.455/1997 (Lei de Tortura), que define no ordenamento jurídico brasileiro o crime de tortura.

A tortura é então definida como a prática que condiciona a pessoa a um intenso sofrimento físico ou mental. Adotou-se uma definição mais breve e menos abrangente do que a da Convenção Interamericana para Punir e Prevenir a Tortura, ratificada pelo Brasil em 1989.

Na Lei nº 9.455/1997, além da tipificação do crime de tortura em si (art. 1º, I, II, e §1º), há vários aspectos a serem destacados: as qualificadoras para tortura praticada por agente público (art. 1º, §4º, I) e quando resulta lesão corporal (art. 1º, §3º); a responsabilização por omissão (art. 1º, §2º); a vedação de extinção da punibilidade (art. 1º, §6º); e o regime prisional

(art. 1º, §7º). O inciso II, e o §1º, ambos do art.1°, da Lei de Tortura, de certa forma complementaram o art. 136 do Decreto-lei nº 2.848/1940 (Código Penal) que versa sobre maus-tratos.

Não há uma definição específica para os crimes sexuais praticados por agentes de Estado como prática de tortura. Assim, as vítimas de tais delitos estariam sujeitas aos artigos comuns sobre crimes sexuais do Código Penal, ou à Lei de Tortura por uma interpretação extensiva (o que é evitado em Direito Penal).

Ora, é difícil saber o que pode ser abarcado pelos incisos I e II do art. 1º da Lei de Tortura, devido à vaga expressão utilizada: "intenso sofrimento físico ou mental", o que dificulta até mesmo a diferenciação entre maus-tratos e tortura. Abre-se, assim, espaço para a arbitrariedade do juiz[33]. Não há uma garantia de que as vítimas de violência de gênero serão protegidas pela Lei, levando em conta os variados tipos de violência praticada na Ditadura, que se entende deveriam ser explicitamente "lembrados" pela legislação.

Se não alcançados pela Lei de Tortura, os agentes públicos que cometem crimes sexuais (diferente dos abarcados pelos crimes hediondos) dentro das repartições não estarão sujeitos à condição de crime inafiançável e insuscetível de graça ou anistia que é atribuída à prática da tortura.

Em análise comparativa com o direito internacional, entende-se que seria apropriado tratar os crimes de violência sexual como crimes autônomos, dado seu caráter de crimes contra a humanidade, pois possuem um significado simbólico e material distintos da "simples" tortura (se é que se pode chamar a tortura de simples). Como Aucía et al.[34] bem colocam:

> [...] de certa forma, todo o contexto concentracionário esteve cingido pela sexualidade, o que dificulta uma análise mais pormenorizada. Ainda assim, dificulta um dos objetivos deste estudo: diferenciar a violência sexual da tortura. Porque em outro sentido, a violência sexual teve um fim específico, em si mesma, que foi a própria satisfação do repressor, do torturador. Satisfação que, por sua vez, tem arestas complexas. Sabe-se que os estupros (ainda que fora dos campos de concentração) buscavam um prazer sexual cingido pela sensação de dominar e humilhar a vítima, a afirmação de um poder que nesse momento é total sobre outro corpo-sujeito sexuado/a. Implica impor-lhe condutas sobre seu corpo e seus genitais que dão prazer ao vitimador e dor (física e/ou emocional) à vítima. É invadir aspectos privados e íntimos para um prazer violento e sexualizado (tradução livre).

Porém, mesmo que não se considere ideal, incluir explicitamente os crimes sexuais na tortura já seria um avanço no sentido de coibir as práticas de discriminação contra a mulher, principalmente em relação à simbologia que esta inclusão acarretaria[35].

---

[33] MACHADO, N. J. de M. Da tortura: aspectos conceituais e normativos. *Revista do Conselho da Justiça Federal*. Brasília, n. 14, mai./ago. 2001, p. 19.

[34] AUCÍA, A. et al. *Grietas en el silencio*: una investigación sobre la violencia sexual en el marco del terrorismo de Estado. 1 ed. Rosario: Cladem, 2011, p. 90-91.

[35] CÁNAVES, 2011, p. 109.

Ademais, para uma garantia de direitos, dado o caráter particular em que a violência sexual de gênero opera, entende-se que poderia ser discutida a sua caracterização como imprescritível (à semelhança do tratamento dado pela legislação supranacional ao crime sexual quando caracterizado como de lesa-humanidade). É muito comum, principalmente quando os atos são de ordem sexual, as vítimas dos regimes ditatoriais permanecerem em silêncio por muitos anos. Até porque muitas vítimas demoram a reconhecer que sofreram violência sexual, seja por negação, seja por acreditarem que apenas a "conjunção carnal" (penetração) configura esse tipo de violência:

> Eu sofri abuso sexual dentro do banheiro [...]. Mas eu levei muito tempo para me tocar que aquilo era abuso sexual, sabe por quê? Eu minimizava aquele episódio porque, afinal, não era pau de arara, não era choque e não era cadeira do dragão. É muito louco isso![36].

4. Conclusão e Considerações Finais

Não há como falar da ditadura militar no Brasil, da repressão, da tortura, sem falar das mulheres. Elas tiveram uma participação ativa nos movimentos pela democracia e contra a ditadura, basta lembrar que do total de presos do regime militar, 20% eram mulheres e do total de mortos e desaparecidos que tiveram seus nomes registrados, cerca de 11% são mulheres[37].

Não há dúvidas que as violações de direitos humanos cometidas contra as mulheres pela ditadura devem ser consideradas sob a ótica de gênero. As mulheres foram humilhadas, sofreram violência física, mental, psicológica com requintes de crueldade que buscavam atingi-las na essência de sua identidade feminina; ser mulher e ativista era considerado algo censurado e subversivo. Os crimes sexuais praticados durante a ditadura são tão graves como outras formas de tortura institucionalizadas à época, como choques elétricos, pau-de-arara, espancamentos, "afogamentos".

Essa violência era cometida por agentes do Governo (militares e policiais), com a utilização do aparato do Estado, numa assimetria de poder focada em combater um "inimigo interno" em nome da "segurança nacional", gerando uma verdadeira guerra oculta, velada (às vezes nem tanto).

Uma das principais preocupações apontadas neste trabalho é a dificuldade da mulher em acionar a justiça quando é vítima de violência como consequência da discriminação histórica. Se atualmente, após diversas conquistas das mulheres, elas ainda são questionadas quanto a sua credibilidade, imagine-se na época da ditadura, quando associada a uma sociedade que clamava pelos valores tradicionais, havia a questão do aparato Estatal que tudo justificava

[36] COMISSÃO NACIONAL DA VERDADE, 2014, p. 418-419.

[37] TELES, 2014, p.14.

em nome da pretensa "segurança nacional". A mulher militante já era, desde logo, classificada como merecedora da violência que sofria, pelo simples fato de "estar ocupando um lugar que não lhe pertencia".

A Comissão Nacional da Verdade mobilizou a opinião pública para as graves violações de direitos humanos ocorridas no regime militar, foi um primeiro passo, mas se está longe de oferecer condições adequadas e oportunidades para uma narrativa pública sobre o estupro e demais violências cometidas contra mulheres. Basta dizer que, ainda hoje, a maioria dos atos de violência contra as mulheres (seja em que contexto for) ficam na impunidade, perpetuando a aceitação social desse fenômeno.

Apesar das grandes conquistas alcançadas nas últimas décadas, entende-se que ainda há passos importantes a serem dados visando à plena garantia dos direitos da mulher:

1. É premente que se investigue e apurem responsabilidades dos agentes públicos inclusive nos crimes sexuais;
2. É preciso expandir, no Brasil, a codificação dos crimes de violência sexual, criando um marco jurídico-legal que reconheça o estupro e outras violências sexuais como crime autônomo, independente dos demais crimes cometidos na ditadura, ainda que todos tenham sido praticados por agentes públicos e, portanto, considerados crimes contra a humanidade, o que os tornaria imprescritíveis (posicionamento para o qual seria possível buscar suporte na legislação supranacional);
3. É fundamental tornar explícito o extrato de gênero existente em crimes de tal natureza, de modo a dar o trato legal mais apropriado para tais situações, adequando-os às suas características únicas.

REFERÊNCIAS

ABREU, A. A. "Quando eles eram jovens revolucionários". In: VIANNA, Hermano. (Org.). *Galeras Cariocas*: territórios de conflitos e encontros culturais. Rio de Janeiro: UFRJ, 1997.

ALVES, M. H. M. *Estado e Oposição no Brasil*: 164-1984. Bauru: Edusc, 2005.

ARNS, P. E. *Brasil*: nunca mais. Petrópolis: Vozes, 1985.

AUCÍA, A.; BERTERAME, M. C.; ZURUTUZA, M. C. "Te volvieron a violar: terrorismo violencia sexual y justicia". *IV Seminario de Políticas de la Memoria, Centro Cultural de la Memoria Haroldo Conti*. Buenos Aires, 2011.

BARRERA, F. "El crimen de violación y violencia sexual en el derecho nacional e internacional". In: VASALLO, M. (Org.). *Grietas en el silencio*: una investigación sobre la violencia sexual en el marco del terrorismo de Estado. 1 ed. Rosario: Cladem, 2011, p. 141-162.

CODATO, A. N. "O Golpe de 1964 e o Regime de 1968: aspectos conjunturais e variáveis históricas". *História. Questões & Debates*, Curitiba, v. 40, p.11-36, 2004.

COMISSÃO NACIONAL DA VERDADE. "Capítulo 10: Violência sexual, violência de gênero e violência contra crianças e adolescentes". In: *Relatório da Comissão Nacional da Verdade*. v.1, Brasília: CNV, 2014. p. 399-435.

DUQUE, A. P. del V. *Direito como tecnologia de gênero*: uma análise a partir dos relatos de tortura a mulheres pela ditadura civil-militar nos processos do Superior Tribunal Militar (1964-1979). 2015, 63 f. Monografia (Graduação em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília, 2015.

GASPARI, E. *A ditadura escancarada*. São Paulo: Companhia das Letras, 2002.

MACHADO, N. J. de M. "Da tortura: aspectos conceituais e normativos". *Revista do Conselho da Justiça Federal*. Brasília, n. 14, p. 14-22, mai./ago. 2001.

RIDENTI, M. S. "As mulheres na política brasileira: os anos de chumbo". *Tempo Social*, Brasil, v. 2, n. 2, p. 113-128, dez. 1990. Disponível em: <http://www.revistas.usp.br/ts/article/view/84806>. Acesso em: 22 mai. 2016.

SARTI, C. A. "O feminismo brasileiro desde os anos 1970: revisitando uma trajetória". Estudos Feministas. *Revista Estudos Feministas*, v. 12, n. 2, p. 35-50, 2004.

TELES, A. "Introdução: Mulheres e crianças inimigas do Estado". In: *Relatório da Comissão Nacional da Verdade*. v.1, Brasília: CNV, 2014. p. 13-20.

TELES, M. A. de A. "Violações dos direitos humanos das mulheres na ditadura". *Revista Estudos Feministas*, Florianópolis, v. 23, n. 3, p. 1001-1022, dez. 2015.

VALFRÉ, V. "Violência sexual ao interrogar mulheres durante Ditadura Militar". *Gazeta Online*. Vitória. 24 mar. 2014. Disponível em: <http://www.gazetaonline.com.br/_conteudo/2014/03/noticias/cidades/1482632-violencia-sexual-ao-interrogar-mulheres-durante-ditadura-militar.html>. Acesso em: 23 mai. 2016.

ZURUTUZA, C. "Crimenes sexuales en contextos concentracionarios: violencia, gênero, subjetividad". In: VASALLO, M. (Org.). *Grietas en el silencio*: una investigación sobre la violencia sexual en el marco del terrorismo de Estado. 1 ed. Rosario: Cladem, 2011, p. 69-114.

ANEXO 4 - Facial Recognition, Law Enforcement and the Identity-Australian Matching Services (IMS) Bill

Information Law (ANU): SCHLOTTFELDT, Shana. Facial Recognition, Law Enforcement and the Identity-Australian Matching Services (IMS) Bill. *Revista dos Estudantes de Direito da Universidade de Brasília*, v. 1, p. 343-357, 2020. Disponível em: https://periodicos.unb.br/index.php/redunb/article/view/30375/27955. ISSN impresso: 1981-9684 / ISSN eletrônico: 2177-6458.

Revista dos Estudantes de Direito da Universidade de Brasília; 18ª edição

FACIAL RECOGNITION, LAW ENFORCEMENT AND THE IDENTITY-AUSTRALIAN MATCHING SERVICES ('IMS') BILL

RECONHECIMENTO FACIAL, APLICAÇÃO DA LEI E O PROJETO DE LEI IDENTITY-MACHING SERVICE (IMS) AUSTRALIANO

Shana Schlottfeldt[1]

Abstract: This paper focus on the use of facial recognition technology ('FRT') by Australian government for the purpose of law enforcement. The use of FRT to law enforcement presents several challenges (risks) for which there are no easy solutions, but that need to be recognized more broadly, such as the lack of accuracy, bias, impact on civil liberties (privacy), security risks. This research has a qualitative nature and was developed through bibliographic research. Part I describes how FRT works and its risks. Part II makes considerations on the employment of FRT in Australia to identity-matching. Part III talks about the Identity Matching Services ('IMS') Bill, introduced in 2018 to facilitate the sharing of identification information (including facial images) within the government; this legislation lapsed on the dissolution of parliament and, as will be discussed, at least how it is now, it should not be revived.

Keywords: Biometrics. Facial recognition. Identity matching. Human rights. Australia.

1 Ph.D. in Informatics from University of Brasília. M.S. in Informatics from Universidad Carlos III de Madrid. LLB exchange student at Australian National University. LLB student at University of Brasília.

Resumo: Este artigo enfoca o uso da tecnologia de reconhecimento facial (FRT) pelo governo australiano para fins de aplicação da lei. O uso da FRT para aplicação da lei apresenta vários desafios (riscos) para os quais não há solução fácil, mas que precisam ser reconhecidos de forma mais ampla, e.g., falta de precisão, preconceito, impacto nas liberdades civis (privacidade) e riscos de segurança. Esta pesquisa possui natureza qualitativa e foi desenvolvida ao por meio de pesquisa bibliográfica. A Seção I descreve como a FRT funciona e seus riscos. A Seção II faz considerações sobre o emprego da FRT na Austrália para fins identificação. A Seção III fala sobre o Projeto de Lei "Identity Matching Services" (IMS), lançado em 2018 para facilitar o compartilhamento de informações de identificação (incluindo imagens faciais) dentro do governo; essa legislação caducou com a dissolução do parlamento e, como será discutido, pelo menos como está agora, não deve ser reapresentada.
Palavras-chave: Biometria. Reconhecimento facial. Identificação. Direitos humanos. Australia.

Submissão: 29/03/2020
Aceite: 27/06/2020

INTRODUCTION

The use of biometrics in law enforcement investigation and other applications has significantly increased in the last few years (LYON, 2008, p. 500). According to the International Standards Organisation, *biometric recognition* is the 'automated recognition of individuals based on their biological and behavioural characteristics', (e.g., fingerprint, DNA, eye retina and irises, voice, facial image, gait and keystroke patterns); and *automated recognition* 'implies that a machine-based system is used for the recognition, either for the full process or assisted by a human being'(ISO/IEC, 2017). In this sense, *facial recognition technology* ('FRT') is the automated process of one-to-many 'matching' faces to determine whether they represent the same individual, utilizing biometric scanning technologies and algorithms (BIOMETRICS GROUP, 2019, p.1; GARVIE, BEDOYA, FRANKLE, 2016, p. 116).

This paper focus on the use of FRT by government for the purpose of law enforcement. Part I describes how FRT works and its risks. Part II makes considerations on the employment of FRT in Australia to identity-matching. Part III talks about the Identity Matching Services ('IMS') Bill, introduced in 2018 to facilitate the sharing of identification information (including facial images) within the government; this legislation lapsed on the dissolution of parliament and, as will be discussed, at least how it is now, it should not be revived.

I HOW DOES FRT WORK AND WHAT ARE THE RISKS?

FRT generally performs at least one of three things (LYNCH, 2018, p. 5-6):

• Identify an unknown person (e.g., from a surveillance camera footage).

• Confirm the identity of a known person (e.g., to unlock a smartphone).

• Look for multiple specific, previously-identified faces (e.g. wanted persons on a subway platform, shoppers in a store, card counters at a casino).

In order to identify an individual, the algorithm proceeds through the following steps (GARVIE, BEDOYA, FRANKLE, 2016, p. 9, 46; ADLER, SCHUCKERS, 2007, 1248-49; RICANEK, BOEHNEN, 2012, p. 95; LYNCH, 2018, p. 4-6; WOODWARD JR et al, 2003, p. 3-4):

• Face detection: find the person within the photo or video segment.

• Normalization: once detected, the face is scaled, rotated and aligned, in order to be easier for the algorithm to compare the images at the 'same position'.

• Extraction of features: attributes that can be numerically quantified (e.g., skin texture, eye distance, shape of chin) are identified. FRT records not the face itself, but the spatial geometry of distinguishing features of the face.

• Pair comparison: the algorithm check pairs of faces (the image is compared to other faces previously collected and stored in a repository) and returns a numerical score indicating their features similarity.

As can be apprehended, FRT is intrinsically probabilistic. Its output is not a binary answer, but a probability match score between the searched face and faces stored in a database. Generally, FRT will return those photos above a similarity threshold, ranked in likelihood order of correct identification (LYNCH, 2018, p. 6).

The use of FRT to law enforcement presents several challenges (risks) for which there are no easy solutions, but that need to be recognized more broadly. Following, we approach some of them.

A ACCURACY

FRT is less accurate than, for instance, fingerprinting, especially when used in real-time or on large databases (GARVIE, BEDOYA, FRANKLE, 2016, p. 3, 46). Several factors influence a match probability/accuracy, such as (BIOMETRICS GROUP, 2019, p. 2; HAMANN, SMITH, 2019):

• The quality of the images (lighting, background, resolution, angle, facial expression, etc.).

• The environmental conditions where the image is captured (lighting, camera position, etc.).

• The size of the watchlist (dataset).

• The thresholds of match.

• The changes face suffers over time (e.g., body weight, facial hair, hairstyle, and the effects of aging).

• A near real-time response or not.

• If there is human action after machine-generated biometric match, and if this person is trained. It has been shown to be beneficial that human double-check the results of FRT, but, without specialized training, in half of the time, human users make the wrong decision about a match (WHITE et al, 2015, p. 6).

Since FRT vary in its ability to identify people, it should report its rate of errors, i.e., the number of false positives (aka 'false accept rate') and false negatives (aka 'false reject rate'), which not always happens (LYNCH, 2018, p. 6).

B. BIAS

Worries with efficacy extend to ethical considerations (INTRONA, NISSEMBAUM, 2009, p. 72). Concerns about potential gender and racial bias within FRT have already been raised (BOULAMWINI, GEBRU, 2018, p. 2-3). Pairs of photos of the same person are presented to the FRT algorithm during training; over time, the algorithm learns 'to concentrate' on the most relevant features. If a training dataset is composed by more samples representing a certain group, the algorithm may learn to better identify members of that group (GARVIE, BEDOYA, FRANKLE, 2016, p. 9). This is behaviour similar to the 'other-race effect', a phenomenon in which people have difficulty telling apart individuals of a different race to their own (ANU, 2019; McKONE et al., p. 1). Studies have shown that FRT misidentified 'people of colour and ethnic minorities, young people, and women' at higher rates than 'whites, older people, and men' (BOULAMWINI, GEBRU, 2018, p. 2-3; BIOMETRICS GROUP, 2019, p. 2). The formers, trigger more false positive recognition, and this kind of inaccuracy has impact on the 'presumption of innocence' by placing on them, the onus to show that they are not who the FRT identifies (LYNCH, 2018, p. 10).

C. IMPACT ON CIVIL LIBERTIES (PRIVACY)

Most of the technology used to track a person aim at belongings, e.g., cell phone, car, and computer. FRT takes tracking to a new level, they 'pursue' the person's body. The distinction is meaningful: you can dispose of your belongings, although your face… (GARVIE, BEDOYA, FRANKLE, 2016, p. 9). Furthermore, FRT can be more invasive than other forms of biometric identification (MANN, SMITH, 2017, p. 125): they can do the tracking remotely, in secrecy, and on a great amount of people (WOODWARD JR et al., 2003, p. 3-4).

Moreover, agencies are targeting to add 'crowd, closed circuit television ('CCTV'), driver's license photographs, social media' to their databases (MANN, SMITH, 2017, p. 121). In this case, anybody, even if not suspected of a crime, could end up in a database without their knowledge (RECTOR, KNEZEVICH, 2016; STONE, ZICKLER, DARRELL, 2010, p. 1408). This kind of surveillance threatens free speech and freedom of association (BIG BROTHER WATCH, 2018, p. 41), having a chilling effect on willingness to engage in public debate, to publicly disclose political views, to associate with others whose religion, values or political views may be considered different from the majority, generating what is called the 'spiral of silence' (STOYCHEFF, 2016, p. 297-299).

D. SECURITY RISKS

Like any other data, government data is also at risk of misuse and breach whether by:

• Insiders (e.g., in 2013, workers of the US National Security Agency ('NSA') were caught using surveillance records to spy on spouses, girlfriends, and boyfriends) (SELYUKH, 2013; GELLMAN, 2013).

• Outsiders (e.g., hackers. In June 2019, the UK Eurofins Forensics Services ('EFS') suffered a cyber-attack. EFS handles about 90% of England and Wales complex forensics toxicology work (over 70,000 criminal cases in the UK each year). A ransom to unlock the frozen accounts was established although it is not clear if EFS paid it) (HOUSE OF COMMONS SCIENCE AND TECHNOLOGY COMMITTEE, 2019, p. 9; SHAW, 2019).

Nonetheless, as mentioned, biometrics is unique to the person and cannot be easily changed, so, the consequences of a breach of face recognition could be more serious than other identifying data (LYNCH, 2018, p. 11).

E. CRIMINAL INVESTIGATION V LAW-ABIDING PEOPLE

Biometrics is being used in a way it has never done before. Historically, fingerprint and DNA databases have been made up of information from criminal arrests or investigations. By running face recognition searches, agencies have built a biometric network that primarily includes law-abiding people. This is unprecedented (GARVIE, BEDOYA, FRANKLE, 2016, p. 2).

II USE OF FRT IN AUSTRALIA

As can be seen, the use of FRT represents a point of tension between collective security and individual privacy (MANN, SMITH, 2017, p. 121; DIXON, 2019, p. 12).

Countries as the UK, US and Russia have integrated FRT with CCTV (known as 'Smart CCTV') and some Australian Jurisdiction, as Northern Territory and Queensland, as well. In New South Wales, FRT was introduced through an amendment to the regulations governing drivers' licenses (NEC, 2015; MANN, SMITH, 2017, p.123; PETRIE, 2018, p. 5; NSW, 2009).

Several advantages have been appointed in the use of FRT (NEC, 2015):

• The system allows fast search through a photography database and match against any image or CCTV footage, as well as photos taken from body-worn camera videos, drones and phone images.

• Compared to fingerprinting, face images can be captured from a distance without touching the person being identified.

• The technology is helping reduce investigation time by enabling investigators to quickly identify or rule out suspects soon after a crime has been committed.

• It could assist police to identify missing persons (including who suffer from dementia or other similar health issues).

The annual cost of identity crime (in which a perpetrator uses a fabricated, manipulated or stolen identity to facilitate the commission of a crime) in Australia is estimated in $2.65 billion (JORNA, SMITH, 2018, p. x). And FRT could help prevent it.

FRT has long been used for immigration control and the issuing of visas. The Migration Act 1958 authorizes the collection of biometric data, including face images, from people (whether citizens or non-citizens) entering or leaving Australia; moreover, visa applicants located in certain countries are asked to supply biometric information (generally their fingerprints and facial image) during the application process (PETRIE, 2018, p.5).

FRT is used by airport SmartGates to check a traveller's identity by matching a live image captured at the SmartGate with the person ePassport photo, without needing to present the passport (O'SULLIVAN, 2018).

In 2015, the Commonwealth government announced that a National Facial Biometric Matching Capability ('NFBMC') was expected to function in 2016, enabling agencies to share facial information for the purpose of FRT (ATTORNEY-GENERAL'S DEPARTMENT, 2015). NFBMC has not been settle yet, but it is worth noting that it is being established through administrative processes in a way that 'does not require expanded police powers or the introduction of specific Commonwealth legislation', i.e., outside of a legislative framework, which weakens external scrutiny (MANN, SMITH, 2017, p. 127-128).

In 2016, under the Australian Criminal Intelligence Commission effort to integrate all police information systems, including biometric databases held by Australian police (state, territory and federal), NEC was contracted to implement the Biometric Identification Services (BIS) (AUSTENDER, 2016). The BIS was expected to form part of the NFBMC. Nevertheless, the project was discontinued in June 2018 due to a 'cost spiral' and a 'systemic pattern of delay', confirmed by the Australian National Audit Office ('ANAO') (AUSTRALIAN CRIMINAL INTELIGENCE COMMISSION, 2018; HENDRY, 2018; AUSTRALIAN NATIONAL AUDIT OFFICE, 2019). Now, NEC is suing the government for their losses (SHARWOOD, 2019).

As often is the case, there is a lag between technological improvements and regulation, especially FRT (MANN, SMITH, 2017, p. 121-122). In the USA, for instance (GARVIE, BEDOYA, FRANKLE, 2016, p. 35):

- 17 states regulated geolocation tracking.
- 13 states regulated the use of drones by the police.
- 9 states regulated police use of automated license plate readers.
- But not a single state has passed a law about the use of FRT.

In Australia, with the lack of a 'constitutional bill of rights or a cause of action for serious invasion of privacy, there are limited protections in relation to biometric information' (MANN; SMITH, 2017, p. 121-122). Although the Australian case *R v Tang* allowed facial mapping expert evidence (under the condition that the expert does not make positive identifications), there is no precedent for the use of FRT for positive identifications in criminal cases in Australia (R v TANG, 2006, §§ 681, 697 [57], 712 [135], 713-14 [143]-[146]). Australian authorities 'have begun amending legislation to enable driver licence photograph databases to be shared with federal agencies' (SMITH; MANN; URBAS, 2018, p. 54). Under these amendments, photos may be released for investigation of 'terrorism offence', 'threat of a terrorist act' and 'terrorist act', or even a 'relevant criminal activity' (MANN; SMITH, 2017, p. 126). The global 'war on terror' and concerns about security have been leading to legislative and executive measures that can be seen, sometimes, as a disproportionately intrusive erosion of civil liberties (COPER, 2007, p. 4). As consequence, the adoption of FRT is happening without serious supervision, without accuracy testing in the field, and without the 'enactment of legal protections to prevent internal and external misuse' (LYNCH, 2018, p. 1). Add to this, concerns related to information provided for a specific use being accessible for another purpose for which consent was neither solicited nor obtained (NICHOLLS, 2015).

III THE IDENTITY-MATCHING SERVICES BILL

In February 2018, the Commonwealth Government introduced the Identity-matching Services Bill 2018 ('IMS Bill') to establish a framework for sharing identification information – including facial

images held in government databases (e.g., driver license, passport, and visa photographs) – between the federal, state and territory government agencies (and even some private organisations) for the purposes of identity-matching (PETRIE, 2018, p. 3-5). The IMS Bill (DEPARTMENT OF HOME AFFAIR, 2019):

• Authorises the Department of Home Affairs to collect, use and disclose identity-matching information.

• Specifies identity-matching services (e.g., the Face Verification Service and the Face Identification Service).

• States the necessity of a legal basis for collecting and disclosing personal information, although do not establish this legal basis.

• Creates an offence for entrusted persons to record or disclose protected information in connection with the services and define circumstances where disclosure will be authorized.

In April 2019, the Bill lapsed on the dissolution of parliament (PARLIAMENT OF AUSTRALIA, 2019). Legislation is an important option for addressing FRT matter, but the IMS Bill presents key issues that should be addressed before considering revive it, including (PETRIE, 2018, p. 17-28):

• Concerns that the broad scope of the Bill 'may enable substantial infringements on privacy rights, allowing disclosure of personal information for an extremely wide range of purposes'.

• The Bill 'provides inadequate protection against misuse of … information', and it 'does not include key safeguards contained in the [Intergovernmental Agreement on Identity Matching Services] IGA (COUNCIL OF AUSTRALIAN GOVERNMENTS, 2017), such as access criteria and limitations on the amount of information released by the identity-matching systems'.

• Private sector access is another concern (it is questioned if it is appropriate).

The literature proposes certain recommendations that should be considered when proposing a bill that deals with FRT, and which the IMS Bill should take into account (GARVIE, BEDOYA, FRANKLE, 2016, p. 35, 62; LYNCH, 2018, p. 24-27; BIG BROTHER WATCH, 2018, p. 41):

• Impose limits on law enforcement face recognition.

• Limit the collection of data to the minimum necessary to achieve

the government's stated purpose.

• Define clear rules on the legal process required for collection.

• Limit the amount and type of data stored and retained.

• Limit retention period.

• Define simple and clear methods for an individual to request biometric removal from the system.

• Limit the association of biometric data in a single database (otherwise, it would increase the potential harm in case of data breach).

• 'Define clear rules for use and sharing (biometrics collected for one purpose should not be used for another)'.

• Enact robust security procedures.

• Define clear notice requirements (due to the fact that face prints can be collected without a person's knowledge).

• Define and standardize audit trails and accountability throughout the system.

• Ensure independent oversight.

IV. CONCLUSION

There are many benefits in the use of FRT, but also associated issues and controversy. On the one hand, FRT is helping achieve a rapid and efficient law enforcement response. On the other hand, FRT impacts peoples' privacy in many ways and will spark even more discussion about privacy boundaries. The use of FRT in Australia is growing, but it lacks a clear legal framework outlining FRT deployment to support law enforcement practices. As the technology improves, FRT role will continue to expand. In this scenario, it is important to try to reach a harmony between the right to privacy (private) and the need for information (public).

V. BIBLIOGRAFY

ADLER, A.; SCHUCKERS, M. E. Comparing Human and Automatic Face Recognition Performance. *IEEE Trans Syst Man Cybern B Cybern*, v. 37, n. 5, 1248-1260. 2007.

ANU. Early Exposure Key to Recognising 'Other-race' Faces. Australian National University (ANU), Newsroom, 13 September 2019. Disponível em: <https://www.anu.edu.au/news/all-news/early-exposure-key-to-recognising-%E2%80%98other-race%E2%80%99-faces>. Acesso em: 20 set. 2019.

ATTORNEY-GENERAL'S DEPARTMENT (Cth). *National Facial Biometric Matching Capability - Privacy Impact Assessment*: Interoperability Hub. August 2015.

AUSTENDER. *Contract Notice View - CN3343259*: Biometric Identification Services. Australian Government's Procurement Information System web page, 23 May 2016. Disponível em: <https://www.tenders.gov.au/Cn/Show/9156D484-FC31-5306-F65D-62AC112F52AE>. Acesso em 20 nov. 2019.

AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION. *Biometric Identification Services Project to Close*. Australian Criminal Intelligence Commission web page, 15 June 2018. Disponível em: <https://www.acic.gov.au/media-centre/media-releases-and-statements/biometric-identification-services-project-close>. Acesso em: 20 nov. 2019.

AUSTRALIAN NATIONAL AUDIT OFFICE. *Report No 24 of 2018–2019*. The Australian Criminal Intelligence Commission's Administration of the Biometric Identification Services Project, 21 January 2019.

BIG BROTHER WATCH. *Face Off*: the Lawless Growth of Facial Recognition in UK Policing. London: Big Brother Watch, May 2018.

BIOMETRICS GROUP. *Ethical Issues Arising from the Police use of Live Facial Recognition Technology*. Biometrics and Forensics Ethics Group Facial Recognition Working Group ('Biometrics Group'). Interim report, February 2019.

BUOLAMWINI, J.; GEBRU, T. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Conference on Machine Learning Research, v. 81, n. 1, 1-15, 2018.

COPER, M. *Three Good Things and Three Not-So-Good Things about the Australian Legal System*. International Association of Law Schools Conference, Learning from Each Other: Enriching the Law School Curriculum in an Interrelated World. Kenneth Wang School of Law,

Soochow University, Suzhou, China, 17-19 October 2007.
COUNCIL OF AUSTRALIAN GOVERNMENTS. Intergovernamental Agreement on Identity Matching Services. October 2017. Disponível em: <https://www.coag.gov.au/sites/default/files/agreements/iga-identity-matching-services.pdf>. Acesso em: 20 nov. 2019.
DEPARTMENT OF HOME AFFAIR. *Face Matching Services*. Fact Sheet, 2017. Disponível em: <https://www.homeaffairs.gov.au/criminal-justice/files/face-matching-services-fact-sheet.pdf>. Acesso em: 20 nov. 2019.
DIXON, R. Functionalism and Australian Constitutional Values in DIXON, R. (ed), *Australian Constitutional Values*. Oxford: Hart Publishing, 2018.
GARVIE. C; BEDOYA, A. M.; FRANKLE, J. *The Perpetual Line-up*: Unregulated Police Face Recognition in America. Washington: Law Center Center on Privacy & Technology, Georgetown University, 2016.
GELLMAN, B. NSA Broke Privacy Rules Thousands of Times per Year, Audit Finds. *The Washington Post*, 15 August 2013. Disponível em: <https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html>. Acesso em: 20 nov. 2019.
HAMANN, K.; SMITH, R. Facial Recognition Technology: Where Will it Take Us?. American Bar Association Criminal Justice Magazine, Spring 2019. Disponível em: <https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/spring/facial-recognition-technology/>. Acesso em: 20 nov. 2019.
HENDRY, J. NEC Loses National Biometrics Database Project. *IT News*, 15 June 2018. Disponível em: <https://www.itnews.com.au/news/nec-loses-national-biometrics-database-project-494059>. Acesso em: 20 nov. 2019.
HOUSE OF COMMONS SCIENCE AND TECHNOLOGY COMMITTEE. *The work of the Biometrics Commissioner and the Forensic Science Regulator*. Report of Session, 17 July 2019.
INTRONA, L. D.; NISSENBAUM, H. *Facial Recognition Technology*: a Survey of Policy and Implementation Issues. New York: The Center for Catastrophe Preparedness & Response, New York University, 2009.
ISO/IEC. ISO 2382-37: Information technology - Vocabulary - Biometrics. 2017.

JORNA, P.; SMITH, R. G. *Identity crime and misuse in Australia 2017.* AIC Statistical Report 10, 31 December 2018.
LYNCH, J. *Face Off*: Law Enforcement Use of Face Recognition Technology. San Francisco: Electronic Frontier Foundation, 2018.
LYON, D. Biometrics, Identification and Surveillance. *Bioethics*, v. 22, n. 9, 499-508. 2008.
MANN, M.; SMITH, M. Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight. *UNSW Law Journal*, v. 40, n. 1, p. 121-145, 2017.
McKONE, E.; WAN, L. PIDCOCK, M.; CROOKES, K.; REYNOLDS, K.; DAWEL, A.; KIDD, E.; FIORENTINI, C. A Critical Period for Faces: Other-race Face Recognition is Improved by Childhood but not Adult Social Contact. Nature, Scientific Reports, v. 12820, n. 9, 1-13, Sep. 2019.
NEC. NEC *Facial Recognition Helps NT Police Solve Cold Cases and Increase Public Safety in Australia*. NEC Web page, 1 September 2015. Disponível em: <https://www.nec.com/en/press/201509/global_20150901_02.html>. Acesso em: 20 nov. 2019.
NICHOLLS, S. Crime Commission Granted Access to Photographs of NSW Citizens to Aid Terrorism Fight. *The Sidney Morning Herald*, 18 October 2015. Disponível em: <https://www.smh.com.au/national/nsw/asio-crime-commission-granted-access-to-photographs-of-nsw-citizens-to-aid-terrorism-fight-20151018-gkbxa6.html>. Acesso em: 20 nov. 2019.
NWS. *Road Transport (Driver Licensing) Amendment (Facial Recognition Technology) Regulation 2009 under the Road Transport (Driver Licensing) Act 1998.*
O'SULLIVAN, M. *Your Face Will Be Your Passport*: Sydney Airport to Trial Biometrics. Sidney Morning Herald, February 2018. Disponível em: <https://www.smh.com.au/business/companies/your-face-will-be-your-passport-sydney-airport-to-trial-biometrics-20180221-p4z14p.html>. Acesso em: 22 nov. 2019.
PARLIAMENT OF AUSTRALIA. *Identity-matching Services Bill 2018 Information.* ParlInfo Search v1.30.0 web page. Disponível em: <https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;-query=Id:%22legislation/billhome/r6031%22>. Acesso em: 2 set. 2019.
PETRIE, C. *Identity-matching Services Bill 2018 and Australian Passports Amendment.* Identity-matching Services. Bill 2018. Bills Digest No 110, 2017–18, 22 May 2018.

R v Tang (2006) 65 NSWLR 681.
RECTOR, K.; KNEZEVICH, A. Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates. *The Baltimore Sun*, 18 October 2016. Disponível em: <https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-20161017-story.html>. Acesso em: 20 nov. 2019.
RICANEK, K.; BOEHNEN, C. Facial Analytics: From Big Data to Law Enforcement. *Computer*, v. 45, n.9, 95-97. 2012.
SELYUKH, A. NSA Staff Used Spy Tools on Spouses, Ex-lovers: Watchdog. *Reuters*, 28 September 2013. Disponível em: <https://www.reuters.com/article/us-usa-surveil-lance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927>. Acesso em: 20 nov. 2019.
SHARWOOD, S. NEC Sues Feds over Binned Biometric Identification Services Project. *IT News*, 19 July 2019. Disponível em: <https://www.itnews.com.au/news/nec-sues-feds-over-binned-biometric-identification-services-project-528468>. Acesso em: 20 nov. 2019.
SHAW, D. *Eurofins Scientific*: Forensic services firm paid ransom after cyber-attack. *BBC News*, 5 July 2019. Disponível em: <https://www.bbc.co.uk/news/uk-48881959>. Acesso em: 22 nov. 2019.
SMITH, M.; MANN, M.; URBAS, G. Facial Recognition in *Biometrics, Crime and Security*. Oxon: Routledge, 2018.
STONE, Z.; ZICKLER, T.; DARRELL, T. Toward Large-Scale Face Recognition Using Social Network Context. *Proceedings of the IEEE*, v. 98, n. 8, 1408-1415, 2010.
STOYCHEFF, E. Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring. JOURNALISM & MASS COMMUNICATION QUARTERLY, v. 93, n. 2, 296-311, 8 March 2016.
WHITE, D.; DUNN, J. D.; SCHIMD, A. C.; KEMP, R. I. Error Rates in Users of Automatic Face Recognition Software. *PLoS ONE*, v. 10, n. 10, 1-14, 2015.
WOODWARD JR, J. D.; HORN, C.; GATUNE, J.; THOMAS, A. *Biometrics*: a Look at Facial Recognition. (Documented Briefing). Santa Monica: RAND Public Safety an Justice, 2003.

ANEXO 5 - Autorregulação e corregulação: duas ferramentas no canivete do regulador

Direito Econômico/Direito Administrativo 3 (UnB): SCHLOTTFELDT, Shana. Autorregulação e corregulação: duas ferramentas no canivete do regulador. *Revista Consultor Jurídico (ConJur)*. 11 jun. 2021. Disponível em: https://www.conjur.com.br/2021-jun-11/opiniao-autorregulacao-corregulacao-ferramentas-canivete-regulador. ISSN 1809-2829.

Consultor Jurídico
conjur.com.br

OPINIÃO

Autorregulação e corregulação: duas ferramentas no canivete do regulador

11 de junho de 2021, 6h31

Por Shana Schlottfeldt

A teoria clássica da regulação ordenadora e criminalizadora, também conhecida como teoria do comando-e-controle, parte do princípio de que o regulado teria seu comportamento moldado rumo aos fins da regulamentação, em resposta a ameaças a condutas desviantes do previsto na norma aplicável ao caso. Assim, o objetivo da multa seria dissuadir da prática em desacordo com a norma.

O Acórdão Tribunal de Contas da União 729/2020, que tratou do monitoramento da arrecadação de multas administrativas emitidas por 15 agências e órgãos de regulação do governo, mostrou que aqueles entes aplicaram, no período sob análise, mais de 651 mil multas, totalizando R$ 18,3 bilhões a serem arrecadados [1]. É uma cifra impressionante!

Apesar de tais dados passarem a impressão de que agências e órgãos de regulação estariam agindo de maneira ativa no sentido da efetivação da melhoria da qualidade dos serviços prestados à população, faz-se necessária uma reflexão sobre o tema. Números tão elevados não só impressionam; na verdade, preocupam.

Emissão de mais multas não significa melhoria de serviços, pode até indicar o contrário: 1) um maior descumprimento das normas estabelecidas; 2) os agentes podem estar prestando serviços ruins; 3) a regulação pode se mostrar demasiadamente severa, necessitando ajustes (o que pode incluir, até mesmo, a desregulação); 4) a agência pode ter falhado em estabelecer normas que produzam incentivos adequados. Ou mesmo, todas as opções anteriores... Pode, na verdade, ser o sinal de que é preciso mudar!

Mais impressionante é saber que, desse total, foram arrecadados pouco mais de R$ 435,4 milhões, correspondendo a 2,37%. Dos 15 órgãos analisados, 11 arrecadaram menos do que 10% do valor das multas aplicadas [2]. Ou seja: a maioria das multas não é paga!

É preciso superar a falácia de que o sucesso da atividade regulatória seja medido pelo número de autuações. Um sistema regulatório rígido, apoiado na aplicação mecânica de normas, em vez de sustentado por uma maior racionalização da atuação estatal, gera uma deturpação das prioridades regulatórias. Mais do que punir, é preciso que se estimulem comportamentos de adequação à regulação.

Da mesma forma que as empresas fazem *planejamento tributário* — estudando maneiras de reduzir legalmente a carga tributária que incide sobre o empreendimento —, elas também fazem *planejamento regulatório*: às vezes infringir uma norma e sujeitar-se à multa pode ser mais "vantajoso", quando avaliado sob a perspectiva de custo-benefício, do que ajustar sua conduta a normas que não levam em conta os contextos (dificuldades e particularidades) de sua implantação. Corrobora com esse entendimento o citado Acórdão do TCU, que constatou que os entes fiscalizados costumam pagar somente multas de menor valor, contestando, administrativa ou judicialmente, multas maiores [3].

Tem-se, assim, dados objetivos que evidenciam o fracasso de conformidade vivenciado em vários setores regulados sob o comando-e-controle.

A título de curiosidade traz-se a "Fábula do Rei Regulador" [4], anedota espirituosa e bastante ilustrativa da espiral regulatória [5], convidando à reflexão:

"*Era uma vez, em um reino não muito distante... havia uma reclamação dos súditos sobre o preço do pão. O rei, indignado, decretou um preço máximo. No dia seguinte, os padeiros reduziram o peso do pão. O rei, para que os padeiros não fugissem do regulamento, decretou um peso mínimo. Então, os padeiros usaram farinha de qualidade inferior. O rei ordenou uma qualidade mínima. Os padeiros, em resposta, só permitiam aos súditos comprar pão se comprassem também leite, que não estava submetido ao controle de preço. O rei emitiu um novo decreto proibindo a venda casada de produtos. No dia seguinte, os produtores colocaram uma fruta cristalizada em cima do pão e disseram que o preço era livre porque não se tratava mais de pão, mas sim de um bolo. O rei então teve que incluir bolos no regulamento. E eles continuaram e continuaram até que o rei se fartou e nacionalizou as padarias. Moral da história: se você não quer ficar preso na espiral regulatória, não regule*".

Diferente do que possa parecer, não se trata de uma ode acrítica à desregulação, mas um

alerta (no mínimo divertido) à regulação excessiva (impensada, insensata, ineficiente), naquela linha: seria cômico se não fosse trágico.

O fenômeno regulatório detém diversas facetas visíveis e invisíveis. Na prática, sanções despropositadas podem representar um estímulo ao inadimplemento: o agente prefere buscar meios para se esquivar da obrigação ou protelá-la (e.g., por meio da judicialização). O saldo final pode ser o aumento do custo do funcionamento da máquina pública sem que isso se reverta em melhora na qualidade ou eficiência da prestação do serviço. A crítica é dolorosa.

De fato, é possível constatar que o discurso de desregulação no Brasil resultou em mais regulação; afinal, o momento de criação de agências reguladoras correspondeu ao fortalecimento da centralização normativa, deixando em evidência o fato de que priorizar uma forma de intervenção indireta sobre a direta não significa, necessariamente, menor intervenção.

O Estado regulador não é um Estado intervencionista, nem mesmo abstencionista/anarcocapitalista. Ele representa um meio termo, um equilíbrio entre dois modelos ideologicamente bem definidos (Estado Social e Estado Liberal), em que o foco da desregulação dirige-se aos excessos ou disfuncionalidades da regulação.

O esforço de modelagem regulatória é, por natureza, complexo e é precisamente o aspecto da procura por respostas inovadoras para os problemas regulatórios, apoiadas em medidas educativas e mecanismos cooperativos baseados no diálogo entre regulador e regulado, que ocupa atenção diferenciada na literatura mais atualizada de regulação [6].

Nesse contexto, a *autorregulação* e a *corregulação*, ao lado de outras técnicas regulatórias, surgem como ferramentas que integram o "canivete suíço" do regulador, i.e., instrumentos dos quais o administrador público pode lançar mão com vistas à conformação eficiente de condutas.

Essas abordagens aparecem como resposta à retórica maniqueísta de oposição entre *desregular* e *regular*, representando uma reflexão mais profunda acerca dos ganhos sociais oriundos da diminuição da regulação estatal voltada à compensação social ou à orientação do mercado.

Segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), na *autorregulação* [7], grupos de empresas de um determinado setor, setores inteiros ou grupos profissionais concordam, voluntariamente, em agir de maneiras prescritas, de

acordo com um conjunto de regras ou princípios decididos por eles próprios [8].

Ocorre uma permuta segundo a qual os entes privados aceitam limitar sua liberdade de ação sob a condição de não haver uma imposição regulatória unilateral; o poder público, por sua vez, lhes confere o poder de fixar normas para si próprios. O grupo é responsável por desenvolver os instrumentos de autorregulação, monitorar a conformidade e garantir a sua aplicação [9]. Os grupos podem ser totalmente responsáveis pelo desenvolvimento dos instrumentos de autorregulação ou podem trabalhar com entidades governamentais e outras partes interessadas, situação em que se tem a chamada *corregulação*.

Na corregulação, geralmente o governo fornece apoio para permitir que as disposições sejam aplicadas e fiscalizadas. Na autorregulação, em geral a fiscalização do cumprimento pelos pares é de responsabilidade do próprio grupo instituidor.

Usados nas circunstâncias certas, esses instrumentos podem oferecer vantagens significativas sobre a regulação tradicional de comando-e-controle, incluindo: 1) maior flexibilidade e adaptabilidade; 2) custos administrativos e de conformidade potencialmente mais baixos; 3) capacidade de abordar questões específicas do setor e do consumidor diretamente; e 4) mecanismos rápidos e baratos de tratamento de reclamações e resolução de disputas. Ambas as abordagens de autorregulação e corregulação têm o potencial de ser instrumentos de política muito eficientes devido à sua flexibilidade: podem ser adaptadas para o problema específico para o qual foram projetadas e podem mudar rapidamente em resposta às mudanças nas circunstâncias.

Sempre houve, no Brasil, um difundido receio — sustentado, quase sempre, em desconhecimento — quanto às categorias de autorregulação e corregulação, como se elas representassem uma forma de deixar o mercado agir descontroladamente.

Neste sentido, a "Autorregulação do Crédito Consignado" pode ser citada como exemplo de uma iniciativa que tem se mostrado positiva: associada à percepção de que o problema de práticas comerciais abusivas no oferecimento de crédito consignado prejudicava não só os consumidores aposentados, mas também o próprio mercado quanto a uma concorrência justa e saudável, a Associação Brasileira de Bancos (ABBC) e a Federação Brasileira de Bancos (Febraban) propuseram o Sistema de "Autorregulação do Crédito Consignado". A assinatura da convenção para adesão é voluntária, mas até fins de 2019 instituições representando 98% do volume da carteira de crédito consignado em todo o país já haviam aderido ao instrumento [10].

O Sistema de Autorregulação entrou em operação em 2 de janeiro de 2020 e além de

estabelecer a governança e o regramento mínimo para o seu funcionamento segundo as regras estatais vigentes, tem três objetivos principais: 1) criar um sistema de bloqueio de ligações à disposição dos consumidores que não queiram receber ofertas de crédito consignado ("não me perturbe"); 2) formar uma base de dados para monitorar reclamações sobre oferta inadequada do produto; e 3) estabelecer medidas voltadas à transparência, ao combate ao assédio comercial e à qualificação de correspondentes.

Complementarmente ao Sistema, e sem prejuízo às punições privadas nele previstas (e.g., multas que variam entre R$ 45 mil e R$ 1 milhão) [11], a Secretaria Nacional do Consumidor (Senacon) e entes integrantes do Sistema Nacional de Defesa do Consumidor (SNDC) fiscalizam sua implementação, além de aplicarem o Código de Defesa do Consumidor (CDC) e outros normativos cabíveis, que não são afastados pela Convenção, adicionando um componente de corregulação ao instrumento autorregulatório.

Perceber-se, com este exemplo, que com a autorregulação e a corregulação o Estado não está renunciando a suas funções, muito pelo contrário! Ele está atuando de forma conjunta com o setor regulado no estabelecimento de diretrizes e procedimentos mínimos, com isso, a proposta tem a capacidade de aumentar a previsibilidade e a segurança jurídica.

Longe de representarem uma forma de deixar o mercado agir descontroladamente, de forma voluntariosa, mecanismos como a autorregulação e a corregulação têm enorme potencial de tornar mais racional e efetiva a regulação.

---

[1] TRIBUNAL DE CONTAS DA UNIÃO [TCU]. *Acórdão TCU-Plenário nº 729/2020*. Relatório de Acompanhamento (RACOM) TC 024.820/2018-0. Relator: Aroldo Cedraz. Data de julgamento: 01/04/2020, Plenário. Disponível em: https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/TC%2520024.820%252F2018-0%2520/%2520/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0/%2520?uuid=e3669810-3a6d-11eb-ad81-51955e150807. Acesso em: 1 jun. 2021.

[2] Id, 2020, Tabela3.

[3] Ibidem, 2020, §§ 39, 41, 46.

[4] BULLARD, Alfredo; ROLDÁN, Nicole; CARO, André. *La Paradoja de la Calidad*

en los Servicios de Telefonía Móvil: cuando más se puede convertir en menos. Congreso Mundial de Móviles de la GSMA. Barcelona, 24 fev. 2014, p. 9. Disponível em: https://www.gsma.com/latinamerica/wp-content/uploads/2014/03/Alfredo-Bullard-Reporte-Paradoja-de-la-Calidad-Reporte-Completo.pdf. Acesso em: 1 jun. 2021.

[5] Situação em que a produção de regulação inefetiva/errada, em vez de gerar desregulação como uma reação, gera mais regulação (para corrigir os erros da regulação que lhe precedeu) e assim sucessivamente, numa espiral sem fim.

[6] ARANHA, Márcio Iorio. *Manual de Direito Regulatório*: Fundamentos de Direito Regulatório. 5. ed. rev. ampl. London: Laccademia Publishing, 2019, p. 74, 145.

[7] Não é crítico para esta discussão, mas merece ser mencionado que a autorregulação é uma forma genérica de regulação que detém significados variados de acordo com a teoria/modelo regulatório adotado (e.g., autorregulação unilateral, ou *unilateral self-regulation*, de uma única empresa; autorregulação da indústria, ou *industry self-regulation*, implicando em atuação coletiva para melhoria da reputação do setor como um todo; autorregulação regulada, ou *enforced self-regulation*, que incorpora consequências punitivas estatais na disciplina normativa proposta pelo regulado e ratificada pelo regulador) cf. Aranha, 2019, p. 147-148.

[8] ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO [OCDE]. *Industry Self-Regulation*: role and use in supporting consumer interests. Relatório DSTI/CP(2014)4/FINAL. 23 mar. 2015, p. 5. Disponível em: https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2014)4/FINAL&docLanguage=En. Acesso em: 1 jun. 2021.

[9] ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO [OCDE]. *Alternatives to Traditional Regulation*. OECD Report. 2006, p. 6. Disponível em: https://www.oecd.org/gov/regulatory-policy/42245468.pdf. Acesso em: 1 jun. 2021.

[10] SECRETARIA NACIONAL DO CONSUMIDOR [SENACON]. *Guia*: Corregulação do Crédito Consignado. Brasília: Secretaria Nacional do Consumidor, Ministério da Justiça e Segurança Pública, mar. 2020, p. 5. Disponível em: https://www.defesadoconsumidor.gov.br/images/2020/Guia---Corregulao-Crdito-Consignado-compactado---final_compressed-1.pdf. Acesso em: 1 jun. 2021.

[11] Na autorregulação tem-se controles internos que podem ser até mais severos para a

empresa do que as punições do poder público. Sobre isso, Aranha (2019, p. 105) esclarece que "[é] um equívoco [...] pressupor-se que a autorregulação seria uma opção de amenização das consequências pelo descumprimento das normas quando comparada com constrangimentos públicos, [...] punições societárias [...] podem ser muito mais severas do que as extrinsecamente implementadas".

Shana Schlottfeldt é analista legislativo da Câmara dos Deputados, doutora pela Universidade de Brasília (UnB), visiting PhD student at University of York, mestre pela Universidad Carlos III de Madrid, bacharelanda em Direito pela UnB, LLB exchange student at Australian National University, membro do Observatório da LGPD-UnB. Suas opiniões não representam as instituições às quais está vinculada.

Revista **Consultor Jurídico**, 11 de junho de 2021, 6h31

ANEXO 6 - A (Ir)Retroatividade da Alteração da Natureza da Ação Penal no Crime de Estelionato pela Lei Anticrime: como ficam as ações penais em curso?

Direito Processual Penal 2 (UnB): FONSECA, Reynaldo Soares da; SCHLOTTFELDT, Shana. A (Ir)Retroatividade da Alteração da Natureza da Ação Penal no Crime de Estelionato pela Lei Anticrime: como ficam as ações penais em curso? *Revista Magister de Direito Penal e Processual Penal*. v. 102, jun./jul. 2021, p. 26-42. ISSN 1807-3395.

102
JUN/JUL 2021

Revista Magister de Direito Penal e Processual Penal

LEX MAGISTER
PRODUTOS JURÍDICOS

ISSN 1807-3395

Revista Magister de Direito Penal e Processual Penal

Ano XVII – Nº 102
Jun-Jul 2021

Repositório Autorizado de Jurisprudência
Supremo Tribunal Federal – nº 38/2007
Superior Tribunal de Justiça – nº 58/2006

Classificação Qualis/Capes: B1

Revista Magister de Direito Penal e Processual Penal

A responsabilidade quanto aos conceitos emitidos nos artigos publicados é de seus autores.

Artigos podem ser encaminhados para o e-mail: editorial@editoramagister.com.br. Não devolvemos os originais recebidos, publicados ou não.

As íntegras dos acórdãos aqui publicadas correspondem aos seus originais, obtidos junto ao órgão competente do respectivo Tribunal.

Esta publicação conta com distribuição em todo o território nacional.

A editoração eletrônica foi realizada pela Editora Magister, para uma tiragem de 3.100 exemplares.

Revista Magister de Direito Penal e Processual Penal
v. 1 (ago./set. 2004)-.– Porto Alegre: Magister, 2004-
Bimestral. Coordenação: Oswaldo Henrique Duek Marques.
v. 102 (jun./jul. 2021)
ISSN 1807-3395

1. Direito Penal – Periódico. 2. Direito Processual Penal – Periódico.

CDU 343(05)

Ficha catalográfica: Leandro Augusto dos S. Lima – CRB 10/1273

Capa: Apollo 13

Editora Magister

Diretor: Fábio Paixão

Alameda Coelho Neto, 20
Boa Vista – Porto Alegre – RS – 91340-340

Apresentação

É com satisfação que apresento a centésima segunda edição da Revista Magister de Direito Penal e Processual Penal, destinada a contribuir para aperfeiçoar as ciências penais e processuais penais.

Abre a sequência de artigos *Tortura e Imprescritibilidade*, de minha autoria com Carolina Alves de Souza Lima, no qual analisamos as circunstâncias aptas a configurar a imprescritibilidade da tortura, com base no Estatuto de Roma e no Direito Penal comum.

A seguir, Reynaldo Soares da Fonseca e Shana Schlottfeldt, com seu escrito *A (Ir)Retroatividade da Alteração da Natureza da Ação Penal no Crime de Estelionato pela Lei Anticrime: como Ficam as Ações Penais em Curso?*, examinam o efeito dessa alteração nos casos de persecuções penais em andamento.

A Revista prossegue com o texto *A Disputa pelo Conceito de Verdade como Compromisso Epistêmico da Atividade Probatória em Processo Penal*, de Pedro Estevam Pinto Serrano e Roberta de Lima e Silva. Nele, os autores discorrem sobre a verdade desde a ótica da filosofia grega até suas implicações em um Estado Democrático de Direito.

Já no artigo *O Delito de Infração de Medida Sanitária em Tempos de Pandemia*, Mauro Luís Silva de Souza e Michael Schneider Flach apreciam a tipologia completa do art. 268 do Código Penal brasileiro, que criminaliza o delito de infração de medida sanitária preventiva, dentre os crimes contra a saúde e a incolumidade pública.

Dando continuidade aos trabalhos, em *"A Dona Delinquente": a Necessidade da Adoção de uma Teoria Criminológica Feminista para a Abordagem de Gênero no Direito Penal*, Letícia Maria de Maia Resende e Edson Vieira da Silva Filho abordam a mulher criminosa no âmbito penal da perspectiva da Criminologia.

No estudo *Ciberterrorismo: os Reflexos da Globalização para a Propagação do Terror*, por sua vez, Ricardo Libel Waldman e Caio César Barros Tatto mostram o avanço tecnológico e o paradigma do ciberterrorismo no ambiente virtual, capaz de causar temor na sociedade mundial.

Na sessão destinada à *Doutrina Estrangeira*, em seu artigo *¿Dolo sin Conocimiento?: Reflexiones en Torno a la Condena por Defraudación Fiscal de Lionel Messi*, o jurista espanhol Ramon Ragués I Vallèz apresenta um rico debate sobre a exigência do conhecimento e da vontade dos elementos do tipo objetivo para caracterizar a conduta dolosa.

Em seguida, na parte destinada ao *Parecer*, a partir de denúncia de crime de condição análoga a de escravo, Jaques de Camargo Penteado enfoca temas relevantes e atuais, com destaque para a tipicidade, imputação objetiva e teoria do domínio do fato.

Como coordenador, estou convencido da excelência e atualidade dos textos apresentados, cuja leitura será, sem dúvida, de grande interesse para os estudiosos das ciências penais e processuais penais.

Oswaldo Henrique Duek Marques

Sumário

Doutrina

Doutrina Estrangeira

Parecer

Jurisprudência

A (Ir)Retroatividade da Alteração da Natureza da Ação Penal no Crime de Estelionato pela Lei Anticrime: como Ficam as Ações Penais em Curso?

Reynaldo Soares da Fonseca

Ministro do Superior Tribunal de Justiça (STJ); Professor Adjunto (licenciado) da Universidade Federal do Maranhão (UFMA), em Colaboração Técnica na Universidade de Brasília (UnB); Professor do Mestrado Profissional em Direito, Regulação e Políticas Públicas na UnB; Membro da Academia Maranhense de Letras; Pós-Doutorado em Democracia e Direitos Humanos pela Universidade de Coimbra; Doutor em Direito Constitucional pela Faculdade Autônoma de Direito de São Paulo (FADISP), com pesquisa realizada na Universidade de Siena – Itália; Mestre em Direito Público pela Pontifícia Universidade Católica de São Paulo (PUC-SP); Especialista em Direito Constitucional (UFMA/UFSC), em Direito Penal pela UnB e em Inteligência Financeira pela Escola de Administração Fazendária (ESAF);
e-mail: reynaldo.fonseca@stj.jus.br.

Shana Schlottfeldt

Analista Legislativo da Câmara dos Deputados; Doutora em Informática pela Universidade de Brasília (UnB); Visiting PhD Student at University of York; Mestre em Informática pela Universidad Carlos III de Madrid; Bacharelanda em Direito pela UnB; LLB Exchange Student at Australian National University; Membro do Comitê Gestor Pró-Equidade de Gênero e Raça da Câmara dos Deputados; Membro do Observatório da LGPD-UnB;
e-mail: shana.schlottfeldt@aluno.unb.br.

RESUMO: O presente artigo trata da alteração operada pela Lei nº 13.964/2019, conhecida como Lei ou Pacote Anticrime, na natureza da ação penal do estelionato, tornando-a, com algumas exceções, pública condicionada à representação. O objetivo foi examinar o efeito dessa alteração sobre as persecuções criminais em andamento. Para tanto, analisou-se uma série de institutos jurídicos relacionados, como a lei penal no tempo, mais especificamente a retroatividade das normas penais híbridas, a natureza da ação penal pública condicionada à representação, bem como a preservação da autonomia da vontade da vítima e dos direitos fundamentais do acusado. Utilizando-se o método hipotético-dedutivo, analisaram-se dois julgados (divergentes) do Superior Tribunal de Justiça (STJ), um julgado do STJ, uniformizando seu entendimento sobre o tema, e um do Supremo Tribunal Federal. Entende-se que a inovação trazida pela Lei Anticrime,

no que diz respeito ao crime de estelionato, apesar de norma mista, não deveria ser aplicada de forma retroativa aos procedimentos já iniciados, dado o caráter de procedibilidade e não prosseguibilidade da nova norma.

PALAVRAS-CHAVE: Lei Anticrime. Crime de Estelionato. Irretroatividade. Ação Penal Pública Condicionada à Representação. Processo Penal em Curso.

Introdução

A Lei nº 13.964, de 24 de dezembro de 2019, que ficou conhecida como Lei ou Pacote Anticrime, traz em sua ementa: "aperfeiçoa a legislação penal e processual penal". Sem dúvidas, a Lei Anticrime alterou substancialmente o Decreto-Lei nº 2.848/1940 (Código Penal, CP), o Decreto-Lei nº 3.689/1941 (Código de Processo Penal, CPP) e diversas outras leis penais extravagantes. Entretanto, se ela realmente aperfeiçoa ou não tais legislações, é algo que o tempo dirá, mas fato é que a novel Lei tem gerado bastante discussão (desde sua tramitação e, agora, após sua promulgação) (SOUZA NETTO; FOGAÇA; GARCEL, 2020, p. 10). Uma dessas controvérsias, diz respeito à modificação realizada no dispositivo do art. 171 do CP, que trata do crime de estelionato e será o objeto de estudo deste artigo.

A partir da reforma legislativa, vários réus passaram a apresentar impugnações referentes à aplicabilidade da nova regra para os casos em que o crime de estelionato foi cometido antes da Lei Anticrime e o Ministério Público já tinha oferecido a denúncia antes do referido estatuto entrar em vigor, *i.e.*, quando ainda não era necessária a representação da vítima (BRASIL, 2020c, p. 11).

O objetivo deste artigo é responder à pergunta: "como agir nas ações penais em curso em que o réu esteja sendo acusado de estelionato comum[1]?"

O questionamento é oportuno, vez que a Lei nº 13.964/2019 é objeto de estudos iniciais pela doutrina e começa a ser analisada pela jurisprudência, como será visto.

---

1 No presente estudo, o que será referido como "estelionato comum" é aquele que não foi excepcionado pelos incisos do novo § 5º, art. 171, do CP, previsto na Lei nº 13.964/2019, que, como será visto, não está sujeito à obrigatoriedade da representação para a propositura da ação penal, *i.e.*, o crime de estelionato que não foi praticado em desfavor da: I – Administração Pública, direta ou indireta; II – criança ou adolescente; III – pessoa com deficiência mental; ou, IV – maior de 70 (setenta) anos de idade ou incapaz.

Este artigo é composto por cinco seções, além desta Introdução e da Conclusão. A seção um apresenta ao leitor a alteração trazida ao art. 171 do CP pela Lei Anticrime. A seção dois trata da aplicação da lei penal no tempo, enquanto que a seção três discorre sobre a legitimidade ativa da ação penal. As seções quatro e cinco versam sobre o posicionamento, respectivamente, da jurisprudência e da doutrina, sobre o tema, evidenciando os argumentos trazidos à discussão. Por fim, apresenta-se a Conclusão, com a manifestação de opinião de qual posicionamento entende-se mais adequado quanto à questão da aplicação do novo dispositivo às ações penais em andamento.

1 A Lei Anticrime e o Crime de Estelionato

O relatório do "Grupo de Trabalho Destinado a Analisar e Debater as Mudanças Promovidas na Legislação Penal e Processual Penal pelos Projetos de Lei nº 10.372, de 2018, nº 10.373, de 2018, e nº 882, de 2019 – GTPENAL" consignou:

> "*4.3.2.1.5. Crime de Estelionato*
>
> O Projeto de Lei nº 10.372, de 2018, propõe a inclusão do § 5º ao tipo penal inscrito no art. 171 do Código Penal (Estelionato), tornando a ação penal condicionada à representação da vítima, nos seguintes termos:
>
> 'Art. 171. (...)
>
> (...)
>
> § 5º Somente se procede mediante representação.'
>
> Conforme atual sistemática penal, a ação penal em relação ao tipo penal descrito no art. 171 do Código Penal é, em regra, pública incondicionada. Entretanto, o art. 182 do mesmo código estabelece que a ação penal é pública condicionada a representação caso o sujeito passivo do crime de estelionato seja: a) o cônjuge desquitado ou judicialmente separado; b) o irmão, legítimo ou ilegítimo; e, c) o tio ou sobrinho, com quem o agente coabita.
>
> Desse modo, concordamos em tornar a ação pública condicionada a representação da vítima como regra geral. Porém, em meu entendimento, se deve manter a ação penal pública incondicionada quando a vítima for: a) a Administração Pública, direta ou indireta; b) criança ou adolescente; ou, c) pessoa com deficiência mental. Sendo assim, acolhemos tal sugestão em nossa proposta de unificação, com os ajustes indicados." (GTPENAL, 2019, p. 175)

Segundo explicação do Ministro Alexandre de Moraes, que presidiu a Comissão de Juristas que analisou o Projeto da Lei Anticrime no âmbito do CNJ, a alteração do art. 171 do CP tratou-se de uma opção do legislador que, no âmbito do Pacote Anticrime, evidenciou a priorização do combate ao crime organizado, ao crime violento e à corrupção, estabelecendo novos me-

canismos para a solução dos delitos praticados sem violência ou grave ameaça, *e.g.*, o acordo de não persecução penal e a necessidade de a vítima manifestar sua vontade para o processamento da ação penal pelo crime de estelionato (BRASIL, 2020c, p. 10; GTPENAL, 2019, p. 8; MORO, 2019, p. 2-4).

Tal medida teria surgido de proposta encaminhada pelo Conselho Nacional dos Chefes de Polícia Civil, a partir da constatação fática que em diversos inquéritos de estelionato, após obter o ressarcimento, a vítima não mais demonstrava interesse na continuidade da investigação (BRASIL, 2020c, p. 10-11). Exemplo disso, é que muitos registros de ocorrência apenas são realizados por exigência dos bancos, como formalidade para levar adiante a contestação da operação fraudulenta e efetivar o ressarcimento da vítima (ALBUQUERQUE, 2020, p. 16).

Diante disso, a Lei Anticrime dispôs:

> "Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
>
> (...)
>
> 'Art. 171. (...)
>
> § 5º Somente se procede mediante representação, salvo se a vítima for:
>
> I – a Administração Pública, direta ou indireta;
>
> II – criança ou adolescente;
>
> III – pessoa com deficiência mental; ou
>
> IV – maior de 70 (setenta) anos de idade ou incapaz.' (NR)"

Assim, a Lei Anticrime inseriu, no art. 171, o § 5º, que modificou a natureza da ação penal, de pública incondicionada (com as exceções do art. 182 do CP) para pública condicionada à representação, exceto se a vítima for: (1) a Administração Pública, direta ou indireta; (2) criança ou adolescente[2]; (3) pessoa com deficiência mental; (4) maior de 70 (setenta) anos de idade[3] ou incapaz[4].

---

2 Conforme o art. 2º da Lei nº 8.069/90 (Estatuto da Criança e do Adolescente), criança é a "pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade";

3 Diferente da majorante do § 4º do art. 171, aqui, a regra da ação penal não utiliza o conceito legal de idoso, que, segundo o art. 1º da Lei nº 10.741/03 (Estatuto do Idoso), é a "pessoa com idade igual ou superior a 60 (sessenta) anos". Apenas se a vítima superar os 70 anos idade é que a ação penal será pública incondicionada.

4 Consoante o art. 4º da Lei nº 10.406/02 (Código Civil, CC), além dos maiores de 16 e menores de 18 anos (já incluídos no art. 171, § 5º, II, do CP), são incapazes, "relativamente a certos atos ou à maneira de os exercer: (...) (II) os ébrios habituais e os viciados em tóxico; (III) aqueles que, por causa transitória ou permanente, não puderem exprimir sua vontade; (IV) os pródigos".

Para o que aqui denominou-se de "estelionato comum" (aquele que não se enquadra nos incisos do § 5º, art. 171, do CP), a propositura da ação penal foi modificada, exigindo que a vítima represente junto à Polícia Judiciária no prazo decadencial de seis meses (arts. 38 do CPP e 103 do CP), não sujeito à regra da interrupção ou suspensão. Após esse prazo, opera-se o instituto da decadência, com a consequência de impedir a propositura da ação penal.

Uma vez que a necessidade de representação traz consigo institutos extintivos da punibilidade, a regra do § 5º deve ser analisada sob a perspectiva da aplicação da lei penal no tempo, que é o que se estudará a seguir.

2 Do Direito Intertemporal e a Natureza Jurídica das Modificações

Pode-se enunciar os seguintes princípios do *direito intertemporal*: (1) irretroatividade da lei penal: é o princípio *tempus regit actum*, *i.e.*, a lei aplicável é a vigente ao tempo da execução do crime (arts. 1º do CP e 5º, XXXIX, da Constituição Federal – CF) (DAMÁSIO DE JESUS, 1988, p. 61-62). Trata-se de uma garantia que o cidadão não será surpreendido por condutas que, até então, não eram tipificadas como crime (BITENCOURT, 2020, p. 463); e (2) extratividade (retroatividade ou ultratividade) da lei mais benéfica: a lei anterior, quando mais favorável, terá ultratividade, prevalecendo ainda que durante a vigência da lei nova; observando-se também o inverso, *i.e.*, a lei posterior mais benéfica retroagirá para alcançar condutas praticadas antes de sua vigência (art. 5º, XL, da CF e parágrafo único, art. 2º, CP) (BITENCOURT, 2020, p. 465).

Busca-se resolver (nem sempre se consegue) as situações de conflito temporal na aplicação da lei penal, com dispositivos, tais como o art. 2º do CP; o art. 13 do Decreto-Lei nº 3.931/1941 (Lei de Introdução ao Código de Processo Penal); art. 66, I, da Lei nº 7.210/84 (Lei de Execução Penal); art. 5º, XXXIX e XL, da CF.

As hipóteses de conflito entre lei nova e anterior são: (a) *abolitio criminis*: a lei nova deixa de considerar crime fato anteriormente tipificado como ilícito penal; (b) *novatio legis* incriminadora: considera crime fato anteriormente não incriminado (é irretroativa, não se aplicando a fatos praticados antes da sua vigência); (c) *novatio legis in pejus*: lei posterior que agravar a situação do sujeito não retroagirá; (d) *novatio legis in mellius*: prevalece a lei que, de qualquer modo, favorece o agente. Segundo Mirabete (1990, p. 62), esta última hipótese não ofenderia o princípio constitucional que salvaguarda a coisa julgada (art. 5º, XXXVI, da CF), pois a norma constitucional protegeria as garantias individuais e não o Estado enquanto titular do direito de punir.

No âmbito do direito intertemporal, *norma processual* é aquela que disciplina o processo e o procedimento, sem relação direta com o direito de punir do Estado. A lei processual não se submete ao princípio da extratividade da lei penal mais benéfica.

Em matéria processual, vige o princípio *tempus regit actum*, que se relaciona aos atos do processo. Assim, conforme prescreve o art. 2º do CPP, a nova lei processual aplica-se de imediato, independentemente se é benéfica ou não, sem efeito retroativo, respeitando-se a validade dos atos praticados sob a vigência da lei processual anterior. Dessa forma, os atos já realizados permanecerão inalterados, os novos deverão obedecer à nova lei (*princípio da imediatidade*).

Contudo, na ordem penal, podem ser encontradas *normas híbridas*, *i.e.*, leis penais que disciplinam matéria tanto de natureza penal quanto de natureza processual penal (MOREIRA, 2020), ou que, apesar de estarem em determinado diploma, possuem natureza distinta do diploma no qual estão inseridas, daí também serem chamadas, nesse caso, de *normas heterotópicas*.

A norma que altera a natureza da ação penal não retroage, salvo para beneficiar o réu. A norma que dispõe sobre a classificação da ação penal influencia decisivamente o *jus puniendi*, pois interfere nas causas de extinção da punibilidade, como a decadência e a renúncia ao direito de queixa, portanto, tem efeito material. Assim, a lei que possui normas de natureza híbrida (penal e processual) não tem pronta aplicabilidade, vigorando a irretroatividade da lei, salvo para beneficiar o réu (BRASIL, 2012, p. 9-11).

3 Legitimidade Ativa da Ação Penal

Com base na titularidade do exercício da ação penal, o art. 100, *caput*, do CP estabelece a regra – a ação penal é pública –, bem como a exceção – exceto quando a lei expressamente a declara privativa do ofendido.

Assim, sob a óptica da legitimação ativa, há duas espécies de ação penal (NUCCI, 2020, p. 198): (1) *pública* (art. 100, § 1º, do CP): quando o autor é o Ministério Público (MP); (1.1) *pública incondicionada*: o MP age de ofício, sem necessidade de requisição ou representação de quem quer que seja; (1.2) *pública condicionada*: o MP só está autorizado a agir caso haja representação do ofendido ou requisição do Ministro da Justiça (casos em que há menção expressa no texto da lei); (2) *privada* (art. 100, § 2º, do CP): quando o autor é a vítima ou seu representante legal, *e.g.*, quando se encontra referência "somente se procede mediante queixa".

A ação privada pode também ser subsidiária da pública, *i.e.*, seria uma ação pública, como regra, mas diante da inércia do órgão acusatório estatal, o direito de agir transferiu-se ao particular (arts. 100, § 3º, do CP, e 29 do CPP).

O § 5º, art. 171, do CP, introduzido pelo Pacote Anticrime, alterou a natureza da ação penal do crime de estelionato, que passou de pública incondicionada para pública condicionada à representação do ofendido (ou de seu representante legal), sem a qual, sequer poderia ser iniciado o inquérito policial (art. 5º, § 4º, do CPP), salvo exceções descritas nos incisos do referido § 5º, art. 171, do CP.

Essa modificação pode parecer simples, mas deve ser analisada com atenção.

No caso do § 5º, art. 171, do CP, tem-se norma híbrida, com conteúdo penal processual e material. Processual, por tratar de condicionalidade da ação penal pública, e material, porque a representação está associada ao prazo decadencial. Ademais, trata-se de alteração que beneficia o investigado, visto que o ofendido poderá renunciar ao prazo decadencial ou não representar. Com isso, a ação penal não poderá ser iniciada, pois ausente requisito de procedibilidade[5], sendo esta uma causa de extinção de punibilidade (METZKER, 2020, p. 26).

A jurisprudência tem entendido que para representar não são necessárias formalidades, a mera demonstração de interesse do ofendido em fazer o agressor responder a ação penal seria suficiente (GRECO, 2010, p. 212; CARNEIRO, 2021). O Tribunal de Justiça do Estado de São Paulo, inclusive, tem adotado o posicionamento que, quando realizado boletim de ocorrência, este, por si só, é capaz de suprir a representação, sendo possível dispensar o formalismo (DAGUER e SOARES, 2020). Dessa forma, encontrando-se nos autos a demonstração do interesse, o requisito de procedibilidade já teria sido cumprido.

Metzker (2020, p. 28) ressalta que, não raro, não se sabe quem é a vítima no estelionato. Diante disso, com a alteração promovida pela Lei Anticrime, o inquérito policial não poderá ser instaurado, pois requer representação. Sequer se pode apontar as exceções (diante das quais ter-se-ia ação pública incondicionada), pois para que ocorram tais hipóteses (art. 171, § 5º, I a IV, do CP),

---

5 Além das condições genéricas da ação penal (possibilidade jurídica do pedido, interesse de agir e legitimidade das partes), em algumas situações, também se exigem "condições específicas" ou "condições de procedibilidade", como nas ações de iniciativa pública condicionada (BADARÓ, 2009, p. 4). As *condições de procedibilidade* são exigidas pela lei para a propositura da ação penal, elas condicionam o exercício da ação penal nos casos determinados pela lei. As *condições de prosseguibilidade* distinguem-se das condições de procedibilidade, pois são aquelas que possibilitam o prosseguimento do processo, em casos determinados pela lei.

imprescindível que se saiba quem é a vítima, justamente para identificar-se a configuração da exceção.

Claro está que, sob a vigência da Lei Anticrime, caso a denúncia ainda não tenha sido ofertada, o MP deve aguardar a representação da vítima ou o decurso do prazo decadencial, cujo termo inicial, para os fatos pretéritos, é a vigência da nova lei.

Diante do exposto, por ter-se norma penal híbrida mais benéfica ao réu, a grande questão que se tem posto quanto à alteração trazida ao art. 171 do CP pela Lei Anticrime é: para os casos em que a denúncia foi ofertada, deve-se fazer retroagir a nova lei? Qual a extensão e o momento até onde ela se opera?

4 Posicionamento dos Tribunais Superiores

4.1 Quinta Turma do STJ – Habeas Corpus 573.093/SC (BRASIL, 2020a)

O assunto foi apreciado pela primeira vez num colegiado do Superior Tribunal de Justiça (STJ), em 09.06.2020, no Habeas Corpus (HC) 573.093/SC, de relatoria do Ministro Reynaldo Soares da Fonseca, na Quinta Turma, que, por unanimidade, não conheceu do HC.

O Ministro-Relator, apontando que o instituto da representação criminal é norma processual mista, posicionou-se no sentido de que a retroatividade da representação no crime de estelionato não alcançaria os processos cuja denúncia já tivesse sido oferecida, *i.e.*, "ações penais anteriores à inovação legislativa que se encontram em trâmite no primeiro grau, nos Tribunais, no STJ e STF" (BRASIL, 2020a, p. 9).

Trouxe o caso da entrada em vigor do art. 88 da Lei nº 9.099/95 (Lei dos Juizados Especiais Cíveis e Criminais), situação na qual o legislador definiu como proceder no caso dos processos em curso (art. 91 da mesma Lei[6]). Todavia, na hipótese em discussão, o legislador não teria se manifestado quanto à aplicação do novo entendimento às ações penais em trâmite, razão pela qual o relator entendeu aplicável a corrente doutrinária de Sanches Cunha, segundo a qual "se a inicial (denúncia) já foi ofertada, trata-se de ato jurídico perfeito, não sendo alcançado pela mudança. Não nos parece correto o entendimento de que a vítima deve ser chamada para manifestar seu interesse em ver prosseguir o processo. Essa lição transforma a natureza jurídica da representação

6 "Art. 91. Nos casos em que esta Lei passa a exigir representação para a propositura da ação penal pública, o ofendido ou seu representante legal será intimado para oferecê-la no prazo de trinta dias, sob pena de decadência."

de condição de procedibilidade em condição de prosseguibilidade. A lei nova não exigiu essa manifestação (como fez no art. 88 da Lei nº 9.099/95)" (BRASIL, 2020a, p. 11).

Assim, a "retroatividade da representação no crime de estelionato deve se restringir à fase policial, não alcançando o processo" (BRASIL, 2020a, p. 2, 12), dada a condição de procedibilidade da representação e não de prosseguibilidade.

Por fim, lembrou que, na hipótese, houve manifestação da vítima no sentido de ver o acusado processado, não se exigindo para tal efeito, consoante a jurisprudência do próprio STJ, formalidade para manifestação do ofendido.

4.2 Sexta Turma do STJ – Habeas Corpus 583.837/SC (BRASIL, 2020b)

O tema foi julgado em 04.08.2020, no HC 583.837/SC, de relatoria do Ministro Sebastião Reis Júnior, pela Sexta Turma do STJ, que por unanimidade votou com o relator.

O Ministro-Relator expôs que o § 5º, art. 171, do CP, acrescido pela Lei Anticrime, tem natureza mista e, diante da omissão legislativa na Lei nº 13.964/2019 em disciplinar os conflitos decorrentes da aplicação da lei penal no tempo, a solução viria pela via interpretativa: aplicar-se-ia retroativamente a nova regra e, por analogia, o art. 91 da Lei nº 9.099/95 (BRASIL, 2020b, p. 15-16).

Aduziu que o legislador não pretendeu, em nenhum momento, criar uma hipótese de *abolitio criminis*, um efeito de extinção de punibilidade. Considerou que o trânsito em julgado da ação penal é o limite para retroatividade do dispositivo (BRASIL, 2020b, p. 12).

Adicionalmente, observou que tanto o ato jurídico perfeito quanto a retroatividade da lei penal mais benéfica são direitos fundamentais de primeira geração (art. 5º, XXXVI e XL, da CF), aos quais o constituinte teria conferido a mesma "estatura constitucional". Assim, no caso em questão, entendeu que considerar o recebimento da denúncia como ato jurídico perfeito inverteria a natureza do direito fundamental, pois equivaleria a permitir que o Estado invocasse uma garantia fundamental frente a um cidadão. Destarte, ainda que se considerasse ato jurídico perfeito nessa hipótese, pelo princípio da proporcionalidade, salvaguardar a retroatividade do § 5º, art. 171, do CP protegeria de maneira mais adequada a dignidade da pessoa humana. Diante do exposto, concluiu pela impossibilidade da oposição da proteção do ato jurídico perfeito à retroatividade do novo dispositivo.

4.3 Primeira Turma do STF – Habeas Corpus 187.341/SP (BRASIL, 2020c)

Em decisão proferida em 13.12.2020, no HC 187.341/SP, de relatoria do Ministro Alexandre de Moraes, a Primeira Turma do Supremo Tribunal Federal (STF) entendeu, por unanimidade, que a regra do § 5º, art. 171, do CP, *não incide* em ações penais em curso, limitando-se a retroagir nos casos em que a denúncia ainda não tenha sido oferecida.

O relator decidiu conhecer o HC em caráter excepcional[7], diante da relevância e singularidade da matéria, devido à multiplicidade de HCs sobre o mesmo assunto, bem como por não haver, ainda, decisão proferida no âmbito do STF cujos precedentes serviriam de parâmetro para as demais instâncias.

O Ministro-Relator entendeu que, diante da natureza mista (penal/processual) da norma constante do § 5º, art. 171, do CP, sua aplicação retroativa seria obrigatória em todas as situações em que não tivesse sido oferecida a denúncia pelo MP (*i.e.*, não iniciada a ação penal), independentemente do momento da prática da infração penal, nos termos do art. 2º do CPP, por tratar-se de verdadeira "condição de procedibilidade da ação penal" (BRASIL, 2020c, p. 1, 12, 18). Entretanto, inaplicável quanto a todas as ações penais já iniciadas antes da entrada em vigor da Lei nº 13.964/2019, pois, quando do oferecimento da denúncia, a norma processual aplicável definia a ação como pública incondicionada, não exigindo qualquer condição para a instauração da persecução penal em juízo (BRASIL, 2020c, p. 20).

Ressaltou, ainda, que entendimento diverso necessitaria de expressa previsão legal, pois estaria transformando a "representação da vítima" em condição de prosseguibilidade da ação penal, alterando sua natureza jurídica de "condição de procedibilidade". Indicou que, em outras hipóteses, sempre houve expressa previsão legal, *e.g.*, a Lei nº 9.099/95. Ademais, já que não existe retratação da representação após o oferecimento da denúncia (art. 25 do CPP), tem-se ato jurídico perfeito, diante do qual a manifestação de interesse ou não da vítima no prosseguimento do feito não repercute na continuidade da persecução penal.

Diante disso, indeferiu a ordem do HC, por entender não cabível a "aplicação retroativa do § 5º do art. 171 do Código Penal, às hipóteses onde o Ministério Público tiver oferecido a denúncia antes da entrada em vigor da Lei nº 13.964/2019" (BRASIL, 2020c, p. 20).

---

7 Superando-se, para conhecer da impetração, a Súmula nº 291 do STF, que dispõe, "[n]ão compete ao Supremo Tribunal Federal conhecer de *habeas corpus* impetrado contra decisão do relator que, em *habeas corpus* requerido a tribunal superior, indefere a liminar".

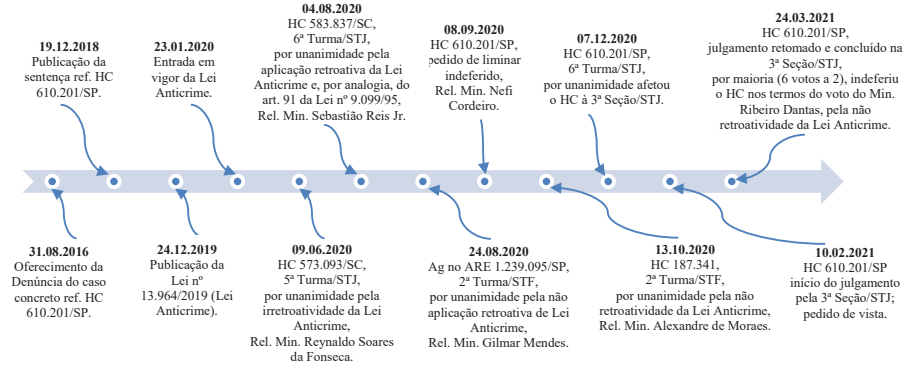
4.4 Terceira Seção do STJ – Habeas Corpus 610.201-SP (BRASIL, 2021a, 2021b)

Cumpre mencionar que em recente julgamento, concluído em 24.03.2021 (durante a elaboração deste artigo), a Terceira Seção do STJ uniformizou sua interpretação a respeito do tema, inclusive com votos da Sexta Turma (da Ministra Laurita Vaz e do Ministro Saldanha Palheiro), no julgamento do HC 610.201-SP, de Relatoria do Ministro Néfi Cordeiro (Figura 1).

A Terceira Seção, por maioria, indeferiu o HC, nos termos do voto do Ministro Ribeiro Dantas, que abriu divergência e foi nomeado relator para o acórdão (pendente de publicação), que foi assim ementado:

> "PROCESSUAL PENAL. *HABEAS CORPUS* SUBSTITUTIVO. ESTELIONATO. LEI Nº 13.964/2019 (PACOTE ANTICRIME). RETROATIVIDADE. INVIABILIDADE. ATO JURÍDICO PERFEITO. CONDIÇÃO DE PROCEDIBILIDADE. *WRIT* INDEFIRIDO.
>
> 1. A retroatividade da norma que previu a ação penal pública condicionada, como regra, no crime de estelionato, é desaconselhada por, ao menos, duas ordens de motivos.
>
> 2. A primeira é de caráter processual e constitucional, pois o papel dos Tribunais Superiores, na estrutura do Judiciário brasileiro é o de estabelecer diretrizes aos demais Órgãos jurisdicionais. Nesse sentido, verifica-se que o STF, por ambas as turmas, já se manifestou no sentido da irretroatividade da lei que instituiu a condição de procedibilidade no delito previsto no art. 171 do CP.
>
> 3. Em relação ao aspecto material, tem-se que a irretroatividade do art. 171, § 5º, do CP decorre da própria *mens legis*, pois, mesmo podendo, o legislador previu apenas a condição de procedibilidade, nada dispondo sobre a condição de prosseguibilidade. Ademais, necessário ainda registrar a importância de se resguardar a segurança jurídica e o ato jurídico perfeito (art. 25 do CPP), quando já oferecida a denúncia.
>
> 4. Não bastassem esses fundamentos, necessário registrar, ainda, prevalecer, tanto neste STJ quanto no STF, o entendimento 'a representação, nos crimes de ação penal pública condicionada, não exige maiores formalidades, sendo suficiente a demonstração inequívoca de que a vítima tem interesse na persecução penal. Dessa forma, não há necessidade da existência nos autos de peça processual com esse título, sendo suficiente que a vítima ou seu representante legal leve o fato ao conhecimento das autoridades' (AgRg no HC 435.751/DF, Rel. Min. Nefi Cordeiro, Sexta Turma, j. 23.08.2018, DJe 04.09.2018).
>
> 5. *Habeas corpus* indeferido."

Figura 1 – Linha do Tempo da temática afeta ao julgamento do HC 610.201/SP (retroatividade da Lei Anticrime quando já ofertada a denúncia pelo MP).



Fonte: Elaboração própria.

5 Posicionamento da Doutrina

Para Metzker (2020, p. 27), a inovação da Lei Anticrime aplicar-se-ia a todos os casos não transitados em julgado, devendo ser realizada a notificação da vítima ou de seu representante legal para informar se deseja representar criminalmente (caso já não tenha sido demonstrado), para que o processo ou inquérito possa permanecer tramitando. O prazo, por analogia com o art. 91 da Lei nº 9.099/95, seria de 30 dias, após o que, não havendo representação ou manifestação de interesse, a ação penal ou o inquérito policial deveria ser extinto em razão da decadência.

Igualmente, Moreira (2020) considera que se deve aplicar o novel dispositivo à ação em curso, ressalvada a coisa julgada, pois considera que se já houve o trânsito em julgado não seria cabível a retroatividade para o seu desfazimento. Como não haveria previsão específica, entende também pela aplicação analógica do art. 91 da Lei nº 9.099/95, contado da data da notificação, ao final do qual seria declarada a extinção da punibilidade pela decadência. Não sendo localizado o ofendido (ou representante), aguardar-se-ia o transcurso do prazo prescricional.

Da mesma forma, Fernandes (2020) conclui que, por tratar-se de norma penal híbrida, deveria retroagir em favor do réu, aplicando-se a todos os casos que não transitaram em julgado. Entende que, caso já iniciada a ação, poderia o réu ter sua punibilidade extinta por ausência de representação do ofendido na fase processual. Apregoa a analogia ao art. 91 da Lei nº 9.099/95. Não havendo representação em 30 dias da notificação, prevaleceria a extinção da punibilidade por decadência (observando-se o prazo de seis meses – arts.

38 do CPP e 103 do CP). Por fim, registra que, em caso de não representação, poder-se-ia entender, ainda assim, pelo prosseguimento do feito, caso em que o investigado/réu poderia utilizar a via do *habeas corpus* objetivando o trancamento do inquérito policial ou da ação penal.

Essa também é a posição de Lima (2020, p. 72) e Leite (2020), para quem não deve ser aplicado o prazo de 30 dias previsto na Lei dos Juizados Especiais, mas o prazo previsto no próprio CPP ou no CP (seis meses).

O Conselho Nacional de Procuradores-Gerais editou enunciados interpretativos sobre a Lei Anticrime, estabelecendo: "ENUNCIADO Nº 4 (ART. 171, § 5º, do CP – ART. 91 da Lei nº 9.099 c/c art. 3º do CPP): Nas investigações e processos em curso, o ofendido ou seu representante legal será intimado para oferecer representação no prazo de 30 dias, sob pena de decadência" (CNPG, 2020, p. 3).

Outro aspecto trazido diz respeito à grande quantidade de processos relativos à norma em estudo e a sobrecarga que acarreta ao Poder Judiciário. Tem-se ponderado que levar em consideração a posição da vítima seria um fator conveniente e favorável, pois ela quem deverá avaliar se seria adequado mover o aparato estatal frente à dimensão do dano suportado (DAGUER; SOARES, 2020).

Entendimento diverso dos expostos é apresentado pelo Professor Rogério Sanches Cunha (2020), que diverge da questão quando já oferecida a denúncia, já que nesse caso ter-se-ia um ato jurídico perfeito, não sendo possível convalidar a condição de procedibilidade para prosseguibilidade.

Conclusão e Considerações Finais

A Lei nº 13.964/2019 (Lei ou Pacote Anticrime) acrescentou o § 5º ao art. 171 do CP, tornando regra para a persecução penal do estelionato, a ação penal pública condicionada à representação, tendo por exceção as situações em que a vítima é a Administração Pública direta ou indireta; criança ou adolescente; deficiente mental; pessoas acima de 70 anos ou incapaz.

A partir da vigência da Lei Anticrime, foram apresentadas muitas impugnações referentes à aplicabilidade da nova regra aos casos de crime de estelionato cometido antes da vigência da Lei, para os quais o MP já havia oferecido a denúncia. Este artigo objetivou responder como agir nessas ações penais em curso.

Foram examinados dois julgados (divergentes) de Turmas especializadas em matéria de Direito Penal do STJ (Quinta e Sexta Turmas), bem como

um julgado da Primeira Turma do STF. Por fim, apresentou-se uniformização da interpretação do STJ em julgamento da Terceira Seção. Além disso, apresentou-se como a doutrina tem se posicionado.

Em síntese, quanto à retroatividade do novo art. 171, § 5º, do CP: (1) a Quinta Turma do STJ entende que ela não alcança os processos cuja denúncia foi oferecida; portanto, a retroatividade da representação no crime de estelionato deveria restringir-se à fase policial, não alcançando o processo; (2) a Sexta Turma do STJ entende que alcança todos os processos em curso, independentemente da fase processual, não gerando a extinção da punibilidade automática dos processos em curso, nos quais a vítima não tenha se manifestado favoravelmente à persecução penal, exigindo a abertura de prazo de 30 dias para representação da vítima; (3) a Primeira Turma do STF entende que não incide em ações penais em curso, limitando-se a retroagir nos casos em que a denúncia ainda não tenha sido oferecida (assim como a decisão da Quinta Turma do STJ).

Em que pese a grande maioria da doutrina ter posicionamento alinhado com a decisão da Sexta Turma do STJ (divergindo apenas quanto ao prazo para decadência), com base nas análises procedidas, entende-se que o posicionamento mais adequado seja o adotado pela Primeira Turma do STF e pela Terceira Seção do STJ.

Dessa forma, na aplicação da Lei Anticrime vislumbram-se duas hipóteses: (1) caso a denúncia ainda não tenha sido oferecida: o MP deve aguardar a representação da vítima ou o decurso do prazo decadencial, cujo termo inicial, para os fatos pretéritos, é a vigência da nova lei; (2) caso a denúncia já tenha sido ofertada: estar-se-ia diante de ato jurídico perfeito, que não seria alcançado pela mudança.

Por fim, não foi objeto deste estudo, mas cumpre mencionar que há vozes discordantes quanto à conveniência da mudança legislativa procedida pela Lei Anticrime no crime de estelionato, preocupação manifestada pelos Ministros Dias Toffoli e Rosa Weber na Sessão de julgamento do HC 187.341/SP, apesar de aquiescerem ao fato de que *legem habemus* (BRASIL, 2020d, 1h18m16s-1h21m00s,1h25m30s-1h26m10s).

TITLE: Fraud and the anticrime act: how to deal with the ongoing criminal prosecutions?

ABSTRACT: This paper deals with the change made by Act no. 13.964, 2019, known as the Anticrime Act, in the nature of the criminal prosecution of fraud, turning it, with some exceptions, into a public action subject to representation. Our objective was to examine the effect of this change on ongoing criminal prosecutions. To this end, a series of related legal institutes was analyzed, such as criminal law over time, more specifically the retroactivity of hybrid criminal rules, the nature of public criminal action subject to representation, as well the preservation of the victim's autonomy and fundamental rights of the accused.

Using the hypothetical-deductive method, we also analyzed two (divergent)judgments from the Superior Court of Justice and one from the Supreme Federal Court. We understood that the innovation brought by the Anticrime Law with regard to the crime of fraud, in despite of being a hybrid criminal rules, should not be applied retroactively to the ongoing criminal prosecutions.

KEYWORDS: Anticrime Act. Fraud. Irretroactivity. Public Criminal Action Subject to Representation. Ongoing Criminal Prosecutions.

Referências

ALBUQUERQUE, C. T. de. Precisamos falar de estelionato: os novos desafios da sociedade da informação. In: ÁVILA, G. N. de; WENCZENOVICZ, T. J. (Org.). *Criminologias e política criminal I*. [Recurso eletrônico on-line]. Florianópolis: CONPEDI, 2020. Disponível em: http://conpedi.danilolr.info/publicacoes/nl6180k3/4b62i7bw/Rmrn5s51roLH8pB5.pdf. Acesso em: 28 fev. 2021.

BADARÓ, G. H. R. I. Rejeição da denúncia ou queixa e absolvição sumária na reforma do Código de Processo Penal: atuação integrada de tais mecanismos na dinâmica procedimental. *Revista Brasileira de Ciências Criminais*, v. 76, jan./fev. 2009, p. 123-180. Disponível em: https://edisciplinas.usp.br/pluginfile.php/5319352/mod_resource/content/1/BADARO%20-%20Rejei%C3%A7%C3%A3o%20da%20den%C3%BAncia.pdf. Acesso em: 28 fev. 2021.

BITENCOURT, Cezar Roberto. *Tratado de direito penal*: parte geral. 26. ed. São Paulo: Saraiva Educação, 2020. v. 1.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. [2019a]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 fev. 2021.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. [2019b]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 20 fev. 2021.

BRASIL. *Decreto-Lei nº 3.689, de 3 de outubro de 1941*. Código de Processo Penal. [2019c]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 20 fev. 2021.

BRASIL. *Lei nº 8.069, de 13 de julho de 1990*. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. [2019e]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 20 fev. 2021.

BRASIL. *Lei nº 9.099, 26 de setembro de 1995*. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. [2018b]. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9099.htm. Acesso em: 20 fev. 2021.

BRASIL. *Lei nº 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm. Acesso em: 20 fev. 2021.

BRASIL. *Lei nº 10.741, de 1º de outubro de 2003*. Dispõe sobre o Estatuto do Idoso e dá outras providências. [2007]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm. Acesso em: 20 fev. 2021.

BRASIL. *Lei nº 13.964, de 24 de dezembro de 2019*. [Lei Anticrime. Pacote Anticrime]. Aperfeiçoa a legislação penal e processual penal. [2019d]. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm. Acesso em: 20 fev. 2021.

BRASIL. Superior Tribunal de Justiça [STJ]. *Habeas Corpus 182.714/RJ*. Processo Penal. Habeas corpus substitutivo de recurso ordinário. Orientação do STF: Não conhecimento. Patente ilegalidade. Concessão de ofício. Violação ao princípio da legalidade penal. Aplicação imediata de norma processual penal material. Relª Minª Maria Thereza de Assis Moura, Sexta Turma, j. 19.11.2012, DJe 29.11.2012 [2012]. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201001533527&dt_publicacao=29/11/2012. Acesso em: 7 mar. 2021.

BRASIL. Superior Tribunal de Justiça [STJ]. *Habeas Corpus 573.093/SC*. Rel. Min. Reynaldo Soares da Fonseca, Quinta Turma, j. 09.06.2020, DJe 18.06.2020 [2020a]. Disponível em: https://scon.stj.jus.br/

SCON/GetInteiroTeorDoAcordao?num_registro=202000865090&dt_publicacao=18/06/2020. Acesso em: 7 mar. 2021.

BRASIL. Superior Tribunal de Justiça [STJ]. *Habeas Corpus 583.837/SC*. Rel. Min. Sebastião Reis Júnior, Sexta Turma, j. 04.08.2020, DJe 12.08.2020 [2020b]. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202001217428&dt_publicacao=12/08/2020. Acesso em: 7 mar. 2021.

BRASIL. Superior Tribunal de Justiça [STJ]. *Terceira Seção – STJ – 10/02/2021*. Sessão de julgamento do Habeas Corpus 610.201-SP – Parte 1 de 2. (1h49m42s). [2021a]. Disponível em: https://www.youtube.com/watch?v=gqV5g6exz10. Acesso em: 26 mar. 2021.

BRASIL. Superior Tribunal de Justiça [STJ]. *Terceira Seção – 24/03/2021*. Sessão de julgamento do Habeas Corpus 610.201-SP – Parte 2 de 2. (1h36m45s). [2021b]. Disponível em: https://www.youtube.com/watch?v=NbHr1UxZpIU. Acesso em: 26 mar. 2021.

BRASIL. Supremo Tribunal Federal [STF]. *Habeas Corpus 187.341-SP*. Processo 0096108-07.2020.1.00.0000. Rel. Min. Alexandre de Moraes, 1ª T., j. 13.10.2020, Processo Eletrônico DJe-263. Divulgado em: 03.11.2020. Publicado em: 04.11.2020 [2020c]. Disponível em: redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754274277. Acesso em: 7 mar. 2021.

BRASIL. Supremo Tribunal Federal [STF]. *Primeira Turma do STF – Videoconferência_13/10/20*. Sessão de julgamento do *Habeas Corpus* 187.341/SP. (1h58m05s). [2020d]. Disponível em: https://www.youtube.com/watch?v=YwSdBR8mrNY. Acesso em: 13 mar. 2021.

CARNEIRO, M. V. de Q. O pacote anticrime e a irretroatividade da necessidade de representação no estelionato quanto aos processos em curso. *Conteúdo Jurídico*. 11 jan. 2021. Disponível em: https://www.conteudojuridico.com.br/consulta/artigos/56044/o-pacote-anticrime-e-a-irretroatividade-da-necessidade-de-representao-no-estelionato-quanto-aos-processos-em-curso. Acesso em: 28 fev. 2021.

CNPG [Conselho Nacional de Procuradores-Gerais]. Enunciados interpretativos da Lei nº 13.964/2019, Lei Anticrime. Grupo Nacional de Coordenadores de Centro de Apoio Criminal – GNCCRIM. Comissão Especial. 2020. Disponível em: https://criminal.mppr.mp.br/arquivos/File/GNCCRIM_-_ANALISE_LEI_ANTICRIME_JANEIRO_2020.pdf. Acesso em: 13 mar. 2021.

DAGUER, B.; SOARES, R. J. A modalidade de ação penal no crime de estelionato e suas implicações após o advento da Lei nº 13.964/2019. *Migalhas*, nº 4.840, 28 abr. 2020. Disponível em: https://www.migalhas.com.br/depeso/325683/a-modalidade-de-acao-penal-no-crime-de-estelionato-e-suas-implicacoes-apos-o-advento-da-lei-13-964-2019. Acesso em: 28 fev. 2021.

FERNANDES, A. M. Cinco alterações significativas a partir do pacote "anticrime". *Consultor Jurídico*. Opinião. Brasília-DF: 18 abr. 2020. Disponível em: https://www.conjur.com.br/2020-abr-18/opiniao-alteracoes-significativas-partir-pacote-anticrime. Acesso em: 28 fev. 2021.

GRECO, Rogério. *Código Penal comentado*. 4. ed. Niterói: Impetus, 2010.

GTPENAL. *Relatório do Grupo de Trabalho Destinado a Analisar e Debater as Mudanças Promovidas na Legislação Penal e Processual Penal pelos Projetos de Lei nº 10.372, de 2018, nº 10.373, de 2018, e nº 882, de 2019 – GTPENAL*. Coordenadora: Deputada Margarete Coelho. Relator: Deputado Capitão Augusto. Brasília: Câmara dos Deputados, 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1772332&filename=RRL+1/2019+GTPENAL. Acesso em: 25 fev. 2020.

JESUS, Damásio de. *Direito penal*. 12. ed. São Paulo: Saraiva, 1988. v. 1.

LEITE, Rodrigo. *Divergência no STJ! A retroatividade do novo § 5º do art. 171 (representação no crime de estelionato)*. [2020]. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2020/08/17/divergencia-no-stj-retroatividade-novo-%c2%a7-5o-art-171-representacao-no-crime-de-estelionato/. Acesso em: 13 mar. 2021.

LIMA, Renato Brasileiro de. *Pacote anticrime*: comentários à Lei 13.964/2019, artigo por artigo. Salvador: Juspodvim, 2020.

METZKER, D. *Lei Anticrime*: comentários às modificações no CP, CPP, LEP, Lei de Drogas e Estatuto do Desarmamento. 1. ed. Timburi: Cia do eBook, 2020.

MIRABETE, Julio Fabbrini. *Manual de direito penal*. São Paulo: Atlas, 1990. v. 1.

MOREIRA, Rômulo de Andrade. O crime de estelionato depende de representação: e agora? *Jusbrasil*. 2020. Disponível em: https://romulomoreira.jusbrasil.com.br/artigos/802022250/o-crime-de-estelionato-depende-de-representacao-e-agora. Acesso em: 2 mar. 2021.

MORO, Sérgio Fernando. *Exposição de Motivos ao Projeto de Lei nº 882/2019*. [2019]. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01nls2l5xb41dvocq34clht53094173.node0?codteor=1712111&filename=Tramitacao-PL+882/2019. Acesso em: 13 mar. 2021.

NUCCI, Guilherme de Souza. *Código de Processo Penal comentado*. 19. ed. Rio de Janeiro: Forense, 2020.

SANCHES CUNHA, Rogério. Informativo STJ 995: não retroage a condição de procedibilidade nas ações penais em curso por estelionato. *Meu Site Jurídico*, Juspodivm, 26 out. 2020. Disponível em: https://meusitejuridico.editorajuspodivm.com.br/2020/10/26/995-nao-retroage-condicao-de-procedibilidade-nas-acoes-penais-em-curso-por-estelionato/. Acesso em: 28 fev. 2021.

SOUZA NETTO, J. L.; FOGAÇA, A. R.; GARCEL, A. Lei Anticrime e a paradoxal afirmação do sistema acusatório. *Revista da Faculdade de Direito da FMP*, 15(1), p. 8-20, 2020. Disponível em: https://www.revistas.fmp.edu.br/index.php/FMP-Revista/article/view/170. Acesso em: 25 fev. 2021.

Recebido em: 09.06.2021

Aprovado em: 30.07.2021

ANEXO 7 - Breve panorama da trajetória histórica do reconhecimento dos direitos das empregadas domésticas no Brasil

Direito do Trabalho (UnB): SCHLOTTFELDT, Shana; BARROS, Elaine Sampaio. Breve panorama da trajetória histórica do reconhecimento dos direitos das empregadas domésticas no Brasil. In: TEIXEIRA, Érica Fernandes, et al. (Org.). *Direitos Sociais*: reflexões e desdobramentos. v. 2. 1. ed. Curitiba: Appris, 2021. Aceito em jun. 2020. No prelo.

SCHLOTTFELDT, Shana; BARROS, Elaine Sampaio. Breve panorama da trajetória histórica do reconhecimento dos direitos das empregadas domésticas no Brasil. In: TEIXEIRA, Érica Fernandes, et al. (Org.). *Direitos Sociais*: reflexões e desdobramentos. v. 2. 1. ed. Curitiba: Appris, 2021. Aceito em jun. 2020. No prelo.

5) BREVE PANORAMA DA TRAJETÓRIA HISTÓRICA DO RECONHECIMENTO DOS DIREITOS TRABALHISTAS DAS EMPREGADAS DOMÉSTICAS NO BRASIL

Shana Schlottfelt[1]

Elaine Sampaio de Barros[2]

INTRODUÇÃO

No decorrer do texto, a referência à categoria de trabalhadores/as domésticos/as será feita no feminino, por ser essa composta majoritariamente por mulheres – aproximadamente 92,3% do total da categoria, segundo dados do Instituto Brasileiro de Geografia e Estatística[3] –, bem como pelo fato de terem sido as mulheres protagonistas dos direitos das trabalhadoras domésticas no cenário político[4].

Esta pesquisa possui natureza qualitativa e foi desenvolvida por meio de pesquisa bibliográfica e jurisprudencial.

São objetivos deste estudo identificar: (1) a evolução histórica da concessão de direitos às empregadas domésticas; (2) as questões jurídicas acerca dos direitos das empregadas domésticas mais enfrentadas pelo Tribunal Regional do Trabalho da 10ª Região (TRT-10ª Região), que tem jurisdição no Distrito Federal-DF e no Estado do Tocantins-TO; (3) como o TRT-10ª Região tem decidido nessas matérias.

---

[1] Doutora em Informática pela Universidade de Brasília. Visiting PhD student at University of York. Mestre em Informática pela Universidade Carlos III de Madrid. Bacharelanda em Direito pela Universidade de Brasília. LLB exchange student at Australian National University. sunb2003@gmail.com. https://orcid.org/0000-0002-5481-0258.

[2] Bacharelanda em Direito pela Universidade de Brasília. elaine279@gmail.com. https://orcid.org/0000-0001-9640-5325.

[3] INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **No dia da mulher, estatísticas sobre trabalho mostram desigualdade.** Rio de Janeiro: IBGE, 2018. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/20287-no-dia-da-mulher-estatisticas-sobre-trabalho-mostram-desigualdade.html. Acesso em: 30 maio 2018.

[4] DULTRA, Eneida; MORI, Natália. **Trabalhadoras domésticas em luta:** direitos, igualdade e reconhecimento. Brasília: CFEMEA-ACDI/CIDA, 2008. p. 5.

O presente estudo é composto por três Seções. Na Seção 1, é feito um recorrido histórico do passado recente do país, buscando a caracterização do trabalho doméstico por seus aspectos de gênero (emprega em sua maioria mulheres), de raça (negra), de ambiente não econômico (desenvolvido no âmbito doméstico, "em casa"), por pessoas em geral com pouca escolaridade, que são mal/pouco remuneradas. Na Seção 2, é abordada a trajetória do reconhecimento formal dos direitos trabalhistas das empregadas domésticas no Brasil. A Seção 3 estuda a jurisprudência do Tribunal Regional do Trabalho da 10ª Região sobre a temática focando no período pós-Emenda Constitucional n.° 72/2013. Por fim, são apresentadas a conclusão e considerações finais acerca do tema.

Caracterização do trabalho doméstico como "de gênero", "de raça" e "de casa"

A construção histórica, social e cultural da ideia de ordem natural e de papéis dela decorrentes são comumente usadas para explicar a naturalização dos estereótipos presentes na sociedade, inclusive, os de gênero, de raça e até mesmo de classe, perpetuar relações de dominação e justificar a não concessão de direitos a certos grupos representativos.

O *ethos* forjado para a mulher contribuiu, ao longo da história do Brasil, para a negação do reconhecimento de direitos essenciais e para a desvalorização de suas atividades, dentre elas, o trabalho doméstico, visto como uma atividade praticamente exclusiva do universo feminino.

O trabalho doméstico é permeado pelo estereótipo de gênero e, por questões históricas, de raça e classe, de tal forma que é entendido como um trabalho de fácil execução, que não demanda maiores habilidades nem conhecimento técnico para ser realizado, sendo, por isso, muitas vezes sequer remunerado ou remunerado somente quando executado por uma terceira pessoa (a empregada doméstica).

Na busca de uma compreensão do perfil e vínculo patrão/empregada domésticas, faz-se necessária uma visita ao (recente) passado escravocrata brasileiro.

No Brasil Colônia, pessoas ditas "decentes" não realizavam trabalhos considerados perigosos, sujos e/ou manuais, cabendo sua execução a escravos, em sua maioria vindos de diversas regiões da África. Eis aqui o surgimento e recrudescimento do estereótipo de raça. Quando se fala do ambiente doméstico, as senhoras brancas não realizavam as atividades de casa, e, sim, as mucamas. Dentro dessa sociedade escravocrata, as mulheres negras possuíam diversos papéis: o de cozinheira, de ama de leite, de cuidadora da casa, de manceba (amante). Todos eles, além de ajudar a reforçar o

estereótipo de gênero, contribuíram para a criação do de raça, ao vincular a imagem da mulher negra ao desempenho de tais atividades.

A subordinação do escravo ao seu senhor acontecia tanto no âmbito econômico quanto no moral. O escravo, por gerar riquezas e ser considerado um bem, um verdadeiro objeto integrante do patrimônio do senhor, tinha o senhor como seu responsável, para representá-lo perante a sociedade e por ele responder. Havia, dessa maneira, uma confusão da relação de subordinação com uma relação afetiva, como acontecia com os escravos considerados "de casa"[5] e que permanece até hoje em diversas relações laborais, destacando-se o caso das empregadas domésticas[6].

O fim da escravidão, com a assinatura da Lei Áurea em 13 de maio de 1888, não foi implementado juntamente com políticas voltadas para a inserção dos ex-escravos na sociedade, deixando-os à mercê de sua própria sorte. Soma-se a isso, o incentivo governamental à imigração em massa de europeus para ocuparem os postos nas grandes lavouras[7] e ao preconceito decorrente da ideia de superioridade dos brancos em relação aos negros. Tem-se, como resultado dessa tessitura complexa, a marginalização social dos ex-escravos. Nesse contexto:

> [...] muitos ex-escravos permaneceram trabalhando para seus antigos senhores, notadamente aqueles que desenvolviam trabalho doméstico. Tornaram-se "criados", alguns hipocritamente considerados como sendo "quase da família", laborando dia e noite unicamente em troca de teto e sustento, sem direito à remuneração, férias ou herança[8].

Diante da dificuldade de inserção no mercado de trabalho enfrentada pela população masculina de libertos e a consequente impossibilidade de aquisição de meios para garantir sua subsistência e de sua família, gerou-se o estereótipo de que "o negro é por natureza vadio e só trabalha debaixo de açoitadas". Nesse contexto, mesmo sendo mal remunerada, praticamente a única que conseguiu inserção no mercado foi a mulher negra, exercendo o lavor de empregada doméstica. Como consequência, tornou-se chefe e provedora das necessidades de sua família, contrariando o entendimento patriarcal do

---

[5] FREYRE, Gilberto. **Casa Grande & Senzala:** formação da família brasileira sob o regime patriarcal. 48. ed. rev. São Paulo: Global, 2003. p. 435.
[6] DAMATTA, Roberto. **O que faz o Brasil, Brasil?** Rio de Janeiro: Rocco, 1986. p. 27-28.
[7] FURTADO, Celso. **Formação econômica do Brasil.** 34. ed. São Paulo: Companhia das Letras, 2007. p. 181.
[8] FERRAZ, Fernando B.; RANGEL, Helano M. V. A discriminação sociojurídica ao emprego doméstico na sociedade brasileira contemporânea: uma projeção do passado colonial. *In:* ENCONTRO NACIONAL DO CONPEDI, XIX., 2010, Fortaleza. **Anais** [...]. Tema: "Direitos Fundamentais e Transdisciplinaridade". Florianópolis: Fundação Boiteux, 2010. v. 1, p. 8644.

papel da mulher dentro da sociedade. Fato gerador de outro estereótipo atribuído ao homem negro, o de "cidadão de segunda categoria", por não conseguir desempenhar o seu papel e ser sustentado por sua mulher[9].

Esse quadro estereotipado acerca do emprego doméstico teve suas raízes na escravidão, mas suas consequências permanecem até os dias atuais. O trabalho doméstico é visto, em sua maioria, como atividade feminina, com predominância negra e caracterizada pelo aspecto informal. Fato é que, segundo dados do IBGE[10], apenas 7,7% dos empregados domésticos são homens, sendo que esse é o emprego de 5,9 milhões de brasileiras. Somente no Distrito Federal, a quantidade de mulheres negras trabalhando como empregada doméstica equivale a 80,4% do total de trabalhadoras nessa atividade[11]. E no Brasil, apenas 28,4% dos empregados domésticos possuem Carteiras de Trabalho e Previdência Social assinada[12]. Isso se deve tanto à falta de interesse dos empregadores, como às barreiras impostas pelas próprias trabalhadoras por acreditarem que assiná-la como empregada doméstica irá "sujar" sua carteira[13].

Além disso, o emprego doméstico também é caracterizado pela lenta concessão de direitos, fato que será melhor abordado na próxima Seção.

Trajetória do reconhecimento dos direitos trabalhistas das empregadas domésticas no Brasil

O emprego doméstico ainda é visto como uma atividade marcada pelo preconceito de gênero, pelo ranço do escravagismo e pela consideração da empregada como "pertencente à família" (mas sem verdadeiramente integrá-la).

Sequer é possível dizer que tal atividade está inserida no rol que engloba o conceito de trabalho decente da Organização Internacional do Trabalho (OIT), pois não está livre de preconceitos, não goza de todos os direitos sociais e muito menos possui condições seguras de trabalho[14].

---

[9] JESUS, Eunice Aparecida de. **Preconceito racial e igualdade jurídica no Brasil.** 1980. Dissertação (Mestrado em Direito do Estado) – Faculdade de Direito, Universidade de São Paulo, USP, São Paulo, 1980. p. 171.

[10] INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE), 2018.

[11] DEPARTAMENTO INTERSINDICAL DE ESTATÍSTICA E ESTUDOS SOCIOECONÔMICOS (DIEESE). **Emprego Doméstico no Distrito Federal, em 2017**. São Paulo: DIEESE, 2018. Disponível em: https://www.dieese.org.br/analiseped/2018/2018empreDomBSB.html. Acesso em: 26 maio 2018.

[12] INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE), 2018.

[13] FERRAZ; RANGEL, 2010, p. 8634.

[14] ORGANIZAÇÃO INTERNACIONAL DO TRABALHO (OIT). **Convenção e Recomendação sobre Trabalho Decente para as Trabalhadoras e os Trabalhadores Domésticos.** Brasília: OIT, 2011. p. 2.

No início do Brasil República, a relação privada era mascarada pelos "ajustes" exigidos pelo Estado, feitos verbalmente e em nada comparados a um contrato empregatício garantidor de direitos. Esse cenário durou por mais de 40 anos, e perdura no tempo como uma "situação irregular"[15].

Um dos primeiros instrumentos legais a tratar especificadamente sobre o tema foi o Decreto n.º 16.107/1923, que definiu as profissões consideradas domésticas. Quase vinte anos após, o Decreto-Lei n.º 3.078/1941 definiu o emprego doméstico, reforçou a obrigatoriedade da carteira profissional para a categoria e a indenização por falta de aviso prévio.

O instrumento legal protetor dos trabalhadores, o Decreto-Lei n.º 5.452/1943 (Consolidação das Leis Trabalhistas – CLT), instituído em 1º de maio de 1943, pouco mais de cinquenta anos após o fim (formal) da escravidão, no art. 7º, "a", excluiu de seu escopo de proteção as empregadas domésticas. Era pacífica e aceitável, naquele tempo, a opinião que as atividades limitadas aos restritos ambientes residenciais carregavam características peculiares, mostrando-se prematuro o desejo de beneficiá-las com certos direitos. Destaque-se que na época em que a CLT entrou em vigor, o Brasil atravessava um período ditatorial sob o governo de Getúlio Vargas. O ambiente econômico na década de 1940 era de considerável atraso. A maioria da população residia no campo. Nas poucas cidades de grande porte, a industrialização dava os primeiros passos. Nesse cenário de incipiente desenvolvimento, não é de se estranhar que o avanço das regras trabalhistas, resultou muito mais de uma iniciativa governamental, para atender a interesses conservadores, do que em decorrência da pressão de um operariado consciente. Claro está que, pela cultura vigente à época, a lei nova jamais poderia ser estendida a toda a classe de trabalhadores.

Ferraz e Rangel[16] apontam duas justificativas para o não reconhecimento do trabalho doméstico como uma relação protegida de emprego: (1) sua característica não econômica; (2) pelo serviço ser prestado a pessoa ou a família; às quais acrescenta-se a justificativa de Carvalho[17]: (3) por medo de atingir a classe média urbana.

Disponível em: http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_169517.pdf. Acesso em: 30 maio 2018.

[15] PAOLI, Maria Celia. Trabalhadores e cidadania. Experiência do mundo público na história do Brasil moderno. *In*: SOUSA JUNIOR, José; AGUIAR, A. (org.) **Introdução crítica ao Direito do Trabalho**. Brasília: Universidade de Brasília, 1993. p. 29.

[16] FERRAZ; RANGEL, 2010, p. 8644.

[17] CARVALHO, José Murilo de. **Cidadania no Brasil:** o longo Caminho. 3. ed. Rio de Janeiro: Civilização Brasileira, 2002. p. 123.

Define-se como uma atividade não econômica aquela não voltada à geração de lucro, como:

> Essas atividades não são organizadas de forma capitalista, porque se realizam no interior de residências particulares e as patroas/patrões não são empresários. O contrato de trabalho firmado, seja verbal ou escrito, define que as empregadas realizam tarefas cujo produto — cozimento de alimentos (bens) ou lavagem de roupas e pratos (serviços) — é consumido diretamente pela família. Esses bens/serviços não circulam no mercado e não se mobiliza capital para a realização dessas tarefas, mas rendas pessoais[18].

Isto é, o tempo validado pelo sistema capitalista é aquele empregado nas atividades de produção e gerador de mais valia[19].

A regulamentação do trabalho doméstico e a concessão de pouquíssimos direitos sociais somente ocorreram com a Lei n.º 5.859/1972, quase trinta anos após a entrada em vigor da CLT. Aquele diploma legal concedeu férias anuais de 20 dias a cada 12 meses trabalhados (art. 3º), concessão inferior ao estipulado pela CLT, diga-se de passagem; bem como a possibilidade de ingresso na Previdência Social (art. 4º). Note-se que a aludida lei se omitiu quanto a aspectos importantes nas relações de trabalho doméstico, nada mencionando a respeito de salário-mínimo, jornada de trabalho, intervalo, descanso semanal remunerado, 13º salário, adicionais, verbas rescisórias, entre outros.

O vazio legal vivenciado pela categoria somente veio a ser preenchido parcialmente com a Constituição Federal de 1988 (CF/1988). Apesar de seu intento de promover direitos e garantias fundamentais a todo(a)s, em seu texto original, não estendeu vários direitos sociais às trabalhadoras domésticas, perpetuando o estereótipo e a desvalorização social relativos ao seu trabalho. Justamente os direitos que "permitem às sociedades politicamente organizadas reduzir os excessos de desigualdade produzidos pelo capitalismo e garantir um mínimo de bem-estar para todos. A ideia central em que se baseiam é a da justiça social"[20].

Originalmente, dos 34 direitos sociais dos trabalhadores previstos no art. 7º, somente 9 foram concedidos às empregadas domésticas, dentre eles o direito ao salário mínimo (IV); irredutibilidade do salário (VI); 13º salário (VIII); repouso semanal remunerado (XV); férias anuais remuneradas, com pelo menos um terço a mais do que o

[18] PEREIRA, Hildete. **O serviço doméstico remunerado no Brasil:** De criadas a trabalhadoras, Texto para Discussão nº 565. Rio de Janeiro: IPEA, 1998, p. 1-2.
[19] DULTRA; MORI, 2008, p. 114.
[20] CARVALHO, 2002, p. 10.

salário normal (XVII); licença maternidade (XVIII); licença paternidade (XIX); aviso prévio proporcional ao tempo de serviço (XXI); e aposentadoria (XXIV).

Essa exclusão de direitos das trabalhadoras domésticas é uma das inconsistências internas da Constituição, pois se pode dizer que ela promoveu a desigualdade ao dignificar todos os trabalhadores, com a exceção do doméstico. Essa situação somente foi atenuada com a Emenda Constitucional (EC) n.º 72/2013, conhecida como PEC das empregadas domésticas, que ao ser promulgada, acrescentou ao rol de direitos garantidos às empregadas domésticas contido no parágrafo único do art. 7º da Constituição, os incisos VII, X, XIII, XVI, XXII, XIV, XXX, XXXI e XXXIII e, quando preenchidos certos requisitos, os incisos I, II, III, IX, XII, XXV e XXVIII.

Em que pesem as alterações promovidas, o emprego doméstico ainda se recente quanto à concessão de alguns direitos, tais como o piso salarial proporcional (art. 7º, V); a jornada de seis horas para trabalho em turnos ininterruptos de revezamento (art. 7º, XIV); a proteção do mercado de trabalho da mulher (art. 7º, XX); o adicional de remuneração para as atividades penosas, insalubres ou perigosas (art. 7º, XXIII) [21].

A Lei n.º 10.208/2001 concedeu à trabalhadora doméstica a faculdade de ser incluída no Fundo de Garantia ao Tempo de Serviço (FGTS) e o direito ao seguro-desemprego. A Lei n.º 11.324/2006 concedeu férias remunerada de 30 dias, com adicional constitucional de 1/3, após doze meses de trabalho prestados a mesma pessoa ou família; proibiu tanto os descontos do salário decorrentes do fornecimento de alimentação, higiene, habitação e vestuário, quanto a dispensa sem justa causa da empregada gestante; alterou a legislação do imposto de renda das pessoas físicas, acrescentado a contribuição patronal paga à Previdência Social pelo empregador doméstico.

Outro dispositivo importante é a Lei Complementar (LC) n.º 150/2015, que definiu, em seu art.1º, empregada doméstica como aquela "que presta serviços de forma contínua, subordinada, onerosa e pessoal e de finalidade não lucrativa à pessoa ou à família, no âmbito residencial destas, por mais de 2 (dois) dias por semana" (BRASIL, 2015) . Essa definição é significativa para diferenciar a empregada doméstica da diarista. Além disso, proibiu a contratação de menores de 18 anos para o exercício de tal atividade; limitou a jornada de trabalho; definiu o valor da hora extraordinária em, no mínimo, 50% superior ao valor da hora normal; permitiu o regime de tempo parcial; regulou o contrato

[21] CALVET, Felipe Augusto de Magalhães. A evolução da legislação do trabalhador doméstico. **Revista eletrônica [do] Tribunal Regional do Trabalho da 9ª Região**, Curitiba, v. 2, n. 17, p. 60-67, abr. 2013. p. 67. Disponível em: https://hdl.handle.net/20.500.12178/96998. Acesso em: 2 jun. 2018.

de experiência; criou normas para a empregada que acompanha o empregador em viagem; tornou obrigatório o registro do horário de trabalho; concedeu intervalo para repouso ou alimentação; instituiu o regime de compensação de jornada; desenvolveu regras para o trabalho noturno; tornou obrigatória a inclusão no FGTS; regulamentou o inc. XXI do art. 7º da CF, sobre o aviso prévio proporcional; concedeu o seguro desemprego e os benefícios concedidos à incapacidade decorrente de um acidente de trabalho; instituiu o Simples doméstico[22].

Essa lei resultou na redução da jornada de trabalho, porém, em nada impactou o salário. No que diz respeito à formalização, houve um aumento, mas não se pode afirmar que isso se deu devido à lei, tendo em vista a possibilidade de substituição da empregada doméstica por uma diarista[23].

A jurisprudência do Tribunal Regional do Trabalho da 10ª Região

A metodologia usada na pesquisa jurisprudencial consistiu-se na análise de 49 acórdãos do TRT-10ª Região, proferidos no período de janeiro de 2013 a maio de 2018. Essa limitação temporal foi escolhida por englobar alguns julgados anteriores à aprovação da EC n.º 72/2013, estendendo-se até 5 anos de sua aprovação.

Foi empregado o mecanismo de pesquisa de jurisprudência do site do TRT-10ª Região[24], usando a expressão "empregada doméstica", na modalidade "expressão exata" e com limitação de resultados para "acórdãos". A consulta retornou 87 acórdãos, dos quais foram selecionados 49. Os critérios para a seleção foram: (i) pertinência temática, excluindo-se os casos que não falavam especificadamente de empregadas doméstica e seus direitos (e.g., casos de caseiros(as), jardineiro(a)s, prestador(a) de serviços gerais); (ii) excluiu-se os casos afetos à aplicação da Súmula de n.º 377 do TST[25]; (iii) excluiu-se questões meramente processuais.

---

[22] Sistema de dados e recolhimento unificado para os tributos na relação de emprego do doméstico.
[23] COSTA, J.; BARBOSA, A. L. N. H.; HIRATA, G. **Efeitos da ampliação dos direitos trabalhistas sobre a formalização, jornada de trabalho e salários das empregadas domésticas**. (Texto para Discussão, n. 2241). Brasília: Ipea, 2016. p. 37.
[24] www.trt10.jus.br/jurisprudencia/jsf/index.jsf. Acesso em: 9 de junho de 2018.
[25] Súmula n.º 377 - PREPOSTO. EXIGÊNCIA DA CONDIÇÃO DE EMPREGADO. Exceto quanto à reclamação de empregado doméstico, ou contra micro ou pequeno empresário, o preposto deve ser necessariamente empregado do reclamado. Inteligência do art. 843, § 1º, da CLT e do art. 54 da Lei Complementar n.º 123, de 14 de dezembro de 2006. BRASIL. Tribunal Superior do Trabalho. **Súmula 377**. Res. 146/2008, DJ 28/04/2008, 02 e 05/05/2008. Disponível em: https://www3.tst.jus.br/jurisprudencia/Sumulas_com_indice/Sumulas_Ind_351_400.html#SUM-377. Acesso em 9 de jun. de 2018.

Após essa triagem inicial, todos os acórdãos selecionados foram agrupados segundo o conteúdo. Constatou-se que as principais questões enfrentadas foram: (1) critérios usados para caracterizar a relação empregatícia (e.g., diarista versus empregada doméstica) (23 casos); (2) aplicação da multa dos art. 467 e 477 da CLT[26] (17 casos); (3) recebimento por horas extras, intervalo intrajornada e férias (7 casos); (4) concessão de FGTS (4 casos); (5) demissão por justa causa (4 casos); (6) possibilidade de assistência sindical (1 caso); (7) recebimento de indenização por danos morais (1 caso); (8) pagamento inferior ao salário mínimo (1 caso); (9) ressarcimento de valor pago em passagem (1 caso).

A **relação empregatícia** foi discutida em 23 casos, dos quais em 5 foi reconhecido o emprego doméstico, sendo que em 18 decidiu-se pela prestação de serviço como diarista. Os principais argumentos para o deferimento da relação de emprego foram: (i) ter trabalhado por pelo menos três dias durante a semana na mesma casa; (ii) ter trabalhado em tempo superior a dez anos, com carteira assinada, apesar de variar a intensidade da prestação de serviço de uma semana para outra; (iii) a não descaracterização do emprego doméstico quando a obreira alimentava animais da fazenda, se o seu labor principal ocorria no âmbito doméstico.

Os principais motivos para o indeferimento da relação de emprego foram: (i) não cumprir o pressuposto da continuidade, disposto no art. 1º, da Lei n.º 5.869/1972, ao trabalhar menos que três, e, às vezes, quatro dias na mesma casa, apesar da LC n.º 150/2015 estabelecer o quantum temporal de mais de dois dias; (ii) a alternância na quantidade de dias trabalhados de uma semana para outra; (iii) trabalhar para pessoa jurídica.

Quanto à **aplicabilidade das multas dos art. 467 e 477 da CLT**, verbas rescisórias, o Tribunal possui uma posição controvertida, ora decidindo pela aplicação, ora a rechaçando. Dos 17 acórdãos analisados sobre a temática, 11 decidiram pela

[26] Art. 467. Em caso de rescisão de contrato de trabalho, havendo controvérsia sobre o montante das verbas rescisórias, o empregador é obrigado a pagar ao trabalhador, à data do comparecimento à Justiça do Trabalho, a parte incontroversa dessas verbas, sob pena de pagá-las acrescidas de cinquenta por cento (Redação dada pela Lei n.º 10.272, de 5.9.2001).
Art. 477. É assegurado a todo empregado, não existindo prazo estipulado para a terminação do respectivo contrato, e quando não haja ele dado motivo para cessação das relações de trabalho, o direto de haver do empregador uma indenização, paga na base da maior remuneração que tenha percebido na mesma empresa (Redação dada pela Lei n.º 5.584, de 26.6.1970). Redação anterior à Lei n.º 13.467, de 2017.
BRASIL. **Decreto-Lei nº 5.452, de 1ºde maio de 1943**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em 9 de junho de 2018.

refutação da multa, ao passo que os outros 6 decidiram pela aplicação, partindo das mais variadas justificativas.

Os principais argumentos usados para o indeferimento foram: (i) o art. 7º, alínea "a", da CLT não compreende as empregadas domésticas no âmbito de incidência de tais multas; (ii) o direito a referida multa não se encontra listado entre os direitos previstos às empregadas domésticas no art. 7º da CF/1988, mesmo com a redação dada pela EC n.º 72/2013; (iii) não existe a previsão legal exigida pela alínea "a" do art. 7º da CLT; (iv) há um entendimento do TST que afasta a aplicação do art. 477 ao contrato de emprego, devido à interpretação literal do art. 7º, alínea "a", da CLT; (v) não há previsão da multa na LC n.º 150/2015, nem na Lei n.º 5.859/72; (vi) não há expressa determinação legal.

Ao passo que os argumentos usados para o deferimento foram: (i) a Constituição contém princípio protetivo, garantindo outros direitos que visem à melhoria da condição social do empregado, por isso, o art. 467 da CLT tem como destinatários todos os trabalhadores; (ii) o art. 477 da CLT é aplicável sempre que houver a inobservância, pelo empregador, do prazo legal; (iii) o art. 477 da CLT é aplicável a qualquer relação de trabalho indistintamente; (iv) aplica-se ao regime doméstico a LC n.º 150/2015 (lei específica), e, subsidiariamente, à CLT.

O direito à **hora extra** foi reconhecido em um dos quatro acórdãos que trataram do tema. Entendeu-se em 2 casos não ser devido o pagamento de horas extras ao período trabalhado anterior à EC n.º 72/2013, pois a limitação da jornada de trabalho e a previsão do pagamento de horas extraordinárias somente ocorreu com a promulgação da EC. Além disso, o Tribunal entendia que antes da LC n.º 150/2015 quem deveria provar a realização de horas extras era a empregada, após a edição da referida LC, por força do art. 12 que instituiu o registro obrigatório do horário de trabalhado, o ônus da prova passou a recair sobre o empregador. Em um dos casos (de 2014), o juiz de primeira instância indeferiu o pedido de concessão do pagamento por falta de regulamentação, o Desembargador que julgou o caso rechaçou esse entendimento, pois considerou que o juiz de origem não deveria ter deixado de analisar a pretensão alegando a inexistência de lei, mas deveria ter usado os métodos de integração constantes no art. 8º da CLT. Por tal motivo, o desembargador determinou o retorno dos autos à primeira instância para novo julgamento.

O pagamento por **intervalo intrajornada** foi analisado em um caso. Entendeu-se somente ser devido o pagamento do período trabalhado posteriormente à LC n.º

150/2015, pelo fato do art. 12 ter tornado obrigatório o registro do horário de trabalho do empregado doméstico.

Em relação às **férias**, foram identificados dois casos, um em 2014 e outro em 2018. No primeiro, decidiu-se pelo pagamento de férias indenizadas, a serem pagas em dobro e acrescidas do terço constitucional, para a obreira que nunca gozou de férias. No outro caso, decidiu-se pelo pagamento em dobro do valor das férias vendidas e pagas de maneira simples.

Sobre o **FGTS**, de quatro casos, em um entendeu-se que a aplicação é uma faculdade do empregador, nos moldes do art. 3º-A da Lei n.º 5.859/72, de maneira que, optando pelo recolhimento, era obrigado a fazê-lo enquanto durasse o contrato de trabalho. Em um caso de 2016, decidiu-se que, pelo fato de a empregadora recolher voluntariamente o FGTS, a empregada dispensada sem justa causa faria jus ao levantamento do FGTS depositado e ao percebimento da multa de 40% (quarenta por cento). Em outro caso, decidiu-se que a LC n.º 150/2015 mudou a forma de recolhimento da multa de 40% do FGTS, ao acrescentar aos 8% já pagos, o valor de 3,2% sobre a remuneração devida à empregada, para o pagamento de indenização por demissão por justa causa ou por culpa do empregador, sendo instituído no art. 22[27] que só é devida a alíquota mensal e antecipada para tais casos. Por fim, em um último caso, entendeu-se não ser devida a multa de 40% do FGTS, pois ela teria a mesma natureza jurídica da multa de 3,2%, diferindo-se somente em relação ao tempo de seu depósito.

Quatro acórdãos versaram sobre **demissão por justa causa**. Foi decidido que: (i) empregada demitida por justa causa não possui direito à estabilidade gestante; (ii) por se tratar da mais severa penalidade aplicada à empregada, o empregador deve provar os motivos da dispensa com prova robusta e convincente.

Em relação à **assistência sindical** para a validade do pedido de demissão do empregado com mais de um ano de serviço, o Tribunal, no único caso julgado sobre o tema, entendeu que não se aplica às trabalhadoras domésticas, uma vez que a profissão é regida por lei própria que não tem previsão legal sobre o tema.

[27] Art. 22. O empregador doméstico depositará a importância de 3,2% (três inteiros e dois décimos por cento) sobre a remuneração devida, no mês anterior, a cada empregado, destinada ao pagamento da indenização compensatória da perda do emprego, sem justa causa ou por culpa do empregador, não se aplicando ao empregado doméstico o disposto nos §§ 1º a 3º do art. 18 da Lei n.° 8.036, de 11 de maio de 1990. BRASIL. **Lei Complementar nº 150, de 1º junho de 2015**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp150.htm. Acesso em: 9 de jun. de 2018.

Em um caso foi discutido o pagamento de **indenização por danos morais** pelo fato de a empregada doméstica ter tido a expectativa de aposentadoria frustrada, após 20 anos de contrato de trabalho sem contribuições previdenciárias por parte da empregadora.

O Tribunal decidiu (no único caso encontrado a respeito) que o **salário** recebido pelo labor pode ser inferior ao mínimo legal quando não forem cumpridas as 8 horas diárias e as 44 horas semanais, sendo proporcional ao tempo trabalhado.

Um caso disse respeito ao **ressarcimento de valores pagos em passagem**. O TRT-10ª Região entendeu ser devido o ressarcimento corrigido do valor, a título de custeio.

Depreende-se que, em alguns casos, os acórdãos prolatados não concederam direitos às empregadas além dos já reconhecidos; em poucos casos, optou-se por seguir o entendimento da jurisprudência ao invés do constante em lei. Além disso, ao aplicar a lei, na maioria das situações, o Tribunal demonstrou interpretá-la de uma maneira literal, concedendo o mínimo legal de direitos à categoria.

Tal constatação corrobora os achados de Dultra e Mori[28], que, no que diz respeito ao emprego das normas atinentes às empregadas domésticas pelo judiciário, observaram que na prática a aplicação se dá de uma maneira legalista e conservadora, desfavorecendo em grande medida as empregadas domésticas. Tal estudo indicou, assim como o nosso, que a principal demanda referente ao trabalho doméstico no poder judiciário envolve o pedido de reconhecimento do vínculo empregatício (em especial a distinção entre diaristas e empregadas domésticas) e os direitos dele resultantes.

CONCLUSÃO

A caminhada histórica dos direitos das empregadas domésticas tem demonstrado que os estereótipos de gênero e raça, presentes na sociedade brasileira, retardaram e ainda postergam a conquista de direitos pela categoria.

A longa espera por reconhecimento de direitos evidencia o desprestígio e a confusa relação entre empregadas domésticas e empregadores, que ao imiscuírem afeto, gentileza e gratidão na relação econômica empregatícia geram a perpetuação de abusos, a negação de direitos e a incapacidade/dificuldade/desinteresse do Governo em alterar/regular relações de trabalho que se mesclam/confundem com relações privadas.

[28] DULTRA; MORI, 2008, p. 62.

O reconhecimento de direitos deve caminhar junto com sua efetividade e com uma aplicação judicial benéfica à trabalhadora, fato que ainda não acontece, pois, como identificado na análise de acórdãos do TRT da 10ª Região, o judiciário não tem realizado uma interpretação favorável à trabalhadora doméstica, prevalecendo a interpretação literal das leis. Além disso, alguns julgados, em vez de aplicar os direitos recentemente conquistados, utilizaram-se de critérios mais desfavoráveis desenvolvidos jurisprudencialmente.

Essa caminhada ainda possui um longo caminho pela frente, almejando a conquista da equiparação dos direitos constitucionalmente previstos para outras categorias e da merecida valorização social.

REFERÊNCIAS

BRASIL. **Lei Complementar nº 150, de 1º junho de 2015.** Dispõe sobre o contrato de trabalho doméstico; altera as Leis nº 8.212, de 24 de julho de 1991, nº 8.213, de 24 de julho de 1991, e nº 11.196, de 21 de novembro de 2005; revoga o incido I do art. 3º da Lei nº 8.009, de 29 de março de 1990, o art. 36 da Lei nº 8.213, de 24 de julho de 1991, a Lei nº 5.859, de 11 de dezembro de 1972, e o inciso VII do art. 12 da Lei nº 9.250, de 26 de dezembro de 1995; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/LCP/Lcp150.htm. Acesso em: 9 de jun. de 2018.

BRASIL. **Decreto-Lei nº 5.452, de 1ºde maio de 1943**. Aprova a Consolidação das Leis do Trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em 9 de junho de 2018.

BRASIL. Tribunal Superior do Trabalho. **Súmula 377**. Exceto quanto à reclamação de empregado doméstico, ou contra micro ou pequeno empresário, o preposto deve ser necessariamente empregado do reclamado. Inteligência do art. 843, § 1º, da CLT e do art. 54 da Lei Complementar n.º 123, de 14 de dezembro de 2006. Res. 146/2008, DJ 28/04/2008, 02 e 05/05/2008. Disponível em: https://www3.tst.jus.br/jurisprudencia/Sumulas_com_indice/Sumulas_Ind_351_400.html#SUM-377. Acesso em 9 de jun. de 2018.

CALVET, Felipe Augusto de Magalhães. A evolução da legislação do trabalhador doméstico. **Revista eletrônica [do] Tribunal Regional do Trabalho da 9ª Região**, Curitiba, v. 2, n. 17, p. 60-67, abr. 2013. Disponível em: https://hdl.handle.net/20.500.12178/96998. Acesso em: 2 jun. 2018.

CARVALHO, José Murilo de. **Cidadania no Brasil:** o longo Caminho. 3. ed. Rio de Janeiro: Civilização Brasileira, 2002.

COSTA, J.; BARBOSA, A. L. N. H.; HIRATA, G. **Efeitos da ampliação dos direitos trabalhistas sobre a formalização, jornada de trabalho e salários das empregadas domésticas**. (Texto para Discussão, n. 2241). Brasília: Ipea, 2016.

DAMATTA, Roberto. **O que faz o Brasil, Brasil?** Rio de Janeiro: Rocco, 1986.

DEPARTAMENTO INTERSINDICAL DE ESTATÍSTICA E ESTUDOS SOCIOECONÔMICOS. **Emprego Doméstico no Distrito Federal, em 2017.** São Paulo: DIEESE, 2018. Disponível em: https://www.dieese.org.br/analiseped/2018/2018empreDomBSB.html. Acesso em: 26 maio 2018.

DULTRA, Eneida; MORI, Natália. **Trabalhadoras domésticas em luta:** direitos, igualdade e reconhecimento. Brasília: CFEMEA-ACDI/CIDA, 2008.

FERRAZ, Fernando B.; RANGEL, Helano M. V. A discriminação sociojurídica ao emprego doméstico na sociedade brasileira contemporânea: uma projeção do passado colonial. *In:* ENCONTRO NACIONAL DO CONPEDI, XIX., 2010, Fortaleza. **Anais** [...]. Tema: "Direitos Fundamentais e Transdisciplinaridade". Florianópolis: Fundação Boiteux, 2010. v. 1, p. 8633-8657.

FREYRE, Gilberto. **Casa Grande & Senzala:** formação da família brasileira sob o regime patriarcal. 48. ed. rev. São Paulo: Global, 2003.

FURTADO, Celso. **Formação econômica do Brasil**. 34. ed. São Paulo: Companhia das Letras, 2007.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. **No dia da mulher, estatísticas sobre trabalho mostram desigualdade.** Rio de Janeiro: IBGE, 2018. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/20287-no-dia-da-mulher-estatisticas-sobre-trabalho-mostram-desigualdade.html. Acesso em: 30 maio 2018.

JESUS, Eunice Aparecida de. **Preconceito racial e igualdade jurídica no Brasil.** 1980. Dissertação (Mestrado em Direito do Estado) – Faculdade de Direito, Universidade de São Paulo, USP, São Paulo, 1980.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. **Convenção e Recomendação sobre Trabalho Decente para as Trabalhadoras e os Trabalhadores Domésticos.** Brasília: OIT, 2011. Disponível em: http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/publication/wcms_169517.pdf. Acesso em: 30 maio 2018.

PAOLI, Maria Celia. Trabalhadores e cidadania. Experiência do mundo público na história do Brasil moderno. *In*: SOUSA JUNIOR, José; AGUIAR; A. (org.) **Introdução crítica ao Direito do Trabalho**. Brasília: Universidade de Brasília, 1993.

PEREIRA, Hildete. **O serviço doméstico remunerado no Brasil:** De criadas a trabalhadoras, Texto para Discussão nº 565. Rio de Janeiro: IPEA, 1998.

ANEXO 8 - Violência sexual contra mulheres: a incorporação da perspectiva de gênero no Direito Internacional Público

Direito Internacional Público (UnB): SCHLOTTFELDT, Shana; RESENDE, Otávio Henrique Mayrink. Violência sexual contra mulheres: a incorporação da perspectiva de gênero no Direito Internacional Público. *Revista Eletrônica do Programa de Pós-Graduação da Câmara dos Deputados (E-Legis)*. ISSN 2175-0688. Aceito em mai. 2021. No prelo.

SCHLOTTFELDT, Shana; RESENDE, Otávio Henrique Mayrink. Violência sexual contra mulheres: a incorporação da perspectiva de gênero no Direito Internacional Público. *Revista Eletrônica do Programa de Pós-Graduação da Câmara dos Deputados (E-Legis)*. ISSN 2175-0688. Aceito em mai. 2021. No prelo.

VIOLÊNCIA SEXUAL CONTRA MULHERES: A INCORPORAÇÃO DA PERSPECTIVA DE GÊNERO NO DIREITO INTERNACIONAL PÚBLICO

SEXUAL VIOLENCE AGAINST WOMEN: THE INCORPORATION OF THE GENDER PERSPECTIVE IN PUBLIC INTERNATIONAL LAW

VIOLENCIA SEXUAL CONTRA MUJERES: LA INCORPORACIÓN DE LA PERSPECTIVA DE GÉNERO EN EL DERECHO PÚBLICO INTERNACIONAL

Shana Schlottfeldt[1]

Otávio Henrique Mayrink Resende[2]

Resumo: O presente artigo analisa o panorama histórico do tratamento dado à violência sexual contra a mulher em contextos de guerra no Direito Internacional, fazendo um apanhado do paulatino reconhecimento da mulher como sujeito de direitos humanos e da incorporação da perspectiva de gênero, voltada para melhor enfocar os múltiplos impactos da violência sexual contra a mulher. O trabalho possui natureza qualitativa, a metodologia empregada utilizou levantamento bibliográfico e análise de fontes primárias, tais como tratados internacionais e resoluções do Conselho de Segurança da ONU. Os resultados apontam para o desenvolvimento de uma legislação, de mecanismos de denúncia e de jurisdição protetores dos direitos das mulheres em nível internacional, limitados, entretanto, pelas práticas nacionais, pelas dificuldades de efetivação dos julgados internacionais no âmbito interno e pela dificuldade de aplicar a responsabilidade individual por tribunais internacionais.

Palavra-chave: Direito Internacional Público; Direitos Humanos; Violência de Gênero; Mulheres; Crimes Sexuais.

Abstract: This article analyzes the historical panorama of the treatment given to sexual violence against women in war contexts in international law, considering the gradual recognition of women as subjects of human rights and the incorporation of the gender perspective, aimed at better focusing the multiple impacts of violence against the woman. This paper has a qualitative approach, using, as primary sources, international treaties and resolutions of the United Nations Security Council. Results point to the development of legislation, denunciation mechanisms and jurisdictions that protect women's rights at international level, limited, however, by national practices, difficulties of internalizing international court decisions, and to characterize individual responsibility for breaking international laws.

[1] Analista Legislativo da Câmara dos Deputados. Membro do Comitê Gestor Pró-Equidade de Gênero e Raça da Câmara dos Deputados. Doutora em Informática pela Universidade de Brasília. Visiting PhD student at University of York. Mestre em Informática pela Universidade Carlos III de Madrid. Bacharelanda em Direito pela Universidade de Brasília. LLB Exchange Student at Australian National University. Orcid: http://orcid.org/0000-0002-5481-0258. E-mail: shana.santos@camara.leg.br

[2] Bacharelando em Direito pela Universidade de Brasília (UnB). E-mail: otavio.hmr@gmail.com

Keywords: Public International Law; Human Rights; Gender Violence; Women; Sexual Crimes.

Resumen: Este documento analiza el panorama histórico del tratamiento de la violencia sexual contra las mujeres en contextos de guerra en el derecho internacional, haciendo un repaso del reconocimiento de la mujer como sujeto de derechos humanos y la incorporación de una perspectiva de género, orientada a enfocar mejor los múltiples impactos de la violencia sexual contra la mujer. El trabajo tiene un carácter cualitativo, la metodología empleada utilizó levantamiento bibliográfico y análisis de fuentes primarias, como tratados internacionales y resoluciones del Consejo de Seguridad de la ONU. Los resultados apuntan al desarrollo de legislación, mecanismos de denuncia y jurisdicción que protegen los derechos de las mujeres a nivel internacional, limitados, sin embargo, por las prácticas nacionales, las dificultades para hacer cumplir las sentencias internacionales a nivel interno y la dificultad para aplicar la responsabilidad individual de los tribunales internacionales.

Palabras clave: Ley internacional publica; Derechos humanos; Violencia de Género; Mujer; Delitos Sexuales.

1 Introdução

O objetivo geral do presente trabalho é estudar a violência sexual contra mulheres em contextos de guerra no âmbito do Direito Internacional Público. O problema de investigação consiste em verificar como as normas internacionais evoluíram em direção à incorporação, no Direito Internacional Público, do reconhecimento da violência sexual cometida contra mulheres no contexto de conflitos armados sob uma perspectiva de gênero, evidenciando inclusive o esforço da mulher em acionar a justiça quando é vítima de violência como consequência da discriminação histórica, mas destacando a importância da investigação dos crimes sexuais cometidos, pois se revestem das características de crimes de lesa-humanidade.

Neste *survey paper* procedeu-se a uma pesquisa indutiva, que tem por propósito sumarizar e organizar a temática na área. Portanto, tem natureza mais descritiva do que analítica, buscando ser um ponto de referência para estudos posteriores.

A metodologia empregada utilizou o levantamento bibliográfico e as etapas nele envolvidas, abrangendo levantamento extensivo de fontes primárias, leitura do material, fichamento, organização lógica do assunto e, por fim, a redação do texto.

As fontes primárias incluíram fontes legais internacionais, a saber, declarações, tratados, pactos, estatutos, protocolos e convenções internacionais que tratam da temática de violência sexual contra mulher em conflitos armados, sobretudo provenientes da Organização das Nações Unidas (ONU), da Organização dos Estados Americanos (OEA), da União Interparlamentar (IPU) e de Conferências Mundiais. Além disso, abarcaram, também, resoluções e informes, estes principalmente provenientes da ONU. Extensivo material relativo a julgamentos e decisões judiciais paradigmáticas no âmbito da violência sexual contra mulher também foram levantados, em especial provenientes do Tribunal Penal Internacional para a ex-Iugoslávia, do Tribunal Penal Internacional para Ruanda, da Corte Interamericana de Direitos Humanos e da Comissão Interamericana de Direitos Humanos, por serem pioneiros ao tratar a temática e cunhar o uso de

tipos penais no contexto internacional. Cada fonte fornece uma pequena parte do quebra-cabeças que permite visualizar de que forma se chegou ao cenário atual.

Como se pode observar, o foco manteve-se em traçar um histórico das primeiras referências a mecanismos de combate à violência sexual cometida contra mulheres no Direito Internacional Público, e sua gradual incorporação normativa, capaz de permitir, não apenas o reconhecimento da mulher como sujeito de direitos, mas também o acionamento de sistemas de denúncia e jurisdição. Nesse sentido, são trazidas fontes legais interacionais, sua aplicação/repercussão jurisdicional, mas não é objetivo deste trabalho trazer o desdobramento doutrinário.

Além desta Introdução (Seção 1), o presente estudo é composto por cinco Seções. Na Seção 2, é feita uma contextualização histórica das primeiras referências a crimes sexuais no direito internacional. Nas Seções 3 e 4 são abordados o reconhecimento da mulher como sujeito de direitos humanos e a incorporação da perspectiva de gênero no Direito Internacional Público, voltados para melhor enfocar os múltiplos impactos da violência sexual contra a mulher. Em especial, a Seção 4 trata da temática por meio do estudo de Resoluções do Conselho de Segurança da ONU e da Jurisprudência Internacional (Tribunal Penal Internacional para a ex-Iugoslávia e Tribunal Penal Internacional para Ruanda; Corte Interamericana de Direitos Humanos; Comissão Interamericana de Direitos Humanos). A Seção 5 traz considerações acerca da efetividade das Cartas Internacionais, tomando como exemplo o contexto brasileiro. Por fim, a Seção 6 apresenta as conclusões.

2 Contextualização Histórica das Primeiras Referências a Crimes Sexuais no Direito Internacional

Historicamente, as primeiras menções a crimes sexuais feitas pelo direito internacional dizem respeito a proibições contra o estupro em situações de guerra. Totila, o Ostrogodo, que invadiu Roma em 546 proibiu seus soldados de estuprarem as mulheres da cidade. Um antigo código de guerra inglês, promulgado em 1385 por Ricardo II, prescreveu o enforcamento para qualquer soldado que violasse uma mulher. Mais tarde, no século XVII, o autor holandês Hugo Grotius discorre sobre o fato de que enquanto alguns países permitiam a violação da dignidade feminina em tempos de guerra, outros, por sua vez, não a autorizavam. Em 1785, no Tratado de Amizade e Comércio celebrado entre Estados Unidos e Prússia, estabeleceu-se que, em uma eventual guerra entre os dois estados, tanto crianças quanto mulheres não seriam molestadas. O *Lieber Code* de 1863, documento adotado tanto pelos EUA como por vários países europeus à época, determinava, em seu art. 44, a pena de morte para soldados que cometesse estupro. Além disso, ainda que as Convenções de Haia de 1899 e 1907 não fizessem referência explícita ao estupro e outras formas de violência sexual, prescreviam a obrigação para com a "honra familiar"

e “práticas e convicções religiosas”, o que (na concepção patriarcal e machista da época) pode ser entendido como uma proteção da mulher contra o estupro (HAGAY-FREY, 2011, p. 60-61).

Desde a Segunda Guerra Mundial (2ª GM), houve dois períodos de grandes avanços no acolhimento de regras internacionais relacionadas aos abusos praticados contra civis durante os combates: (1) o pós-guerra imediato, quando o mundo confrontou-se com as atrocidades nazistas e com os crimes quase comparáveis das tropas japonesas na Ásia (dentre outras barbaridades, tropas japonesas cometeram o Massacre de Nanquim, também conhecido como “Estupro de Nanquim”, episódio de assassinatos e estupros em massa de civis, ocorrido em 1937); e (2) na década de 1990, após o fim da Guerra Fria, em reação à limpeza étnica na ex-Iugoslávia e ao genocídio em Ruanda (NEIER, 2005, p. 37).

A 2ª GM representou um divisor de águas na história dos direitos humanos. O regime nazista mostrou de maneira clara e inegável a possibilidade de suprimir séculos de lutas políticas e conquistas jurídicas (FACCHI, 2011, p. 127). Os avanços pós-2ª GM incluíram o estabelecimento dos tribunais para crimes internacionais em Nuremberg e Tóquio (infelizmente, os crimes sexuais cometidos não foram julgados por tais tribunais) (BARRERA, 2011, p. 143); a designação de determinadas ofensas como crimes contra a humanidade; a adoção da Convenção do Genocídio[3] pela Organização das Nações Unidas (ONU) e o acolhimento por praticamente todos os governos do mundo das Convenções de Genebra, de 1949, base do Direito Internacional Humanitário, determinando certas violações como “graves ofensas”, ou crimes de guerra, aplicando, pela primeira vez, proibições a conflitos armados internos.

Os conflitos na ex-Iugoslávia e em Ruanda inspiraram o estabelecimento dos primeiros tribunais para crimes internacionais desde Nuremberg e Tóquio; a extensão do conceito de crime de guerra para certas ofensas cometidas em conflitos internos; os primeiros julgamentos e condenações por genocídio e a adoção de um tratado para o estabelecimento de um tribunal para crimes internacionais permanentes (NEIER, 2005, p. 37-38).

Segundo Hagay-Frey (2011, p. 157-158), tratando-se especificamente dos crimes de violência sexual, o direito internacional poderia ser dividido em três grandes momentos:

1. *Era do Silêncio*: época em que se encontram pouca ou nenhuma menção a atos de violência sexual nas leis internacionais. É um período em que prevalece a ideia de submissão feminina de modo que o estupro era percebido tanto como uma forma de derrotar o inimigo quanto como um modo de melhorar o ânimo dos soldados. Nesse sentido, as leis internacionais eram criadas por homens para proteger homens, deixando de lado a violência contra a mulher. Essa Era compreenderia também as

[3] A convenção para a prevenção e a repressão do crime de Genocídio, concluída em Paris, a 11/12/1948, por ocasião da III Sessão da Assembleia Geral das Nações Unidas foi ratificada pelo Brasil em 4/9/1951, e promulgada pelo Decreto nº 30.822/1952.

duas grandes guerras, incluindo os tribunais penais internacionais de Nuremberg e Tóquio, para os quais a grande quantidade de provas testemunhais e documentais não foi suficiente para punir os crimes sexuais nas sentenças proferidas.

2. *Era da Honra*: quebra-se o longo silêncio do direito internacional com a assinatura da Convenção de Genebra de 1949. Apesar do reconhecimento do crime de estupro na legislação internacional, tal ato era entendido como uma violação à honra da mulher, e não como crimes contra sua dignidade ou contra sua integridade física, psicológica e emocional. Nessa perspectiva, tais práticas assumiam um papel secundário nas normas internacionais.
3. *Era Atual*: teve seu início com o estabelecimento dos tribunais penais internacionais para Ruanda e para a ex-Iugoslávia, criados com o objetivo de julgar os crimes de guerra praticados nesses países. As sentenças promulgadas em tais cortes representaram um verdadeiro marco histórico, ao elencar os crimes sexuais em todas as categorias de crime existentes no direito internacional. O Estatuto de Roma, amplamente reconhecido perante a comunidade internacional, veio logo em seguida e assentou tal entendimento, embora sem a extensão atribuída pelas cortes.

3 Evolução das normas internacionais

No contexto histórico que Hagay-Frey (2011, p. 157) chama a "Era do Silêncio", em que pese os Tribunais de Nuremberg e Tóquio não terem julgado, ao menos de uma maneira séria[4], os crimes sexuais cometidos, em 20 de dezembro de 1945, os Aliados promulgaram a *Control Council Law nº10* para punição de pessoas culpadas por crimes de guerra, contra a paz ou contra a humanidade (MOLINER, 2003, p. 33), nela, é apresentada uma enumeração, não exaustiva, dos crimes considerados contra a humanidade, incluindo o estupro (violação sexual) (BARRERA, 2011, p. 143).

Em 10 de dezembro de 1948, a Assembleia Geral da ONU, aprovou a Declaração Universal dos Direitos do Homem. Em seu preâmbulo, onde são apresentados os valores nos quais se fundamenta e os ideais aos quais aspira, já emerge uma concepção que vai além da visão do garantismo liberal: o comprometimento dos países membros e das Nações Unidas em perseguir a realização de "direitos iguais para homens e mulheres"[5]. Os direitos atribuídos à liberdade de expressão e de credo religioso, juntamente com a liberdade do medo e da necessidade são afirmados não só como um valor individual, mas como uma necessidade social, cuja negação "conduziu a atos de barbárie que ofendem a consciência da humanidade" (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948b).

[4] No tribunal de Tóquio houve condenação de um general militar, Matsui Iwane, e do Ministro de Relações Exteriores do Japão, Hirota Köri, pelo episódio conhecido como "Estupro de Nanquim" (BROOK, 2001, p. 679).

[5] "[...] os povos das Nações Unidas proclamam, de novo, a sua fé nos direitos fundamentais do Homem, na dignidade e no valor da pessoa humana, na igualdade de direitos dos homens e das mulheres [...]".

Dada sua importância, cumpre destacar as Convenções de Genebra, uma série de tratados elaborados durante quatro Convenções que aconteceram de 1864 a 1949 e que constituíram a base dos direitos humanitários internacionais. A assinatura da Convenção de Genebra de 1949, dada a sua importância, marca o início do que Hagay-Frey (2011, p. 157-158) denomina a "Era da Honra".

O art. 3º, da Convenção de Genebra I, estabelece o patamar mínimo de obrigações estatais para com a pessoa no marco de um conflito armado interno:

> **Artigo 3º**[...]
> 1) As pessoas que não tomem parte diretamente nas hostilidades [...] serão, em todas as circunstâncias, **tratadas com humanidade, sem nenhuma distinção de caráter desfavorável baseada na raça, cor, religião ou crença, sexo, nascimento ou fortuna, ou qualquer outro critério análogo**.
> Para este efeito, são e manter-se-ão proibidas, em qualquer ocasião e lugar, relativamente às pessoas acima mencionadas:
> **a) As ofensas contra a vida e a integridade física, especialmente o homicídio sob todas as formas, mutilações, tratamentos cruéis, torturas e suplícios;** [...]
> **c) As ofensas à dignidade das pessoas, especialmente os tratamentos humilhantes e degradantes;**
> (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948a, grifo nosso)

O art. 14 da Convenção de Genebra III dispõe sobre o respeito cabido aos presos, destacando que "as mulheres devem ser tratadas com todo o respeito devido ao seu sexo e se beneficiar em todos os casos de um tratamento tão favorável como o que é dispensado aos homens" (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1949).

No mesmo sentido, o art. 27 da Convenção de Genebra IV dispõe:

> **Artigo 27 -** As pessoas protegidas têm direito, em todas as circunstâncias, ao respeito da sua pessoa, da sua honra, dos seus direitos de família, das suas convicções e práticas religiosas, dos seus hábitos e costumes. **Serão tratadas, sempre, com humanidade e protegidas especialmente contra todos os atos de violência ou de intimidação, contra os insultos e a curiosidade pública**. **As mulheres serão especialmente protegidas contra qualquer ataque à sua honra, e particularmente contra violação, prostituição forçadas ou qualquer forma de atentado ao seu pudor** (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1950, grifo nosso).

Depreende-se do art. 27, que se tem, a partir de então, a tipificação da violação sexual como crime de direito internacional.

O marco estabelecido pela Convenção IV e pelo Protocolo II Adicional às Convenções de Genebra relativo à Proteção das Vítimas dos Conflitos Armados[6] foi o de determinar os crimes sexuais como de direito internacional, evidenciando a necessidade da incorporação de uma perspectiva de gênero ao Direito Internacional com o fito de dar visibilidade ao impacto, eminentemente diferenciado, que os conflitos armados têm nas mulheres (BARRERA, 2011, p.145).

[6] Decreto nº 849, de 25/6/1993, que promulga os Protocolos I e II de 1977 adicionais às Convenções de Genebra de 1949, adotados em 10/6/1977 pela Conferência Diplomática sobre a Reafirmação e o Desenvolvimento do Direito Internacional Humanitário aplicável aos Conflitos Armados.

4 A incorporação da perspectiva de gênero no direito internacional

Na segunda metade do século XX acontece, também, outra passagem fundamental na história dos direitos humanos: sua extensão às mulheres. Em grande parte do mundo, a igualdade jurídica entre os dois sexos, reivindicada por séculos, formaliza-se: os titulares de direitos já não são apenas os homens, mas todas as pessoas (FACCHI, 2011, p. 139).

Nos países ocidentais, a passagem essencial para a paridade foi a conquista do direito de voto, que abriu às mulheres o caminho para a conquista progressiva de outros direitos, associado a isso, conforme visto, as Cartas do pós-guerra promulgaram a igualdade dos direitos entre os gêneros (à época dizia-se igualdade entre os sexos) e deram início à transformação no processo de reformas jurídicas (caminhando no sentido da disponibilidade do próprio corpo, da autodeterminação, dos seus bens, do seu trabalho, da sua liberdade, acesso a todos os trabalhos e cargos públicos, etc.) (FACCHI, 2011, p. 139-140).

É importante pontuar que o tratamento sem levar em consideração as especificidades dos destinatários da norma faz com que seus resultados sejam aplicados a um "sujeito universal" que não existe, de maneira que a "generalização para todos os indivíduos é insuficiente e não dá conta das experiências de mulheres e homens indistintamente" (DUQUE, 2015, p. 16).

Nesse sentido, conforme pontua Bobbio, (2004, p.31):

> Manifestou-se nestes últimos anos uma nova linha de tendência, que se pode chamar de especificação; ela consiste na **passagem gradual, porém cada vez mais acentuada, para uma ulterior determinação dos sujeitos titulares de direitos** [...]. **Essa especificação ocorreu com relação seja ao gênero**, seja às várias fases da vida, seja à diferença entre estado normal e estados excepcionais da existência humana [...] (grifo nosso).

Assim, em que pesassem as igualdades proclamadas, ainda se observava (e pode-se dizer com segurança que ainda se observa) a discriminação de gênero. Diante disso, a Assembleia da ONU proclamou a Declaração sobre a Eliminação da Discriminação contra a Mulher (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1967).

Entretanto, o documento que efetivamente consubstancia a internacionalização dos direitos das mulheres é a Convenção sobre a Eliminação de toda Discriminação contra as Mulheres (CEDAW)[7], adotada pela ONU em 1979. Seu preâmbulo declara que os direitos das mulheres são parte integrante dos direitos humanos. Esse ato se fundamenta na constatação de que "as mulheres continuam a ser objeto de graves discriminações", e isto acontece apesar de a paridade jurídica entre os sexos já ter sido confirmada nas declarações internacionais, bem como

[7] Assinada pelo Brasil em 31/3/1981 e ratificada em 1/2/1984 (INTER-PARLAMENTARY UNION, 2003). O Estado brasileiro ao ratificar a CEDAW, formulou reservas aos art. 15, parágrafo 4º; art. 16, parágrafo 1º, alíneas (a), (c), (g) e (h); e art. 29. As reservas aos art. 15 e 16, retiradas em 1994, foram feitas devido à incompatibilidade da Convenção com a legislação brasileira, principalmente em matéria civil, em relação à assimetria entre os direitos do homem e da mulher. A reserva ao art. 29, diz respeito à disputa entre Estados partes quanto à interpretação da Convenção e continua vigorando. Quanto ao Protocolo Adicional à Convenção, o Brasil tornou-se parte em 2002 (OBSERVATÓRIO BRASIL DA IGUALDADE DE GÊNERO, 2016).

terem sido adotados instrumentos específicos para "promover o princípio da igualdade entre homens e mulheres". Disso se deduz que, a realização dos direitos das mulheres não exige apenas a extensão formal dos direitos existentes. Os Estados membros comprometem-se a tomar todas as medidas adequadas para garantir a paridade de direitos entre homens e mulheres nos vários âmbitos da vida social, eliminando as discriminações de direito e de fato (INTER-PARLAMENTARY UNION, 2003). Assim se manifesta a CEDAW quanto ao que se entende por discriminação contra a mulher:

> Artigo 1º - Para os fins da presente Convenção, a expressão "discriminação contra a mulher" significará toda a distinção, exclusão ou restrição baseada no sexo e que tenha por objeto ou resultado prejudicar ou anular o reconhecimento, gozo ou exercício pela mulher, independentemente de seu estado civil, com base na igualdade do homem e da mulher, dos direitos humanos e liberdades fundamentais nos campos político, econômico, social, cultural e civil ou em qualquer outro campo.

A CEDAW é também o primeiro documento internacional que coloca o efetivo acesso das mulheres aos direitos fundamentais como uma questão prioritária para a humanidade em seu conjunto. O ponto de vista das mulheres, portanto, é assumido como fundamento de direitos e medidas particulares, expressão de exigências tipicamente femininas.

Além disso, a CEDAW concorda que os direitos das mulheres podem ter aplicações variadas em diferentes países e que as culturas tradicionais podem ter um papel determinante em sua limitação. O acesso efetivo aos direitos é colocado como um objetivo para o qual não bastam reformas jurídicas, mas são necessárias transformações econômicas, sociais e culturais, e, em particular, uma educação para os direitos que compreenda "modificar os padrões socioculturais de conduta de homens e mulheres, com vistas a alcançar a eliminação dos preconceitos e práticas consuetudinárias, e de qualquer outra índole que estejam baseados na ideia de inferioridade ou superioridade de qualquer dos sexos ou em funções estereotipadas de homens e mulheres".

Ao ratificar a CEDAW, os governos se comprometem a adotar internamente uma série de medidas para pôr fim à discriminação contra a mulher. Entretanto, uma de suas fragilidades é a quase ausência de sanções contra os governos que não cumpram com os compromissos assumidos.

O Brasil também é signatário do Protocolo Facultativo à CEDAW, por meio do Decreto nº 4.316/2002. O protocolo facultativo autoriza o envio de queixas por particulares ou grupos de particulares diretamente ao Comitê da CEDAW, aumentando ligeiramente a sua autonomia frente às soberanias estatais.

Em junho de 1993, ocorre em Viena, Áustria, a Conferência Mundial dos Direitos Humanos. Nela, é reconhecido que "os direitos humanos das mulheres e das meninas são inalienáveis e constituem parte integral e indivisível dos direitos humanos universais", e que a "violência de gênero e todas as formas de abuso e exploração sexual [...] são incompatíveis com

a dignidade e valor da pessoa humana e devem ser eliminadas" (CONFERÊNCIA MUNDIAL DOS DIREITOS HUMANOS, 1993).

Dada sua relevância, merece menção a Declaração sobre a Eliminação da Violência contra as Mulheres, proclamada pela Assembleia Geral da ONU, em sua Resolução 48/104, de 20 de dezembro de 1993. Essa Declaração é o primeiro documento internacional de direitos humanos voltado exclusivamente para a violência contra a mulher incorporando, assim, a violência contra a mulher no marco conceitual dos direitos humano:

> Artigo 1º - Para os fins da presente Declaração, a expressão "violência contra as mulheres" significa qualquer ato de violência baseado no gênero do qual resulte, ou possa resultar, dano ou sofrimento físico, sexual ou psicológico para as mulheres, incluindo as ameaças de tais atos, a coação ou a privação arbitrária de liberdade, que ocorra, quer na vida pública, quer na vida privada (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1993a).

Vai-se consolidado, pouco a pouco, talvez mais devagar do que se gostaria, mas ainda sim de maneira constante, a noção de que as mulheres são também sujeitos internacionais de direitos.

Em 1994, a Organização dos Estados Americanos (OEA) deu força de lei à Declaração sobre a Eliminação da Violência contra as Mulheres por meio da Convenção para Prevenir, Punir e Erradicar a Violência Contra a Mulher (Convenção de Belém do Pará), suprindo lacuna da CEDAW que não havia tratado daquele tema (BARSTED, 2001, p.4). A Convenção é o primeiro tratado internacional de proteção aos direitos humanos das mulheres a reconhecer expressamente a violência contra a mulher como um problema generalizado na sociedade, além disso, reconheceu, de forma bastante contundente que a violência contra a mulher é um tipo específico, o qual se baseia no gênero, independente de classe, religião, idade, ou qualquer outra condição da mulher (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 1994).

O art. 7 da Convenção de Belém do Pará estabelece ainda que é dever do Estado-Parte "incorporar na sua legislação interna normas penais, civis, administrativas e de outra natureza, que sejam necessárias para prevenir, punir e erradicar a violência contra a mulher, bem como adotar as medidas administrativas adequadas que forem aplicáveis", já o art. 8º determina ao Estado-Parte "promover e apoiar programas de educação governamentais e privados, destinados a conscientizar o público para os problemas da violência contra a mulher, recursos jurídicos e reparação relacionados com essa violência".

Importante pontuar que o Caso Maria da Penha[8] foi o primeiro em que houve aplicação da Convenção de Belém do Pará. Diante desse contexto de internacionalização, grupos feministas

[8] Em 1983, a biofarmacêutica Maria da Penha Maia Fernandes, sofreu dupla tentativa de homicídio por parte de seu então marido dentro de sua própria casa, em Fortaleza, Ceará: (1) na primeira tentativa, o agressor atirou contra suas costas enquanto ela dormia, deixando-a paraplégica (2) na segunda, tentou eletrocutá-la no banho. Em 1998, passados mais de 15 anos do crime, apesar de haver duas condenações pelo Tribunal do Júri do Ceará (uma de 1991 e outra de 1996), ainda não havia uma decisão definitiva no processo e o agressor permanecia em liberdade, motivo pelo qual Maria da Penha, o CEJIL-Brasil (Centro para a Justiça e o Direito Internacional, Capítulo Brasil) e o CLADEM-Brasil (Comitê Latino-Americano e do Caribe para a Defesa dos Direitos da Mulher, Capítulo Brasil) enviaram o caso à

e organizações não-governamentais se articularam para aprovação do Projeto de Lei que deu origem à Lei nº 11.340/06 (Lei Maria da Penha), que cria mecanismos para coibir a violência doméstica e familiar contra a mulher. Em que pese o avanço representado e os resultados observados, cumpre apontar que a efetividade da Lei ainda encontra vários obstáculos concernentes à própria cultura social, patriarcal e machista de nosso país.

A 4ª Conferência Mundial das Mulheres, realizada em Pequim, em 1995, partiu de uma avaliação dos avanços obtidos desde as conferências anteriores (Nairobi, 1985; Copenhague, 1980; e México, 1975) e de uma análise dos obstáculos a superar para que as mulheres pudessem exercer plenamente seus direitos e alcançar seu desenvolvimento integral como pessoas. Nela, foi elaborada a Declaração e Plataforma de Ação de Pequim, um instrumento essencial de direitos humanos das mulheres que identificou doze áreas de preocupação prioritária, dentre elas a violência contra a mulher e os efeitos dos conflitos armados sobre a mulher. Foram consagradas três inovações dotadas de grande potencial transformador na luta pela promoção da situação e dos direitos da mulher: o conceito de gênero, a noção de empoderamento e o enfoque da transversalidade. Desses três, destaca-se o conceito de gênero que "permitiu passar de uma análise da situação da mulher baseada no aspecto biológico para uma compreensão das relações entre homens e mulheres como produto de padrões determinados social e culturalmente, e portanto passíveis de modificação" (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1996).

O Capítulo "D" da Plataforma de Ação de Pequim é dedicado inteiramente à Violência contra a Mulher, dos quais destacam-se, além do item 113 que reproduz o art. 2º da Declaração sobre a Eliminação da Violência contra as Mulheres, o item 118, que assim dispõe:

> 118. **A violência contra a mulher é uma manifestação das relações de poder historicamente desiguais entre mulheres e homens, que têm causado a dominação da mulher pelo homem, a discriminação contra ela e a interposição de obstáculos ao seu pleno desenvolvimento**. **A violência contra a mulher** ao longo do seu ciclo vital **deriva essencialmente de hábitos culturais**, em particular dos efeitos prejudiciais de algumas práticas tradicionais ou consuetudinárias e de todos os atos de extremismo relacionados com raça, sexo, idioma ou religião, que **perpetuam a condição de inferioridade conferida à mulher** no seio da família, no local de trabalho, na comunidade e na sociedade. **A violência contra a mulher é agravada por pressões sociais, como a vergonha de denunciar certos atos; pela falta de acesso da mulher à informação, à assistência e à proteção jurídicas; pela falta de leis que efetivamente proíbam a violência contra a mulher**; pelo fato de que não são devidamente emendadas as leis vigentes; pela falta de empenho das autoridades públicas na difusão das leis vigentes e no seu cumprimento; e **pela ausência de meios educacionais e de outro tipo para combater as causas e as conseqüências da violência**. As imagens de violência contra a mulher que aparecem nos meios de comunicação, em particular as representações de estupro ou de escravidão sexual, assim como a utilização de mulheres e meninas como objetos sexuais, inclusive a pornografia, são fatores que contribuem para a prevalência contínua dessa

Comissão Interamericana de Direitos Humanos da Organização dos Estados Americanos (CIDH/OEA). Em 2001, a CIDH responsabilizou o Estado brasileiro por omissão, negligência e tolerância, considerando que nesse caso se davam as condições de violência doméstica e de tolerância pelo Estado definidas na Convenção de Belém do Pará (ORGANIZAÇÃO DOS ESTADOS AMERICANOS, 2001).

> violência, prejudicial à comunidade em geral e, em particular, às crianças e aos jovens [...] (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1996, grifo nosso).

No contexto sob consideração, da violência sexual, são também importantes o Capítulo "E", que trata da "Mulher e os Conflitos Armados", e o Capítulo "I", sobre "Os Direitos Humanos da Mulher" (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1996).

Todo este avanço normativo associado às experiências dos Tribunais Penais Internacionais para a Ex-Iugoslávia e Ruanda (TPIY e TPIR), criados em 1993 e 1994, respectivamente, culminaram na aprovação, em 1998, do Estatuto de Roma (que rege o Tribunal Penal Internacional – TPI), onde, *pela primeira vez, a violência sexual aparece como um crime independente* (TRIBUNAL PENAL INTERNACIONAL, 1998).

O Estatuto de Roma reconhece os crimes de gênero, alçando os crimes sexuais à condição de crimes contra a humanidade (e, portanto, imprescritíveis) (art. 7º, 1, g, conjugado ao art. 29) quando cometidos no contexto de um ataque generalizado e sistemático contra a população civil (art. 7º, 2, a).

A procuradora Ela Wiecko V. de Castilho (2005, p. 1) tece as seguintes considerações acerca da abordagem de gênero introduzida pelo Estatuto de Roma:

> O TPI é atualmente um dos mecanismos mais desenvolvidos em matéria de justiça de gênero, pois incorpora (a) uma definição de gênero, (b) o princípio da não-discriminação baseada em gênero, (c) normas de procedimento e prova, proteção e participação em relação a vítimas e testemunhas de crimes de violência sexual, e (d) criminaliza em nível internacional a violência sexual e gênero.

A Tabela 1 traz uma lista dos principais instrumentos internacionais de proteção dos direitos humanos, ratificados pelo Brasil.

Tabela 1 - Principais Tratados, Declarações, Pactos, Planos de Ação e Convenções Internacionais de Proteção aos Direitos Humanos

Aprovação no Organismo Internacional	**Ratificação pelo Brasil**	**Instrumento Internacional**
1945	1945	Carta das Nações Unidas
1948	1948	Convenção contra o genocídio
1948	1948	Declaração universal dos direitos humanos
1966	1992	Pacto internacional dos direitos civis e políticos
1966	1992	Pacto internacional dos direitos econômicos sociais e culturais
1979	1984/1994	Convenção sobre a eliminação de todas as formas de discriminação contra as mulheres
1984	1989	Convenção contra a tortura e outros tratamentos ou penas cruéis, desumanos ou degradantes
1986	1989	Convenção Interamericana para prevenir e punir a tortura
1993	1993	Declaração sobre a eliminação da violência contra a mulher
1994	1995	Convenção Interamericana para prevenir, punir e erradicar a violência contra a mulher (Convenção de Belém do Pará)

Aprovação no Organismo Internacional	Ratificação pelo Brasil	Instrumento Internacional
1995	1995	Plataforma de Ação da IV Conferência Mundial sobre a Mulher
1998	2002	Estatuto de Roma
2000	2002	Protocolo Facultativo à Convenção sobre a eliminação de todas as formas de discriminação contra as mulheres

Fonte: Barsted (2001, p. 5-6), com modificações.

Em 2001, Radhika Coomaraswamy, Relatora Especial sobre a Violência Contra a Mulher da ONU, apresentou o informe sobre *La violencia contra la mujer perpretada y/o condonada por el Estado, en tiempos de conflicto armado (1997-2000)*, no qual aponta:

> [...] **que mulheres e meninas têm sido violadas por forças governamentais e outros atores não estatais, pela polícia, responsável por sua proteção, por guardas de campos de refugiados e de fronteiras, por vizinhos, por políticos locais e alguma vezes por membros da família sob ameaça de morte**. Têm sido lesadas ou mutiladas sexualmente e frequentemente têm sido mortas ou se deixado morrer. As mulheres **têm sido objeto de comentários humilhantes após terem sido desnudas, têm sido obrigadas a desfilar ou dançar nuas diante de soldados ou em público e a realizar tarefas domésticas penosas estando desnudas**. As mulheres e meninas têm sido obrigadas a "casar-se" com soldados, termo eufemístico empregado para designar o que essencialmente é uma violação reiterada e uma escravidão sexual, elas e seus filhos têm padecido deficiências como consequência da exposição a armas químicas. [...]
>
> A Relatora Especial destaca que **ainda há um descompasso entre o reconhecimento por parte da comunidade internacional de que aqueles que cometeram violações e outros atos de violência por razão de gênero são responsáveis perante a lei e devem ser castigados**, e a vontade política dos Estados Membros de aplicar o direito internacional humanitário e as normas de direitos humanos, e reitera que **os transgressores devem arcar com suas responsabilidades**. A atual impunidade daqueles que aplicaram o sistema japonês de escravidão militar durante a segunda guerra mundial é apenas um dos muitos exemplos dessa **desídia de alguns Estados Membros que não investigam os atos de violação e violência sexual do passado, nem judicializam nem castigam os responsáveis. Isso contribui para criar um clima de impunidade que hoje perpetua a violência contra a mulher** [...] (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2001, grifo nosso).

Estas foram as principais base legais internacionais que tratam da temática de violência sexual contra mulher em contexto de guerra (declarações, tratados, pactos, estatutos, protocolos e convenções). Elas lançaram as bases para o desenvolcimento de legislações nacionais internas ao fixarem os parâmetros/patamares mínimos de direitos humanos a serem seguidos. Posteriormente, os maiores avanços internacionais na temática passaram a dar-se por meio de Resoluções e pela jurisprudência internacional que começou a aplicar tais parâmetros. Estes serão os temas das seções seguintes.

4.1 Resoluções do Conselho de Segurança da ONU

O Conselho de Segurança das Nações Unidas é um dos principais órgãos da ONU, encarrega-se de zelar pela manutenção da paz e da segurança internacional, recomendar a admissão de novos membros à Assembleia Geral e aprovar qualquer mudança na Carta das Nações Unidas. Suas decisões são geralmente denominadas *resoluções*; possuem valor jurídico vinculante e têm por objetivo indicar a solução para alguma contrariedade relacionada à manutenção ou promoção da paz e segurança internacionais. Trata-se do único órgão do sistema internacional capaz de adotar decisões obrigatórias para todos os 193 Estados-membros da ONU, podendo, inclusive, autorizar intervenção militar para garantir a execução de suas resoluções (ONU, 2021).

O Conselho de Segurança das Nações Unidas já aprovou cinco resoluções que discorrem em específico sobre a problemática dos crimes sexuais, apresentando um enfoque de gênero.

A Resolução nº 1325/2000 incidiu sobre a condição da mulher em situações de conflitos, ressaltando a necessidade de proteção contra crimes sexuais e urgindo para que se considere a perspectiva de gênero em toda a arquitetura de resolução do conflito:

> 10. Apela a todas as partes envolvidas em conflito armado para que tomem medidas especiais de proteção das mulheres e das jovens contra a violência baseada na diferença de gênero, em particular a violação e outras formas de abuso sexual, bem como todas as outras formas de violência que ocorrem em situações de conflito armado;
> 11. Realça a responsabilidade que todos os Estados têm de pôr fim à impunidade e processar os responsáveis por genocídio, crimes contra a humanidade, e crimes de guerra, incluindo os que se relacionam com o sexo e qualquer outro tipo de violência contra as mulheres e as meninas, e, a este propósito, sublinha a necessidade de, sempre que possível, excluir tais crimes das provisões de anistia; (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2000).

A Resolução nº 1820/2008, condena veementemente a prática de violência sexual como tática de guerra em situações de conflito, lembrando a possibilidade de tais práticas se constituírem como crimes de guerra, crimes contra a humanidade e de genocídio:

> 4. Observa que estupro e outras formas de violência sexual podem constituir crime de guerra, crime contra a humanidade ou ato constitutivo de genocídio. Salienta a necessidade da exclusão dos crimes de violência sexual das disposições de anistia no tratante de processos de resolução de conflitos. Apela aos países membros para que cumpram com suas obrigações de julgar os indivíduos responsáveis por tais atos, garantam a todas as vítimas de violência sexual, especialmente mulheres e meninas, proteção da lei e direito de justiça, e salienta a importância do fim da impunidade de tais atos como parte de uma abordagem global em busca da paz sustentável, justiça, verdade e reconciliação nacional; (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2008)

A Resolução nº 1888/2009, também é considerada como um avanço nas leis internacionais, pois criou o Escritório do Representante Especial do Secretário-Geral para Violência Sexual em Conflitos. Este escritório foca sua atuação em países tidos como prioritários no combate à violência contra a mulher. Entre seus objetivos estão a luta contra a impunidade de crimes de violência sexual, bem como a proteção e o empoderamento das mulheres em situação de conflito (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2009).

A Resolução nº 1960/2010 declara que a violência sexual é praticada de modo sistemático e disseminado em situações de conflito, constituindo grave violação dos direitos humanos. Além disso, propõe mecanismos institucionais que visem a proteger e prevenir crimes de tal natureza além de avançar no combate à impunidade em conflito (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2010).

Por fim, a Resolução nº 2106/2013 apresenta um enfoque de gênero, afirmando a necessidade da busca pela igualdade já no momento posterior ao conflito, além de objetivar a consolidação das conquistas da Resolução nº 1325/2000 (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 2013).

4.2 Jurisprudência Internacional

A jurisprudência, entendida como o conjunto de decisões uniformes e constantes dos tribunais, proferidas para a solução judicial de conflitos, envolvendo casos semelhantes (DINIZ, 2008, p. 295), tem apresentado relevância cada vez mais acentuada considerando-se as decisões internacionais em casos de violência sexual.

Em princípio, a jurisprudência tem a sua obrigatoriedade restrita ao caso em que a decisão foi proferida, mas, ao aplicar diferentes preceitos normativos de forma lógica e sistemática, serve como parâmetro para outros julgamentos, envolvendo questões iguais ou semelhantes. Neste sentido, exerce o importante papel de atualizar as disposições legais, tornando-as compatíveis com a evolução social.

Nesse diapasão, serão apresentadas, a seguir, decisões no âmbito de sentenças de tribunais internacionais consideradas importantes no que diz respeito ao reconhecimento, julgamento e punição da violência sexual (para uma explanação dos casos remete-se os leitores às referências bibliográficas citadas).

4.2.1 O Tribunal Penal Internacional para a ex-Iugoslávia

Inaugura o que Hagay-Frey (2011, p. 158) chama de “Era Atual” do Direito Internacional quanto à temática dos crimes de violência sexual.

No final do século XX, a península balcânica foi palco de inúmeros conflitos étnicos que resultaram em um saldo de milhares de mortes e um número incalculável de refugiados. Tais conflitos foram considerados como os mais intensos desde a Segunda Guerra Mundial. Além disso, crimes sexuais eram praticados de maneira disseminada e sistemática contra a população civil e utilizados como instrumento de guerra, limpeza étnica e humilhação. Neste contexto, foi criado o Tribunal Penal Internacional para a ex-Iugoslávia (TPIY) (HAGAY-FREY, 2011, p. 80; ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1993b).

Cerca de 20.000 a 44.000 mulheres foram vítimas de abuso sexual no período compreendido entre 1992 e 1994, na Iugoslávia. A maior parte dos estupros foi praticada por homens sérvios contra meninas e mulheres mulçumanas e croatas. Além disso, muitas mulheres foram presas em casas ou hotéis, tornando-se escravas sexuais. As vítimas eram repetidamente estupradas ao longo de vários meses e tratadas com violência e crueldade (CHIAROTTI, 2011, p. 185).

O estupro era utilizado como forma de humilhação e dano à honra das vítimas e de suas famílias, pois, segundo o Islamismo, as vítimas de estupro são consideradas impuras, indesejáveis e impróprias ao casamento. Isso frequentemente conduzia ao banimento das vítimas, e em alguns casos, a sua própria morte pela família ou por membros da comunidade. Por fim, o estupro era usado como forma de exaltar a honra dos agressores e elevar a moral dos seus próprios soldados (HAGAY-FREY, 2011, p. 80-81).

Em 1993, um grupo de mulheres que faziam parte da ONG *Women in the Law Project* (WILP) enviou uma delegação para o local dos conflitos responsável pela elaboração de um relatório que pedia que o crime de estupro fosse inserido nos tipos penais internacionais, caracterizando-o como uma grave violação das Convenções de Genebra (WOMEN IN THE LAW PROJECT, 1994, p. 91-93).

O Art. 5º, g, do Estatuto do Tribunal Penal Internacional para a Ex-Iugoslávia (ETPIY) representou um marco na história do direito penal internacional ao *elencar pela primeira vez o "estupro" como "crime contra a humanidade"*. Tal codificação também inovou ao considerar o estupro não como uma violação à honra da mulher, mas sim como um atentado à humanidade, rompendo com a compreensão vigente à época (HAGAY-FREY, 2011, p. 83).

O Tribunal sustentou que tanto o estupro como outros tipos de agressão sexual constituíam grave violação das Convenções de Genebra, das leis costumeiras de guerra e poderiam ser consideradas como crimes de tortura e genocídio.

O ETPIY incentivou a participação feminina em todo o processo judicial, com a presença de investigadoras, pesquisadoras, consultoras legais, juízas ou procuradoras. Tal fomento foi importante para o sucesso do tribunal, tendo em vista a maior sensibilidade das mulheres para uma perspectiva de gênero nos crimes (ASKIN, 1999, p. 302-303).

Outro avanço importante consta das Regras de Procedimento e Prova do Tribunal Penal Internacional para a Ex-Iugoslávia, documento que estabeleceu regras mais flexíveis e apropriadas para colher o testemunho e garantir a efetiva proteção das vítimas de abuso sexual. A Regra 34 desse documento, além de criar uma unidade específica para acolher e aconselhar as testemunhas e vítimas de abuso sexual, também fomenta a contratação de mulheres qualificadas a fim de prestarem um atendimento adequado à vítima (HAGAY-FREY, 2011, p. 84-85).

Quanto aos julgamentos, destacam-se:

1. O primeiro julgamento, contra Dusko Tadic: estabeleceu importante precedente no direito internacional para os crimes sexuais. O réu foi acusado de cometer crimes contra a humanidade por seu envolvimento em uma campanha de terror que compreendeu mortes, torturas, agressões sexuais (praticadas tanto contra homens quanto contra mulheres) e outros tipos de abusos físicos e psicológicos.
2. Caso nº IT-96-21-T, Promotoria vs. Zejnil Delalić, Zdravko Mucić alias "Pavo", Hazim Delić, Esad Landžo alias "Zenga" (Čelebići): julgou crimes de exploração sexual e tortura de prisioneiros no Campo Čelebići, vários soldados foram acusados, entre eles, Hazim Delić, o guarda do Campo, condenado por usar o estupro como técnica de tortura contra mulheres prisioneiras. Essa foi a primeira vez que o estupro foi reconhecido como crime de tortura no direito internacional, além disso, entendeu o Tribunal que se deve creditar ao testemunho de vítimas de violência sexual a mesma credibilidade que se confere a vítimas de outros crimes, não se lhes exigindo, comprovação da declaração:
3. Caso nº IT-95-17/1-T, Promotoria vs. Anto Furundžija: inovou ao elaborar uma definição do crime de estupro que não se limitava à penetração vaginal ou anal, mas que incluía violações orais.

> 185. Thus, the Trial Chamber finds that the following may be accepted as the objective elements of rape:
> **(i) the sexual penetration, however slight:**
> **(a) of the vagina or anus of the victim by the penis of the perpetrator or any other object used by the perpetrator; or**
> **(b) of the mouth of the victim by the penis of the perpetrator;**
> (ii) by coercion or force or threat of force against the victim or a third person (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1998, p. 73, grifo nosso).

Além disso, estabeleceu que é proibido não só praticar o estupro ou a agressão sexual, mas também planejá-los, ordená-los, instigá-los ou ajudar na sua execução.

4. Caso nº IT-96-23-T & IT-96-23/1-T, Promotoria vs. Dragloljub Kunarac, Radomir Kovač e Zoran Vuković: primeiro caso em que um réu foi acusado *exclusivamente* por cometer crimes sexuais contra mulheres.

4.2.2 O Tribunal Penal Internacional para Ruanda

O Tribunal Penal Internacional para Ruanda (TPIR) foi criado em novembro de 1994 para levar a cabo o julgamento dos casos de crimes contra a humanidade e genocídio ocorridos durante a guerra civil naquele país. Durante a sua existência, houve mais de cinquenta julgamentos e trinta condenações. A base do direito material aplicável ao TPIR foi a Convenção para a Prevenção e a Repressão de Crimes de Genocídio, de 1948, as quatro Convenções de Genebra, de 1949, e seus três protocolos adicionais (PAULA, 2011, p. 53-54).

Nesse Tribunal, houve o primeiro enquadramento judicial do tipo crime sexual, que foi entendido pela corte como instrumento de genocídio. Assim sendo, o próprio ato de lesão corporal grave em massa por meio de violência sexual constitui-se em ato genocida (PAULA, 2011, p. 62). Como afirma Susana Chiarotti (2011, p. 181):

> Esta es la primer sentencia de un tribunal penal internacional que define la violencia sexual: "cualquier acto de naturaleza sexual que se comete contra una persona en circunstancias coactivas" y la violación sexual como: "una invasión física de naturaleza sexual, cometida contra una persona bajo circunstancias coactivas". A la vez, considera a ambas como delito de lesa humanidade.

O único crime sexual previsto expressamente no art. 3º do Estatuto do Tribunal Penal Internacional para Ruanda (ETPIR) era tipificado pela penetração do ânus, da vagina ou da boca da vítima pelo agente, utilizando-se este de qualquer objeto (PAULA, 2011, p. 67), crimes de natureza sexual que não envolvessem a penetração seriam enquadrados ou no inciso sobre tortura ou no inciso sobre outros atos inumanos.

Entretanto, com sentença proferida naquele Tribunal, *pela primeira vez estende-se o conceito de violência sexual para além do estupro (penetração)*, compreendendo qualquer ato de natureza sexual contra uma pessoa em circunstância de coação, não sendo necessária a comprovação de uso de força física. Admite-se que a violência sexual pode ocorrer mesmo mediante atos que não envolvam penetração e sequer contato físico, como, por exemplo, expor a pessoa à nudez, ameaças, intimidação, extorsão e outros tipos de maus tratos que se usam do medo ou desespero para constituir coação (CHIAROTTI, 2011, p. 182). A violência sexual foi incluída entre atos inumanos, que atentam contra a dignidade humana, causadores de danos físicos e mentais graves. O TPIR aponta, ainda, que o elemento mental do estupro como crime contra a humanidade consiste na intenção de perpetrar a penetração sexual proibida sabendo que ocorre sem o consentimento da vítima.

O julgado mais relevante sobre crimes sexuais nesse contexto de guerra civil é o de Jean Paul Akayesu, da Comuna Taba. Ele era burgomestre da comuna, a mais alta autoridade local, e, sob sua administração, mais de duas mil pessoas foram brutalmente aniquiladas e outras tantas foram mutiladas e violentadas sexualmente (PAULA, 2011, p. 93). Ele foi sentenciado à prisão perpétua num julgamento que durou sessenta dias, tendo sido condenado em nove das quinze acusações, inclusive na de ter cometido crime sexual.

4.2.3 Comissão Interamericana de Direitos Humanos

A Comissão Interamericana de Direitos Humanos (CIDH) é um órgão autônomo da OEA encarregado da promoção e proteção dos direitos humanos no continente americano. Juntamente com a Corte Interamericana de Direitos Humanos (CorteIDH), integra o Sistema Interamericano

de Proteção dos Direitos Humanos (SIDH). Tem sede em Washington e é composta por sete juristas eleitos que representam, em conjunto, os países membros da OEA.

As atividades da CIDH são desenvolvidas em torno de três núcleos: (1) o sistema de petição individual; (2) o monitoramento da situação dos direitos humanos nos Estados membros; (3) a atenção a linhas temáticas prioritárias. E direcionados de maneira complementar pelos seguintes conceitos: (1) o princípio *pro personae*, segundo o qual uma norma deve ser sempre interpretada da maneira mais favorável ao ser humano; (2) a necessidade de acesso; (3) a justiça; (4) a incorporação da perspectiva de gênero em todas as suas atividades (OEA, 2021).

Os casos paradigmáticos da CIDH quanto ao reconhecimento da violência sexual são relacionados abaixo.

- **Caso Raquel Martín de Mejía vs. Peru. Caso Nº 10.970. Informe Nº 5/96, de 1/3/1996 (CENTRO PELA JUSTIÇA E O DIREITO INTERNACIONAL, 1996)**: nesse caso, a Corte determinou que os *estupros cometidos devem ser considerados como crimes de tortura e contra a humanidade (lesa-humanidade)*. Também estabeleceu que não havia um contexto à época que permitisse à vítima denunciar o ocorrido, ressaltando o estigma que a violência sexual significa para aqueles que a sofrem. Apontou que a abusos cometidos por membros do Estado são resultado da omissão deste e constituem violações aos direitos humanos das vítimas, em particular à sua integridade física e mental, constituindo no caso específico, crime de tortura. O Informe da Corte a respeito do caso evidencia o sofrimento psicológico e as marcas que o estigma da violência sexual deixam em suas vítimas:

> Raquel Mejía fue víctima de violación, y en consecuencia de un acto de violencia contra su integridad que le causó "penas y sufrimientos físicos y mentales". Como surge de su testimonio, luego de ser violada "estaba en un estado de shock, sentada sola en [su] habitación". **No se animó a realizar la denuncia pertinente por miedo a sufrir el "ostracismo público". "Las víctimas de abusos sexuales no denuncian estos hechos porque [se] sienten humilladas. Además nadie quiere reconocer públicamente que ha sido violada. No se sabe cómo puede reaccionar el marido. [Por otro lado] la integridad de la familia está en juego, los hijos pueden sentirse humillados de saber que esto le ha ocurrido a su madre"** (CENTRO PELA JUSTIÇA E O DIREITO INTERNACIONAL, 1996, p. 97-98, grifo nosso).

O Tribunal reconhece que as vítimas de estupro por agentes do Governo não denunciam estes abusos por medo da humilhação pública e pela percepção que os responsáveis nunca serão punidos, somando-se a isso o fato de normalmente serem ameaçadas de sofrer represarias contra elas mesmas ou seus familiares.

- **Ana, Beatriz e Celia González Pérez vs. México. Caso nº 11.565. Informe nº 53/01, de 4/4/2001 (COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS, 2001)**: em sua sentença, a Comissão Interamericana de Direitos Humanos (CIDH) entendeu que

a violência sexual, sob determinadas circunstâncias (como as encontradas no caso em julgamento) *constitui crime de tortura* e faz as seguintes considerações:

> **45. La violación sexual cometida por miembros de las fuerzas de seguridad de un Estado contra integrantes de la población civil constituye en todos los casos una grave violación de los derechos humanos protegidos en los artículos 5 y 11 de la Convención Americana, así como de normas de derecho internacional humanitario** […] las consecuencias de la violencia sexual "son devastadoras para las víctimas desde el punto de vista físico, emocional y psicológico".
> 47. **En el derecho internacional, bajo determinadas circunstancias, la violación constituye además tortura** […]
> La violación produce un sufrimiento físico y mental en la víctima. Además de la violencia sufrida al momento que se perpetra, las víctimas habitualmente resultan lesionadas, o en algunos casos, incluso quedan embarazadas. El hecho de ser objeto de un abuso de esta naturaleza les ocasiona asimismo un trauma psicológico, que resulta por un lado del hecho de ser humilladas y victimizadas, y por el otro, de sufrir la condena de los miembros de su comunidad, si denuncian los vejámenes de los que fueron objeto […].
> 48. **El Relator Especial de las Naciones Unidas contra la Tortura ha señalado que la violación es uno de los métodos de tortura física, utilizada en algunos casos para castigar, intimidar y humillar** […]
> **La violación de una persona detenida por un agente del Estado debe considerarse como una forma especialmente grave y aberrante de tratamiento cruel**, dada la facilidad con la cual el agresor puede explotar la vulnerabilidad y el debilitamiento de la resistencia de su víctima. Además, la violación deja profundas huellas psicológicas en la víctima que no pasan con el tiempo como otras formas de violencia física y mental.
> 49. […] La jurisprudencia internacional y los informes del Relator Especial demuestran un impulso hacia la definición de la violación como tortura cuando se verifica en el marco de la detención e interrogatorio de las personas y, en consecuencia, como una violación del derecho internacional. La violación se utiliza por el propio interrogador o por otras personas asociadas con el interrogatorio de una persona detenida, como medio de castigar, intimidar, coaccionar o humillar a la víctima, o de obtener información, o una confesión de la víctima o de una tercera persona (COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS, 2001, grifo nosso).

4.2.4 Corte Interamericana de Direitos Humanos

Conforme acima mencionado, a CorteIDH é um órgão judicial autônomo, integrante do SIDH. Está sediado em San José, Costa Rica e tem por propósito aplicar e interpretar a Convenção Americana de Direitos Humanos, bem como outros tratados de Direitos Humanos. Os casos emblemáticos da CorteDH relativos a crimes de violência sexual contra a mulher são apresentados abaixo.

- **Caso Penal Miguel Castro Castro vs. Peru – Sentença de 25/11/2006 (CORTE INTERAMERICANA DE DIREITOS HUMANOS, 2006)**: nesse julgado, a Corte *define o que é violência sexual e deixa claro que o crime adquire matizes diferentes no que diz respeito às mulheres* a quem afeta em maior proporção, em especial se são mães ou se estão grávidas. Também estabeleceu que a inspeção vaginal, empreendida no âmbito do caso, não requerida por um motivo de saúde e executada em um hospital militar,

caracteriza-se como estupro (violação sexual) e pelos efeitos que provoca é considerada tortura.

Estabeleceram ainda que, no caso em questão, as mulheres foram afetadas de maneira distinta e mais gravosa comparadas aos homens, pois *a violência que sofreram lhes foi dirigida especificamente pelo fato de serem mulheres*. A violência sexual que sofreram foi utilizada como um *ato simbólico para humilhá-las*, tinha por objetivo castigar, intimidar, pressionar, degradar, castigar, reprimir. Constituíram uma maneira de "dar uma mensagem, uma lição".

No contexto considerado, um tratamento mais cruel e violento foi dispensado às mulheres consideradas "suspeitas", acusadas por delitos de terrorismo e traição à pátria.

A nudez forçada por longo período a que foram submetidas as mulheres no hospital militar foi considerada ato violador da dignidade pessoal, bem como violência sexual. O fato caracterizador da violência sexual foi terem sido constantemente vigiadas por guardas do sexo masculino, o que agravava o temor constante de sofrerem violação sexual, provocando grave sofrimento psicológico e moral que se somaram ao sofrimento físico de suas feridas.

Inclui-se, também, como violência sexual o fato de terem que utilizar o banheiro acompanhadas por guarda homem, armado, que não lhes permitia fechar a porta e lhes apontava a arma enquanto fazia suas necessidades fisiológicas.

Importante precedente foi considerar que:

> 306. […] la violencia sexual se configura con acciones de naturaleza sexual que se cometen en una persona sin su consentimiento, que además de comprender la invasión física del cuerpo humano, pueden incluir actos que no involucren penetración o incluso contacto físico alguno.
> 310. […] la violación sexual no implica necesariamente una relación sexual sin consentimiento, por vía vaginal, como se consideró tradicionalmente. Por violación sexual también debe entenderse actos de penetración vaginales o anales, sin consentimiento de la víctima, mediante la utilización de otras partes del cuerpo del agresor u objetos, así como la penetración bucal mediante el miembro viril (CORTE INTERAMERICANA DE DIREITOS HUMANOS, 2006, p. 107-108).

Estabeleceu-se que a violência sexual praticada por um agente do Estado é particularmente grave e reprovável tendo em vista a vulnerabilidade da vítima e o abuso de poder do agente.

- **González e outras vs. México ("Campo Algodonero") – Sentença de 16/11/2009 (CORTE INTERAMERICANA DE DIREITOS HUMANOS, 2009b)**: *a Corte utilizou pela primeira vez a expressão feminicídio para se referir ao homicídio da mulher por razões de gênero* tendo como causas estruturais a violência de gênero persistente e a cultura discriminatória contra as mulheres. Definiu a competência da Corte para julgar violações à Convenção de Belém do Pará. *Utilizou, também pela primeira vez, o conceito de estereótipo de gênero* (preconcepção quanto aos atributos, características e papéis que

"deveriam" ser desempenhados por homens e mulheres, respectivamente), apontando-o como causa e consequência da violência de gênero contra a mulher.

Afirmou que a impunidade – seja pela inação estatal, pela tolerância à violência contra a mulher, pela desqualificação da credibilidade da vítima, pela atribuição tácita da responsabilidade dos fatos à vítima – provoca um círculo vicioso que favorece a perpetuação da violência em fator do gênero e é, por si só, uma discriminação quanto ao acesso à justiça.

- **Massacre de las Dos Erres vs. Guatemala – Sentença de 24/11/2009 (CORTE INTERAMERICANA DE DIREITOS HUMANOS, 2009a)**: nessa sentença, a Corte decidiu que os estupros cometidos no âmbito do caso julgado foram uma *prática estatal dirigida contra a dignidade da mulher* em nível cultural, social, familiar e individual, que *deveriam ser considerados crimes contra a humanidade*.

5 Acerca da efetividade das Cartas Internacionais

Sob a perspectiva do arcabouço brasileiro, a aplicabilidade dos preceitos internacionais somente é possível a partir do momento em que cumpridos os requisitos solenes para a sua devida integração à ordem jurídico constitucional, a saber: (i) celebração da convenção internacional; (ii) aprovação pelo Parlamento; e (iii) ratificação pelo Chefe de Estado – a qual se conclui com a expedição de Decreto, de cuja edição derivam três efeitos básicos que lhe são inerentes: (a) a promulgação do tratado internacional; (b) a publicação oficial de seu texto; e (c) a executoriedade do ato internacional, que, somente a partir desse momento, passa a vincular e a obrigar no plano do direito positivo interno (BRASIL, 2009, p. 1139).

Há dispositivos na Constituição Federal (CF/88) que sinalizam uma abertura constitucional ao direito internacional e, ao direito supranacional. A saber:

> Art. 4º .....
>
> Parágrafo único. A República Federativa do Brasil buscará a integração econômica, política, social e cultural dos povos da América Latina, visando à formação de uma comunidade latino-americana de nações. [...]
>
> Art. 5º .....
>
> § 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.
>
> § 3º Os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes às emendas constitucionais. (Incluído pela Emenda Constitucional nº 45, de 2004)
>
> § 4º O Brasil se submete à jurisdição de Tribunal Penal Internacional a cuja criação tenha manifestado adesão. (Incluído pela Emenda Constitucional nº 45, de 2004)

Segundo Celso de Mello (BRASIL, 2009, p.1150), o parágrafo único do art. 4º, representa uma clara opção do constituinte pela integração do Brasil em organismos supranacionais.

Cumpre ressaltar, também, que "vários países latino-americanos caminharam no sentido de sua inserção em contextos supranacionais, reservando aos tratados internacionais de direitos humanos lugar especial no ordenamento jurídico, algumas vezes concedendo-lhes valor normativo constitucional", o que revela "uma tendência contemporânea do constitucionalismo mundial de prestigiar as normas internacionais destinadas à proteção do ser humano" (BRASIL, 2009, p. 1151).

Entretanto, o problema principal do processo de internacionalização é o da efetividade dos direitos proclamados nas cartas internacionais. Como exemplo, ainda hoje, quase setenta anos após a Declaração Universal, os direitos nela enunciados são, em grande parte, inefetivos; mais exatamente, sua prática está amplamente entregue às instituições nacionais. Em alguns países, e em alguns períodos, a violação daqueles direitos constituiu e constitui a normalidade, conforme mostram testemunhos e relatos de agências internacionais. Observou-se, como no Brasil ditatorial, a instauração de regimes autoritários que, com frequência, embora reconhecessem oficialmente os direitos enunciados nas declarações internacionais, não favoreceram sua prática e justificaram a violação em nome de outras prioridades: da unidade política à estabilidade, à religião, ao desenvolvimento econômico (FACCHI, 2011, p.138).

O sistema internacional de proteção dos direitos humanos, não dispõe de um órgão jurisdicional com competência para julgar casos individuais de violação limitando-se à emissão de relatórios, elaborados pelos Estados-Partes e, por vezes, a "comunicações interestatais e petições individuais consideradas pelos Comitês ou Comissões (órgãos não-jurisdicionais) criados especialmente para fiscalizar o cumprimento de convenções internacionais" (BARRETO, 2012, p.12).

Apesar das inegáveis contribuições, uma dificuldade persiste quanto à implementação das sentenças de Cortes internacionais no plano doméstico, nomeadamente em assegurar a efetiva investigação dos fatos, bem como a identificação e sanção dos responsáveis pelas violações, especialmente quando estejam ou possam estar envolvidos agentes do Estado (CEIA, 2013, p.151).

A proteção da comunidade internacional, por meio de órgãos judiciários transnacionais, é uma tentativa de dar efetividade aos direitos humanos. Faltam, entretanto, normas que estabeleçam sanções para os governos que não respeitam os direitos, bem como faltam organismos de justiça transnacional para aplicar essas normas e proferir a sanção. A instituição de um Tribunal Penal Internacional é um passo importante nessa direção (FACCHI, 2011, p. 138).

Na falta de garantias jurídicas, os instrumentos de que dispõe a comunidade internacional para pressionar os governos são sobretudo: (1) as sanções econômicas; (2) o embargo; (3) a importância de manter boas relações com os países vizinhos e, em geral, com os outros Estados (FACCHI, 2011, p. 139).

Cumpre destacar que o órgão da ONU encarregado de monitorar, especificamente, a implementação da Convenção da Mulher é o Comitê da CEDAW. Esse Comitê tinha apenas competência para analisar os relatórios elaborados pelos Estados-Partes. Mas, a aprovação, em março de 1999, do Protocolo Opcional ao CEDAW (documento E/CN.6/1999/WG/L.2), permitiu que mulheres ou grupos de mulheres de Estados que o ratifiquem possam fazer denúncias ou petições individuais ou em grupo por violações de seus direitos, perante o Comitê.

Conforme visto, outro instrumento relevante é a CIDH, à qual o Brasil reconhece a competência contenciosa e na qual já teve alguns casos julgados. Não há, entretanto, especificidade em relação a crimes de gênero ou crimes sexuais na jurisprudência dessa Corte em julgados do Brasil. A CIDH considera os crimes contra a humanidade como imprescritíveis e inanistiáveis (CORTE INTERAMERICANA DE DIREITOS HUMANOS, 2010, p. 47) e conta com uma Relatoria sobre os Direitos da Mulher. Em razão do princípio ordenador do Sistema Internacional ser a soberania dos Estados, não existe a competência exclusiva de jurisdição de um órgão supraestatal sobre as matérias relacionadas (BULL, 1977, p. 2). Nesse sentido, as sanções cabíveis não podem envolver o cerceamento de liberdade de particulares (o que contrariaria o princípio da soberania estatal) debilitando o poder punitivo de tais organizações e tratados internacionais[9], que só possuem efetividade real verificada historicamente contra particulares em cenários onde o poder estatal jurisdicionante estava em si debilitado, como ao fim de guerras ou de atos de genocídio.

O sistema jurisdicional internacional, conforme a jurisprudência das cortes que vinculam o Brasil, tem poderes de jurisdição majoritariamente contra os Estados que ratificam as convenções, e não contra os cidadãos dessas nações. Somente em casos específicos foram formadas cortes políticas extra-convencionais para a punição de crimes de guerra e genocídio, como da ex-Iugoslávia e em Ruanda, lugares onde a soberania estatal estava deveras fragilizada e onde a intervenção internacional já estava instalada. A real efetividade dos tribunais internacionais de direitos humanos só será alcançada com uma mudança substancial nos princípios fundantes do Sistema Internacional de Estados soberanos, com a possibilidade do julgamento de indivíduos e a efetivação dos julgados de direito internacional no âmbito nacional.

[9] Destaque-se que, diferente da CIDH, o Tribunal Penal Internacional (TPI) estabelece em seu "Capítulo VII - As penas", mais especificamente no art. 77 que: "o Tribunal pode impor à pessoa condenada por um dos crimes previstos no art. 5º do presente Estatuto uma das seguintes penas: a) Pena de prisão por um número determinado de anos, até ao limite máximo de 30 anos; ou b) Pena de prisão perpétua, se o elevado grau da ilicitude do fato e as condições pessoais do condenado o justificarem. 2 - Além da pena de prisão, o Tribunal poderá aplicar: a) Uma multa, de acordo com os critérios previstos no Regulamento Processual; b) A perda de produtos, bens e haveres provenientes, direta ou indiretamente, do crime, sem prejuízo dos direitos de terceiros que tenham agido de boa-fé." (TRIBUNAL PENAL INTERNACIONAL, 1998).

6 Conclusão e Considerações finais

No presente artigo, buscou-se analisar o panorama histórico do reconhecimento e combate à violência sexual contra a mulher em contextos de guerra no Direito Internacional Público.

Por muito tempo, pouca ou nenhuma menção a atos de violência sexual são encontradas nas leis internacionais, período em que as leis internacionais eram feitas por homens para homens, num verdadeiro apagamento pelo não reconhecimento da violência contra a mulher. Esse período foi rompido com a assinatura da Convenção de Genebra de 1949 ao reconhecer o crime de estupro na legislação internacional.

Nesse contexto, seguiram-se diversos instrumentos legais internacionais (sejam eles declarações, tratados, pactos, estatutos, protocolos ou convenções internacionais) – que podem ser entendidos como acordos decorrentes da convergência de juízos entre sujeitos de direito internacional, formalizada por escrito, objetivando produzir efeitos jurídicos no plano internacional, i.e., estipular direitos e obrigações entre si – que foram paulatinamente reconhecendo a mulher não só como sujeito de direitos humanos, mas admitindo uma incorporação da perspectiva de gênero, voltada para melhor enfocar os múltiplos impactos da violência sexual contra a mulher. Dentre os principais normativos, destacam-se: a CEDAW, a Convenção de Belém do Pará, o Estatuto de Roma.

Igualmente importantes têm se mostrado as Resoluções do Conselho de Segurança da ONU que discorrem sobre a problemática dos crimes sexuais com enfoque de gênero, sobretudo por seu efeito vinculante aos países membros da ONU.

Nesta lógica, também foram abordadas decisões jurisprudenciais internacionais paradigmáticas, que trouxeram pela primeira vez o reconhecimento de situações e tipos penais relacionados ao tema. Destacaram-se as decisões no âmbito do Tribunal Penal Internacional para a ex-Iugoslávia, do Tribunal Penal Internacional para Ruanda, da Corte Interamericana de Direitos Humanos e da Comissão Interamericana de Direitos Humanos. Em conjunto, tais decisões firmaram importantes marcos tais como: elencar pela primeira vez o estupro como crime contra a humanidade (crime de lesa-humanidade) e, portanto, imprescritível; considerar o estupro não como uma violação à honra da mulher, mas sim como um atentado à humanidade; considerar que o estupro poderia ser considerado como crimes de tortura e genocídio; inovação ao estender-se o conceito de violência sexual para além do estupro (penetração) e deixar claro que o crime adquire matizes diferentes no que diz respeito às mulheres; o reconhecimento do uso da violência sexual como ato simbólico para humilhação; a utilização, pela primeira vez, da expressão feminicídio para se referir ao homicídio da mulher por razões de gênero; o uso, pela primeira vez do conceito de estereótipo, apontando-o como causa e consequência da violência de gênero contra a mulher; o reconhecimento que a prática estatal dirigida contra a dignidade da mulher em nível cultural, social, familiar e individual também deve ser considerada crimes contra a humanidade.

Os resultados apontam para o desenvolvimento de uma legislação, de mecanismos de denúncia e de jurisdição protetores dos direitos das mulheres em nível internacional, limitados, entretanto, pelas práticas nacionais, pelas dificuldades de efetivação dos julgados internacionais no âmbito interno e pela dificuldade de aplicar a responsabilidade individual por tribunais internacionais.

Por fim, cumpre destacar que o mapeamento aqui procedido alcança até meados de 2010. Assim, muitos outros desdobramentos importantes se seguiram e devem ser objeto de trabalhos futuros.

Referências

ASKIN, K. D. **War Crimes against Women**: Prosecution in International War Crimes Tribunal. TheHague: KluwerLaw International, 1997.

BARRERA, F. El crimen de violación y violencia sexual en el derecho nacional e internacional. In: VASALLO, M. (Org.). **Grietas en el silencio**: una investigación sobre la violencia sexual en el marco del terrorismo de Estado. 1 ed. Rosario: Cladem, 2011, p. 141-162.

BARSTED, L. L. **Os Direitos Humanos na Perspectiva de Gênero**. I Colóquio de Direitos Humanos. São Paulo, Brasil, 2001.

BARRETO, R. F. Direitos Humanos segundo os paradigmas de gênero.2012, 26 f. Monografia (Graduação em Direito) – Centro de Ciências Jurídicas, Universidade Estadual da Paraíba, Campina Grande, 2012.

BOBBIO, N. **A era dos direitos**. Rio de Janeiro: Campus/Elsevier, 2004.ISBN 13: 978-85-352-1561-8.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 466.343-1-SP. Recorrente: Banco Bradesco S/A. Recorrido: Luciano Cardoso Santos. Relator: Ministro Cezar Peluso. **Diário da Justiça Eletrônico** 104/2009, Divulgação 4/6/2009, Publicação, 5/6/2009, Ementário nº 2363-06. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=595444. Acesso em: 22 mai. 2020. p. 1106-1330.

BROOK, T. The Tokyo Judgment and the Rape of Nanking. **The Journal of Asian Studies**, v. 60, n. 3, p. 673-700, ago. 2001.

BULL, H. **A Sociedade Anárquica**: um estudo da ordem política mundial. Brasília: Editora Universidade de Brasília, 2002.

CASTILHO, A. W. V. **O Estatuto de Roma na Perspectiva de Gênero**. Brasília, DF: Procuradoria Geral da República, 2005. Disponível em: http://pfdc.pgr.mpf.mp.br/atuacao-e-conteudos-de-apoio/publicacoes/mulher/estatuto_roma.pdf. Acesso em: 20 mai. 2020.

CEIA, E. M. A Jurisprudência da Corte Interamericana de Direitos Humanos e o Desenvolvimento da Proteção dos Direitos Humanos no Brasil. **R. EMERJ**, Rio de Janeiro, v. 16, n. 61, p. 113-152, jan.-fev.-mar. 2013.

CENTRO PELA JUSTIÇA E O DIREITO INTERNACIONAL [CEJIL]. **Comisión IDH - Raquel Martín de Mejía vs. Perú -Caso Nº 10.970**. Informe Nº 5/96, de 1/3/1996. [1996].

Disponível em: https://www.cejil.org/sites/default/files/legacy_files/II.%20Comisi%C3%B3n%20Interamericana%20de%20Derechos%20Humanos_1.pdf. Acesso em: 20 mai. 2020.

CHIAROTTI, S. Jurisprudencia internacional sobre violencia sexual. In: VASALLO, M. (Org.). **Grietas en el silencio**: una investigación sobre la violencia sexual en el marco del terrorismo de Estado. 1 ed. Rosario: Cladem, 2011, p. 163-229.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. Caso Ana, Beatriz e Celia González Pérez vs. México. Caso nº 11.565. Informe nº 53/01, de 4/4/2001. [2001]. Disponível em: https://www.cidh.oas.org/annualrep/2000sp/CapituloIII/Fondo/Mexico11.565.htm. Acesso em: 21 mai. 2020.

CONFERÊNCIA MUNDIAL DOS DIREITOS HUMANOS, 1993, Viena. **Declaração e Programa de Ação de Viena**, 1993. Disponível em: http://www.direitoshumanos.usp.br/index.php/Sistema-Global.-Declara%C3%A7%C3%B5es-e-Tratados-Internacionais-de-Prote%C3%A7%C3%A3o/declaracao-e-programa-de-acao-de-viena.html. Acesso em: 22 mai. 2020.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Caso do Presídio Miguel Castro Castro vs. Peru**. Sentença de 25 de novembro de 2006. [2006]. Disponível em: https://summa.cejil.org/pt/entity/rqtvhocegnt2csor? Acesso em: 10 out. 2020.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Caso de la masacre de las Dos Erres vs. Guatemala**. Sentencia de 24 de noviembre de 2009. [2009a]. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_211_esp.pdf. Acesso em: 20 mai. 2020.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Caso González y Otra ("Campo Algodonero") vs. México**. Sentencia de 16 de noviembre de 2009. [2009b] Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_205_esp.pdf. Acesso em: 10 out. 2020.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Caso Gomes Lund e outros ("Guerrilha do Araguaia") vs. Brasil**. 2010. Disponível em: http://www.corteidh.or.cr/docs/casos/articulos/seriec_219_por.pdf. Acesso em: 20 mai. 2020.

DINIZ, M. H. **Compêndio de introdução à ciência do Direito**. 19. ed. São Paulo: Saraiva, 2008.

DUQUE, A. P. del V. **Direito como tecnologia de gênero**: uma análise a partir dos relatos de tortura a mulheres pela ditadura civil-militar nos processos do Superior Tribunal Militar (1964-1979). 2015, 63 f. Monografia (Graduação em Direito) – Faculdade de Direito, Universidade de Brasília, Brasília, 2015.

FACCHI, A. **Breve História dos Direitos Humanos**. São Paulo: Loyola, 2011. ISBN: 978-85-15-03801-5.

HAGAY-FREY, A. **Sex and gender crimes in the new International Law**: Past, Present and Future. Boston: MartinusNijhoff. 2011. ISBN: 0924-4549.

INTER-PARLAMENTARY UNION. **The Convention on the Elimination of all Forms of Discrimination against Women and its Optional Protocol**: Handbook for Parliamentarians. Switzerland: United Nations, 2003.

MOLINER, S. U. **Antecedentes Históricos de la Corte Penal Internacional:** La Corte Penal Internacional (um estudio interdisciplinar).Valencia: Tirantlo Blanch, 2003.

NEIER, A. Guerra e crimes de guerra: uma breve história. In: BARTOV, O; NOLAN, M; GROSSMANN, A. **Crimes de guerra**: culpa e negação no século XX. Rio de Janeiro: Difel, 2005. p. 37-43. ISBN: 857432065X.

OBSERVATÓRIO BRASIL DA IGUALDADE DE GÊNERO. **O Comitê CEDAW:** Comitê para a Eliminação de todas as Formas de Discriminação contra a Mulher. Disponível em: http://www.observatoriodegenero.gov.br/eixo/internacional/instancias-regionais/o-comite-CEDAW-2013-comite-para-a-eliminacao-de-todas-as-formas-de-discriminacao-contra-a-mulher. Acesso em: 22 mai. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Convenção para a prevenção e a repressão do crime de genocídio**, ONU, 1948a. Disponível em: http://www.direitoshumanos.usp.br/index.php/Sistema-Global.-Declara%C3%A7%C3%B5es-e-Tratados-Internacionais-de-Prote%C3%A7%C3%A3o/convencao-para-a-prevencao-e-a-repressao-do-crime-de-genocidio-1948.html. Acesso em: 21 mai. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal Dos Direitos Humanos**, ONU, 1948b. Disponível em: http://www.direitoshumanos.usp.br/index.php/Sistema-Global.-Declara%C3%A7%C3%B5es-e-Tratados-Internacionais-de-Prote%C3%A7%C3%A3o/declaracao-universal-dos-direitos-humanos.html. Acesso em: 21 mai. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **IIIConvenção de Genebra Relativa ao Tratamento dos Prisioneiros de Guerra**, ONU, 1949. Disponível em: http://www.direitoshumanos.usp.br/index.php/Sistema-Global.-Declara%C3%A7%C3%B5es-e-Tratados-Internacionais-de-Prote%C3%A7%C3%A3o/iii-convencao-de-genebra-relativa-ao-tratamento-dos-prisioneiros-de-guerra-1949.html. Acesso em: 21 mai. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Convenção de Genebra IV**, ONU, 1950. Disponível em: http://www.direitoshumanos.usp.br/index.php/Conven%C3%A7%C3%A3o-de-Genebra/convencao-de-genebra-iv.html. Acesso em: 21 mai. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração sobre a Eliminação da Discriminação contra a Mulher**. Tradução livre para o português, do texto em inglês do Alto Comissariado das Nações Unidas para os Direitos Humanos. Genebra: 1967. Disponível em: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cdhm/comite-brasileiro-de-direitos-humanos-e-politica-externa/DecEliDiscMul.html. Acesso em: 22 mai. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração sobre a Eliminação da Violência contra as Mulheres**. 1993a. Disponível em: http://direitoshumanos.gddc.pt/3_4/IIIPAG3_4_7.htm. Acesso em: 22 mai. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **UNSC Resolution 827 of the Security Council of the United Nations**. ONU, 1993b.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Report of the Fourth World Conference on Women (1995)**, Beijing, 4-15 September 1995. New York. 1996. (A/CONF.177/20/Rev.1)

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Case nº IT-95-17/1-T**: Prosecutor vs. Anto Furundžija, Judgement.10 Dec. 1998. Disponível em: http://www.icty.org/x/cases/furundzija/tjug/en/fur-tj981210e.pdf. Acessoem: 21 mai. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **La violencia contra la mujer perpetrada y/o condonada por el Estado, en tiempos de conflicto armado (1997-2000)**. Doc.

E/CN.4/2001/73, 2001. Disponível em: http://www.acnur.org/t3/fileadmin/Documentos/BDL/2001/1275.pdf?view=1. Acesso em: 22 mai. 2020.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **United Nations Security Council**. [2021]. Disponível em: https://www.un.org/securitycouncil/. Acesso em: 25 mar. 2021.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **UNSC Resolution 1325**. ONU, 2000.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **UNSC Resolution 1820**. ONU, 2008.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **UNSC Resolution 1888**. ONU, 2009.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **UNSC Resolution 1960**. ONU, 2010.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **UNSC Resolution 2106**. ONU, 2013.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Convenção Interamericana para prevenir, punir e erradicar a violência contra a mulher, "Convenção de Belém do Pará"**. OEA, Belém do Pará, Brasil, 9 jun. 1994. Disponível em: https://www.cidh.oas.org/basicos/portugues/m.Belem.do.Para.htm. Acesso em: 22 mai. 2020.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Inter-American Commission on Human Rights**. Disponível em: https://www.oas.org/en/iachr/mandate/what.asp. Acesso em: 25 mar. 2021.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Relatório N° 54/01, Caso 12.051 - Maria da Penha Maia Fernandes**, 4 abr. 2001. Disponível em: https://www.cidh.oas.org/basicos/portugues/m.Belem.do.Para.htm. Acesso em: 22 mai. 2020.

PAULA, L. A. M de. **Genocídio e o Tribunal Penal Internacional para Ruanda**. 2011, Dissertação (Mestrado em Direito) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011.

TRIBUNAL PENAL INTERNACIONAL, 17 jul. 1998. **Estatuto de Roma**. 1998. Disponível em:http://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/estatuto_roma_tpi.pdf. Acesso em: 22 mai. 2020.

WOMEN IN THE LAW PROJECT. No Justice, No Peace: Accountability for Rape and Gender-Based Violence in the Former Yugoslavia. 1994. **Hastings Women's Law Journal**, v. 5, n. 1, p. 91-127. 1994. Disponível em: http://repository.uchastings.edu/hwlj/vol5/iss1/5. Acesso em: 28 mai. 2020.

Artigo submetido em: 2021-01-06
Artigo reapresentado em: 2021-04-26
Artigo aceito em: 2021-05-12

ANEXO 9 - Revisão de decisão tomada com base em tratamento automatizado

Anuário do Observatório da LGPD (UnB): SCHLOTTFELDT, Shana. *Revisão de decisão tomada com base em tratamento automatizado*. Selecionada em jun. 2021 para compor o Primeiro Anuário da LGPD-UnB.

SCHLOTTFELDT, Shana. *Revisão de decisão tomada com base em tratamento automatizado*. Selecionada em jun. 2021 para compor o Primeiro Anuário da LGPD-UnB.

REVISÃO DE DECISÃO TOMADA COM BASE EM TRATAMENTO AUTOMATIZADO

Shana Schlottfeldt [1]

Dispositivo LGPD

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019)

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

§ 3º (VETADO). (Incluído pela Lei nº 13.853, de 2019)

Dispositivo GDPR

Artigo 22º - Decisões individuais automatizadas, incluindo definição de perfis

1. O titular dos dados tem o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, incluindo a definição de perfis, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar.

2. O nº 1 não se aplica se a decisão:

a) For necessária para a celebração ou a execução de um contrato entre o titular dos dados e um responsável pelo tratamento;

b) For autorizada pelo direito da União ou do Estado-Membro a que o responsável pelo tratamento estiver sujeito, e na qual estejam igualmente previstas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular dos dados; ou

c) For baseada no consentimento explícito do titular dos dados.

3. Nos casos a que se referem o nº 2, alíneas a) e c), o responsável pelo tratamento aplica medidas adequadas para salvaguardar os direitos e liberdades e legítimos interesses do titular dos dados, designadamente o direito de, pelo menos, obter intervenção humana por parte do responsável, manifestar o seu ponto de vista e contestar a decisão.

4. As decisões a que se refere o nº 2 não se baseiam nas categorias especiais de dados pessoais a que se refere o artigo 9º, nº 1, a não ser que o nº 2, alínea a) [titular dos dados tiver dado seu consentimento] ou g) [o tratamento for necessário por motivos de interesse público relevante], do mesmo artigo sejam aplicáveis e sejam aplicadas medidas adequadas para salvaguardar os direitos e liberdades e os legítimos interesses do titular.

[1] Doutora em Informática pela Universidade de Brasília (UnB), Brasil. Visiting PhD student at University of York, Reino Unido. Mestre em Informática pela Universidad Carlos III de Madrid, Espanha. Graduanda em Direito pela UnB. LLB exchange student at Australian National University, Australia. Membro do Comitê Gestor Pró-Equidade de Gênero e Raça da Câmara dos Deputados, Brasil. Pesquisadora vinculada ao Observatório da LGPD da UnB, Brasil. Orcid: https://orcid.org/0000-0002-5481-0258.

Considerandos relevantes:

(63) Modalidades e âmbito do direito de acesso.

(71) Direito de não estar sujeito a uma decisão automatizada.

(72) Aplicabilidade do GDPR à criação de perfis.

Introdução

O uso de decisões automatizadas que afetam a vida das pessoas está se tornando dia a dia mais comum. As máquinas podem aprovar pedidos de empréstimo (FTC, 2012; HARRIS, 2018); decidir se alguém deve merecer liberdade condicional ou ficar atrás das grades (BRENNAN *et al.*, 2009; LARSON *et al.*, 2016; VAN EIJK, 2017); tomar decisões de emprego (GEE, 2017; DASTIN, 2018); excluir ou colocar em desvantagem os potenciais clientes de empresas de saúde complementar de acordo com seu histórico médico; decidir acerca da empregabilidade e assim por diante (NIKLAS *et al*., 2015; COURT..., 2019; O'NEIL, 2016; COHEN, 2020, 1398).

Essas decisões são tomadas diretamente sobre o indivíduo, mas podem estar envoltas em camadas impenetráveis de complexidade e opacidade. Por exemplo, um *score* de crédito ruim pode custar a quem vai atrás de um financiamento ou empréstimo centenas de milhares de reais a mais, mas essa pessoa nunca saberá/entenderá exatamente como esse *score* foi calculado. Pior do que isso, um algoritmo pode classificar alguém como um cliente "não confiável", mas nunca lhe "contar" sobre essa decisão (MARQUES e MUCELIN, 2021, p. 143).

Este artigo trata do direito do titular de solicitar a revisão de decisões tomadas com base em tratamento automatizado de dados pessoais. Nesse sentido, procedeu-se à análise do art. 20 da Lei nº 13.079/2018 (Lei Geral de Proteção de Dados, LGPD) e do art. 22 do *General Data Protection Regulation* (GDPR, ou Regulamento Geral sobre a Proteção de Dados, RGPD)[2], que tratam sobre a temática no Brasil e na Europa, respectivamente. Por essenciais à discussão, são tratados tópicos correlatos, como discriminação algorítmica e *profiling*. Como estudo de caso, são apresentadas duas decisões sobre o tema, o Recurso Especial (Resp) 1.419.697/RS, em que se discutiu a legalidade do *credit scoring*, e o Caso 2020-0.436.002, da Autoridade de Proteção de Dados Austríaca, à luz do GDPR. Por fim, são apresentadas as considerações finais que dão conta da importância do estabelecimento e consolidação de um direito à revisão de decisões automatizadas e que os normativos brasileiro e europeu acerca da matéria, afora pequenos detalhes, são bastante semelhantes.

[2] O Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, "relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)".

1. Comentários

1.1. O que são decisões automatizadas?

A expressão Sistemas de Decisão Automatizados (*Automated Decision Systems*, ADS), no contexto da tomada de decisão, é usada para se referir às tecnologias que apoiam ou substituem o julgamento dos tomadores de decisão humanos. Sejam de fato sistemas, algoritmos ou simplesmente a aplicação de cálculos estatísticos. Esses sistemas usam técnicas como regressão, inferência baseada em regras, raciocínio baseado em casos, análise preditiva e inteligência artificial (e.g., *deep learning*, aprendizado de máquina, algoritmos genéticos, redes neurais), geralmente em combinação uns com os outros para processar dados e encontrar correlações entre eles, fazendo previsões com base em tais correlações (AUTOMATED ASSISTANCE IN ADMINISTRATIVE DECISION-MAKING WORKING GROUP, 2007, p. 4-6; MOLNAR e GILL, 2018, p. 2; BIONI e MARTINS, 2020c).

A automatização de processos decisórios inicialmente foi vista como ferramenta capaz de trazer objetividade à decisão, superando tendências de vieses e discriminação, entretanto, logo percebeu-se que ela poderia assimilar aquelas tendências já existentes nos processos tradicionais de tomada de decisões, conduzindo, igualmente, a resultados discriminatórios agora sob uma roupagem de "verdade objetiva" (BAROCAS e SELBST, 2016, p. 677; MENDES e MATTIUZZO, 2019, p. 40).

Pesquisas mostram que os humanos são psicologicamente desencorajados a desafiar decisões baseadas em IA devido ao ônus de refutá-las (McGREGOR *et al.*, 2019, p. 317-318). Assim, ainda que a decisão automatizada sirva apenas de recomendação para tomada de decisão, ela pode ser um elemento decisivo, pois para desconsiderá-la o operador humano teria que fundamentar sua opção em elementos aferíveis quantitativamente tanto quanto as previsões algorítmicas e todo espaço de subjetividade seria eliminado (BIONI e MARTINS, 2020a). Na prática, quem decide é o algoritmo, daí a importância de um direito à revisão.

1.2. Discriminação algorítmica

Segundo Barocas e Selbst (2016), ainda que se defenda que técnicas algorítmicas eliminam os preconceitos humanos no processo de tomada de decisão, um algoritmo é tão bom quanto os dados com os quais trabalha (conforme o conhecido adágio "*garbage in, garbage out*", literalmente "lixo entra, lixo sai", i.e., dados de entrada falhos produzem saídas falhas). E não raro, os dados frequentemente refletem padrões históricos de preconceito[3] e discriminação contra minorias, i.e., padrões preexistentes de exclusão e desigualdade. Além disso, uma vez

[3] Por exemplo, se uma empresa usa um algoritmo de contratação treinado com dados históricos que favorecem homens, brancos, de meia-idade, o resultado provavelmente desfavorecerá mulheres, pessoas de cor e pessoas mais jovens ou mais velhas que seriam igualmente qualificadas para preencher a vaga.

que quase sempre a discriminação resultante é uma propriedade emergente não intencional do uso do algoritmo (e não uma escolha intencional/consciente de seus programadores), pode ser particularmente difícil identificar o problema e sua origem.

Nesse contexto, utiliza-se a termo "discriminação algorítmica" para situações que refletem afirmações inconsistentes ou em que as afirmações, ainda que lógicas, consideram pessoas não como indivíduos, mas como parte de um grupo. Mendes e Mattiuzzo (2019, p. 47) apontam que ao contrário da discriminação pensada como exclusão do indivíduo de um grupo, quando se fala em discriminação algorítmica, os efeitos se verificam pela inclusão em um grupo e o consequente julgamento desse indivíduo, não por suas características particulares, mas pelas características do grupo no qual foi classificado. Trata-se de uma generalização.

Ainda segundo Mendes e Mattiuzzo (2019, p. 51-53), seriam quatro os tipos de discriminação algorítmica: (i) por erro estatístico: geralmente decorre de um erro cometido pelo responsável pelo desenho do algoritmo (e.g., utilização de dados incorretos ou de modelos estatísticos inadequados); (ii) por generalização: decorre da própria natureza de qualquer emprego probabilístico (e.g., não refletir os *outliers*[4]); (iii) pelo uso de informações sensíveis: embora possa ser estatisticamente correta, baseia-se em dados legalmente protegidos; geralmente, para que seja considerado discriminatório, além de utilizar dado sensível, deve embasar-se em característica endógena ou que distinga um grupo historicamente discriminado[5] (e.g., características discriminatórias e estereotipadas clássicas como nacionalidade e identidade de gênero); (iv) limitadora do exercício de direitos: o problema é resultado da relação entre a informação utilizada pelo algoritmo e a concretização de um direito (e.g., na Alemanha, aqueles que acessavam sua informação de *score*, tinham sua pontuação reduzida),

1.3. Profiling

Cada indivíduo tem o direito a não ser "simplificado, objetivado, e avaliado fora de contexto" (ROSEN *apud* RODOTÁ, 2008, p. 12). Apesar disso, não raro, os gestores precisam tomar decisões num cenário de conhecimento e recursos limitados. Assim, utilizam-se de características observáveis como substitutas (*proxies*) de características não observáveis (MENDES e MATTIUZZO, 2019, p. 50).

[4] *Outliers* são dados que se diferenciam de todos os demais, são os "pontos fora da curva", i.e., um valor que foge do que seria considerado padrão.

[5] "[...] é um dos tipos mais perversos de discriminação, ao reforçar o tratamento discriminatório e automatizá-lo, tornando mais difícil para os membros de tais agrupamentos superarem determinada situação prejudicial" (MENDES e MATTIUZZO, 2019, p. 54).

O *profiling* (perfilhamento, perfilação ou definição de perfis[6]) de indivíduos tem o potencial de criar sérios riscos na medida em que podem diminuir ou aumentar oportunidades sociais em aspectos relevantes da vida da pessoa conforme a categorização ou o *score* atribuído ao seu perfil (MENDES e FONSECA, 2021, p. 99). E isso ocorre não devido a algo que a pessoa efetivamente tenha feito, mas por causa das inferências ou correlações feitas por algoritmos "sugerindo" que ela pode vir a se comportar de maneira que a torna "arriscada" ou "inadequada", e.g., para concessão de crédito ou de seguro, para uma vaga de emprego, para admissão em escolas ou outras instituições (CITRON e PASQUALE, 2014, p. 24).

A situação pode ser agravada quando a formação de perfis se dá baseada em dados pessoais sensíveis, pela possibilidade maior de gerar discriminações "seja porque dados pessoais, aparentemente não 'sensíveis', podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esfera individual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas" (RODOTÁ, 2008, p. 84).

Nossa LGPD adota um conceito amplo de dado pessoal, assim como a matriz europeia, embasada na ideia de que "todo dado pessoal tem importância e valor" (VIOLA e TEFFÉ, 2021, p. 131). Mesmo dados que pareçam irrelevantes em determinadas circunstâncias, que não referenciem uma pessoa diretamente, quando tratados, organizados e cruzados, podem resultar em informação específica sobre um indivíduo, que pode ser, inclusive, de caráter sensível, como constatado pela Corte Constitucional Alemã no paradigmático julgamento sobre a Lei do Censo de 1983 (MENDES, 2018, p. 187-192). Neste mesmo sentido, o julgamento histórico no Brasil, de maio de 2020, em sede de controle de constitucionalidade no qual o Supremo Tribunal Federal (STF) reconheceu a proteção de dados pessoais como direito fundamental autônomo, baseado na lógica que não há dados "irrelevantes, neutros ou insignificantes", afirmando a proteção constitucional ao dado pessoal (MENDES, 2020; MENDES e FONSECA, 2020; RUARO e SARLET, 2021, p. 204).

1.4. LGPD: transparência, outros princípios e direitos

A transparência é um dos temas mais críticos e debatidos quando se fala em ADS. Pasquale (2015, p. 3) usa o termo "caixa preta" como metáfora para se referir a sistemas cujo funcionamento é misterioso, no qual é possível observar dados de entradas (*inputs*) e dados de

[6] Segundo o art. 4º(4) do GDPR, entende-se por "'definição de perfis', qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações" (PARLAMENTO EUROPEU e CONSELHO EUROPEU, 2016).

saídas (*outputs*), mas entre uma e outra instância, não se sabe o que aconteceu. Com a crescente automatização de decisões, ainda que a palavra final seja dada por um humano, o processo decisório pode ter sido baseado em uma análise algorítmica, de maneira que nem mesmo o tomador da decisão conseguiria explicá-la. Neste sentido, vêm-se defendendo o **direito ao devido processo informacional**, relacionado à garantia de entender (receber uma explicação) e poder contestar decisões que afetem os interesses do titular de dados (BIONI e MARTINS, 2020b). O Ministro Gilmar Mendes, no julgamento da ADI 6.389 (Caso IBGE), reconheceu a importância dessa garantia "como corolário da dimensão subjetiva do direito à proteção de dados pessoais [...] sobretudo em relação a práticas de tratamento de dados capazes de sujeitar o indivíduo a julgamentos preditivos e peremptórios" (BRASIL, 2020, p. 114).

A ideia por trás do "devido processo informacional" encontra analogia com o "devido processo legal": da mesma forma que uma pessoa não pode ser privada de sua vida, liberdade, propriedade, sem o devido processo legal, certos tipos de levantamentos, usos e disseminação de informação podem ser desafiados a fim de permitir que os titulares dos dados possam entender e se posicionar frente a decisões que tenham impacto em seus interesses (CITRON e PASQUALE, 2014, p. 19-20).

A falta de transparência é um ponto de atenção no que diz respeito à discriminação algorítmica por pelo menos três motivos: (i) pode impossibilitar evidenciar que algum tipo de discriminação ocorreu; (ii) pode dificultar a prevenção de discriminações; (iii) em vez de combater resultados discriminatórios, pode acabar por reforçá-los (MENDES e MATTIUZZO, 2019, p. 47).

A LGPD é uma lei principiológica, que prevê explicitamente o **princípio da transparência** (art. 6º, VI), que juntamente com o **princípio do livre acesso** (art. 6º, IV), dá origem ao **direito de acesso** aos dados pessoais (art. 18, II), este, por sua vez, é robustecido pelo art. 19; todos estes dispositivos juntos, permitem ao titular tomar conhecimento dos dados utilizados para decisão, bem como da forma e da duração do tratamento. A esse arcabouço, se agrega o **princípio da qualidade dos dados** (art. 6º, V), por meio do qual o titular pode demandar atualização e correção de dados incompletos, inexatos ou desatualizados (art. 18, III). Neste contexto, também importantes os **direitos à oposição e exclusão** (art. 18, VI), quando algum tratamento não devesse ser feito, ou algum dado específico não devesse ser considerado/utilizado. E, tão importante quanto os demais, o **princípio da não-discriminação** (art. 6º, IX), e.g., acionado caso o titular suponha estar sofrendo discriminação em razão de vieses.

De uma leitura sistemática da LGPD ter-se-ia a consubstanciação de outros dois direitos (MONTEIRO, 2018, p. 3): (i) **direito à explicação**: verdadeiro corolário do direito à transparência, diz respeito ao direito a receber informações úteis, suficientes, claras e compreensíveis, capazes de permitir ao titular entender a racionalidade e os critérios utilizados para o tratamento de seus dados pessoais para uma determinada finalidade; (ii) **direito à revisão de decisões automatizadas**: direito do titular requerer a revisão de uma decisão totalmente automatizada que impacte seus interesses, produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente (art. 20, LGPD).

1.4.1. Art. 20 da LGPD

Conforme a redação constante do Parecer ao Projeto de Lei (PL) nº 4.060/2012, o art. 20 da LGPD determinava o direito de revisão como um direito de revisão humana, i.e., feito por uma pessoa natural (COMISSÃO ESPECIAL, 2018, p. 71). Contudo, a Lei nº 13.853/2019, que alterou a LGPD para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados (ANPD) (conversão da Medida Provisória nº 869/2018), além de alterar a redação do *caput* do art. 20 (excluindo da redação final a expressão "por pessoa natural"), vetou seu §3º, conforme Mensagem nº 288, de 8 de julho de 2019 (BRASIL, 2019c), que dispunha, igualmente, que a revisão de que trata o *caput* do artigo deveria ser realizada por pessoa natural (BRASIL, 2019b). Daí ter-se chegado à redação atual do art. 20 da LGPD (conforme constante do início deste *paper*).

Contudo, dois importantes pontos esperam por uma melhor definição (BIONI; MARTINS, 2020): (i) quais os parâmetros do direito de revisão, já que não há **mais** a previsão expressa da revisão humana na LGPD; (ii) o que de fato são decisões tomadas **unicamente** com base em tratamento automatizado, i.e., no âmbito da discussão aqui empreendida, essencial estabelecer qual será a interpretação dada ao termo "unicamente": (ii.a) **literal**, o que praticamente esvaziará o direito de revisão ou; (ii.b) **sistemática e ampliativa**, na qual se dará abertura para efetiva aplicação do direito de revisão, considerando-se o grau de automatização dos processos decisórios, ainda que não totalmente automatizados. Entende-se que esta última seria uma interpretação possível e adequada, capaz de permitir ao cidadão, de maneira mais propícia, o exercício de seus direitos e garantias fundamentais.

Corrobora esse entendimento, discussão internacional acerca da temática de revisão de decisões automatizadas, como o posicionamento do *Information Commissioner's Office* (ICO) do Reino Unido, segundo o qual para descaracterizar uma decisão tomada unicamente com base em tratamento automatizado, o envolvimento humano deve ser ativo e não apenas um gesto simbólico, i.e., se um humano revisa a decisão antes de ela ser aplicada e tem discricionariedade

para alterá-la, e não simplesmente aplicando a decisão tomada pelo sistema automatizado (ICO, 2021).

Segundo Juliana Sakai, em levantamento que buscou mapear a maneira como sistemas de decisão automatizada têm sido utilizados no âmbito do Poder Público (Projeto Transparência Algorítmica), todos os órgãos consultados informaram que ADS têm sido usados somente para dar suporte à tomada de decisão humana, e não eles mesmos como tomadores de decisão (SAKAI *et al.*, 2020; TRANSPARÊNCIA BRASIL, 2020, p. 19-21). Isso evidencia a disputa entre três eixos: (i) o conceito de "decisão unicamente automatizada"; (ii) a prática corrente no uso de sistemas de decisão; e (iii) a viabilização do exercício de direito de revisão. Ou seja, para dar alguma efetividade ao art. 20 da LGPD, sua interpretação necessariamente deveria ser ampliativa.

Diante do exposto, entende-se que a LGPD garante (MONTEIRO, 2018, p. 14):

1. Acesso aos tipos de dados pessoais e aos dados propriamente ditos usados como entrada do sistema responsável pelo processo de decisão automatizada;
2. Se o processo automatizado tiver por finalidade formar um perfil comportamental, ou se utilizar de um perfil comportamental para tomada de decisão, o direito de acesso aos dados poderá incluir, os dados anonimizados utilizados para enriquecer tais perfis (art. 12, §2º, LGPD);
3. O direito de receber explicações claras acerca dos critérios utilizados para tomar a decisão automatizada, observados os segredos comercial e industrial (art. 20, §1º, LGPD), que devem ser analisados no caso concreto, pois estes conceitos não se encontram definidos na LGPD (vide Seção 1.4.2);
4. A possibilidade de auditoria pela ANPD para verificação de aspectos discriminatórios (art. 20, §2º, LGPD).
5. O direito de requerer revisão (que se entende deva ser promovida por **pessoa natural**, em consonância com os debates doutrinários nacionais e internacionais a respeito do assunto, apesar de não garantida pela legislação brasileira atual), caso a decisão automatizada tenha consequências nos interesses do titular, o que se presumiria, no caso de perfis.

Por fim, independentemente do direito à revisão de decisões automatizadas, em havendo dano em razão do tratamento de dados pessoais, surge a obrigação de reparação. Quanto a isso, cumpre mencionar a Seção III do Capítulo VI, da LGPD, que trata "Da Responsabilidade e do Ressarcimento de Danos", em especial o *caput* do art. 42, que dispõe que 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" (BRASIL, 2019a).

1.4.2. Segredo comercial e industrial

Apesar de poder-se ocultar a lógica do processamento com base no segredo, o direito à revisão pode ser articulado ao acesso à informação analisada para se chegar à categorização/pontuação, permitindo ao titular promover a correção e/ou atualização dos dados que levaram à definição do perfil, o que lhe possibilitaria obter classificação eventualmente mais vantajosa.

Diante disso, importa destacar que a ideia de explicabilidade quando aplicada ao processo decisório, geralmente se refere às "razões ou justificativas para aquele resultado em particular, e não a uma descrição do processo decisório em geral" (DOSHI-VELEZ e KORTZ, 2017)

Destarte, existem alguns mecanismos indiretos que permitem analisar se decisões automatizadas estão sendo tomadas de forma justa, com respeito aos princípios legais, sem a quebra do segredo de negócio: (i) informação sobre os tipos de dados usados para alimentar a base de dados; (ii) quais decisões são realmente tomadas por ADS; (iii) como tais decisões podem afetar direitos fundamentais; (iv) quais populações são afetadas pela decisão automatizada; (v) quais testes foram feitos com o ADS para evitar discriminações (BIONI; MARTINS, 2020).

1.4.3. Evolução do direito à revisão no Brasil

No Brasil, o direito à revisão de decisões automatizadas evoluiu de uma proteção setorial para uma geral.

A Lei nº 8.978/1990 (Código de Defesa do Consumidor, CDC) enuncia o direito à transparência associada ao dever de informação derivado da boa-fé objetiva (art. 4º, *caput*; art. 4º, III; art. 6º, III; art. 8º, todos do CDC). Assim, caso tenha havido uma decisão automatizada numa relação de consumo, o consumidor tem direito a conhecer os dados utilizados na tomada de decisão.

Com base no direito à transparência e à não-discriminação, a Lei nº 12.414/2011 (Lei do Cadastro Positivo) já previa o direito à explicação e à revisão de decisões automatizadas, no microssistema do setor de crédito (art. 5º, IV a VII, Lei do Cadastro Positivo), formando o arcabouço de tais direitos nas relações de consumo (MONTEIRO, 2018, p. 8). Além disso, a Lei do Cadastro Positivo buscou limitar os tipos de dados que poderiam ser utilizados para o *credit scoring*, proibindo a utilização de informações "que não estiverem vinculadas à análise de risco de crédito e aquelas relacionadas à origem social e étnica, à saúde, à informação

genética, ao sexo e às convicções políticas, religiosas e filosóficas" (art. 7º, I) i.e., dados pessoais sensíveis na atual inteligência da LGPD (art. 5º, II).

Contudo, o CDC e a Lei do Cadastro Positivo formam um microssistema de proteção de dados pessoais, restrito, malogradamente, à concessão de crédito (MONTEIRO, 2018, p. 8).

Neste sentido, a LGPD a veio para dar uma abrangência maior ao direito à revisão, não só quanto ao universo de sua incidência (qualquer decisão tomada unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluída a concessão de crédito, mas agora não só limitada a ela), mas quanto ao momento anterior de seu exercício, incluindo "as decisões destinadas a definir o [...] perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade" (art. 20, *caput*), assegurando um compromisso maior com a transparência da trilha decisória percorrida para se chegar à deliberação final.

1.5. Art. 22 do GDPR

O art. 22 do GDPR tem as suas raízes nos art. 12(a) e art. 15 da Diretiva de Proteção de Dados 95/46/CE[7]. Uma das principais diferenças é que o GDPR tem um escopo de aplicação mais amplo, pois incide no "processamento automatizado, incluindo criação de perfil", enquanto a legislação anterior dispunha só ser aplicável se uma forma de criação de perfil estivesse envolvida. Além disso, o art. 22(4), do GDPR aborda explicitamente a utilização de dados sensíveis, estabelecendo uma proibição qualificada de decisões baseadas nas categorias de dados enumeradas no art. 9º(1), do GDPR (que trata exatamente de dados sensíveis).

As "Diretrizes sobre tomada de decisão individual automatizada e criação de perfil" (WP 251 ver.01) do *Article 29 Data Protection Working Party* (WP29), recepcionadas pelo *European Data Protection Board* (EDPB), apontam que o art. 22(1) do GDPR pode ser enquadrado como uma proibição geral de "decisões individuais automatizadas, incluindo definição de perfis". Nesse sentido, afirma que (WP29, 2018, p. 19):

> O termo "direito" na disposição não significa que o art. 22(1), se aplica apenas quando ativamente invocado pelo titular dos dados. O art. 22(1) estabelece uma proibição geral para a tomada de decisões baseada exclusivamente no processamento automatizado. Esta proibição aplica-se quer o titular dos dados tome ou não medidas em relação ao tratamento dos seus dados pessoais (livre tradução).

Tal interpretação é embasada tanto nos princípios do GDPR, quanto no objetivo de dar aos titulares o controle sobre seus dados pessoais (autodeterminação informativa), que pauta o

[7] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, "relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados", foi revogada em 2018 pelo GDPR.

Regulamento como um todo. Além disso, o WP29 faz referência ao Considerando 71 do GDPR, o que implica que o Regulamento não impede a utilização de ADS ou a definição de perfis, contanto que o processamento atenda à definição do art. 22(1), caso em que será necessário garantir que se está coberto por ao menos uma das exceções constantes do art. 22(2).

O primeiro elemento capaz de acionar o art. 22 do GDPR é a presença de uma "decisão", que pode ser interpretada em sentido amplo, e.g., atos oficiais de autoridades públicas, como decisões sobre declarações de impostos (BRKAN, 2019, p. 102); recusas automáticas de pedidos de crédito *online* ou decisões semelhantes no contexto de práticas de recrutamento eletrônico. Em um sentido mais geral, as decisões também podem ser vistas como uma atitude ou posição particular tomada em relação a uma pessoa, se essa posição tiver, pelo menos, probabilidade de ser posta em prática (MENDOZA e BYGRAVE, 2017, p. 10-11).

Outro elemento de atenção é a palavra "exclusivamente" na expressão "decisão tomada exclusivamente com base no tratamento automatizado". Sua avaliação depende se a intervenção humana é possível de uma perspectiva técnica ou se o processo de tomada de decisão é construído de forma exclusivamente algorítmica, sem espaço para o envolvimento humano.

Se o processo permitir tecnicamente a intervenção humana, então deve-se avaliar se a ação realizada por pessoa natural é "significativa" ou apenas um "gesto simbólico" procedimental (WP29, 2018, p. 21). Para cumprir este critério, a intervenção deve ser "realizada por quem tenha autoridade e competência para alterar a decisão". Além disso, o ser humano envolvido não deve apenas ter o poder de mudar a decisão, mas realmente exercer essa competência "considerando todos os dados relevantes" e verificando a substância e a exatidão da decisão gerada pela máquina (WP29, 2018, p. 8).

A decisão deve "produzir efeitos jurídicos" sobre o titular dos dados o que ocorre quando ela é vinculativa e afeta os direitos ou interesses jurídicos da pessoa, e.g., o cancelamento de um contrato, a decisão de uma autoridade tributária sobre a declaração de imposto de renda de um indivíduo ou a recusa de um benefício social concedido por lei (WP29, 2018, p. 21). Ou pode "afetar significativamente o titular dos dados de forma similar" (à produção de efeitos jurídicos). Em princípio, satisfazer este critério significa que os impactos da decisão devem ser suficientemente grandes, apesar de não alterar a posição jurídica do indivíduo. Alguns critérios para efeitos significativos incluem (WP29, 2018, p. 21): (i) afetar significativamente as circunstâncias, comportamento ou escolhas dos indivíduos em questão; (ii) ter um impacto prolongado ou permanente no titular dos dados; ou (iii) no seu extremo, levar à exclusão ou discriminação de indivíduos.

O art. 22(3), do GDPR estabelece uma lista não exaustiva de salvaguardas aos titulares dos dados, ainda que não esteja claro como estas salvaguardas serão operacionalizadas e qual seu efeito prático, e.g., como seria a intervenção humana na prática, quando o site ou a plataforma tecnicamente não o permitir; caso o titular dos dados, apresente seus pontos de vista ou conteste uma decisão, isso conduzirá a sua anulação? (BRKAN, 2019, p. 108).

Por fim, o art. 22(4) traz uma proibição qualificada quanto ao uso de dados sensíveis.

2. Estudos de Caso

2.1. Brasil – Resp 1.419.697/RS (score crediting)

Apenas recentemente a LGPD entrou totalmente em vigor (à exceção das sanções – art. 52 a 54 –, que só vigoraram em agosto de 2021, o restante da Lei teve sua vigência a partir de setembro de 2020), seus detalhes e adequações devem ser promovidos pela ANPD, pelo Legislativo e pelo Judiciário, ao longo do tempo. Em que pese o Judiciário ter sido progressivamente mais mobilizado para definir os alcances e limites da LGPD, não se tem ciência de caso acionando a incidência do art. 20. Neste sentido, será trazida à discussão caso anterior à vigência da LGPD, mas que trata da temática, ainda que no microssistema da concessão crédito (do sistema de *score crediting*).

O julgamento do Recurso Especial (REsp) 1.419.697/RS, de relatoria do Ministro Paulo de Tarso Sanseverino, julgado na Segunda Seção do Superior Tribunal de Justiça (STJ) serviu de paradigma para controvérsia tratada pelo Tema 710, "acerca da natureza dos sistemas de *scoring* e a possibilidade de violação a princípios e regras do Código de Defesa do Consumidor capaz de gerar indenização por dano moral", no qual ficou firmada a tese que (BRASIL, 2014, grifo meu):

> I - O sistema "**credit scoring**" é um método desenvolvido para avaliação do risco de concessão de crédito, a partir de **modelos estatísticos, considerando diversas variáveis, com atribuição de uma pontuação ao consumidor avaliado** (nota do risco de crédito). [...] III - Na avaliação do risco de crédito, devem ser respeitados os limites estabelecidos pelo sistema de proteção do consumidor no sentido da **tutela da privacidade e da máxima transparência nas relações negociais**, conforme previsão do CDC e da Lei n. 12.414/2011. IV - Apesar de **desnecessário o consentimento do consumidor consultado**, devem ser a ele **fornecidos esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valoradas**. V - O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), **pode ensejar a responsabilidade objetiva e solidária** do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de **utilização de informações excessivas ou sensíveis** (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de **comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados**.

Também como resultado do julgamento, foi enunciada a Súmula nº 550/STJ que dispõe que "[a] utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, **que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo**" (BRASIL, 2015, grifo meu).

Segundo o relator, já se tinha à época um: (i) direito de acesso do consumidor às informações existentes sobre ele em cadastros e bancos de dados, além das respectivas fontes; (ii) dever de clareza dos arquivos; (iii) direito de retificação de informações incorretas; (iv) fixação de uma vida útil para essas informações (cinco anos) (BRASIL, 2014, p. 34). O que poderia ser sintetizado em cinco deveres a serem cumpridos pelo fornecedor do serviço: (a) dever de veracidade; (b) dever de clareza; (c) dever de objetividade; (d) vedação de informações excessivas; (e) vedação de informações sensíveis (a fim de evitar a utilização discriminatória da informação) (BRASIL, 2014, p. 35-36).

Ao decidir sobre o *credit scoring*, o STJ afirmou indiretamente o direito à revisão, ao aplicar direitos básicos do CDC, como o "dever de informação" e a "transparência". Além disso, o STJ levou em consideração os princípios da "necessidade" e da "não-discriminação" ao balizar os dados que poderiam ser usados para fins de score de crédito (BRASIL, 2014, p. 39, grifo do original):

> Não podem ser valoradas pelo fornecedor do serviço de "credit scoring" **informações sensíveis**, como as relativas à cor, à opção sexual ou à orientação religiosa do consumidor avaliado, **ou excessivas**, como as referentes a gostos pessoais, clube de futebol de que é torcedor etc.

Esta decisão firma o entendimento que para fins de análise de concessão de crédito (princípio da finalidade) está vedada a utilização de quaisquer informações de natureza personalíssima, não relacionada à finalidade esperada com a análise de crédito (princípio da não discriminação) (MULHOLLAND, 2018, p. 166)

A decisão afirmou ainda que, apesar da "metodologia em si de cálculo da nota de risco de crédito [...] constitui[r] segredo da atividade empresarial, cujas fórmulas matemáticas e modelos estatísticos naturalmente não precisam ser divulgadas" (BRASIL, 2014, p. 37), essas informações, quando solicitadas, devem ser prestadas ao consumidor avaliado, com a indicação clara e precisa dos bancos de dados utilizados possibilitando o exercício do controle da veracidade dos dados, inclusive para poder retificá-los ou melhorar a sua performance. Ademais, devem ser prestadas também as informações pessoais do consumidor que foram

consideradas para que ele possa exercer o direito de controle quanto às informações excessivas ou sensíveis (BRASIL, 2014, p. 38).

2.2. Europa – Caso 2020-0.436.002 (score - Áustria)

O Caso 2020-0.436.002, apresentado junto à *Datenschutzbehörde* (DSB), Autoridade de Proteção de Dados Austríaca, apesar de não decidir pela incidência explícita do art. 22 do GDPR, traz uma série de considerações importantes acerca de direitos aqui tratados.

A ré teria calculado um *marketing score* chamado "Dominanten Geo Milieus" em relação ao autor (DSB, 2020). Esse score consistiria em supostas probabilidades (expressas em um número percentual) de que o autor pertenceria a um determinado grupo dentre "conservadores", "tradicionalistas", "hedonistas" ou "individualistas digitais". Em maio de 2019, o autor enviou à ré uma solicitação de acesso sobre como o *score* foi calculado, com base no art. 15(1)(h) do GDPR. Em junho de 2019, a ré recusou-se a fornecer a informação por entender que se qualificava como segredo comercial. Diante disso, o autor apresentou uma queixa junto à DSB.

Em 2020, quando decidiu o caso, a DSB inicialmente considerou que o *score* em questão constitui dado pessoal nos termos do art. 4(1) do GDPR, uma vez que foi atribuído a pessoas singulares. Além disso, considerou que as atividades de processamento que conduzem à criação desse *score* constituem perfis, conforme art. 4(4) do GDPR. Tendo em vista o Considerando 71 do GDPR e as diretrizes constantes do WP 251 rev.01, a DSB enfatizou que o GDPR diferencia entre a criação de perfis nos termos do art. 4(4) e a tomada de decisão automatizada nos termos do art. 22: para uma atividade de processamento ser qualificada como criação de perfis, não é necessário que esta atividade seja realizada exclusivamente de maneira automatizada.

Em seguida, o DSB avaliou se o reclamante tinha direito à informação nos termos do art. 15(1)(h) do GDPR em relação ao *score* e se a ré havia infringido esse direito. De acordo com a DSB, o direito ao abrigo do art.15(1)(h) do GDPR não se limita aos casos de tomada de decisão automatizada do art. 22(1) e (4) do GDPR, mas também abrange outros casos, como o perfil em questão: a utilização da expressão "pelo menos nesses casos", no art. 15(1)(h), aponta para um âmbito amplo de aplicação. Consequentemente, a DSB não viu necessidade de avaliar mais se o *score* também se qualificava como tomada de decisão automatizada de acordo com o art. 22 do GDPR.

Por último, a DSB entendeu que a ré não é obrigada a divulgar o algoritmo, código-fonte ou código compilado que foi usado ao criar o *score*. Em vez disso, deve fornecer as seguintes informações conexas ao cálculo da pontuação: (i) parâmetros/variáveis de entrada e como eles surgiram (e.g., usando informações estatísticas); (ii) efeito dos parâmetros/variáveis

de entrada na pontuação; (iii) explicação do motivo pelo qual ao titular dos dados foi atribuído um determinado resultado de avaliação; (iv) lista de possíveis categorias de perfil; ou (v) informações equivalentes que permitam ao titular dos dados exercer os seus direitos de retificação e eliminação, bem como examinar a legalidade do processamento.

3. Considerações Finais

A LGPD é uma lei principiológica, da qual derivam (implícita e explicitamente) diversos direitos, um deles diz respeito ao direito à revisão de decisões automatizadas, previsto no art. 20. Este direito se reveste de especial importância diante de problemas relacionados à utilização de ADS, tais como a falta de transparência, dificuldade de identificar e corrigir erros, reforço de desigualdades (vieses). Na Europa, esse direito é tratado, principalmente, pelo art. 22 do GDPR. Ambos normativos apresentam diversas similaridades (o que é natural, tendo em vista que o GDPR serviu de inspiração para a LGPD). Entretanto, há certas distinções importantes: (i) o GDPR impõe algumas restrições não presentes na LGPD: (i.a) não inclui o caso dos dados anonimizados (previstos no art. 12, §2º, LGPD); (i.b) limita o direito de oposição quando a base legal para tratamento dos dados for o consentimento explícito ou a execução de um contrato (art. 22(2), GDPR); (ii) mas, o GDPR prevê explicitamente a intervenção humana (art. 22(3), GDPR), enquanto da LGPD não consta tal previsão. De qualquer forma, no Brasil ou na Europa, percebe-se que definir os contornos, limites e conferir efetividade ao direito à revisão automatizada será papel das Autoridades de Proteção de Dados, da doutrina e da jurisprudência.

Bibliografia

ACLU, American Civil Liberties Union; CENTER FOR DEMOCRACY & TECHNOLOGY; ELECTRONIC FRONTIER FOUNDATION; NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE; RAICU, Irina; SUZOR, Nicolas; WEST, Sarah Myers; ROBERTS, Sarah T. *Santa Clara Principles on transparency and accountability in content moderation*. 7 mai. 2018. Disponível em: https://santaclaraprinciples.org/. Acesso em: 28 ago. 2021.

AUTOMATED ASSISTANCE IN ADMINISTRATIVE DECISION-MAKING WORKING GROUP. *Automated Assistance in Administrative Decision-Making Better Practice Guide*. Canberra: Australian Government, 2007.

BAROCAS, Solon; SELBST, Andrew D. Big Data's Disparate Impact. *California Law Review*, v. 104, n. 3, p. 671-732, jun. 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899.#. Acesso em: 30 ago. 2021.

BIONI, Bruno; MARTINS, Pedro. *Devido processo informacional*: um salto teórico-dogmático necessário? . 2020a. Disponível em: https://d335luupugsy2.cloudfront.net/cms%2Ffiles%2F108127%2F1599509820Ensaio_Devido_Processo_Informacional_-_V2.pdf. Acesso em: 10 jun. 2021.

BIONI, Bruno; MARTINS, Pedro. O que você precisa ler para entender sobre devido processo informacional. *Data Privacy Brasil*, 2020b. Disponível em: https://conteudo.dataprivacy.com.br/devido-processo-informacional. Acesso em: 29 jun. 2021.

BIONI, Bruno; MARTINS, Pedro. *Série LGPD em Movimento*: LGPD e Decisões Automatizadas. 14 dez. 2020c. Disponível em:

https://www.observatorioprivacidade.com.br/2020/12/14/serie-lgpd-em-movimento-lgpd-e-decisoes-automatizadas/.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 jun. 2021.

BRASIL. *Lei nº 13.853, de 8 de julho de 2019*. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. (Conversão da Medida Provisória nº 869, de 2018). 2019b. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em: 22 jun. 2021.

BRASIL, Presidência da República. *Mensagem nº 288, de 8 de julho de 2019*. Comunica veto parcial ao Projeto de Lei de Conversão nº 7, de 2019 (MP nº 869/2018), que "Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências". 2019c. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Msg/VEP/VEP-288.htm. Acesso em: 22 jun. 2021.

BRASIL, Superior Tribunal de Justiça (Segunda Seção). Resp nº 1.419.697/RS. Relator: Min. Paulo de Tarso Sanseverino, julgado em 12/11/2014, DJe 17/11/2014. . 2014. Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/114173/REsp1419697.pdf. Acesso em: 10 jun. 2021.

BRASIL, Superior Tribunal de Justiça (Segunda Seção). *Súmula nº 550*. 2015. Disponível em: https://scon.stj.jus.br/SCON/sumanot/toc.jsp?livre=(sumula%20adj1%20%20550).sub. Acesso em: 15 ago. 2021.

BRASIL, Supremo Tribunal Federal (Plenário). *Referendo na Medida Cautelar na Ação Direta de inconstitucionalidade (ADI) nº 6.389/DF*. Ementa medida cautelar em ação direta de inconstitucionalidade. Referendo. Medida provisória nº 954/2020. Emergência de saúde pública de importância internacional decorrente do novo coronavírus (covid-19). Compartilhamento de dados dos usuários do serviço telefônico fixo comutado e do serviço móvel pessoal, pelas empresas prestadoras, com o instituto brasileiro de geografia e estatística. Fumus boni juris. Periculum in mora. Deferimento. Relatora: Min. Rosa Weber, julgado em 07/05/2020, processo eletrônico dje-270, divulg 11-11-2020, public 12-11-2020. 12 nov. 2020. Disponível em: http://portal.stf.jus.br/processos/downloadPeca.asp?id=15344950131&ext=.pdf. Acesso em: 29 jun. 2021.

BRENNAN, Tim; DIETERICH, William; EHRET, Beate. Evaluating the Predictive Validity of the Compas Risk and Needs Assessment System. *Criminal Justice and Behavior*, v. 36, n. 1, p. 21-40, 2009. Disponível em: https://doi.org/10.1177/0093854808326545. Acesso em: 30 ago. 2021.

BRKAN, Maja. Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International Journal of Law and Information Technology*, v. 27, n. 2, p. 91–121, Summer 2019. Disponível em: https://doi.org/10.1093/ijlit/eay017. Acesso em: 1 set. 2021.

BUTLER, Sarah. Court tells Uber to reinstate five UK drivers sacked by automated process. *The Guardian*, 14 abr. 2021. Disponível em: https://www.theguardian.com/technology/2021/apr/14/court-tells-uber-to-reinstate-five-uk-drivers-sacked-by-automated-process. Acesso em: 1 set. 2021.

CITRON, Danielle Keats; PASQUALE, Frank A. The Scored Society: Due Process for Automated Predictions. Washington Law Review, v. 89, p. 1-31, 2014. Disponível em: https://ssrn.com/abstract=2376209. Acesso em: 29 jun. 2021.

COHEN, Julie E. Examined Lives: Informational Privacy and the Subject as Object. *Stan. L. Rev.*, v. 52, p. 1373-1438, 2000. Disponível em: https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1819&context=facpub. Acesso em: 7 set. 2021.

COMISSÃO ESPECIAL, destinada a proferir parecer ao Projeto de Lei nº 4.060, de 2012. *Parecer ao Projeto de Lei nº 4.060, de 2012*

(Tratamento e Proteção de Dados Pessoais) (Apenso PLs nº 5.276/16 e 6.291/16). Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Autor: Deputado Milto Monti. Relator: Deputado Orlando Silva., 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305

http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1664206. Acesso em: 22 jun. 2021.

COURT hearing in lawsuit against System Risk Indication (SyRI). *Privacy First*, 2019. Disponível em: https://www.privacyfirst.eu/court-cases/680-court-hearing-in-lawsuit-against-system-risk-indication-syri.html. Acesso em: 22 ago. 2021.

DASTIN, Jeffrey. Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*, 10 out. 2018. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G. Acesso em: 30 ago. 2021.

DOSHI-VELEZ, Finale; KORTZ, Mason A. *Accountability of AI Under the Law*: The Role of Explanation. Berkman Klein Center Working Group on Explanation and the Law, Berkman Klein Center for Internet & Society working paper, p. 1-15, 2017. Disponível em: http://nrs.harvard.edu/urn-3:HUL.InstRepos:34372584. Acesso em: 30 ago. 2021.

DSB, Datenschutzbehörde. (Austria) - GZ: 2020-0.436.002 of September 8, 2020 (case number: DSB-D124.909). Machine translation of the German original. European Case Law Identifier (ECLI) ECLI:AT:DSB:2020:2020.0.436.002. GDPRHub, 8 set. 2020. Disponível em: https://gdprhub.eu/index.php?title=DSB_(Austria)_-_2020-0.436.002. Acesso em: 1 set. 2021.

FTC, Federal Trade Commission. *Report to Congress Under Section 319 of the Fair and Accurate Credit Transactions Act of 2003*. dez. 2012. Disponível em: https://www.ftc.gov/sites/default/files/documents/reports/section-319-fair-and-accurate-credit-transactions-act-2003-fifth-interim-federal-trade-commission/130211factareport.pdf. Acesso em: 30 ago. 2021.

GEE, Kelsey. In Unilever's Radical Hiring Experiment, Resumes Are Out, Algorithms Are In. *The Wall Street Journal*, 26 jun. 2017. Disponível em: https://www.wsj.com/articles/in-unilevers-radical-hiring-experiment-resumes-are-out-algorithms-are-in-1498478400. Acesso em: 30 ago. 2021.

HARRIS, John. The tyranny of algorithms is part of our lives: soon they could rate everything we do. *The Guardian*, Opinion, Big Data, 5 mar. 2018. Disponível em: https://www.theguardian.com/commentisfree/2018/mar/05/algorithms-rate-credit-scores-finances-data. Acesso em: 28 jun. 2021.

ICO, Information Comissioner's Office. *In the picture*: A data protection code of practice for surveillance cameras and personal. Version 1.2. London: ICO, Information Comissioner's Office, 2017. Disponível em: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf. Acesso em: 13 jul. 2021.

ICO, Information Comissioner's Office. *What does the UK GDPR say about automated decision-making and profiling*?, 2021. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-does-the-uk-gdpr-say-about-automated-decision-making-and-profiling/. Acesso em: 9 set. 2021.

LARSON, Jeff; MATTU, Surya; KIRCHNER, Lauren; ANGWIN, Julia. How We Analyzed the COMPAS Recidivism Algorithm. *ProPublica*, 23 mai. 2016. Disponível em: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm. Acesso em: 28 jun. 2021.

MARQUES, Claudia Lima; MUCELIN, Guilherme. Novo Mercado de Consumo 'Simbiótico' e a Necessidade de Proteção de Dados dos Consumidores. In: SARLET, G. B. S.;TRINDADE, M. G. N., et al (Ed.). *Proteção de dados: temas controvertidos*. Indaiatuba: Foco, 2021. p.133-183.

McGREGOR, Lorna; MURRAY, Daragh; NG, Vivian. International Human Rights Law as a Framework for Algorithmic Accountability. *International & Comparative Law Quarterly*, v. 68, n. 2, p. 309 - 343 2019. Disponível em:

https://doi.org/10.1017/S0020589319000046. Acesso em: 29 jun. 2021.

MENDES, Laura Schertel. A vulnerabilidade do consumidor quanto ao tratamento de dados pessoais. *Revista de Direito do Consumidor*, v. 102, p. 19-43, nov./dez. 2015.

MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. *Jota*, 10 mai. 2020. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais-10052020. Acesso em: 22 jun. 2021.

MENDES, Laura Schertel Ferreira. Habeas data e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais e Justiça*, v. 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel; FONSECA, Gabriel ampos Soares da. Proteção de dados para além do consentimento: tendências de materialização. (cap. 4). In: DONEDA, D.;SARLET, I. W., et al (Ed.). *Tratado de Proteção de Dados*. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados. *Revista de Direito do Consumidor*, v. 130, p. 471-478, jul./ago. 2020.

MENDES, Laura Schertel; MATTIUZZO, Marcela. Discriminação Algorítmica: Conceito, Fundamento Legal e Tipologia. *RDU*, v. 16, n. 90, p. 39-64, nov.-dez. 2019.

MENDOZA, Isak; BYGRAVE, Lee A. *The Right Not to Be Subject to Automated Decisions Based on Profiling*. University of Oslo Faculty of Law Legal Studies Research Paper Series No. 2017-20, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855. Acesso em: 1 set. 2021.

MOLNAR, Petra; GILL, Lex. *Bots at the Gate*: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System. International Human Rights Program, Faculty of Law, University of Toronto and the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto, 2018.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? *Instituto Igarapé - Artigo Estratégico,* v. 39, dez. 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2018/12/Existe-um-direito-a-explicacao-na-Lei-Geral-de-Protecao-de-Dados-no-Brasil.pdf.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (lei 13.709/18). R. Dir. Gar. Fund, v. 19, n. 3, p. 159-180, set./dez. 2018. Disponível em: http://dx.doi.org/10.18759/rdgf.v19i3.1603. Acesso em: 15 ago. 2021.

NIKLAS, Jędrzej; SZTANDAR-SZTANDERSKA, Karolina; SZYMIELEWICZ, Katarzyna. *Profiling the unemployed in Poland: social and political implications of algorithmic decision making*. Warsaw: Fundacja Panoptykon, 2015. Disponível em: https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf. Acesso em: 29 jun. 2021.

O'NEIL, Cathy. *Weapons of math destruction*: how big data increases inequality and threatens democracy. 1 ed. New York: Crown, 2016.

PARLAMENTO EUROPEU. *Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Jornal Oficial nº L 281 de 23/11/1995 p. 0031 - 0050. 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acesso em: 1 ago. 2021.

PARLAMENTO EUROPEU; CONSELHO EUROPEU. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE* (Regulamento Geral sobre a Proteção de Dados, RGPD, ou General Data Protection Regulation, GDPR). EUR-Lex, Access to

European Union Law, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 10 jul. 2021.

PASQUALE, Frank. *The Black Box Society*: The Secret Algorithms That Control Money and Information. Cambridge (Massachusetts), London: Harvard University Press, 2015.

RB AMSTERDAM, Rechtbank Amsterdam [District Court of Amsterdam]. *C/13/696010 / HA ZA 21-81*. European Case Law Identifier: ECLI:NL:RBAMS:2021:1415. GDPRHub, 24 fev. 2021a. Disponível em: https://gdprhub.eu/index.php?title=Rb._Amsterdam_-_C/13/696010_/_HA_ZA_21-81. Acesso em: 1 set. 2021.

RB AMSTERDAM, Rechtbank Amsterdam [District Court of Amsterdam]. *C/13/696010 / HA ZA 21-81*. European Case Law Identifier: ECLI:NL:RBAMS:2021:1415. Rechtspraak, 24 fev. 2021b. Disponível em: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2021:1415&showbutton=true&keyword=ECLI%3ANL%3ARBAMS%3A2021%3A1415. Acesso em: 1 set. 2021.

RODOTÁ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUARO, Regina Linden; SARLET, Gabriele Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) - Lei 13. 709/2018. In: DONEDA, D.;SARLET, I. W., et al (Ed.). *Tratado de Proteção de Dados*. Rio de Janeiro: Forense, 2021.

SAKAI, Juliana; BUTALLA, Vanessa; ROBERTO, Enrico; BIONI, Bruno; MARTINS, Pedro. *LGPD e decisões automatizadas*. [1h53min26seg]. Data Privacy Brasil, LGPD em Movimento, 3 dez. 2020. Disponível em: https://www.youtube.com/watch?v=SNg8N7eCU6k. Acesso em: 17 jul. 2021.

TRANSPARÊNCIA BRASIL. *Recomendações de governança*: uso de inteligência artificial pelo poder público. fev. 2020. Disponível em: https://www.transparencia.org.br/downloads/publicacoes/Recomendacoes_Governanca_Uso_IA_PoderPublico.pdf. Acesso em: 28 ago. 2021.

VAN EIJK, Gwen Socioeconomic marginality in sentencing: The built-in bias in risk assessment tools and the reproduction of social inequality. *Punishment & Society*, v. 19, n. 4, p. 463-481, 2017. Disponível em: https://doi.org/10.1177/1462474516666282. Acesso em: 30 ago. 2021.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7.º e 11. In: DONEDA, D.;SARLET, I. W., et al (Ed.). *Tratado de Proteção de Dados*. Rio de Janeiro: Forense, 2021.

WP29, Article 29 Data Protection Working Party. *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. WP251rev.01. 6 fev. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/redirection/document/49826. Acesso em: 15 ago. 2021.