UNIVERSIDADE FEDERAL DE JUIZ DE FORA
FACULDADE DE DIREITO
SAMUEL RODRIGUES DE OLIVEIRA

SORRIA, VOCÊ ESTÁ SENDO FILMADO: tecnologias de reconhecimento facial, privacidade e proteção de dados

Juiz de Fora
2020

SAMUEL RODRIGUES DE OLIVEIRA

SORRIA, VOCÊ ESTÁ SENDO FILMADO: tecnologias de reconhecimento facial, privacidade e proteção de dados

Dissertação apresentada ao programa de Pós-graduação *Stricto Sensu* em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Mestre no Mestrado em Direito e Inovação, sob a orientação do Prof. Dr. Sergio Marcos Carvalho de Ávila Negri.

Juiz de Fora
2020

Ficha catalográfica elaborada através do programa de geração
automática da Biblioteca Universitária da UFJF,
com os dados fornecidos pelo(a) autor(a)

Rodrigues de Oliveira, Samuel.
SORRIA, VOCÊ ESTÁ SENDO FILMADO : tecnologias de reconhecimento facial, privacidade e proteção de dados / Samuel Rodrigues de Oliveira. -- 2020.
149 f.

Orientador: Sergio Marcos Carvalho de Ávila Negri
Dissertação (mestrado acadêmico) - Universidade Federal de Juiz de Fora, Faculdade de Direito. Programa de Pós-Graduação em Direito, 2020.

1. Privacidade. 2. Proteção de dados. 3. Reconhecimento facial. 4. Vigilância . I. Carvalho de Ávila Negri, Sergio Marcos, orient. II. Título.

FOLHA DE APROVAÇÃO

SAMUEL RODRIGUES DE OLIVEIRA

SORRIA, VOCÊ ESTÁ SENDO FILMADO: tecnologias de reconhecimento facial, privacidade e proteção de dados

Dissertação apresentada ao programa de Pós-graduação *Stricto Sensu* em Direito da Faculdade de Direito da Universidade Federal de Juiz de Fora, como requisito parcial para obtenção do grau de Mestre no Mestrado em Direito e Inovação, sob a orientação do Prof. Dr. Sergio Marcos Carvalho de Ávila Negri, submetida à Banca Examinadora composta pelos membros:

Orientador: Prof. Dr. Sergio Marcos Carvalho de Ávila Negri
Universidade Federal de Juiz de Fora

Profª. Drª Caitlin Sampaio Mulholland
PUC-Rio

Prof. Dr. Marcos Vinício Chein Feres
Universidade Federal de Juiz de Fora

PARECER DA BANCA

( ) APROVADO

( ) REPROVADO

Juiz de Fora, 26 de junho de 2020

DEDICATÓRIA

Dedico este trabalho à memória do Professor Denis Franco Silva, cujos ombros me permitiram, um dia, enxergar mais longe.

AGRADECIMENTOS

Em primeiro lugar, agradeço àqueles que me trouxeram à vida, cuidaram e amaram ao longo de minha existência. À minha mãe, Deusimar, por nutrir em mim a paixão pelos estudos e por me fazer entender a importância da educação. Ao meu pai, José Geraldo, por não ter medido esforços para que eu atingisse meus objetivos e concretizasse meus sonhos.

Agradeço ao Professor Sergio Negri, por ter aceitado participar comigo desta empreitada. Sua orientação e apoio foram cruciais para que superasse tantos percalços e chegasse aonde estou.

Agradeço ao Aluísio, por todo o companheirismo do qual pude desfrutar nestes últimos anos, e por ter sido, acima de tudo, um amigo capaz de entender as minhas aflições e de me ajudar a vencê-las.

Agradeço ao Ramon, por termos crescido e produzido juntos, mas, principalmente, pela amizade que hoje existe além das fronteiras da academia.

Agradeço à Núbia, por ter trazido leveza para esta etapa ao me fazer rir em tantas conversas e pelo zelo e prontidão com que realizou a revisão deste texto.

Agradeço aos amigos que, de uma forma ou de outra, se fizeram presentes diretamente no processo de elaboração desta pesquisa. Ao Luiz Guilherme, por solucionar tantas dúvidas linguísticas e pelos momentos de procrastinação; à Jéssica e à Linemara, por toda atenção dada.

Agradeço aos professores com quem tive contato ao longo de toda a minha formação, por haverem sido fontes de inspiração e, nos tempos em que vivemos, de coragem; em especial, Marquinhos e Caitlin, por aceitarem avaliar este trabalho.

Agradeço à Universidade Federal de Juiz de Fora, por ser uma instituição de ensino pública, gratuita e de tamanha qualidade. Agradeço à Faculdade de Direito e ao Programa de Pós-Graduação em Direito e Inovação, na pessoa de todos os professores e funcionários que contribuem para o funcionamento de tão necessárias instituições.

Agradeço, por fim, a todos aqueles que, à sua maneira, estiveram presentes ao longo desta jornada.

"For Sabina, living in truth, lying neither to ourselves nor to others, was possible only away from the public: the moment someone keeps an eye on what we do, allowances for that eye, and nothing we do is truthful. Having a public, keeping a public in mind, means living in lies. Sabina despised literature in which people give away all kinds of intimate secrets about themselves and their friends.
A man who loses his privacy loses everything, Sabina thought. And a man who gives it up of his own free will is a monster."

Milan Kundera

RESUMO

Os avanços recentes da ciência de dados e da inteligência artificial, somados à suposta demanda por segurança no mundo contemporâneo, fizeram surgir a sociedade da vigilância, que se apresenta como um pan-óptico digital. Nesse contexto, tecnologias de reconhecimento facial destacam-se enquanto ferramentas de vigilância, cuja ubiquidade se torna cada vez mais evidente. Tais tecnologias, contudo, podem representar um grande risco à privacidade e à salvaguarda de dados pessoais. Diante disso, esta dissertação tem como objetivos investigar quais são as implicações do desenvolvimento e da utilização de tecnologias de reconhecimento facial no direito à privacidade e no direito à proteção de dados e analisar o papel regulatório do Direito em relação a essas inovações. Trata-se de uma pesquisa de caráter exploratório, realizada mediante análise bibliográfica e documental. Conclui-se que, embora as legislações gerais de proteção de dados possam orientar a regulação das tecnologias de reconhecimento facial, é necessário um debate mais aprofundado e esclarecido sobre o tema a fim de desenvolver instrumentos normativos aptos a regular adequadamente essas tecnologias.

Palavras-chave: *big data*; direitos da personalidade; inteligência artificial; vigilância.

ABSTRACT

Recent advances in data science and artificial intelligence, coupled with the supposed demand for security in the contemporary world, have given rise to the surveillance society, which presents itself as a digital pan-optic. In this context, facial recognition technologies stand out as surveillance tools whose ubiquity becomes increasingly evident. Such technologies, however, can pose a great risk to privacy and the safeguarding of personal data. Therefore, this dissertation aims to investigate the implications of the development and use of face recognition technologies on the right to privacy and the right to data protection, and to analyze the regulatory role of the Law regarding these innovations. It is an exploratory research, carried out through bibliographic and documental analysis. The conclusion is that, although general data protection legislation can guide the regulation of facial recognition technologies, we need a more in-depth and enlightened debate on the subject in order to develop normative instruments capable of adequately regulating these technologies.

Keywords: artificial intelligence; big data; personality rights; surveillance.

LISTA DE ILUSTRAÇÕES

Figura 1 - Ilustração da análise da biometria facial 23

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
Art.	Artigo
ACLU	*American Civil Liberties Union*
APP	Aplicativo
CCTV	*Closed-circuit television*
CFTV	Circuito Fechado de Televisão
EUA	Estados Unidos da América
FRA	*Fundamental Rights Agency*
FRT	*Facial recognition technology*
GDPR	*General Data Protection Regulation*
IA	Inteligência artificial
IoT	*Internet of Things*
LGPD	Lei Geral de Proteção de Dados
MIT	*Massachusetts Institute of Technology*
n.º	Número
p.	página
PEC	Projeto de Emenda à Constituição
PL	Projeto de Lei
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
RIDPD	Relatório(s) de Impacto à Proteção de Dados Pessoais
SEC	*Section*
TIC	Tecnologia(s) da Informação e Comunicação
TRF	Tecnologia(s) de reconhecimento facial
UE	União Europeia

LISTA DE SÍMBOLOS

§	Parágrafo (quando se referir à legislação brasileira)
%	Porcentagem
§	Seção (quando se referir à legislação estadunidense)

SUMÁRIO

1 INTRODUÇÃO 13
1.1 Apresentação do tema, problema e objetivos 13
1.2 Apontamentos metodológicos 17
1.3 Organização da pesquisa 18
2 TECNOLOGIAS DE RECONHECIMENTO FACIAL: O QUE, COMO, ONDE 20
2.1 Um breve histórico das tecnologias de reconhecimento facial: das câmeras de videomonitoramento ao *big data* 20
2.2 Atuais usos de tecnologias de reconhecimento facial 24
2.2.1 No Brasil 25
2.2.2 No mundo 29
2.3 Questões atinentes às tecnologias de reconhecimento facial 35
2.3.1 A falta de precisão 37
2.3.2 Enviesamento 39
2.3.2.1 O machismo algorítmico 45
2.3.2.2 O racismo algorítmico 48
3 ACABOU-SE A PRIVACIDADE? REPENSANDO DIREITOS NO CONTEXTO DO PAN-ÓPTICO DIGITAL 53
3.1 Da sociedade de vigilância ao pan-óptico digital 53
3.2 O pan-óptico digital 60
3.3 Rediscutindo o direito à privacidade 66
3.3.1 Como o reconhecimento facial afeta a privacidade? 73
3.4 O direito à proteção de dados 81
3.4.1 Dados que deixam rastros 83
3.4.2 O corpo como unidade 85
4 EM BUSCA DE UM MODELO REGULATÓRIO PARA TECNOLOGIAS DE RECONHECIMENTO FACIAL 88
4.1 As justificativas para o emprego de tecnologias de reconhecimento facial 88
4.2 Enquadrando corretamente o debate "segurança *vs.* proteção de dados" 91
4.3 Os diferentes caminhos para a regulação 94
4.4 A regulação por princípios 97
4.5 A Lei Geral de Proteção de Dados Pessoais (LGPD) 101
4.5.1 Princípios da finalidade, adequação e necessidade 104

4.5.1.2 Consentimento 108
4.5.2 Princípios da transparência, livre acesso e qualidade dos dados 110
4.5.3 Princípios da segurança e prevenção 114
4.5.3.1 Princípio da precaução 115
4.5.4 Princípio da não discriminação 116
4.5.5 Princípio da responsabilização e prestação de contas 117
4.6 No Brasil: PL 9736/2018 e PL 4612/2019 119
4.7 Ideais regulatórios: exemplos a serem seguidos? 121
4.7.1 As disposições da Agência dos Direitos Fundamentais da União Europeia sobre tecnologias de reconhecimento facial 122
4.7.2 A *Ordinance* NO. 107-19 da cidade de São Francisco (EUA) 125
5 CONSIDERAÇÕES FINAIS 128
REFERÊNCIAS 131

1 INTRODUÇÃO

"Let there be a digital future, but let it be a human future first."

Soshana Zuboff

1.1 Apresentação do tema, problema e objetivos

A informação sempre foi um elemento essencial para o desenvolvimento humano. Hoje, mais do que nunca. Sedimentada pela evolução tecnológica, a sociedade de informação criou mecanismos capazes de processar e transmitir informações de modo cada vez mais veloz, ocasionando novas formas de organização social (BIONI, 2018). Se no passado nos organizávamos como uma sociedade presencial, atualmente somos, em grande parte, digitais. Isso implica sociabilidades amplamente mediadas por tecnologias, que fomentam relações mercadológicas, pessoais, econômicas, culturais e até mesmo de vigilância, o que se dá por meio da expansão do ciberespaço (RODOTÀ, 2008). Essa expansão, que surge da interconexão mundial dos computadores, se ampliou e amplia exponencialmente mediante os avanços tecnológicos, culminando numa verdadeira "galáxia da internet" (CASTELLS, 2003).

Nesse cenário, a ciência de dados e a inteligência artificial (IA) despontam como nichos tecnológicos de indescritível ubiquidade. Aplicadas nos mais diversos âmbitos do cotidiano, essas "novas" áreas do conhecimento fazem com que questões éticas atinentes à tecnologia ganhem cada vez mais atenção e importância (RICHARDS, 2013). Do emprego maciço das inovações tecnológicas decorrem alguns fenômenos. Dentre eles, a consolidação da vigilância, tema da presente pesquisa.

Muitos não percebem, mas a realização de tarefas básicas do dia-a-dia, como ir de carro ao supermercado para fazer compras, pode nos expor a inúmeras dimensões de vigilância. John Gilliom e Torin Monahan (2013) propõem um teste rápido para se descobrir se estamos, em algum aspecto, submetidos a esse fenômeno:

> Você tem alguma dessas coisas: um telefone celular, um cartão de crédito ou débito, um documento de identificação? Você faz alguma dessas coisas: usa o Google, G-mail ou Facebook, vai à escola, tem um trabalho, dirige um carro? Se a resposta para qualquer uma dessas perguntas é "sim", então você está sob vigilância (GILLIOM; MONAHAN, 2013, p. 8, tradução nossa).

Cada um desses itens, lugares e atividades é um agente-chave nos sistemas sobrepostos de observação, de coleta de dados e de avaliação que compõem uma "sociedade de vigilância". E todavia a maioria das pessoas associe a palavra "vigilância" a câmeras de vídeo instaladas

em portarias ou postes espalhados pelas cidades, o escopo da vigilância vai além, atingindo patamares de diversidade e aplicabilidade inéditos há até pouco tempo (GILLIOM; MONAHAM, 2013). A questão é que, por mais que a vigilância envolva diversos aspectos que não a utilização de câmeras de vídeo, o emprego desses aparatos tecnológicos tem adquirido novas dimensões, especialmente devido ao surgimento de modernos sistemas de reconhecimento facial, como buscaremos demonstrar. Segundo Gilliam e Monaham, "as boas e velhas câmeras de vídeo ainda são amplamente utilizadas e permanecem um potente símbolo" da vigilância (p. 133, tradução nossa).

Há que se ter em mente que, simultaneamente ao desenvolvimento da ciência de dados e das tecnologias de IA, ocorreram mudanças paradigmáticas das noções de democracia e direitos fundamentais. Houve um aumento das funções estatais, culminando na transformação do próprio Estado, que passou a assumir demandas mais complexas e em maior número. Isso gerou uma tendência mundial de implementação de atividades e serviços públicos geridos por sistemas de IA, inclusive no que tange à vigilância, com destaque para as tecnologias reconhecimento facial (EGGERS, SCHATSKY e VIECHNICKI, 2017; MEHR, 2017), o que também contribui para a formação de uma "sociedade de vigilância".

Não há dúvidas, ressalve-se, de que a vigilância existe há muito tempo. Maneiras mais antigas, menos formais e menos técnicas de vigilância já ocorriam quando as pessoas se observavam dentro de famílias, pequenas cidades, escolas e instituições religiosas. A vigilância, inicialmente, não era institucionalizada. A questão é que novas formas de vigilância surgiram à medida que as instituições mudaram e se tornaram menos centrais diante de uma população crescente, agora urbanizada, globalizada e móvel. Com o início da era da informação e com a disseminação de instrumentos tecnológicos (computadores, telefones celulares, *wearables*[1], etc.) a preços acessíveis, a vigilância adquiriu uma dimensão altamente tecnológica, instalando-se no centro de muitos aspectos de nossas vidas (GILLIOM; MONAHAN, 2013).

Alguém poderia dizer que não se importa com a questão da vigilância e que, portanto, não enxerga propósito na discussão que se pretende realizar. O argumento que com maior frequência se apresenta é o clássico, famigerado "não tenho nada que esconder". Mas –

[1] O termo "*wearables*" pode ser traduzido livremente como "dispositivos vestíveis". Refere-se a itens tecnológicos como *smartwatches* (relógios inteligentes) e *smart glasses* (óculos inteligentes).

parafraseando Edward Snowden[2] – afirmar que você não se importa com a questão da vigilância pois não tem nada a esconder é a mesma coisa que afirmar que não se importa com o direito à liberdade de expressão pois não tem nada a dizer. A questão da vigilância deveria preocupar a todos. Principalmente porque, em uma sociedade de vigilância, os conceitos de "certo" e "errado" são tão abstratos que se tornam opacos, ininteligíveis.

Gilliom e Monaham (2013) argumentam que, na sociedade de vigilância, as definições de "errado" podem mudar, se adaptando a interesses distintos, como os de mercado e de governança. Podem incluir coisas como participar de manifestações políticas, ter problemas de saúde, perder o emprego, ser jovem demais, ser velho demais, ser homem ou ser mulher, ou pertencer a qualquer grupo étnico, racial ou religioso. Em resumo, existem tantas definições diferentes e conflitantes de "errado" que possivelmente estamos fazendo algo de errado todo o tempo. Isso se explica, em grande parte, "porque as instituições estão procurando diferentes tipos de erros" (GILLIOM; MONAHAN, 2013, p. 13, tradução nossa). Assim, atualmente, as diferentes concepções de errado vão além de fumar maconha ou furtar uma loja. Todo padrão que possa representar um risco – em aspectos econômicos, políticos, sociais – é considerado desviante, impróprio. Logo, "como cada um de nós apresenta algum tipo de risco para alguma instituição em algum momento de nossas vidas, todos estamos fazendo algo errado" (GILLIOM; MONAHAN, 2013, p. 13, tradução nossa).

Ao redor do globo, não faltam exemplos de como a vigilância tem se consolidado mediante a utilização de sistemas de reconhecimento facial baseados em IA para fins de segurança e controle. Na China, 200 milhões de câmeras compõem um sistema de vigilância capaz de identificar basicamente qualquer um dos 1.4 bilhões de habitantes do país[3]. Na capital dos Emirados Árabes Unidos, Dubai, um gigantesco "túnel-aquário", localizado no principal aeroporto da cidade, conta com mais de 80 câmeras de segurança, que escaneiam o rosto das pessoas à medida que caminham por ele; realizada a análise das imagens obtidas, o sistema de segurança ou permite que a pessoa ingresse livremente no país ou emite um alerta, indicando a necessidade de uma análise mais aprofundada acerca de sua liberação[4]. Já nos Estados Unidos

[2] "Ultimately, saying that you don't care about privacy because you have nothing to hide is no different from saying you don't care about freedom of speech because you have nothing to say" (SNOWDEN, 2019, p. 162).
[3] Disponível em: https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html. Acesso em: 23 set. 2019.
[4] Disponível em: https://www.theverge.com/2017/10/10/16451842/dubai-airport-face-recognition-virtual-aquarium. Acesso em: 23 set. 2019.

da América, no ano de 2016, ao menos 50% dos cidadãos adultos já constavam em bases de dados de reconhecimento facial do governo[5].

No Brasil, destaca-se o chamado RIO+SEGURO, "um programa pioneiro no Brasil que associa planejamento, inteligência e tecnologia na prevenção à desordem urbana e à criminalidade", conforme consta no sítio eletrônico do projeto[6]. A inteligência e tecnologia a que se referem a descrição do programa correspondem, na realidade, ao uso de *softwares* de reconhecimento facial baseados em IA, a fim de se identificar e, consequentemente, prender suspeitos e foragidos. No estado da Bahia, tem ganhado força um projeto semelhante. Intitulado "Vídeo Policiamento", o sistema emprega técnicas de inteligência artificial na análise de imagens obtidas mediante videomonitoramento, efetuadas em âmbito estadual. Segundo Rui Costa, governador do estado, o projeto "é uma ferramenta que fará o reconhecimento não só de criminosos, mas a meta é colocar todos os 15 milhões de baianos (sic)"[7]. Importante lembrar que na cidade de Salvador, em março de 2019, ocorreu a primeira prisão possibilitada pelo uso de uma tecnologia de reconhecimento facial[8].

Diante do contexto apresentando, é possível afirmar que vivemos em um "pan-óptico digital" (HAN, 2018a, 2018b), o que nos leva ao seguinte problema: o regime de proteção de dados pessoais no Brasil é suficiente para salvaguardar os direitos à privacidade e à proteção de dados no que se refere à utilização de tecnologias de reconhecimento facial? Objetivamos, de maneira geral, compreender de que maneiras as novas tecnologias de vigilância, nomeadamente as tecnologias de reconhecimento facial, afetam a privacidade e o direito à proteção de dados. De maneira mais específica, procuramos: analisar e entender o funcionamento de tais tecnologias; discutir a evolução do direito à privacidade na chamada "sociedade da vigilância"; analisar o surgimento do direito à proteção de dados; compreender a influência e as implicações que o recente avanço tecnológico exerce sobre esses direitos; e, por fim, debater se o aparato legal do qual dispomos atualmente – especialmente, a Lei Geral de Proteção de Dados (LGPD) – é suficiente para a garantia dos direitos à privacidade e à proteção de dados na conjuntura analisada.

---

[5] Disponível em: https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/. Acesso em: 23 set. 2019.
[6] Disponível em: http://maisseguro.rio. Acesso em: 23 set. 2019.
[7] Disponível em: http://www.casacivil.ba.gov.br/2018/12/1271/Lancado-sistema-de-videomonitoramento-inteligente-de-seguranca.html. Acesso em: 23 set. 2019.
[8] Disponível em: https://www.tecmundo.com.br/seguranca/139262-carnaval-tem-primeiro-preso-via-camera-reconhecimento-facial-brasil.htm. Acesso em: 23 set. 2019.

A hipótese levantada é que o uso de tecnologias de reconhecimento facial para fins de vigilância pode ocasionar graves violações ao direito à privacidade e ao direito à proteção de dados, e que as legislações existentes no Brasil que dispõem sobre a proteção de dados pessoais não regulam de maneira satisfatória tais direitos quando se trata do uso de sistemas de reconhecimento facial. Pretendemos responder à questão proposta a partir de um levantamento bibliográfico sobre o tema, bem como a partir da análise documental de diferentes legislações relacionadas à matéria. Nesse sentido, além da LGPD e demais instrumentos normativos brasileiros, pretendemos analisar o decreto (*ordinance)* n.º 107-19 da cidade de São Francisco, na Califórnia, aprovado em 14/06/2019 pelo Conselho de Supervisores da cidade, que proíbe o uso de sistemas de vigilância para fins de segurança na jurisdição do município.

1.2 Apontamentos metodológicos

Devido à natureza do tema abordado na presente pesquisa, é possível classificá-la, no que tange a seus objetivos, como uma pesquisa exploratória. Segundo Gil (2002), esse tipo de pesquisa objetiva proporcionar maior familiaridade com o problema, a fim de torná-lo mais explícito ou de construir hipóteses. Expõe o autor que

> Estas pesquisas têm como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a constituir hipóteses. Pode-se dizer que estas pesquisas têm como objetivo principal o aprimoramento de idéias (*sic*) ou a descoberta de intuições. Seu planejamento é, portanto, bastante flexível, de modo que possibilite a consideração dos mais variados aspectos relativos ao fato estudado. Na maioria dos casos, essas pesquisas envolvem: (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; e (c) análise de exemplos que "estimulem a compreensão" (GIL, 2002, p. 41).

A pesquisa bibliográfica foi feita a partir do levantamento de referências teóricas já analisadas e publicadas por meios escritos e eletrônicos, como livros, artigos científicos e páginas de sítios eletrônicos. Como aponta Fonseca (2002) a pesquisa científica pode basear-se fundamentalmente na pesquisa bibliográfica, “procurando referências teóricas publicadas com o objetivo de recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta” (FONSECA, 2002, p. 32). Diante da relativa novidade do tema aqui abordado, e da escassez de estudos e publicações e atinentes ao assunto, tanto em nível nacional quanto internacional, a pesquisa bibliográfica revela-se de grande importância para a concretização dos objetivos pretendidos.

Junto do levamento bibliográfico, será empregado o método de análise documental. Como nos aponta Cellard (2008), a técnica da análise documental é extremamente importante

para que deduções válidas sejam realizadas a partir de documentos selecionados. Conforme expõe o autor, o documento possibilita "acrescentar a dimensão do tempo à compreensão social" (2008, p. 295), sendo fonte valiosa nas ciências sociais por possibilitar reconstruções e por diminuir, ao menos em parte, a influência exercida pela presença ou intervenção do pesquisador. Ainda segundo o autor (2008, p. 296), o pesquisador enfrenta o desafio, na pesquisa documental, de avaliar a credibilidade e a representatividade dos documentos escolhidos.

Nesse sentido, revela-se imprescindível o estudo da Lei Geral de Proteção de Dados Pessoais (LGPD), por se tratar do principal documento normativo nacional no que diz respeito à proteção de dados pessoais. Apresentamos e discutimos, brevemente, os Projetos de Lei 9736/2018 e 4612/2019, que se relacionam diretamente com a matéria. Ainda, com vistas a se analisar a regulamentação de tecnologias de vigilância baseados em IA, elegemos a *ordinance* NO. 107-19, da cidade de São Francisco, no estado da Califórnia, nos Estados Unidos da América. Apesar de considerada por muitos como a capital global da tecnologia, lar do *Silicon Valley,* foi justamente na cidade de São Francisco onde se elaborou um dos primeiros instrumentos normativos, em âmbito mundial, a dispor sobre a proibição do uso de tais tecnologias. Destarte, por se tratarem instrumentos normativos – que são, afinal, documentos – lançamos mão da técnica de análise documental na presente pesquisa.

1.3 Organização da pesquisa

Neste capítulo introdutório, apresentamos o tema, problema e objetivos da pesquisa, bem como as estratégicas metodológicas que serão empregadas. Justificamos a escolha por uma pesquisa exploratória, devido à natureza do tema estudado, e discutimos os métodos a serem empregados, quais sejam, levantamento bibliográfico e análise documental. Ainda, apresentamos sucintamente as justificativas para a escolha da legislação brasileira (LGPD), dos Projetos de Lei 9736/2018 e 4612/2019 e da *ordinance* NO. 107-19 de São Francisco como instrumentos aptos a conduzir o debate que pretendemos realizar.

Buscamos, no segundo capítulo, traçar um breve panorama acerca do uso de tecnologias de reconhecimento facial, discutindo o seu desenvolvimento e formas de emprego, desde o surgimento dos chamados "circuitos fechados de televisão" até as tecnologias mais recentes,

que se valem de tecnologias de inteligência artificial e *big data*[9]. Realizamos ainda a problematização dessas tecnologias no que tange à própria limitação tecnológica e ao enviesamento dos algoritmos, que se manifesta, sobretudo, em resultados machistas e/ou racistas.

No capítulo 3, apresentamos as bases teóricas que serão adotadas no presente trabalho. São discutidas a ideia de "sociedade de vigilância", a partir da obra de Stefano Rodotà (2004; 2008), e o conceito de "pan-óptico digital", proposto pelo filósofo sul-coreano Byung Chul-Han (2018a; 2018b). Discutimos ainda a expansão da privacidade, também a partir da obra de Rodotà, conciliada com a teoria da privacidade de Daniel Solove (2008, 2011). Buscamos, com isso, demonstrar como a sociedade de vigilância se apresenta como um verdadeiro pan-óptico digital. Argumentamos ser necessária a releitura do conceito de privacidade, e tentamos expor de que maneira as tecnologias de reconhecimento facial impactam o direito à privacidade. Além disso, abordamos a importância de se enxergar o direito à proteção de dados enquanto um direito autônomo e central à discussão que realizamos aqui.

O capítulo 4, por sua vez, tem como objetivo debater os caminhos para a regulação das tecnologias de reconhecimento facial. Analisamos as justificativas frequentemente apresentadas para o seu uso, procurando enquadrar de maneira mais acertada o debate "segurança *vs.* privacidade/proteção de dados". Discorremos sobre estratégias de autorregulação e heterorregulação, e sobre como leis gerais de proteção de dados têm sido utilizadas para endereçar as questões atinentes ao tratamento de dados por sistemas de inteligência artificial. Discutimos a regulação por princípios, e como, no contexto brasileiro, a LGPD pode ser utilizada a fim de regular tecnologias de reconhecimento facial. Apresentamos e analisamos sucintamente dois projetos de lei em tramitação no Brasil sobre a matéria. Concluímos o capítulo expondo as orientações da Agência dos Direitos Fundamentais da União Europeia sobre tecnologias de reconhecimento facial, bem como as disposições da legislação municipal de São Francisco que decidiu pela proibição de tais tecnologias.

Finalmente, no capítulo 5, a discussão levantada ao longo do trabalho é retomada e resumidamente exposta, para que se apresentem as considerações finais.

---

[9] Apesar da importância do fenômeno, não há uma definição clara sobre seu significado (FLORIDI, 2012). Todavia, é possível perceber que o termo "*big data*" se refere a uma extensa variedade de fenômenos cujo foco é a análise de grandes bancos de dados (MITTELSTADT; FLORIDI, 2016).

2 TECNOLOGIAS DE RECONHECIMENTO FACIAL: O QUE, COMO, ONDE

"If you want to keep a secret, you must also hide it from yourself."

George Orwell

2.1 Um breve histórico das tecnologias de reconhecimento facial: das câmeras de videomonitoramento ao *big data*

Nas palavras de Stefano Rodotà, "o corpo humano está em contínua transformação" (2004, p. 91). Em meados do século passado, nosso corpo deixou de ser uma unidade e passou a ser decomposto em partes: órgãos, tecidos, células e gametas foram separados de sua matriz e colocados em circulação de maneira independente. E nas últimas décadas, com a consolidação da sociedade de informação e devido à contraposição do corpo físico ao corpo eletrônico, o corpo humano "conheceu a crise de sua materialidade" (RODOTÀ, 2004, p. 91). Essa contraposição tomou a centralidade dos debates acerca do corpo humano, até que a importância do corpo físico voltou à tona. Segundo o jurista italiano, "nos últimos tempos, reafirmou-se a importância do físico desde que os dados biométricos passaram a se revelar um instrumento indispensável para a definição e o reconhecimento da identidade pessoal" (RODOTÀ, 2004, p. 91).

Fato é que o crescimento populacional e sua respectiva consolidação nas áreas urbanas implica uma maior demanda pela atuação do Estado. Como consequência, a administração pública depara-se com uma série de desafios concernentes aos mais diversos setores, inclusive de vigilância e controle social. Marina Barros e Jamila Venturini, discutindo os desafios inerentes às chamadas "cidades inteligentes", apontam que "o uso das Tecnologias de Informação e Comunicação (TIC) e processamento de grandes volumes de dados tem se mostrado atrativo para gestores públicos, dado seu potencial de auxiliar no planejamento urbano" (BARROS; VENTURINI, 2018, p. 32).

Nessa mesma lógica, Rodotà discorre sobre como o avanço incontido da internet, com a crescente e intensa coleta de dados pessoais, somada à interconexão entre diversos bancos de dados que realizam o cruzamento de informações, faz surgir uma sociedade pautada pelo controle, pela vigilância e pela classificação. Para o autor, a sociedade da informação "ameaça sombrear o crescimento igualmente intenso dos bancos de dados mais tradicionais, aqueles com finalidade de segurança, que também são modificados pelas tecnologias e pela realidade de um

mundo sem fronteiras" (RODOTÀ, 2008, p. 146). Exemplos do emprego de tais tecnologias, como exposto anteriormente, são cada vez mais comuns, sendo, nas palavras do jurista italiano, "uma tendência que já parece irresistível, comum aos mais diversos países" (RODOTÀ, 2008, p. 147).

Como se pode observar, é interessante para os gestores públicos o uso de novas tecnologias alimentadas pelo *big data* devido ao potencial que tais tecnologias possuem de auxiliar no planejamento urbano. Esse uso ao mesmo tempo é impulsionado pelo setor privado, que busca expandir seus mercados através, por exemplo, da "Internet das coisas" (IoT, do inglês, *Internet of Things*). Nesse sentido, Caitlin Mulholland elucida que a IoT possibilita não apenas a comunicação e realização de funções específicas entre as coisas, como também gera "cada vez mais constante coleta, transmissão, guarda e compartilhamento de dados entre os objetos e, consequentemente, entre as empresas que disponibilizam este tipo de tecnologia às pessoas" (2018, p. 485, 486). Observe-se:

> É no âmbito da tecnologia conhecida como Internet das Coisas – ou *Internet of Things*, ou, ainda, IoT – que se desenvolve o argumento desta perspectiva, revelando um dos principais debates que se realiza neste âmbito e que se refere à proteção da privacidade ou dos dados pessoais que são disponibilizados e coletados por estas "coisas" conectadas. Em poucas palavras, a IoT representa inovação tecnológica que permite a criação de ambiente interligado através de sensores que conectam objetos ou bens por meio da internet possibilitando não só a comunicação e realização de funções específicas entre as coisas, como gerando a cada vez mais constante coleta, transmissão, guarda e compartilhamento de dados entre os objetos e, consequentemente, entre as empresas que disponibilizam este tipo de tecnologia às pessoas (2018, p. 485, 486).

Destaca-se, ainda, o atual entusiasmo no que diz respeito à pesquisa e desenvolvimento de tecnologias de inteligência artificial. Com início aproximadamente em 2010, este *boom* foi movido pelos seguintes fatores: criação de métodos estatísticos e probabilísticos cada vez mais sofisticados; a disponibilidade de ampla e crescente quantidade de dados; a acessibilidade a um enorme, e relativamente barato, poder computacional; e a transformação cada vez maior dos ambientes com as novas tecnologias de informação, como a automação residencial e a criação de cidades inteligentes (FLORIDI et al., 2017). Tais fatores, que se retroalimentam, possibilitaram o crescimento exponencial da criação e aperfeiçoamento de sistemas de IA nos últimos anos, não aparentando ser uma tendência passageira.

Conquanto inexista consenso na literatura especializada sobre o conceito de inteligência artificial, é possível afirmar, em linhas gerais, tratar-se da tentativa de reprodução

da cognição humana e seus mais variados componentes – como o aprendizado, a memória e o processo de tomada de decisões – mediante o uso de *softwares* computacionais. Não obstante, uma boa definição acerca do conceito de IA é aquela formulada por John McCarthy, considerado o "pai da inteligência artificial". Para o autor, constrói-se uma inteligência artificial (I.A) ao se fazer com que uma máquina se comporte de maneira que, caso se tratasse de um ser humano, fosse considerada inteligente (MCCARTHY, 2000).

Todo esse contexto permitiu o desenvolvimento ainda mais acelerado de tecnologias de reconhecimento facial, o que, como aponta Vu (2018), foi inicialmente resultado da incapacidade do cérebro humano de processar, memorizar e lembrar-se de milhares de faces com que se depara todos os dias. Contudo, com o aumento de viajantes internacionais ao redor do globo, e especialmente depois dos eventos do 11 de Setembro nos Estados Unidos da América, agências governamentais têm se utilizado de todos os meios para desenvolver maneiras eficientes e precisas de regular o afluxo de pessoas através da identificação dos indivíduos, a fim de garantir que nenhuma ameaça conhecida seja permitida, pois, argumenta-se, isso pode colocar em risco os cidadãos de uma sociedade (VU, 2018, p. 11-12; RODOTÀ, 2008).

O termo "tecnologia de reconhecimento facial" (comumente abreviado para FRT, do Inglês, "*facial recognition technology*") refere-se à habilidade que *softwares* de computador possuem de reconhecer e identificar rostos humanos específicos a partir de fotos ou vídeos. Utilizando-se de amplas bases de dados, e valendo-se de conexões de internet ultra velozes, as tecnologias de reconhecimento facial identificam e catalogam detalhes de cada indivíduo a fim de processar imagens obtidas em um computador, *smartphone* ou câmera de vigilância; os dados processados podem ser usados, então, para uma extensiva gama de propósitos (NABEEL, 2019).

Em linhas gerais, um sistema de reconhecimento facial opera mediante o uso de biometria para mapear características faciais de uma pessoa presente em uma fotografia ou vídeo, comparando as informações obtidas com um banco de dados de rostos conhecidos para encontrar uma correspondência. Embora as técnicas empregadas variem, os sistemas de reconhecimento facial geralmente operam a partir de etapas comuns, conforme expõe Weschler (2007). Primeiramente, uma imagem do rosto da pessoa é capturada a partir de uma foto ou vídeo; em seguida, o *software* de reconhecimento facial analisa a "geometria" do rosto, identificando fatores, como a distância entre os olhos e a distância da testa ao queixo. Assim,

elabora-se uma "assinatura facial" a partir da identificação dos pontos de referência faciais. Simplificadamente, isso se dá da seguinte forma:

Figura 1 - Ilustração da análise da biometria facial. Disponível em: https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html.

Em seguida, o terceiro passo consiste na comparação da assinatura facial – que nada mais é que uma fórmula matemática – a um banco de dados de rostos conhecidos, pré-coletados e armazenados. Finalmente, realiza-se a etapa de determinação, em que pode ocorrer a verificação (quando se analisa uma determinada assinatura digital em comparação a uma única outra, já definida) ou identificação (quando se compara determinada assinatura digital a diversas outras constantes do banco de dados) do rosto analisado.

Clive Norris (2003) argumenta que a introdução de sistemas de vigilância baseados em circuitos fechados de televisão (CFTV/CCTV)[10] desde o século passado alterou fundamentamente a natureza da *surveillance,* da vigilância ostensiva, tanto quantitativamente quanto qualitativamente. Para o autor, simplificadamente, com a introdução da tecnologia de circuitos fechados de televisão,

> o escopo da vigilância foi expandido para um nível inimaginável com base na co-presença; o escopo da vigilâncianão mais se restringe às limitações espaciais inerentes à vigilância presencial; o escopo da vigilância fica livre das restrições temporais da interação face-a-face e da presença humana; a

[10] *CCTV,* sigla em inglês para *closed-circuit television*. Em português, utiliza-se o termo "circuito fechado de televisão", ou "CFTV". Corresponde a um sistema de TV em que os sinais não são distribuídos de forma pública, mas monitorados, principalmente para fins de vigilância e segurança. Será adotado, no presente trabalho, o acrônimo em português, "CFTV".

> vigilância e a intervenção autoritária tornam-se funcionalmente separadas; o ato de vigilância se torna mais democrático: todos ficam igualmente sujeitos ao olhar de vigilância; o projeto disciplinar do *panopitcon* é expandido à medida que o controle social inclusivo é promovido sobre a exclusão (NORRIS, 2003, p. 253, tradução nossa)[11].

Norris reconhece ainda que a transição para uma sociedade digital resultou na intensificação da sociedade de vigilância. Tradicionalmente, os sistemas inteligentes de vigilância se valiam da tecnologia de reconhecimento facial apenas para fornecer uma confirmação visual de eventos. Agora, com sistemas digitais que possibilitam o reconhecimento de pessoas a partir de cruzamento de informações com enormes bancos de dados, a própria imagem de vídeo torna-se a fonte de informação.

Softwares de reconhecimento facial dotados de IA representam, portanto, um significativo avanço multificional em relação às informações geradas em um circuito fechado de televisão. Explica-se: uma vez que as imagens são dispostas em um banco de dados digital, e o processamento dessas imagens é realizado por meio de algoritmos, o potencial de conexão com bancos de dados já existentes é dramaticamente amplicado (NORRIS, 2003, p. 269), e "a ligação de informações extraídas de imagens de CFTV a informações relacionadas a identidade em bases de dados exponicialmente aumenta o seu "efeito pan-óptico" (NORRIS, 2003, p. 270, tradução nossa).

2.2 Atuais usos de tecnologias de reconhecimento facial

Na sociedade de informação, "o corpo torna-se um instrumento para recrudescer as medidas de segurança (...) através da invasão tentacular das tecnologias de controle da vida cotidiana" (RODOTÀ, 2004, p. 93). Essa invasão da vida cotidiana se dá, decerto, mediante o emprego de tecnologias de reconhecimento facial. A fim de situar os leitores do presente trabalho no que diz respeito à ubiquidade dessas tecnologias, serão expostos, de maneira mais ou menos detalhada, alguns exemplos atuais de sua utilização. Importante salientar, novamente, que as TRFs podem ser empregadas tanto para fins privados, comerciais, quanto para fins de segurança pública e vigilância, sendo que, por vezes, esses fins se confundem. Posto isso, os

[11] No original: "the surveillance gaze has been expanded to a level unimaginable on the basis of co-presence; the surveillance gaze becomes removed from spatial constraints implicit in face-to-face surveillance; the surveillance gaze becomes freed from the temporal constraints of face-to-face interaction and co-presence; surveillance and authoritative intervention become functionally separate; the act of surveillance becomes more democratic: all become equally subject to the surveillance gaze; the disciplinary project of the panopticon is expanded as inclusionary social control is promoted over exclusion (NORRIS, 2003, p. 253).

casos apresentados atenderão a um propósito ilustrativo, sem a preocupação de se distinguir entre os objetivos com que são utilizadas as tecnologias.

2.2.1 No Brasil

Por aqui, as tecnologias de reconhecimento facial vêm aos poucos ganhando espaço e adentrado diferentes âmbitos. A iniciativa privada, como se espera, tem investido em sistemas que permitam o reconhecimento de clientes. Hoje em dia, o dono ou gerente de uma loja pode não só saber quantas pessoas entraram em seu estabelecimento, mas também determinar qual seu sexo, idade e se compraram algo. Além disso, é possível, por meio das câmeras, identificar suas emoções. Assim, o empresário pode saber, por exemplo, se o preço praticado desagrada aos clientes ou entender o que eles pensam sobre determinado produto em uma degustação. Redes populares, como O Boticário[12] e Hering têm adotado as tecnologias, o que culminou, inclusive, em um processo judicial contra a marca de roupas devido à coleta e ao tratamento não autorizado de dados dos clientes[13].

Na área da educação, professores do Instituto Federal do Espírito Santo (Ifes) têm utilizado um aplicativo chamado *I Am Here* para substituir as tradicionais chamadas orais: basta que o professor abra o aplicativo e peça para os alunos olharem para a câmera de seu celular; ao tirar uma foto da turma, o *app* identifica a face dos alunos presentes e as compara com as imagens cadastradas no sistema do Instituto[14]. A Totvs, empresa brasileira de *softwares*, tem desenvolvido um programa capaz de informar aos pais, por meio de uma notificação no celular, o momento exato em que as câmeras da escola registraram seus filhos entrando na sala de aula[15].

Nem mesmo o sagrado escapa às inovações, uma vez que igrejas também têm adotado a tecnologia. A partir de câmeras panorâmicas de alta resolução, é possível identificar informações pessoais – como sexo e idade –, além da assiduidade dos fiéis nos cultos. A partir

---

[12] "Boticário vai ter ferramentas de reconhecimento facial". Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/11/epoca-negocios-artur-grynbaum-vamos-ter-ferramentas-de-reconhecimento-facial.html.

[13] Hering é processada por uso de reconhecimento facial sem consentimento. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/hering-e-processada-por-uso-de-reconhecimento-facial-sem-consentimento/89877.

[14] "Professores brasileiros realizam chamada por reconhecimento facial". Disponível em: https://olhardigital.com.br/noticia/professores-brasileiros-realizam-chamada-por-reconhecimento-facial/92046?fbclid=IwAR2oNQc_gDOdMPFYh7vE2j5n58qbCVYTfvvVqHPik3Gujg263dgLQT5QnMI

[15] "Áreas de comércio, serviço e transportes investem em identificação por imagem." Disponível em: https://www1.folha.uol.com.br/mercado/2018/04/areas-de-comercio-servico-e-transportes-investem-em-identificacao-por-imagem.shtml.

disso, são gerados relatórios para cada pessoa, incluindo estatísticas sobre seu comportamento. De acordo com Marcelo Scharan, CEO da Kuzzma, empresa estrangeira do ramo de IA que desenvolveu sistemas de reconhecimento facial para igrejas, o *software* permite determinar até mesmo se alguém precisa de uma visita pastoral[16].

Como se pode observar, as tecnologias de reconhecimento facial encontram aplicabilidade nas mais diversas esferas do cotidiano. Contudo, a área que será mais afetada por essas novas tecnologias, ao menos em um futuro próximo, é a de segurança pública. O Metrô da cidade de São Paulo, *e. g.*, publicou recentemente edital de licitação para implantação de sistemas de monitoração eletrônica por imagens de suas principais linhas[17]. A maior rede metroviária do Hemisfério Sul, com fluxo diário de mais de 3 milhões de passageiros, contará, em até 3 anos, com mais de 5.200 câmeras que realizarão o reconhecimento facial de passageiros, bem como identificação e rastreio de objetos[18].

Sobre o uso das tecnologias no metrô de São Paulo, interessante apontar que no final de 2018 a concessionária ViaQuatro, responsável por uma das linhas do sistema metroviário, foi alvo de processo judicial movido pelo Idec (Instituto Brasileiro de Defesa do Consumidor). A rede de câmeras de reconhecimento facial implementada pela empresa identificava o estado emocional e a reação das pessoas aos anúncios publicitários veiculados nos trens, definindo se elas se revelavam insatisfeitas, surpresas ou "neutras" com determinadas propagandas, além de coletarem dados como gênero e faixa etária dos passageiros – o que era feito sem o consentimento dos cidadãos[19].

Ainda na área de transportes, destaca-se o emprego de tecnologias de reconhecimento facial nos aeroportos do país. Com um avanço aparentemente mais veloz que nos demais aeroportos do mundo, já são 14 os aeroportos brasileiros que contam com módulos de

---

[16] "Empresas lançam serviço de reconhecimento facial para igrejas no Brasil". Disponível em: https://www.cartacapital.com.br/sociedade/empresas-lancam-servico-de-reconhecimento-facial-para-igrejas-no-brasil/?fbclid=IwAR2fOHTl84aZ6ZjBnWvbver0-UbLB_bhksR_WoHbFdBHhHtOw240tdYkaUI.

[17] "Metrô compra sistema de monitoramento eletrônico com reconhecimento facial". Disponível em: http://www.metro.sp.gov.br/noticias/28-06-2019-metro-compra-sistema-de-monitoramento-eletronico-com-reconhecimento-facial.fss

[18] "Metrô de SP terá vigilância com reconhecimento facial". Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/07/metro-de-sp-tera-vigilancia-com-reconhecimento-facial.shtml

[19] "Concessionária é alvo de processo por leitura facial no metrô de SP". Disponível em: https://www1.folha.uol.com.br/tec/2018/08/idec-pede-indenizacao-de-r-100-mi-a-empresa-que-identifica-emocoes-no-metro.shtml.

reconhecimento facial para facilitar o trabalho das autoridades aduaneiras na hora de identificar pessoas no momento de seu desembarque nos aeroportos do Brasil[20].

O debate sobre reconhecimento facial no país, todavia, veio à tona durante o carnaval de 2019: conforme exposto na introdução, em março do ano passado ocorreu, na cidade de Salvador, a primeira prisão do país realizada graças à identificação facial de um suspeito. Este, um homem de 19 anos, encontrava-se fantasiado de mulher em um dos mais populares circuitos carnavalescos da capital baiana quando fora flagrado por câmeras de reconhecimento facial instaladas pela Secretaria de Segurança Pública da Bahia (SSP-BA). Ainda durante o carnaval baiano, nos quatro dias da Micareta de Feira de Santana, o sistema de videomonitoramento, que capturou os rostos de mais de 1,3 milhões de pessoas, gerou 903 alertas. A partir dos alertas, foram identificados 18 foragidos, e, destes, 15 foram presos[21]. Em termos percentuais, portanto, considerando-se todos os alertas emitidos, menos de 2% foram de fato úteis à pretensa busca por segurança pública.

A despeito do baixo índice de retorno observado, interessante destacar que o governo estadual da Bahia investiu mais de R$ 18 milhões nos *softwares* de reconhecimento facial, com operação na capital e região metropolitana. Segundo o site institucional do governo,

> Com a nova tecnologia, os operadores policiais que atuam no COI [Centro de Operações e Inteligência de Segurança] passam a ter acesso, em tempo real e de maneira mais rápida, a um sistema que executa o reconhecimento facial de pessoas e de placas veiculares, e compartilha informações. A ferramenta também possibilita pesquisa e registro, permitindo traçar a trajetória de pessoas ou veículos, suspeitos ou não, bem como a análise situacional de um determinado período de gravação, encurtando pesquisas em vídeos muito longos (GOVERNO DO ESTADO DA BAHIA, 2018).

A prefeitura do Rio de Janeiro tem operado de maneira similar. Conforme exposto na introdução, o programa RIO+SEGURO surgiu com o intuito de combater delitos e identificar suspeitos por meio de reconhecimento facial, e monitorar o deslocamento de agentes – guardas municipais e policiais militares – com base em relatórios de inteligência artificial. Inicialmente, o programa operava apenas em dois bairros da Zona Sul da cidade, Copacabana e Leme. Em fase de expansão, o projeto vem sendo aplicado na Cidade Universitária e será instaurado na

[20] "Reconhecimento facial intensifica segurança nos aeroportos". Disponível em: http://intra.serpro.gov.br/tema/noticias-tema/reconhecimento-facial-intensifica-seguranca-nos-aeroportos.

[21] "Exclusivo: levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros". Disponível em: https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/.

Zona Oeste da cidade ainda no ano de 2020[22]. O governo do estado, por sua vez, planeja abrir licitação para a contratação de uma empresa responsável por criar um sistema reconhecimento facial com câmeras acopladas nos uniformes dos policiais militares. O objetivo é realizar a transmissão das imagens em tempo real para o CICC (Centro Integrado de Comando e Controle) da PM, onde será feita o cruzamento das imagens capturadas com aquelas presentes no banco de dados da Polícia Civil fluminense[23].

Nesse ponto, há que se mencionar que o sistema de reconhecimento facial adotado pela prefeitura do Rio de Janeiro falhou logo no segundo dia de uso. Em julho de 2019, uma mulher foi erroneamente detida e encaminhada à delegacia em Copacabana, depois que o sistema a "confundiu" com outra mulher, que já estava presa[24]. Evidenciam-se, assim, dois problemas do uso de tecnologias de reconhecimento facial, que serão melhor discutidos posteriormente: a falta de acurácia (precisão) e a falha na atualização dos bancos de dados dos sistemas de identificação (ao que tudo indica, o banco de dados da Polícia Civil não fora devidamente atualizado, o que levou à detenção de uma pessoa incorretamente identificada como outra, já presa).

Ainda em relação ao Brasil, apesar da ausência de dados oficiais, estima-se que, até o final de 2019, 151 pessoas haviam sido presas por meio do uso de tecnologias de reconhecimento facial no país[25]. O levantamento foi realizado pela Rede de Observatórios de Segurança, uma iniciativa de instituições acadêmicas e da sociedade civil de diferentes estados brasileiros, cujo objetivo é monitorar e difundir informações sobre segurança pública, violência e direitos humanos. O resultado do relatório aponta para outra questão concernente ao uso de tecnologias de reconhecimento facial na área de segurança pública: em relação aos casos em

---

[22] "Prefeitura anuncia expansão do programa Rio+Seguro para Jacarepaguá e Campo Grande." Disponível em: https://oglobo.globo.com/rio/prefeitura-anuncia-expansao-do-programa-rioseguro-para-jacarepagua-campo-grande-1-24168451.

[23] "Policiais do Rio vão testar câmera no uniforme para reconhecer criminosos". Disponível em: https://www.mobiletime.com.br/noticias/13/01/2020/policiais-do-rio-vao-testar-camera-no-uniforme-para-reconhecer-criminosos/

[24] "Em fase de testes, reconhecimento facial no Rio falha no 2º dia". Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/07/em-fase-de-testes-reconhecimento-facial-no-rio-falha-no-2o-dia.shtml.

[25] "151 pessoas são presas por reconhecimento facial no país; 90% são negras". Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/11/151-pessoas-sao-presas-por-reconhecimento-facial-no-pais-90-sao-negras.shtml?fbclid=IwAR2DZDMPKee642p3Ru7uUECj8qlMNUVk80_19uW0SqXyXQihxnLFwERqdqk.

que havia disponibilidade de informações sobre raça e cor das pessoas detidas, 90,5% dos abordados eram negros e 9,5% eram brancos (CESEC, 2019).

2.2.2 No mundo

A nível mundial, não faltam casos aptos a ilustrar como as tecnologias de reconhecimento facial têm sido empregadas. O já citado Aeroporto Internacional de Dubai, cuja capacidade excede os 90 milhões de passageiros por ano, utiliza o chamado *biometric boarding* ("embarque biométrico"), possibilitado mediante o reconhecimento facial dos passageiros no momento em que passam pelo portão de embarque – o que se dá, ao menos por enquanto, com prévia autorização[26]. *Por enquanto*, pois novas tecnologias, como o "túnel-aquário virtual", têm sido desenvolvidas, de modo a possibilitar a identificação biométrica por reconhecimento facial até mesmo sem o consentimento dos passageiros. Em outros países como, observa-se a mesma tendência, já adotada em importantes aeroportos: JFK, de Nova Iorque, e Heathrow, em Londres, são apenas alguns exemplos[27].

Indo na contramão da União Europeia, que planeja, ao menos temporariamente, banir as tecnologias de reconhecimento facial em locais públicos[28], em janeiro deste ano a cidade de Londres oficializou o uso de câmeras de reconhecimento facial em tempo real pelas ruas da cidade. Sob o pretexto de combate à criminalidade e aumento da segurança pública, a polícia londrina lançará mão de câmeras de vigilância para identificar pessoas consideradas "suspeitas", medida criticada por especialistas e juristas. De acordo com um levantamento realizado pela Universidade de Essex, 81% dos alertas feitos pelo sistema durante o período de teste estavam incorretos[29].

[26] "Where your data travels when you use biometric boarding at Dubai airport". Disponível em: https://wired.me/technology/privacy/emirates-facial-recognition/.
[27] "Facial recognition is coming to US airports, fast-tracked by Trump". Disponível em: https://www.theverge.com/2017/4/18/15332742/us-border-biometric-exit-facial-recognition-scanning-homeland-security.
[28] "EU considers temporary ban on facial recognition in public spaces". Disponível em: https://www.politico.eu/article/eu-considers-temporary-ban-on-facial-recognition-in-public-spaces/.
[29] "Londres terá câmeras de reconhecimento facial em tempo real". Disponível em: https://tecnoblog.net/322623/londres-cameras-reconhecimento-facial-tempo-real/.

Nos Estados Unidos da América, por sua vez, o FBI[30] e o ICE[31] têm utilizado livremente a base de dados do DMV[32], que contém a foto da carteira de motorista de milhões de cidadãos estadunidenses, para realizar a identificação facial de suspeitos. Tal uso tem ocorrido sem o prévio consentimento dos cidadãos e/ou autorização judicial ou legal, o gerou questionamentos por parte de Representantes do Congresso e de órgãos da sociedade civil[33].

Recentemente, também nos Estados Unidos, tem chamado a atenção a "parceria" estabelecida entre departamentos de polícia locais e a Amazon, gigante do setor tecnológico e varejista do país[34]. Até janeiro de 2019, haviam sido identificados 770 departamentos de polícia que se valiam das imagens captadas pela *Ring*, uma campainha eletrônica, desenvolvida pela Amazon, que funciona como uma espécie de câmera de segurança. Embora a campainha em si não disponha de tecnologia de reconhecimento facial, e embora não seja a própria Amazon a ceder as imagens obtidas, a empresa tem assistido a polícia a obter mais facilmente as gravações com os usuários do produto, fornecendo um canal direto entre os policiais e os proprietários da *Ring*[35].

Propositalmente deixados por último, os exemplos mais contundentes de emprego de tecnologias de reconhecimento facial na atualidade encontram-se na China. Se para a congressista estadunidense Alexandria Ocasio-Cortez o uso dessas tecnologias nos EUA já parece "coisa de *Black Mirror*"[36], a realidade chinesa pode ser considerada uma distopia ainda mais perturbadora do que aquelas imaginadas por roteiristas de ficção científica. Com uma

---

[30] Acrônimo de "Federal Bureau of Investigation", unidade de polícia do Departamento de Justiça dos Estados Unidos, que atua de maneira semelhante à Polícia Federal no Brasil.
[31] Acrônimo de Immigration and Customs Enforcement", livremente traduzido como "Departamento de Imigração e Alfândega".
[32] Acrônimo de *Department of Motor Vehicles*, ou "Departamento de Veículos Motorizados", em tradução livre.
[33] "FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches". Disponível em: https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/.
[34] "Here's where the US government is using facial recognition technology to surveil Americans". Disponível em: https://www.vox.com/recode/2019/7/18/20698307/facial-recognition-technology-us-government-fight-for-the-future.
[35] "How Amazon's Ring is creating a surveillance network with video doorbells". Disponível em: https://www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell-hacks.
[36] A deputada norte-americana faz alusão à série de ficção científica *Black Mirror*, produzida pela Netflix, ao discursar sobre o uso de tecnologias de reconhecimento facial nos Estados Unidos da América. A série é uma antologia de ficção científica que explora um futuro próximo, onde a natureza humana e as inovações tecnológicas encontram-se em intenso conflito. Disponível em: https://futurism.com/the-byte/aoc-warns-facial-recognition-real-life-black-mirror?utm_campaign=later-linkinbio-futurism&utm_content=later-4882971&utm_medium=social&utm_source=instagram.

população de aproximadamente 1 bilhão e 400 milhões de pessoas, quase todas identificadas em um gigantesco banco de dados biométricos, o plano do governo chinês é criar um sistema de reconhecimento facial capaz de identificar seus cidadãos em menos de 3 segundos, apresentando uma taxa de acurácia de 90%, o que já tem sido utilizado em diversas cidades chinesas[37].

De maneira semelhante ao que se observa no Brasil, a China tem aplicado as novas tecnologias à área da educação. Algumas escolas do país têm adotado sistemas de reconhecimento facial para determinar se os alunos, em sua maioria no ensino fundamental, estão prestando atenção nas aulas e se estão gostando da atuação dos professores[38]. Além disso, diversas universidades hoje utilizam sistemas de reconhecimento facial para permitir o ingresso de alunos e funcionários nos seus *campi*.

Em Pequim, segunda cidade mais populosa da do país asiático, foi inaugurado, em setembro de 2019, o maior aeroporto do mundo, *Beijing Daxing International Airport*, cuja capacidade de operação estimada é de mais de 100 milhões de passageiros por ano. Enquanto no antigo aeroporto da cidade tecnologias de reconhecimento facial têm sido testadas de maneira limitada, o novo terminal conta com um sistema de reconhecimento facial que opera desde as catracas na estação do trem que leva ao aeroporto até os caixas do *duty-free*, que passam a dispensar a apresentação do passaporte para a validação de compras de produtos sem impostos nas lojas do aeroporto[39].

Com o intuito de intensificar a vigilância sobre a população e dirimir os métodos para os cidadãos se manterem anônimos na internet, uma nova resolução do governo chinês foi implantada para a aquisição de *chips* de telefones celulares. Desde o final de 2019, a obtenção de um novo número está condicionada à verificação biométrica facial do consumidor, cabendo às empresas de telefonia tirar a foto de seu cliente no momento da compra, para que seja

[37] "Drones, facial recognition and a social credit system: 10 ways China watches its citizens". Disponível em: https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china.
[38] "Pay attention at the back: Chinese school installs facial recognition cameras to keep an eye on pupils". Disponível em: https://www.scmp.com/news/china/society/article/2146387/pay-attention-back-chinese-school-installs-facial-recognition.
[39] "Facial Recognition Is Everywhere at China's New Mega Airport". Disponível em: https://www.bloomberg.com/news/articles/2019-12-11/face-recognition-tech-is-everywhere-at-china-s-new-mega-airport.

posteriormente comparada àquela presente na base de dados oficial do governo[40]. No mesmo sentido, a polícia de Cantão recentemente lançou um aplicativo para *smartphones* denominado "Zhen Ni"[41], cujo objetivo é permitir que as pessoas requeiram a verificação biométrica facial de seus contatos em determinados contextos, mediante uma conexão ponta-a-ponta, uma novidade dentro das tecnologias de reconhecimento facial[42].

Cabe destacar que o aplicativo *Zhen Ni* funciona como uma ferramenta complementar a outro aplicativo amplamente difundido em território chinês, o *WeChat*, um serviço multiplataforma de mensagens instantâneas[43], utilizado por 83% de todos os usuários de *smartphones* no país e por 92% dos usuários habitantes das grandes cidades. Apesar de extremamente popular, o *app* de mensagens parece[44] não se preocupar com a privacidade de seus usuários: diferentemente de aplicativos como *WhatsApp* e *Telegram*, o *WeChat* não dispõe de criptografia ponta-a-ponta[45], o que significa que *hackers* e até mesmo o governo possuem um acesso relativamente facilitado ao conteúdo das conversas entre usuários[46].

Além das câmeras "tradicionais", estimadas em mais de 200 milhões espalhadas pelo território do país, *drones* em formato de pombas, projetados para imitar com precisão o movimento dos animais de verdade, têm sido utilizados para fins de monitoramento e vigilância. Dotados de câmeras, *GPS*[47], sistema de controle de voo e antenas para comunicação

---

[40] "China introduces facial recognition for WeChat transfers, mandatory biometric scans for SIM cards." Disponível em: https://www.biometricupdate.com/201912/china-introduces-facial-recognition-for-wechat-transfers-mandatory-biometric-scans-for-sim-cards.

[41] Em Inglês, o aplicativo é chamado "The Real You". Em tradução livre para o português, "Você Mesmo", ou "Você de Verdade".

[42] "A new Chinese app allows people to use facial verification on their friends and acquaintances". Disponível em: https://qz.com/1759284/a-new-chinese-police-app-allows-peer-to-peer-facial-scans/.

[43] O aplicativo *WeChat* foi desenvolvido pela Tencent na China, no ano de 2011. A Tencent é o maior e mais utilizado portal de serviços de internet do país, que, por sua vez, pertence à Naspers, um conglomerado de mídia com sede na África do Sul, cujas principais operações envolvem meios eletrônicos e mídias impressas.

[44] Cabe, aqui, uma explicação à ironia presente no texto: o governo chinês não autoriza a utilização de aplicativos de mensagens com criptografia. A solução encontrada por aqueles que buscam privacidade *on-line* é lançar mão de ferramentas próprias para criptografia, como o *app "LeakZero"*. Sobre o tema: "The one app in China making secure messaging possible". Disponível em: https://www.abacusnews.com/digital-life/one-app-china-making-secure-messaging-possible/article/3026055.

[45] Resumidamente, a criptografia de ponta-a-ponta é um recurso de segurança cujo objetivo é proteger dados de usuários durante uma troca de mensagens, de forma que o conteúdo da conversa só possa ser acessado pelos dois extremos da comunicação: o remetente e o(s) destinatário(s).

[46] "Outside of China, WeChat is a fish out of water". Disponível em: https://www.techinasia.com/outside-china-wechat-is-a-fish-out-of-water.

[47] Do inglês, "*global positioning system"*. Em português, sistema de posicionamento global. O termo refere-se a um sistema de navegação por satélite que fornece a um aparelho receptor móvel a sua

via satélite, os pássaros-robôs são utilizados por mais de 30 agências militares e governamentais em cinco diferentes províncias, especialmente nas regiões que fazem fronteira com outros países[48]. Ainda no contexto de uso de tecnologias de inteligência artificial para fins militares, a China tem produzido e vendido "drones assassinos", veículos aéreos autônomos e não tripulados, equipados com metralhadoras e capazes de levar a cabo ataques a alvos específicos[49]. Embora não disponham – ao menos, até o momento – de sensores de reconhecimento facial para identificação de alvos, bastaria um simples *upgrade* dos robôs para integrar a função.

Por fim, é imprescindível mencionar os "*Social Credit Scores"*, termo que poderia ser traduzido como "sistemas de crédito social". Tal qual o próprio nome indica, tratam-se de sistemas de avaliação de crédito, que se diferenciam essencialmente daqueles existentes em países ocidentais pelo fato de se basearem não somente em informações financeiras, mas também comportamentais. Resumidamente, os *social credit scores* operam mediante parcerias entre o governo e empresas privadas, que coletam e analisam diversos dados dos cidadãos: desde as finanças e históricos de crédito de uma pessoa, passando por suas atividades em redes sociais, registros de compras *on-line*, dados referentes a saúde, análises sobre o pagamento de impostos e cumprimento de obrigações legais e, inclusive, sua rede de amizades e relacionamentos. Tudo isso somado ao sofisticado mecanismo de reconhecimento facial utilizado pelo governo. Assim, ações que seriam consideradas corriqueiras e até mesmo "normais" em diversos locais do mundo, como atravessar fora da faixa de pedestres, passear com seu cachorro sem o uso de coleira ou jogar lixo no chão – essa, espera-se, não tão normal assim – implicariam a perda de pontos nos sistemas de crédito, o que pode resultar em prejuízos graves para o indivíduo que for identificado, por meio do sistema de câmeras, cometendo tais infrações[50].

---

posição, assim como o horário, sob quaisquer condições atmosféricas, a qualquer momento e em qualquer lugar na Terra, desde que o receptor se encontre no campo de visão de um determinado número de satélites.

[48] "China takes surveillance to new heights with flock of robotic Doves, but do they come in peace?". Disponível em: https://www.scmp.com/news/china/society/article/2152027/china-takes-surveillance-new-heights-flock-robotic-doves-do-they.

[49] "China is selling autonomous killer drones to the middle east. Disponível em: https://futurism.com/the-byte/china-selling-autonomous-killer-drones.

[50] "Chinese Social Credit Score: Utopian Big Data Bliss Or Black Mirror On Steroids?". Disponível em: https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#1d04a6f148b8.

De maneira geral, os sistemas de crédito chineses – que não se diferenciam substancialmente de scores já adotados em demais países, como o FICO nos Estados Unidos[51] e o Serasa Score no Brasil[52,53] – possuem elevada aprovação entre os chineses[54]. Contudo, uma base de dados específica, mantida pela Corte Suprema Popular chinesa, tem chamado a atenção e despertado preocupação entre juristas e demais cidadãos. O tribunal possui uma *watchlist*[55] com a identificação de cidadãos que o governo alega não terem cumprido com decisões judiciais, como pagar uma multa, ou até mesmo que não tenham "pedido desculpas" consideradas sinceras por determinado juiz. Não bastassem as punições imediatamente decorrentes de se estar na lista, como a vedação à compra de passagens de avião ou a proibição de matricular os filhos em escolas particulares, a conjugação da referida base de dados com as exponenciais ferramentas de reconhecimento facial tem gerado situações dignas de distopias literárias: quando uma pessoa na lista se desloca para certos lugares em Pequim, seu rosto e número de identificação são projetados em enormes *outdoors* eletrônicos, a fim de alertar os demais cidadãos que ali se encontram sobre a presença daquele indivíduo[56].

"Ao menos o Brasil está muito longe de se tornar uma ditadura orwelliana como a China", pensaria alguém mais desavisado. A realidade, porém, aponta o contrário. No início de 2019, senadores e deputados federais do Partido Social Liberal (PSL) estiveram na China, a convite do Partido Comunista de Pequim, com o intuito de conhecer e importar as tecnologias de reconhecimento facial utilizadas no país[57]. Rafael Zanatta (2019a) esclarece que a visita é

---

[51] "How the West Got China's Social Credit System Wrong". Disponível em: https://www.wired.com/story/china-social-credit-score-system/.

[52] Sobre o tema, ver: "O que é o score de crédito?". Disponível em: https://www.serasaconsumidor.com.br/ensina/aumentar-score/o-que-e-score-de-credito/

[53] Sobre *profiling* (perfilização) no Brasil, recomenda-se a leitura: ZANATTA, R. *Perfilização, Discriminação e Direitos*: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.researchgate.net/publication/331287708_Perfilizacao_Discriminacao_e_Direitos_do_Codigo_de_Defesa_do_Consumidor_a_Lei_Geral_de_Protecao_de_Dados_Pessoais.

[54] Em pesquisa recente, 80% dos entrevistados aprovam total ou parcialmente os sistemas de crédito social, 19% nem desaprovam nem aprovam os sitemas de crédito, enquanto apenas 1% relatou desaprovação forte ou moderada. Sobre o tema: "China's social credit systems are highly popular – for now". Disponível em: https://www.merics.org/en/blog/chinas-social-credit-systems-are-highly-popular-now.

[55] O termo frequentemente utilizado é *blacklist* (traduzido como *lista negra*), o qual preferimos substituir por *watchlist*, que pode ser traduzido como *lista de vigilância*.

[56] "How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens". Disponível em: https://time.com/collection/davos-2019/5502592/china-social-credit-score/.

[57] Bancada do PSL vai à China conhecer sistema que reconhece rosto de cidadãos. Disponível em: https://www1.folha.uol.com.br/mercado/2019/01/bancada-do-psl-vai-a-china-importar-sistema-que-reconhece-rosto-de-cidadaos.shtml.

resultado de um alinhamento estratégico entre interesses chineses e brasileiros: de um lado, “o racional ‘tecno-solucionista’” dos parlamentares brasileiros eleitos, que buscam uma resposta para o problema da segurança pública no Brasil, e, de outro, o interesse da potência asiática em exportar as tecnologias que tem desenvolvido e empregado, além de dominar o mercado de inteligência artificial no âmbito da “governança social”.

O “passeio” da comitiva, composta por 12 parlamentares, partiu de uma iniciativa de um grupo do próprio partido. O principal resultado da aproximação com a China foi a apresentação do Projeto de Lei (PL) n.º 4.612 de 2019. De autoria do deputado Bibo Nunes (PSL/RS), o PL “dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos” (BRASIL, 2019). Cumpre destacar, todavia, que a iniciativa legislativa sobre a matéria não é inédita no país: o PL n.º 9.736, de 2018, apresenta “por objetivo tornar obrigatória a identificação biométrica de custodiados pelo Estado pelo método do reconhecimento facial” (BRASIL, 2018b). As propostas de regulamentação do uso de tecnologias de reconhecimento facial no Brasil serão abordadas de maneira mais aprofundada posteriormente, no capítulo 5 do presente trabalho.

2.3 Questões atinentes às tecnologias de reconhecimento facial

Nas palavras de Rafael Zanatta (2019a), “é evidente que essas tecnologias [de reconhecimento facial] geram problemas de privacidade e lesionam direitos que julgamos ser fundamentais”, culminando, por vezes, em choques com “os valores mais básicos que estruturam um Estado Democrático de Direito”. Para Woodrow Hartzog e Evan Sellinger (2018), o reconhecimento facial é a ferramenta perfeita para a opressão, pois, além de ferir o direito à privacidade, também permite que uma série de outros abusos e atividades “corrosivas” ocorram, tais como a perseguição a “pessoas de cor” e grupos étnicos, o aumento do assédio, a constante e ostensiva coação policial e a perpetuação do capitalismo de vigilância.

Os potenciais efeitos lesivos das tecnologias de reconhecimento facial se estendem, gerando, inclusive, ameaças à própria noção de democracia. Imagine-se, por exemplo, que determinado governo utilize técnicas de reconhecimento facial para identificar manifestantes em um protesto e enquadra-los como “terroristas”, com base em discutíveis leis de segurança, o que culminaria em extensivos danos ao direito à liberdade de reunião, de associação e de

expressão. Ou, então, imagine-se que, em tempos de *fake news*[58], as *deepfakes*[59] sejam utilizadas com o fim de produzir falsas (mas facilmente críveis) informações sobre determinado candidato. Alimentadas por dados biométricos faciais, as *deepfakes* vêm despertando a preocupação de especialistas em todo o mundo[60,61], colocando em xeque até mesmo a máxima popular do "só acredito vendo". Ainda que sedutores, os debates sobre a relação entre tecnologias de reconhecimento facial e participação política e sobre *deepfakes* serão travados em momento oportuno, cabendo, nesta dissertação, apenas as breves menções realizadas. Será dada maior atenção aos problemas diretamente relacionados ao uso de reconhecimento facial para fins de segurança pública e vigilância, nosso objeto de análise.

Neste ponto, cabe notar que pesquisas recentes destacaram a enorme falta de diversidade no setor da ciência da computação. Descataram-se também as grandes diferenças demográficas entre as populações que se beneficiam e lucram com a eficiência da inteligência artificial e aquelas populações que suportam o custo dos vieses e da exploração da IA (CRAWFORD et al., 2019). A indústria da tecnologia, dentro da qual se encontra a ciência da computação, responsável pelo desenvolvimento de tecnologias como IA e reconhecimento facial, é majoritariamente liderada por homens brancos e de alto poder aquisitivo (WEST; WHITTAKER; CRAWFORD, 2019). O resultado da ausência de diversidade são tecnologias frequentemente enviesadas, prejudiciais a mulheres, pessoas negras e minorias étnicas.

---

[58] Termo em inglês para "notícias falsas", ocasionalmente publicadas por veículos de comunicação ou compartilhadas em mídias sociais, como se fossem informações reais.

[59] *Deepfake* é a siglonimização dos termos "*deep learning*" (aprendizado profundo, um ramo do aprendizado de máquina) e "*fake*"(falso). Trata-se, grosso modo, de uma técnica de síntese de imagens ou sons humanos realizada por meio de inteligência artificial. As *deepfakes* e as tecnologias de reconhecimento facial se relacionam da seguinte maneira: *deepfakes* funcionam a partir de redes neurais que analisam grandes conjuntos de amostras de dados para aprender a imitar as expressões faciais, maneirismos, voz e inflexões de uma pessoa. Esse processo envolve inserir imagens de duas pessoas em um algoritmo de aprendizado profundo para treiná-lo para trocar os seus rostos. Em outras palavras, as *deepfakes* usam tecnologias de mapeamento facial e algoritmos de inteligência artificial para trocar o rosto de uma pessoa pelo de outra, em um vídeo ou imagem (WESTERLUND, 2019).

[60] "The Best (And Scariest) Examples Of AI-Enabled Deepfakes". Disponível em: https://www.forbes.com/sites/bernardmarr/2019/07/22/the-best-and-scariest-examples-of-ai-enabled-deepfakes/?fbclid=IwAR2s0NplLXqtxLTyIB1zXdesqabyEh2sTryVQXYHkNOnMli0WDmbUdytwno#581402022eaf.

[61] "There Are Now 15,000 Deepfake Videos on Social Media. Yes, You Should Worry". https://www.forbes.com/sites/johnbbrandon/2019/10/08/there-are-now-15000-deepfake-videos-on-social-media-yes-you-should-worry/?fbclid=IwAR0DepPtIJu4z4hZfTLQqEMNYRsqqmrt2BEWX5Bw71Sz439xvp_F-Sxma0M#2b4400493750

2.3.1 A falta de precisão

Antes de se aprofundar a discussão sobre vieses na inteligência artificial e nas ferramentas de reconhecimento facial, há que se discutir um problema de ordem "técnica": a falta de precisão, ou acurácia, dessas tecnologias. Tomemos o exemplo do *software* "Rekognition", da Amazon. Segundo a empresa,

> com o Amazon Rekognition, você pode identificar objetos, pessoas, texto, cenas e atividades em imagens e vídeos, além de detectar qualquer conteúdo inapropriado. O Amazon Rekognition também fornece recursos de análise facial e pesquisa facial altamente precisos que você pode usar para detectar, analisar e comparar rostos para uma ampla variedade de casos de uso de verificação de usuários, contagem de pessoas e segurança pública (AMAZON WEB SERVICES, 2020).

Na prática, contudo, os resultados apresentados não se revelam "altamente precisos", como consta na descrição do produto. Em um teste conduzido pela União Americana pelas Liberdades Civis (ACLU, no acrônimo em inglês), a tecnologia de reconhecimento facial da Amazon identificou incorretamente o rosto de 28 membros do Congresso estadunidense[62], "confundindo-os" com outras pessoas que já haviam sido presas.

À primeira vista, a taxa de erro do *software*, que é de aproximadamente 5%, não parece tão significante. Entretanto, se somada a outros fatores, como o racismo estrutural e institucional presente em diversas sociedades, os resultados decorrentes das falhas da tecnologia podem culminar em irreparáveis prejuízos, uma vez que a identificação incorreta de uma pessoa pode custar a sua liberdade ou até mesmo a sua vida. Um incidente na cidade de São Francisco, nos EUA, fornece uma ilustração perturbadora desse risco: a polícia parou um carro e algemou sua ocupante, uma mulher negra, já idosa, forçando-a a ajoelhar-se com uma arma apontada para seu rosto. Tudo isso porque um leitor automático de placas identificou indevidamente seu carro como um veículo roubado (SNOW, 2018). Ressalve-se que, embora no incidente descrito a polícia de São Francisco não estivesse fazendo o uso do *Rekognition*, a ferramenta tem sido utilizada pela polícia do estado de Oregon, e, até o ano de 2018, também era empregada no estado da Flórida[63].

---

[62] "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots". Disponível em: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[63] "Orlando police once again ditch Amazon's facial recognition software". Disponível em: https://www.theverge.com/2019/7/18/20700072/amazon-rekognition-pilot-program-orlando-florida-law-enforcement-ended.

No Reino Unido, por sua vez, os sistemas de reconhecimento facial oficiais do governo empregados em aeroportos têm sido alvos de críticas por estarem incorretamente identificando passageiros como criminosos foragidos. Frequentemente, os viajantes têm suas viagens atrasadas, sendo, inclusive, detidos sem observância de elementos ínsitos ao devido processo legal[64]. Em um estudo realizado pela Universidade de Essex[65], constatou-se que a tecnologia utilizada pela polícia metropolitana de Londres, que consiste no processamento em tempo real de dados biométricos para verificação facial, possui uma taxa de acertos que gira em torno de meros 19%: de 42 pessoas identificadas como "suspeitas" pelo sistema, apenas 8 de fato correspondiam àquelas presentes no banco de dados do governo.

De igual modo, é necessário ter em mente que as tecnologias de reconhecimento facial estão sujeitas a fraudes, o que compromete sua segurança e, consequentemente, sua confiabilidade. Isso porque, mesmo hoje, as tecnologias de reconhecimento facial não são tão "fortes". A título exemplificativo, a organização holandesa *Consumentenbond* testou o sistema de reconhecimento facial de 110 *smartphones* atualmente disponíveis no mercado. Como resultado, descobriu que 42 dos dispositivos – de marcas renomadas, como Samsung, Lenovo/Motorola e BlackBerry – poderiam ser desbloqueados mediante a mera utilização de uma foto do usuário[66]. E mesmo sistemas mais sofisticados, como o *TrueDepth*[67], adotado pela Apple, podem ser fraudados, ainda que com mais trabalho: uma impressão 3D bem-feita, em tese, poderia permitir que alguém burlasse o item de segurança. Por enquanto, resta-nos especular, mas tudo indica que a mente humana, muito provavelmente, irá encontrar novas formas de ludibriar os sistemas de reconhecimento facial.

Por fim, além dos casos em que a falta de acurácia das tecnologias de reconhecimento facial é mais explícita, outras situações, não tão óbvias, revelam-se dignas de atenção. *Exempli gratia,* os softwares disponíveis atualmente são capazes de diferenciar gêmeos idênticos? A resposta é sim, e não. Pesquisadores da Universidade de Virgínia Ocidental, nos EUA, construíram bancos de dados compostos por imagens de gêmeos idênticos para fins de pesquisa

---

[64] "Border control systems face fire from travellers wrongly delayed". Disponível em: https://www.theguardian.com/politics/2019/sep/07/border-control-systems-face-fire-from-travellers-wrongly-delayed.

[65] O estudo completo está disponível no link: http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf.

[66] "The Flaws and Dangers of Facial Recognition". Disponível em: https://securitytoday.com/articles/2019/03/01/the-flaws-and-dangers-of-facial-recognition.aspx.

[67] Diferentemente de sistemas mais comumente adotados em *smartphones*, que operam mediante a comparação de fotos, o *Face ID* da Apple utiliza imagens infravermelhas, mais precisas, para realizar o reconhecimento facial do usuário.

de reconhecimento facial[68]. Os algoritmos utilizados são capazes de, a partir do reconhecimento dos elementos faciais, criar um modelo da imagem e criptografar os dados biométricos nela contidos. Utilizando-se imagens de alta definição, é possível apontar mínimas diferenças entre gêmeos "idênticos" e realizar, assim, a diferenciação. No entanto, embora seja viável realizar a comparação da imagem de um gêmeo idêntico com um pequeno banco de dados de imagens, à medida que o banco de dados aumenta, o desempenho – isto é, a capacidade de identificação – do algoritmo se deteriora, pois há uma chance maior de que outras imagens faciais apresentem características semelhantes, dificultando a diferenciação.

Em testes práticos, ainda que não necessariamente científicos, a resposta ao questionamento acima se repetiu. O "*Windows Hello*", ferramenta de reconheciento facial do sistema operacional Windows 10, da Microsoft, foi capaz de realizar a identificação correta de gêmeos idênticos[69]. Já o *FaceId* da Apple, ao ser submetido a testes com gêmeos idênticos não apresentou resultados satisfatórios, evidenciando falhas no *software* de identificação facial[70]. Logo, embora frequentemente confiemos em sistemas de IA porque os consideramos mais seguros e precisos (POLLI, 2017), é imprescindível ter em mente que as inovações tecnológicas não são tão confiáveis quanto gostaríamos que fossem. Isso se dá por diferentes motivos, dentre eles a existência de vieses, tema que será abordado a seguir.

2.3.2 Enviesamento

Realizando-se um breve recuo, é possível constatar que a discussão sobre novas tecnologias e enviesamento tiveram origem há algumas décadas. Ainda em 1999, Clive Norris e Gary Armstrong realizaram um estudo sobre a operação de diferentes centros de circuitos fechados de televisão na Inglaterra. Os autores demonstram que a vigilância realizada por imagens é direcionada e está sujeita a variáveis sociológicas, como classe, idade, raça e gênero. No estudo, constatou-se que: 9 em cada 10 alvos de vigilância eram homens; que 4 em cada 10 eram adolescentes; e que 3 em cada 10 eram negros, o que não correspondia, proporcionalmente, à população negra das localidades analisadas. Em geral, os homens tinham quase duas vezes mais chances de serem alvos de vigilância do que sua presença na população

[68] "Distinguishing Identical Twins". Disponível em: https://cacm.acm.org/news/226789-distinguishing-identical-twins/fulltext.
[69] "Can facial recognition software differentiate between identical twins?". Disponível em: *https*://www.sciencefocus.com/future-technology/can-facial-recognition-software-differentiate-between-identical-twins/
[70] "Is the iPhone X's Facial Recognition Twin Compatible?". Disponível em: https://www.youtube.com/watch?v=e8-yupM-6Oc.

sugeriria; da mesma forma, os adolescentes, responsáveis por menos de 20% da população, representavam 40% das fiscalizações direcionadas. Além disso, Norris e Armstrong calcularam que a chance de pessoas negras serem alvo de vigilância era de 150% a 250% maior do que a chance de pessoas brancas, quando considerada a sua proporção em termos populacionais (NORRIS, 2003, p. 265; NORRIS; ARMSTRONG, 1999, p. 267).

Para John Gilliom e Torin Monahan (2013), sistemas de segurança podem conter e reproduzir preconceitos, ainda que não se manifestem tão claramente. Os autores apontam que, nos dias de hoje, os sistemas de segurança são cada vez mais eletrônicos e automatizados. Nossos dispositivos e aparelhos tecnológicos – desde programas antivírus até câmeras de reconhecimento facial – são empregados para identificar ameaças, e, a partir disso, proteger pessoas e propriedades. Embora, apontem, "isso não seja necessariamente uma coisa ruim, significa que as pessoas estão confiando bastante nas tecnologias para trabalhar, geralmente sem muita evidência" (GILLIOM; MONAHAN, 2013, p. 125, tradução nossa)[71]. Além disso, os sistemas automatizados "obscurecem as exclusões sociais inerentes à segurança, o que pode fazer com que os preconceitos pareçam naturais ou inexistentes, a menos que você seja a pessoa a ser discriminada" (GILLIOM; MONAHAN, 2013, p. 125, tradução nossa)[72].

Hoje, poder-se-ia argumentar que as novas tecnologias de reconhecimento facial, devido aos sistemas de inteligência artificial que empregam, eliminam a discricionariedade e os preconceitos humanos. Isso porque, ao lançarem mão de algoritmos, as pessoas esperam que o uso da tecnologia em substituição à atividade humana resulte em menos vieses inconscientes. Todavia, essa mentalidade geralmente decorre de um caso de *"mathwashing"*[73]*,* que nada mais é que a nossa tendência de atribuir objetividade à tecnologia (POLLI, 2017). Feliz e necessariamente, discussões sobre enviesamento nas novas tecnologias têm se tornado cada vez mais comuns. *Biased algorithms* – algoritmos enviesados – recentemente tornaram-se alvo de interesse e debate, fazendo emergir a importância de se discutir como erros e preconceitos humanos são incorporados às inovações tecnológicas (UNIVERSITY OF BATH, 2018).

---

[71] No original: "Although that's not necessarily a bad thing, it does mean people are placing a lot of faith in technologies to work, often without much evidence" (GILLIOM; MONAHAN, 2013, p. 125, grifo dos autores).

[72] No original: "Additionally, automated (or partially automated) systems obscure the social exclusions inherent in security, which can make biases seem natural or nonexistent unless you're the one being discriminated against" (GILLIOM; MONAHAN, 2013, p. 125).

[73] Termo em inglês que pode ser traduzido como "lavagem matemática". É uma alusão ao termo "*brainwashing*", que por sua vez se traduz como "lavagem cerebral".

A importância de discutir os *built-in biases* – "vieses embutidos" – dos sistemas de segurança (e dos sistemas de inteligência artificial de maneira geral) decorre do fato de esses sistemas serem frequentemente apontados como alternativas neutras, imparciais, em detrimento do julgamento humano (GILLIOM; MONAHAN, 2013, p. 126). Contudo, segundo John Kelleher e Brendan Tierney (2018), os algoritmos atuam de uma maneira mais amoral do que propriamente objetiva. Desse modo, quanto mais arraigado for determinado preconceito em certa sociedade, maiores as chances de que um algoritmo, ao ser alimentado com dados a respeito dessa sociedade, sendo provável que o algoritmo extraia e replique esse padrão discriminatório.

Para compreender como as atuais tecnologias "tornam-se" enviesadas, é preciso, em primeiro lugar, compreender seu funcionamento. As atuais ferramentas de reconhecimento facial operam mediante *softwares* de inteligência artificial, que, por sua vez, empregam diferentes métodos – *neural networks, machine learning, deep learning*, entre outros – com o objetivo de simular, de maneira mais precisa possível, o raciocínio humano. Esses *softwares* funcionam a partir da combinação entre códigos (regras) e programação (procedimentos lógicos). À combinação entre regras e procedimentos lógicos representados por funções matemáticas dá-se o nome de "algoritmo". Colocando em termos simples, uma inteligência artificial é um algoritmo cuja função é reproduzir, em algum aspecto, faculdades humanas.

Adotamos, neste trabalho, uma entendimento sobre inteligência artificial que se enquadra naquilo que John Searle denomina "IA fraca". Para Searle, é inegável que programas de computadores, assim como os computadores em si, são ferramentas úteis para o estudo da mente humana e o desenvolvimento de tecnologias, hoje imprescindíveis à vida humana. Contudo, um programa de inteligência artificial pode ser considerado como, no máximo, a *simulação* de um processo cognitivo humano, mas não um processo cognitivo *per se*. Em outras palavras, sistemas de IA podem agir de forma inteligente, isto é, agir *como se* fossem inteligentes – ou *como se* tivessem mentes. Assim, esses sistemas, apesar de agirem de forma inteligente, não seriam entidades genuinamente inteligentes, mas, no máximo simulações de comportamentos inteligentes, não tendo raciocínio nem vontades, pois a máquina se baseia no insumo do conhecimento fornecido por um programador, necessariamente humano (SEARLE, 1997).

Por outro ladro, há quem defenda a existência de "IA forte". Isso significa acreditar que a mente está para o cérebro da mesma maneira que um *software* está para o *hardware* do

computador (SEARLE, 1997, p. 26). Essa visão tem por consequência a constatação de que não há nada essencialmente biológico na mente humana, e, nesse sentido, o cérebro integra, por acaso, o grande número de tipos de computadores que poderiam sustentar os programas que compõem a inteligência humana. Seguindo esta visão, qualquer sistema físico que tivesse o programa certo, com *inputs* e *outputs* adequados, teria uma mente exatamente no mesmo sentido em que humanos possuem uma mente. O único impedimento à replicação da consciência humana seria, portanto, o fato de ainda não terem sido criados *hardwares* e *softwares* necessários para tanto, tratando-se apenas de uma questão de tempo até que fosse possível *replicar* a consciência humana. Para os autores que acreditam em tal visão, os cérebros e mentes artificiais seriam equivalentes, em todos os aspectos, aos cérebros e mentes humanas (SEARLE, 2006).

No presente trabalho, reitera-se, os sistemas de IA serão compreendidos como inteligências artificiais fracas, consoante o entendimento de Searle. Os argumentos apresentados pelo autor demonstram que sistemas de IA funcionam a partir de uma lógica puramente sintática, desprovida de conteúdo semântico; assim, apenas *mimetizam* o comportamento intencional através de parâmetros pré-estabelecidos de *inputs* e *outputs* (SEARLE, 2006, p 90). Posto isso, temos que os algoritmos são passíveis de enviesamento devido ao fato de atenderem exclusivamente ao modo e critérios aplicados pelo seu criador, o programador. Como não é possível, por enquanto, se falar em uma inteligência artificial verdadeiramente autônoma, os *softwares* existentes operam de maneira condicionada, sempre respondendo aos *inputs* e *outputs* pré-determinados e estabelecidos por quem desenvolve o programa (SEARLE, 2006, p 90). Disso decorre que o resultado das eventuais decisões tomadas por um *software* de IA – incluindo-se aqueles destinados ao reconhecimento facial – continuará fortemente influenciado pelos valores, crenças e convicções da pessoa que o criou, por mais que se busque uma pretensa imparcialidade e superação do subjetivismo humano.

O viés é uma característica inevitável da vida, resultado da visão necessariamente limitada do mundo que qualquer pessoa ou grupo tem. Mas o viés social pode ser refletido e amplificado pela inteligência artificial de maneiras perigosas, seja para decidir quem recebe um empréstimo bancário ou decidir quem é vigiado em determinado sistema de reconhecimento facial (SMITH, 2019). Para Ana Frazão, "é muito provável que a programação possa estar permeada de vieses e preconceitos dos programadores, intencionais ou não, que podem levar a erros de diagnóstico ou a graves discriminações" (2019b, p. 39). Desses vieses e preconceitos pode decorrer a comum confusão entre "causa e correlação". Assim, é possível que "as

correlações encontradas no processamento sejam consideradas equivocadamente causalidades, fator que pode reforçar discriminações" (FRAZÃO, 2019b, P. 39).

Frazão conclui que "os algoritmos podem perpetuar injustiças, preconceitos e discriminações" (FRAZÃO, 2019b, p. 39). Logo, identificar e analisar possíveis vieses em sistemas de IA é extremamente importante, à medida que temos dependido cada vez mais de computadores, que empregamos para processar a linguagem natural que os humanos usam, por exemplo, ao fazer pesquisas de texto *on-line*, categorizar imagens e traduções automatizadas, apontam Aylin Caliskan e Joanna Bryson, pesquisadoras da Universidade de Bath, no Reino Unido[74].

Porém, como exatamente um viés é inserido na inteligência artificial? Olga Russakovsky expõe três principais causas que podem gerar algoritmos enviesados[75]. Em primeiro lugar, é comum que o viés se encontre nos dados que são utilizados para alimentar determinado programa. Não raramente, *softwares* de reconhecimento facial desenvolvidos nos países ocidentais são alimentados por bancos de dados compostos por imagens, em sua maioria, de homens brancos e de meia idade, com pouca ou nenhuma representatividade de mulheres, pessoas negras e pessoas mais velhas. A segunda causa diz respeito aos algoritmos em si e ao modo como são programados para realizar associações e interpretar dados. A terceira, por sua vez, refere-se ao fator humano *per se*: geralmente, os pesquisadores e desenvolvedores de IA são pessoas do sexo masculino, provenientes de determinadas demografias raciais, que cresceram em áreas socioeconômicas elevadas, e são, principalmente, pessoas sem deficiência.

Especificamente em relação à primeira causa apresentada, aponta Thomas Redman (2018) que a baixa qualidade dos dados é "o inimigo número um" do uso eficiente e difundido da inteligência artificial baseada em *machine learning*. O aprendizado de máquina demanda uma elevada qualidade dos dados, e dados "ruins" podem ocasionar complicações em momentos distintos do desenvolvimento de determinado programa: a primeira delas surge imediatamente com os dados utilizados para o treinamento do modelo preditivo, denominados

[74] "Biased bots: Human prejudices sneak into AI systems". Disponível em: https://www.bath.ac.uk/announcements/biased-bots-human-prejudices-sneak-into-ai-systems/.
[75] "Dealing With Bias in Artificial Intelligence". Disponível em: https://www.nytimes.com/2019/11/19/technology/artificial-intelligence-bias.html?fbclid=IwAR2nyAo-nFfh-H6P0XwYsGq0pZ4tXFpV1vPIMxE_Ztea1nJ7dAmsTqL96Uk.

"dados históricos"; a segunda, no momento de análise dos novos dados utilizados para tomar decisões futuras.

Segundo o autor, para treinar adequadamente um modelo preditivo, os dados históricos devem atender a padrões de qualidade excepcionalmente amplos e elevados. Primeiro, os dados devem estar certos: devem ser precisos, adequadamente rotulados, não duplicados, e assim por diante. Além disso, é preciso ter os dados *corretos*, isto é, dados imparciais, em toda a gama de entradas para as quais se pretende desenvolver o modelo preditivo. No entanto, ainda hoje em dia, a maioria dos dados utilizados em inteligências artificiais não atende aos padrões básicos, não sendo, portanto, "dados corretos". Os motivos para tanto variam de desenvolvedores de dados que não entendem o que é "esperado", e, portanto, criam bases de dados pouco representativas ou incompletas, a processos lógicos excessivamente complexos e até erros humanos.

Demandas e problemas cada vez mais complexos exigem não apenas mais dados, mas dados mais abrangentes e mais diversificados, a fim de se evitarem vieses (REDMAN, 2018). No entanto, o que se vê atualmente vai na contramão desse entendimento: segundo estudo realizado pelo *National Institute of Standards and Technology* (NIST)[76] dos Estados Unidos, a maioria dos sistemas de reconhecimento facial presentes no país apresentam vieses[77]. O Instituto testou 189 algoritmos de reconhecimento facial de 99 desenvolvedores, que representam a maioria dos desenvolvedores comerciais. Foram testados sistemas de empresas como a Microsoft, a alemã Cognitec e a chinesa Megvii; contudo, não foram testados os sistemas da Amazon, Apple, Facebook e Google, porque as companhias se recusaram a submeter seus algoritmos para o estudo. Apesar de os sistemas analisados serem sistemas comerciais, vale ressaltar que muitos deles são empregados por diferentes órgãos de segurança pública nos EUA.

Joy Buoloamnwi, pesquisadora do MIT (*Massachussets Institute of Technology*) e uma das responsáveis pelo estudo, destaca que, embora alguns pesquisadores e fornecedores de sistemas de reconhecimento biométrico facial afirmem que o viés algorítmico não é um problema, ou que é um problema já superado, a análise realizada forneceu uma abrangente refutação de tais alegações. Verificou-se que: as taxas de erro mais altas ocorreram na

[76] Em português, "Instituto Nacional de Padrões e Tecnologias".
[77] "Many Facial-Recognition Systems Are Biased, Says U.S. Study". Disponível em: https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.

identificação de nativos americanos; os sistemas identificaram falsamente os idosos até 10 vezes mais do que adultos de meia idade; os *softwares* apresentaram mais dificuldade em identificar mulheres do que homens; e identificaram falsamente rostos afro-americanos e asiáticos com uma taxa de erro de 10 a 100 vezes mais que os rostos caucasianos. É possível compreender como a ciência de dados pode, na realidade, perpetuar e reforçar preconceitos, se não empregada com a devida cautela (KELLEHER; TIERNEY; 2018). Diante disso, nos tópicos a seguir, serão discutidos especificamente os vieses relativos a gênero e raça/cor.

2.3.2.1 O machismo algorítmico

Compreender por que determinados autores consideram as tecnologias de reconhecimento facial como ferramentas "perfeitas para opressão" (HARTZOG; SELLINGER, 2018) não demanda muito esforço. As já mencionadas *deepfakes*, aprimoradas devido à conciliação de tecnologias de mapeamento facial e algoritmos de inteligência artificial, ilustram essa afirmação. Ainda que as discussões sobre o uso de imagens falsas, sejam estas fotos ou vídeos, tenham se concentrado principalmente em seu potencial impacto na política, vários especialistas em direitos humanos e ética tecnológica têm alertado para outro dano potencial, aparentemente ignorado: as consequências possivelmente devastadoras para as mulheres e outras populações vulneráveis que são vítimas da tecnologia (HAO, 2019a, 2019b).

Tomemos o aplicativo denominado *DeepNude*[78] como exemplo. Embora o nome do programa torne quaisquer explicações basicamente dispensáveis, cabe dizer que sua função é "remover" as roupas de mulheres, trocando-as por corpos nus, altamente realísticos. Em outras palavras, o aplicativo é capaz de inserir o rosto de uma mulher – o software não funciona com rostos masculinos – em um corpo nu, criado digitalmente, de modo que ela aparente estar sem roupa alguma. Ainda que o corpo retratado na imagem final não seja de fato o corpo da vítima da *deepfake*, as chances de ocorrerem danos emocionais e à imagem da mulher são elevadas. Outros programas, como o *FakeApp* e *FindPornFace*[79], têm sido empregados com o objetivo de criar vídeos falsos, de conteúdo sexual, para fins de *revenge porn*[80]. É o caso, dentre

[78] "An AI app that 'undressed' women shows how deepfakes harm the most vulnerable". Disponível em: https://www.technologyreview.com/s/613898/an-ai-app-that-undressed-women-shows-how-deepfakes-harm-the-most-vulnerable/?fbclid=IwAR0w2t6Q9i3xiCkeeZJFBOBhseWoH-mTFAh3DZVM4-8ayqWYNd6Xp6y_tGg.

[79] "People Are Using AI to Create Fake Porn of Their Friends and Classmates". Disponível em: https://www.vice.com/en_us/article/ev5eba/ai-fake-porn-of-friends-deepfakes.

[80] A expressão pode ser traduzida como "pornografia de vingança". Originalmente, refere-se à conduta de se utilizar de imagens ou vídeos, previamente e voluntariamente obtidos no decorrer de um relacionamento, divulgando-os para fins de retaliação ou extorsão.

inúmeros, de Rana Ayubb. Grupos de extrema direita da Índia inseriram o rosto da jornalista em um vídeo pornográfico, divulgando-o massivamente pelo WhatsApp, Facebook e Twitter, como forma de vingança devido aos protestos que Ayubb realizou em razão do estupro e morte de uma garota de 8 anos de idade no país[81].

Se é verdade que o passado pode fornecer lições para o futuro, muitos das novas tecnologias de videovigilância também se tornarão ferramentas de voyeurismo. Alguns dos primeiros estudos sobre o emprego de vigilância por vídeo descobriram que os operadores das salas de controle, que em sua maioria eram homens, usavam os CFTV para acompanhar mulheres, aproximar suas nádegas ou seios e imprimir "capturas de tela" de suas imagens GILLIOM; MONAHAN, 2013, p. 137). Gilliom e Monaham questionam: "com todos os melhoramentos tecnológicos, é possível achar que essas práticas irão se dissipar?" (2013, p. 137).

Importante destacar, neste ponto, que as tecnologias de reconhecimento facial podem adquirir caráter machista/misógino de maneira proposital, por "dolo" de seus programadores, como nos exemplos descritos acima, mas também podem fazê-lo não intencionalmente, em uma espécie de "culpa", o que ocorre com maior frequência. Observe-se: em 2014, a Facebook anunciou que seu software de reconhecimento facial possuía uma acurácia de 97%. A base de dados do programa, contudo, consistia em 77% de indivíduos do sexo masculino, e 80% das pessoas possuíam a pele clara[82]. Quando analisados rostos de mulheres e de pessoas negras, a precisão do programa caía consideravelmente. Isso porque a base de dados com que o *software* fora alimentado encontrava-se, ainda que não propositalmente, enviesada, dada a baixa representatividade de mulheres e pessoas negras.

Essa "tendência" é observada em diversos outros programas de reconhecimento facial. Joy Buolamwini e Timnit Gebru (2018) analisaram como os *softwares* de reconhecimento facial das principais empresas de tecnologia desempenhavam a identificação de gênero. Foram analisados, além dos sistemas da Amazon, IBM e Microsoft, os sistemas *Face*++, *Clarifai* e *Kairos*. De maneira geral, todos os *softwares* apresentaram melhor desempenho em rostos

[81] "I was vomiting: Journalist Rana Ayyub reveals horrifying account of deepfake porn plot". Disponível em: https://www.indiatoday.in/trending-news/story/journalist-rana-ayyub-deepfake-porn-1393423-2018-11-21.
[82] "Response: Racial and Gender bias in Amazon Rekognition — Commercial AI System for Analyzing Faces". Disponível em: https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced.

masculinos do que femininos, e todos tiveram melhor desempenho em rostos de pele clara do que rostos de pele mais escura. As taxas de erro foram de 35% para mulheres de pele mais escura, de 12% para homens de pele mais escura, de 7% para mulheres de pele mais clara e não mais de 1% para homens de pele mais clara (BUOLAMWINI; GEBRU; 2018, p. 8).

Em mais um exemplo, podemos apontar o estudo[83] realizado pelo NIST (*National Institute of Standards and Technology*) sobre a utilização dos *softwares* de reconhecimento facial da empresa francesa Idemia, empregados para controle de migrações na França, Austrália e Estados Unidos. O estudo consistia em testar se os algoritmos eram capazes de analisar se duas fotos distintas eram da mesma pessoa, de maneira semelhante ao que faz um agente de segurança ao verificar se a foto de um passaporte corresponde ao seu portador. Quando configurados para realizar o reconhecimento facial de mulheres, os sistemas apresentavam taxa de erro de 1 para 10.000; contudo, quando se tratavam de rostos de mulheres negras, a taxa de erro aumentava para 1 para 1.000, sendo, portanto, 10 vezes maior. Embora a acurácia do programa seja elevada, os resultados do estudo revelam outro aspecto que deve ser levado em consideração: as opressões resultantes da sua utilização são interseccionais[84].

Os vieses presentes em algoritmos podem, em alguns casos, transformá-los em ferramentas de opressão e violência, devido ao caráter discriminatório que, propositalmente ou não, assumem. É possível perceber, a partir da análise dos dados trazidos, que tecnologias de reconhecimento facial enviesadas geram mais danos em potencial a mulheres do que a homens, e que esses danos são ainda mais evidentes quando falamos em mulheres negras – o que nos leva ao próximo tópico da presente pesquisa.

---

[83] "The Best Algorithms Struggle to Recognize Black Faces Equally". Disponível em: https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/

[84] O conceito de interseccionalidade foi criado pela filósofa feminista Kimberlé Crenshaw, nos anos 90, nos EUA. Para a autora, "A interseccionalidade (...) busca capturar as consequências estruturais e dinâmicas da interação entre dois ou mais eixos da subordinação. Ela trata especificamente da forma pela qual o racismo, o patriarcalismo, a opressão de classe e outros sistemas discriminatórios criam desigualdades básicas que estruturam as posições relativas de mulheres, raças, etnias, classes e outras. Além disso, a interseccionalidade trata da forma como as políticas específicas geram opressões que fluem ao longo de tais eixos, constituindo aspectos dinâmicos ou ativos do desempoderamento" (CREENSHAW, 2002, p. 177). O conceito foi trazido apenas para indicar que as discussões sobre enviesamento tecnológico, gênero e raça devem ser aprofundadas – o que não será feito no presente trabalho.

2.3.2.2 O racismo algorítmico

O fato de que algoritmos podem reforçar preconceitos é particularmente problemática quando a ciência de dados é aplicada para fins de vigilância e policiamento (KELLEHER; TIERNEY; 2018, p. 191). No estudo de Norris e Armstrong (1999), constatou-se que os jovens, os homens e os negros foram alvos de vigilância de maneira sistemática e desproporcional, pois a vigilância exercida sobre essas pessoas não se deu por causa de seu envolvimento em crimes ou situações de desordem, mas com base apenas em suspeitas categóricas, sem razões fundamentadas e/ou aparentes. Segundo os autores, "como essa diferenciação não se baseia em critérios objetivos e comportamentais e individualizados, mas apenas em ser categorizada como parte de um grupo social específico, essas práticas são discriminatórias" (NORRIS; ARMSTRONG, 1999, p. 150, tradução nossa[85]). Assim, em vez de promover uma vigilância democrática, a confiança em suspeitas categóricas e infundadas intensifica a vigilância daqueles que já são historicamente marginalizados, aumentando ainda mais suas chances de estigmatização, agora por meios “oficiais”, empregados pelos governos (NORRIS, 2003, p. 266).

Os autores ressalvam que se poderia argumentar que as estatísticas relacionadas à criminalidade mostram que os homens, jovens e negros possuem maior envolvimento na prática de crimes. Assim, transformá-los em “alvos” de sistemas de vigilância apenas refletiria a realidade da distribuição da criminalidade. Esse argumento, contudo, é circular: a produção de estatísticas oficiais também é baseada em hipóteses pré-concebidas sobre como se dá a prática da criminalidade, o que, por si só, leva a ações policiais – formais e informais – de caráter discriminatório. Ainda segundo os pesquisadores, as autorias de crimes são mais igualmente distribuídas entre a população em geral do que revelam as estatísticas oficiais. Isso faz com o poder dos operadores de CFTV seja extremamente discricionário[86], pois podem determinar

[85] No original: “As this differentiation is not based on objective behavioural and individualised criteria, but merely on being categorised as part of a particular social group, such practices are discriminatory” (NORRIS; ARMSTRONG, 1999, p. 150).

[86] No original: “Of course, it may be argued that since those officially recorded as deviant, are disproportionately young, male, black, and working class, targeting such groups merely reflects the underlying reality of the distribution of criminality. Such an argument is, however, circular: the production of the official statistics is also based on pre-given assumptions as to the distribution of criminality, which itself leads to the particular configuration of formal and informal operational police practice. As self-report studies of crime reveal, offending is in fact, far more evenly distributed

quem será vigiado, por quanto tempo, e quando se iniciará seu monitoramento, o que acaba por produzir um "padrão de vigilância altamente diferenciado, levando ao monitoramento massivamente desproporcional de homens jovens, particularmente se são negros ou visivelmente identificáveis como pertencentes a determinados grupos culturais" (NORRIS; ARMSTRONG, 1999, p. 150, tradução nossa)[87].

A discricionaridade que os controladores de CFTV possuíam há 20 anos pertence hoje aos programadores. O seu potencial lesivo, contudo, foi exponencialmente ampliado, devido à capacidade de abrangência dos sistemas modernos de reconhecimento facial. Ressalte-se, como exposto anteriormente, que as tecnologias de reconhecimento facial podem adquirir caráter discriminatório propositalmente, por "dolo" de seus desenvolvedores, ou podem fazê-lo sem que haja tal intenção, em uma espécie de "culpa".

No que tange à primeira hipótese, temos o caso do software *Faception,* desenvolvido por uma *startup* israelense. Segundo seus desenvolvedores, "nossa personalidade é determinada por nosso DNA e refletida em nosso rosto, como um tipo de sinal"[88]. Partindo dessa premissa, o *Faception* se diz capaz de identificar traços da personalidade de uma pessoa a partir tão somente da análise de sua biometria facial – podendo classifica-la como "pedófila", "terrorista" ou "uma boa jogadora de poker"[89]. O programa ganhou destaque após os atentados ocorridos em Paris, em novembro de 2015, quando Shai Gilboa, CEO da empresa, divulgou que a inteligência artificial desenvolvida foi capaz de classificar 9 dos 11 autores do ataque como "terroristas" sem que suas imagens houvessem sido previamente inseridas nos bancos de dados. Chama à atenção o fato de todos possuírem ascendência árabe, característica levada em conta pelo algoritmo e que foi suficiente para identifica-los como terroristas.

---

throughout the population than reflected in the official statistics" (NORRIS; ARMSTRONG, 1999, p. 150).

[87] No original: "The sum total of these individual discretionary judgments produces, as we have shown, a highly differentiated pattern of surveillance leading to a massively disproportionate targeting of young males particularly, if they are black or visibly identifiable as having subcultural affiliations. (NORRIS; ARMSTRONG, 1999, p. 150).

[88] "Can you spot a terrorist just by looking at their face? New software can tell if you are anything from a paedophile to an ace poker player by analysing your features". Disponível em: https://www.dailymail.co.uk/news/article-3606811/Can-spot-terrorist-just-looking-face-Israeli-company-claims-predict-paedophiles-geniuses-ace-poker-players-analysing-features.html.

[89] "Controversial software claims to tell personality from your face". Disponível em: more: https://www.newscientist.com/article/2090656-controversial-software-claims-to-tell-personality-from-your-face/#ixzz6DlZQPj3uhttps://www.newscientist.com/article/2090656-controversial-software-claims-to-tell-personality-from-your-face/.

Em relação à segunda hipótese, não é difícil perceber como determinadas inteligências artificiais negligenciam dados relativos à raça/cor de pele e, eventualmente, ocasionam situações de discriminação. Possivelmente o caso mais grotesco – logo, mais emblemático – de um algoritmo racista seja o do *software* de reconhecimento facial da Google. Em 2015, o aplicativo *Google Photos* identificou e rotulou duas pessoas negras como "gorilas"[90]. À época, a gigantesca empresa de tecnologia prometeu tomar providências imediatas, mas a solução apresentada veio apenas três anos depois, e pode-se dizer que foi tão grotesca quanto a falha original. A fim de evitar que pessoas negras fossem novamente identificadas como gorilas, a Google excluiu os termos relacionados aos animais de seu software, bem como removeu as imagens de chimpanzés, macacos e demais primatas de sua base de dados[91].

Nem todas as ocorrências "racismo algorítmico", todavia, são tão explícitas e esdrúxulas[92]. O enviesamento de tecnologias de reconhecimento facial no que tange aos critérios relativos a raça/cor de pele pode ser percebido em situações mais sutis. É o caso, por exemplo, das câmeras fotográficas da Nikon dotadas de uma ferramenta capaz de reconhecer quando a pessoa fotografada havia fechado o olho, a fim de sugerir que se tirasse uma nova fotografia. Embora a ideia pareça interessante, as câmeras falhavam em identificar se pessoas asiáticas haviam piscado ou não, erroneamente sugerindo que o haviam feito, quando, na realidade, estavam de olhos abertos[93] – curiosamente, a Nikon, empresa de renome mundial na indústria fotográfica, é japonesa. No mesmo sentido, o sistema de reconhecimento facial do *iPhone*, celular da Apple, tem apresentado dificuldades em diferenciar rostos asiáticos. Usuários do smartphone na China relataram que o sistema "confunde" seus rostos, desbloqueando indevidamente o aparelho[94].

Há que se ter em mente, contudo, que danos verdadeiramente severos podem decorrer do uso de tecnologias de reconhecimento facial com viés racista, como nos permite enxergar o

---

[90] "A major flaw in Google's algorithm allegedly tagged two black people's faces with the word 'gorillas'". Disponível em: https://www.businessinsider.com/google-tags-black-people-as-gorillas-2015-7

[91] "Google's solution to accidental algorithmic racism: ban gorillas". Disponível em: https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people.

[92] Sobre o tema, ver: SILVA, Tarcízio. Linha do Tempo do Racismo Algorítmico. *Blog do Tarcízio Silva*, 2019. Disponível em: https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo/. Acesso em: 14 jan. 2020.

[93] "Are Face-Detection Cameras Racist?". Disponível em: http://content.time.com/time/business/article/0,8599,1954643,00.html.

[94] "Chinese iPhone X owners claim Apple's facial recognition cannot tell them apart". Disponível em: https://metro.co.uk/2017/12/22/iphone-x-racist-cant-tell-chinese-people-apart-apple-customers-claim-7178957/.

estudo realizado pela ACLU – mencionado no tópico 3.1.1 deste trabalho. Utilizando o software Rekognition, o estudo comparou a imagem dos 535 deputados e senadores estadunidenses a uma base de dados composta por 25.000 fotos, publicamente disponibilizadas, de pessoas que já haviam sido presas no país. Dentre as 28 identificações incorretas apontadas pelo programa, 11 correspondiam a pessoas negras, entre homens e mulheres, de diferentes idades. Isso equivale a aproximadamente 40% dos erros, ao passo que apenas 20% dos membros do congresso são negros. Outro estudo sobre o mesmo programa – este realizado pelo MIT – apontou que mulheres negras foram erroneamente identificadas como homens em 31% das análises realizadas[95].

Discorrendo sobre o uso do Rekognition nos Estados Unidos, Jacob Snow (2018) alerta para as chances de a tecnologia "influenciar" o pensamento, e, consequentemente, o comportamento de um agente de segurança. Imagine-se, por exemplo, que um policial, mediante o uso de uma tecnologia de reconhecimento facial, identifique que determinada pessoa a ser abordada fora presa por porte ilegal de armas. Seja a identificação correta ou não, é provável que essa identificação gere determinado "viés" no comportamento do policial, havendo grandes chances de isso implicar uma diferente abordagem à pessoa identificada, como no caso da idosa, negra, violentamente abordada em São Francisco (caso narrado no item 3.3.1).

É notório que as identificações incorretas recaem desproporcionalmente sobre a população negra, socialmente marginalizada nos Estados Unidos e em outros países, como o Brasil. Segundo dados do IBGE, pretos e pardos correspondem a 55,8% da população[96] brasileira. Contudo, 90,5% dos presos por monitoramento facial no Brasil são negros. A natureza antecipatória do policiamento preditivo significa que os indivíduos podem ser tratados de maneira diferente, não por causa do que fizeram, mas por causa de inferências baseadas em dados sobre o que poderiam fazer. Como resultado, esses tipos de sistemas podem reforçar práticas discriminatórias, replicando os padrões em dados históricos e criar "profecias auto-realizáveis" (KELLEHER; TIERNEY; 2018, p. 196). Transpondo o prognóstico do uso das tecnologias de reconhecimento facial para o Brasil, um país cuja polícia mata por confundir

[95] "MIT researchers: Amazon's Rekognition shows gender and ethnic bias (updated)". Disponível em: https://venturebeat.com/2019/01/24/amazon-rekognition-bias-mit/.
[96] "Número de brasileiros que se declaram pretos cresce no país, diz IBGE". Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2019/05/22/ibge-em-todas-as-regioes-mais-brasileiros-se-declaram-pretos.htm.

guarda-chuvas com fuzis[97] ou furadeiras com metralhadoras[98], chega a ser desolador imaginar o que poderia acontecer caso uma pessoa fosse erroneamente identificada como um potencial criminoso ou confundida com um violento foragido.

Natalie Byfield (2018) sintetiza a discussão do racismo em sistemas de vigilância. Para a autora, a vigilância baseada em/orientada por critérios raciais é um componente intrínseco do chamado "estado racial". A denominada "vigilância racial" – assim como todas as demais formas de vigilância – se vale de técnicas, políticas e processos sociais com o objetivo de "tornar visível o invisível", coletando dados sobre o cidadão observado para fins de classificação, tendo como propósito último o controle social (BYFIELD, 2018, p. 5). A análise de dados biométricos tem sido historicamente empregada como uma "tecnologia de vigilância e controle de movimentos negros" (BROWNE, 2015, p. 25-26, apud BYFIELD, 2018, p. 13, tradução nossa) [99], o que se intensificou com o desenvolvimento tecnológico ocorrido nos últimos anos. Segundo Byfield, a coleta de dados pessoais representa, portanto, uma forma de gerenciamento policial das populações (OLIVEIRA, 2019b). Disso decorre, enfim, o aumento e o acúmulo de poder dos vigilantes sobre os vigiados (BYFIELD, 2018), assunto que será abordado no capítulo seguinte.

[97] "PM confunde guarda-chuva com fuzil e mata garçom no Rio, afirmam testemunhas". Disponível em: https://brasil.elpais.com/brasil/2018/09/19/politica/1537367458_048104.html.
[98] "Policial do Bope confunde furadeira com arma e mata morador do Andaraí". Disponível em: http://g1.globo.com/rio-de-janeiro/noticia/2010/05/policial-do-bope-confunde-furadeira-com-arma-e-mata-morador-do-andarai.html.
[99] No original: "technology in the surveillance of black mobilities and of black stabilities and containment" (BROWNE, 2015, p. 25-26, apud BYFIELD, 2018, p. 13).

3 ACABOU-SE A PRIVACIDADE? REPENSANDO DIREITOS NO CONTEXTO DO PAN-ÓPTICO DIGITAL

"It seems to me, Golan, that the advance of civilization is nothing but an exercise in the limiting of privacy."

Isaac Asimov

3.1 Da sociedade de vigilância ao pan-óptico digital

Por que o termo "sociedade de vigilância"? Porque, virtualmente, todas as atividades sociais, institucionais e negociais que possuem alguma relevância em nossa sociedade envolvem a coleta e o monitoramento sistemático de dados, bem como a análise desses dados com o objetivo de tomar decisões, minimizar riscos, classificar grupos sociais e exercer poder. A vigilância é, portanto, "monitorar as pessoas a fim de regular ou governar seu comportamento" (GILLIOM; MONAHAN, 2013, p. 9, tradução nossa) [100].

Devido às crescentes tentativas de regulamentação e controle, até mesmo as emoções das pessoas, em sua mais profunda intimidade, estão suscetíveis a violações, como expõe Rodotà:

> Nem mesmo a esfera mais íntima escapa a invasões. São oferecidos programas que analisam cada mínima inflexão da voz para estabelecer se está dizendo a verdade. Graças à análise computadorizada das expressões faciais, de cada movimento dos músculos do rosto com o *Facial Action Coding System*, procura-se descobrir os estados 'alma – a dimensão mais recôndita da pessoa – do mesmo modo que a memória individual é sondada na busca de "impressões cerebrais" que revelem lembranças de fatos passados e possam ser tomadas como prova de participação naquele episódio (RODOTÀ, 2004, p. 93).

Assim, o corpo humano, que há até pouco havia sido deixado de lado em detrimento do corpo eletrônico, volta a receber relevância, de modo renovado, tornando-se "fonte de novas informações, objeto de um contínuo *data mining*, verdadeira mina a céu aberto da qual se extraem dados continuamente" (RODOTÀ, 2004, p. 93). Percebida a fragilidade de se confiar somente no corpo eletrônico – baseado em números e palavras-chave facilmente fraudáveis ou falsificáveis – o corpo físico readquire importância ao transformar-se em senha, em código. Para reagir à falta de segurança das senhas eletrônicas, aponta Rodotà, surgiram novas

[100] No original: "We define surveillance as *monitoring people in order to regulate or govern their behaviour"* (GILLIOM; MONAHAN, 2013, p. 9, grifo dos autores).

tecnologias que se caracterizam pelo uso cada vez mais maciço de dados biométricos, "possibilitando assim a realização de controles generalizados em todos os cidadãos" (2004, p. 92).

Nesse movimento, "o físico toma o lugar das abstratas palavras-chave" (RODOTÀ, 2004, p. 93) e elementos corporais, como impressões digitais, o formato da mão ou dos dedos, a formação dos vasos sanguíneos que compõem a retina, os anéis coloridos em torno da pupila, o andar, a voz, e, claro, os traços faciais tornam-se elementos aptos a identificar uma pessoa. Recorre-se cada vez mais frequentemente a esses dados biométricos para finalidades de identificação ou confirmação de identidade para acesso a serviços diversos. Dados esses que têm sido importantes não só em atividades banais, como sacar dinheiro em um caixa eletrônico ou acessar um *smartphone*, mas também em situações mais complexas, como votar ou ingressar em um país. Isto posto, conclui Rodotà, "se o corpo pode converter-se em senha, as tecnologias de localização farão nascer uma *networked person*" (2004, p. 95).

O autor italiano ressalva que o "retorno ao físico não implica a dissociação entre corpo e tecnologia" (RODOTÀ, 2004, p. 94). Isso porque "as inovações tecnológicas que permitem a renovada decomposição do corpo mediante a coleta de informações reduzem a identidade do sujeito a um só detalhe" (RODOTÀ, 2004, p. 94). Por "detalhe", entendamos qualquer dado biométrico, como uma digital, uma íris, uma assinatura facial. Nesse cenário, a vigilância social se baseia em uma espécie de "coleira eletrônica" (RODOTÀ, 2004). Devido às novas tecnologias, o corpo humano pode ser comparado a um objeto qualquer em movimento. Enquanto objeto, pode ser vigiado à distância. Da vigilância surge, consequentemente, o controle.

O processo de agregação de dados sobre uma pessoa cria, nas palavras de Daniel Solove, uma "pessoa digital": "um retrato composto de fragmentos de informações combinadas" (SOLOVE, 2008, p. 125, tradução nossa). Destarte, poderíamos considerar que as mudanças promovidas pelas novas tecnologias afetam a própria antropologia das pessoas (RODOTÀ, 2004). Afetam, afinal, o que é *ser* humano. Hoje somos continuamente perscrutados através de câmeras de vídeo e de técnicas biométricas, o que nos individualiza cada vez mais e cada vez mais nos torna *networked persons*. Nos tornamos "pessoas permanentemente em rede, configuradas a emitir e receber pulsos que permitem esquadrinhar e reconstruir movimentos, hábitos, contatos, alterando sentido e conteúdo da autonomia das pessoas. (RODOTÀ, 2004, p. 95)". Disso decorrem novos e ainda mais dramáticos problemas, devido principalmente ao fato

de que alguns dados biométricos contêm uma multiplicidade de informações, em sua maioria sensíveis, que excedem a finalidade de identificação ou de verificação (RODOTÀ, 2004, p. 94).

É preocupante que esses dados sejam utilizados não somente para fins de identificação ou confirmação imediatos que se "esgotam" no momento em que se realiza o reconhecimento. Dados biométricos podem ser empregados como "elementos de classificação permanente, para controles ulteriores em relação ao momento da identificação ou da autenticação, isto é, da confirmação de uma identidade (RODOTÀ, 2004, p. 93)", culminando no que Frank Pasquale (2015) denomina "*one-way mirror*"[101]. Governos e grandes *players* econômicos têm obtido dados pessoais de maneira unilateral, adquirindo e armazenando informações sobre os cidadãos, ao passo que estes nada sabem sobre esses agentes, tampouco possuem conhecimento sobre a dimensão em que se dá a coleta de seus dados.

Cabe, aqui, um apontamento. As pessoas tendem a crer que as atividades de vigilância e monitoramento são praticadas exclusivamente pelos governos. Logo, creem que conversas privadas, ligações telefônicas, pesquisas em sites de busca e publicações em rede sociais estariam "a salvo" dos olhos dos agentes governamentais. Contudo, hoje resta evidente o envolvimento de entes privados nessas práticas: a parceria público-privada na vigilância é forte, continuará a crescer, e é muito bem escondida de qualquer mecanismo de prestação de contas efetivo[102] (GILLIOM; MONAHAN, 2013, p. 139). O monitoramento e a vigília constantes sobre cada passo da vida das pessoas leva a um verdadeiro capitalismo de vigilância (ZUBOFF, 2019), cuja principal consequência é a constituição de uma sociedade também de vigilância (FRAZÃO, 2019b).

Rodotà reconhece que "existem evidentemente muitas boas razões que sustentam a necessidade de usar todas as oportunidades oferecidas pelas novas tecnologias para proteger a sociedade dos crimes", devendo-se "buscar o equilíbrio entre a visão individualista da privacidade e a satisfação das demandas da sociedade" (RODOTÀ, 2008, p. 147). No mesmo sentido, Norris (2003, p. 276) aponta que determinados autores argumentam que é a primeira

[101] Em português, a expressão *"one-way mirror"* poderia ser traduzida como "espelho investigativo", ou, em termos técnicos, como "espelho semitransparente". O termo se refere aos espelhos utilizados frequentemente para investigação criminal, pois reflete um dos lados, enquanto se releva transparente para o outro.

[102] No original: "The public-private partnership in surveillance is strong, will continue to grow, and is very well hidden from any meaningful accountability" (GILLIOM; MONAHAN, 2013, p. 139).

vez na história que temos a oportunidade de experimentar formas de controle que não levam em consideração categorias de divisão social. Critérios como idade, sexo, raça, beleza e vestuário seriam, assim, considerados irrelevantes.

Todavia, é importante que tais colocações sejam analisadas com certa cautela. Há que se considerar que "os riscos da sociedade da vigilância ligam-se tradicionalmente ao uso político de informações para controlar os cidadãos", e que o escopo da vigilância torna-se constante em cada momento da vida, apresentando-se como "um traço próprio das relações de mercado, cuja fluidez diz respeito à possibilidade de dispor livremente de um conjunto crescente de informações" (RODOTÀ, 2008, p. 113). É preciso levar em consideração que a economia movida a dados e o capitalismo de vigilância são "as duas faces da mesma moeda pois, quanto maior a importância dos dados, mais incentivos haverá para o aumento da vigilância e, por conseguinte, maior será a coleta de dados" (FRAZÃO, 2019b, p. 28).

Esses incentivos para o aumento da vigilância se justificam pela demanda por segurança, embasada por sua suposta necessidade. Assim, "fazendo 'infinita' a guerra, infinitas também devem ser as formas de controle, com uma mudança qualitativa nas relações entre Estado e cidadãos, com transformações profundas na organização social como um todo" (RODOTÀ, 2004, p. 92). Isso ocasiona a consolidação da imagem do "homem de vidro",

> o verdadeiro cidadão desse novo mundo. Uma imagem que, não por acaso, provém diretamente do tempo do nazismo e que propõe uma forma de organização social profundamente alterada, uma espécie de transformação irrefreável da "sociedade da informação" em "sociedade da vigilância**"** (RODOTÀ, 2008, p. 113).

O avanço das tecnologias de informação e comunicação, notadamente a partir do recente desenvolvimento de técnicas de inteligência artificial, resultaram em mudanças na subjetividade das relações entre o ser humano e a tecnologia (DONEDA et al., 2018). Como aponta Rodotà (2008, p. 113), as tecnologias da comunicação e da informação naturalmente entram em conflito com o direito de construir livremente a própria esfera privada (entendida como autodeterminação informativa, como poder de controlar a circulação das próprias informações).

Além disso, a metáfora do homem de vidro reflete a ideia de um Estado que pode inteirar-se completamente da vida das pessoas, de modo que seus jurisdicionados não possuem o *status* de cidadãos, mas sim de súditos (RODOTÀ, 2011, p. 15). As consequências desse

fenômeno, aponta Rodotà, são “dramáticas para as pessoas e destrutivas para a democracia”, pois

> se uma pessoa deseja preservar uma esfera mínima de privacidade e intimidade, e deseja que ninguém saiba certas informações sobre si mesma, ela se torna, segundo o Estado, "alguém que tem algo a esconder" e automaticamente torna-se um suspeito, um "inimigo do povo". Essa é uma lógica típica dos regimes totalitários e, portanto, contrária à democracia (RODOTÀ, 2011, p. 16, tradução nossa).

Assim, é imprescindível que se reestruture a noção de cidadania, dentro da qual se encontra a ideia de privacidade, sob o risco de que este se torne um direito vazio, incapaz de atender às demandas impostas pela nova relação entre pessoa e tecnologia na sociedade contemporânea. Para tanto, é também imprescindível se endereçar e analisar os problemas que despontam, inevitavelmente, com a consolidação da sociedade da vigilância. Uma das principais questões – como expõem Rodotà (2008), Norris (2003), Lianos e Douglas (2000), entre outros – é a utilização das informações pessoais para a construção de perfis individuais ou de grupo, porque

> as informações utilizadas são, de fato, sempre parciais e incompletas, mesmo quando se recorre a uma multiplicidade de bancos de dados. Além disso, permanece controversa, e a ser comprovada, a plena validade científica dos modelos usados para produzir novas informações (perfis ou outras) com base em dados coletados. Chega-se assim a "metaconhecimentos" sobre as pessoas, que dificilmente podem ser verificados pelos interessados, embora até embasem decisões sobre eles. Diante dessa nova situação, parece insuficiente a garantia oferecida por algumas legislações, de proibir que decisões judiciais administrativas, que impliquem uma avaliação de comportamento, se baseiem unicamente em elaborações automáticas de informações que forneçam um perfil da personalidade do interessado. Com efeito, os perfis são utilizados para decisões que, para a maioria dos cidadãos são mais freqüentes (sic) e, no mais das vezes, mais significativas do que as judiciais ou administrativas, e que são aquelas que dizem respeito a cidadão consumidor ou usuário de serviços (RODOTÀ, 2008, p. 115).

Importa considerar, portanto, que os sistemas de vigilância baseados em reconhecimento facial, inclusive os mais modernos, são profundamente simples, redutivos, pois não utilizam outra lógica senão aquela que houver sido inserida em seu *software* por um programador humano. O ponto final desse processamento é a criação de um sistema binário de classificação: o acesso é aceito ou negado; a identidade é confirmada ou rejeitada; o comportamento é legítimo ou ilegítimo (NORRIS, 2003, p. 276). A partir daí, surgem implicações fundamentais para a base normativa do controle social. Explica-se: o controle (vigilância) que se realiza presencialmente é negociado. Não é absoluto, mas sim baseado em uma avaliação moral complexa do caráter, que avalia a identidade, a aparência e o

comportamento da pessoa através das lentes de relevância específica de determinado contexto. Essa negociação tem uma função moral e educativa crucial, pois é por meio da negociação – da aprovação e desaprovação – que os valores sociais são aprendidos e reforçados, uma vez que a classificação realizada por sistemas inteligentes de vigilância e controle não se baseia em avaliação moral diferenciada e multifacetada, mas no elemento único de mediação que o sistema reconhece (NORRIS, 2003).

Em outras palavras, para um algoritmo não há indivíduos bons e ruins, honestos e desonestos, pobres ou ricos. Existem simplesmente detentores ou não detentores da possibilidade acesso e ingresso a determinados lugares, bens e serviços (NORRIS, 2003, p. 276-277). Expusemos anteriormente que aqueles favoráveis ao emprego de tecnologias de reconhecimento facial para fins de vigilância e argumentam que o seu possibilitaria uma vigilância "democrática", em comparação aos sistemas tradicionais de vigilância, face-a-face, presenciais. Porém, como demonstra o já citado estudo realizado por Norris e Armstrong (1999), os jovens, os homens e as pessoas negras tornam-se alvo de maneira sistemática e desproporcional de sistemas de vigilância. Não por causa de seu envolvimento em crimes ou desordens, mas por "nenhuma razão óbvia" e com base apenas em suspeitas categóricas. Essa diferenciação, segundo os autores, não se baseia em critérios objetivos, comportamentais e individualizados, mas apenas no fato de pertencerem a um grupo social específico, o que torna essas práticas evidentemente discriminatórias.

De acordo com Natalie Byfield, o uso de tecnologias de reconhecimento facial para vigilância traz consequências diretas no que diz respeito à violação de direitos humanos. Particularmente, a vigilância orientada por critérios raciais – como exposto na seção sobre racismo algorítmico – "existe na arena do aumento do poder do Estado em sua capacidade de exercer controle sobre toda a sua população e/ou sobre os segmentos específicos da população que escolhe atingir"[103] (BYFIELD, 2018, p. 13). Assim, o Estado passa a possuir um poder ainda maior sobre direitos subjetivos desses grupos, tais como o direito de associação, de reunião, direitos da personalidade e até mesmo sobre o direito à presunção de inocência.

Ademais, ainda segundo Norris (2003, p. 277), se os sistemas de vigilância não são universais em sua aplicação, existe um risco real de que eles sejam empregados de forma

[103] No original: "exist in the arena of increased power of the state in its ability to exert control over its entire population and/or the specific segments of the population it chooses to target" (BYFIELD, 2018, p. 13).

discricionária. Quando o são, comunidades específicas ficam sujeitas a um monitoramento intensivo e extensivo centrado na punição, enquanto outras encontram-se sujeitas a uma vigilância mais "favorável". Observe-se, por exemplo, que esses sistemas não são projetados para identificar um furto, e sim para reconhecer um indivíduo previamente classificado como praticante de tal delito. Um sistema de vigilância poderia, pois, ser utilizado para solicitar que a equipe de segurança de determinada loja concentre sua vigilância especificamente em um indivíduo, na esperança de capturá-lo "em ação" (NORRIS, 2003, p. 278).

Todo o contexto descrito gera implicações diretas não apenas no comportamento de uma pessoa, mas principalmente no que concerne ao respeito à sua identidade, cuja própria construção passa a ser definida por algoritimos. No mundo atual, "corpos anônimos podem ser transformados em sujeitos digitais, identificados e relacionados às suas personas digitais que residem em bases de dados eletrônicas" (NORRIS, 2003, p. 278)[104] – *networked persons*, nas palavras de Rodotà. O fato de sermos sujeitos digitais amplia as possibilidades de violação de nossa privacidade, aqui considerada como o direito da pessoa de escolher aquilo que está disposta a revelar às demais. Por sua vez, as violações do direito à privacidade às quais estamos sujeitos acarretam a desapropriação do espaço de construção de nossa própria identidade (BAIÃO; GONÇALVES, 2014).

A desapropriação do espaço de construção da identidade decorre do fato de os algoritmos serem tidos como absolutos, verdadeiros em todos os casos. Como aponta Ana Frazão (2019b), uma inteligência artificial, independente do fim para que seja utilizada, baseia-se em padrões tidos como inquestionáveis, privilegiando-se dados numéricos, estáticos, em detrimento de outras formas de conhecimento igualmente importantes para os assuntos humanos. Como consequência, ocorre "uma perda – não um ganho – de liberdade, já que tais práticas procuram moldar e predizer o comportamento dos indivíduos de acordo com trajetórias de oportunidades e desejos que são determinadas externamente" (FRAZÃO, 2019b, p. 34). A perda de liberdade, já existente em uma sociedade de vigilância, torna-se ainda mais cristalina no contexto do pan-óptico digital, como se verá a seguir.

[104] No original: "anonymous bodies can be transformed into digital subjects, identified and linked to their digital personae residing in electronic databases" (NORRIS, 2003, p. 278).

3.2 O pan-óptico digital

As discussões sobre vigilância ostensiva e suas consequências na construção da esfera individual não vêm de hoje. Do contrário, ganham relevância a partir do final do século XVIII, com Jeremy Bentham; perpassam o âmbito literário e infiltram o imaginário popular através de obras como "Admirável Mundo Novo", de Aldous Huxley e "1984", de George Orwell; adquirem densidade teórica e novas aplicações em décadas mais recentes, a partir, principalmente, das contribuições de Michel Foucault. Atualmente, readquirem importância na sociedade de vigilância, consolidando-se, por fim e por ora, naquilo que Byung-Chul Han denomina "pan-óptico digital".

O conceito de panóptico foi apresentado pela primeira vez em 1787, pelo filósofo Jeremy Bentham, em uma série de cartas que seriam posteriormente reunidas e publicadas sob o título "O Panóptico ou a casa de inspeção". O autor concebeu a noção de um panóptico no plano físico, estrutural, ao imaginar a projeção arquitetônica de um prédio que servisse como instalação de encarceramento capaz de maximizar o controle das pessoas nele inseridas. Para Bentham,

> quanto mais constantemente as pessoas a serem inspecionadas estiverem sob a vista das pessoas que devem inspecioná-las, mais perfeitamente o propósito do estabelecimento terá sido alcançado. A perfeição ideal, se esse fosse o objetivo, exigiria que cada pessoa estivesse realmente nessa condição, durante cada momento do tempo. Sendo isso impossível, a próxima coisa a ser desejada é que, em todo momento, ao ver razão para acreditar nisso e ao não ver a possibilidade contrária, ele deveria *pensar* que está nessa condição (BENTHAM, 2008, p. 18, grifo do autor).

Michel Foucault, por sua vez, formaliza seus pensamentos acerca do panoptismo no livro "Vigiar e punir: o nascimento das prisões", publicado em 1975. Referindo-se às ideias de Bentham, Foucault reconhece que o efeito mais importante do panóptico é "induzir no detento um estado consciente e permanente de visibilidade que assegura o funcionamento automático do poder" (FOUCAULT, 1999, p. 224). Isso se dá, explica, mediante a inversão do princípio da masmorra: a luz e o olhar de um vigia são melhores instrumentos para o exercício do poder do que a sombra, que ainda permitia certa proteção dos vigiados, pois "a visibilidade é uma armadilha" (FOUCAULT, 1999, p. 224). O objetivo do panóptico é, portanto

> fazer com que a vigilância seja permanente em seus efeitos, mesmo se é descontínua em sua ação; que a perfeição do poder tenda a tornar inútil a atualidade de seu exercício; que esse aparelho arquitetural seja uma máquina de criar e sustentar uma relação de poder independente daquele que o exerce; enfim, que os detentos se encontrem presos numa situação de poder de que

> eles mesmos são os portadores. Para isso, é ao mesmo tempo excessivo e muito pouco que o prisioneiro seja observado sem cessar por um vigia: muito pouco, pois o essencial é que ele se saiba vigiado; excessivo, porque ele não tem necessidade de sê-lo efetivamente (FOUCAULT, 1999, p. 224, 225).

A mera ideia de vigilância contínua, ainda que não efetivada em seu exercício, proporciona uma subjetivação do efeito da disciplina. A inovação do panóptico está nisto: a coação decorre da indução de que se está sendo observado. Assim, "uma sujeição real nasce mecanicamente de uma relação fictícia" (FOUCAULT, 1999, p. 225), não sendo mais necessário recorrer à força física para obrigar o condenado ao bom comportamento. A pessoa submetida a um campo de visibilidade, e que disso tem ciência, espontaneamente retoma as limitações do poder, fazendo-as funcionar sobre si mesma.

Segundo o filósofo francês, a aplicação desse modelo de vigilância pode ser eficaz em qualquer instituição. Escolas, hospitais, oficinas e prisões podem empregá-lo, bastando a adoção da arquitetura correta, isso é, capaz de tomar o lugar da força física. O panóptico de Bentham, encarado como uma utopia do encarceramento perfeito, é superado por Foucault. Não mais um edifício físico, o panóptico agora é "compreendido como um modelo generalizável de funcionamento; uma maneira de definir as relações do poder com a vida cotidiana dos homens" (FOUCAULT, 1999, p. 228). Em outras palavras,

> o Panóptico não deve ser compreendido como um edifício onírico: é o diagrama de um mecanismo de poder levado à sua forma ideal; seu funcionamento, abstraindo-se de qualquer obstáculo, resistência ou desgaste, pode ser bem representado como um puro sistema arquitetural e óptico: é na realidade uma figura de tecnologia política que se pode e se deve destacar de qualquer uso específico (FOUCAULT, 1999, p. 228, 229).

Foucault traz, então, a noção de "disciplina-mecanismo": o panoptismo se apresenta como "um dispositivo funcional que deve melhorar o exercício do poder tornando-o mais rápido, mais leve, mais eficaz, um desenho das coerções sutis para uma sociedade que está por vir" (1999, p. 232). Graças ao panoptismo, a disciplina deixa de se identificar com uma instituição ou com um aparelho, tornando-se ela própria um tipo de poder, culminando na formação de uma sociedade disciplinar (FOUCAULT, 1999, p. 238). No entanto, ressalva o autor que a modalidade disciplinar do poder não substituiu todas as demais. Na realidade ela se "infiltrou no meio das outras", ora desqualificando-as, ora prolongando-as, e, por fim, assegurando uma "distribuição infinitesimal das relações de poder" (FOUCAULT, 1999, p. 239).

Conquanto as contribuições de Foucault acerca do panoptismo sejam extremamente importantes, fundamentais para os debates que sucederam às suas publicações, suas análises sobre a sociedade disciplinar não refletem de forma exata seu tempo (HAN, 2018b), quiçá este que vivemos hoje. No que concerne às técnicas de poder, o pensador francês "não reconhece que o regime neoliberal de dominação se apropria completamente das tecnologias do eu" (HAN, 2018b, p. 43). O que significa dizer que, na sociedade atual, as técnicas de poder assumem formas sutis, garantindo que as pessoas ajam sobre si mesmas de forma a reproduzir o contexto de dominação dentro de si, mas interpretando-o como liberdade. Como expõe Byung-Chul Han, "aqui coincidem a otimização de si e a submissão, a liberdade e a exploração. Esse estreitamento entre liberdade e exploração na forma de exploração de si escapa ao pensamento de Foucault" (2018b, p. 44).

Diante disso, Han afirma que a sociedade digital apresenta uma estrutura panóptica especial, por ele denominada "pan-óptico digital" (HAN, 2018a, 2018b). O panóptico de Bentham expõe os prisioneiros (ou, na verdade, quem quer que se vigie) ao isolamento, pois consiste, originariamente, de células isoladas umas das outras. O pan-óptico digital, em contrapartida, pressupõe a conexão e comunicação intensa de seus habitantes. Assim, não é o isolamento espacial e comunicativo que torna possível o exercício do poder na sociedade de vigilância digital. São a hiperconexão e a hipercomunicação que tornam viável o controle total (HAN, 2018a, p. 122, 123).

Logo, os habitantes do pan-óptico digital não se enxergam como prisioneiros – nem o são, se tomada a palavra em seu sentido coloquial. Todavia, "vivem na ilusão da liberdade" (HAN, 2018a, p. 123). Diferente do que ocorre na sociedade de Oceania, descrita por Orwell em "1984", não nos deparamos a todo momento com letreiros dizendo "o Grande Irmão está de olho em você" (ORWELL, 1949, p. 2). O *Big Brother* orwelliano, apesar de nunca visto pessoalmente, vê a todos e a todos controla; no pan-óptico digital, o controle é exercido de outras maneiras. Ora é exercido mediante a coleta, o armazenamento e o processamento de informações fornecidas espontaneamente pelas pessoas, processo que Han denomina "autoexposição" (2018a, p. 124). Ora é exercido mediante esses mesmos mecanismos, mas sem o consentimento dos titulares dos dados. Ora, sem que sequer possuam ciência disso. Tais processos, por fim, muitas vezes se confundem: liberdade e controle tornam-se indistinguíveis, consumando-se a sociedade de controle (HAN, 2018a, p. 124).

O pan-óptico digital é, dessa forma, um sistema "dominado pela aparência de liberdade e comunicação ilimitadas", no qual "a transparência e a informação substituem a verdade" (HAN, 2018b, p. 56). Para o filósofo sul-coreano, "o novo objetivo do poder não consiste na administração do passado, mas no controle psicopolítico do futuro" (HAN, 2018b, p. 56). O pan-óptico digital diferencia-se do *Big Brother* de Orwell, pois, na sociedade digital, as pessoas não se sentem realmente vigiadas ou ameaçadas. Contudo, "é exatamente essa sensação de liberdade, inexistente no Estado de vigilância de Orwell, que constitui um problema" na sociedade digital (HAN, 2018b, p. 57).

Um problema ainda maior – como já pontuamos – diz respeito a quem exerce o controle no contexto do pan-óptico digital. O exercício do poder não se encontra mais atrelado necessariamente ao Estado, ou ao poder familiar, ou ao poder institucional, como descrito por Foucault. O poder de vigiar, que antes pertencia a esses entes, hoje é atribuído também às grandes corporações. Nessa conjuntura,

> a distinção entre o *Big Brother* e os prisioneiros dilui-se cada vez mais. Aqui, todos observam e vigiam a todos. Não são apenas serviços secretos do governo que nos espionam. Empresas como o Facebook ou o Google trabalham elas mesmas como serviços secretos. Elas expõem a nossa vida para conseguir capital em troca das informações espionadas. Firmas espionam os seus funcionários. Bancos examinam a fundo potenciais clientes de crédito (HAN, 2018a, p. 124).

Han aponta ainda que até as próprias coisas – os objetos que utilizamos cotidianamente – se tornaram emissoras ativas de informações sobre as pessoas. A expansão da internet das pessoas (*web 2.0*) para a internet das coisas (*web 3.0*) completa a sociedade de controle digital, pois a internet das coisas torna possível um registro quase total da vida (HAN, 2018b, p. 86). Nesse mesmo sentido, Rodotà (2013) aponta que o advento da *web 3.0* não só tornou possível a consolidação da internet das coisas, mas também tornou patente a exigência de uma nova abordagem no que concerne aos problemas da vigilância.

Explica-se: antes de tudo, a vigilância não é apenas o resultado de uma atividade deliberada e específica, mas também um subproduto do comportamento das pessoas, que cedem voluntariamente muitas informações sobre si. Em segundo lugar, a vigilância não é apenas o resultado de um tratamento consciente dos dados, mas, em um número crescente de casos, o resultado das funções atribuídas aos algoritmos. Ainda, a vigilância não visa a controlar pessoas individualmente, atividades particulares ou segmentos específicos da sociedade, mas está se tornando um procedimento universal, envolvendo as pessoas em geral. Por fim, os riscos da

vigilância não surgem principalmente das atividades dos órgãos de segurança pública, mas da coleta incessante por entes comerciais privados[105] (RODOTÀ, 2013).

Nesse contexto, Ana Frazão (2019b) elucida que essa massa de dados pessoais entregues ao controle das plataformas digitais recebeu aperfeiçoamentos de controle, armazenamento e utilização com o advento do *big data* e *big analytics*[106]. A autora enfatiza que "o *Big Data* tudo vê, sendo capaz de capturar todas as pegadas digitais dos usuários para, a partir daí, utilizar seus 'poderes' não apenas para registrar e processar o passado e o presente, como também para antecipar e decidir o futuro das pessoas" (FRAZÃO, 2019b, p. 38). Essa alta capacidade de vigilância confere às plataformas digitais o poder sobre nossas escolhas, nos influencia e nos limita em nossas atividades e experiências. Sem dúvida, expõe Han, "os *big data* tornam possível uma forma de controle muito eficiente", uma vez que

> o pan-óptico digital oferece uma visão em 360° dos seus internos. O pan-óptico de Bentham está ligado à óptica perspectivista. Desse modo, são inevitáveis pontos cegos nos quais os prisioneiros podem perseguir seus pensamentos e desejos secretos sem serem notados. A vigilância digital é mais eficiente porque é aperspectivista. Ela é livre de limitações perspectivistas que são características da óptica analógica. A óptica digital possibilita a vigilância a partir de qualquer ângulo. Assim, elimina pontos cegos. Em contraste com a óptica analógica e perspectivista, a óptica digital pode espiar até a *psique* (HAN, 2018b, p. 78).

Embora as preocupações a respeito da relação entre novas técnicas computacionais e a expansão da vigilância ostensiva tenham adquirido novas proporções nos últimos 10 anos (FLORIDI et al., 2017), Frazão esclarece que a preocupação a respeito da relação entre *big data* e a solidificação de uma sociedade de vigilância não é tão recente. Desde 2004, Richard Thomas, que à epoca era *Information Commissioner*[107] do Reino Unido, "já alertava para os

[105] No original: "But it's true data the passing to the Web 2.0 implies a fresh approach to the surveillance issues. And this is more and more true if we look at the Web 3.0, the Internet of things. First of all, surveillance is not only the result of a deliberate and specific activity, but also a by-product of the behaviour of the same individuals, leaving voluntarily a lot of informations [sic] about them. Second: surveillance is not only the result of conscious data treatment, but in an increasing number of cases the result of the place given to algorithms. Third: surveillance is not aimed to controlling single individuals, particular activities or specific segments of the society, but is becoming a universal procedure, involving the people at large. Fourth: the risks of the surveillance do not come out especially from the activities of public security agencies, but from the unrelenting collection by private, commercial bodies." (RODOTÀ, 2013)

[106] Nome dado à análise de grandes volumes de dados, que são traduzidos em informações, geralmente por meio de algoritmos.

[107] O termo "*information commisioner"* pode ser traduzido livremente como "comissário de informação". Refere-se, no Reino Unido, ao cargo responsável por desempenhar uma série de funções específicas relativas às leis sobre a proteção dos dados e a liberdade de informação (*Data Protection*

perigos do fenômeno que via ocorrendo em seu país e que descrevia como um '*sleepwalking into a surveillance society*[108]'" (FRAZÃO, 2019b, p. 27).

Para Gilliom e Monaham, uma maneira mais inteligente de se pensar sobre a vigilância hoje começa com uma nova avaliação da natureza e das implicações das constantes e crescentes mudanças, tanto as tecnológicas quanto as políticas. Isso significa analisar como a vigilância é realmente utilizada, quem a utiliza e como isso afeta nosso mundo. Significa entender a vigilância como uma forma de poder e governança entranhada no tecido de nossas vidas, e entender que a vigilância não é mais uma breve intrusão ou uma ideia assustadora de um filme, mas sim um modo de vida. Significa compreender que estamos envolvidos de tal maneira no pan-óptico digital que se torna impossível escapar da vigilância. Significa, por fim, conceber a vigilância como "*our way of life"* (GILLIOM; MONAHAN, 2013).

Os sistemas de vigilância fazem mais do que apenas assistir, observar: eles nos perscrutam. Nesse movimento, a sociedade de vigilância, hoje compreendida como um pan-óptico digital, nos molda, criando versões incompletas e "estranhas" de quem realmente somos (GILLIOM; MONAHAN, 2013). Além disso, a vigilância transforma nosso mundo ao estabelecer padrões de recompensas e punições que guiam nossas escolhas e comportamentos (pense-se, por exemplo, em *scores* de crédito ou sistemas de videomonitoramento presentes na maioria dos centros urbanos). Era esse o propósito do *Big Brother* de Orwell, do pan-óptico de Bentham e de Foucault. É esse o propósito do pan-óptico digital em que hoje vivemos.

Pensando-se especificamente em sistemas vigilância baseados em reconhecimento facial, há que se levar em consideração a importância do físico na era da informação. O corpo, como exposto alhures, volta a ser considerado um conjunto de dados, um sistema informativo, "aspecto essencial da sociedade de informação e de sua aproximação à realidade virtual" (RODOTÀ, 2004, p. 91). Isso porque

> mais recentemente, voltou-se a prestar atenção aos componentes físicos, sobretudo porque a realidade desmaterializada, em muitas situações, pode não garantir segurança na identificação do sujeito a que se quer referir. (...) Uma vez confiada a identidade unicamente a dados destituídos de qualquer relação com a pessoa concreta a que se referem, cresce o risco de furtos de identidade

and Freedom of Information Acts), que incluem a promoção da aplicação de boas práticas e o cumprimento dos princípios de ambas as leis, abrangendo igualmente o cumprimento da proteção de dados por parte dos respectivos controladores; incentivo à elaboração por terceiros de códigos de boa prática e a divulgação ao público de informações sobre as leis.

[108] Literalmente, a oração poderia ser traduzida como "sonambulando em direção a uma sociedade de vigilância".

> mediante a simples apropriação de um código numérico, de uma palavra-chave, de um algoritmo (RODOTÀ, 2004, p. 92).

Os sistemas de vigilância configuram novas e singulares expressões de poder (GILLIOM; MONAHAN, 2013), que hoje se valem não só de dados eletrônicos, mas também de dados biométricos para garantir a efetividade do exercício de tal poder. Os dados biométricos faciais, facilmente obteníveis, adquirem especial relevância na consolidação do pan-óptico digital. Neste cenário, "deterioram-se as tradicionais formas de controle social, cujo lugar é assumido, no entanto, por controles mais penetrantes e globais, tornados possíveis pelo tratamento eletrônico das informações" (RODOTÀ, 2008, p. 95). A vigilância intensificada, a integração de dados de várias fontes, o redirecionamento de dados e a governança antecipada (ilustrada pelos programas de policiamento preditivo) podem resultar em uma sociedade na qual um indivíduo seja tratado como suspeito devido a uma sequência de ações ou encontros aleatórios e inocentes, mas que foram julgados suspeitos por um sistema regulatório orientado por dados.

Para Kelleher e Tierney (2018), viver nesse tipo de sociedade mudaria nosso *status* de "cidadãos livres" para "prisioneiros", constantemente autodisciplinados pelo medo, nas formas estabelecidas no panóptico de Bentham. Ainda segundo os autores, "a distinção entre indivíduos que acreditam e agem como se estivessem livres de vigilância e indivíduos que se autodisciplinam por medo de habitar um panóptico é a principal diferença entre uma sociedade livre e um estado totalitário" (KELLEHER; TIERNEY; 2018, p. 198). É claro que um grau considerável de controle social é necessário e desejável a todas as sociedades (SOLOVE, 2008 p. 125), sendo imprescindível que se encontre um equilíbrio entre os distintos interesses em jogo. Diante disso buscaremos, nos tópicos seguintes, discutir como ficam os direitos à privacidade e à proteção de dados no contexto do pan-óptico digital.

3.3 Rediscutindo o direito à privacidade

Dificilmente alguém negaria a relevância que o direito à privacidade possui no que concerne a diversos aspectos sociais e jurídicos. Como argumenta Solove (2008), muitos reconhecem o valor da privacidade para a liberdade, a democracia, o bem-estar social e individual. Muitos reconhecem, inclusive, que vale a pena protegê-la a despeito dos custos significativos que tal proteção implica, uma vez que o compromisso da sociedade com a privacidade geralmente envolve restringir ou mesmo sacrificar interesses importantes, como a liberdade de expressão e de imprensa, a aplicação eficiente de medidas de segurança pública,

ou acesso a determinadas informações. Assim, como já apontamos, é necessário compreender em quais hipóteses a balança penderá em favor da privacidade, e em quais a favor dos intereses mencionados. Para isso é necessário que, primeiramente, saibamos o que é privacidade (SOLOVE, 2008, p. 12). Compreender *o que é privacidade* é essencial para se tomar decisões jurídicas e políticas. Mas quando protegemos a "privacidade", o que exatamente estamos protegendo?

Nas palavras de Joana Machado e Sergio Negri, "privacidade não é uma norma jurídica autoevidente, um dado" (2017, p. 370). A colocação sintetiza, de forma precisa, o que pretendemos argumentar neste tópico: que "a noção de privacidade não pode ser vista como algo unificante, como um conceito capaz de condensar padrões uniformemente difusos na coletividade" (MACHADO; NEGRI, 2017, p. 370). Certo é que privacidade e modernidade se relacionam diretamente. Partindo dessa premissa, podemos compreender como "as diversas dimensões históricas da privacidade representam respostas ao desenvolvimento das tecnologias de comunicação" (MACHADO; NEGRI, 2017, p. 370).

Na realidade, há séculos que o desenvolvimento de novas tecnologias levanta a preocupação de que a privacidade estaria sendo lentamente extirpada, mas foi a profunda proliferação de novas tecnologias de informação durante o século XX que fez com que a privacidade se tornasse "uma questão de linha de frente em todo o mundo" (SOLOVE, 2008, p. 4, tradução nossa). Se já em 1964 jornalistas afirmavam que a privacidade estava "rapidamente evaporando" (SOLOVE, 2008), no mundo atual não parece exagero dizer que essa evaporação tem ocorrido de maneira exponencial. Basta observar o avanço incontido da tecnologia e do crescimento desenfreado do poder dos governos e das grandes corporações, como buscamos demonstrar no capítulo anterior. Para Gilliom e Monaham, a "promessa que o direito à privacidade um dia ofereceu está sendo rapidamente ultrapassada (2013, p. 13)[109]".

Diante desse cenário, caso não seja rediscutido, o direito à privacidade em breve tornar-se-á completamente defasado, inútil. Para Rodotà, até mesmo "a própria palavra 'privacidade' corre o risco de se tornar inadequada, não mais capaz de singularizar corretamente a realidade que deveria representar, se restar confinada a seu significado original" (RODOTÀ, 2004, p. 97). Na árdua tarefa de solucionar os desafios que hoje emergem, tornou-se necessário abandonar antigas abordagens e referências, pois até mesmo termos recorrentes, como *big brother* e

[109] No original: "the promise that the right to privacy may have once offered is being quickly outstripped" (GILLIOM; MONAHAN, 2013, p. 13).

privacidade por vezes revelam-se insuficientes para descrever a dinâmica decorrente das novas tecnologias, das novas formas de poder e das novas políticas globais (GILLIOM; MONAHAM, 2013). Todavia, embora seja frequentemente utilizado como um termo guarda-chuva, de conceituação abstrata, o termo "privacidade" mantém sua importância devido à função heurística que assume (SOLOVE, 2008), e por isso defendemos sua utilização.

Ainda de acordo com Gilliom e Monaham (2013, p.15), dicotomias simplistas com as quais frequentemente nos deparamos podem levar a conclusões errôneas, ou, no mínimo, precipitadas: dizer que a vigilância se opõe à privacidade, ou que a segurança se opõe à liberdade seriam maneiras superficiais de se estruturar um debate. Essas dicotomias corroboram a construção de um debate dramático e apaixonado, mas em pouco ajudam quando se trata de pensar adequadamente as novas questões que decorrem do uso de novas tecnologias de vigilância. Até porque, esclarece Solove (2011, p. 2), o debate entre privacidade e segurança sempre foi enquadrado incorretamente porque a troca entre esses valores normalmente é vista como uma questão de "tudo ou nada", quando, na realidade, a proteção da privacidade não implica a destituição de medidas de segurança, exigindo "apenas" regulamentação e supervisão. Em suma, como o vocabulário estabelecido e determinadas ideias consolidadas no âmbito jurídico não são capazes de fazer justiça à nossa nova e complexa conjuntura (GILLIOM; MONAHAN, 2013, p. 15), faz-se necessária uma análise mais profunda sobre como proteger adequadamente os valores que julgamos merecedores de proteção.

Historicamente, conforme aponta Danilo Doneda (2006), a privacidade é compreendida a partir da dicotomia público-privado. Para o autor, o direito à privacidade sempre partiu de ideias sobre quais atividades deveriam ser exercidas na esfera pública e quais deveriam estar restritas ao espaço privado dos indivíduos, sendo limitado por uma compreensão de que a habitação dos indivíduos seria o local de refúgio do escrutínio público. Assim, há uma seleção entre as informações que podem ser partilhadas publicamente e aquelas que devem ser mantidas no sigilo privado. Ainda que informações da vida íntima sejam compartilhadas com maior ou menor número de pessoas, se restringem ao controle dos indivíduos e ao seu interesse de mantê-las distantes do público em geral.

Nesse contexto, a privacidade pode ser compreendida como "*right to be let alone*"[110], tal como postulado por Samuel Warren e Louis Brandeis, em seu célebre trabalho "*The Right to Privacy"* (1890, p. 195). Em outras palavras, o direito à privacidade significava a garantia

[110] Literalmente, "direito de ser deixado só".

de não violação ou invasão dos aspectos privativos de uma pessoa, tal como preceituam o artigo 5º, X da Constituição Federal[111] e o art. 21 do Código Civil[112] brasileiro ao disporem sobre a inviolabilidade da vida privada (BIONI, 2018, p. 95-96). A privacidade, em um primeiro momento, pode ser compreendida como um direito guiado pela liberdade negativa de seu titular, que decide sobre quais aspectos de sua vida estão contidos em sua esfera privada e que, portanto, são tutelados por esse direito (RODOTÀ, 2012, p. 320).

O entendimento clássico sobre o direito à privacidade como *the right to be let alone*, todavia, há tempos se revela limitado e insuficiente. Embora interligadas, "as novas dimensões da privacidade, vistas em uma perspectiva funcional, destacam-se, às vezes, da ideia original" (MACHADO; NEGRI, 2017, p. 370). Nesse sentido, Rodotà ressalta a necessidade de ampliação do conceito de direito à privacidade em uma sociedade altamente digitalizada:

> Se este é o quadro global a ser observado, não é mais possível considerar os problemas da privacidade somente por meio de um pêndulo entre "recolhimento" e "divulgação"; entre o homem prisioneiro de seus segredos e o homem que nada tem a esconder; entre a "casa-fortaleza", que glorifica a privacidade e favorece o egocentrismo, e a "casa-vitrine", que privilegia as trocas sociais; e assim por diante. Essas tendem a ser alternativas cada vez mais abstratas, visto que nelas se reflete uma forma de encarar a privacidade que negligencia justamente a necessidade de dilatar esse conceito para além de sua dimensão estritamente individualista, no âmbito da qual sempre esteve confinada pelas circunstâncias de sua origem (RODOTÀ, 2008, p. 25).

A privacidade no âmbito da comunicação eletrônica pode se manifestar também como a necessidade de anonimato e de ter controle sobre as próprias informações:

> Em uma dimensão que se torna cada vez mais diferenciada e complexa, a demanda por privacidade não se manifesta apenas na sua forma tradicional, como direito de impedir aos outros a coleta e a difusão de informações sobre o interessado. No âmbito da comunicação eletrônica, ela pode se exprimir sobretudo como uma necessidade de anonimato ou, melhor dizendo, como exigência de assumir a identidade preferida, apresentando-se com um nome, um sexo, uma idade que podem ser diferentes daqueles efetivamente correspondentes aos dados do indivíduo. Requer-se assim a tutela de uma identidade nova, de uma intimidade construída, como condição necessária

[111] "Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

[112] "Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma."

> para o desenvolver a própria personalidade, para alcançar plenamente a liberdade existencial (RODOTÀ, 2008, p. 116).

O processo evolutivo do conceito de "direito à privacidade", portanto, vai desde a ideia de ser deixado só até uma compreensão de direito de controle sobre as informações pessoais e de construção da esfera privada. Assim, a evolução do direito à privacidade envolve necessariamente a proteção de dados pessoais (RODOTÀ, 2008, p. 17), implicando uma transformação do conceito, que passa a abarcar, além do poder de exclusão (ou seja, de impedimento de interferências alheias), a centralidade do controle do indivíduo sobre suas informações pessoais. Enquanto a influência da tecnologia dos computadores levou à reconceituação da privacidade como o "direito a controlar o uso que os outros façam das informações que me digam respeito", os avanços tecnológicos mais recentes fizeram surgir "um outro tipo de definição, segundo o qual a privacidade se consubstancia no 'direito do indivíduo de escolher aquilo que está disposto a revelar aos outros'" (RODOTÀ, 2008, p. 74). A concepção de privacidade caminhou da sequência "pessoa-informação-sigilo" para "pessoa-informação-circulação-controle" (RODOTÀ, 2008, p. 93). Nas palavras de Machado e Negri,

> (...) o direito à autodeterminação informativa ganha cada vez mais espaço e autonomia. Nesse processo de constante expansão e criação de novos direitos, a própria noção de privacidade é constantemente redefinida para se adaptar a novas situações (2017, p. 370, 371).

Sem embargo, devemos reconhecer as limitações da concepção da privacidade como o direito de controle sobre informações pessoais. Para Solove (2008, P. 24), atribuir como característica principal do direito à privacidade a capacidade de controlar o acesso a informações limita o seu escopo, pois não leva em consideração aspectos da privacidade que não são puramente informativos, tais como o direito de uma pessoa tomar decisões sobre seu corpo, ou decidir sobre a criação de seus filhos. Além disso, a conceituação de privacidade como direito de controle sobre informações pessoais "é muito vaga porque falha em definir os tipos de informações sobre as quais os indivíduos devem ter controle" (SOLOVE, 2008, p. 24).

Ainda segundo o autor, privacidade não é simplesmente uma prerrogativa individual, um assunto meramente subjetivo (SOLOVE, 2008, p. 25). É também uma questão do que determinada sociedade considera digno de proteção. Além disso, como argumenta Paul Schwartz (apud. SOLOVE, 2008, p. 29), é errado presumir que as pessoas possuem autonomia para exercer o controle sobre seus dados em todas as situações. Schwartz esclarece que até mesmo a autodeterminação individual seria moldada pelo processamento de dados pessoais, de modo que a própria capacidade de tomada de decisão seria reduzida pelas disparidades de

conhecimento e poder de barganha no que diz respeito ao uso e controle de informações pessoais. Daí podemos concluir que a privacidade envolve não somente o controle individual, mas também a regulamentação social da informação (SOLOVE, 2008, p. 30).

Assim sendo, é preciso compreender como as esferas pública e privada se organizam em uma sociedade digital. Para Gary Marx (2001), as concepções de "público" e "privado" são fluidas e contextuais, e seus significados variáveis, a depender das situações em que são discutidas. No que tange à concepção de "privado", Solove acertadamente aponta que aquilo que consideramos privado muda com o decorrer do tempo:

> Embora alguma forma de dicotomia entre público e privado tenha sempre existido ao longo da história da civilização ocidental, os assuntos considerados públicos e privados evoluíram devido a mudanças de atitudes, instituições, condições de vida e tecnologia. Os assuntos que consideramos privados são moldados pela cultura e pelo tempo e diferem entre sociedades e épocas (SOLOVE, 2008, p. 50, tradução nossa).

Já no que se refere à importância do "público", concordamos com Byung-Chul Han, quando afirma que o alicerce da esfera pública é o respeito. A esfera pública pressupõe "um não olhar para a vida privada" (HAN, 2018a, p. 12), sendo a tomada de distância elemento constitutivo do espaço público. Hoje, porém, "domina uma falta total de distância, na qual a intimidade é exposta publicamente e o privado se torna público". Tal falta de distância leva à confusão entre privado e público, alimentada principalmente pela comunicação digital, que "fornece essa exposição pornográfica da intimidade e da esfera privada" (HAN, 2018a, p. 13).

Destarte, especialmente em relação ao tema aqui tratado, *i.e.*, a utilização de sistemas de reconhecimento facial baseados em IA para fins de controle, é importante apontar que o simples "fato de participarmos desta época é suficiente para que soframos constante vigilância, através de câmeras, sensores e o monitoramento dos dados que produzimos diariamente, seja em redes sociais, ou através do uso dos dispositivos conectados à Internet das coisas (IoT)" (SOUZA, 2018, p. 577). Isso significa que, voluntária ou involuntariamente, vivemos sob o constante monitoramento possibilitado pelo avanço tecnológico. Voluntariamente, pois em diversas ocasiões cedemos "livremente" nossos dados pessoais ao governo e a corporações privadas; involuntariamente, pois em diversas outras situações encontramo-nos vigiados, sem que a nós seja dada a oportunidade de consentirmos no que diz respeito a tal vigilância. Assim, ora abrimos mão da nossa esfera privada, ora ela nos é extirpada.

Nesse sentido, John Gilliam e Torin Monaham (2013) dissertam sobre como diferentes abordagens sobre a privacidade são apresentadas quando intelectuais e juristas tentam usar a ideia de privacidade para discorrer sobre os problemas e eventuais danos decorrentes da vigilância. Às vezes, a privacidade é percebida como o direito de ser deixado só; outras vezes, como o direito de controlar informações sobre si mesmo; e em outras como um valor social referente à autonomia de grupos, famílias e indivíduos. Obviamente, elucidam os autores, a privacidade tem grande relevância quando se discutem sistemas de vigilância, sendo um direito que definitivamente terá importância permanente nas lutas jurídicas e políticas que busquem regulamentar práticas de vigilância (GILLIOM; MONAHAN, 2013, p. 146). Não obstante, um número crescente de especialistas em vigilância tem deixado de enquadrar seu trabalho dentro do que poderia ser chamado de "paradigma da privacidade". Isso não quer dizer que a privacidade não é mais valorizada, ou que é irrelevante para explicar os desafios da vigilância, mas sim que a privacidade entendida em seu conceito tradicional deve dar lugar a um entendimento mais flexível, diversificado e atualizável da dinâmica de poder e vigilância atual.

Quando a vigilância caracteriza quase todos os aspectos da vida social, mas a maioria das práticas de vigilância não é democrática, estamos logicamente nos movendo em direção a uma sociedade menos democrática (GILLIOM; MONAHAN, 2013). É o que indica Ana Frazão, ao discorrer sobre a importância dos efeitos discriminatórios das decisões tomadas por inteligências artificiais:

> Importante considerar, também, que, diante das preocupações com os efeitos discriminatórios das decisões algorítmicas, especialmente quando totalmente automatizadas e sem qualquer tipo de controle ou intervenção humana, as discussões sobre privacidade também passam a estar conectadas cada vez mais com a igualdade (FRAZÃO, 2019c, p. 107).

A privacidade é, afinal, "uma construção que permanece em disputa e sujeita a constantes redefinições" (MACHADO; NEGRI, 2017, p. 372). Tal qual expõe Ana Frazão, não é possível definir "nem mesmo um conceito essencial ou um denominador comum para a definição de privacidade" (FRAZÃO, 2019c, p. 105). Em várias situações, se faz necessário transcender as noções tradicionais de privacidade. Ou, ao menos, enxergá-las em conexão com outros direitos ou garantias fundamentais. Compreender, pois, as múltiplas facetas desse direito é fundamental para que se reconheça quão complexas são as discussões hodiernas em torno daquilo que consideramos "privacidade" (FRAZÃO, 2019c).

Atualmente emergem novos desdobramentos no que tange à privacidade, como aponta Nadezhda Purtova (2018). É necessário ainda se discutir os *information-induced harms* (em

tradução livre, “danos causados pela informação”), que devem ser entendidos amplamente como qualquer consequência negativa, pública ou individual, do processamento de informações. Aliás, cabe dizer: a própria definição de dados pessoais sensíveis “está ligada muito mais à proteção da igualdade e da não discriminação do que propriamente à intimidade” (FRAZÃO, 2019c, p. 107). Para Rodotà, a inclusão de dados pessoais biométricos como dados pessoais sensíveis “deriva de sua potencial inclinação para serem utilizados com finalidades discriminatórias” (2008, p. 96), tornando-os merecedores de maior proteção.

À vista disso, também a discussão sobre o uso de tecnologias de vigilância baseadas em reconhecimento facial deve ir além da discussão sobre violações à privacidade em seu sentido tradicional. À proteção da privacidade estão ligadas a tutela da liberdade e a própria preservação da individualidade da pessoa (FRAZÃO, 2019c). O aspecto do direito à privacidade como direito à intimidade não é o único afetado pelo uso de tais tecnologias. O debate acerca de como TRFs afetam o direito à intimidade precisa, afinal, “ceder espaço” para outros debates igualmente importantes, como a violação do direito à igualdade, à liberdade e até mesmo à democracia, como se verá a seguir.

3.3.1 Como o reconhecimento facial afeta a privacidade?

Antes de respondermos à pergunta acima, cabe realizarmos um retorno à teoria da privacidade[113] apresentada por Solove (2008), para quem a privacidade deve ser compreendida a partir de uma abordagem pragmática. Isso significa dizer que o ponto focal da teoria da privacidade deve ser os problemas que desejamos que a lei busque solucionar mediante a sua aplicação (SOLOVE, 2008, p. 75). Nas palavras do autor:

> Um problema referente à privacidade interfere em atividades específicas, e o valor dado à proteção contra esse problema decorre da importância de salvaguardar as atividades nas quais o problema interferiu. Depois de identificado o interesse pela proteção da privacidade e seu valor, o próximo passo é ponderar o interesse pela privacidade em relação ao valor de quaisquer interesses contrários. Práticas que causam problemas à privacidade

[113] Solove apresenta uma teoria da privacidade baseada em quatro dimensões principais: método, grau de generalidade, variabilidade e foco. No que diz respeito ao método, Solove, valendo-se da noção de “família de semelhanças” de Wittgenstein, afirma que a privacidade não é *uma* “coisa”, mas sim um conjunto de coisas distintas que estão relacionadas. Sobre a generalidade, o autor afirma que as questões atinentes à privacidade devem ser endereçadas contextualmente, em detrimento de uma abordagem abstrata. No que se refere à variabilidade, Solove argumenta que a noção de privacidade deve ser flexível o suficiente para se adaptar ao caráter dinâmico e em constante evolução que possui. Por fim, no que concerne ao foco, defende que, em vez de ponderarmos a natureza da privacidade no abstrato, devemos partir de problemas concretos e partir daí utilizar a teoria desenvolvida como uma melhor maneira de entender e resolver esses problemas (SOLOVE, 2008, p. 40, 41).

> geralmente não são totalmente negativas - elas trazem benefícios. Depois de ponderarmos o interesse pela privacidade contra o dano, podemos determinar como a privacidade deve ser protegida em um caso específico. Em alguns casos, a privacidade pode superar o interesse compensatório ou vice-versa (SOLOVE, 2008, p. 76, tradução nossa)[114].

Em muitos casos, prossegue Solove, é possível encontrar um equilíbrio, uma solução que proteja tanto a privacidade quanto os interesses conflitantes. Mas, ressalva, "esse equilíbrio depende primeiro da identificação dos interesses da privacidade, e é aqui que a lei e a política geralmente se perdem" (SOLOVE, 2008, p. 76, tradução nossa). Os problemas referentes à privacidade surgem, assim, quando as atividades de governos, empresas, organizações e pessoas interrompem as atividades das demais pessoas (SOLOVE, 2008, p. 76). Em relação ao valor da privacidade, o autor afirma que devemos compreendê-lo em termos de suas consequências práticas: a privacidade deve ser ponderada contra valores conflitantes e deve prosperar quando produzir o melhor resultado para a sociedade (SOLOVE, 2008, p. 87).

Nesse sentido, Rodotà (2011) pontua que os regimes democráticos atuam, ou deveriam atuar, consoante lógicas distintas àquelas dos regimes totalitários, "baseando as possíveis limitações à privacidade no princípio democrático" (RODOTÀ, 2011, p. 16, tradução nossa). Em uma sociedade democrática, somente são admissíveis limitações da privacidade que se revelem verdadeiramente necessárias. Desse modo, se estabelece uma "firme relação entre democracia e respeito à vida privada", e qualquer medida que busque limitar a privacidade só será legítima se superar o "teste da democracia" (RODOTÀ, 2011, p. 16, tradução nossa).

Diante disso, podemos reformular a pergunta apresentada no título deste tópico do seguinte modo: como ponderar as liberdades individuais, especificamente o direito à privacidade, e a crescente busca pela segurança pública e demais interesses sociais? Para John Kelleher e Brendan Tierney (2018, p. 181), no contexto de uma *data-driven society*[115], essa antiga questão poderia ser colocada da seguinte maneira: o que nós, enquanto sociedade, enxergamos como meios razoáveis de coletar e utilizar dados pessoais em contextos diversos, como combater o terrorismo, melhorar a medicina, apoiar pesquisas públicas, combater crimes,

---

[114] No original: A privacy problem disrupts particular activities, and the value of protecting against the problem stems from the importance of safeguarding the activities that are disrupted. After identifying the privacy interest and its value, the next step is to weigh the privacy interest against the value of any countervailing interests. Practices that cause privacy problems often are not wholly negative—they have benefits. Once we weigh the privacy interest against the harm, we can determine how' privacy should be protected in a particular case. In some instances, privacy might outweigh the countervailing interest or vice versa (SOLOVE, 2008, p. 76).

[115] A expressão poderia ser traduzida livremente como "sociedade orientada por dados".

detectar fraudes, avaliar riscos de crédito, providenciar subscrições para seguros e promover propagandas direcionadas a grupos específicos?

Segundo os autores, se absorvermos ainda que uma fração do frenesi comercial que envolve a ciência de dados, teríamos a sensação de que qualquer problema pode ser resolvido usando tecnologias de ciência de dados, desde que se disponham de dados suficientes (KELLEHER; TIERNEY, 2018). Esse *marketing* do poder da ciência de dados alimenta a visão de que uma abordagem de governança baseada em dados é a melhor maneira de lidar com problemas sociais complexos, como pobreza, saúde pública, falta de investimento em educação e criminalidade. Assim, tudo o que precisaríamos fazer para resolver esses problemas é colocar sensores em nossas sociedades para rastrear tudo, mesclar todos os dados e executar os algoritmos apropriados para gerar os *insights* que forneceriam a solução para essas questões. Quando essa ideia é aceita, alguns processos são frequentemente intensificados: soluções tecnológicas se imbricam cada vez mais ao cotidiano; a coleta de dados se torna expande; o processamento de informações se torna mais expressivo.

O primeiro desses processos, portanto, refere-se ao fato de que as sociedades têm se tornado mais tecnocráticas, com diversos aspectos da vida sendo regulados por sistemas orientados por dados. Como subproduto dessa regulação tecnocrática, tem-se a proliferação dos sensores que suportam os sistemas de regulação automatizados (KELLEHER; TIERNEY; 2018, p. 196). Para exemplos de como esse fenômeno se manifesta em diversas sociedades atuais, basta um breve retorno ao capítulo anterior.

O segundo processo, por sua vez, concerne à coleta de dados pessoais. Para Solove (2008), embora nem toda coleta de dados[116,117] constitua uma atividade danosa à privacidade, a

[116] Solove utiliza a expressão "*information collection"*, cuja tradução é "coleta de informações". Todavia, aqui fazemos alusão aos ensinamentos de Doneda (2006), que diferencia os termos "dado" e "informação". Em suas palavras, "o dado estaria associado a uma espécie de 'pré-informação', anterior à interpretação e ao processo de elaboração. (...) Sem aludir ao significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega em si também um sentido instrumental, no sentido de uma redução de um estado de incerteza" (DONEDA, 2006, p. 152).

[117] Para Floridi (2005), podemos compreender "informação" como um conteúdo semântico, desde que composto de um ou mais dados, desde que devidamente agrupados e com sentido. Assim, uma informação necessariamente é composta por dados, ou, no mais simples dos casos, por apenas um dado. Nas palavras do autor: "*It is common to think of information as consisting of data. It certainly helps, if only to a limited extent. For, unfortunately, the nature of data is not well-understood philosophically either, despite the fact that some important past debates—such as the one on the given and the one on sense data—have provided at least some initial insights. There still remains the advantage, however, that the concept of data is less rich, obscure and slippery than that of*

coleta de dados pessoais pode por si só ocasionar violações a esse direito, independentemente de as informações decorrentes da coleta serem publicamente reveladas. Vale notar que a coleta de dados ocorre de duas formas principais, mediante atividades de *vigilância* ou de *interrogação* (SOLOVE, 2008, p. 102-104). Importa-nos, neste momento, a primeira.

A atividade de vigiar consiste em "assistir, ouvir ou registrar as atividades de um indivíduo" (SOLOVE, 2008, p. 104), o que ocorre cotidianamente, como buscamos expor no capítulo 2. O problema ocorre quando a vigilância é empregada de maneira excessiva ou desproporcional, gerando um estado de monitoramento contínuo. Devido a seus efeitos inibitórios, a vigilância pode ser uma ferramenta de controle social – o que não a torna automaticamente prejudicial, uma vez que o controle social pode ser benéfico e toda sociedade necessita exercê-lo em um grau considerável. O excesso de controle, no entanto, é claramente nocivo e incabível em uma democracia (RODOTÀ, 2011), pois pode afetar negativamente a liberdade, a criatividade e o autodesenvolvimento (SOLOVE, 2008, p. 108, 2011, p. 178-180).

A vigilância, e notadamente a vigilância operada mediante reconhecimento facial, é também uma forma abrangente de poder investigatório. Ela se estende para além de meras "buscas", pois registra comportamentos, interações sociais e potencialmente tudo o que uma pessoa faz (SOLOVE, 2008, p. 109). Em vez de se restringir à coleta de dados específicos, a vigilância pode ensejar a apreensão de uma quantidade significativa de informações que extrapola o limite do razoável; em outras palavras, a vigilância não apenas busca informações de maneira direcionada, mas também funciona como uma "rede de arrasto", recolhendo uma quantidade significativa de dados além do que originalmente se pretendia investigar (SOLOVE, 2011, p. 179). Adicionalmente, ao contrário de uma atividade investigativa tradicional, que geralmente ocorre uma única vez, a vigilância eletrônica opera de modo permanente (SOLOVE, 2011, p. 179), o que pode acarretar a normalização de um estado de exceção.

Ademais, devemos considerar que um sistema de vigilância dotado de um número expressivo de câmeras de segurança, *softwares* de reconhecimento facial e amplas bases de dados pode facilmente se tornar uma ferramenta para o rastreio dos movimentos de qualquer pessoa (SOLOVE, 2011). A vigilância, principalmente aquela que ocorre em público, operada por entidades governamentais, pode ainda ter um efeito inibitório (SOLOVE, 2008, 2011), o que torna as pessoas menos propensas a se associar a determinados grupos, a participar de

---

information, and hence easier to handle. (...) information cannot be dataless but, in the simplest case, it can consist of a single datum" (FLORIDI, 2005).

comícios ou a simplesmente se exporem publicamente. O efeito inibitório da vigilância é especialmente pujante quando as pessoas estão envolvidas em protestos ou dissidências políticas, pois, se identificadas, podem enfrentar perseguição, sanções públicas e até mesmo serem enquadradas em "listas negras" devido às suas opiniões divergentes (SOLOVE, 2011, p. 179).

O terceiro e último processo ao qual voltaremos nossa atenção está relacionado ao processamento de informações, que Solove define como "o uso, armazenamento e manipulação de dados que foram coletados" (SOLOVE, 2008, p. 117, tradução nossa). Assim, o processamento de informações não envolve a coleta de dados, dizendo respeito apenas ao modo como dados já coletados são tratados, o que se dá de cinco formas diferentes: combinação[118], identificação, uso secundário, inseguridade[119] e exclusão (SOLOVE, 2008). Embora todas as formas possam de algum modo interferir no direito à privacidade, discorreremos brevemente sobre as três primeiras.

A combinação é o agrupamento de dados e/ou informações sobre uma pessoa. Nas palavras de Solove, "uma informação específica aqui ou ali não é muito reveladora, mas, quando combinados, *bits* e dados começam a formar o retrato de uma pessoa", pois "o todo se torna maior que as partes" (SOLOVE, 2008, p. 118, tradução nossa). Quando analisadas conjuntamente, determinadas informações podem revelar novos fatos sobre uma pessoa, os quais ela possivelmente não esperava que fossem conhecidos no momento de coleta de seus dados. Aliás, é importante mencionar que as pessoas esperam certos limites sobre o que é conhecido sobre elas (SOLOVE, 2008). Em outras palavras, expomos seletivamente nossos dados e informações porque possuímos uma expectativa quanto à profundidade de conhecimento que as demais pessoas, empresas e governo irão adquirir sobre nós. Todavia, não nos damos conta de que, quando combinados, esses dados permitirão que aquele que os agregou possua muito mais conhecimento sobre as nossas vidas do que originalmente esperávamos. Dessa forma, a combinação pode ampliar o poder que alguém tem sobre outra pessoa, visto que o "dossiê" criado a partir desse recurso frequentemente é utilizado para julgá-la (SOLOVE, 2008, p. 119).

Identificação, como o próprio termo indica, consiste em conectar informações a uma determinada pessoa. Nas palavras de Roger Clarke (apud SOLOVE, 2008, p. 122),

[118] Solove utiliza o termo "*aggregation*" (SOLOVE, 2008, p. 117).
[119] Solove utiliza o termo "*insecurity*" (SOLOVE, 2008, p. 117).

"identificação é a associação de dados com um ser humano em particular". A identificação nos permite tanto verificar a identidade de uma pessoa em situações corriqueiras, como realizar um saque em uma agência bancária ou assinar um contrato, quanto, por exemplo, descobrir a autoria de um crime a partir de vestígios deixados para trás (SOLOVE, 2008, p. 112, 113). Além de necessária, a identificação é, em muitos casos, benéfica, pois reduz o risco de fraudes, conferindo legitimidade a diversos procedimentos. Mas a identificação pode, igualmente, afetar a estrutura social ao aumentar o nível de conhecimento – e, consequentemente, de controle – que o governo possui sobre seus jurisdicionados. Recorrer à identificação sempre foi uma ferramenta crucial para governos radicais que objetivam detectar dissidentes, radicais ou cidadãos desfavorecidos, configurando-se, portanto, como um meio eficiente para controlar as pessoas (SOLOVE, 2008, p. 135). Ademais, a identificação, por conectar pessoas aos seus respectivos dados, acaba por "amarrar" uma "bagagem informacional" a elas (SOLOVE, 2008, p. 124), como veremos mais adiante[120].

O uso secundário de dados, ao qual Kelleher e Tierney (2018) referem-se como "*control creep*", consiste no redirecionamento de dados coletados para um propósito para outro que não o propósito original. Kelleher e Tierney ilustram esse fenômeno com o seguinte exemplo: câmeras rodoviárias foram instaladas em Londres com o objetivo principal de regular o congestionamento e implementar taxas de congestionamento, mas foram redirecionadas para tarefas de segurança (KELLEHER; TIERNEY, 2018, p. 196). Outro exemplo de uso secundário de dados é a tecnologia chamada *ShotSpotter,* que consiste em uma rede de microfones em toda a capital inglesa, projetada para identificar tiros e relatar suas localizações, mas que também registra conversas, algumas das quais foram usadas para obter condenações criminais. Há, ainda, o uso de sistemas de navegação veicular para monitorar e multar os motoristas de carros alugados que saem de determinado estado (KELLEHER; TIERNEY, 2018, p. 196).

Um aspecto relevante do uso secundário é a possibilidade de se cruzar dados de diferentes fontes, a fim de fornecer uma imagem mais completa de uma sociedade e, assim, potencialmente desbloquear *insights* mais profundos sobre os problemas nela existentes (SOLOVE, 2008). Muitas vezes, são apresentadas "boas razões" para redirecionar os dados, de modo que frequentemente são feitos pedidos para que dados mantidos por diferentes ramos do governo sejam cruzados para fins legítimos – como para embasar pesquisas em saúde, ou em

[120] O tema será tratado com maior profundidade no item "3.4.1 – Dados que deixam rastros" do presente trabalho.

determinadas investigações criminais. Do ponto de vista das liberdades civis, no entanto, essas tendências são muito preocupantes (KELLEHER; TIERNEY, 2018, p. 197).

Isso porque o recurso maciço a soluções baseadas em dados biométricos é, ao fim e ao cabo, uma "panaceia tecnológica" (RODOTÀ, 2004), sendo que a opinião pública, como já argumentado, tende a superestimar sua precisão, associando impropriamente tais tecnologias a uma proteção absoluta contra o terrorismo e a criminalidade (RODOTÀ, 2004, p. 99). Para Rodotà, essa falsa certeza é atualmente associada a um "progressivo mitridatismo[121] social", o que significa dizer que a difusão e a consolidação do uso de recursos biométricos em situações além das necessárias fazem com que as pessoas "percam, progressivamente, a sensibilidade necessária para prevenir os riscos para sua privacidade, para a tutela de sua liberdade pessoal" (RODOTÀ, 2004, p. 100). Nesse processo,

> a sociedade fica anestesiada em razão do esmaecimento crescente das percepções acerca da perda de controle exclusivo do próprio corpo. E estas considerações referentes aos dados biométricos têm um significado mais geral relativamente ao conjunto de tecnologias às quais, abandonando-se a uma perigosa derivação cultural e política, se deseja sempre mais delegar a solução de complexos problemas sociais (RODOTÀ, 2004, p. 100).

Dessa "anestesia" decorre a consolidação de um controle institucional, visado por governos e empresas privadas e realizado mediante a parceria desses entes (GILLIOM; MONAHAN, 2013; HAN, 2018a; RODOTÀ, 2008). Como muito dos dados são coletados, armazenados e utilizados sem a ciência e o consentimento de seus titulares, "as pessoas não podem refutar ou mesmo saber as evidências que são usadas contra elas, com o que se inibe o dissenso e a mudança social e ainda se abre margem para enorme potencial de manipulação" (FRAZÃO, 2019b, p. 40). O processo de classificação referido por Rodotà (2004; 2008) torna-se, portanto, uma importante ferramenta de demarcação do poder, uma vez que os algoritmos hoje armazenam e definem nossas "identidades datificadas" (CHENEY-LIPPOLD apud FRAZÃO, 2019b, p. 35). Essa "organização do conhecimento e da vida" acaba por moldar "as condições e as possibilidades daqueles que serão classificados" (FRAZÃO, 2019b, p. 35).

Não é exagero, portanto, dizer que os sistemas de vigilância hoje se revelam como novas expressões de poder (GILLIOM; MONAHAN, 2013). Tais sistemas são capazes de coletar e

[121] O mitridatismo é a prática de imunização contra determinado veneno ou patógeno mediante a ministração gradual e contínua de doses não letais da substância.

armazenar imensuráveis quantidades de dados; além disso, realizam a análise e o cruzamento dessas informações. E, tal qual destacado anteriormente, fazem mais do que apenas assistir:

> efetivamente, trabalham para moldar nossas identidades e nos categorizar por meio de padrões sociais existentes e ainda vinculados a desigualdades de raça, classe e gênero para que, a partir daí, passemos a ser tratados diferentemente e a ter nossas escolhas e comportamentos alterados mediante premiações e punições (FRAZÃO, 2019b, P. 40)

Nesse movimento de escrutínio dos cidadãos, é possível perceber claramente como os sistemas de vigilância – especialmente, para nós, as tecnologias de reconhecimento facial – afetam o direito à privacidade em seu sentido clássico. A privacidade, entendida como direito à intimidade e como "direito de ser deixado só" (WARREN; BRANDEIS, 1890), é nítida e negativamente atingida por sistemas que perscrutam o indivíduo, o qual sequer pode "se defender" das invasões continuamente operadas nos mais diversos contextos.

Claramente, a privacidade hoje não se restringe à noção de intimidade e ao direito a ser deixado só. Acertadamente expõe Ana Frazão que "a ampliação do direito à privacidade e a sua maior imbricação com outros direitos fundamentais não afasta, de forma alguma, a importância do sentido clássico de privacidade como intimidade" (2019c, p. 109). Para a autora, "é inequívoco que a privacidade continua a ser importante referencial para o endereçamento do problema do tratamento dos dados pessoais, o que torna necessária a reflexão sobre o seu real sentido na atualidade" (FRAZÃO, 2019c, p. 104). Os domínios da privacidade, agora ampliados, abrangem o controle sobre as informações que digam respeito à pessoa, bem como o direito à liberdade, à igualdade e à não discriminação (RODOTÀ, 2008; FRAZÃO, 2019c), e também nesses aspectos da privacidade enxergamos ameaças e/ou violações postas pelas tecnologias de reconhecimento facial.

No que tange à liberdade, é necessário considerar que as tecnologias de reconhecimento facial permitem que se extraia do corpo físico um elemento que dele é constitutivo: a biometria. Se dessa extração decorrem vigilância ostensiva e monitoramento constante, extingue-se o agir livre, e, consequentemente, a liberdade individual. Isso porque, nas palavras de Snowden (2014), "sob observação, nós agimos de maneira menos livre, o que significa que somos efetivamente menos livres"[122]. Sem a tutela efetiva da privacidade, uma sociedade não se pode dizer verdadeiramente democrática (RODOTÀ, 2011). Em relação à igualdade e à não

[122] No original: "Under observation, we act less free, which means we effectively are less free" (SNOWDEN, 2014).

discriminação, as colocações realizadas em momentos anteriores da presente pesquisa[123] ilustram de maneira precisa como tecnologias de reconhecimento facial afetam tais aspectos da privacidade.

3.4 O direito à proteção de dados

Outra importante questão diz respeito ao direito à proteção dos dados pessoais. Como acertadamente afirmam Machado e Negri, "na sociedade de informação, a proteção de dados se descolou, paulatinamente, do próprio discurso abstrato da privacidade" (2017, p. 370). Isso não significa que a proteção de dados pessoais é uma simples extensão do processo evolutivo do conceito de privacidade, mas indica que se estabelece como um direito autônomo, que necessita clareza e especificidade normativa (COSTA; OLIVEIRA, 2019, p. 10). Logo, mesmo que proteção de dados esteja evidentemente relacionada à tutela da privacidade, o direito à proteção de dados encontra-se ainda mais afastada da dicotomia do público e do privado[124]. Suas fundamentações e razões de ser são distintas. Nesse ponto, o direito à privacidade diferencia-se essencialmente do direito à proteção de dados, sendo um equívoco dogmático indicar a proteção de dados pessoais como uma mera evolução do direito à privacidade (BIONI, 2018, p. 98-99).

Nas sociedades digitais, o tratamento de dados tem se tornado cada vez mais expansivo, impactando cada vez mais pessoas e realidades sociais. Em tal contexto, a proteção de dados pessoais ergue-se como a tutela da "própria dimensão relacional da pessoa humana" (BIONI, 2018, p. 99). Uma vez que o direito à privacidade é atrelado a uma divisão das esferas pública e privada da vida, o vasto leque de liberdades individuais relacionados à proteção de dados pessoais extrapola os limites da tutela do direito à privacidade (BIONI, 2018). Como expõe

---

[123] O tópico "2.3 – Questões atinentes às tecnologias de reconhecimento facial" discute especificamente sobre como novas tecnologias podem afetar o direito à privacidade no que diz respeito à igualdade e à não discriminação.

[124] Não compreendemos o direito à privacidade como um direito individual, constantemente em tensão com os interesses comuns, como nos termos postos pelo liberalismo tradicional, pois compreender a privacidade somente em seus aspectos individuais faz com que o direito à privacidade seja depreciado (SOLOVE, 2008, p. 89). Também não compreendemos a privacidade como um direito individual que necessariamente se opõe aos interesses da sociedade e ao bem comum, como trazido pela crítica comunitarista à privacidade. Parece-nos mais apropriada a compreensão de Solove, para quem é necessária uma abordagem pragmática do direito à privacidade. Para o autor, embora a privacidade proteja os interesses de um indivíduo, não significa que seja um direito meramente individualista. Entender a privacidade como tendo um valor social não implica a oposição do indivíduo em relação à comunidade: a privacidade protege aspectos da individualidade que possuem um alto valor social; "protege os indivíduos não apenas pelo bem deles, mas também pelo bem da sociedade" (SOLOVE, 2008, p. 92).

Mulholland (2018, p. 171), o direito à privacidade é o *locus* constitucional da proteção de dados de dados pessoais, uma vez que "os dados são elemento constituinte da identidade da pessoa e que devem ser protegidos na medida em que compõem parte fundamental de sua personalidade, que deve ter seu desenvolvimento privilegiado, por meio do reconhecimento de sua dignidade". Contudo, o direito à proteção de dados não se confunde com o direito à privacidade, tampouco nele se esgota.

Segundo Ana Frazão, muito mais do que um problema apenas de privacidade, a proteção de dados é fundamento para a preservação da individualidade, da liberdade e da própria democracia (FRAZÃO, 2019b, p. 38). Fato é que a proteção dos dados pessoais atualmente constitui um dos aspectos mais significativos da liberdade das pessoas (RODOTÀ, 2004). Todavia, não se trata de uma ideia abstrata de liberdade. Pelo contrário, as garantias referentes à proteção de dados devem sempre estar imbricadas à pessoa a quem essas garantias devem se referir. Destarte, faz-se imprescindível considerar que "um outro corpo está diante de nós – fragmentável, multiplicável, manipulável, falsificável – e é este novo corpo que torna possíveis novas formas de controle, e exige portanto novas e mais potentes garantias" (RODOTÀ, 2004, p. 106). Isso porque as novas tecnologias de coleta e processamento de dados biométricos permitiram que se superasse a dicotomia existente o corpo físico e o corpo eletrônico, fazendo com que, novamente, o corpo e a liberdade pessoal a ele relativa se apresentem "no palco do mundo como a premissa para um agir livre" (RODOTÀ, 2004, p. 106).

Nas sociedades hiper conectadas, "a estreita relação entre o desenvolvimento mais recente dos mecanismos de inteligência artificial com a maior disponibilidade de informação deixou seus reflexos na regulação que começou a ser concebida em relação à proteção de dados pessoais", como expõem Doneda et al. (2018). Ainda segundo os autores,

> recentemente, o desenvolvimento e a implementação de tecnologias de inteligência artificial (IA) proporcionou efeitos que, muitas vezes, não podem mais ser compreendidos em termos meramente quantitativos, e que implicam uma mudança na subjetividade das relações entre as pessoas e a tecnologia" (DONEDA et al., 2018, p. 2).

Essa mudança de subjetividade, pontua-se, não se restringe à seara econômica. Indo além, apresenta inúmeras repercussões nas esferas pessoais dos cidadãos, culminando na "total reestruturação das relações sociais e políticas" (FRAZÃO, 2019b, p. 24). Nos últimos anos, cresceu a consciência da proteção dos dados pessoais como aspecto essencial da liberdade pessoal e a proteção de dados, por conseguinte, adquiriu "importância transversal" (RODOTÀ,

2004), tornando-se instrumento de salvaguarda das vidas e liberdades individuais, bem como da própria sociedade e da noção de democracia (FRAZÃO, 2019b).

Assim, num contexto de modificações significativas na relação entre ser humano e tecnologia, emerge uma nova concepção integral da pessoa: conforme exposto alhures, o corpo é, ao mesmo tempo, físico e eletrônico. E a projeção da pessoa no mundo corresponde ao "forte direito de não perder jamais o poder de manter pleno controle" sobre ambos os aspectos de sua identidade (RODOTÀ, 2004, p. 96, 97). Disso decorre que "a unidade da pessoa somente pode ser reconstituída estendendo ao corpo eletrônico o sistema de garantais elaborado para o corpo físico" (RODOTÀ, 2004, p. 106), o que nos leva a duas colocações. A primeira delas diz respeito à "pegada digital" (KELLEHER; TIERNEY, 2018), também denominada "memória total de caráter digital" (HAN, 2018a) e as implicações que esse fenômeno gera no que diz respeito às liberdades pessoais. A segunda refere-se à ideia de "corpo como unidade" (RODOTÀ, 2004).

3.4.1 Dados que deixam rastros

À medida que se envolvem em sociedades tecnicamente modernas e se movem através delas, as pessoas não têm escolha a não ser deixar um rastro de dados para trás. No mundo real, a proliferação do videomonitoramento significa que os dados de localização podem ser coletados sobre um indivíduo sempre que ele aparece na rua, ou em uma loja, ou em um estacionamento (KELLEHER; TIERNEY, 2018, p. 198). Já no mundo *on-line*, são coletados dados sobre indivíduos quando eles acessam sites, quando enviam um e-mail, quando realizam compras online, quando curtem ou postam algo em uma rede social. Kelleher e Tierney ilustram o que denominam "pegada digital":

> para colocar em perspectiva a quantidade de dados que são coletados sobre o indivíduo médio em uma sociedade tecnologicamente moderna, um relatório da Autoridade Holandesa de Proteção de Dados em 2009 estimou que o cidadão holandês médio foi incluído em 250 a 500 bancos de dados, com esse número subindo para 1.000 bancos de dados para pessoas mais ativas KELLEHER; TIERNEY, 2018, p. 199, tradução nossa).

Através do processo denominado por Solove (2008) de combinação, todos os dados relacionados a uma pessoa, quando tomados em conjunto, definem a sua *pegada digital*. A combinação cria, como já citamos, uma *pessoa digital*, "um retrato composto de fragmentos de informações" (SOLOVE, 2008, p. 125, tradução nossa). O processo de identificação, por sua

vez, vai além, conectando a pessoa digital diretamente a uma pessoa determinada “no mundo real” (SOLOVE, 2008, p. 126).

Consideradas as implicações no que refere à privacidade, a existência de uma pegada digital pode ser problemática em diversos aspectos. Primeiro, os dados podem ser coletados sobre um indivíduo sem seu conhecimento ou consciência. Segundo, em alguns contextos, um indivíduo pode optar por compartilhar dados sobre si mesmo e suas opiniões, mas pode ter pouco ou nenhum conhecimento ou controle sobre como esses dados são usados ou como serão compartilhados e reaproveitados por terceiros (KELLEHER; TIERNEY, 2018, p. 199). Essa incerteza sobre como informações serão utilizadas no futuro, decorrente do uso secundário de dados, cria nas pessoas uma sensação de impotência e vulnerabilidade (SOLOVE, 2008, p. 132), acentuando a assimetria de poder existente entre os detentores e os titulares dos dados.

A pegada digital é problemática também porque, como expõe Han, somos “prisioneiros de uma memória total de caráter digital” (2018b, p. 86). Enquanto o pan-óptico vislumbrado por Bentham carecia de um sistema de registro eficiente, pois contava apenas com o livro das punições disciplinares que listava os castigos aplicados e suas causas, e enquanto o *Big Brother* de Orwell era incapaz de manter o registro da vida das pessoas, os *big data* possibilitam o armazenamento virtualmente infinito de informações. Assim, “já por esse motivo, o pan-óptico digital é mais eficiente do que o benthamiano” (HAN, 2018b, p. 86).

A vigilância e o controle são uma parte inerente da comunicação digital (HAN, 2018a). Todavia, geram o “assujeitamento” da sociedade, culminando, por fim, em uma armadilha perigosa para os próprios indivíduos, que consentem silenciosamente com os dispositivos de vigilância, sem perceber que “essas invasões constantes em sua esfera de intimidade acabam por desapropriá-los de seu espaço de construção de identidade e, consequentemente, do valor dignidade que lhe é devido” (BAIÃO; GONÇALVES, 2014).

Segundo Han (2018a), essa conjuntura implica uma mudança de paradigma, no qual o pan-óptico digital se apresenta não como uma sociedade disciplinar biopolítica, tal qual posto por Foucault (2008), mas sim como uma “sociedade da transparência psicopolítica”; no lugar do biopoder, assume importância o psicopoder. Como aponta o autor, a psicopolítica, somada à vigilância digital, adquire a capacidade de ler e controlar pensamentos, e, consequentemente, influenciar o comportamento das pessoas. Nesse processo, “a vigilância digital toma o lugar da ótica inconfiável, ineficiente e perspectivista do Big Brother” (HAN, 2018a, p. 130, 131), sendo

eficiente justamente por ser aperspectivista, e pelo fato de o psicopoder possuir condições de intervir nos processos psicológicos.

No que tange à coleta e uso de dados, expõe o autor sul-coreano que

> o *data-mining* torna visível os modelos coletivos de comportamento dos quis não se está, enquanto indivíduo, nem sequer consciente. Assim, ele torna acessível o inconsciente-coletivo. Em analogia ao inconsciente-ótico, pode-se também chamá-lo de inconsciente-digital. O psicopoder é mais eficiente do que o biopoder na medida em que vigia, controla e influencia o ser humano não de fora, mas sim a partir de dentro. A psicopolítica se empodera do comportamento social das massas ao acessar a sua lógica inconsciente. A sociedade digital de vigilância, que tem acesso ao inconsciente-coletivo, ao comportamento social futuro das massas, desenvolve traços totalitários. Ela nos entrega à programação e ao controle psicopolíticos. A era da biopolítica está, assim, terminada. Dirigimo-nos, hoje, à era da psicopolítica digital. (HAN, 2018a, p. 134)

Nesse sentido, como exposto por Rodotà, cresceu, nos últimos anos, a pressão para reduzir a proteção dos dados pessoais, seja em nome de uma "personalização" na oferta de bens e serviços, seja em nome da luta contra o terrorismo e a violência. Contudo, "cresceu também a consciência da proteção destes dados como aspecto essencial da liberdade pessoal" (RODOTÀ, 2004, p. 96). Atualmente, as possibilidades de intervenção individual se alargaram, mas se expandiram igualmente, ou ainda mais, "as oportunidades de intervenções políticas de controle do corpo através das tecnologias" (RODOTÀ, 2004, p. 106), o que nos leva ao debate do tópico seguinte.

3.4.2 O corpo como unidade

A segunda colocação à qual dedicaremos atenção diz respeito à compreensão do corpo como uma unidade. Como brilhantemente expõe Stefano Rodotà, o tratamento de dados pessoais, incluindo-se aqui de maneira destacada os dados pessoais biométricos, "deve ser considerado como se referisse ao corpo em seu conjunto, ou melhor, a uma pessoa, que deve ser respeitada em sua integridade física e psíquica" (RODOTÀ, 2004, p. 96).

Para entender melhor a necessidade de se considerar os dados físicos e digitais como sendo igualmente importantes para a compreensão do corpo como uma unidade, tomemos o exemplo trazido por Gilliom e Monaham (2013). De acordo com os autores, a vigilância contemporânea é, em grande parte e ao menos incialmente, abstrata e remota: um amontoado de computadores coleta, compartilha e manipula dados, sendo que, frequentemente, sequer sabemos o que está de fato acontecendo. Porém, não há nada de abstrato no fato de alguém

tentar apalpar a minha (ou a sua) virilha, como frequentemente se faz em abordagens policiais. A maioria das pessoas acharia ofensivo, invasivo e inapropriado esse tipo de contato. Achariam o mesmo caso uma pessoa estranha observasse seus corpos nus, mesmo que tal estranho estivesse de longe e que as imagens estivessem ligeiramente borradas. Por que não aplicar essa lógica diante da violação de dados pessoais, e, principalmente, de dados pessoais biométricos?

Aprofundando-se a discussão em torno do exemplo dado, Gilliom e Monaham (2013) destacam que é possível considerar ainda que uma pessoa, em princípio, não se oporia ao fato de se realizarem revistas íntimas em aeroportos, pois compreenderia que tais procedimentos são necessários para uma maior segurança dos demais passageiros e até mesmo da ordem pública. Contudo, tal pessoa muito provavelmente ficaria ofendida caso fosse escolhida "aleatoriamente" para uma inspeção de rotina, em que fosse sistemática e intensivamente revistada (GILLIOM; MONAHAN, 2013, p. 124). Transportemos esse raciocínio para um contexto de uso de sistemas de vigilância por reconhecimento facial: abstratamente, muitos de nós não nos sentimos ofendidos ao nos depararmos com anúncios como "sorria, você está sendo filmado", ostensivamente exibidos em *shopping centers*, supermercados, prédios públicos e até mesmo em ruas de nossas cidades. Mas o mesmo não poderia ser dito caso descobríssemos que nós, especificamente nós, nos tornamos alvos de vigilância.

Sobrepondo-se as considerações de Rodotà àquelas realizadas por Gilliom e Monaham, podemos afirmar que a coleta massiva de dados pessoais, ao fim e ao cabo, não se difere de uma apalpada não desejada na virilha. O uso indiscriminado de tecnologias de reconhecimento facial sem ciência e quiçá consentimento do titular dos dados obtidos através das imagens representa uma violação ao corpo da pessoa, e, consequentemente, à sua dignidade. A proteção dos dados pessoais apresenta-se como condição para o respeito do próprio princípio da igualdade (RODOTÀ, 2004). Não podemos ter um peso e duas medidas quando se trata do cumprimento desse princípio. Não podemos fingir não nos importarmos que o governo e órgãos de segurança empreguem mecanismos de vigilância ostensiva, quando, na realidade, nos ofendemos com a prática devido às claras violações que ocasionam ao direito à privacidade e à proteção de dados.

Na conjuntura de uma sociedade de vigilância, é necessária uma estratégia dirigida a reduzir a manipulação de dados pessoais e a limitar sua coleta ao mínimo necessário para atingir finalidades legítimas (RODOTÀ, 2004, p. 103), pois somente uma estratégia com tais finalidades

> permite salvaguardar a integridade do corpo, a liberdade pessoal e a liberdade da vigilância. Em particular, a tutela da integridade não deve considerar apenas um corpo cujos componentes físico e eletrônico se entretecem continuamente. Deve ser adequada a uma realidade em que, cada vez mais frequentemente, encontramos um corpo "multiplicado" e "distribuído" (RODOTÀ, 2004, p. 105).

No atual contexto de utilização de dados biométricos, a conexão necessariamente existente entre corpo físico, dados pessoais e governança social pode assumir, nas palavras de Rodotà, "contornos dramáticos". Inegavelmente, "passado e futuro entrelaçam-se novamente e nos obrigam a fixar os olhos neste intolerável presente e na desforra do corpóreo que não desejaríamos presenciar" (RODOTÀ, 2004, p. 106). A desforra do corpóreo significa, hoje, a coleta e utilização abusiva de dados pessoais, biométricos ou não, o que, por sua vez, faz evocar imediatamente o respeito à dignidade da pessoa (RODOTÀ, 2004). E disso decorrem certas implicações, fundamentais para a salvaguarda do referido princípio, às quais dedicaremos atenção no próximo capítulo.

4 EM BUSCA DE UM MODELO REGULATÓRIO PARA TECNOLOGIAS DE RECONHECIMENTO FACIAL

"É isso que, sob certa perspectiva, tenta fazer o Direito: compreender o mundo para organizar o caos potencial de todas as coisas."

Sérgio Branco

4.1 As justificativas para o emprego de tecnologias de reconhecimento facial

Para compreendermos como deve se dar a regulação das tecnologias de reconhecimento facial é preciso, em primeiro lugar, discutir as razões apresentadas para justificar seu uso. A razão mais apresentada é a busca pela segurança. Não poderia ser diferente, afinal, é a mesma justificativa que se apresenta em virtualmente todas as situações que digam respeito a vigilância. Embora há muito tempo os governos se valham do argumento de que o aumento da vigilância está diretamente relacionado ao aumento da segurança (KELLEHER; TIERNEY, 2018), o apelo aos dados pessoais como instrumento de controle é um fenônemo que ganhou força nas últimas décadas. Com o avanço da ciência de dados, as antigas formas de vigilância ganham fôlego e se elevam a um novo patamar, baseando-se agora nas possibilidades trazidas pela tecnologia. Como expõe Rodotà, "o impulso para o emprego máximo dos dados biométricos foi recentemente reforçado pela importância que assumiu a luta contra o terrorismo, que tende a fazer prevalecer a finalidade da segurança sobre todas as outras" (2004, p. 95).

É possível observar que desde o início deste século cresceu a pressão para que se reduza a proteção dos dados pessoais em nome da guerra contra o terror. Particularmente depois dos atentados ocorridos em setembro de 2001 nos Estados Unidos da América, estabeleceu-se a ideia de que é necessário um *tradeoff*[125] entre proteção de dados e segurança. A partir de então, os governos passaram a coletar mais dados sobre as pessoas e a engajar-se em mais atividades de vigilância (SOLOVE, 2011), lançando mão de inéditas ferramentas de coleta e armazenamento de dados, que tornaram basicamente impossível viver nos dias de hoje sem gerar milhares de registros sobre as mais diversas atividades cotidianas.

[125] *Tradeoff* é um termo da língua inglesa utilizado para se referir a uma decisão que consiste na escolha de uma opção em detrimento de outra, inatingíveis ao mesmo tempo. Embora possa ser traduzido, a depender do contexto, como "troca", "câmbio" ou "escolha", optaremos por manter o termo em Inglês devido ao sentido mais amplo que possui.

Nesse *tradeoff*, a proteção de dados pessoais frequentemente é deixada de lado. Os interesses decorrentes da busca por segurança são facilmente compreendidos, pois a vida e a integridade das pessoas estão em jogo, ao passo que o direito à privacidade e à proteção de dados são abstratos e vagos (SOLOVE, 2011). Como consequência, as pessoas acreditam que precisam abrir mão de sua privacidade e de seus dados pessoais para estarem mais seguras. O que é compreensível, pois todos queremos ser protegidos contra eventuais danos. O crime e a violência estão "no topo da lista de coisas que todos gostaríamos de evitar" (GILLIOM; MONAHAN, 2013, p. 142, tradução nossa), então faz sentido que não nos importemos de abrir mão de alguns (ou muitos) de nossos dados pessoais em favor de um sistema de vigilância recrudescido, desde que este efetivamente nos proteja.

O problema é que, na realidade, mais vigilância não significa mais segurança. Gilliom e Monaham afirmam que "infelizmente, estudo atrás de estudo mostra que a vigilância tecnológica não é muito boa na prevenção de crimes e é provavelmente ainda menos efetiva na prevenção do terrorismo" (2013, p. 142, tradução nossa). Ainda segundo os autores, por mais desenvolvidos do ponto de vista tecnológico, e por mais impressionantes que sejam, os sistemas de vigilância digital nem sempre funcionam. Mais precisamente, eles nem sempre produzem os resultados desejados ou prometidos. O uso de câmeras de segurança e, recentemente, de tecnologias de reconhecimento facial, não impede a ocorrência de crimes. O que frequentemente ocorre é que a presença de aparatos de vigilância faz com que os crimes simplesmente ocorram em outros lugares, menos vigiados (GILLIOM; MONAHAM, 2013; NORRIS, 2004).

Ademais, o videomonitoramento não impede a ocorrência de crimes violentos, provavelmente porque esses crimes geralmente são espontâneos, não premeditados (KING; MULLIGAN; RAPHAEL, 2008). Além de sistemas de vigilância não necessariamente aumentarem a segurança, eles podem tornar as pessoas menos seguras se virem câmeras e erroneamente presumirem que alguém está assistindo e que prontamente irá socorrê-las se necessário, uma vez que a maioria das câmeras não é monitorada em tempo real (SOLOVE, 2011; GILLIOM; MONAHAN, 2013). Assim, apesar de câmeras de segurança possivelmente reduzirem a ocorrência de crimes de menor potencial lesivo, como furtos e roubos, não são efetivas na maioria das situações. De maneira geral, soluções mais simples, como melhorar a iluminação de uma rua, mostram-se mais eficazes na redução da criminalidade (GILLIOM; MONAHAN, 2013, p. 135).

Não podemos negar, contudo, o fato de que muitas coisas no mundo nos assustam. O medo de perder bens que arduamente conquistamos através do nosso trabalho, a violência em grandes centros urbanos, a possibilidade – ainda que remota – de sermos vítimas de um ataque terrorista são apenas alguns exemplos. Como elucidam Gilliom e Monaham (2013), todas essas ameaças contribuem para a nossa cultura de inseguridade; em face disso, nós nos apegamos a basicamente qualquer promessa de segurança. Ainda que haja pouca evidência de que o fortalecimento de sistemas de vigilância nos traga, de fato, mais segurança, governos, indústria e mídia parecem trabalhar em conjunto para "criar um mundo que se mostre tão assustador que a vigilância ostensiva parece a única resposta sensata" (GILLIOM; MONAHAN, 2013, p. 124, tradução nossa).

Os autores expõem que a indústria da segurança é uma indústria global multibilionária, considerada "à prova de recessões", porque governos, empresas e pessoas nela investem e adquirem seus produtos independentemente das condições gerais da economia. Embora investir em segurança implique exorbitantes custos financeiros, os custos sociais implicados não ficam atrás:

> direitos individuais são reduzidos em portais de segurança, como aeroportos e fronteiras. Alguns viajantes recebem tratamento preferencial, enquanto outros são submetidos a perfilizações baseadas em critérios raciais, étnicos, religiosos ou políticos. Existem *drones* com capacidade para matar pessoas inocentes em zonas de guerra, que estão sendo empregados nas cidades como uma nova forma de manutenção da ordem. Grandes cidades estão utilizando videomonitoramento "inteligente" para prever crimes, reprimir dissidentes e rastrear incansavelmente as pessoas. E informações [dados] estão fluindo livremente entre os setores público e privado, às vezes permitindo que os agentes governamentais contornem as leis destinadas a proteger os cidadãos da espionagem injustificada do governo (GILLIOM; MONAHAN, 2013, p. 142, tradução nossa).

Os custos sociais são realmente grandes. Mas valem a pena? A questão da segurança, muitas vezes, parece apenas mais uma "demanda manufaturada". Embora, como expusemos anteriormente, certo grau de controle social seja necessário e benéfico, até que ponto realmente precisamos de novas técnicas e formas de vigilância, e até que ponto temos sido meros consumidores dessa indústria, alimentados pela ilusão da insegurança?

Nesse sentido, uma outra justificativa para o uso de tecnologias de reconhecimento facial é aquela que Bruce Schneier (2009) cunhou "*security theater*". O termo refere-se a medidas que fazem com que as pessoas se *sintam* mais seguras, mas que em nada contribuem, de fato, para a sua segurança. O autor cita como exemplo o fato de tropas da Guarda Nacional

dos EUA terem permanecido por meses nos aeroportos do país após os atentados terroristas de 2001, mas com seus armamentos descarregados. Como a segurança é tanto um sentimento quando uma realidade, o *security theater* encontra espaço na interação entre os líderes políticos e os cidadãos. Segundo Schneier, quando as pessoas se sentem ameaçadas, elas buscam algo que as faça se sentir seguras, ao passo que os governantes, em resposta às crises de segurança, oferecem quaisquer soluções que pareçam acalmar os ânimos da população, ainda que não sejam uma solução verdadeira.

Para Solove (2011), programas de vigilância que se enquadram na definição de *security theater* possuem uma virtude, que é a capacidade de amenizar a sensação de insegurança, pois são altamente visíveis. Porém, ainda que acalmar o medo da população seja importante, o *security theater* não passaria, no final das contas, de uma mentira contada pelos governantes. Proteger direitos de maneira significativa requer que estes sejam sacrificados apenas quando as medidas de segurança forem realmente eficazes, e não em função de mentiras, independentemente de quão nobre seja a intenção por trás delas (SOLOVE, 2011).

Não obstante as justificativas apresentadas, há situações em que as tecnologias de reconhecimento facial são úteis, como para a identificação de criminosos após o cometimento de delitos (GILLIOM; MONAHAM, 2013) ou controle de passaportes. Disso decorre a importância de desmistificarmos a crença de que existe obrigatoriamente um *tradeoff* entre segurança e direitos da personalidade. Nem todos os sacrifícios de nossas liberdades são indevidos, infundados; às vezes, é importante que estes sejam realizados, desde que se justifique adequadamente por que são necessários (SOLOVE, 2011). Nesse sentido, a discussão em torno do uso de videomonitoramento é um exemplo do que Solove (2011) denomina "a falácia do tudo ou nada". Os debates sobre o tema tipicamente opõem os benefícios das novas tecnologias à proteção da privacidade, mas regulamentar a vigilância não significa aboli-la, como veremos no próximo tópico.

4.2 Enquadrando corretamente o debate "segurança *vs.* proteção de dados"

Como procuramos demonstrar, nos últimos anos intensificaram-se as discussões sobre a questão da segurança – ainda que sejam, por vezes, ilegítimas. Nesse contexto, ganhou força a ideia de que um afrouxamento na proteção de dados pessoais seria uma maneira eficaz de se combater a violência e até mesmo o terrorismo. Porém, se seguirmos esse raciocínio, "a questão corre o risco de ser posta de maneira imprópria, como se segurança e proteção de dados fossem

valores incompatíveis e como se a tutela de um excluísse automaticamente qualquer relevância do outro" (RODOTÀ, 2004, p. 95).

O argumento de que os direitos à privacidade e à proteção de dados e segurança são mutuamente exclusivos deriva da "falácia do tudo ou nada". Sacrificar a nossa privacidade não nos torna automaticamente mais seguros, e nem todas as medidas de segurança são invasivas à privacidade. Não há nenhuma correlação entre a eficácia de uma medida de segurança e a consequente redução da liberdade que ela provoca (SOLOVE, 2011, p. 34), de modo que medidas de segurança realmente eficazes não precisam ser aquelas que mais afetam nossos direitos. Aliás, geralmente, medidas de segurança realmente eficientes são quase invisíveis. Schneier (2009) aponta que, no caso de combate ao terrorismo nos EUA, tais medidas incluem, dentre outras, o aprimoramento das habilidades de coleta de informações dos serviços secretos, a contratação de especialistas culturais e tradutores de árabe, a construção de pontes com as comunidades islâmicas, tanto nacionalmente quanto internacionalmente. Para nossa "surpresa", essas medidas não incluem novas e dispendiosas ferramentas de policiamento, ou leis que permitam o acesso a dados e informações de cidadãos.

Nesse sentido, nas palavras de Rodotà, "a formulação correta do problema exige não somente um balanceamento entre os diversos interesses em jogo, mas uma avaliação preventiva das modalidades e dos efeitos de uma eventual compressão da proteção dos dados pessoais" (2004, p. 95). Ao buscarmos um equilíbrio entre segurança e privacidade, não devemos colocar de um lado da balança todo o peso da medida de segurança e do outro todos os danos que essa medida pode causar. Isso porque toda medida de segurança deve, na realidade, ser submetida à devida regulamentação e subsequente supervisão (SOLOVE, 2011). Assim,

> o lado de segurança da balança deve avaliar apenas até que ponto essa supervisão e regulamentação reduzem a eficácia da medida de segurança. Se, por exemplo, a supervisão e a regulamentação judiciais projetadas para proteger a privacidade resultarem em atrasos, burocracias e limitações que tornam uma medida de segurança 10% menos eficaz, não faz sentido equilibrar toda a medida de segurança com a privacidade. Em vez disso, o equilíbrio deve estar entre a privacidade e a diminuição de 10% na eficácia da medida (SOLOVE, 2011, p. 36, tradução nossa).

A escolha a ser feita, portanto, não é entre adotar uma medida de segurança ou fazer nada, mas entre adotar uma medida de segurança com supervisão e regulamentação ou uma medida de segurança que decorra exclusivamente do arbítrio daqueles que estão no poder. Em muitos casos, a supervisão e a regulamentação não diminuem substancialmente a eficiência de uma medida de segurança, de modo que o custo para proteger a privacidade e os dados pessoais

dos cidadãos é muito baixo. Em outros casos, contudo, a opção pela segurança pode implicar uma diminuição tamanha na proteção dos dados pessoais a ponto de acarretar violações à dignidade da pessoa humana. Nesses, a modalidade de segurança em jogo deverá ser excluída ou reformulada, uma vez que a dignidade humana constitui hoje uma referência ineludível (RODOTÀ, 2004, p. 95).

Infelizmente, como aponta Solove (2011), a busca pelo equilíbrio quase nunca é avaliada adequadamente. Quando a balança é utilizada sob a influência de argumentos falaciosos, ela tende a pender drasticamente para o lado da segurança, fazendo com que os custos da proteção dos direitos individuais sejam falsamente inflados e as medidas de segurança ganhem mais peso do que deveriam. No entanto, ao ponderarmos direitos individuais e liberdades contra interesses governamentais, é imperativo que a ponderação seja feita apropriadamente. Ainda segundo o autor, a maneira correta de reconciliar a privacidade e a proteção de dados é colocar os programas de segurança sob supervisão, limitando usos futuros dos dados pessoais e garantindo que os programas sejam executados de forma equilibrada e controlada (SOLOVE, 2011, p. 207).

Ao discorrer sobe a implementação de tecnologias de reconhecimento facial para fins de vigilância, Zanatta (2019b) levanta alguns questionamentos: seria possível instituir um sistema de supervisão e *accountability* dessas tecnologias? Seria possível realizar análises de custo-benefício que levassem em consideração critérios como "custos sociais" e "custos à liberdade" previamente à implementação das medidas de segurança? Seria possível incluir a participação de acadêmicos e de instituições do terceiro setor no processo de tomada de decisão? Seria possível, ainda, a criação de uma legislação que obrigasse a elaboração de avaliações de impacto antes que se adquiram sistemas de reconhecimento facial?

Conduzir o debate corretamente significa, então, fazer as perguntas certas. Devemos questionar quão eficaz é a medida de segurança a ser adotada e quais são os problemas que esta causa à privacidade e à proteção de dados; se existe alguma solução alternativa, e se é possível garantir a proteção de direitos individuais sem que se reduza a eficácia da medida de segurança. Devemos, ainda, estabelecer como deve se dar a regulamentação e supervisão dessa medida. Nesse sentido, Solove propõe que sejam feitas perguntas básicas no momento de avaliação de uma medida de segurança:

1. A medida de segurança funciona bem?
2. Ela causa algum problema à privacidade e às liberdades civis?

> 3. Que tipo de supervisão e regulamentação pode resolver ou amenizar estes problemas?
>
> 4. Se deve haver uma troca entre privacidade e segurança, até que ponto uma medida de segurança deve ser limitada para proteger a privacidade? Até que ponto esses limites impedirão a eficácia da medida de segurança? Os benefícios do regulamento valem o custo em termos de eficácia reduzida? (SOLOVE, 2011, p. 208, 209, tradução nossa)

É preciso rigor para avaliar o emprego de medidas de segurança. Quando estas envolvem o uso de novas tecnologias cujas consequências são, no mínimo, problemáticas, o rigor deve ser multiplicado. O resultado pode ser não só uma melhor proteção da privacidade e dos dados pessoais, mas também o desenvolvimento de um sistema de segurança mais eficaz e bem planejado. Restringir medidas de segurança ineficazes é uma vitória tanto do ponto de vista dos direitos individuais quanto do ponto de vista da própria segurança, pois pode levar à procura por alternativas ainda melhores (SOLOVE, 2011).

4.3 Os diferentes caminhos para a regulação

O fenômeno do *big data* foi um fator decisivo para que definíssemos a vida moderna como "a era da informação" (MITTELSTADT; FLORIDI, 2016). Uma das promessas que surgem com esse fenômeno é a possibilidade de se compreender o mundo através dos dados. Tal promessa é tentadora, amplamente sustentada por argumentos que buscam justificar o desenvolvimento e a adoção de infraestruturas baseadas em dados, principalmente em se tratando daquelas relativas à segurança (KELLEHER; TIERNEY, 2018; RODOTÀ, 2008). Ao mesmo tempo, governos, sociedade civil e até mesmo o mercado têm tido dificuldade para entender de que maneira a ciência de dados pode impactar, a médio e longo prazo, o mundo em que vivemos hoje[126].

[126] Neste ponto, é importante que não confundamos o verdadeiro problema posto pelo *big data*. Brendon Mittelstadt e Luciano Floridi (2016) pontuam que o termo "*big*" (grande, em Inglês) é empregado, de maneira geral, porque os dados a que se referem a expressão *big data* são difíceis de classificar e analisar com as tecnologias de computação existentes. Assim, o principal problema seria possuirmos uma quantidade de dados maior do que aquela que podemos processar, e a solução se encontraria no desenvolvimento de melhores técnicas e tecnologias de análise de dados. Todavia, "grande" é um predicativo relativo (FLORIDI, 2012), sendo empregado em termos procedimentais, não quantitativos, de modo que o que hoje é considerado grande pode não o ser daqui a alguns anos devido ao avanço das técnicas computacionais e de *big analytics*. Ademais, é provável que esse avanço gere, na realidade, ainda mais dados (MITTELSTADT; FLORIDI, 2016), o que nos levaria de volta ao primeiro problema. Floridi aponta que do uso de grandes bases de dados decorrem problemas epistemológicos e éticos. O problema epistemológico refere-se aos "pequenos padrões": com o *big data*, muitos dados podem ser gerados e processados rapidamente e a baixo custo, e a partir de praticamente qualquer coisa, gerando uma infinidade de pequenos padrões. Esses pequenos padrões podem representar um risco, principalmente quando combinados mediante o cruzamento de bancos de

Somado à dificuldade de se preverem as implicações do emprego desregrado da ciência de dados em nossa sociedade, encontra-se o problema que Solove (2008) chama de "expectativa de privacidade": tem se tornado cada vez mais difícil esperar por privacidade no mundo de hoje. Devido à coleta massiva de dados, à presença cada vez maior de câmeras de vigilância e à crescente facilidade de divulgação de informações, assistimos resignados a violações à nossa privacidade. Por esses motivos, as pessoas estão "frequentemente lamentando a constante erosão da privacidade" (SOLOVE, 2008, p. 74, tradução nossa). Disso decorre a necessidade de olharmos não para quais são de fato as nossas expectativas quanto a esse direito, num exame puramente descritivo, mas sim para quais elas deveriam ser, numa análise normativa (SOLOVE, 2008). Nesse sentido, diante de nós se descortinam algumas opções: a autorregulação das tecnologias de reconhecimento facial; a heterorregulação, em uma arquitetura precaucionária de danos; ou o banimento total dessas tecnologias.

De acordo com Bruno Ricardo Bioni e Maria Luciano, "as incertezas quanto aos benefícios e os riscos pelo emprego de tecnologias de reconhecimento facial formaram uma arena regulatória efervescente" (2019, p. 221), que se encontram divididas em três eixos:

> a) de um lado, ainda há parte do setor privado que acredita na suficiência de diretrizes éticas e autorregulação enquanto uma estratégia regulatória que não colocaria entraves ao desenvolvimento da tecnologia em questão;
>
> b) no outro extremo, há vozes que clamam pelo banimento da tecnologia por vislumbrar no seu design riscos exacerbados para fins de opressão;
>
> c) ao centro desse movimento pendular, encontra-se uma estratégia que visa desenhar uma arquitetura precaucionária de danos, de modo que o emprego de tecnologias de reconhecimento facial deveria ser antecedido de ações por parte do seu próprio proponente que mitigassem seus eventuais malefícios (BIONI; LUCIANO, 2019, p. 222).

A regulação pela tecnologia, à qual iremos nos referir como tecnorregulação[127], está relacionada ao fato de os atuais avanços tecnológicos obrigarem os legisladores a forjar maneiras mais sofisticadas de se pensar a aplicação da lei (PAGALLO et al., 2015, p. 3). Nas palavras de Eduardo Magrani, tecnorregulação é a regulação realizada através do próprio *design* dessas novas tecnologias (2019, p. 27), estando, portanto, inserida em seus códigos. Dado o rápido desenvolvimento de tecnologias de *big data*, não surpreende que as estruturas legais em

---

dados distintos, porque "ultrapassam o limite do que é previsível e, portanto, do que pode ser antecipado, não apenas sobre o comportamento da natureza, mas também das pessoas" (FLORIDI, 2012, tradução nossa). O problema ético, por sua vez, diz respeito a *como* vamos empregar os dados, estando mais conectado ao tema da presente pesquisa.

[127] Ugo Pagallo et al. (2015, p. 3) empregam o termo "*techno-regulation*" ou "*legal regulation by design*".

vigor e as discussões éticas sobre o uso dados não acompanhem esses avanços (KELLEHER; TIERNEY, 2018, p. 183). O direito, afinal de contas, sempre parece estar muitos passos atrás da tecnologia, o que faz com que a tecnorregulação aparente ser uma forma muito mais eficiente, e consequentemente necessária, de controle.

A dificuldade que o direito tem de acompanhar o desenvolvimento tecnológico decorre de alguns fatores. Um deles é o otimismo geral em relação aos novos produtos e serviços possibilitados pela inovação tecnológica, que decorre do excesso de confiança neles depositados e também, evidentemente, dos benefícios que proporcionam. Outro fator é a incapacidade técnica que os reguladores possuem de compreender o funcionamento de novas tecnologias. Outro, o enorme esforço para antecipar os impactos sociais que as novidades trarão. De acordo com Ana Frazão (2019b, p.31), esses fatores criam "ônus adicionais para os reguladores que, premidos entre a assimetria informacional e os benefícios das inovações", não sabem como frear a imposição da tecnocracia e proteger efetivamente as pessoas. Esse contexto permitiu que vários negócios "evoluíssem em um ambiente no qual o suposto vácuo regulatório fosse convenientemente preenchido pela autorregulação criada pelos agentes em seu próprio benefício" (FRAZÃO, 2019b, p. 31).

Todavia, como argumenta Frazão, a regulação pelos algoritmos configura uma espécie de "controle sem controle" (2019b, p. 36), o que acaba por aumentar o poder que corporações e órgãos do governo possuem. A autorregulação que vemos hoje em dia é "abusiva e sem limites, estabelecida apenas em favor dos interesses das próprias plataformas" de tecnologia (FRAZÃO, 2019b, p. 48). Para a autora, a confiança depositada em uma *data-driven approach* como a solução para os problemas socioeconômicos desconsidera que uma das principais consequências desse processo é tornar a sociedade cada vez mais tecnocrática. Ainda que uma abordagem orientada por dados seja positiva quando considerados critérios como eficiência do sistema, os problemas que dela decorrem, do ponto de vista das liberdades civis, não podem ser ignorados.

Segundo Pagallo et al. (2015), a tecnorregulação impõe dois desafios particularmente perturbadores ao Estado de direito. Primeiro, a crença em tecnologias supostamente perfeitas e autorreguláveis pode ser altamente paternalista e até mesmo autoritária, uma vez que soluções tecnocratas, como *privacy by design*, acabam moldando condutas individuais. Segundo, a pretensão de órgãos governamentais e corporações privadas de solucionar os problemas existentes na sociedade da informação através de técnicas de *design* e de configurações de código, isto é, incorporando salvaguardas legais às novas tecnologias, frequentemente ocasiona

a condição ilegítima na qual governos buscam regular unilateralmente condutas, impondo normas a pessoas que sequer são ouvidas durante o processo de tomada de decisões que certamente irão afetá-las.

Sem dúvidas, como afirma Rodotà, "a valoração social do impacto das inovações cientificas e tecnológicas é hoje um dever de todas as instituições públicas e privadas" (2004, p. 104). A importância da tecnorregulação não pode ser ignorada. Mas é preciso levar em conta que também o direito é um importante instrumento para a salvaguarda de garantias individuais. O direito à privacidade e à proteção de dados existem porque, em algum momento, as sociedades perceberam a importância de proteger esses valores não apenas para preservar o *status quo*, mas também para modificar a realidade ao diminuir deficiências e resolver problemas. Construímos leis para estabelecer um estado de coisas que queremos, não apenas para preservar realidades pré-existentes, e nessa empreitada cabe ao direito ser empregado proativamente a fim de criar o nível de proteção que desejamos (SOLOVE, 2008).

É importante que tenhamos em mente que o dever a que Rodotà se refere é ainda maior em se tratando das instituições que possuem a obrigação de garantir, mediante a proteção da privacidade e dos dados pessoais, "uma dimensão essencial da liberdade dos nossos contemporâneos" (2004, p. 104). A conjuntura econômica, política e social do século XXI tornou a proteção da privacidade e dos dados pessoais mediante a heterorregulação necessária, imprescindível e sobretudo urgente. Considerando a importância do direito como um sistema eficaz de regulação, e também que um dos objetivos do direito é preservar a liberdade individual e a autonomia humana, a regulação tecnológica deve ser orientada pelos princípios basilares do Estado de Direito, de modo que o direito seja, assim, uma *meta-tecnologia* apta a guiar a tecnorregulação (PAGALLO et al., 2015).

4.4 A regulação por princípios

Desde meados da década de 1960, as tentativas de regulação da proteção de dados pessoais fazem referência a princípios a fim de delimitar materialmente seus objetivos e linhas de atuação principais. Esses princípios frequentemente se faziam – e fazem – presentes em diversos ordenamentos jurídicos, o que nos permite vislumbrar a "convergência das soluções legislativas quanto à matéria em diversos países, bem como uma tendência sempre mais marcada rumo à consolidação de certos princípios básicos e sua vinculação sempre mais estreita com a proteção da pessoa e com os direitos fundamentais" (DONEDA, 2011, p. 98).

Doneda (2011) observa que nos EUA, em 1973, um estudo realizado pela *Secretary for health, education and welfare* concluiu que a tutela da privacidade de uma pessoa se relaciona diretamente com a proteção de seus dados pessoais. A concepção de privacidade[128] definida pelo órgão não forneceu uma base para determinar *a priori* quais dados pessoais poderiam/deveriam ser registrados e utilizados. Todavia, foi capaz de fundamentar o estabelecimento de procedimentos que garantissem ao indivíduo o direito de participar de maneira significativa nas decisões sobre a coleta e uso de seus dados e informações pessoais. Foram determinados, princípios fundamentais para a proteção da privacidade, assim apresentados:

> Não deve existir nenhum sistema de registro de dados pessoais cuja própria existência seja secreta.
>
> Deve existir uma maneira de um indivíduo descobrir quais informaçãos que lhe digam respeito estão contidas em determinado registro e como são utilzadas.
>
> Deve existir uma maneira de um indivíduo impedir que informações sobre ele obtidas para um determinado fim sejam utilizadas ou disponibilizadas para outros fins sem o seu consentimento.
>
> Deve existir uma maneira de um indivíduo corrigir ou modificar um registro de informações identificáveis a seu respeito.
>
> Qualquer organização que crie, mantenha, use ou divulgue registros de dados pessoais identificáveis deve assegurar a confiabilidade dos dados para seu uso pretendido e deve tomar precauções razoáveis para evitar o uso indevido dos dados (ESTADOS UNIDOS DA AMÉRICA, 1973, tradução nossa).

Esses princípios, posteriormente referidos como *Fair Information Principles*, foram repetidos em importantes instrumentos internacionais de proteção de dados (DONEDA, 2011), dentre os quais se destacam as *Diretivas para Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais* da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), em 1980, e a *Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal* (Convenção 108), conhecida como

[128] A relação entre privacidade e proteção de dados foi formulada nos seguintes termos: "A privacidade de um indivíduo é afetada diretamente pelo tipo de divulgação e de utilização feitas com as informações registradas a seu respeito. Um registro contendo informações sobre um indivíduo que permitam a sua identificação deve, portanto, ser regido por procedimentos que concedam ao indivíduo o direito de participar na decisão sobre qual será o conteúdo do registro, bem como sobre como deverão ser feitos o uso e a divulgação de das informações pessoais nele contido. Qualquer gravação, divulgação e uso de informações pessoais identificáveis não regidas por tais procedimentos deve ser proibida como uma prática de informação desleal, a menos que tal gravação, divulgação ou uso seja especificamente autorizado por lei" (ESTADOS UNIDOS DA AMÉRICA, 1973, tradução nossa).

Convenção de Estrasburgo, de 1981. Doneda (2011, p. 99, 100) sintetiza os princípios presentes nos referidos documentos:

> a) *Princípio da publicidade* (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos;
>
> b) *Princípio da exatidão*: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade;
>
> c) *Princípio da finalidade*, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade);
>
> d) *Princípio do livre acesso*, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos;
>
> e) *Princípio da segurança física e lógica*, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

Importante notar que os oito princípios básicos[129] estabelecidos originalmente pela OCDE em 1980 foram "deixados intactos" na atualização das Diretivas ocorrida em 2013. Isso demonstra a importância de uma regulação baseada em princípios, uma vez que estes deveriam orientar o desenvolvimento de novas tecnologias, e não o contrário, como afirma Solove (2011). Os estatutos legais devem ser flexíveis o suficiente para atender às novas tecnologias – como se propõem as Diretivas da OCDE – e, para tanto, devem ter como ponto de origem alguns princípios básicos. Sobre tecnologias de vigilância de maneira geral, argumenta o autor que estas devem ser orientadas pelos seguintes princípios:

> 1. *Minimização da coleta e do uso*. O governo deve procurar minimizar o grau de coleta de informações pessoais além do que é necessário para fins de segurança. Os usos futuros dos dados devem ser limitados para que os dados

[129] Os princípios são: *collection limitation principle; data limitation principle; purpose specification principle; use limitation principle; security safeguard principle; openness principle; individual participation principle; accountability principle* (OCDE, 1980, 2013).

> coletados para uma finalidade não sejam usados, algum dia, de forma inesperada, para uma finalidade não relacionada. E os dados devem ser excluídos após um período de tempo razoável.
>
> 2. *Suspeita individualizada*. O governo deve restringir a coleta de informações a circunstâncias que envolvam suspeitas específicas. (...)
>
> 3. *Supervisão*. A coleta e o uso de informações por parte do governo devem ser submetidos a uma supervisão significativa. Autoridades governamentais devem ser supervisionadas para assegurar que elas mantenham suas atividades limitadas, evitem abusos de poder, e sejam responsabilizados por seu comportamento (SOLOVE, 2011, p. 172, tradução nossa).

Particularmente em relação às tecnologias de videomonitoramento, Solove propõe que se observem os seguintes princípios:

> 1. *Prestação de contas (accountability) e transparência*. Toda vigilância por vídeo deve ser sujeita a supervisão e revisão. Devem ser mantidos dados sobre o desempenho e a eficácia da vigilância, bem como de quaisquer abusos e problemas.
>
> 2. *Fortes penalidades para abusos*. Qualquer vazamento ou uso indevido de informações de vigilância por vídeo deve ser sujeito a fortes penalidades.
>
> 3. *Exclusão de dados antigos*. Os dados obtidos através de videomonitoramento não devem ser mantidos indefinidamente. Devem ser apagados após um período de tempo, o que evita mau uso futuro.
>
> 4. *Prevenção de "mission creep" (uso secundário de dados)*. O uso secundário de dados refere-se ao fenômeno de uma tarefa se expandir para além dos seus parâmetros originais. No caso da vigilância por vídeo, significa que os dados coletados para um propósito sejam utilizados para outros fins, ou tecnologias instaladas para um propósito sendo posteriormente utilizadas para outro. As finalidades da vigilância devem ser especificadas com antecedência, e os dados coletados através da vigilância devem ser usados apenas para essas finalidades. Qualquer novo uso dos dados deve ser aprovado judicialmente, e somente após o governo demonstrar que os benefícios dos usos prevalecem sobre quaisquer danos à privacidade e às liberdades civis.
>
> 5. *Proteção dos direitos da Primeira Emenda*[130]. Os dados obtidos através de videomonitoramento referentes a discursos, protestos, associação política, religião e exploração de ideias e conhecimentos devem estar sujeitos às mais rigorosas proteções. O governo deve evitar o uso desses dados, exceto sob as circunstâncias inevitáveis (SOLOVE, 2011, p. 181, tradução nossa).

Como as tecnologias de reconhecimento facial se encontram, na maior parte das vezes, atreladas ao uso de tecnologias de videomonitoramento, os princípios aplicáveis a estas devem se estender àquela. Muitas desses princípios, aliás, ora são semelhantes, ora se sobrepõem. A

[130] O autor escreve considerando as disposições do ordenamento jurídico estadunidense. De maneira geral, poderíamos compreender o quinto princípio como sendo a "proteção dos direitos e garantias fundamentais".

questão é que a utilização de sistemas de IA vem ocorrendo sem o correspondente e devido debate ético e jurídico (FRAZÃO, 2019b), e o mesmo se aplica ao uso massivo de videomonitoramento.

Devido à ausência de legislações específicas sobre o desenvolvimento e emprego dessas tecnologias, e considerando que geralmente elas envolvem o processamento de dados pessoais, as questões atinentes ao tema têm sido endereçadas em leis de proteção de dados. Segundo Bioni e Luciano:

> Na medida em que boa parte dos processos de decisões automatizadas com o emprego de IA envolverá o processamento de dados pessoais, leis gerais de proteção de dados, talhadas com base em uma mentalidade de regulação de risco e no princípio da accountability, são vetores de democratização do próprio processo de regulação de tal tecnologia (BIONI; LUCIANO, 2019, p. 217).

4.5 A Lei Geral de Proteção de Dados Pessoais (LGPD)

A ausência de regulação própria de tecnologias de inteligência artificial faz com que as questões a elas referentes sejam tratadas em legislações gerais de proteção de dados, "tomando emprestadas" determinadas instruções normativas. Em âmbito global, a Regulação Geral de Proteção de Dados da União Europeia ganha destaque, assim como as Diretivas de Privacidade da OCDE. No Brasil, a Lei n.º 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe de maneira específica sobre a proteção de dados pessoais – o que não significa que a matéria não fosse disciplinada em diplomas legais esparsos. Nos termos do *caput* de seu art. 1º, a LGPD

> dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018a).

Longe de ser um instrumento de tutela apenas do direito à privacidade, a Lei Geral de Proteção de Dados Pessoais brasileira pretende proteger situações existenciais diversas, sobretudo aquelas relativas à liberdade, tendo como escopo principal "resgatar a dignidade dos titulares de dados e seus direitos básicos relacionados à autodeterminação informativa" (FRAZÃO, 2019c, p. 100). A LGPD é, dessa forma, um importante instrumento para o

reconhecimento da proteção de dados pessoais como um direito fundamental autônomo[131]. Frazão explica que

> seja em razão do amplo alcance da LGPD, seja em razão da sua preocupação com a tutela das situações existenciais dos titulares de dados, pode-se dizer que foi acolhida concepção convergente com a daqueles que, a exemplo de Rodotá, sustentam que a proteção de dados consiste corresponde a verdadeiro direito fundamental autônomo, expressão da liberdade e da dignidade humana, que está intrinsecamente relacionada à impossibilidade de transformar os indivíduos em objeto de vigilância constante (FRAZÃO, 2019c, p. 103).

O advento da LGPD no contexto de consolidação de um pan-óptico digital evidencia também o seu papel de reforçar o devido e imprescindível controle que as pessoas precisam exercer sobre seus dados pessoais. Não à toa, são agora compreendidas como *titulares* de seus dados pessoais[132]. Nessa perspectiva, a Lei se apresenta como "um freio e um agente transformador das técnicas atualmente utilizadas pelo capitalismo de vigilância, a fim de conter a maciça extração de dados e as diversas aplicações e utilizações que a eles podem ser dadas" (FRAZÃO, 2019c, p. 103). Isso porque um dos meios de refrear o poder de agentes detentores de dados, como governos e grandes corporações, "é o reconhecimento e o reforço dos direitos dos titulares de dados, inclusive no que impõem padrões de segurança, transparência e *accountability* para todas as formas de tratamento de dados" (FRAZÃO, 2019b, p. 48).

Analisando-se ainda o art. 1º da LGPD, dois pontos merecem destaque. O primeiro deles diz respeito ao conceito de *tratamento de dados pessoais*, que vem definido em seu art. 5º, inciso X. De acordo com o dispositivo, tratamento é

> 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 (BRASIL, 2018a).

O segundo ponto, por sua vez, concerne aos meios em que a LGPD é aplicável: a expressão *inclusive nos meios digitais* deixa claro que a Lei não está restrita ao meio digital. Pelo contrário, se aplica a todos os meios pelos quais dados podem ser coletados e utilizados (FRAZÃO, 2019b). Assim, não restam dúvidas quanto à sua aplicabilidade quando falamos de

---

[131] Nesse sentido, a Proposta de Emenda à Constituição (PEC) 17/2019 "acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria" (BRASIL, 2019). A PEC foi aprovada pelo Plenário do Senado Federal e, até o momento, aguarda a análise da Câmara dos Deputados.

[132] O art. 5º, inciso V, da LGPD considera titular a "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento" (BRASIL, 2018a).

dados biométricos faciais, sejam estes coletados em ambientes “físicos”, através, por exemplo, de câmeras de videomonitoramento, ou em ambientes virtuais.

No entanto, cabe agora uma importante observação. A LGPD é o principal diploma legal brasileiro a dispor sobre o tratamento de dados pessoais. Todavia, conforme a determinação de seu art. 4º, inciso III, a Lei não se aplica ao tratamento de dados pessoais realizados para fins exclusivamente de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. O objetivo dessa limitação é a suposta garantia do interesse público de combater infrações penais, crime organizado, fraudes digitais ou até mesmo terrorismo. Dessa forma, no âmbito do setor público, o uso de tecnologias de reconhecimento facial para os referidos fins encontra-se parcialmente excepcionado do escopo de aplicação da LGPD (BIONI; LUCIANO, 2019).

Parcialmente excepcionado, pois a inaplicabilidade da Lei nesses contextos não é absoluta. O art. 4º, em seu parágrafo primeiro, determina, além da necessidade de legislação específica para regulação das hipóteses do inciso III, que os princípios gerais de proteção ao titular de dados continuarão orientando qualquer esfera de tratamento, até mesmo em contextos de interesse público:

> 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 (BRASIL, 2018a).

Sendo assim, a regulação de tecnologias de reconhecimento facial para fins de segurança demandará a criação de lei específica. Nesse caso, o dever de observância dos princípios gerais de proteção de dados pessoais se revela uma forma de garantia dos direitos de seus titulares, a fim de impedir tratamentos irregulares ou abusivos por parte do Poder Público.

É importante ressaltar que, em se tratando da regulação de tecnologias de reconhecimento facial, apenas a Lei Geral de Proteção de Dados não é suficiente para endereçar todas as questões decorrentes do uso dessas tecnologias, ainda que não estejamos falando do seu uso para fins de segurança – cuja regulação depende, conforme exposto, de legislação específica. Segundo Frazão, quando o tratamento de dados pessoais é realizado por agentes detentores de posições dominantes nos mercados em que atuam, como empresas de tecnologia ou grandes plataformas digitais, a LGPD provavelmente não será capaz de disciplinar

integralmente as questões relativas à atuação desses entes (FRAZÃO, 2019b). Nas palavras da autora,

> embora a heterorregulação – aqui traduzida pela LGPD e todas as demais leis e atos normativos estatais que se destinam a regular o tratamento de dados no Brasil – seja fundamental para endereçar o problema do tratamento de dados pessoais, isso não quer dizer que ela, sozinha, seja suficiente para tal propósito (FRAZÃO, 2019c, p. 117).

Isso não é, absolutamente, uma tentativa de diminuir a relevância de uma lei geral de proteção de dados. Antes, reconhecemos o papel "crucial e necessário" da LGPD, uma vez que oferece "uma base comum de regras e princípios que poderá ser utilizada por outras áreas, sempre que tiverem que lidar com a problemática dos dados" (FRAZÃO, 2019b, p. 48).

Esses princípios, disciplinados ao longo de toda a Lei e também em legislações esparsas, encontram-se sintetizados em seu art. 6º. São eles: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas. Todos eles, em maior ou menor medida, deverão ser observados quando da regulação de tecnologias de reconhecimento facial. Em face disso, a seguir serão feitas breves considerações sobre a sua importância para a elaboração de uma eventual lei sobre TRFs. Devido à proximidade que alguns desses princípios guardam entre si, ora serão trabalhados em um único tópico, ora separadamente.

4.5.1 Princípios da finalidade, adequação e necessidade

O primeiro princípio elencado nos incisos do art. 6º da LGPD é o da finalidade, que diz respeito à "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018a). Em seguida, guardando estreita relação com o princípio da necessidade, encontra-se o da adequação, definido como a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (BRASIL, 2018a).

O princípio da finalidade dos dados determina que esta deve poder ser conhecida antes que ocorra a sua coleta, especificando-se na relação entre os dados colhidos e a finalidade perseguida. Isso significa que o princípio da adequação, denominado por Rodotà (2008) de *pertinência*, é uma manifestação da finalidade. Para o autor, a finalidade ainda se especifica na relação entre a finalidade da coleta e a utilização dos dados (*princípio da utilização não-*

abusiva) e na eliminação, ou na transformação em dados anônimos das informações que não são mais necessárias (*princípio do direito ao esquecimento*).

O princípio da finalidade possui ainda grande relevância prática, pois nele se estruturam critérios para determinar a razoabilidade do uso de determinados dados para além dos fins previstos, fora dos quais ocorreria abusividade no tratamento (DONEDA, 2011). Atualmente, com a possibilidade de armazenamento infinito de dados graças às técnicas de *big data*, todas as pegadas digitais das pessoas podem ser capturadas (KELLEHER; TIERNEY, 2018), de modo que os detentores dos dados podem não apenas registrar e processar todo o passado, mas também antecipar e decidir o futuro das pessoas (FRAZÃO, 2019b). Nesse sentido, o princípio da finalidade é crucial para que se evite o uso secundário de dados, como debatido no Capítulo 3 deste trabalho.

Relacionado aos dois primeiros, talvez um dos princípios que mais se mostra relevante ao debate sobre tecnologias de reconhecimento facial seja o da necessidade. De acordo com o inciso III do art. 6º, o princípio da necessidade corresponde à "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, 2018a). Especialmente no que tange ao tratamento de dados para fins de segurança pública, o art. 4º, §1º, determina que as medidas previstas pelo poder público deverão ser proporcionais e *estritamente necessárias* ao atendimento do interesse público.

Segundo Rodotà, no momento de regulação de tecnologias que fazem uso de dados pessoais biométricos, primeiramente se faz necessária uma estratégia capaz limitar a coleta desses dados ao mínimo necessário para atingir finalidades legítimas (2004, p. 103), bem como reduzir ao máximo a sua manipulação. Para o jurista italiano,

> se parece reducionista e perigosa uma formulação que leve a concluir que "nós somos os nossos dados", é indubitável porém que o nexo entre corpo, informações pessoais e controle social pode assumir contornos dramáticos, a ponto de fazer evocar de imediato o respeito à dignidade da pessoa, o qual impõe uma interpretação particularmente rigorosa do princípio da estrita necessidade na coleta e no tratamento de informações, no sentido de que somente se deve recorrer a dados capaz de identificar um sujeito quando este recurso for a única forma de alcançar tal finalidade (RODOTÀ, 2004, p. 97).

Não há dúvida, como argumentado anteriormente, de que a utilização de dados biométricos pode oferecer novas formas de segurança e simplificação das atividades cotidianas. Todavia, essas considerações não são suficientes, sendo imprescindível "observar

analiticamente as diversas espécies de dados biométricos, as finalidades para as quais podem ser utilizados e as modalidades de utilização" (RODOTÀ, 2004, p. 98). Nesse sentido, não basta determinarmos se é viável ou não, do ponto de vista tecnológico, utilizar programas de reconhecimento facial para fins de vigilância. A sua utilização demanda "uma aproximação tecnicamente prudente, "sem os entusiasmos e as certezas definitivas que, com frequência, vêm proclamados sobretudo por quem tem interesse direto em colocar no mercado tecnologias ligadas a esses dados" (RODOTÀ, 2004, p. 98).

Em relação ao princípio necessidade, Rodotà traz ainda duas indicações. Uma delas diz respeito à necessidade de uma avaliação rigorosa no uso de dados biométricos com referência à sua confiabilidade, o que irá variar a depender da tecnologia. Argumenta o autor que, quando recorremos a dados biométricos, a utilização de tais dados só é legítima quando não for possível alcançar a mesma finalidade de dados que não envolvam o corpo. Diante da multiplicidade de técnicas e ferramentas hoje disponíveis, não é inviável buscarmos soluções que preservem a privacidade e os dados pessoais dos cidadãos. A segunda indicação, de caráter geral, é que o uso de dados biométricos deve ser submetido a um teste de compatibilidade com os valores democráticos, aplicável a toda utilização de dados biométricos:

> Mais relevante ainda, todavia, é a consideração que diz respeito ao número de sujeitos de quem são colhidas as informações. As coletas generalizadas, de fato, sobretudo quando justificadas por razões de segurança, modificam a percepção social que delas se tem e acabam por transformar todos os cidadãos em suspeitos em potencial: "*a nation under suspicion"*, com já se disse. Fazem aumentar, além do mais, a vulnerabilidade social, sendo muito difícil eliminar completamente o risco de abusos, dada a enorme quantidade de dados, ou defender grandes bancos de dados de violações, que poderiam vir até de grupos terroristas ou criminosos, gerando um perigoso efeito bumerangue (RODOTÀ, 2004, p. 99).

É nesse sentido que Pasquale (2015) afirma que devemos reclamar nosso direito à presunção de inocência. Pode ser que não possamos impedir a coleta de nossos dados pessoais, mas devemos ao menos tentar regular a maneira como são utilizados. Embora Pasquale reconheça que é "mais fácil falar do que fazer" (2015, p. 57, tradução nossa), a alternativa – permanecer de braços cruzados diante dos abusos cometidos por autoridades governamentais – é ainda pior.

Ao pensar a regulação de tecnologias de reconhecimento facial (ou qualquer tecnologia que envolva o uso de dados biométricos), não podemos nos limitar a uma análise do tipo custo-benefício (RODOTÀ, 2004). Principalmente porque, como aponta Frazão (2019c), direitos fundamentais não podem estar sujeitos a esse tipo de juízo, uma vez que são deontológicos e

vinculantes. Ainda que houvesse um *tradeoff* entre o direito à inovação (aqui concretizado nas TRFs) e direitos individuais, "seria preciso ponderar que a inovação não é um valor absoluto e que, exatamente por isso, não pode ser perseguida de forma irrestrita e às custas do sacrifício das situações existenciais mais elementares dos titulares de dados" (FRAZÃO, 2019c, p. 111).

Além disso, devemos levar em consideração que se determinada tecnologia ou técnica pode ser substituída, ela não é, afinal, necessária. Rodotà (2004, p. 100) utiliza como exemplo o emprego de impressões digitais para fins de identificação. Em primeiro lugar, aponta, devemos levar em consideração a possibilidade de utilização ulterior desses dados, já que os sinais continuamente deixados permitem reconstituir a movimentação das pessoas, de modo que não bastaria que se invocassem medidas de segurança com o objetivo de impedir o uso indevido das impressões digitais. Na realidade, seria preferível *substituir* a sua utilização enquanto instrumento de identificação ou de autenticação por dados biométricos não rastreáveis, como o reconhecimento da íris. Embora o autor fale sobre o uso de impressões digitais, o exemplo se aplica de maneira ainda mais contundente quando pensamos no emprego em tecnologias de reconhecimento facial.

A solução apresentada por um jovem programador brasileiro é uma ilustração contundente de como tecnologias de reconhecimento facial podem ser substituídas, ao mesmo tempo em que se mantém (ou, até mesmo, aumenta) a eficácia de sistemas de segurança, sem prejuízos aos direitos individuais. Nicholas Guimarães desenvolveu um algoritmo batizado *AllSeenEye*[133,134], que identifica a presença de armas de fogo em determinado local, a partir da análise das imagens obtidas por câmeras de segurança. O sistema é capaz de identificar qual tipo de arma (se um revólver, pistola, fuzil, *etc.*) aparece na cena, emitindo um alerta em tempo real para autoridades. Além disso, a ferramenta conta com a possibilidade de emitir notificações caso haja alguma transmissão em redes sociais em que ocorra o aparecimento de alguma arma, o que poderia diminuir a projeção de ataques terroristas como os ocorridos na Nova Zelândia, em março de 2019[135].

---

[133] *AllSeenEye* é a junção das palavras *all, seen* e *eye*, que formam a expressão "o olho que tudo vê".
[134] "Guns recognition". Disponível em: https://aiquimist.com/index.php/guns-recognition/.
[135] "Atentados em mesquitas da Nova Zelândia deixam pelo menos 49 mortos". Disponível em: https://brasil.elpais.com/brasil/2019/03/15/internacional/1552616642_719105.html.

4.5.1.2 Consentimento

A concretização dos princípios da finalidade, adequação e necessidade pressupõe que haja prévia informação e consentimento do titular dos dados quanto ao tratamento destes (OLIVEIRA; LOPES, 2019). Assim, ainda que não se enquadre como um princípio orientador do regime de proteção de dados pessoais, o consentimento adquire relevância, apresentando-se, na maioria dos casos, como meio de legitimar o tratamento de dados pessoais. Segundo Mulholland, a Lei Geral de Proteção de Dados brasileira adota uma forte fundamentação no consentimento do titular de dados para admitir tais tratamentos (2018, p. 168).

Nos termos legais, consentimento é a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada" (art. 5º, XII). Em relação ao tratamento de dados pessoais sensíveis, dentre os quais se incluem os dados biométricos[136], a Lei estipula ainda, em seu art. 11, inciso I, que o consentimento deverá ocorrer de forma específica e destacada e para finalidades específicas, configurando uma espécie de consentimento qualificado.

No entanto, o consentimento para o tratamento de dados sensíveis é dispensado quando envolver "dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos", nos termos do art. 11, inciso II, alínea "b". Desse modo, o consentimento do titular dos dados sensíveis, qualificado ou não, torna-se desnecessário em hipóteses que se refiram à persecução do interesse público, bastando a publicidade da referida dispensa[137]. Nas palavras de Mulholland, isso se dá "em decorrência de uma ponderação de interesses realizada pela lei, aprioristicamente, que considera mais relevantes e preponderantes os interesses de natureza pública frente aos interesses do titular, ainda que estes tenham qualidade de Direito Fundamental" (2018, p. 168). Porém, esse posicionamento legislativo é passível de críticas, "especialmente se considerarmos que a proteção do conteúdo dos dados pessoais sensíveis é fundamental para o pleno exercício de Direitos Fundamentais, tais como os da igualdade, liberdade e privacidade" (MULHOLLAND, 2018, p. 168).

---

[136] Conforme a definição da LGPD, dado pessoal sensível é o "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" (BRASIL, 2018a, grifo nosso).

[137] É o que dispõe o art. 11, §2º, da LPGD: " 2º Nos casos de aplicação do disposto nas alíneas 'a' e 'b' do inciso II do caput deste artigo pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do inciso I do caput do art. 23 desta Lei" (BRASIL, 2018a).

Nesse sentido, diversos autores já manifestaram preocupações quanto ao tratamento de dados pessoais sensíveis sem consentimento e/ou consciência dos seus titulares. Pasquale (2015), por exemplo, utiliza a metáfora do *one-way mirror* para descrever como governos e empresas coletam e armazenam dados sobre cidadãos sem que estes, muitas vezes, sequer saibam disso. Schneier (2015) ressalta a consolidação de um controle institucional, operado mediante a coleta e uso de dados pessoais secretamente. Kelleher e Tierney reconhecem que a coleta de dados de uma pessoa sem seu conhecimento ou consentimento é "claramente preocupante" (2018, p. 201, tradução nossa). Segundo Rodotà, sob o ponto de vista específico da proteção de dados pessoais sensíveis, uma questão importante que deve ser levantada é "representada pelo fato de que alguns sistemas biométricos se baseiam em dados que, como aqueles relativos às impressões digitais e ao DNA, podem ser obtidos sem que as pessoas às quais se referem tenham disso tenham qualquer consciência" (2004, p. 100), o que ocorre porque determinados dados pessoais biométricos podem ser obtidos a partir de vestígios involuntariamente deixados por seus titulares. O autor usa como exemplo amostras de DNA ou impressões digitais, que podem ser colhidas em ambientes onde uma pessoa esteve, ainda que por um breve período de tempo. A nosso ver, tal raciocínio se torna ainda mais evidente quando pensamos na coleta de biometrias faciais, que sequer demandam a presença de um elemento "físico" – um fio de cabelo, um objeto que a pessoa tenha tocado – para sua obtenção.

Independentemente da espécie de dado pessoal sensível à qual nos refiramos, importa-nos ter em mente que a facilidade para sua obtenção "pode incentivar utilizações excessivas, ou até mesmo ilegítimas, sob a alegação, justamente, do baixo índice de invasão na coleta de tais dados" (RODOTÀ, 2004, p. 100). Bioni questiona se "deve haver uma esfera mínima de controle por parte do titular dos dados, mesmo nos casos em que não há a aplicação da base legal do consentimento" (2019, sem paginação). Acreditamos que sim, porque "ausência de consentimento não equivale a ausência de controle" (BIONI, 2019, sem paginação). Nesse sentido, a teoria da privacidade contextual proposta por Helen Nissenbaum (2015) apresenta-se como um caminho para se pensar a questão do consentimento no emprego de tecnologias de reconhecimento facial por parte do poder público.

Resumidamente, a principal premissa da teoria da privacidade contextual é a de que o fluxo de informações pessoais deve ser apropriado de acordo com as suas respectivas esferas sociais (NISSENBAUM, 2015). Nas palavras da autora,

> a tese central da teoria da integridade contextual é que o que incomoda as pessoas, o que nós vemos como perigoso, ameaçador, perturbador ou irritante, o que nos deixa indignados, resistentes, inseguros e ultrajados nas nossas experiências com sistemas e práticas contemporâneas de coleta, associação, análise e disseminação de informações não é que eles diminuem nosso controle e trespassam nossos segredos, mas que eles transgredem normas informacionais relativas-contextuais (NISSEMBAUM, 2015, p. 186, tradução nossa).

Essas normas informacionais[138] preservam a integridade dos contextos sociais em que vivemos nossas vidas, apoiando e promovendo os valores, objetivos e fins em torno dos quais esses contextos são orientados (NISSENBAUM, 2015). Logo, a partir de uma análise contextual, o titular dos dados é capaz de estipular quais são as legítimas expectativas que possui e o modo como ocorrerá o fluxo de seus dados, o que determina, então, a sua integridade (BIONI, 2019). Bioni elucida que

> a privacidade contextual reside justamente na fidelidade depositada pelo emissor de uma informação ao(s) seu(s) recipiente(s), na legítima expectativa de que seus dados pessoais serão usados e compartilhados de acordo com o contexto de uma relação preestabelecida ou a razão pela qual foi publicizado um dado; particularmente, na esperança de que o trânsito das suas informações pessoais não minará e trairá a sua capacidade de livre desenvolvimento da personalidade e de participação social (BIONI, 2019, sem paginação).

O produto da teoria da privacidade contextual é, portanto, a consideração de que em cada contexto o titular dos dados pessoais tem legítimas expectativas de como eles irão fluir de forma apropriada (BIONI, 2019). Para nós, parece legítima a expectativa que uma pessoa possui de *não* ter seus dados biométricos faciais colhidos, armazenados e utilizados para fins vigilância, monitoramento, perfilização etc., ainda que isso ocorra em nome da segurança e/ou do interesse público. Contudo, não sendo este o foco do presente trabalho, por ora encerramos a discussão levantada neste tópico, deixando claro que o tema é merecedor de um debate aprofundado.

4.5.2 Princípios da transparência, livre acesso e qualidade dos dados

Um aspecto relevante no que concerne ao tratamento de dados pessoais é transparência na coleta e manuseamento dos dados, bem como o acesso que o indivíduo possui a eles. Segundo Pasquale (2015), a falta de transparência é o resultado da ação deliberada de agentes econômicos e estatais, que se beneficiam da ausência de controle. Todavia, é imprescindível

[138] Bioni (2019) apresenta a expressão *normas informacionais* como abreviação de *normas informacionais relativas-contextuais*.

que sejam postas em operação estratégias integradas, capazes de regular a circulação de informações em seu conjunto (RODOTÀ, 2008). Nesse sentido, percebemos a importância dos princípios da transparência e do livre acesso, dispostos, respectivamente, nos incisos VI e IV do art. 6º.

A transparência significa a "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, 2018a). Cabe ressaltar que o princípio não está adstrito ao momento de coleta de dados pessoais. Ao contrário, deve permear todas as etapas do tratamento. Embora a disposição legal pareça clara, a discussão sobre a transparência no caso de tecnologias de reconhecimento facial não é tão simples (BIONI; LUCIANO, 2019). Mike Ananny e Kate Crawford (2018) argumentam que a transparência de sistemas de IA frequentemente é vista de maneira idealizada, mas que, na prática, apresenta limitações e pode gerar outros problemas, como danos à privacidade e exposição de grupos marginalizados.

De acordo com os autores, tecnologias baseadas em dados não são compostas apenas por códigos e dados. São, na realidade, uma *assemblage* de fatores humanos e não humanos, que incluem desde técnicas de computação a normas jurídicas e agendas governamentais por trás do uso dos sistemas automatizados. Nesse sentido, não basta que o algoritmo em si seja transparente: todo o sistema deve ser. Além disso, a transparência, sozinha, não é capaz de promover a *accountability*[139] de um sistema. É necessário que reconheçamos as limitações desse princípio, para que sejamos capazes de utilizar "os limites da transparência como ferramentas conceituais para compreender como *assemblages* algorítmicas devem ser responsabilizadas" (ANANNY; CRAWFORD, 2018, tradução nossa).

O livre acesso, por sua vez, é a "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, 2018a). Em conjunto com a transparência, esse princípio assume o papel de reforçar a posição dos indivíduos frente aos controladores de dados, para suprir, "no limite do possível, o *gap* de poder entre estes e os 'senhores da informação'" (RODOTÀ, 2008, p.

[139] O termo *accountability* está relacionado aos conceitos de "responsabilidade (objetiva e subjetiva), controle, transparência, obrigação de prestação de contas, justificativas para as ações que foram ou deixaram de ser empreendidas, premiação e/ou castigo" (PINHO; SACRAMENTO, 2009, p. 1364). Devido à dificuldade de se traduzir o termo para o português, ora utilizaremos a palavra em inglês, ora traduziremos como "responsabilização" ou "prestação de contas", como veremos mais adiante.

68). O direito de acesso se configura, portanto, como “um instrumento capaz de determinar formas de redistribuição de poder” (RODOTÀ, 2008, p. 73). Importante destacar que este direito

> supera o âmbito das informações pessoais e a sua disciplina tende a se conjugar com a outra, mais geral, de um "direito à informação", também esse encarado em uma versão ativa e dinâmica: não mais, portanto, como simples "direito a ser informado mas como o direito a ter acesso direto a determinadas categorias de informações, em mãos públicas e privadas. Aqui desponta claramente a ligação entre os desenvolvimentos institucionais e as inovações tecnológicas: justamente estes tornam possível propor uma generalização do direito de acesso, no momento em que eliminam os obstáculos de caráter "físico" que, no passado, tornavam impossíveis ou extremamente difíceis os acessos à distância, múltiplos, distribuídos em um arco de tempo mais amplo que aquele do horário ordinário dos escritórios, e assim por diante (RODOTÀ, 2008, p. 69).

Nas palavras de Rodotà, o “direito de acesso” é, “antes de tudo, um instrumento diretamente acionável pelos interessados, que podem utilizá-lo não somente com a finalidade de simples conhecimento, mas também para promover propriamente a efetividade” dos direitos relacionados à proteção de dados pessoais (RODOTÀ, 2008, p. 60). O autor defende que deve ser concedido à pessoa o poder de controle direto e contínuo sobre os coletores de informações, independentemente da existência de uma violação a seus direitos, alterando-se assim a técnica de proteção da privacidade e se deslocando a atenção em direção ao bom funcionamento das regras sobre a circulação de informações.

Conquanto esse seja o cenário ideal, a realidade tem demonstrado que são as pessoas que têm se tornado cada vez mais “transparentes” – cada vez mais submetidos à vigilância – e que os órgãos públicos possuem cada vez menos controle político e legal no que tange aos dados pessoais dos cidadãos (RODOTÀ, 2013). Nesse sentido e a título exemplificativo, Barros e Venturini, em análise sobre o município do Rio de Janeiro, expõem que “as atividades do Estado – inclusive na área de segurança pública e vigilância – seguem secretas e pouco sujeitas a escrutínio público, enquanto os cidadãos encontram-se cada vez mais expostos tanto frente ao próprio Estado, quanto a outros agentes privados” (BARROS; VENTURINI, 2018, p. 43) .

Referindo-se à pesquisa realizada pela Fundação Getúlio Vargas (FGV) em 2016, cujo objetivo obter dados da gestão municipal e avaliar o grau de transparência das Prefeituras brasileiras com relação à gestão de dados, a oferta de serviços online e a existência de iniciativas de cidades inteligentes na área de segurança pública, as autoras concluem que “boa parte dos municípios avaliados ainda estão despreparados para enfrentar os novos desafios colocados

pelas práticas de *big data* no que diz respeito às suas políticas de gestão da Tecnologia da Informação e de tratamento de dados pessoais" (BARROS; VENTURINI, 2018, p. 42). Aduzem ainda que,

> na prática, isso significa que os interesses comerciais e corporativos encontram um terreno suscetível à discricionariedade do agente, ou seja, as decisões de contratação, da escolha de padrões, tecnologias, proteções entre outros elementos de uma política de informação municipal ficam na mão do gestor e, de acordo com a pesquisa, há pouca ou quase nenhuma transparência sobre isso. (BARROS; VENTURINI, 2018, p. 42)

Ademais, Mulholland e Frajhof questionam os sistemas de IA dotados de *machine learning*[140], apontando que um fator a se levar em consideração em sistemas de autoaprendizagem "é justamente o fato de que a transparência dos métodos utilizados e, consequentemente, dos resultados alcançados, fica deslocada, abrindo espaço para uma opacidade típica de sistemas autoritários não regulados" (2019, p. 272, 273). Dessa maneira, reitera-se a importância de um dos principais elementos da proteção de dados: o direito de acesso, que significa o poder incondicional que a pessoa deve ter de saber *quem* possui *quais* dados sobre ela e *como* esses dados são usados (RODOTÀ, 2013). Permitir que o cidadão saiba quais são as práticas de vigilância e coleta de dados empregadas pelo Estado, e como se dá o recolhimento, uso e distribuição de seus dados significa, portanto, "dar ao cidadão a garantia do exercício do controle social sobre a administração pública" (BARROS; VENTURINI, 2018, p. 43).

Os princípios da transparência e do livre acesso se relacionam, em grande medida, ao princípio da qualidade dos dados, uma vez que este exige que os dados sejam objetivos, exatos e atualizados, e aqueles asseguram o conhecimento e os meios de correção de informações equivocadas (OLIVEIRA; LOPES, 2019). Nos termos do art. 4º, inciso V, o referido princípio corresponde à "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".

Frazão (2019b) destaca que, a fim de que haja um mínimo de confiança e tranquilidade quanto ao uso de algoritmos baseados em *big data*, são necessários dois tipos de controle

[140] *Machine learning* (traduzido como "aprendizado de máquina") é uma área da ciência da computação, no campo da inteligência artificial. *Grosso modo,* é uma modalidade de programação usada nos computadores, formada por regras previamente definidas que permitem que os computadores tomem decisões com base nos dados prévios e em dados gerados e/ou empregados pelo usuário.

referentes à qualidade. Primeiro, deve haver o controle sobre a qualidade dos dados em si, para verificar se atendem "aos requisitos da veracidade, exatidão, precisão, acurácia e sobretudo adequação e pertinência diante dos fins que justificam a sua utilização". Depois, é necessário avaliar "a qualidade do processamento de dados, a fim de saber se, mesmo a partir de dados de qualidade, a programação utilizada para o seu tratamento é idônea para assegurar resultados confiáveis" (FRAZÃO, 2019b, p. 38).

Em suma, os princípios da transparência, do livre acesso e da qualidade de dados encontram-se amplamente relacionados. A transparência e a possibilidade de acesso são indispensáveis para que possamos avaliar a qualidade dos dados e/ou do tratamento dado a eles, revelando-se, portanto, princípios cruciais para impedir a consolidação de uma *black box society* (PASQUALE, 2015).

4.5.3 Princípios da segurança e prevenção

O princípio da segurança, concretizado no art. 6º, em seu inciso VII, determina a "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" (BRASIL, 2018a). A Seção I do Capítulo da LGPD trata especificamente sobre a segurança na proteção de dados pessoais, estabelecendo, inclusive, que as práticas de segurança devem ser adotadas desde fase de concepção do produto ou do serviço de tratamento de dados até a sua execução (art. 46, §2º).

Prevenção, por sua vez, diz respeito à "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (art. 6º, inciso VIII). Podemos perceber, em vista de todas as discussões trazidas nesta pesquisa, que pensar em prevenção de danos decorrentes do uso de tecnologias de reconhecimento facial não é uma tarefa fácil. De acordo com Frazão, em se tratando do emprego de algoritmos para tomada de decisões automatizadas, "o jeito mais efetivo para minimizar o risco de resultados não desejados é por meio de testes extensivos, a fim de se fazer uma longa lista dos tipos de maus resultados que podem ocorrer e tentar excluí-los sempre que se mostrarem presentes" (FRAZÃO, 2019b, p. 42).

Há, porém, casos em que a realização de testes não é possível ou não se revela totalmente eficiente. Pensemos, por exemplo, no já mencionado fato de o sistema de reconhecimento facial adotado pela prefeitura do Rio de Janeiro ter falhado logo em seu segundo dia de uso, identificando incorretamente uma mulher, o que ocasionou a sua injusta detenção. Ou, então,

no caso do sistema adotado pela cidade de Londres: ainda que mais de 80% dos alertas feitos pelo sistema durante o período de teste estivessem incorretos, a polícia insistiu em sua adoção. Somente a aplicação da tecnologia na prática seria capaz de demonstrar, de fato, quais são os danos que determinadas práticas implicariam. Nesse sentido, antes mesmo da adoção da tecnologia ou da realização de testes, é imperioso avaliar minimamente os riscos decorrentes de seu uso, inclusive para o fim de delimitar quais técnicas de vigilância sequer deveriam ser empregadas.

4.5.3.1 Princípio da precaução

Devemos relembrar que problemas decorrentes de algoritmos enviesados são mais comuns do que deveriam (como exposto no Capítulo 3). Isso o que ocorre por diversas razões, como a falta de regulação, monopólios no setor de IA, assimetrias de poder entre empresas e usuários, a distância cultural entre os responsáveis por pesquisas em tecnologia e a diversidade das populações nas quais essa tecnologia é utilizada (NORRIS, 2003). Isso parece "indicar o abismo entre desenvolvedores desse tipo de tecnologia e aqueles que são impactados por ela" (BIONI; LUCIANO, 2019, p. 208), o que tem levado à maior demanda social no que tange à transparência e à precaução na utilização de tecnologias de IA (FLORIDI et al., 2017).

Segundo Bioni e Luciano, "o princípio da precaução fornece um substrato importante para se pensar medidas e estratégias de regulação de IA, notadamente como lidar com situações de riscos de danos ou de desconhecimento dos potenciais malefícios e benefícios desse tipo de tecnologia" (2019, p. 228). O desenvolvimento recente de tecnologias de informação e comunicação tornou ainda mais patente os potenciais danos e violações a direitos decorrentes do tratamento indevido de dados pessoais. Assim, tornou-se mais complexo o processo de cognição, avaliação e gerenciamento dos riscos de uma economia de dados, sendo que aqueles que detêm os dados passaram a deter também uma "superioridade informacional ainda maior frente aos demais atores cidadãos e órgãos fiscalizadores desse ecossistema" (BIONI; LUCIANO, 2019, p. 216).

Especialmente em relação à utilização de reconhecimento facial baseado em IA, as incertezas quanto aos benefícios e os riscos revelam-se mais evidentes, pelos diversos motivos expostos anteriormente. No que concerne às possibilidades de regulamentação de tais tecnologias, é possível apontar três entendimentos distintos, comparáveis e diferenciáveis devido à carga de atribuição de obrigações precaucionárias diante das incertezas e dos benefícios de seu uso. Num extremo, parte do setor privado acredita em uma "tecnorregulação",

suprida pelas diretrizes éticas do mercado, que evitaria entraves ao desenvolvimento das TRFs. Na outra extremidade, busca-se o banimento total de tecnologias de reconhecimento facial, sob o argumento de que haveria, em seu próprio *design*, um risco desproporcional de opressão e discriminação. "Ao centro desse movimento pendular, encontra-se uma estratégia que visa desenhar uma arquitetura precaucionária de danos", que indica que o emprego de tecnologias de reconhecimento facial deveria ser antecedido de ações por parte do seu próprio proponente, capazes de mitigar seus eventuais malefícios (BIONI; LUCIANO, 2019, p. 221,222).

Independente de qual caminho seja adotado, é preciso considerar que tecnologias de IA, principalmente aquelas que se baseiam na análise dados, não são completamente objetivas e neutras. Tais sistemas "carregam escolhas das entidades e pessoas envolvidas na sua construção, sendo modulado pela agenda política e aspectos socioeconômico, de forma implícita ou explícita, que lhes são subjacentes" (BIONI; LUCIANO, p. 228). Nesse sentido,

> o princípio da precaução apresenta dois vetores de regulação que merecem atenção: a) a abertura do debate regulatório a todos os atores envolvidos na implementação dessa tecnologia (e nas escolhas que ela impõe), de desenvolvedores àqueles que sofrerão seus possíveis efeitos, o que é um requisito obrigatório de um sistema democrático com históricas dinâmicas de assimetria de poder e informação; b) a atribuição de obrigações que reduzam as incertezas quanto aos benefícios e riscos em questão, de sorte a determinar a adoção ou não de IA (BIONI; LUCIANO, p. 228).

4.5.4 Princípio da não discriminação

O princípio da não discriminação há tempos havia conquistado espaço nas legislações sobre proteção de dados (OLIVEIRA; LOPES, 2019). Nos termos do art. 6, inciso IX, trata-se da "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos", estando intimamente ligado ao tratamento diferenciado da categoria dos dados sensíveis. Estes, segundo a definição de Maria Celina Bodin de Moraes, são os "dados pessoais que dizem respeito à saúde, opiniões políticas ou religiosas, hábitos sexuais etc. *aptos a gerar situações de discriminação e desigualdade*" (2010, p. 3, grifo nosso), o que justifica o tratamento especial a eles dispensado.

Nos primeiros capítulos deste trabalho, buscamos demonstrar como o uso de algoritmos, particularmente aqueles empregados em sistemas de reconhecimento facial, pode perpetuar injustiças, preconceitos e discriminações. O tratamento de dados e informações sobre uma pessoa, principalmente aqueles que dizem respeito a aspectos íntimos ou "frágeis" de suas

vidas, pode ser utilizado para toda sorte de discriminações e abusos (FRAZÃO, 2019b). O princípio da não discriminação, evidentemente, tem como objetivo evitar que isso aconteça.

Aliás, cabe dizer que mesmo que o raciocínio matemático efetuado por um sistema de IA esteja correto, este, em si, pode constituir uma espécie de discriminação, "na medida em que o julgamento a respeito de uma pessoa é feito a partir de critérios gerais que desconsideram a sua individualidade" (FRAZÃO, 2019b, p. 34). Por esse motivo, é necessário cuidado com o emprego de tecnologias sem que haja mecanismos de correção de resultados ou de responsabilização de seus desenvolvedores e/ou empregadores.

4.5.5 Princípio da responsabilização e prestação de contas

O princípio da *accountability*, traduzido na LGPD em seu art. 6º, inciso X, como *responsabilização e prestação de contas*, refere-se ao dever de "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, 2018a).

Para Anna Maria Campos (1990), nas sociedades democráticas, é natural e esperável que os governos e o serviço público sejam responsáveis perante os cidadãos, de modo que a noção de *accountability* e o aperfeiçoamento das práticas administrativas andam juntas. A *accountability* pode ser compreendida, então, como uma questão inerente à democracia: "quanto mais avançado o estágio democrático, maior o interesse pela *accountability*", que "tende a acompanhar o avanço de valores democráticos, tais como igualdade, dignidade humana, participação, representatividade" (CAMPOS, 1990, p. 33).

Em que pese a dificuldade de tradução[141] do termo *accountability*, a noção de que não apenas governos, mas também corporações e demais instituições devem ser considerados

[141] Campos iniciou a problematização acerca da tradução do termo *accountability* para a língua portuguesa em 1975, mas, tendo desistido de encontrar uma tradução exata, concentrou-se em compreender seu significado. Para a autora, *accountability* pode ser compreendido "como sinônimo de responsabilidade objetiva ou obrigação de responder por algo: como um conceito oposto a - mas não necessariamente incompatível com - responsabilidade subjetiva. Enquanto a responsabilidade subjetiva vem de dentro da pessoa, a *accountability*, sendo uma responsabilidade objetiva, 'acarreta a responsabilidade de uma pessoa ou organização perante uma outra pessoa, fora de si mesma, por alguma coisa ou por algum tipo de desempenho (MOSHER, 1968, p. 7)'" (CAMPOS, 1990, p. 33). Todavia, ainda hoje "adota-se o pressuposto de que não existe mesmo uma palavra única que o expresse em português. O que se percebe são 'traduções' diferentes para o termo por parte de vários autores, ainda que os termos produzidos possam estar próximos ou convergentes. Em síntese, não existe perfeita concordância nas traduções" (PINHO; SACRAMENTO, 2009, p. 1346). Pinho e Sacramento concluem que "não existe um termo único em português que defina a palavra *accountability*, havendo que trabalhar com uma forma composta. Buscando uma síntese,

responsáveis por seus atos encontra-se plenamente consolidada em inúmeros ordenamentos jurídicos na atualidade. Isso decorre, sobretudo, da consciência de que sistemas algorítmicos para tomada de decisões podem ser utilizados de maneira ilícita ou abusiva, culminando na violação de direitos. Assim, caso ocorra algum dano ao titular dos dados em decorrência da não observação dos princípios da segurança, prevenção ou não discriminação, o princípio da responsabilização e prestação de contas se apresenta como fundamento apto a ensejar a reparação ou minimização do prejuízo ocorrido.

Em relação ao tratamento de dados pessoais nas hipóteses do art. 4º, inciso III[142], os princípios da responsabilização e prestação de contas se concretizam através, principalmente, dos relatórios de impacto à proteção de dados pessoais (doravante, RIPDP), como dispõe o art. 4º, §3º: "a autoridade nacional emitirá opiniões técnicas ou recomendações referentes às exceções previstas no inciso III do caput deste artigo e deverá solicitar aos responsáveis relatórios de impacto à proteção de dados pessoais" (BRASIL, 2018a). Em linhas gerais, esses relatórios são a documentação através da qual o controlador deve registar todos os processos do tratamento de dados, bem como as medidas que adotou para mitigar os possíveis riscos aos direitos dos titulares dos dados (BIONI; LUCIANO, 2019).

Nos termos legais, conforme art. 5º, XVII, relatório de impacto à proteção de dados pessoais é a "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" (BRASIL, 2018a). Embora os RIDPD adquiram cada vez mais importância nas leis de proteção de dados pessoais, a lei geral brasileira não os regulamentou adequadamente (BIONI; LUCIANO, 2019). A despeito de algumas menções ao instrumento, a ausência de um capítulo próprio para tratar da matéria

---

accountability encerra a responsabilidade, a obrigação e a responsabilização de quem ocupa um cargo em prestar contas segundo os parâmetros da lei, estando envolvida a possibilidade de ônus, o que seria a pena para o não cumprimento dessa diretiva" (2009, p. 1348).

[142] "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" (BRASIL, 2018a).

faz com que o RIDPD esteja condicionado à regulamentação posterior por parte da Autoridade Nacional de Proteção de Dados (ANPD), conforme disposto no art. 55-J da Lei[143].

Dessa forma, como a LGPD não procedimentaliza "minimamente em que situações os RIPDP são obrigatórios, muito menos quais devem ser os elementos a compor tal documentação, a incerteza quanto aos malefícios de uma atividade não justifica inação" (BIONI; LUCIANO, 2019). Em se tratando de tecnologias de reconhecimento facial, cujos riscos foram exaustivamente demonstrados anteriormente, a regulamentação dos RIDPD se revela-se, portanto, tanto crucial quanto urgente.

4.6 No Brasil: PL 9736/2018 e PL 4612/2019

Até o momento, neste capítulo, buscamos analisar como a legislação brasileira, nomeadamente a LGPD, pode servir como baliza normativa para a instituição de tecnologias de reconhecimento facial. Todavia, a própria Lei dispõe que 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 deverá ser regido por legislações específicas, o que demonstra a necessidade de um debate ainda mais pontual sobre o assunto. No país, a discussão é incipiente, fazendo-se presente, em âmbito legislativo, no PL 9736/2018 e no PL 4612/2019.

O primeiro deles, PL 9736/2018, de autoria do deputado Julio Lopes (Partido Progressista/RJ), objetiva acrescentar dispositivo à Lei de Execuções Penais (Lei n.º 7.210/1984), a fim de incluir a previsão de identificação por reconhecimento facial aos elementos constitutivos da guia de recolhimento para execução penal. O projeto visa à inclusão do seguinte artigo: "Art. 107-A. As informações constantes da guia de recolhimento serão complementadas pela identificação biométrica por reconhecimento facial, quando o custodiado for recolhido a um estabelecimento penal". Dessa forma, pretende-se que os dados biométricos faciais dos custodiados passem a constar na guia de recolhimento disciplinada no art. 105 e seguintes da referida lei.

A justificação do PL se baseia, principalmente, no aumento da população carcerária no Brasil: "Com o aumento da população no Brasil, o sistema de identificação civil, usado para

[143] "Art. 55-J. Compete à ANPD: XIII - 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 previstos nesta Lei" (BRASIL, 2018a).

fins de identificação criminal, precisa ser aperfeiçoado. Tal medida se justifica pela necessidade do aumento da segurança nos estabelecimentos penais, o que segue uma tendência mundial" (BRASIL, 2018b). O Projeto explica ainda que

> a identificação criminal por reconhecimento facial já vem sendo adotada em outros países que passam por problemas em suas unidades prisionais e constitui-se em uma medida inovadora. Nos Estados Unidos da América, por exemplo, vem sendo utilizada com sucesso até mesmo fora do sistema prisional, em aeroportos e outros locais públicos, para a rápida identificação de fugitivos ou pessoas com mandados de prisão pendentes de cumprimento (BRASIL, 2018b).

No entanto, as justificativas se resumem à "necessidade do aumento de segurança" e à adoção de medidas semelhantes em outros países, não havendo maiores explicações quanto à efetividade da medida e sua real necessidade. Tampouco se explicam as maneiras como os dados serão coletados, armazenados e empregados, faltando clareza no que se refere às finalidades do tratamento dos dados.

O PL 4612/2019, por sua vez, é mais extenso e abrangente, tendo sido, inclusive, apensado ao PL 12/2015[144]. De autoria do deputado Bibo Nunes, do PSL/RS, "dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamento" (BRASIL, 2019).

Em sua justificação, o projeto aponta que "inúmeros são os benefícios para a sociedade" decorrentes do emprego de tecnologias de reconhecimento facial, que "vão dos movimentos do rosto em lugar de mouses ou controles de vídeo game até os códigos de segurança para acesso a sistemas fechados", sendo somente esses os benefícios descritos. O texto traz ainda a consideração de que "com a progressiva disseminação dessas tecnologias, nossos rostos serão nossas identidades muito brevemente", o que faria com que as informações e dados pessoais biométricos se tornem "cada vez mais sensíveis". Diante disso,

> o desenvolvimento e uso de tais tecnologias demanda regulamentação para garantir proteção dos cidadãos contra atos de discriminação e deturpação de seus usos. Urge que preservamos a privacidade do cidadão e defendamos as suas liberdades. *Exceto se por interesse única e exclusivamente do Estado* (BRASIL, 2019, grifo nosso).

[144] O Projeto de Lei em questão dispõe sobre a utilização de sistemas de verificação biométrica em âmbito nacional. Inteiro teor disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1296692&filename=PL+12/2015. Acesso em: 28 jan 2020.

O PL reconhece a necessidade de se criar um marco regulatório capaz de garantir o uso legítimo e responsável de tecnologias de reconhecimento facial, apresentando-se como tal. Porém, falha em definir o que seria "interesse do Estado", não apontando as finalidades específicas do uso dessas tecnologias. Além do mais, como procuramos argumentar no início deste capítulo, afirmar que determinada medida deve ser tomada por ser "do interesse do Estado" pode ser problemático, ora devido ao fato de a medida não ser estritamente necessária (por existirem melhores soluções não adotadas ou analisadas pelo ente público), ora devido ao fato de frequentemente os entes públicos adotarem medidas apenas para fins de *security theater*.

Devido à extensão do PL 4612/2019 e à incipiência da discussão no âmbito da Câmara dos Deputados, nos limitaremos, por enquanto, à apresentação dos pontos citados acima, bem como à indicação da necessidade de uma análise mais aprofundada sobre a iniciativa legislativa.

4.7 Ideais regulatórios: exemplos a serem seguidos?

Não é nosso objetivo, nesta pesquisa, realizar um estudo comparado[145] de normas reguladoras de tecnologias de reconhecimento facial. Entretanto, na presente era da globalização, não há dúvidas de que o ordenamento jurídico de um país deve levar em consideração os desenvolvimentos normativos de outros Estados (BASEDOW, 2014). Com isso em mente, buscaremos, nos tópicos a seguir, apresentar disposições normativas estrangeiras que podem se revelar úteis e, consequentemente, orientar a criação de uma legislação brasileira sobre a matéria.

[145] Reconhecemos a complexidade de se realizar um estudo empregando a metodologia do direito comparado, devido, sobretudo, à multiplicidade de métodos compreendidos dentro dessa disciplina. Para Jürgen Basedow (2014), isso advém da existência de diferentes "clientes" do direito comparado, que são as pessoas e/ou instituições a quem a análise de diferentes ordenamentos jurídicos irá atender. Nesse sentido, aponta o autor, acadêmicos de direito constantemente se valem do direito comparado, principalmente quando o tratamento de determinada matéria em seu ordenamento é incipiente, incompleta ou até mesmo incoerente. Assim, frequentemente buscam inspiração em outros sistemas legais, a fim de aperfeiçoar ou melhor compreender o seu próprio direito, tomando emprestadas ideias reconhecidas em ordenamentos jurídicos estrangeiros e transplantando-as para a sua própria realidade (BASEDOW, 2014). Em vista disso, optamos por apenas trazer reflexões a partir do direito estrangeiro, sem a pretensão de apresentar uma análise de direito comparado.

4.7.1 As disposições da Agência dos Direitos Fundamentais da União Europeia sobre tecnologias de reconhecimento facial

Em novembro de 2019, a Agência dos Direitos Fundamentais[146] (FRA[147]) da União Europeia publicou o artigo intitulado *Facial recognition technology: fundamental rights considerations in the context of law enforcement*. O objetivo da publicação, a primeira específica sobre o assunto realizada pela agência, foi analisar as implicações aos direitos fundamentais decorrentes do uso de tecnologias de reconhecimento facial ao vivo[148] para fins de segurança pública e controle de fronteiras. Para tanto, apresentaram-se dados e análises recentes sobre o tema, bem como entrevistas conduzidas com especialistas e autoridades nacionais de países europeus que têm empregado e/ou testado essas tecnologias.

O documento aponta que a imagem facial de uma pessoa constitui um dado pessoal biométrico, nos termos do artigo 4º, item 14, do GDPR[149]:

> "Dados biométricos" [são] dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, *nomeadamente imagens faciais* ou dados dactiloscópicos (UNIÃO EUROPEIA, 2016, grifo nosso).

Destaca ainda que, conforme artigo 9º, item 1, os dados pessoais biométricos são compreendidos como uma *categoria especial* de dados pessoais, por serem aptos a revelar a origem racial ou étnica de uma pessoa. Devido à sua natureza sensível, as imagens faciais encontram-se dentro da definição de *categorias especiais de dados pessoais* ou *dados pessoais sensíveis*[150], de modo que recebem maior proteção e salvaguardas adicionais em comparação com outros dados pessoais (FRA, 2019).

---

[146] Segundo o sítio eletrônico da União Europeia, "a Agência dos Direitos Fundamentais (FRA) da União Europeia presta serviços de aconselhamento fundamentado e independente aos responsáveis políticos nacionais e da UE, contribuindo assim para alimentar o debate, as políticas e a legislação em matéria de direitos fundamentais e torná-los mais eficazes". Disponível em: https://europa.eu/european-union/about-eu/agencies/fra_pt#em-s%C3%ADntese. Acesso em: 20 maio 2020.

[147] Acrônimo de *Fundamental Rights Agency*.

[148] O artigo emprega o termo *live facial recognition technology*, que se refere à comparação de imagens obtidas a partir de câmeras de segurança em circuitos fechados de televisão com imagens presentes em bases de dados governamentais (FRA, 2019).

[149] Embora frequentemente se traduza para a língua portuguesa como "Regulamento Geral de Proteção de Dados" (RGPD), utilizaremos, no presente trabalho, o acrônimo em língua inglesa, GDPR, em função da maior familiaridade com o termo.

[150] Na Lei geral brasileira, o termo utilizado é "dado pessoal sensível" (art. 5º, II). Importante notar que, assim como a LGPD, o GDPR não traz o conceito de dados pessoais sensíveis, limitando-se à enunciação de tipos de dados que assim são considerados (RIGOLON KORKMAZ, 2019).

O documento prossegue, apontando que a plena observância dos direitos fundamentais é um requisito para quaisquer atividades referentes a *law enforcement*[151], independentemente das tecnologias utilizadas (FRA, 2019). Nesse sentido, a União Europeia e o regime internacional de direitos humanos estabelecem um referencial normativo para criação, desenvolvimento e implementação de tecnologias de reconhecimento facial, que ajuda a avaliar se determinada tecnologia está em consonância com os direitos humanos. No entanto, os direitos fundamentais normalmente não são direitos absolutos, podendo estar sujeitos a limitações. Assim, a FRA apresenta requisitos gerais a serem seguidos para determinar se um direito fundamental pode ou não ser limitado em detrimento de novas tecnologias. Esses requisitos foram retirados do artigo 52, item 1, da Carta dos Direitos Fundamentais da UE, cuja disposição é a seguinte:

> Qualquer restrição ao exercício dos direitos e liberdades reconhecidos pela presente Carta deve ser prevista por lei e respeitar o conteúdo essencial desses direitos e liberdades. Na observância do princípio da proporcionalidade, essas restrições só podem ser introduzidas se forem necessárias e corresponderem efetivamente a objetivos de interesse geral reconhecidos pela União, ou à necessidade de proteção dos direitos e liberdades de terceiros (UNIÃO EUROPEIA, 2012).

Qualquer limitação a um direito fundamental deve, portanto: 1. ser prevista em lei; 2. respeitar o conteúdo essencial dos direitos fundamentais; 3. estar em consonância com objetivos de interesse geral da União Europeia; e 4. ser proporcional. A Agência destaca que todos esses requisitos devem sem cumpridos, enfatizando que qualquer limitação do exercício de direitos e liberdades reconhecidos pela Carta deve respeitar "a essência" desses direitos e liberdades (FRA, 2019). Isso significa dizer que direitos fundamentais – como o direito à privacidade ou à proteção de dados – podem ser limitados até certa medida, mas não completamente desconsiderados. Uma vez determinado que a medida de segurança a ser adotada não viola o núcleo essencial e inalienável de um direito, deve-se proceder à análise da necessidade e proporcionalidade dessa medida, como disposto no artigo acima. Desse modo,

> um objetivo de interesse geral – como a prevenção de crimes ou a busca pela segurança pública – não é, por si só, suficiente para justificar uma interferência. Qualquer interferência em um direito elencado na Carta precisa ser examinada para saber se o objetivo apresentado não pôde ser obtido por

[151] A expressão *law enforcement* pode ser traduzida, a depender do contexto, como *cumprimento da lei*, *aplicação da lei*, *manutenção da ordem,* dentre outros. Pode se referir também ao conceito de *segurança pública* (como no caso em questão), assim como aos órgãos legais encarregados da implementação de disposições normativas.

> outros meios que interfiram menos no direito garantido (FRA, 2019, tradução nossa).

Outro ponto levantado pela FRA diz respeito à importância da supervisão da observância dos direitos fundamentais por parte de órgãos independentes. Destaca-se que a supervisão independente é um componente essencial da proteção de dados pessoais na UE, encontrando amparo legal no artigo 8º, item 3, da Carta dos Direitos Fundamentais[152]. Nas palavras trazidas pela Agência, "tendo em vista as questões de direitos fundamentais em jogo e sua complexidade, a supervisão independente é essencial para proteger verdadeiramente as pessoas cujos direitos podem ser afetados pela tecnologia de reconhecimento facial" (FRA, 2019, tradução nossa).

O artigo discute ainda quais direitos fundamentais são especificamente afetados pelo uso de tecnologias de reconhecimento facial para fins de segurança. Embora não se proponha a realizar uma análise exaustiva do tema, apresenta uma lista de exemplos pertinentes, destacando-se, dentre eles, os seguintes: direitos à privacidade e à proteção de dados pessoais; direito à não discriminação; direito à liberdade de expressão e à liberdade de associação e reunião.

Sobre os direitos à privacidade e à proteção de dados pessoais, a FRA traz a seguinte consideração:

> Os direitos à vida privada e à proteção de dados são centrais para a implantação de tecnologias de reconhecimento facial em locais públicos. Embora os dois estejam intimamente relacionados, são direitos distintos e autônomos. Eles também são descritos [respectivamente] como o direito "clássico" à proteção da privacidade, e como um direito mais "moderno", o direito à proteção de dados. Ambos se esforçam para proteger valores semelhantes, *i.e.*, a autonomia e a dignidade humana dos indivíduos, garantindo-lhes uma esfera pessoal na qual eles podem desenvolver livremente suas personalidades, pensar e moldar suas opiniões. Assim, formam um requisito essencial para o exercício de outros direitos fundamentais, como a liberdade de pensamento, consciência e religião (artigo 10 da Carta [de Direitos Fundamentais da União Europeia]), liberdade de expressão e informação (artigo 11 da Carta) e liberdade de reunião e de associação (artigo 12 da Carta) (FRA, 2019, tradução nossa).

[152] "Artigo 8º. Proteção de dados pessoais 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respetiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."

Como o uso de tecnologias de reconhecimento facial implica a colheita, comparação e armazenamento de imagens faciais em bancos de dados para fins de identificação, ele constitui uma interferência direta aos direitos à privacidade e à proteção de dados pessoais (FRA, 2019). Os dados biométricos faciais são, afinal, dados pessoais sensíveis, e o tratamento desses dados significa necessariamente a diminuição do grau de respeito aos direitos citados. Logo, tratamentos dessa natureza devem ser sujeitos a testes de estrita necessidade e proporcionalidade, incluindo uma evidente base legal que justifique seu uso e um objetivo legítimo pretendido (FRA, 2019). A Agência argumenta ainda que a colheita e o processamento de imagens faciais para a utilização em TRFs precisa estar estritamente alinhada ao regime de proteção de dados pessoais europeu.

Assim, de acordo com os princípios gerais de proteção de dados estabelecidos pelo GDPR e pela Carta, todo e qualquer tratamento de dados faciais biométricos deve:

> a) ser lícito, justo e transparente;
>
> b) seguir um propósito específico, explícito e legítimo (claramente definido na legislação do Estado-Membro ou da União Europeia); e
>
> c) cumprir com os requisitos de minimização do uso de dados, precisão dos dados, limitação de armazenamento, segurança dos dados e responsabilidade e prestação de contas (FRA, 2019, tradução nossa).

4.7.2 A *Ordinance* NO. 107-19 da cidade de São Francisco (EUA)

Dentro da discussão aqui trazida, uma estratégia regulatória que ganha destaque é a *Ordinance*[153] NO. 107-19, da cidade de São Francisco (EUA). A norma chama atenção, imediatamente, pela jurisdição a que se refere, uma vez que regula o uso de tecnologias de reconhecimento facial para fins de vigilância no maior município da área da Baía de São Francisco, que abriga o chamado Vale do Silício – região na parte sul da baía, conhecida por ser um dos maiores centros globais de tecnologia e inovação e sede de empresas como Apple, Google, Microsoft, Tesla, dentre centenas de outras. Promulgada em junho de 2019 pelo Conselho de Supervisores da cidade, a lei conta com a seguinte ementa:

> emenda o Código Administrativo para exigir que os departamentos da Cidade que adquiram tecnologia de vigilância, ou que celebrem acordos para receber informações de tecnologia de vigilância de terceiros, apresentem uma Política

[153] O termo *ordinance* pode ser traduzido, literalmente, como *portaria* ou *decreto*. Todavia, no sistema jurídico estadunidense, o termo se refere à "lei adotada por uma câmara municipal, conselho de supervisores do município ou outro conselho de administração municipal" (LEGAL INFORMATION INSTITUTE, 2020), o que corresponde, no nosso ordenamento jurídico, ao conceito de lei municipal.

> de Tecnologia de Vigilância aprovada pelo Conselho de Supervisores, com base em uma política ou políticas desenvolvidas pelo Comitê de Tecnologia da Informação (COIT), e um Relatório de Impacto da Vigilância ao Conselho em relação a qualquer solicitação de fundos para a aquisição de tal tecnologia ou para aceitar e despender fundos de reserva para tal fim, ou ainda para adquirir equipamentos ou serviços de tecnologia de vigilância; exige que cada departamento da Cidade que possua e opere equipamentos ou serviços de tecnologia de vigilância já existentes apresente ao Conselho uma proposta de Política de Tecnologia de Vigilância que regule o uso da tecnologia de vigilância; e exige que o Controlador, na qualidade de Auditor de Serviços da Cidade, audite anualmente o uso de equipamentos ou serviços de tecnologia de vigilância e a conformidade de tal uso com uma Política de Tecnologia de Vigilância aprovada e forneça um relatório de auditoria ao Conselho de Supervisores (CITY AND COUNTY OF SAN FRANCISCO, 2019, tradução nossa).

Conforme disposto na *SEC.* 19B.2*,* a ementa ao Código Administrativo condiciona o uso de tecnologias de vigilância à aprovação, pelo Conselho de Supervisores da Cidade, de uma Política de Tecnologia para Vigilância. Essa Política é elaborada pelo COIT, após o departamento interessado na aquisição/implementação da tecnologia de vigilância submeter ao órgão um Relatório de Impacto da Vigilância, nos termos da §19B.2 (b)(1). Os demais requisitos para a elaboração da Política encontram-se dispostos nos parágrafos seguintes da subseção.

Importante notar que a Política de Tecnologia para Vigilância só será aprovada se a avaliação realizada pelo Conselho determinar que os impactos positivos da implantação da tecnologia superam os seus efeitos negativos; que os direitos e liberdades civis serão resguardados; e que o uso da tecnologia de vigilância a que se refere a Política não será utilizada com base em fatores discriminatórios ou parciais, nem terá impacto desproporcional a qualquer grupo ou comunidade[154]. Além disso, em caso de aprovação da Política, os órgãos municipais passam a ter a obrigação de submeter relatórios anuais de vigilância[155], que devem ser individualizados em relação a cada tecnologia empregada.

---

[154] "*SEC. 19B.4. STANDARD FOR APPROVAL. It is the policy of the Board of Supervisors that it will approve a Surveillance Technology Policy ordinance only if it determines that the benefits the Surveillance Technology ordinance authorizes outweigh its costs, that the Surveillance Technology Policy ordinance will safeguard civil liberties and civil rights, and that the uses and deployments of the Surveillance Technology under the ordinance will not be based upon discriminatory or viewpoint-based factors or have a disparate impact on any community or Protected Class*" (CITY AND COUNCIL OF SAN FRANCISCO, 2019).

[155] "*SEC. 19B.6. ANNUAL SURVEILLANCE REPORT. (a) A Department that obtains approval for the acquisition of Surveillance Technology under Section 19B.2 must submit to the Board of Supervisors and COIT and make available on its website, an Annual Surveillance Report for each Surveillance Technology used by the City Department within 12 months of Board approval of the applicable Surveillance Technology Policy* (…)" (CITY AND COUNCIL OF SAN FRANCISCO, 2019).

A *ordinance* reconhece ainda que, não obstante tecnologias de vigilância representem uma ameaça à privacidade de todas as pessoas, historicamente foram empregadas a fim de intimidar e oprimir certos grupos e comunidades mais do que outros, incluindo aqueles definidos por critérios de raça, etnia, origem, religião, orientação sexual, renda ou perspectiva política[156]. Particularmente sobre tecnologias de reconhecimento facial, a norma dispõe que a propensão dessas tecnologias para colocar em perigo os direitos civis e as liberdades individuais supera substancialmente seus supostos benefícios. Além disso, o seu uso exacerba injustiças raciais e ameaça a nossa possibilidade de viver livres do contínuo monitoramento do Estado[157].

Portanto, em regra, a *ordinance* NO. 107-19 veda a aplicação de tecnologias de reconhecimento facial, estabelecendo a necessidade de um debate público e informado sobre decisões relacionadas a essas tecnologias[158]. Essas decisões devem ocorrer, sempre que possível, após forte deliberação, dado o impacto que podem causar a diversos direitos e liberdades civis[159]. Em suma, a decisão da cidade de São Francisco, ao aplicar fortemente o princípio da precaução (BIONI; LUCIANO, 2019), reconhece que os riscos apresentados por tecnologias de vigilância são maiores que seus eventuais benefícios, e estabelece importantes medidas de precaução que devem ser tomadas a fim de mitigar os danos que decorreriam do seu uso.

---

156 "*SEC. 1. General Findings. (c) While surveillance technology may threaten the privacy of all of us, surveillance efforts have historically been used to intimidate and oppress certain communities and groups more than others, including those that are defined by a common race, ethnicity, religion, national origin, income level, sexual orientation, or political perspective"* (CITY AND COUNCIL OF SAN FRANCISCO, 2019).

157 "*SEC. 1. General Findings. (d) The propensity for facial recognition technology to endanger civil rights and civil liberties substantially outweighs its purported benefits, and the technology will exacerbate racial injustice and threaten our ability to live free of continuous government monitoring"* (CITY AND COUNCIL OF SAN FRANCISCO, 2019).

158 "*SEC. 1. General Findings. (a) It is essential to have an informed public debate as early as possible about decisions related to surveillance technology*" (CITY AND COUNCIL OF SAN FRANCISCO, 2019).

159 "*SEC. 1. General Findings. (b) Whenever possible, decisions relating to surveillance technology should occur with strong consideration given to the impact such technologies may have on civil rights and civil liberties*" (CITY AND COUNCIL OF SAN FRANCISCO, 2019).

5 CONSIDERAÇÕES FINAIS

Uma simples observação da história nos permite enxergar como novas tecnologias, a despeito dos inúmeros benefícios a elas inerentes, apresentam diversos e inesperados efeitos indesejados. Santos Dumont, inventor do avião, passou os últimos anos de sua vida lamentando que sua criação tenha se tornado um braço das forças armadas no mundo, amplamente utilizado em guerras. Oppenheimer, embora não haja demonstrado remorso por seu papel no desenvolvimento da bomba atômica, reconheceu que seu uso se deu de maneira desproporcional e injusta. Hoje, a internet, as TICs, a inteligência artificial são tecnologias que possuem tantas benesses que sequer conseguiríamos menciona-las todas. Todavia, se mal utilizadas, podem representar uma grave ameaça ao exercício da liberdade individual e até mesmo à própria democracia.

Guardadas as devidas proporções, não é difícil vislumbrar os potenciais danos que podem ser causados por tecnologias de reconhecimento facial. Para dizer o mínimo, seria ingenuidade acreditar que não existirão malefícios decorrentes de sua utilização, principalmente se considerados fatores como os graves problemas presentes em diversas sociedades – racismo estrutural e institucional, machismo, xenofobia – e as limitações técnicas dos *softwares* de identificação biométrica. Não obstante, o que temos visto, com cada vez maior intensidade e abrangência, é a utilização dessas tecnologias para fins de controle social e vigilância, como expusemos no segundo capítulo desta pesquisa.

Parece óbvio – e, em certa medida, o é – que o uso de tecnologias de reconhecimento facial implica uma ameaça ao direito à privacidade. Mas, indo além do senso comum, procuramos demonstrar que o direito à privacidade não é uma só "coisa", não comportando uma definição a partir de um conceito hermético. No contexto de uma sociedade de vigilância, que se manifesta como um pan-óptico digital, o direito à privacidade supera a noção de um direito à intimidade e a ser deixado só, relacionando-se diretamente a aspectos como controle sobre as informações pessoais, igualdade, não discriminação e liberdade. Tentamos demonstrar, a partir de discussões teóricas e exemplos práticos, que as TRFs afetam a privacidade no tange a cada um desses aspectos.

Ademais, atualmente, extremamente necessário é o debate sobre o direito à proteção de dados pessoais, que paulatinamente se descolou do direito à privacidade, apresentando-se enquanto um direito fundamental autônomo. Argumentamos, no terceiro capítulo, que o reconhecimento facial significa uma interferência explícita a esse direito. A biometria facial é,

afinal, um dado biométrico, considerado um dado pessoal sensível. O processamento desses dados, principalmente se realizado concomitantemente ao tratamento de outros dados pessoais, pode criar um registro tão extenso de informações referentes a uma pessoa que culminaria na consolidação definitiva da metáfora do homem de vidro. Independentemente do termo que se use – pegada digital, pessoa digital, memória total –, fato é que o conhecimento profundo sobre a vida de uma pessoa pode servir para que se cometam abusos, discriminações e manipulações, o que representa, dessa forma, a possibilidade de controle total sobre ela.

Diante disso, pensaríamos que, caso se tratasse de uma balança, esta penderia em favor do banimento das tecnologias de reconhecimento facial. Porém, evidentemente, o que tem ocorrido é o contrário. Isso se explica, sobretudo, porque acreditamos na falsa ideia de que existe um *tradeoff* necessário entre segurança e privacidade, ou segurança e proteção de dados, isto é, que o aumento de um implica a diminuição do outro. Trata-se de um pensamento tão enraizado em nossa sociedade que as pessoas não só aceitam se submeterem à vigilância, como também, muitas vezes, defendem apaixonadamente o uso de novas tecnologias para esse fim. E justamente nisso reside a ironia presente no título deste trabalho.

Tecnologias de reconhecimento facial, a despeito de todos os seus pontos negativos, não parecem ser uma tendência passageira. Assim, a sua regulação se revela não só necessária, mas urgente. Apontamos, no capítulo 4, que existem diferentes caminhos para isso. Dentre eles, destaca-se a heterorregulação: o Direito pode, e deve, ser uma meta-tecnologia orientadora do desenvolvimento das TRFs. Todavia, faltam-nos normas que regulamentem especificamente essas tecnologias. Em razão dessa escassez, as legislações gerais de proteção de dados frequentemente são empregadas com esse propósito, uma vez que se tratam de inteligências artificiais que envolvem o processamento de dados pessoais. Logo, os princípios reguladores do regime de proteção de dados são "tomados emprestados", servindo também à regulação dessas tecnologias.

No cenário brasileiro, a Lei Geral de Proteção de Dados Pessoais abarca parcialmente a regulação das tecnologias de reconhecimento facial. No que se refere ao tratamento de dados para fins de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, a Lei prevê a necessidade de criação de legislações específicas que regulamentem a matéria, mas dispõe que os princípios gerais de proteção ao titular de dados serão aplicáveis a qualquer hipótese de tratamento, ainda que seja de interesse público. Nesse sentido, os Projetos de Lei 9736/2018 e 4612/2019 versam, respectivamente, sobre a regulação de tecnologias de identificação biométrica e sobre a regulação de tecnologias

de reconhecimento facial. Devido à incipiência dos projetos, optamos por apresenta-los brevemente, sem nos prolongarmos em sua análise. Finalmente, encerramos o desenvolvimento da pesquisa expondo as orientações da Agência dos Direitos Fundamentais da União Europeia sobre tecnologias de reconhecimento facial, bem como a legislação municipal de São Francisco, nos EUA, que decidiu pela proibição de tais tecnologias.

A partir das discussões trazidas, pudemos compreender a importância dos direitos à privacidade e à proteção de dados pessoais, e como as tecnologias de reconhecimento facial afetam esses direitos. Pudemos, ainda, confirmar a hipótese levantada inicialmente: que o uso de tecnologias de reconhecimento facial para fins de vigilância sem que haja real necessidade ocasiona graves violações aos direitos à privacidade e à proteção de dados, e que a legislação brasileira, não obstante forneça um substrato para a regulação dessas tecnologias, carece de especificidade, o que deverá ser endereçado em legislações próprias sobre o assunto.

Gostaríamos de crer, assim como Rodotà, que o Ocidente tivesse afastado de si qualquer prática totalitária, e que a fundação das civilizações modernas tivesse sido acompanhada da renúncia definitiva à coleta de informações pessoais, que, de tão intensa, é capaz de negar a própria humanidade. Mas cremos, tal qual o jurista italiano, que a vigilância não é um fado. Assim sendo, essa dissertação se propõe a ser uma pequena contribuição ao caro debate que se trava em torno das tecnologias de reconhecimento facial, pleiteando que sejam, ao menos, reconsideradas.

REFERÊNCIAS

ADEE, Sally. “Controversial software claims to tell personality from your face”. *NewScientist*, [*s.l.*], 27 maio 2016. Disponível em: more: https://www.newscientist.com/article/2090656-controversial-software-claims-to-tell-personality-from-your-face/#ixzz6DlZQPj3uhttps://www.newscientist.com/article/2090656-controversial-software-claims-to-tell-personality-from-your-face/. Acesso em: 14 jan. 2020.

AFFONSO, Carlos. Por que é um risco um cadastro com rosto, RG e até nosso modo de andar. *Tecfront*, [*s. l.*], 11 out. 2019. Disponível em: https://tecfront.blogosfera.uol.com.br/2019/10/11/governo-cria-base-de-dados-unificada-que-liga-cpf-rosto-e-forma-de-andar/?fbclid=IwAR2iG0scPfo7sA6Ajh1aRlyH39qN1cmPisqZA3hDLTYUOWNcU8IhTSm4Vlk. Acesso em: 14 jan. 2020.

AFFONSO, Carlos. Você tem cara de que? Veja como robô rotula Bolsonaro, Faustão e Trump. *Tecfront*, [*s. l.*], 23 set. 2019. Disponível em: https://tecfront.blogosfera.uol.com.br/2019/09/23/voce-tem-cara-de-que-veja-como-robo-rotula-bolsonaro-faustao-e-trump/?fbclid=IwAR00ZFQV8U6OoY9YNE8Dhh2kCC6gjqOr4jte46UtWkxmvTdJbXIts70CH0I. Acesso em: 14 jan. 2020.

AGÊNCIA PÚBLICA. Empresas lançam serviço de reconhecimento facial para igrejas no Brasil. *Carta Capital*, [*s.l.*]. Disponível em: https://www.cartacapital.com.br/sociedade/empresas-lancam-servico-de-reconhecimento-facial-para-igrejas-no-brasil/?fbclid=IwAR2fOHTl84aZ6ZjBnWvbver0-UbLB_bhksR_WoHbFdBHhHtOw240tdYkaUI. Acesso em: 14 jan. 2020.

ALBUQUERQUE, Ana Luiza. Em fase de testes, reconhecimento facial no Rio falha no 2º dia. *Folha de S. Paulo*. Rio de Janeiro, 17 jul. 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/07/em-fase-de-testes-reconhecimento-facial-no-rio-falha-no-2o-dia.shtml. Acesso em: 23 jan. 2020.

AMAZON WEB SERVICES. *Amazon Rekognition***:** Automatize sua análise de imagem e vídeo com machine learning. [*s.l.*], 2020. Disponível em: https://aws.amazon.com/pt/rekognition/. Acesso em: 26 jan. 2020.

ANNANY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New media & society*, p. 1-17, 2016. Disponível em: http://mike.ananny.org/papers/anannyCrawford_seeingWithoutKnowing_2016.pdf. Acesso em: 20 ago. 2019.

ANDERSON, Tim. *Oppenheimer’s Dilemma*. [*S.l.*], 19 abr. 2016. Disponível em: http://large.stanford.edu/courses/2016/ph241/anderson1/. Acesso em: 22 jan. 2020.

ASIMOV, Isaac. *Foundation’s Edge*. Nova York: Bantam Bell, 1982.

AURELI, Sofia. Programador brasileiro cria algoritmo que reconhece armas de fogo. *Olhar Digital*, [*s. l.*], 10 out. 2019. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/programador-brasileiro-cria-algoritmo-que-

reconhece-armas-de-fogo/91415?fbclid=IwAR36BmOvvnLQztonUpm-7BqoH8LuOf20Y13ACNcaYo44rOk-BvGV1g0L7dQ. Acesso em: 14 jan. 2020.

BAIÃO, Kelly Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana. *Civilistica.com*. Rio de Janeiro, a. 3, n. 2, jul.-dez./2014. Disponível em: http://civilistica.com/wp-content/uploads/2015/02/Baião-e-Gonçalves-civilistica.com-a.3.n.2.2014.pdf . Acesso em: 09 jul. 2019.

BARBON, Júlia. 151 pessoas são presas por reconhecimento facial no país; 90% são negras. *Folha de S. Paulo*. Rio de Janeiro, 22 nov. 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/11/151-pessoas-sao-presas-por-reconhecimento-facial-no-pais-90-sao-negras.shtml?fbclid=IwAR2DZDMPKee642p3Ru7uUECj8qlMNUVk80_19uW0SqXyXQihxnLFwERqdqk. Acesso em: 14 jan. 2020.

BARBOSA, Bernardo. Número de brasileiros que se declaram pretos cresce no país, diz IBGE. *UOL*, São Paulo, 22 maio 2019. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2019/05/22/ibge-em-todas-as-regioes-mais-brasileiros-se-declaram-pretos.htm. Acesso em: 20 jan. 2020.

BARROS, Marina; VENTURINI, Jamila. OS DESAFIOS DO AVANÇO DAS INICIATIVAS DE CIDADES INTELIGENTES NOS MUNICÍPIOS BRASILEIROS. In: MAGRANI, Eduardo. (Org.). *Horizonte presente*: Debates de tecnologia e sociedade. 1ed. Rio de Janeiro: Letramento, 2019, v. 1, p. 31-45.

BASEDOW, Jürgen. Comparative Law and its Clients. *The American Journal of Comparative Law*, v. 62, 2014, p. 821-857.

BENTHAM, Jeremy. O Panóptico ou a casa de inspeção. In: SILVA, Tomaz Tadeu da (org.). *O Panóptico*. 2. ed. Belo Horizonte: Autêntica, 2008.

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

BIONI, Bruno Ricardo; LUCIANO, Maria. O Princípio da Precaução na Regulação de Inteligência Artificial: seriam as leis de proteção de dados o seu portal de entrada? In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Org.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

BIRNBAUM, Emily. Supreme Court declines to hear Facebook facial recognition case. *The Hill*, [*s.l.*], 21 jan. 2020. Disponível em: https://thehill.com/policy/technology/479126-supreme-court-declines-to-hear-facebook-facial-recognition-case. Acesso em: 22 jan. 2020.

BLOOMBERG NEWS. Facial Recognition Is Everywhere at China's New Mega Airport. *Bloomberg*, [*s.l.*], 11 dez. 2019. Disponível em: https://www.bloomberg.com/news/articles/2019-12-11/face-recognition-tech-is-everywhere-at-china-s-new-mega-airport. Acesso em: 23 jan. 2020.

BRANCO, Sérgio. Prefácio. In: MAGRANI, Eduardo**.** *Entre dados e robôs*: Ética e Privacidade na Era da Hiperconectividade. 2.ed. Porto Alegre: Arquipélago Editorial, 2019.

BODIN DE MORAES, Maria Celina. Ampliando os direitos da personalidade. In: *Na medida da pessoa humana*. Rio de Janeiro: Renovar, 2010, p. 1-20.

BRANDON, John. There Are Now 15,000 Deepfake Videos on Social Media. Yes, You Should Worry. *Forbes*, [*s.l.*], 8 out. 2019. Disponível em: https://www.forbes.com/sites/johnbbrandon/2019/10/08/there-are-now-15000-deepfake-videos-on-social-media-yes-you-should-worry/?fbclid=IwAR0DepPtIJu4z4hZfTLQqEMNYRsqqmrt2BEWX5Bw71Sz439xvp_F-Sxma0M#2b4400493750. Acesso em: 14 jan. 2020.

BRASIL. *Constituição* (1988). Constituição da República Federativa do Brasil. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 30 jan. 2020.

BRASIL. Lei n.º 10.406, de 10 de janeiro de 2002. *Código Civil*. Brasília, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 30 jan. 2020.

BRASIL. Lei 13.709/2018, de 14 de agosto de 2018a. Regulamenta a proteção de dados. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 23 jul. 2019.

BRASIL. Câmara dos Deputados. Projeto de Lei N.º 12/2015, de 02 de fevereiro de 2015. Dispõe sobre a utilização de sistemas de verificação biométrica e dá outras providências. Brasília, 02 fev. 2015. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1296692&filename=PL+12/2015. Acesso em: 28 jan. 2020.

BRASIL. Câmara dos Deputados. Projeto de Lei N.º 9.736, de 07 de março de 2018b. Acrescenta dispositivo à Lei n.º 7.210, de 11 de julho de 1984, para incluir a previsão de identificação por reconhecimento facial. Brasília, 07 mar. 2018. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2169011. Acesso em: 28 jan. 2020.

BRASIL. Câmara dos Deputados. Projeto de Lei N.º 4.612, de 21 de agosto de 2019. Dispõe sobre o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional, bem como outras tecnologias digitais voltadas à identificação de indivíduos e à predição ou análise de comportamentos. Brasília, 21 ago. 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2216455. Acesso em: 28 jan. 2020.

BRASIL. Senado Federal. Proposta de Emenda à Constituição n° 17, de 2019. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/135594. Acesso em: 30 jan. 2020.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. *Proceedings of Machine Learning Research*, [*s.l.*],

2018. Disponível em: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf. Acesso em: 17 fev. 2020.

BUOLAMWINI, Joy. Response: Racial and Gender bias in Amazon Rekognition — Commercial AI System for Analyzing Faces. *Medium*, [*s.l.*], 25 jan. 2019. Disponível em: https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced. Acesso em: 17 fev. 2020.

BYFIELD, Natalie P. Race science and surveillance: police as the new race scientists. *Social Identities*, vol. 25, n. 1, p. 91-96, 2018. Disponível em: https://doi.org/10.1080/13504630.2017.1418599. Acesso em: 17 fev. 2020.

CAMPBELL, Charlie. How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens. *Times*, Shengdu, 2019. Disponível em: https://time.com/collection/davos-2019/5502592/china-social-credit-score/. Acesso em: 24 jan. 2020.

CAMPOS, Anna Maria. *Accountability:* quando poderemos traduzi-la para o Português. *Revista de Administração Pública*, 1990 (Fev./abr.). Disponível em: http://bibliotecadigital.fgv.br/ojs/index.php/rap/article/view/9049/8182. Acesso em: 20 mar. 2020.

CASTELLS, Mannuel. *A Galáxia da Internet*: reflexões sobre a Internet, os negócios e a sociedade. Tradução de Maria Luiza X. de A. Borges, revisão Paulo Vaz. Rio de Janeiro: Jorge Zahar, 2003.

CELLARD, André. A análise documental. In: POUPART, Jean et. al. (Org). *A pesquisa qualitativa***:** enfoques epistemológicos e metodológicos. Petrópolis: Vozes, 2008.

CESEC (CENTRO DE ESTUDOS DE SEGURANÇA E CIDADANIA). *Retratos da Violência*: Cinco meses de monitoramento, análises e descobertas. Disponível em: http://observatorioseguranca.com.br/wp-content/uploads/2019/11/1relatoriorede.pdf. Acesso em: 26 jan. 2020.

CHEN, Stephen. China takes surveillance to new heights with flock of robotic Doves, but do they come in peace?. *South China Morning Post*, Pequim, 24 jun. 2018. Disponível em: https://www.scmp.com/news/china/society/article/2152027/china-takes-surveillance-new-heights-flock-robotic-doves-do-they. Acesso em: 23 jan. 2020.

CITY AND COUNTY OF SAN FRANCISCO. Board of Supervisors. *Ordinance NO. 107-19*, de 2019. Administrative Code – Acquisition of Surveillance Technology. Disponível em: https://sfgov.legistar.com/View.ashx?M=F&ID=7321214&GUID=0045453C-D4AB-4620-81AC-CB75FBF5649C. Acesso em: 23 jun 2019.

COLE, Samantha. People Are Using AI to Create Fake Porn of Their Friends and Classmates". *Vice*, [*s.l.*], 26 jan. 2018. Disponível em: https://www.vice.com/en_us/article/ev5eba/ai-fake-porn-of-friends-deepfakes. Acesso em: 22 jan. 2020.

CONSTANTINE, Zoi. Where your data travels when you use biometric boarding at Dubai airport. *Wired,* [*s.l.*], 22 set. 2019. Disponível em: https://wired.me/technology/privacy/emirates-facial-recognition/. Acesso em: 22 jan. 2020.

CRAWFORD, Kate; PAGLEN, Trevor. *Excavating AI*: The Politics of Images in Machine Learning Training Sets. Disponível em: https://www.excavating.ai. Acesso em: 14 jan. 2020.

CRAWFORD, Kate *et al. AI Now 2019 Report*. AI Now Institute, Nova Iorque, 2019, Disponível em: https://ainowinstitute.org/AI_Now_2019_Report.html. Acesso em: 22 jan. 2020.

CRENSHAW, Kimberlé. Documento para o encontro de especialistas em aspectos da discriminação racial relativos ao gênero. *Revista de Estudos Feministas*, 2002, v. 7, n. 12, p. 171-88.

DELCKER, Janosch; SMITH-MEYER, Bjarke. EU considers temporary ban on facial recognition in public spaces. *POLITICO*, [*s.l.*], 17 jan. 2020. Disponível em: https://www.politico.eu/article/eu-considers-temporary-ban-on-facial-recognition-in-public-spaces/. Acesso em: 27 jan. 2020.

DESJARDINS, Jeff. Every Single Cognitive Bias in One Infographic. *Visual Capitalist,* [*s.l.*], 25 set. 2017. Disponível em: https://www.visualcapitalist.com/every-single-cognitive-bias/?fbclid=IwAR0NDq7ExQx5Y1s17-Rx_XM-upY8_dTW2wJK56dyIrmLREGMdXOmUMAQeGg. Acesso em: 14 jan. 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico,* Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo et al. Considerações iniciais sobre inteligência artificial, ética e autonomia pessoal. *Pensar*, Fortaleza, v. 23, n. 4, p. 1-17, out./dez. 2018.

DOURADO, Maria. 99, Itaú e Quod são notificados por usar reconhecimento facial. *Olhar Digital*, [*s. l.*], 04 jun. 2019. Disponível em: https://olhardigital.com.br/noticia/99-itau-e-quod-sao-notificados-pelo-uso-do-reconhecimento-facial-em-seus-servicos/86491?fbclid=IwAR3h5I8t2SAw6z_EMkxkGxZdYs15FUH1pPK1f2olgGZk1uSuFcLr8R-4yQk. Acesso em: 14 jan. 2020.

EGGERS, W.; SCHATSKY, D.; VIECHNICKI, P. *AI-augmented government*: Using cognitive technologies to redesign public sector work. [*s.l.*], 2017. Disponível em: https://www2.deloitte.com/insights/us/en/focus/cognitive-technologies/artificial-intelligence-government.html. Acesso em: 5 ago. 2018.

ESTADÃO CONTEÚDO. Boticário vai ter ferramentas de reconhecimento facial. *Época Negócios*, [*s.l.*], 11 nov. 2019. Disponível em: https://epocanegocios.globo.com/Tecnologia/noticia/2019/11/epoca-negocios-artur-grynbaum-vamos-ter-ferramentas-de-reconhecimento-facial.html. Acesso em: 22 jan. 2020.

ESTADOS UNIDOS DA AMÉRICA. *Records, computers and the rights of citizens*. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973. Disponível em: https://epic.org/privacy/hew1973report/c3.htm. Acesso em: 25 set. 2019.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA). *Facial recognition technology:* fundamental rights considerations in the context of law enforcement.

Disponível em: https://fra.europa.eu/en/publication/2019/facial-recognition?fbclid=IwAR0x1fPeMzs61bU4Z0UaSH3FIRb2vpFPy5XZIyZzLKj3KN2Ap376s5QEcvQ. Acesso em: 14 jan. 2020.

EVANS, Melanie. Facial-Recognition Software Was Able to Identify Patients From MRI Scans. *The Wall Street Journal*, [*s.l.*], 23 out. 2019. Disponível em: https://www.wsj.com/articles/facial-recognition-software-was-able-to-identify-patients-from-mri-scans-11571864543?fbclid=IwAR3zp_mgemWGEgsw81MCnbaxCjbI4tQOxje4aRECYYWUALGXE1oCN2T9nHc. Acesso em: 14 jan. 2020.

FABRÍCIO FILHO. Professores brasileiros realizam chamada por reconhecimento facial. *Olhar Digital*, [*s. l.*], 24 out. 2019. Disponível em: https://olhardigital.com.br/noticia/professores-brasileiros-realizam-chamada-por-reconhecimento-facial/92046?fbclid=IwAR2oNQc_gDOdMPFYh7vE2j5n58qbCVYTfvvVqHPik3Gujg263dgLQT5QnMI. Acesso em: 14 jan. 2020.

FAULKNER, Wendy. The technology question in feminism: a view from feminist technology studies. *Women's Studies International Forum*, v. 24, n. 1, p. 79–95, 2001.

FINANCIAL TIMES. Facial recognition's risks demand a temporary halt. *Financial Times*, [*s.l.*], 21 jan. 2020. Disponível em: https://www.ft.com/content/39432390-3c3e-11ea-b232-000f4477fbca. Acesso em: 22 jan. 2020.

FLORIDI, Luciano. Big Data and Their Epistemological Challenge. *Philosophy & Technology,* v. 25, p. 435-437, 2012..

FLORIDI, Luciano. Four challenges for a theory of informational privacy. *Ethics and Information Technology*, [*s.l.*], v. 8, n. 3, p.109-119, 25 out. 2006.

FLORIDI, Luciano. Soft ethics, the governance of the digital and the General Data Protection Regulation. *Philosophical Transactions of The Royal Society A Mathematical Physical and Engineering Sciences*. Disponível em: https://www.researchgate.net/publication/328292318_Soft_ethics_the_governance_of_the_digital_and_the_General_Data_Protection_Regulation. Acesso em: 23 jun. 2019.

FLORIDI, L. et al. AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines*. Disponível em: https://www.researchgate.net/publication/329192820_AI4People-An_Ethical_Framework_for_a_Good_AI_Society_Opportunities_Risks_Principles_and_Recommendations. Acesso em: 23 jun. 2019.

FLORIDI, L. et al. Artificial Intelligence and the 'Good Society': the US, EU, and UK approach. *Science and Engineering Ethics*. Springer, 2017, p. 1-24.

FLORIDI, L.; TADDEO, M.. What is data ethics?. *Philosophical Transactions of The Royal Society A Mathematical Physical and Engineering Sciences*. 2016. Disponível em: https://www.researchgate.net/publication/310393920_What_is_data_ethics. Acesso em: 23 jun. 2019.

FONSECA, J. J. S. *Metodologia da pesquisa científica*. Fortaleza: UEC, 2002. Apostila.

FORTES, Leandro. Memórias da angústia: Às vésperas do centenário do vôo histórico do 14-Bis, cartas inéditas revelam a depressão dos últimos anos de Santos Dumont. *Revista Época*, [*s.l.*], 10 set. 2004. Disponível em: http://revistaepoca.globo.com/Revista/Epoca/0,,EDG66403-6011,00-MEMORIAS+DA+ANGUSTIA.html. Acesso em: 22 jan. 2020.

FOUCAULT, Michel. *Vigiar e punir*: nascimento da prisão. 20. ed. Petrópolis: Vozes, 1999.

FOUCAULT, Michel. *Nascimento da Biopolítica*. São Paulo: Martins Fontes, 2008.

FRAZÃO, Ana. Direitos Básicos Dos Titulares De Dados Pessoais. *Revista Do Advogado*, São Paulo, n. 144, nov. 2019a.

FRAZÃO, Ana. Fundamentos da proteção de dados pessoais. Noções introdutórias para a compreensão da importância da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1.ed. São Paulo: Thomson Reuters Brasil, 2019b. p. 23-52.

FRAZÃO, Ana**.** Objetivos e Alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1. ed. São Paulo: Thomson Reuters Brasil, 2019c. p. 99-129.

FRAZÃO, Ana; OLIVA , Milena D.; ABÍLIO, Vivianne S. *Compliance* de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA , Milena D. (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 677-713.

FREIRE, Victor. Reconhecimento facial intensifica segurança nos aeroportos. *Arquivo Serpro*, *[s.l.*], [201-?]. Disponível em: http://intra.serpro.gov.br/tema/noticias-tema/reconhecimento-facial-intensifica-seguranca-nos-aeroportos. Acesso em: 22 jan. 2020.

FUSSEY, Pete; MURRAY, Daragh. Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. *The Human Rights, Big Data and Technology Project*, Londres, jul. 2019. Disponível em: http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf. Acesso em: 05 fev. 2020.

GHAFFARY, Shirin; MOLLA, Rani. Here's where the US government is using facial recognition technology to surveil Americans. *Vox*, [*s.l.*], 10 dez. 2020. Disponível em: https://www.vox.com/recode/2019/7/18/20698307/facial-recognition-technology-us-government-fight-for-the-future. Acesso em: 26 jan. 2020.

GIL, A. C. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Atlas, 2002.

GILLIOM, John; MONAHAN, Torin. *Supervision*: An introduction to the surveillance society. Chicago: The University of Chicago Press, 2013.

GOVERNO DO ESTADO DA BAHIA. *Lançado sistema de videomonitoramento inteligente de segurança*. Disponível em: http://www.casacivil.ba.gov.br/2018/12/1271/Lancado-sistema-de-videomonitoramento-inteligente-de-seguranca.html. Acesso em: 20 ago. 2019.

GOVERNO DO ESTADO DE SÃO PAULO. *Metrô compra sistema de monitoramento eletrônico com reconhecimento facial*. Disponível em: http://www.metro.sp.gov.br/noticias/28-06-2019-metro-compra-sistema-de-monitoramento-eletronico-com-reconhecimento-facial.fss. Acesso em: 22 jan. 2020.

Guns recognition. *Aiquimist¸* 2019. Disponível em: https://aiquimist.com/index.php/guns-recognition/. Acesso em: 20 jan. 2020.

HAMILL, Jasper. "Chinese iPhone X owners claim Apple's facial recognition cannot tell them apart". *METRO News*, [*s.l.*], 22 dez. 2017. Disponível em: https://metro.co.uk/2017/12/22/iphone-x-racist-cant-tell-chinese-people-apart-apple-customers-claim-7178957/. Acesso em: 20 jan. 2020.

HAN, Byung-Chul. *No enxame:* perspectivas do digital. Tradução de Lucas Machado. Petrópolis, RJ: Vozes, 2018a.

HAN, Byung-Chul. *Psicopolítica:* O neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018b.

HAO, Karen. An AI app that "undressed" women shows how deepfakes harm the most vulnerable. *MIT Technology Review*, [*s. l.],* 28 jun. 2019a. Disponível em: https://www.technologyreview.com/s/613898/an-ai-app-that-undressed-women-shows-how-deepfakes-harm-the-most-vulnerable/?fbclid=IwAR0w2t6Q9i3xiCkeeZJFBOBhseWoH-mTFAh3DZVM4-8ayqWYNd6Xp6y_tGg. Acesso em: 14 jan. 2020.

HAO, Karen. This is how AI bias really happens - and why it's so hard to fix. 2019b. *MIT Technology Review*. Disponível em: https://www.technologyreview.com/s/612876/this-ishow-ai-bias-really-happensand-why-its-so-hard-to-fix/ . Acesso em: 14 jan. 2020.

HARTZOG, Woodrow; SELLINGER, Evan. Facial Recognition Is the Perfect Tool for Oppression. *Medium*, [*s.l.*], 02 ago. 2018. Disponível em: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66. Acesso em: 14 jul. 2019.

HARWELL, Drew. FBI, ICE find state driver's license photos are a gold mine for facial-recognition searches. *The Washington Post*, [*s.l.*], 07 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: 26 jan. 2020.

HERN, Alex. Google's solution to accidental algorithmic racism: ban gorillas. *The Guardian*, [*s.l.*], 12 jan. 2018. Disponível em: https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people. Acesso em: 14 jan. 2020.

HOUSER, Kristin. AOC WARNS THAT FACIAL RECOGNITION IS "REAL-LIFE 'BLACK MIRROR'". *Futurism*, [*s.l.*], 16 jan. 2020. Disponível em: https://futurism.com/the-byte/aoc-warns-facial-recognition-real-life-black-mirror?utm_campaign=later-linkinbio-futurism&utm_content=later-4882971&utm_medium=social&utm_source=instagram. Acesso em: 22 jan. 2020.

IFLScience. *An Anonymous Company Will Pay $128,000 For The Rights To Your Face*. Disponível em: https://www.iflscience.com/technology/an-anonymous-company-will-pay-128000-for-the-rights-to-your-

face/?fbclid=IwAR1s7sA4aw6OrCvuaH_Mo4MfmgcNLodtT1kH-5mFYSssGUlhJfLW1yrvHAQ. Acesso em: 14 jan. 2020.

IFLScience. *This Conversation Between A Passenger And An Airline Should Absolutely Terrify You.* Disponível em: https://www.iflscience.com/technology/this-conversation-should-terrify-you-viral-thread-about-airport-tech-is-creeping-out-the-internet/?fbclid=IwAR15WeYBbKT_6t82-6FAekrHmYNSZeokTx90dtIWmKaRBxbwy2rAXvLxZyw. Acesso em: 14 jan. 2020.

INDIA TODAY WEB DESK. I was vomiting: Journalist Rana Ayyub reveals horrifying account of deepfake porn plot. *India Today*, Nova Deli, 21 nov. 2018. Disponível em: https://www.indiatoday.in/trending-news/story/journalist-rana-ayyub-deepfake-porn-1393423-2018-11-21. Acesso em: 22 jan. 2020.

JIAQUAN, Zhou. Drones, facial recognition and a social credit system: 10 ways China watches its citizens. *South China Morning Post, [s.l.],* 04 ago. 2018. Disponível em: https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china. Acesso em: 14 jan. 2020.

JUVENAL, Decimo Junio. *Satiras***.** Rio de Janeiro: Tecnoprint, [19--]. 141p.

KELLEHER, John D; TIERNEY, Brendan. *Data Science.* Cambridge: The MIT Press, 2018.

KELION, Leo.Emotion-detecting tech should be restricted by law - AI Now. *BBC News* [s.*l.*], 12 dez. 2019. Disponível em: https://www.bbc.com/news/technology-50761116?fbclid=IwAR1JGVjq3R-PjiN-1rStJq4D-GxlMoYu-kyppIJ6eXfkeQ7OjP7P2R6HM0o. Acesso em: 14 jan. 2020.

KING, Jennifer; MULLIGAN, Deidre; RAPHAEL; Steven. *CITRIS Report:* The San Franciscos Community Safety Camera Program. Disponível em: www.muniwireless.com/reports/sf-video-study-2008.pdf. Acesso em: 20 jan. 2020.

KOSTKA, Genia. "China's social credit systems are highly popular – for now". *MERICS Blog*, [*s.l.*], 17 set. 2018. Disponível em: https://www.merics.org/en/blog/chinas-social-credit-systems-are-highly-popular-now. Acesso em: 24 jan. 2020.

KUNDERA, Milan. *The Unbearable Lightness of Being.* Londres: Faber & Faber, 2000.

LAFLOUFA, Jacqueline. Futuro exige homem multidisciplinar para driblar automatismo do algoritmo. *Tab*, [*s. l.*], 20 ago. 2019. Disponível em: https://tab.uol.com.br/noticias/redacao/2019/08/20/futuro-multidisciplinar-exige-tolerancia-no-mercado-de-trabalho.htm?fbclid=IwAR3vmS_3WDKxjyzRmcSDdLeJEtjUe-PjkRtMwJt1kDXthh_s93-jazAcODA. Acesso em: 14 jan. 2020.

LEGAL INFORMATION INSTITUTE. Cornell Law School. *Wex*, 2020. Disponível em: https://www.law.cornell.edu/wex/ordinance. Acesso em: 30 jan. 2020.

LENTINO, Amanda. This Chinese facial recognition start-up can identify a person in seconds. *CNBC Disruptor,* 17 maio 2019. Disponível em: https://www.cnbc.com/2019/05/16/this-chinese-facial-recognition-start-up-can-id-a-person-in-seconds.html. Acesso em: 14 jan. 2020.

LEVY, Pierre. *A conexão planetária*: o mercado, o ciberespaço, a consciência. Tradução de Maria Lúcia Homem e Ronaldo Entler. São Paulo: Editora 34, 2001.

LI, Jane. "A new Chinese app allows people to use facial verification on their friends and acquaintances". *Quartz*, [*s.l.*], 02 dez. 2019. Disponível em: https://qz.com/1759284/a-new-chinese-police-app-allows-peer-to-peer-facial-scans/. Acesso em: 23 jan. 2020.

LOBEL, Fabrício. Metrô de SP terá vigilância com reconhecimento facial. *Folha de S. Paulo*, [*s.l.*], 17 jul. 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/07/metro-de-sp-tera-vigilancia-com-reconhecimento-facial.shtml. Acesso em: 14 jan. 2020.

LOMAS, Natasha. Europe should ban AI for mass surveillance and social credit scoring, says advisory group. *TechCrunch*, [*s.l.*], 26 jun. 2019. Disponível em: https://techcrunch.com/2019/06/26/europe-should-ban-ai-for-mass-surveillance-and-social-credit-scoring-says-advisory-group/. Acesso em: 14 jan. 2020.

MACHADO, Joana; NEGRI, Sergio. Ensaio sobre a promessa jurídica do esquecimento: uma análise a partir da perspectiva do poder simbólico de Bourdieu. *Revista Brasileira de Políticas Públicas*, v. 7, p. 368-383, 2018.

MACHADO, Ricardo. A repolitização do uso de dados depois de 15 anos de tecnotopia. Entrevista especial com Rafael Zanatta. *Instituto Humanitas Unisinos*, São Leopoldo, 17 out. 2019. Disponível em: http://www.ihu.unisinos.br/159-noticias/entrevistas/593533-a-repolitizacao-do-uso-de-dados-depois-de-15-anos-de-tecnotopia-entrevista-especial-com-rafael-zanatta?fbclid=IwAR0WshBF8GSxWNFCSNNHpEHxJaLAP85WgQ71K9WU3xachzcVXkpu1Wi5A9g. Acesso em: 14 jan. 2020.

MADDEN, Mary. *Privacy, Security, and Digital Inequality*: How Technology Experiences and Resources Vary by Socioeconomic Status, Race, and Ethnicity. Disponível em: https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf. Acesso em: 23 jun. 2019.

MAGRANI, Eduardo**.** *Entre dados e robôs*: Ética e Privacidade na Era da Hiperconectividade. 2.ed. Porto Alegre: Arquipélago Editorial, 2019.

MARR, Bernard. Chinese Social Credit Score: Utopian Big Data Bliss Or Black Mirror On Steroids?. *Forbes*, [*s.l.*], 21 jan. 2019. Disponível em: https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#1d04a6f148b8. Acesso em: 23 jan. 2020.

MARR, Bernard. The Best (And Scariest) Examples Of AI-Enabled Deepfakes. *Forbes*, [*s.l.*], 22 jul. 2019. Disponível em: https://www.forbes.com/sites/bernardmarr/2019/07/22/the-best-and-scariest-examples-of-ai-enabled-deepfakes/?fbclid=IwAR2s0NplLXqtxLTyIB1zXdesqabyEh2sTryVQXYHkNOnMli0WDmbUdytwno#581402022eaf. Acesso em: 14 jan. 2020.

MARX, Gary T. Murky conceptual waters: The public and the private. *Ethics and Information technology*, v. 3, n. 3, p. 157-169, 2001.

MASHABLE. Is the iPhone X's Facial Recognition Twin Compatible?. 2018. Disponível em: https://www.youtube.com/watch?v=e8-yupM-6Oc. Acesso em: 05 fev. 2020.

MCCARTHY, John. *What is artificial intelligence?*. Stanford, 2000. Disponível em: http://www-formal.stanford.edu/jmc/whatisai.pdf. Acesso em: 5 ago. 2018.

MEHR, H. *Artificial Intelligence for Citizen Services and Government*. [S.l], 2017. Disponível em: https://ash.harvard.edu/files/files/artificial_intelligence_for_citizen_services.pdf. Acesso em: 5 ago. 2018.

MITCHELL, Gareth. Can facial recognition software differentiate between identical twins? *BBC Science Focus Magazine,* [*s.l.*]. Disponível em: *https*://www.sciencefocus.com/future-technology/can-facial-recognition-software-differentiate-between-identical-twins/. Acesso em: 14 jan. 2020.

MITTELSTADT, Brent D,; FLORIDI, Luciano. The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Sci Eng Ethics*, v. 22, p. 303-341, 2016. Disponível em: https://www.researchgate.net/publication/305813620_The_Ethics_of_Big_Data_Current_and_Foreseeable_Issues_in_Biomedical_Contexts. Acesso em: 06 maio 2020.

MOLLA, Rani. How Amazon's Ring is creating a surveillance network with video doorbells. *Vox*, [*s.l.*], 10 jan. 2020. Disponível em: https://www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell-hacks. Acesso em: 26 jan. 2020.

MOON, Louise. Pay attention at the back: Chinese school installs facial recognition cameras to keep an eye on pupils. *South China Morning Post*, [*s.l.*], 16 maio 2018. Disponível em: https://www.scmp.com/news/china/society/article/2146387/pay-attention-back-chinese-school-installs-facial-recognition. Acesso em: 23 jan. 2020.

MOURA, Carolina. PM confunde guarda-chuva com fuzil e mata garçom no Rio, afirmam testemunhas. *El País*, Rio de Janeiro, 19 set. 2018. Disponível em: https://brasil.elpais.com/brasil/2018/09/19/politica/1537367458_048104.html. Acesso em: 20 jan. 2020.

MULHOLLAND, Caitlin. Dados pessoais sensíveis e a tutela de Direitos Fundamentais. Uma análise à luz da Lei geral de Proteção de Dados (Lei 13.709/18). *Revista Direitos e Garantias Fundamentais*, Vitória, 2018, v. 19, n. 3, p. 159-180.

MULHOLLAND, Caitlin**.** A TUTELA DA PRIVACIDADE NA INTERNET DAS COISAS (IOT). In: Magrani, Eduardo. (Org.). *Horizonte presente:* Debates de tecnologia e sociedade. 1ed. Rio de Janeiro: Letramento, 2019, v. 1, p. 485-495.

MULHOLLAND, Caitlin; FRAJHOF, Isabella Z. Inteligência Artificial e a Lei Geral de Proteção de dados Pessoais: breves anotações sobre o direito à explicação perante a tomada de decisões por meio de *machine learning*. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (Org.). Inteligência artificial e direito: ética, regulação e responsabilidade. São Paulo: Thomson Reuters Brasil, 2019.

MULSHINE, Molly. "A major flaw in Google's algorithm allegedly tagged two black people's faces with the word 'gorillas'". *Business Insider*, [*s.l.*], 01 jul. 2015. Disponível em: https://www.businessinsider.com/google-tags-black-people-as-gorillas-2015-7. Acesso em: 14 jan. 2020.

NABEEL, Fahad. Regulating Facial Recognition Technology in Public Places. *Centre for Strategic and Contemporary Research*, 2019. Disponível em: https://www.academia.edu/39871139/Regulating_Facial_Recognition_Technology_in_Public_Places. Acesso em: 20 jul. 2019.

NBC NIGHTLY NEWS. *Social Credit System Coming To China, With Citizens Scored On Behavior.* Disponível em: https://www.youtube.com/watch?v=NOk27I2EBac. Acesso em: 14 jan. 2020.

NISSENBAUM, Helen. *Privacy in context*: technology, policy, and the integrity of social life. Stanford: Stanford University Press, 2010.

NOGUEIRA, Luiz. Hering é processada por uso de reconhecimento facial sem consentimento. *Olhar Digital*, [*s.l.*], 03 set. 2019. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/hering-e-processada-por-uso-de-reconhecimento-facial-sem-consentimento/89877. Acesso em: 22 jan. 2020.

NORRIS, Clive. From personal to digital CCTV, the panopticon, and the technological mediation of suspicion and social control. In: LYON, David. *Surveillance as social sorting*: privacy, risk, and digital discrimination. Routledge: New York, 2003. p. 247-281.

NORRIS, Clive; ARMSTRONG, Gary. *The Maximum Surveillance Society*: The Rise of CCTV. Oxford: Berg, 1999.

NUNES, Pablo. Exclusivo: levantamento revela que 90,5% dos presos por monitoramento facial no Brasil são negros. *The Intercept Brasil*, [*s.l.*], 21 nov. 2019. Disponível em: https://theintercept.com/2019/11/21/presos-monitoramento-facial-brasil-negros/. Acesso em: 20 jan. 2020.

OLIVEIRA, Fabiana. O que tem a ver consentimento e vigilância? Diálogos especulativos com Joana Varon. *Lavits, [s.*l], 10 jul. 2019a. Disponível em: http://lavits.org/o-que-tem-a-ver-consentimento-e-vigilancia-dialogos-especulativos-com-joana-varon/?lang=pt. Acesso em: 14 jan. 2020.

OLIVEIRA, Fabiana. 'Os dados são uma forma de gerenciamento policial das populações', afirma Natalie Byfield. *Lavits, [s.*l], 27 ago. 2019b. Disponível em: http://lavits.org/os-dados-sao-uma-forma-de-gerenciamento-policial-das-populacoes-afirma-natalie-byfield/?lang=pt. Acesso em: 14 jan. 2020.

OLIVEIRA, Felipe. Áreas de comércio, serviço e transportes investem em identificação por imagem. *Folha de S. Paulo*, [*s.l.*], 8 abr. 2018. Disponível em: https://www1.folha.uol.com.br/mercado/2018/04/areas-de-comercio-servico-e-transportes-investem-em-identificacao-por-imagem.shtml. Acesso em: 14 jan. 2020.

OLIVEIRA, Marco Aurélio Bellizze; LOPES, Isabela Maria Pereira. Os princípios norteadores da proteção de dados pessoais no Brasil e sua otimização pela Lei 13.709/2018. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

O'NEIL, Cathy. *Weapons of math destruction*: how Big Data increases inequality and threatens democracy. New York: Broadway Books, 2017.

ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 23 de setembro de 1980. Disponível em: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Acesso em: 30 jan. 2020.

ORGANIZAÇÃO PARA COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OCDE*). THE OECD PRIVACY FRAMEWORK.* Disponível em: https://www.oecd.org/internet/ieconomy/privacy-guidelines.htm. Acesso em: 30 jan. 2020.

PAIVA, Fernando. Policiais do Rio vão testar câmera no uniforme para reconhecer criminosos. *Mobile Time*, [*s.l.*], 13 jan. 2020. Disponível em: https://www.mobiletime.com.br/noticias/13/01/2020/policiais-do-rio-vao-testar-camera-no-uniforme-para-reconhecer-criminosos/. Acesso em: 17 jan. 2020.

PASCU, Luana. China introduces facial recognition for WeChat transfers, mandatory biometric scans for SIM cards. *Biometric Update*, [*s.l.*], Disponível em: https://www.biometricupdate.com/201912/china-introduces-facial-recognition-for-wechat-transfers-mandatory-biometric-scans-for-sim-cards. Acesso em: 23 jan. 2020.

PAGALLO, Ugo et al. *New technologies and law: global insights on the legal impacts of technology, law as meta-technology and techno regulation*, 2015. Disponível em: https://lawschoolsgloballeague.com/wp-content/uploads/2017/01/New-Technologies-and-Law-Research-Group-Paper-2015.pdf. Acesso em: 06 maio 2020.

PASQUALE, Frank. *The black box society.* Cambridge: Harvard University Press, 2015.

PINHO, José Antonio Gomes de; SACRAMENTO, Ana Rita Silva. Accountability: já podemos traduzi-la para o português? *Revista de Administração Pública*, Rio de Janeiro, 43(6), 2009. (Nov./Dez.). Disponível em: https://www.scielo.br/pdf/rap/v43n6/06.pdf. Acesso em: 20 mar. 2020.

POLLI, Frida. The Dark Side Of Artificial Intelligence. *Forbes,* [*s.l.*], 5 dez. 2017. Disponível em: https://www.forbes.com/sites/fridapolli/2017/12/05/the-dark-side-of-artificial-intelligence/#285d55212614. Acesso em: 14 jan. 2020.

PREFEITURA DO RIO DE JANEIRO. *RIO+ SEGURO*. Disponível em: http://maisseguro.rio. Acesso em: 20 ago. 2019.

PUIGDEMONT, Oriol. Atentados em mesquitas da Nova Zelândia deixam pelo menos 49 mortos. *El País*, 15 mar. 2019. Disponível em: https://brasil.elpais.com/brasil/2019/03/15/internacional/1552616642_719105.html. Acesso em: 20 jan. 2020.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, p. 40-81, 2018.

REBELLO, Aiuri. Bancada do PSL vai à China conhecer sistema que reconhece rosto de cidadãos. *Folha de S. Paulo*, [*s.l.*], 16 jan. 2019. Disponível em: https://www1.folha.uol.com.br/mercado/2019/01/bancada-do-psl-vai-a-china-importar-sistema-que-reconhece-rosto-de-cidadaos.shtml. Acesso em: 14 jan. 2020.

REDMAN, Thomas C.. If Your Data Is Bad, Your Machine Learning Tools Are Useless. *Harvard Business Review*, [*s.l.*], 02 abr. 2018. Disponível em: https://hbr.org/2018/04/if-your-data-is-bad-your-machine-learning-tools-are-useless?fbclid=IwAR0II73DwyASn1EVnxROD6XLemYjhA0xPlYOW5ueohtteFodU5HRkw1fZcU. Acesso em: 14 jan. 2020.

REUTERS. The one app in China making secure messaging possible. *Abacusnews*, [*s.l.*], 06 set. 2019. Disponível em: https://www.abacusnews.com/digital-life/one-app-china-making-secure-messaging-possible/article/3026055. Acesso em: 23 jan. 2020.

RICHARDS, N. M.; SMART, W. D. *How should the law think about robots?*, 2013. Disponível em: https://ssrn.com/abstract=2263363. Acesso em: jan. 2018.

RIGOLON KORKMAZ, Maria Regina D. C. Dados sensíveis na Lei Geral de Proteção de Dados Pessoais: mecanismos de tutela para o livre desenvolvimento da personalidade. Dissertação (Mestrado em Direito). Faculdade de Direito, Universidade Federal de Juiz de Fora. Juiz de Fora, 118p. 2019.

ROBITSZKI, Dan. CHINA IS SELLING AUTONOMOUS KILLER DRONES TO THE MIDDLE EAST. *Futurism*, [*s.l.*], 6 nov. 2019. Disponível em: https://futurism.com/the-byte/china-selling-autonomous-killer-drones. Acesso em: 23 jan. 2020.

RODOTÀ, Stefano. Transformações do corpo. *Revista Trimestral de Direito Civil*, v. 19, n. 5, 2004, p. 91-107.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. Democracia y protección de datos. *Cuadernos de Derecho Público*, Maio. 2011. Disponível em: https://revistasonline.inap.es/index.php/CDP/article/view/690/745. Acesso em: 23 jan. 2020.

RODOTÀ, Stefano. Some Remarks on Surveillance today. *European Journal of Law and Technology*, Vol. 4, No. 2, 2013. Disponível em: http://ejlt.org/article/view/277/388. Acesso em: 20 ago. 2019.

RODRIGUES, Renan. Prefeitura anuncia expansão do programa Rio+Seguro para Jacarepaguá e Campo Grande. *O Globo*, [*s.l.*], 02 jan. 2020. Disponível em: https://oglobo.globo.com/rio/prefeitura-anuncia-expansao-do-programa-rioseguro-para-jacarepagua-campo-grande-1-24168451. Acesso em: 20 jan. 2020.

ROSE, Adam. Are Face-Detection Cameras Racist?. *TIME*, [*s.l.*], 22 jan. 2020. Disponível em: http://content.time.com/time/business/article/0,8599,1954643,00.html. Acesso em: 20 jan. 2020.

SEARLE, John. *A Redescoberta da Mente*. São Paulo: Martins Fontes, 2006.

SEARLE, John. *The mystery of consciousness*. New York: The New York Review of Books, 1997.

STATT, Nick. See how an AI system classifies you based on your selfie. *The Verge*, [*s. l.*], 16 set. 2019. Disponível em: https://www.theverge.com/tldr/2019/9/16/20869538/imagenet-

roulette-ai-classifier-web-tool-object-image-recognition?fbclid=IwAR1olVnH9mQcN2rIzc_7up3PSoqgtQfY8G33biKAMEuSDYvm8ncM8JcPoUg. Acesso em: 14 jan. 2020.

SCHIPPERS, Birgit. Facial recognition: ten reasons you should be worried about the technology. *The Conversation*, [*s. l.*], 21 ago. 2019. Disponível em: https://theconversation.com/facial-recognition-ten-reasons-you-should-be-worried-about-the-technology-122137. Acesso em: 14 jan. 2020.

SCHNEIER, Bruce. *Beyond Security Theater*, nov. 2009. Disponível em: https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html. Acesso em: 20 jan. 2020.

SILVA, Tarcízio. Linha do Tempo do Racismo Algorítmico. *Blog do Tarcízio Silva*, 2019. Disponível em: https://tarciziosilva.com.br/blog/posts/racismo-algoritmico-linha-do-tempo/. Acesso em: 14 jan. 2020.

SILVA, Victor Hugo. Londres terá câmeras de reconhecimento facial em tempo real. *Tecnoblog*, [*s.l.*], 24 jan. 2020. Disponível em: https://tecnoblog.net/322623/londres-cameras-reconhecimento-facial-tempo-real/. Acesso em: 26 jan. 2020.

SIMONITE, Tom. The Best Algorithms Struggle to Recognize Black Faces Equally. *Wired*, [*s.l.*], 22 jul. 2019. Disponível em: https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/. Acesso em: 22 jan. 2020.

SINGER, Natasha; METZ, Cade. Many Facial-Recognition Systems Are Biased, Says U.S. Study. *The New York Times*, [*s.l.*], 19 dez. 2019. Disponível em: https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=2ahUKEwiXyILc7b3nAhVELLkGHZ3jDcIQFjACegQICxAH&url=https%3A%2F%2Fwww.nytimes.com%2F2019%2F12%2F19%2Ftechnology%2Ffacial-recognition-bias.html&usg=AOvVaw0DCNbFnv5PXnSJw2Lwk9Jp. Acesso em: 22 jan. 2020.

SMITH, Craig. Dealing With Bias in Artificial Intelligence. *The New York Times*. Nova Iorque, 19 nov. 2019. Disponível em: https://www.nytimes.com/2019/11/19/technology/artificial-intelligence-bias.html?fbclid=IwAR2nyAo-nFfh-H6P0XwYsGq0pZ4tXFpV1vPIMxE_Ztea1nJ7dAmsTqL96Uk. Acesso em: 14 jan. 2020.

SNOW, Jacob. Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots. *ACLU Blog*, [*s.l.*], 18 jul. 2018. Disponível em: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28. Acesso em: 23 jan. 2020.

SNOWDEN, Edward. *Live Q&A with Edward Snowden*: Thursday 23rd January, 8pm GMT, 3pm EST. Disponível em: https://edwardsnowden.com/asksnowden/. Acesso em: 14 jan. 2020.

SNOWDEN, Edward. *Permanent Record*. Nova Iorque: Metropolitan Books, 2019.

SOLOVE, Daniel J. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.

SOLOVE, Daniel. *Nothing to Hide*: The False Tradeoff between Privacy and Security. New Haven: Yale University Press, 2011

SOLOVE, Daniel. Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, v. 126, p. 1880-1903, 2013. Disponível em: http://www.harvardlawreview.org/media/pdf/vol126_solove.pdf . Acesso em 15 jun. 2019.

SOPRANA, Paula. Analistas veem risco à privacidade com tecnologia de reconhecimento facial. *Folha de S. Paulo*, [*s.l.*], 17 jan. 2019. Disponível em: https://www1.folha.uol.com.br/tec/2019/01/analistas-veem-risco-a-privacidade-com-tecnologia-de-reconhecimento-facial.shtml. Acesso em: 14 jan. 2020.

SOPRANA, Paula. Concessionária é alvo de processo por leitura facial no metrô de SP. *Folha de S. Paulo*, [*s.l.*], 31 ago. 2018. Disponível em: https://www1.folha.uol.com.br/tec/2018/08/idec-pede-indenizacao-de-r-100-mi-a-empresa-que-identifica-emocoes-no-metro.shtml. Acesso em: 14 jan. 2020.

SOUZA, Renato Rocha. SOBRE A ÉTICA HUMANA E A ÉTICA DOS ALGORITMOS. In: Magrani, Eduardo. (Org.). *Horizonte presente:* Debates de tecnologia e sociedade. 1ed. Rio de Janeiro: Letramento, 2019, v. 1, p. 577-586.

STATT, Nick. Orlando police once again ditch Amazon's facial recognition software. *The Verge*, [*s.l.*], 18 jul. 2019. Disponível em: https://www.theverge.com/2019/7/18/20700072/amazon-rekognition-pilot-program-orlando-florida-law-enforcement-ended. Acesso em: 23 jan. 2020.

SYMANOVICH, Steve. *How does facial recognition work?*. Disponível em: https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html. Acesso em: 19 fev. 2020.

TABAK, Bernardo. Policial do Bope confunde furadeira com arma e mata morador do Andaraí. *G1***,** Rio de Janeiro, 19 maio 2010. Disponível em: http://g1.globo.com/rio-de-janeiro/noticia/2010/05/policial-do-bope-confunde-furadeira-com-arma-e-mata-morador-do-andarai.html. Acesso em: 20 jan. 2020.

TAYLOR, Diana. Border control systems face fire from travellers wrongly delayed. *The Guardian*, [*s.l.*], 07 set. 2019. Disponível em: https://www.theguardian.com/politics/2019/sep/07/border-control-systems-face-fire-from-travellers-wrongly-delayed. Acesso em: 23 jan. 2020.

THUY, Ong. *Dubai Airport is going to use face-scanning virtual aquariums as security checkpoints.* Disponível em: https://www.theverge.com/2017/10/10/16451842/dubai-airport-face-recognition-virtual-aquarium. Acesso em: 20 ago. 2019.

TOMLINSON, Simon. Can you spot a terrorist just by looking at their face? New software can tell if you are anything from a paedophile to an ace poker player by analysing your features. *DailyMail*, [*s.l.*], 24 maio 2016. Disponível em: https://www.dailymail.co.uk/news/article-3606811/Can-spot-terrorist-just-looking-face-Israeli-company-claims-predict-paedophiles-geniuses-ace-poker-players-analysing-features.html. Acesso em: 14 jan. 2020.

UNDERWOOD, Sarah. Distinguishing Identical Twins. *Communications of the ACM*, [*s.l.*], 12 abr. 2018. Disponível em: https://cacm.acm.org/news/226789-distinguishing-identical-twins/fulltext. Acesso em: 14 jan. 2020.

UNIÃO EUROPEIA. *Carta dos Direitos Fundamentais da União Europeia*, de 26 de outubro de 2012. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN. Acesso em: 30 jan. 2020.

UNIÃO EUROPEIA. Regulamento n.º 2016/679, 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). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT#ntc7-L_2016119PT.01000101-E0007. Acesso em: 30 jan. 2020

UNIÃO EUROPEIA. *Agência dos Direitos Fundamentais da União Europeia (FRA)*, [*s.l.*], 19 fev. 2019. Disponível em: https://europa.eu/european-union/about-eu/agencies/fra_pt#em-s%C3%ADntese. Acesso em: 20 maio 2020.

UNIVERSITY OF BATH. *Biased bots:* Human prejudices sneak into AI systems. Bath, 20 dez. 2018. Disponível em: https://www.bath.ac.uk/announcements/biased-bots-human-prejudices-sneak-into-ai-systems/. Acesso em: 14 jan. 2020.

VERBEEK, P. Morality in Design: Design Ethics and the Morality of Technological Artifacts. In: Pieter E. Vermaas, Peter Kroes, Andrew Light, Steven A. Moore (eds.). *Philosophy and Design*: from Engineering to Architecture. Dordrecht: Springer, 2008, p. 91-103

VU, Brandon. "A Technological and Ethical Analysis of Facial Recognition in the Modern Era." In: *A Technological and Ethical Analysis of Facial Recognition in the Modern Era*, 2018. Disponível em: https://www.academia.edu/38066258/A_Technological_and_Ethical_Analysis_of_Facial_Recognition_in_the_Modern_Era. Acesso em: 20 jun. 2019.

WADDELL, Kaveh. *Half of American Adults Are in Police Facial-Recognition Database*. Disponível em: https://www.theatlantic.com/technology/archive/2016/10/half-of-american-adults-are-in-police-facial-recognition-databases/504560/. Acesso em: 20 ago. 2019.

WEBER, Rolf H. Internet of Things–New security and privacy challenges. *Computer Law & Security Review*, v. 26, n. 1, p. 23-30, 2010.

WARREN, Samuel D.; BRANDEIS, Louis D.. The Right to Privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, p.193-220, 14 dez. 1890.

WECHSLER, H. *Reliable face recognition methods*: system design, implementation and evaluation. Springer, 2007.

WEST, Sarah Myers; WHITTAKER, Meredith; CRAWFORD, Kate. Discriminating Systems: Gender, Race and Power in AI. *AI Now Institute,* [*s.l.*], 2019. Disponível em: https://ainowinstitute.org/ discriminatingsystems.html. Acesso em: 20 jun. 2019.

WESTERLUND, Mika. The Emergence of Deepfake Technology: A Review. In: *Technology Innovation Management Review*, [*s.l.*], nov. 2019. Disponível em: https://timreview.ca/article/1282. Acesso em: 16 fev. 2020.

WIGGERS, Kyle. MIT researchers: Amazon's Rekognition shows gender and ethnic bias (updated). *Venture Beat*, [*s.l.*], 24 jan. 2019. Disponível em: https://venturebeat.com/2019/01/24/amazon-rekognition-bias-mit/. Acesso em: 20 jan. 2020.

ZAAGMAN, Elliott. "Outside of China, WeChat is a fish out of water". *Tech In Asia*, 13 out. 2017. Disponível em: https://www.techinasia.com/outside-china-wechat-is-a-fish-out-of-water. Acesso em: 23 jan. 2020.

ZANATTA, Rafael. Ética, Tecnologia e Rupturas Tecnológicas: entrevista com Ricardo Abramovay. *In*: ZANATTA, Rafael; DE PAULA, Pedro; KIRA, Beatriz. *Economias do Compartilhamento e o Direito*. Curitiba: Juruá, 2017. Disponível em: https://www.researchgate.net/publication/338749802_Etica_Tecnologia_e_Rupturas_Tecnologicas_entrevista_com_Ricardo_Abramovay. Acesso em: 22 jan. 2020

ZANATTA, Rafael. A importação das tecnologias chinesas de reconhecimento facial. *E-mancipação*, [*s.l.*], 18 jan. 2019a. Disponível em: https://rafazanatta.blogspot.com/2019/01/a-importacao-das-tecnologias-chinesas.html. Acesso em: 14 jan. 2020.

ZANATTA, Rafael. Reconhecimento facial em debate. *E-mancipação*, [*s.l.*], 25 jul. 2019b. Disponível em: https://rafazanatta.blogspot.com/2019/07/reconhecimento-facial-em-debate.html. Acesso em: 14 jan. 2020.

ZIZI, Martin. The Flaws and Dangers of Facial Recognition. *Security Today*, [*s.l.*], 01 mar. 2019. Disponível em: https://securitytoday.com/articles/2019/03/01/the-flaws-and-dangers-of-facial-recognition.aspx. Acesso em: 26 jan. 2020.

ZUBOFF, Shoshana. *The age of surveillance capitalism*. New York: Public Affairs, 2019.