CAMILA MATTOS DA COSTA

Entre reconhecíveis e irreconhecíveis: Aspectos políticos, econômicos e éticos da adoção de tecnologias de reconhecimento facial no Brasil

Tese de Doutorado
Fevereiro de 2024

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
ESCOLA DE COMUNICAÇÃO SOCIAL
INSTITUTO BRASILEIRO DE INFORMAÇÃO EM CIÊNCIA E TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO

CAMILA MATTOS DA COSTA

ENTRE RECONHECÍVEIS E IRRECONHECÍVEIS: ASPECTOS POLÍTICOS, ECONÔMICOS E ÉTICOS DA ADOÇÃO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL NO BRASIL

RIO DE JANEIRO
2024

CAMILA MATTOS DA COSTA

ENTRE RECONHECÍVEIS E IRRECONHECÍVEIS: ASPECTOS POLÍTICOS, ECONÔMICOS E ÉTICOS DA ADOÇÃO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL NO BRASIL

Tese apresentada ao Curso de Doutorado em Ciência da Informação do Programa de Pós-Graduação do Instituto Brasileiro de Informação em Ciência e Tecnologia e à Universidade Federal do Rio de Janeiro, como requisito à Defesa de Tese de Doutorado em Ciência da Informação.

Orientador: Professor Doutor Arthur Coelho Bezerra.

Rio de Janeiro

2024

CIP - Catalogação na Publicação

C183e

Costa, Camila Mattos da
ENTRE RECONHECÍVEIS E IRRECONHECÍVEIS: ASPECTOS POLÍTICOS, ECONÔMICOS E ÉTICOS DA ADOÇÃO DE TECNOLOGIAS DE RECONHECIMENTO FACIAL NO BRASIL / Camila Mattos da Costa. -- Rio de Janeiro, 2024.
229 f.

Orientador: Arthur Coelho Bezerra.
Tese (doutorado) - Universidade Federal do Rio de Janeiro, Escola da Comunicação, Instituto Brasileiro de Informação em Ciência e Tecnologia, Programa de Pós-Graduação em Ciência da Informação, 2024.

1. Tecnologias de Reconhecimento Facial. 2. Colonialismo de Dados. 3. Colonialismo Digital. 4. Ética Intercultural da Informação. I. Bezerra, Arthur Coelho, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

CAMILA MATTOS DA COSTA

ENTRE RECONHECÍVEIS E IRRECONHECÍVEIS:

ASPECTOS POLÍTICOS, ECONÔMICOS E ÉTICOS DA ADOÇÃO DA TECNOLOGIA DE RECONHECIMENTO FACIAL NO BRASIL

Tese de Doutorado apresentada ao Programa de Pós-Graduação em Ciência da Informação do convênio entre o Instituto Brasileiro de Informação em Ciência e Tecnologia (IBICT) e a Universidade Federal do Rio de Janeiro (UFRJ), como requisito parcial à obtenção do título de Doutor em Ciência da Informação.

Orientador: Prof. Dr. Arthur Coelho Bezerra.

Rio de Janeiro, 27 de fevereiro de 2024.

Prof. Dr. Arthur Coelho Bezerra (Orientador/a) PPGCI IBICT-UFRJ

gov.br Documento assinado digitalmente
ANGELICA ALVES DA CUNHA MARQUES
Data: 28/02/2024 13:58:41-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Angélica Alves da Cunha Marques (Membro interno) PPGCI IBICT-UFRJ

gov.br Documento assinado digitalmente
PAULO CESAR CASTRO DE SOUSA
Data: 06/03/2024 15:30:33-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Paulo César Castro (Membro interno) PPGCI IBICT-UFRJ

gov.br Documento assinado digitalmente
BRUNO DE VASCONCELOS CARDOSO
Data: 04/03/2024 11:10:17-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Bruno de Vasconcelos Cardoso (Membro externo) PPGSA UFRJ

gov.br Documento assinado digitalmente
DAVID BAIAO NEMER
Data: 28/02/2024 16:23:38-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. David Baião Nemer (Membro externo) University of Virginia

Prof. Dr. Ricardo Medeiros Pimenta (Membro suplente interno) PPGCI IBICT-UFRJ

Em memória de Julian Kariri Kariwu

AGRADECIMENTOS

Aos que me ensinaram a voar: Jander, Márcia e Gustavo. Porto seguro e pista de decolagem. Dentro de mim, tem vocês o tempo todo no mundo. Agradeço a minha família, Carolina, Raphael, Tabatha; sem esquecer de Alice e da corujinha, Laura, da minha avó, Clemilda, e de meus tios, Ana Lúcia, Josely e Claudio.

Agradeço todos os dias pela sorte algorítmica que me permitiu encontrar João Vinagre. Faltam palavras enquanto sobram outras tantas alegrias.

Agradeço às pessoas amigas queridas que não me deixaram desistir e que ainda, apesar de tudo, me olham com espanto de admiração, carinho e afeto: Alexandre Pereira, Carlos Cianci, Carolina Matielo, Heder Santana, Ingrid Marques, Karyne Fatturi, Mayara Fonseca, Mohara Valle, Otávio Augusto Cassiano e Renan Hubner.

Rodrigo Aldeia, obrigada pelos montes que atravessamos e os picos que conquistamos juntos e separados. Ao menino Antônio, desejo todas as alegrias do mundo e a doçura de todas as frutas.

Por todos os sons que trouxe à minha vida, agradeço a Bernardo Oliveira.

Não posso deixar de lembrar de Jonas Ferrigolo. Obrigada por muitos momentos, pela escuta, pelas parcerias e pela disponibilidade para tanto.

Aos orientes: Ana Lucia, Aneli, Marcia, Talita, Aureste e Dulce. Orientem-se, moças e rapaz, pela constelação do Cruzeiro do Sul. Agradeço aos amigos e amigas que fiz no doutorado. Em especial, a Patrícia Costa, Tainá Regly e Josir Gomes.

Aos meus amigos do mestrado: Alexandre, Iuri e Sérgio. A Alexandre e Iuri por tornarem qualquer missão possível. Finalmente, alcancei vocês! A Sérgio, que não deixou que eu perdesse a oportunidade de tentar o doutorado-sanduíche.

Gostaria de agradecer à Evelyn Muguet que tomou conta dos meus fiéis companheiros, Txuri e Una para que eu pudesse viajar para o Doutorado Sanduíche e pela companhia de muitos dias. Também preciso agradecer pela companhia de Dandara Abreu.

Eu, que sou chegada e partida, barco à vela em busca de portos distantes, agradeço, em Portugal, a Ariadne Fujioka, a Pedro Almeida, a Pedro Pedrosa e ao Filho da Fruta, David Dias. No Espírito Santo, Hendrigo Venes, Matheus Oliveira e

Michel. Agradeço aos que me mantiveram sã em Minas Gerais: João Vallo e Giselle Moreira.

A Tai Barroso, cujo cuidado me permitiu atravessar o rio que separa os vivos dos mortos.

A Maria do Céu e a Dionísio, por me receberem com tanta doçura em sua amável família. Agradeço à dona Lurdes pelo cuidado e pela organização da bagunça que tantas vezes fiz.

Arthur Bezerra, meu muito obrigada pelo espaço do exercício da liberdade, da autonomia e pelos debates que foram alimento para o meu intelecto.

Meu agradecimento honesto ao sol de uma constelação inteira que é Gustavo Saldanha. Agradeço a Liz-Rejane que me apresentou a um novo mundo possível e serei eternamente grata pela escuta cuidadosa. Meus sinceros agradecimentos a Ricardo Pimenta, pela sensibilidade com que vê a vida e pela generosidade com que desempenha seus papéis.

Agradeço também a Paulo César Castro pelo encontro que mudou o destino da tese e suas considerações na qualificação e defesa. Agradeço aos membros da banca, Angélica Marques, Bruno Cardoso e David Nemer, pela leitura atenta e pelas considerações na qualificação e na defesa de doutorado. Meus mais sinceros agradecimentos aos que encontrei na Universidade do Porto e, em especial, a Fernanda Ribeiro.

Na solidão da tese, agradeço aos membros do Nosso Bloco: foi mais fácil pela companhia de vocês em noites barulhentas. Em especial, a Francisco Machado.

Aos que cuidaram do meu corpo e do meu “espírito”: Dr. Nilson, Gustavo e Isabel.

Agradeço a Rodrigo Taka pela ajuda com planilhas.

Aos muitos trabalhadores de plataforma cujo trabalho se tornou indispensável no mundo de hoje e que, tantas vezes, permitiu que eu comesse em meio ao caos da rotina.

Agradeço também às pessoas que compõem a Campanha Tire Meu Rosto da sua Mira pelo trabalho de militância pelo banimento do reconhecimento facial no Brasil. Em especial, a Horrara Moreira e Raquel Rachid.

À CAPES pelo financiamento 001.

Como diz Vinícius de Morais, “embora haja tanto desencontro, a vida é a arte do encontro”. Na verdade, é melhor usar as palavras de Violeta Parra e dizer, por fim, “g*racias a la vida que me ha dado tanto”*.

Eu sou é eu mesmo. Divêrjo de todo o mundo…
Eu quase que nada sei. Mas desconfio de muita coisa.
O Grande Sertão Veredas – João Guimarães Rosa

RESUMO

COSTA, Camila Mattos da. **Entre reconhecíveis e irreconhecíveis:** aspectos políticos, econômicos e éticos da adoção de tecnologias de reconhecimento facial no Brasil. Orientador: Arthur Bezerra Coelho. 2024. 228 f. Tese (Doutorado em Ciência da Informação) – Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2024.

Tecnologias de reconhecimento facial têm sido utilizadas no Brasil e no mundo com objetivos diversos. Podem atuar no combate a crimes, na busca de pessoas foragidas e/ou desaparecidas, para ingresso em estabelecimentos, no pagamento de contas. Suas diversas utilidades têm causado a sensação de que são cada vez mais imprescindíveis. Contudo, seus impactos são muitos e ainda seguem sob observação. O objetivo deste estudo é analisar aspectos políticos, econômicos e éticos da adoção de ferramentas de reconhecimento facial no Brasil, por meio das abordagens metodológicas exploratória, indutiva-dedutiva e quali-quantitativa. Foram utilizados métodos de revisão não sistemática de literatura, análise documental e de conteúdo, que permitiram a análise de 121 projetos e leis. Desses, foram 44 projetos que tramitam na Câmara dos deputados e 77 leis e projetos oriundos de Assembleias Legislativas de estados brasileiros e do Distrito Federal. Foram feitos 85 pedidos de acesso à informação para 73 órgãos, em nível estadual, e analisados relatórios sobre a adoção de tecnologias de reconhecimento facial no Brasil. O reconhecimento facial tem ganhado cada vez mais destaque no país, o que pode ser observado pelo crescimento da legislação e do debate sobre o tema na Câmara dos deputados e nas assembleias legislativas, além do aumento de projetos de uso dessa tecnologia em andamento. Entre deputados, o debate ético tem aparecido como algo de solução simples, a partir da confiança da maioria dos legisladores de que tecnologias de reconhecimento facial são benéficas. Ainda assim, são diversos os exemplos que envolvem pessoas erroneamente identificadas em casos de falsos positivos e falsos negativos, causando prejuízos a suas vidas. Os gastos econômicos da adoção de tecnologias de reconhecimento facial ainda são de difícil mensuração, pois os contratos são recentes ou de difícil acompanhamento por meio dos mecanismos de transparência existentes. Ainda assim, foi possível observar que diversos estados brasileiros já têm utilizado tecnologias de reconhecimento facial na educação e na segurança pública e seu uso tem crescido. Não é possível afirmar que as tecnologias de reconhecimento facial sejam de fato eficientes para a segurança pública e para a educação. Contudo, há uma preocupação grande com os danos advindos da sua utilização no Brasil por causa dos erros da tecnologia e

da relação com a comodificação da vida, das dinâmicas do colonialismo de dados e do colonialismo digital. Para concluir, defende-se que a ética intercultural da informação é um caminho que favorecerá a imaginação a dar lugar a um novo mundo em que a tecnologia esteja a serviço de comunidades e dos seres que coabitam o planeta.

Palavras-chave: reconhecimento facial; colonialismo de dados; colonialismo digital; ética intercultural da informação.

ABSTRACT

COSTA, Camila Mattos da. **Between recognition and unrecognition:** political, economic and ethical aspects of adopting facial recognition technologies in Brazil. Supervisor: Arthur Coelho Bezerra. 2024. 228 p. Thesis (Doctorate in Information Science). Federal University of Rio de Janeiro, Rio de Janeiro, 2024.

Facial recognition technologies have been used, both in Brazil and around the world, with a wide array of objectives. Fighting crime, searching missing or escaping individuals, building entry permissions, bill payments identification. Its utilities make it appear as if they are becoming more and more indispensable. Its negative impacts, however, are also many and are still subject to being observed. The main goal of this study is to analyze the political, economic and ethical aspects of the adoption of facial recognition tools in Brazil. Done through an exploratory, inductive-deductive and qualitative-quantitative methodological approach. non-systematic literature review methods, document analysis and content analysis were used, which made it possible to analyze 121 projects and laws. Among these were 44 projects which proceeded in the Congress (Câmara dos Deputados) and 77 laws and projects which originated in all of the Brazilian states and DF's State Assemblies (Assembleias Legislativas). 85 requests for information access were made to 73 state level organisms and reports about the adoption of facial recognition tools in Brazil were also analyzed. Interest in Facial Recognition has been growing in the country, which can be seen in the growth of legislation and debates around the theme in the Congress (Câmara dos Deputados) and State Assemblies (Assembleias Legislativas), which are added to the projects for the usage of these technologies that are ongoing. Between all the deputies, the ethical debate has been theorized as an easy solution, as the general belief of legislators is that facial recognition technologies are beneficial. Nevertheless, there are countless examples of erroneous identifications in case of both fake positives and negatives that caused harm in these people's lives. The economic costs of the adoption of facial recognition technologies cannot be easily measured yet, as these contracts are fairly recent or cannot be tracked using the transparency tools available. Nevertheless, it was possible to observe that a wide array of Brazilian states have already been using facial recognition technologies in the education and public safety sectors and that their use has been increasing. It's not possible to conclude that facial recognition technologies are in fact efficient for both public safety and education. However, there's a growing

concern with the damage that comes from the usage of facial recognition technologies in Brazil mainly due to technological errors and its relation with the commodification of life, the dynamics of data colonialism and digital colonialism. To conclude, it is defended that the intercultural ethics of information is a path that favors the imagination to give place to a new world in which technology is at the service of the communities and beings which inhabit planet Earth.

Keywords: facial recognition; data colonialism; digital colonialism; intercultural information ethics.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABIS - Sistema Automatizado de Identificação Biométricas;
Brapci - Base de Dados Referencial de Artigos de Periódicos em Ciência da Informação;
CeSeC - Centro de Estudo de Segurança e Cidadania;
CCTV - Closed-circuit television;
CI - Ciência da Informação;
IA - Inteligência artificial;
INSS - Instituto Nacional de Segurança Social;
LAI - Lei de Acesso à Informação;
LDB - Lei de Diretrizes e Bases da Educação;
LGPD - Lei Geral de Proteção de Dados;
PC - Polícia Civil;
PCDF - Polícia Civil do Distrito Federal;
PDL - Projeto de Decreto Legislativo;
PL - Projeto de Lei;
PM - Polícia Militar;
SERPRO - Serviço Federal de Processamento de Dados;
SSP - Secretaria de Segurança Pública;
TIC - Tecnologia de Informação e Comunicação;
TICs - Tecnologias de Informação e Comunicação;
TRF - Tecnologia de Reconhecimento Facial;
TRFs - Tecnologias de Reconhecimento Facial;
TSOV - Tecnologias de Segurança Orientadas à Vigilância.

SUMÁRIO

1 INTRODUÇÃO

Controle, vigilância e segurança são questões que afetam a vida de todos os indivíduos em sociedade. Essas não são palavras que indicam algo negativo em um primeiro momento. Afinal, é possível afirmar que todos querem uma vida plena em que se sintam seguros. Desse modo, esses não são problemas novos, nem circunscritos a um pequeno número de pessoas, mas têm interessado à coletividade como um todo ao longo do tempo.

A maior parte de nós, cidadãos, desconhece a política de segurança pública, não faz muita ideia de como as políticas públicas para as cidades são planejadas e ignora os gastos com a implementação de tecnologias de vigilância e controle. A realidade é que, ao menos no Brasil, sabemos muito pouco sobre como, quanto e o que o Estado faz com o dinheiro do contribuinte e de que maneira isso afeta a vida dos cidadãos quando, na realidade, é o Estado quem nos deveria prestar contas. O que sabemos é que parece cada vez mais difícil fugir da vigilância que se distribui em diversas áreas da vida social.

Nesse contexto, percebo a vigilância distribuída, conceito elaborado por Fernanda Bruno (2009), como uma das características do regime de informação (Frohmann,1995; González de Gómez, 2002) que vigora na atualidade, dentro do regime capitalista.

Regime de informação torna-se uma categoria de análise apropriada na medida em que permite um diagnóstico de época a partir de uma perspectiva macro. Nesse sentido, o regime é percebido como a combinação

> de uma relação de forças, definindo uma direção e arranjo de mediações comunicacionais e informacionais dentro de um domínio funcional (saúde, educação, previdência, etc.), territorial (município, região, grupo de países) ou de sua combinação (González de Gómez, 2002, p. 40).

Já a vigilância distribuída é percebida como a

> definição do estado geral da vigilância nas sociedades contemporâneas. Em linhas breves, trata-se de uma vigilância que tende a se tornar incorporada a diversos dispositivos, serviços e ambientes que usamos cotidianamente, mas que se exerce de modo descentralizado, não hierárquico e com uma diversidade de propósitos, funções e significações nos mais diferentes setores: nas medidas de segurança e circulação de pessoas, informações e bens; nas estratégias de consumo e marketing; nas formas de

> comunicação, entretenimento e sociabilidade; na prestação de serviços, etc. (Bruno, 2009, p. 2)

Segundo Shoshana Zuboff (2018, p. 18), *o big data* (termo que se refere a grandes bases de dados) é o "componente fundamental de uma nova lógica de acumulação, profundamente intencional e com importantes consequências". Nesta fase do capitalismo, a informação tem papel preponderante. Nela, procura-se "prever e modificar o comportamento humano como meio de produzir receitas e valor de mercado". É, portanto, necessária a identificação e teorização dessa lógica de acumulação presentemente institucionalizada produtora de "agenciamentos em hiperescala de dados objetivos e subjetivos sobre indivíduos e seus *habitat* no intuito de conhecer, controlar e modificar comportamentos para produzir novas variedades de mercantilização, monetização e controle" (Zuboff, 2018, p. 18).

O que diferencia a vigilância atualmente, tornando-a distribuída, é sua incorporação em diversos dispositivos, serviços e ambientes de uso cotidiano. Assim, ela é exercida de modo descentralizado, não hierárquico e com diversos propósitos, funções e significados em setores diversos. A vigilância agora é para todos (Bruno, 2009) e está em todos os lugares: espaços públicos e privados. É o que pode ser observado com a adoção do reconhecimento facial em setores como escolas, transporte público, autenticação de indivíduos, por exemplo. Além disso, problemas de segurança pública são respondidos com tecnologias de vigilância em detrimento de políticas públicas que envolvam melhoras econômicas ou promoção de bem-estar social (Čas *et al*, 2017).

É importante destacar que autoras como Shoshana Zuboff e Fernanda Bruno não estão necessariamente falando da extração massiva de dados pelo Estado, mas por corporações privadas. Contudo, em tempos de neoliberalismo e vigilância massiva, fica cada vez mais difícil definir as fronteiras entre a vigilância de Estado e a vigilância empresarial, pois diversos serviços públicos usam bases de dados privadas e também bases de dados públicas são ofertadas como serviços.

As diversas inovações tecnológicas no campo das Tecnologias de Informação e Comunicação (TICs) têm possibilitado a transformação de comportamentos e práticas sociais em dados passíveis de quantificação. Além disso, os dados e metadados advindos desse processamento sofrem vigilância contínua por parte de empresas e governos. Trata-se de processos denominados por Jose Van Djick (2014) de dataficação e datavigilância. A organização e classificação da informação

por algoritmos encontra-se cada vez mais presente em esferas diversas da vida humana, de modo a mediar a execução de tarefas simples e complexas.

Tal processo do capitalismo deve ser entendido como um sistema em que um pequeno grupo de empresas de tecnologia integraram de modo vertical uma variedade de serviços e funções no cotidiano (Hill, 2019). Todavia, mais do que integração, este sistema pode ser caracterizado por uma lógica distinta que envolve a prestação de serviços ou a conexão de provedores de serviços e usuários, em troca de dados, utilizados para melhor orientar e disciplinar, de modo mais eficiente, tanto usuários quanto provedores (Kalpokas, 2019). Essa é uma configuração que José van Dijck, Poell e de Waal (2018) definem como sociedade de plataforma; que Shoshana Zuboff (2018; 2021) entende por capitalismo de vigilância; Eygene Morozov (2015) e Yeshimabeit Millner e Amy Traub (2021) designam como capitalismo de dados.

Contudo, vale lembrar o destaque de Deivison Faustino e Walter Lippold (2023, p. 47) sobre o uso de expressões, como sociedade da informação, capitalismo de plataforma e capitalismo de vigilância, que podem sugerir o aparecimento de um novo tipo de sistema social, podendo causar um superdimensionamento capaz de criar a ilusão de que há uma “ruptura entre o ‘velho’ capitalismo, baseado na exploração de mais-valor, e o ‘sistema social atual’, pretensamente informatizado, quando, na verdade, seguimos submetidos – de maneira ainda mais precária e violenta que antes –” à complexidade sociometabólica do capital.

Apesar de concordar com Faustino e Lippold (2023), acredito que o uso de tais expressões são uma tentativa de diferenciar o tempo histórico em que vivemos das diferentes fases do sistema capitalista. Por isso, manterei seu uso ao longo do trabalho.

Essas expressões buscam descrever o modelo econômico construído a partir da extração e comodificação de dados, além do uso de *big data* e algoritmos como meios para obter concentração e consolidação do poder, de modo que se intensificam as desigualdades já existentes no capitalismo, como raça, classe, gênero e deficiência (Yeshimabeit; Traub, 2021) porque os processos mediados por *big data* não são capazes de inventar o futuro, mas o programam a partir do passado (O'Neil, 2020).

David Lyon (2019) defende que o capitalismo de vigilância está diretamente ligado a uma cultura de vigilância dependente dos dados que opera de formas diferentes, além de possuir consequências diversas. Para o autor, o capitalismo de vigilância é a fonte que possibilita a cultura de vigilância e vice-versa. Focar nele é observar como a vigilância avança para partes fundamentais da economia política no século XXI. Nesse sentido, deve-se entender o extensivo poder e rentabilidade dos dados pessoais, observando-se que não somente corporações privadas, mas setores governamentais, sistemas de saúde, estabelecimentos de ensino e policiamento e segurança sentem ansiedade para adotar soluções de *big data*.

Segundo Shoshana Zuboff (2021), o capitalismo de vigilância possui três dimensões: i) exploração de várias fontes de dados a registrar tudo de forma generalizada; ii) extração de dados, processo de direção única, sem relação ou responsabilidades estruturais, mas dependente de sinais subjetivos; e iii) análise que significa que a autoridade (espiritual) é suplantada pela técnica (material).

Há diversas formas de considerar a cultura de vigilância. De um lado, relaciona-se com as experiências de vigilância cotidianas. Afinal, os indivíduos convivem com câmeras em espaços públicos e privados, cruzam áreas de segurança em aeroportos, deparam-se com ferramentas de controle e vigilância em prédios, veículos e outros locais. Todos esses dispositivos coletam, armazenam, transmitem e analisam dados. Por outro lado, a cultura de vigilância reside em práticas mais ativas desempenhadas por pessoas, usando mecanismos de busca convencionais ou, mais provavelmente, por meio das mídias sociais.

Yeshimabeit Millner e Ammy Traub (2021) apontam que o problema central não reside nas tecnologias de vigilância em si mesmas, mas nos modos como são utilizadas para reforço das desigualdades de poder preexistentes ou, como assinala Frank Pasquale (2015), o problema da coleta massiva de dados não está na informação em si mesma, mas em seu uso.

O capitalismo de vigilância localiza-se à frente do atual “modo de produção informacional dominante” – conforme a definição de “regime de informação” de González de Gómez (2002, p. 34), anteriormente apresentada.

> um modo de produção informacional dominante em uma formação social, conforme o qual serão definidos sujeitos, instituições, regras e autoridades informacionais, os meios e os recursos preferenciais de informação, os padrões de excelência e os arranjos organizacionais

> de seu processamento seletivo, seus dispositivos de preservação e distribuição (González de Gómez, 2002, p. 34)[1]

Insere-se, portanto, na ordem social capitalista e possui dimensões econômicas, políticas e sociais inter-relacionadas, conforme apontam Nancy Fraser e Rahel Jaeggi (2020). Por isso, é importante analisar as estruturas desse conjunto de determinações e atores múltiplos. Afinal, o capitalismo não é capaz de sobreviver sem a existência de uma privilegiada vinculação do privado com o Estado. Carlos Eduardo Martins (2011) aponta que "longe de significarem realidades que se articulam externamente a partir de lógicas distintas, o econômico e o político constituem dimensões indissociadas de um mesmo processo", ou seja, são a gênese e o desenvolvimento do capitalismo. Por isso, é importante analisar os agenciamentos coletivos que carregam os algoritmos em si também no que refere ao *big data* e aos processos de regulação algorítmica (Morozov, 2018).

A Ciência da Informação (CI) brasileira tem debatido os regimes de informação há cerca de 25 anos (González de Gómez, 1999; 2002; 2012; 2019; Alves; Bezerra, 2019). No entanto, pouco tem sido pensado sobre como os regimes de informação e suas transformações afetam a vida das pessoas por meio da urbanização, da digitalização do cotidiano e da segurança pública[2]. Arthur Bezerra coloca algumas questões relevantes, tais como

> 1) Por que os regimes de informação são como são e não de outra forma? 2) Quais os obstáculos que impedem que os regimes de informação sejam melhores do que são? 3) Como agir para vencer tais obstáculos e transformar os regimes de informação? (Bezerra, 2020, p. 30)

---

[1]O conceito de regime de informação foi elaborado por Bernd Frohmann com base na Teoria Ator-Rede, de Bruno Latour. Maria Nélida González de Gómez aprofunda o conceito. Em 2022, o filósofo sul-coreano Byung-Chul Han publica o livro *Infocracia*. Nele, Regime de informação aparece definido pelo autor como "a forma de dominação na qual informações e seu processamento por algoritmos e inteligência artificial determinam decisivamente processos sociais, econômicos e políticos. Em oposição ao regime disciplinar, não são corpos e energias que são explorados, mas informações e dados. Não é, então, a posse de meios de produção que é decisiva para o ganho de poder, mas o acesso a dados utilizados para vigilância, controle e prognóstico de comportamento psicopolíticos. O regime de informação está acoplado ao capitalismo da informação, que se desenvolve em capitalismo da vigilância e que degrada os seres humanos em gado, em animais de consumo e dados". (Han, 2022, p. 8). Contudo, coletar dados para fins de vigilância só é possível a partir da posse dos meios de produção da tecnologia e dos dispositivos de vigilância e de produção de dados.

[2]Em levantamento realizado em novembro de 2019 na BRAPCI, o termo "segurança pública" recuperou apenas 26 resultados. O termo "regime de informação" recupera 96. A combinação entre os termos "segurança pública" e "regime de informação" recuperou apenas um. O artigo recuperado foi *Vigilância e cultura algorítmica no novo regime de mediação da informação*, de Arthur Coelho Bezerra (2017). Se considerarmos que regime de informação é um conceito e segurança pública corresponde a um campo de estudos, mas também político e de atuação, fica evidente a desproporcionalidade dos resultados obtidos. Este é só um exemplo que não pretendeu ser exaustivo, mas ilustrar um ponto.

Assim, pretende-se pensar a adoção de ferramentas de reconhecimento facial a partir de tais perguntas e da abordagem da teoria crítica da informação (Bezerra, 2019).

> Em nossa teoria crítica da informação, o conceito de regime de informação servirá de orientação para a proposição de diagnósticos de época que sejam capazes de, conforme afirma Frohmann, "mapear os conflituosos processos que resultam em estabilizações provisórias e inquietas de conflitos entre grupos sociais, interesses, discursos e até mesmo artefatos científicos e tecnológicos" (1995, s/p). Em tais diagnósticos, fenômenos como vigilância digital, mineração de dados pessoais e invasão de privacidade, filtragem algorítmica da informação, desinformação e circulação de fake news serão analisados sob a ótica da *crítica negativa*, na medida em que se constituam como obstáculos que impedem que o regime de informação em vigor seja melhor do que poderia ser, tendo em vista o interesse dos indivíduos" (Bezerra, 2019, p. 29-30)

A teoria crítica pode ser usada para aprofundar o pensamento a respeito dos dados, favorecendo a compreensão de suas manifestações na vida cotidiana. Desse modo, a teoria crítica serve, então, para politizar os algoritmos (Didier; Isin; Ruppert, 2019) e nossa relação com eles.

Na teoria crítica, conforme apontado por Melo (2011, p. 252),

> o teórico não busca separar-se do objeto que estuda, não atribui a seus próprios procedimentos investigativos uma postura desinteressada e neutra, limitada à mera quantificação, classificação e comparação de fenômenos observáveis[3].

É a partir desse referencial que pretendo analisar a adoção de tecnologias de reconhecimento facial no Brasil.

O reconhecimento facial é definido como um sistema que mapeia características da face de indivíduos, presentes em fotografias ou vídeos, confrontando as informações extraídas com uma base de dados de rostos conhecidos, objetivando encontrar correspondência entre as imagens (Oliveira, 2021).

> Embora as técnicas empregadas variem, os sistemas de reconhecimento facial geralmente operam a partir de etapas comuns

[3]A outra opção metodológica que considero digna de explicação é a escrita desta tese em primeira pessoa. O "nós" do "eu e a ciência" deixa de fora muitos outros nós. O que personifico aqui, incomum em algumas ciências e mais comum em outras, é o eu que carrega um emaranhado de nós entrelaçados a partir de relações sociais complexas dentro e fora e da ciência. Falam os todos que me formaram enquanto sujeito político na boca (e nos dedos) do eu que significo o mundo para, então, tentar transformá-lo.

> [...]. Primeiramente, uma imagem do rosto da pessoa é capturada a partir de uma foto ou de um 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. 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. (Oliveira, 2021, p. 47)

O reconhecimento facial pode ser definido como um *software* de reconhecimento biométrico com a capacidade de verificar ou identificar um indivíduo por suas características pessoais, em um banco de dados de rostos. Tem sido comumente utilizado para autenticar usuários por meio de serviços de verificação de identidade. Utiliza algoritmos de aprendizado de máquina na pesquisa, captura e análise de contornos faciais para, então, combinar com um banco de dados pré-existente.

São sistemas implementados com o objetivo de identificar sujeitos em vídeos, fotos ou em tempo real, muito utilizados em setores diversos, tais como o judiciário, o varejo e o comércio eletrônico, o automotivo, o setor médico e o de saúde, a mídia, o de entretenimento, entre outros. A utilização de tais sistemas está em alta demanda com base no argumento das crescentes preocupações com a segurança. Operadores da lei têm adotado o reconhecimento facial com cada vez mais frequência para identificar os suspeitos capturados por meio de videomonitoramento, mídia social, entre outros (Emergen Research, 2022).

> Reconhecimento facial, como o próprio termo indica, é um método de identificação ou verificação da identidade de uma pessoa a partir da imagem do seu rosto. No contexto atual, as tecnologias de reconhecimento facial (TRF) correspondem a softwares, programas de computador, que empregam diferentes técnicas de inteligência artificial para reconhecer ou identificar rostos humanos a partir de uma imagem, geralmente obtida a partir de fotos ou vídeos. Esse reconhecimento só é possível, da forma que ocorre hoje, graças à existência de enormes bases de dados (*big data*), nas quais estão registradas imagens dos rostos de um incontável número de pessoas. Capturada a imagem de um indivíduo (seja a partir de meios “tradicionais”, como câmeras de videomonitoramento, seja a partir de uma foto publicada em uma rede social), sua biometria facial é extraída, e os dados processados podem ser utilizados para uma extensiva gama de propósitos. Em linhas gerais, um sistema de

> reconhecimento facial funciona mediante o uso de identificação biométrica para mapear características faciais de uma pessoa presente em uma fotografia ou em um vídeo, comparando as informações obtidas com um banco de dados de rostos conhecidos para encontrar uma correspondência. (Oliveira, 2021, p. 47)

Esse tipo de tecnologia pode ser utilizado para a comprovação de identidade dos indivíduos e para, supostamente, reprimir crimes relativos à identidade; possibilitar acesso a serviços e espaços públicos e privados; identificar criminosos; constituir prova de vida (bastante utilizada pelo governo brasileiro por meio de aplicativos e do egov); liberar equipamentos, entre outras utilizações. Destaca-se que as tecnologias biométricas não se restringem ao reconhecimento facial. Podem utilizar a análise de impressões digitais, retina, íris, a voz, o modo de caminhar, além de outros dados pessoais biométricos como, por exemplo, a análise de sentimentos. Os dispositivos tecnológicos analisam métricas individuais que seriam exclusivas e únicas, de modo a identificá-los e reconhecê-los, conforme apontam Pablo Nunes, Mariah Rafaela Silva e Samuel R. de Oliveira (2022).

O Decreto Federal Nº 10.046, publicado em 9 de outubro de 2019, dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados, define em seu inciso II do artigo 2º que os “atributos biométricos” de interesse do Cadastro são as

> características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar (Brasil, 2019).

No que tange à vigilância e ao monitoramento de dados privados, Bezerra (2019, p. 38) aponta que

> os fenômenos de vigilância e monitoramento de dados privados, filtragem algorítmica da informação, circulação de notícias falsas e demais técnicas de desinformação que grassam no regime de informação contemporâneo são consideradas a partir de suas perspectivas negativas de controle, manipulação, exclusão e opressão de indivíduos e grupos sociais, que representam obstáculos à privacidade, liberdade e autonomia informacional dos indivíduos. (Bezerra, 2019, p. 38)

Parece-me que vigilância, controle e segurança se tornam problemas quando a sociedade deixa de compreender suas razões e os mecanismos pelos quais

operam, perdendo quase que completamente a noção das forças políticas e econômicas que atuam por trás de tais objetivos. São algumas dessas redes que pretendo demonstrar neste estudo.

Além disso, creio que a adoção de ferramentas de vigilância e controle no Brasil parece ter caráter neoliberal, concentrando contratos financeiros em empresas de telefonia e corporações privadas de capital internacional e nacional – envolvendo grandes, pequenas e médias empresas articuladas em *lobby* – enquanto os debates éticos em torno de sua implementação são pouco realizados ou invisibilizados por parte de agentes que supostamente estão em busca de mais inteligência e racionalidade algorítmica. Tudo isso ocorre em contínuo cenário de privatização do Estado e de seus serviços.

Contudo, outro importante destaque a respeito da adoção de certas tecnologias está no fato de que elas camuflam vieses humanos. Afinal, nos modelos estão inseridos uma série de pressupostos, muitos dos quais prejudiciais, segundo Cathy O'Neil (2020). De acordo com Teresa Numerico (2023), os dados são uma perspectiva do mundo, assim como todas as representações o são. Por isso, falham em representar a totalidade do que é dataficado e necessitam de todo tipo de explicações externas para serem implementados em sistemas preditivos e relacionados às características dos indivíduos, suas preferências e comportamentos.

Identifico como ferramentas de controle e vigilância aquelas adotadas por gestores públicos ou não que ampliam a vigilância sobre cidadãos, espaços e territórios. Para fins deste estudo, centrarei a análise no reconhecimento facial.

Muitas dessas tecnologias vêm inseridas em projetos que visam tornar as cidades mais modernas, sob o discurso das *smart cities*[4]. As cidades inteligentes ou *smart cities* são cidades nas quais diversos tipos de tecnologia são implementados com

> o objetivo de otimizar o uso de seus recursos, produzir novas riquezas, mudar o comportamento dos usuários ou prometer novos tipos de ganho no que se refere, por exemplo, à flexibilidade, segurança e sustentabilidade – ganhos que decorrem essencialmente do ciclo de retroalimentação inerente à implementação e ao uso de dispositivos inteligentes providos de conectividade, sensores e / ou telas. (Morozov; Bria, 2019)

[4]O Centro de Operações Rio, na cidade do Rio de Janeiro, é um exemplo de aplicação de tecnologias do gênero.

Morozov e Bria (2019) prosseguem ainda a afirmar que grande parte do valor atribuído a esse tipo de tecnologia deriva da integração dos sistemas. De modo mais específico, elas coletam dados preexistentes oriundos de serviços públicos ou privados, integrando-os a uma interface fácil de manusear e com grande visibilidade. Tal processo promete mecanismos para a resolução de problemas de forma imediata e eficiente, com base na tecnologia.

Já outros tipos de tecnologias objetivam o controle de pessoas nos transportes públicos, a identificação de suspeitos em multidão, a busca de crianças e desaparecidos. São muitas as razões para a adoção do reconhecimento facial e é por isso que se torna importante explorar o tema sob a perspectiva da CI, da ética da informação, da teoria crítica e dos estudos de vigilância.

As iniciativas voltadas para a adoção do reconhecimento facial no Brasil e no mundo estão inseridas nos estudos de vigilância (Friedewald *et al*, 2017; Bigo; Isin; Ruppert, 2019). Além dos muitos pesquisadores acadêmicos que o abordam, o tema também tem sido objeto de artistas como Banksy e Weiwei, por exemplo, que expressam suas preocupações com a vigilância por meio de câmeras. As obras desses artistas demonstram que o videomonitoramento une sujeitos de culturas diferentes em nações e espaços diferentes. A videovigilância e o reconhecimento facial são problemas que concernem aos países ocidentais e orientais. Da adoção do videomonitoramento decorre o desenvolvimento de ferramentas de vigilância biométrica, como o reconhecimento facial.

Não se trata, contudo, de impedir que esse fluxo de dados aconteça, mas de compreender o que opera por trás deles e aprender a controlar seus usos. Faz-se necessário colocar governos e corporações sob o mesmo padrão de transparência que é imposto ao demais membros da sociedade, complementando ainda com novas formas de *accountability*. É preciso redefinir o que são usos justos ou injustos da informação, alterando o estado de vigilância atual, e assegurar que as decisões tomadas por/em redes sociotécnicas sejam justas e não discriminatórias. Se isso não for feito logo, a opacidade presente nessas redes tende a aumentar (Pasquale, 2015). A discussão política a respeito dos dados deve preocupar-se não apenas com as lutas políticas sobre a produção de dados e os seus desdobramentos, mas também em perceber como os dados geram novas formas de relações de poder e de política entre escalas diferentes e interligadas. (Bigo; Isin; Ruppert, 2019)

A ética intercultural da informação, proposta por Rafael Capurro, parte da reflexão “sobre as possibilidades e realização da liberdade humana no contexto da rede digital mundial (Internet), bem como a troca, combinação e utilização desta informação no meio da comunicação transmitida digitalmente” (Capurro, 2001, p. 41), lidando com questões descritivas e críticas em diferentes culturas e tempos para favorecer o crescimento de uma ética intercultural da informação. Temas estudados pela ética da informação incluem privacidade, identidade, justiça, guerra cibernética, a sociedade de vigilância, entre outros. Lidam também com os impactos econômicos e políticos da informação tecnológica (Capurro, 2013).

O objetivo geral da presente tese é analisar aspectos políticos, econômicos e éticos da adoção de ferramentas de reconhecimento facial no Brasil para refletir sobre os aspectos éticos da adoção do reconhecimento facial no cotidiano. Já os objetivos específicos são identificar iniciativas legislativas a favor e contra a adoção de ferramentas de reconhecimento facial no Brasil; analisar os discursos políticos em torno das tecnologias de vigilância e reconhecimento facial; observar o investimento financeiro para a adoção de tecnologias de reconhecimento facial nos estados; verificar a relação entre a verba utilizada para a criação e a manutenção de ferramentas de vigilância e empresas privadas.

As tecnologias de reconhecimento facial têm sido alvo de questionamentos e críticas no mundo por inúmeras razões, tais como seus vieses racistas e o seu potencial de aprofundamento do encarceramento. A vigilância tem crescido como uma preocupação nas ciências, principalmente as sociais e sociais aplicadas, como a CI. Tal fato pode ser observado pelo aumento de publicações a respeito da temática, conforme pôde ser verificado de maneira exploratória na Base de Dados Referencial de Artigos de Periódicos em Ciência da Informação (Brapci).

Contudo, a mesma base recupera apenas dois resultados para reconhecimento facial e zero quando realizada a busca por videomonitoramento e videovigilância e na busca combinada entre os termos, vídeo e monitoramento. Não pretendo ser exaustiva com esses resultados, mas indicar que o reconhecimento facial ainda é um assunto pouco explorado no âmbito da CI, merecendo mais atenção, pois sua utilização tem crescido em diversos setores. Torna-se, pois, uma oportunidade de discussão de um tema não apenas de modo retrospectivo, ou seja, de forma a analisar algo cuja inserção é completa na sociedade, mas de atuar de modo a regular aquilo que ainda está em discussão de forma propositiva.

Ao ser apresentada a temas ligados à vigilância e aos algoritmos, o assunto começou a me angustiar de forma geral. Não importa onde eu estivesse, passei a observar as câmeras de vigilância ao meu redor. Parece que o grande irmão *orwelliano* estava em todo lugar: na padaria, no elevador, no transporte público, no banco e até mesmo na casa de alguns indivíduos. O videomonitoramento, no Brasil, já é percebido como algo a ser tratado com naturalidade. Todos devemos sorrir, pois estamos sendo filmados. Para mim, seguiu sem fazer sentido que todos nós tenhamos facilidade para aceitar a disseminação dessas ferramentas.

Frequentemente, tenho tido que explicar o problema da disseminação de câmeras de vigilância. Os argumentos a favor costumam orbitar na premissa de que só temem os que devem. Explico que isso é falso. Há uma série de atividades, hábitos e fatos de nossas vidas que gostaríamos de manter circunscritos aos indivíduos com quem partilhamos alguma intimidade. E é esse o problema da vigilância massiva: a intimidade de todos nós é invadida sem que tenhamos a percepção de que isso ocorre, quem mantém nossas imagens, o que é feito com elas e como serão usadas no futuro.

Ao realizar parte das pesquisas para o doutorado em Portugal, no período de outubro de 2021 a setembro de 2022, percebi que a frequência com que me deparava com as câmeras de vigilância era bastante menor. Alguns lugares ainda pareciam seguros e distantes dos olhos do *big brother* (Orwell, 1978). Percebi que outras ferramentas voltadas para a vigilância possuem utilização bastante pequena, se comparada ao Brasil. Portugal e Brasil não podem ser comparados por diversas razões: tamanho, população, economia e estatísticas da violência são apenas algumas delas. Mesmo assim, viver em um mundo em que ainda é possível fazer algo longe das câmeras interessa-me muito.

Entretanto, esse mundo não é o lugar das metrópoles brasileiras. Na realidade, o contexto brasileiro tem demonstrado que as câmeras são um fato. Apesar da dificuldade de aferir a eficiência de sua implementação, sua adoção é crescente e parece impossível parar tal situação. Já o reconhecimento facial ainda pode ser modificado, eu quero crer. Há estados do país sem legislação específica para a adoção de tecnologias do gênero e outros que ainda não colocaram as Tecnologias de Reconhecimento Facial (TRFs) em uso. Outros começam a pensar em leis para banir tais tecnologias. E é por isso que se torna tão importante debatê-lo agora. Ainda é possível propor algo que sirva como base para a regulamentação,

por estados e municípios, dessa tecnologia no Brasil. Por isso, pareceu-me estratégico concentrar os esforços na adoção do reconhecimento facial no Brasil, em vez do grande guarda-chuva do videomonitoramento que abarca esta tecnologia.

Justifico este estudo pelo desejo de abordar o reconhecimento facial a partir de uma perspectiva que aponte os problemas da tecnologia, de forma a verificar se sua adoção realmente vale a privacidade e a intimidade de todos nós. É por isso que é tão necessário entender sua adoção no Brasil. Norteio-me pelas seguintes hipóteses:

a) o videomonitoramento e o reconhecimento facial estão intrinsecamente ligados ao processo de terceirização da segurança pública;

b) Há diferenças consideráveis no discurso diante da adoção de ferramentas de reconhecimento facial no que se refere aos espectros políticos da direita e da esquerda. Tal diferença pode ser observada na dicotomia expressa em direitos individuais de intimidade e privacidade x proteção do patrimônio;

c) Os gastos com a adoção dessas ferramentas não compensam o resultado obtido;

d) Há dilemas éticos que não são superados de uma forma global, mas sempre aparecerão em perspectiva. Por exemplo, a avaliação do que é mais importante entre privacidade e segurança, apesar da privacidade parecer levemente derrotada neste momento.

Este trabalho divide-se da seguinte maneira: são sete capítulos, a contar, inclusive, com introdução (capítulo 1) e considerações finais (capítulo 7).

No segundo capítulo, abordo as questões teóricas relativas ao controle e à vigilância sobre cidadãos. Procuro aproximar a adoção do reconhecimento facial no Brasil de temas como vigilância, capitalismo de vigilância e capitalismo de dados, colonialismo digital e colonialismo de dados, ética algorítmica e ética da informação, entre outros.

O terceiro capítulo discute de que maneira agem os atores políticos quando o assunto é o reconhecimento facial, por meio da apresentação e análise de discursos políticos e de normativas legais em tramitação ou aprovadas nos 26 estados, no Distrito Federal e em nível federal. São diversos os agentes que atuam na criação das políticas públicas. Portanto, tentarei evidenciar as disputas em torno do reconhecimento facial no Brasil a partir de parlamentares eleitos, apesar de reconhecer a importância de organizações não governamentais, vereadores,

prefeitos, governadores e outros membros do Executivo, além de ativistas e estudiosos. Este é também o capítulo mais extenso do trabalho, pois é nele que apresento a maior parte dos dados e análises.

O quarto capítulo apresenta dados econômicos a respeito da implementação de ferramentas de videomonitoramento e reconhecimento facial nos estados Brasileiros. A economia não é a única forma de mensuração da eficiência de algo, contudo é muitas vezes um parâmetro eficiente na hora de analisar se determinada ferramenta deve ser continuamente utilizada. Antes da apresentação dos dados obtidos por meio da lei de acesso à informação, apresento um panorama da adoção do reconhecimento facial no mundo e no Brasil, para contextualizar o leitor a respeito do que tem sido adotado e de que forma, além do que tem sido proibido ou criticado com relação ao reconhecimento facial.

O quinto capítulo discute implicações éticas e práticas da utilização das mesmas ferramentas no que toca aos processos democráticos e aos direitos à privacidade e à intimidade, além de apontar quem são os sujeitos que têm sido as maiores vítimas de ferramentas de vigilância e controle na configuração que o capitalismo tem no Brasil atualmente.

O sexto capítulo objetiva trazer horizontes que permitam compreender as possibilidades de ação diante das ferramentas de reconhecimento facial, favorecendo maior controle por parte da sociedade.

Este estudo tem caráter exploratório quali-quantitativo. Os métodos de abordagem são o dialético, o indutivo-dedutivo e os procedimentos envolvem pesquisa bibliográfica e documental. Segundo Marina Marconi e Eva Lakatos (2003, p. 106), o método dialético “penetra o mundo dos fenômenos através de sua ação recíproca, da contradição inerente ao fenômeno e da mudança dialética que ocorre na natureza e na sociedade”. O método indutivo-dedutivo é utilizado para observar os fenômenos, descobrir sua relação e provocar generalizações a partir da observação (Marconi; Lakatos, 2003).

Trata-se de pesquisa interdisciplinar e está inserida nos estudos de vigilância. Segundo David Lyon (2002), tais estudos objetivam compreender os modos cada vez mais complexos de coleta, armazenamento, transmissão, verificação e utilização de dados pessoais como formas de gerir e influenciar populações e pessoas.

São diversos os problemas práticos que envolvem o acesso aos documentos e materiais produzidos pelas forças policiais (Bayley, 2017). Tal crítica pode ser

estendida a toda política que envolve a segurança pública. Muitas vezes, o trabalho com a temática torna-se uma investigação. Some-se a isso, a cultura do segredo (Bobbio, 2015) que ainda impera no Brasil, apesar do que promulga a Constituição Federal (Brasil, 1988) e da Lei Acesso à Informação (LAI) (Brasil, 2011), além de seus mecanismos de regulamentação (Brasil, 2012). Mesmo assim, é preciso buscar os vestígios e tecer verdadeiras investigações.

São poucos os estudos que analisam as políticas públicas de segurança em andamento no Brasil, conforme o identificado por Trindade (2015). A elaboração de pesquisas que envolvem temas relativos à segurança esbarra muitas vezes na cultura organizacional enredada em desconfiança, preconceito e diversos entraves institucionais. Além disso, observa-se que muitas políticas na área da segurança acontecem muito mais devido ao apelo eleitoral que possuem do que a sua eficácia no enfrentamento ao problema da violência (Trindade, 2015) e de outros problemas sociais.

As tecnologias de reconhecimento facial envolvem múltiplos sujeitos e constituem um campo em disputa. Assim, coexistem *think thanks*, ONGs, juristas, políticos, jornalistas, pesquisadores, cidadãos e operadores da lei, sejam eles das polícias ou do judiciário. Além disso, estão fortemente ligadas aos projetos de urbanismo e planejamento das cidades, como pode ser constatado na adoção das tecnologias da informação e comunicação no urbanismo em prol das cidades inteligentes. Por isso, é importante identificar de que maneira esses discursos refletem na adoção de ferramentas de vigilância nas cidades brasileiras, pois

> o regime de informação remete à distribuição do poder formativo e seletivo entre atores e agências organizacionais, setores de atividades, áreas do conhecimento, regiões locais e redes internacionais e globais, seja pela definição e construção de zonas e recursos de visibilidade informacional, seja pela sonegação e/ou substituição de informações de outro modo socialmente disponíveis ou acessíveis, seja por efeitos não totalmente intencionais da agregação de ações e meios, sobre aquilo que se define, propicia e mobiliza como valores de informação (González de Gómez, 2012, p. 28)

Para identificar os aspectos políticos da adoção de ferramentas de controle e vigilância que envolvem os diversos atores citados, públicos ou privados, a respeito das tecnologias de vigilância, foram utilizadas notícias publicadas em jornais, revistas e órgãos oficiais, presentes na internet, acerca do posicionamento de autoridades públicas ou de entidades privadas.

Destaco que matérias de jornais e revistas também são consideradas documentos neste estudo, logo, fontes documentais. Isso ocorre porque o tema do reconhecimento facial ainda é relativamente novo e as peças jornalísticas têm aparecido como um importante elemento para compreender o impacto da adoção de ferramentas de reconhecimento facial no Brasil e no mundo. Contudo, reconheço a importância do cruzamento de fontes para garantir a fidedignidade das informações consultadas.

Serão utilizados procedimentos da análise documental, análise de discurso e análise de conteúdo para interpretar os dados. A bibliografia apresentada foi feita com base na revisão não sistemática de literatura.

A coleta de dados para verificação das implicações econômicas da adoção dessas ferramentas foi feita por meio do portal da transparência ativa e passiva e de pedidos de informação. Busquei identificar a aquisição e manutenção de *softwares* e a instalação de câmeras por órgãos estaduais. As informações incompletas ou indisponíveis foram solicitadas por meio de pedidos de informação, que nem sempre foram respondidos pelos órgãos.

Foram realizados 85 pedidos de acesso à informação para 73 órgãos em nível estadual. A partir de suas respostas, busquei contratos nos Portais da Transparência estaduais. Além disso, analisei 44 projetos que tramitam na Câmara dos Deputados e 77 leis e projetos oriundos de Assembleias Legislativas, o que totalizou 121 documentos.

Segundo André Cellard (2012), a análise documental permite deduções válidas com base nos documentos. Já Eni Orlandi (2009) define que a análise de discurso busca observar a relação entre aquilo que é dito e a ideologia, observando os sentidos em suas materialidades históricas e linguísticas. A análise de conteúdo pode ser definida como o conjunto de técnicas de análise que objetiva obter, com base em procedimentos sistemáticos e objetivos de descrição de conteúdos, indicadores, quantitativos ou não, que permitam inferir conhecimentos (Bardin, 1977).

A partir das propostas legislativas apresentadas anteriormente, observo quais partidos políticos promovem proposições parlamentares, em qual espectro político encontram-se, quais são as diretrizes que podem ser extraídas da legislação, o objetivo da legislação proposta e de que maneira os temas da privacidade e

intimidade aparecem nas matérias legislativas. Também verifico o crescimento de proposições para a regulamentação da tecnologia.

Com a análise documental, busco respostas para uma série de perguntas, tais como: quantas são as leis para regulação do reconhecimento facial? Como tem sido o crescimento de proposições nesta matéria? Quais são os partidos envolvidos nas proposições? Onde está mais presente? Existe ausência de regulação, mas a tecnologia vem sendo adotada na unidade da federação correspondente? Em caso positivo, que órgãos a estão utilizando? Com que objetivos? Desde quando? De que empresa é a tecnologia utilizada? Quanto foi gasto? Quem desenvolveu a tecnologia? Quais são as bases de dados utilizadas por tais empresas? Quem faz a manutenção de tais sistemas? Quais são os problemas éticos atualmente identificados na utilização de tecnologias de reconhecimento facial? Há formas de diminuir ou mitigar tais problemas? Quem são os maiores impactados pela utilização deste tipo de tecnologia? De que maneira? Quais são as vantagens de seu uso? Há casos em que o reconhecimento facial vale a pena? É proporcional utilizar reconhecimento facial em locais públicos? A humanidade é capaz de desenvolver tais ferramentas, mas deveria desenvolvê-las?

Para começar a tentar responder tais questões, apresento a seguir os marcos teóricos utilizados nesta tese.

2 DA INFORMAÇÃO NO CAPITAL

Atenção, precisa ter olhos firmes
Pra este Sol, para esta escuridão
Divino Maravilhoso – Caetano Veloso e Gilberto Gil

O último século foi cheio de transformações no modo de produção capitalista. Tais mudanças têm alterado a maneira que as pessoas vivem em sociedade e suas relações com dispositivos sociotécnicos dentro do regime de informação vigente.

Percebo que um regime de informação é composto pelas relações estruturais e infraestruturais que operam dentro dessa fase do modo de produção capitalista. Uma das dimensões da configuração atual do capitalismo é a vigilância distribuída que molda sensibilidades e sociabilidades, mantendo os indivíduos cada vez mais submersos em suas amarras dos detentores dos mecanismos de controle. Conforme lembra Shoshana Zuboff,

> cada época da história do capitalismo rumou em direção a uma lógica de acumulação dominante – o capitalismo corporativo baseado na produção em massa do século XX se transformou no capitalismo financeiro no fim do século, uma forma que persiste até hoje. (Zuboff, 2018, p. 22)

A partir disso, a autora aponta para a lógica de acumulação emergente do que chama de capitalismo de vigilância que se utiliza da coleta, extração e análise de dados gerados por indivíduos no uso de tecnologias digitais, fazendo do *big data* tanto sua condição quanto sua expressão (Zuboff, 2018). Para Deivison Faustino e Walter Lippold (2023), este processo culmina na acumulação primitiva de dados.

Os diversos processos sociais ocidentais que culminam no modelo de acumulação flexível tornam o saber uma mercadoria-chave que é adquirida e vendida por e para quem pagar mais, sendo organizada em bases competitivas (Harvey, 1998).

Amplia-se o valor em esferas antes consideradas improdutivas, o que pode ser evidenciado devido à “tendência global de expansão da terceirização em todos os ramos da produção e, em particular, nos serviços”, tornando a terceirização um dos mecanismos vitais do capitalismo para a intensificação da exploração do trabalho, inclusive em ramos anteriormente desprezados pelo sistema capitalista (Antunes, 2018, p. 52).

> Desse modo, além de a terceirização ampliar espetacularmente a extração de mais-valor[5] nos espaços privados, dentro e fora das empresas contratantes, ela também inseriu abertamente a geração de mais-valor no interior do serviço público, por meio do enorme processo que introduziu práticas privadas (as empresas terceirizadas e seus assalariados terceirizados) no interior de atividades cuja finalidade original era produzir valores socialmente úteis, como saúde, educação, previdência etc. (Antunes, 2018, p. 53).

O capitalismo de vigilância encontra terreno fértil com a difusão do neoliberalismo, promotor de desmonte do Estado, fragilizando cidadãos que se tornam consentidamente submissos ao capitalismo eletrônico. As disputas ideológicas parecem perder sentido diante da incapacidade de resolução de conflitos gerados pela precarização do trabalho, desemprego e insegurança, além das sucessivas denúncias de corrupção. A política causa desconfiança, fazendo se duvidar da democracia, mas também motiva a articulação em organizações extrapartidárias para defendê-la ou mudá-la. Muitos apegam-se a líderes incapazes de melhorar as condições de vida das populações que lideram (Garcia Canclini, 2019), o que parcialmente explica o crescimento da extrema-direita em diversos lugares do mundo.

Apesar de todas as transformações, o sistema permanece capitalista. Dentro de sua lógica intrínseca, ele não pode abdicar dos meios técnicos e sociais para sua reprodução de modo contínuo, pois isso significa correr o risco de colapsar. O ponto é que as muitas transformações tecnológicas decorrentes do estágio atual de acumulação capitalista incorporam “diferenças singulares não apenas quando comparadas ao período mercantilista ou fordistas, mas, sobretudo, quando comparadas consigo mesmas alguns poucos anos atrás” (Faustino; Lippold, 2023, p. 23).

Tal contexto tem redefinido a luta de classes e ampliado as desigualdades e a violência inerente ao sistema de exploração do capitalismo, além de criar novas possibilidades para dominar e explorar. E aqui vale relembrar o que trazem Deivison Faustino e Walter Lippold (2023): o capitalismo foi e permanece de modo irremediável atravessado pelo racismo, pelo sexismo, por violências de gênero, pela transfobia, pelo antropocentrismo especista e por muitas outras formas de violência.

[5] Mais-valor (ou mais-valia, na tradução antiga) é o termo utilizado por Marx para se referir ao excedente de trabalho produtivo que resulta da diferença entre o salário do trabalhador e o valor que este gera ao capitalista.

Alguns estudiosos demonstraram-se entusiasmados com a disseminação das redes sociotécnicas (Castells, 1999; Levy, 1999). Outros têm visto com preocupação a importância da extração massiva de dados e algoritmos no cotidiano (Pasquale, 2015; Zuboff, 2018 e 2021; Benjamin, 2019; Silva, 2022; Morozov, 2015 e 2018; Van Dijck, 2014; Bezerra, 2019 e 2020). A questão é que já não é possível manter-se indiferente a elas. A informação tem papel bastante importante nas configurações assumidas pelo capital ao longo do tempo e, em especial, na atualidade. Por isso, a seguir, abordo o lugar da informação no capitalismo atualmente.

2.1 Extração massiva e colonialismos sociotécnicos

As tecnologias da informação e comunicação estão presentes no cotidiano, nos métodos científicos, nos processos industriais, nas estruturas políticas, econômicas e culturais. Grandes mudanças tecnológicas e culturais, como as provocadas pelas TICs, modificam estruturas, sistemas, instituições, normas de informação e comunicação e causam crises de diversos tipos, provocando questões sobre o *ethos* que sustenta as relações sociais. Abre-se espaço para o surgimento de expectativas quanto a mudanças nas relações de poder, em especial por parte de grupos marginalizados e oprimidos (Capurro, 2010).

Especialmente após a década de 1990, com a maior difusão da internet, ideias a respeito do seu potencial para a interação, colaboração e compartilhamento organizaram a gramática das redes sociotécnicas e influenciaram dinâmicas sociais (Silva, 2022). Em parte, a recepção otimista diante das redes sociotécnicas estava baseada na ideia de que representavam uma ferramenta “indispensável para movimentos políticos não convencionais, ao potencializar o impacto de formas menores ou marginais de oposição”, o que não tem se mostrado necessariamente verdadeiro (Crary, 2023, p. 18).

Esse cenário implica mudança nas formas de relacionamento com o mundo, pois os indivíduos moldam e são moldados pela tecnologia que afeta sociabilidades cada vez mais mediadas por dispositivos tecnológicos, impactando nas relações pessoais, culturais, de mercado, socioeconômicas e no campo da vigilância (Oliveira, 2021).

A mediação tecnológica em redes sociotécnicas não tem apenas refletido processos sociais, mas produzido as estruturas sociais em que se vive (Van Dijck, 2018), alterando profundamente padrões de vida e governança (Kalpokas, 2019). Tem sido cada vez mais notória a regulação algorítmica (Morozov, 2018) – e sociedades têm lidado melhor com os efeitos dos problemas do que com suas causas (Kalpokas, 2019). Apesar de seus benefícios imediatos, este tipo de regulação pode levar a humanidade a um regime político no qual todas as decisões serão tomadas pelas empresas de tecnologia e pelos burocratas estatais (Morozov, 2020).

Da presença ubíqua das tecnologias de informação e comunicação na vida social, decorrem preocupações importantes a respeito do aumento da vigilância; o desgaste da confiança em governos e instituições (Oliveira; 2020); as violações de direitos humanos; os vieses discriminatórios presentes nos algoritmos (Silva, 2022; O'Neil, 2020; Benjamin, 2019; Oliveira, 2021; Noble, 2021). O que parece ocorrer é uma simulação permanente do novo, ao mesmo tempo em que são mantidas relações de controle e poder que já existem (Crary, 2016). Coloca-se, então, a questão não sobre quem sairá beneficiado do processo de dataficação da vida, mas quem sofrerá com ele (O'Neil, 2020).

A extração de dados acontece não apenas em momentos particulares, mas de modo cumulativo. Isso quer dizer que os dados coletados, em momento determinado, podem ser combinados com os coletados de nós ou de outras pessoas de outros tempos. Dessa forma, torna-se a vida humana parte de uma vasta cadeia de comparações e análises contínuas por parte de instituições externas que frequentemente têm seus modelos matemáticos opacos sob a proteção de segredos intelectuais, conforme lembram Gabriel Pereira e Nick Couldry (2023). Isso acontece porque a extração de dados é fundamental para a economia (Nemer, 2021).

IAs aprendem por meio de extensas coleções de dados, que são compilados de maneiras que não são nem tecnicamente imparciais nem socialmente neutras. Os dados brutos não são inerentes, pois dependem do trabalho humano, de informações pessoais e de comportamentos sociais que se acumulam ao longo do tempo, através de redes complexas e classificações controversas. (Pasquinelli; Joler, 2020).

Essas noções adicionadas aos conceitos de capitalismo de vigilância ressaltam a importância da informação no estágio atual do sistema capitalista. Nesse sentido, as formas como a coleta e a organização da informação ocorrem são também motivo de preocupação. Extensa quantidade de dados a respeito dos indivíduos é produzida, captada, processada e analisada. O *big data* pode ser descrito a partir de seu volume extremo de dados, sua variedade nos tipos e sua velocidade de processamento desses (Kelleher; Tierney, 2018, p. 9). É inegável o papel desempenhado pelos algoritmos responsáveis pelo processamento e análise de *big data* no atual capitalismo.

A importância dos dados não reside apenas no fato de dizerem respeito a qualquer pessoa conectada em redes sociotécnicas, mas também porque reconfiguram as relações entre estados, sujeitos e cidadãos. O termo *big data* é usado para assinalar o afastamento das formas convencionais de produção e análise de dados estatísticos (Dratwa, 2017). Para Jim Dratwa (2017), os dados não são apenas uma representação, mas um objeto produzido segundo o interesse daqueles que exercem o poder. O autor parte do pressuposto de que a produção de dados é uma prática social e frequentemente política que envolve agentes representados não apenas por aqueles sobre quem são produzidos, ou seja, objetos de dados, mas considera aqueles para os quais o envolvimento determina o modo de produção dos dados, a saber, os sujeitos dos dados.

A capacidade operacional das máquinas do tempo presente, ou seja, dos computadores e das câmeras de vigilância, permite maior controle por parte de corporações e do Estado por meio do desenvolvimento e emprego de técnicas de *machine learning* que pode ser entendido como “um ramo da inteligência artificial e da ciência da computação” concentrado “no uso de dados e algoritmos para imitar a maneira como os humanos aprendem, melhorando gradualmente sua precisão” (IBM Cloud Education, 2020). Ou seja, aquilo que é aprendido pela máquina a partir do processamento de novos dados (*input*) realimenta a inteligência artificial da máquina, de modo a refiná-la. Cathy O'Neil (2020) indica que aquilo que é aprendido alimenta o modelo novamente, de modo a refiná-lo.

A criação de ferramentas de reconhecimento biométrico de qualquer tipo está inserida nesse processo de intenso desenvolvimento de ferramentas de *machine learning*, ou seja, no aprimoramento da capacidade para lidar com grandes

quantidades de dados. Isso remete ao que Didier Bigo, Engin Isin e Evelyn Ruppert (2019) lembram ao afirmar que os dados somente fazem sentido quando alguma informação é extraída deles.

Cathy O'Neil (2020) destaca que, se comparadas ao cérebro humano, essas ferramentas não são tão eficientes quanto parecem, pois “um programa de *machine learning*, em contrapartida, normalmente irá precisar de milhões ou bilhões de pontos de dados para criar seus modelos estatísticos de causa e efeito”.

A abundância de dados oriundos de sensores em quase todos os espaços tem permitido acesso a detalhes antes inimagináveis. O desenvolvimento de ferramentas de extração de dados e metadados digitais, além da criação de grandes bancos de dados com informações sobre milhões ou até bilhões de pessoas, transformaram não apenas a vida privada e a economia, mas também os processos de governança (Kalpokas, 2019). A quantificação do mundo não é exclusividade do tempo histórico em que se vive atualmente, conforme pode ser visto nos trabalhos de Michel Foucault (2008; 1977) com o desenvolvimento de ferramentas estatísticas e de registro. A coleta e armazenamento de dados permaneceu por muito tempo próxima ao monopólio estatal (Foucault, 1977), o que tem sido desafiador.

A soberania estatal para coletar e acumular dados populacionais, territoriais, de saúde, econômicos e de segurança vem sendo desafiada por diferentes corporações, agências, autoridades e organizações que estão a produzir dados em abundância sobre indivíduos em que as interações, transações e movimentações atravessam as fronteiras dos Estados em novos e complicados padrões. (Bigo; Isin; Rupert, 2017).

Os modelos estatísticos sempre influenciaram a cultura e a política. Eles não surgiram apenas com o aprendizado de máquina: essa é só uma nova maneira de automatizar a técnica da modelagem estatística (Pasquinelli; Joler, 2020). Contudo, é a primeira vez na história que uma quantidade tão grande de dados está disponível e pode ser aliada a poderosos computadores para seu processamento, o que favorece a utilização de ferramentas de *machine learning* (O'Neil, 2020)

No meio desse processo, as imagens constituem mais um dos elementos quantificáveis e transformados em dados. Tudo isso decorre com base em uma pretensa neutralidade das redes sociotécnicas e na esperança de que sejam capazes de resolver problemas complexos. A sociedade passa a não ter muitas

alternativas para fugir do controle e da vigilância distribuída, pois esses dispositivos passam a ser adotados por governos e empresas, obrigando sua utilização para o acesso aos serviços oferecidos. Jonathan Crary (2016) destaca que uma das consequências que podem derivar da apresentação de uma nova era tecnológica é a aparente inevitabilidade histórica atribuída a mudanças econômicas de larga escala e a microfenômenos da vida cotidiana, fazendo com que “muitos aspectos da realidade social contemporânea sejam aceitos como circunstâncias necessárias, inalteráveis, como se fossem fatos da natureza” (Crary, 2016).

As operações que envolvem os dados e sua extração massiva e análise configuram os “ativos da vigilância” e podem ser caracterizadas como bens roubados e contrabando, pois são tomados sem que seja produzida uma contrapartida, sem que os produtores desses dados tenham consciência das práticas e efeitos dessa coleta massiva por parte de empresas de tecnologia (Zuboff, 2018, p. 39).

Estados e corporações têm usado seu poder extraterritorial para coletar dados de modo a antecipar, analisar e impedir ameaças; para moldar o ambiente estratégico a seu favor; para promover os seus interesses através da circulação de bens e serviços, informação e capital. Também se utilizam de novas tecnologias de informação e comunicação para alargar os sistemas de comando e controle militar (Deibert; Pauly, 2019).

Este processo remete aos colonialismos digital e de dados.

Duas tendências materializam a existência do colonialismo digital. A primeira é a emergente nova partilha territorial da Terra entre os atuais grandes monopólios pertencentes à indústria da informação, conhecidos como *big techs,* que se encontram bastante concentrados no Vale do Silício, mas não exclusivamente, e que “atualiza no imperialismo, o subimperialismo e o neocolonialismo tardio ao reduzir o chamado Sul global a mero território de mineração extrativista de dados informacionais” (Faustino; Lippold, 2023, p. 24). A segunda é também intitulada colonialismo de dados e tem subsumido cada vez mais profundamente “a vida humana, o ócio, a criatividade, a cognição e os processos produtivos às lógicas extrativistas, automatizadas e panópticas do colonialismo digital” (Faustino; Lippold, 2023, p. 24). Colonialismo digital é um fenômeno mais amplo do que o colonialismo de dados, estando o segundo incluso no primeiro.

O colonialismo de dados envolve não apenas os “novos tipos de relações humanas que permitem a extração de dados para a mercantilização” (Couldry; Mejias, 2019, p. 337), como também o universo de interações homem-objeto, objeto-objeto e humano-algoritmo, levando a novas formas de colonização por meio de dados, baseadas em infraestruturas materiais e construções simbólicas que reforçam práticas colonizatórias (Ricaurte, 2019).

A configuração que o colonialismo assume atualmente é dataficada e sua violência, frequentemente sutil, provoca a precarização de trabalhadores, apontando para uma dominação social emaranhada e gamificada que acaba por formatar sujeitos subjugados pela servidão das máquinas e sistemas de algoritmos de grandes corporações do Norte Global (Silveira *apud* Faustino; Lippold, 2023).

> Vivemos hoje uma informática de dominação, uma computação que bloqueia a tecnodiversidade e as possibilidades dos povos de criarem e recriarem seus aparatos tecnológicos. Mulheres, negros e povos originários são orientados a se contentar com a condição de usuários das soluções criadas pelas big techs. O colonialismo dissemina que o único modo de criar tecnologias é esse que nos subordina e nos modula. Afinal, as plataformas digitais alegam buscar apenas e tão somente a melhora de nossa experiência. Para tal, extraem constantemente nossos dados a fim de realizar predições, a ponto de não precisarmos mais querer, uma vez que os algoritmos que aprendem com os dados de comportamento poderão predizer nossas vontades (Silveira *apud* Faustino; Lippold, 2023, p. 18).

Este processo dá origem a novas formas de acumulação e valorização dos dados nas quais a fonte de autoridade e legitimidade é capaz de atravessar os limites da soberania dos Estados, produzindo efeitos internacionais. Constitui a emergência de um espaço transnacional que salienta lógicas de ação transversais e transgride distinções entre o interno e o externo, o nacional e o estrangeiro (Bigo; Isin; Ruppert, 2019).

O modelo de negócio de extração, processamento e análise massiva de dados ocorre mundialmente. Contudo, seus efeitos não são iguais, pois o fluxo de dados é da periferia para o centro, como lembram Sérgio Amadeu da Silveira, Joyce Souza, João Francisco Cassino, Débora Franco Machado e outros (2022).

Já o colonialismo digital é uma das características do estágio em que se encontra o modo de produção capitalista e consiste na divisão do mundo entre os

grandes monopólios da dita indústria da informação (Faustino; Lippold, 2023). Nas palavras de Deivison Faustino e Walter Lippold:

> É, sim, pois, a expressão objetiva (e subjetiva) da composição orgânica do capital em seu atual estágio de desenvolvimento e se materializa a partir da dominação econômica, política, social e racial de determinados territórios, grupos ou países, por meio de tecnologias digitais (Faustino; Lippold, 2023, p. 80)

O colonialismo de dados é uma das facetas do colonialismo digital, também identificado como tecnocolonialismo (Dowbor, 2022) e *i-colonialism*. Conforme apontam Deivison Faustino e Walter Lippold (2023), pode ser expresso pela acumulação primitiva de dados, destacando-se por subsumir com cada vez mais força e violência a vida humana aos processos de valorização do valor do capitalismo.

> O colonialismo de dados não é mera inovação tecnológica e um modo de organização do processo de trabalho, mas um direcionamento da tecnologia para captação de dados de empresas e usuários comuns com finalidades diversas, que vão do simples mapeamento de seu perfil para fins comerciais e políticos à extração massiva de dados populacionais para o complexo treinamento de máquinas algorítmicas e redes neurais. Os dados, aqui, se convertem em matéria-prima preciosa a ser obtida por violentos ou consensuais processos de extrativismo: a acumulação primitiva dos dados (Faustino; Lippold, 2023, p. 94).

Como a acumulação primitiva se conecta com os dados? A ideia de que os dados podem ser uma representação inequívoca da realidade, sem intermediários, pressupõe que eles não estão situados em contextos de representação específicos (Numerico, 2023)

O colonialismo de dados pode ser pensado a partir de duas dimensões: a primeira, de caráter metafórico, está relacionada à intensidade e ao alcance com que as tecnologias da informação estão a “colonizar” cada vez mais setores da vida humana. A segunda, de dimensão econômica, relaciona-se com “os sentidos dessa colonização, uma vez que ela, em suas expressões políticas ou subjetivas, tem de fundo a subsunção real de parcelas cada vez maiores de tempo humano para as finalidades de acumulação de capital (Faustino; Lippold, 2023, p. 96). Aliás, a apropriação do tempo pelo capital também é uma questão para Johnathan Crary

(2016), ao denunciar que o capitalismo tenta domar também o sono para ocupar todos os espaços da existência.

Segundo Alejandro Mayoral Baños (2023), as noções de colonialismo digital e de dados não pretendem desconsiderar a violência histórica do colonialismo, mas refletir sobre os métodos, práticas e formas de opressão que se transformam ao longo do tempo e acabam por refletir nas tecnologias digitais. O colonialismo baseia-se em métodos de opressão social, econômica, política e sistêmica com o objetivo de assegurar a extração e a desapropriação de recursos de diversos locais.

Como alertam Eygene Morozov e Francesca Bria (2019), aquele que controlar os meios de produção, a análise e o armazenamento da maior parte dos dados, conseguirá a melhor inteligência artificial, tornando os demais dependentes dela. A exploração dos dados parece ser capaz de exacerbar a expansão da lógica capitalista neoliberal (Bigo; Isin; Ruppert, 2019).

Para Paola Ricaurte (2019), a extração, armazenamento, processamento e análise de dados constituem um processo muito mais amplo que precisa ganhar uma análise decolonial, pois deve-se perguntar quais são as implicações do processo de colonização de dados para sociedades e indivíduos localizados nas ditas margens econômicas e de que maneira as relações de poder subjacentes afetam as comunidades que existem fora desta ordem de conhecimento. O extrativismo de dados implica que tudo é uma fonte de dados. Nessa perspectiva, a própria vida não configura mais do que um fluxo de dados contínuo. Percebe-se onipresença de tecnologias e regimes de dados em todas as esferas da vida humana.

Surge, então, a metáfora dos dados como o novo petróleo. Cabe questionar, então, quem detém os dados e o lucro que deles deriva (Dratwa, 2017)? Morozov (2018) provoca, então, ao questionar quem será o novo Saddam Hussein.

A extração massiva de dados atualmente tem funcionado de modo a coletar de modo predatório dados de indivíduos e comunidades. Zigmunt Bauman (2012) relembra Rosa Luxemburgo que explicava que o sistema capitalista só é capaz de avançar enquanto existir terras disponíveis para sua expansão e exploração. Ao mesmo tempo, “o capitalismo destrói o que quer que possa permitir que grupos e comunidades busquem práticas de apoio mútuo e de subsistência autossuficiente” (Crary, 2023, p. 5).

Segundo José van Dijck, Thomas Poell e Martijn de Waal (2018), o mecanismo da comodificação envolve a transformação de objetos *online* e *offline*, atividades, emoções e ideias em *commodities*. Por isso, diante do cenário de exploração e comodificação da vida, deve-se fortalecer a busca por práticas de apoio mútuo. Para tal, é necessário compreender de que modo governos e instituições públicas agem como forças centrais no processo de colonização de dados, internamente e em escala internacional, de forma sistêmica, embora a força central desse processo resida nas *big techs*. Isso está relacionado ao desenvolvimento de um arcabouço regulatório e legal; à concepção de políticas públicas; à utilização de sistemas de inteligência artificial para a administração pública; à contratação de serviços tecnológicos; à aquisição de produtos para fins de administração pública e vigilância; à implementação de políticas públicas e agendas digitais; e à facilitação e educação para o desenvolvimento das forças de trabalho.

Governos passam a ser a principal clientela de empresas de serviços de IA para a tomada de decisões públicas com dados de propriedade empresarial e pública, a contratação de serviço empresarial e a aquisição de produtos para diversos fins como a ciberdefesa, vigilância, infraestrutura de telecomunicações e transportes, *smart cities*, servidores, além de atuarem em agendas para o desenvolvimento digital e da força de trabalho (Ricaurte, 2019). Parte-se de uma premissa colonizadora que pressupõe que as regiões periféricas querem e adotam satisfeitas as tecnologias do ocidente e que, necessariamente, tais comunidades se beneficiarão com elas (Crary, 2023).

A extração e acumulação massiva de dados envolve não apenas capital econômico, mas também capital cultural (Dratwa, 2017). Modificações intensas ocorrem no campo das forças produtivas, de modo a afetar o conjunto da vida social. Acontece a aceleração do tempo histórico, impactando nas estruturas societárias em andamento e submetendo a política, o cotidiano e as formas de pensamento a grandes mudanças (Martins, 2011).

A integração intensa do tempo e das atividades humanas aos parâmetros do intercâmbio eletrônico demanda um alto investimento em pesquisas que se dediquem à redução do tempo de tomada decisória, à eliminação do tempo ocioso e da contemplação (Crary, 2016) que influencia tanto o que ocorre na vida pessoal quanto na profissional. A comodificação da vida e o estabelecimento de uma ordem

social mediada por dados limita as possibilidades de uma existência fora do regime dataísta, pois o ato de estar fora significa exclusão (Ricaurte, 2019). Presenciam-se mudanças profundas na forma como o conhecimento e a inovação são produzidas, processadas e legitimadas.

A atualidade é marcada por ambivalências: na participação cuja tensão reside entre o empoderamento e a instrumentalização ou subjugação; na partilha tensionada entre os ideais de bem comum e as novas formas de apropriação, mercantilização e exploração; na aprendizagem e na reflexividade que reside entre a capacidade de imaginar o novo ou aceitar o que ocorre (Dratwa, 2017).

Tudo isto coloca o colonialismo de dados em um arranjo de processos que é parte da epistemologia dominante que se traduz na dominação de corpos, afetos e territórios (Ricaurte, 2019), pois os dados não apenas capturam processos sociais, mas colonizam mentes, almas, corpos e espaços (Bigo; Isin; Ruppert, 2019).

Diversas esferas da vida humana têm sido mediadas por aplicativos e plataformas dominadas por *big techs* do Vale do Silício. O tempo é cada vez mais roubado. Ainda que a dinâmica subjacente esteja ligada ao lucro e à competitividade entre empresas pelo mercado, o ritmo acelerado do aprimoramento e da reconfiguração dos sistemas, modelos e plataformas faz parte de um processo de reinvenção do sujeito e intensificação do controle (Crary, 2016).

Para Giles Deleuze (1992), a vigilância e o domínio sobre os corpos, que antes teriam sido primordialmente exercidos no *locus* de instituições disciplinares, como a escola, a prisão, as forças armadas ou o hospital, conforme o estudado por Michel Foucault (1977), passam a ser ubíquos na sociedade de controle, que em todos os locais e situações absorve, registra e acumula dados sobre as atividades humanas. E são esses os aspectos que abordo na próxima seção.

2.2 É preciso estar atento

No campo dos estudos da vigilância, os trabalhos dos filósofos Michel Foucault (1977) e Giles Deleuze (1992) possuem bastante importância, tendo recebido atenção de diversos pesquisadores e pesquisadoras.

Para o exercício do poder, conforme o apontado por Michel Foucault (1977, p. 188) é preciso ter um instrumento de

> vigilância permanente, exaustiva, onipresente, capaz de tornar tudo visível, mas com a condição de se tornar ela mesma invisível". São como "milhares de olhos postados em toda parte, atenções móveis e sempre alerta, uma longa rede hierarquizada (Foucault, 1977, p. 188),

assim como os milhares de câmeras espalhadas pelas cidades ou uso de massivas bases de dados que analisam os comportamentos humanos, ambos utilizados com a finalidade de manutenção da ordem e da segurança.

Conforme Michel Foucault,

> A "disciplina" não pode se identificar com uma instituição nem com um aparelho; ela é um tipo de poder, uma modalidade para exercê-lo, que comporta todo um conjunto de instrumentos, de técnicas, de procedimentos, de níveis de aplicação, de alvos; ela é uma "física" ou uma "anatomia" do poder, uma tecnologia. E pode ficar a cargo seja de instituições "especializadas" (as penitenciárias, ou as casas de correção do século XIX) seja de instituições que dela se servem como instrumento essencial para um fim determinado (as casas de educação, os hospitais), seja de instâncias preexistentes que nela encontram maneira de reforçar ou de reorganizar seus mecanismos internos de poder (um dia se precisará mostrar como as relações intra-familiares, essencialmente na célula pais-filhos, se "disciplinaram", absorvendo desde a era clássica esquemas externos, escolares, militares, depois médicos, psiquiátricos, psicológicos, que fizeram da família o local de surgimento privilegiado para a questão disciplinar do normal e do anormal), seja de aparelhos que fizeram da disciplina seu princípio de funcionamento interior (disciplinação do aparelho administrativo a partir da época napoleônica), seja enfim de aparelhos estatais que têm por função não exclusiva mas principalmente fazer reinar a disciplina na escala de uma sociedade (a polícia). (Foucault, 1977, p. 189)

Para Gilles Deleuze, após a Segunda Guerra Mundial, a sociedade disciplinar passa a integrar dispositivos de controle. Segundo o filósofo, as sociedades do controle e da disciplina têm seus tipos de máquina próprios. Para o autor, as máquinas existentes em cada época são capazes de exprimir "as formas sociais capazes de lhes darem nascimento e utilizá-las" (Deleuze, 1992). Por exemplo, "as antigas sociedades de soberania manejavam máquinas simples, alavancas, roldanas, relógios". As mais recentes sociedades disciplinares "tinham por equipamento máquinas energéticas, com o perigo passivo da entropia e o perigo ativo da sabotagem". Já "as sociedades de controle operam por máquinas de uma terceira espécie, máquinas de informática e computadores, cujo perigo passivo é a interferência, e o ativo a pirataria e a introdução de vírus" (Deleuze, 1992, p. 3).

As máquinas deste tempo são os computadores, *smartphones* e câmeras de segurança. O caráter dispersivo do sistema capitalista vigente é evidente. Nele, o controle dá-se em “curto prazo e de rotação rápida, mas também contínuo e ilimitado, ao passo que a disciplina era de longa duração, infinita e descontínua” (Deleuze, 1992, p. 3). Com isto, não se pretende insinuar que a atual faceta do sistema capitalista teve a capacidade de acabar com a miséria do mundo. Bastante longe disso, diga-se. Por isso, Deleuze (1992) aponta que o grande número de indivíduos dificulta a utilização das tradicionais estratégias disciplinares de confinamento. Para o autor, “o controle não só terá que enfrentar a dissipação das fronteiras, mas também a explosão dos guetos e favelas” (Deleuze, 1992, p. 3-4). Desse modo, o controle e a disciplina funcionam como facetas do modo de produção capitalista atualmente.

A coleta, a análise e o armazenamento massivo de dados do capitalismo de vigilância inserem-se em uma cultura de vigilância, conforme pôde ser visto anteriormente em Lyon (2019). A vigilância tem emergido como uma forma de controle importante por parte de governos, empresas e indivíduos (Lyon, 2007). Ela é um componente central da modernidade (Lyon, 2013).

Fernanda Bruno (2009, p. 1-2) compreende por

> vigilância a atividade de observação sistemática e focalizada de indivíduos, populações ou informações relativas a eles, tendo em vista extrair conhecimento e intervir sobre os mesmos, de modo a governar suas condutas ou subjetividades (Bruno, 2009, p. 1-2).

Está baseada em tríplice regime de legitimação: o da segurança, o da visibilidade midiática e o da eficiência, principalmente no que concerne aos serviços das redes e tecnologias de comunicação. Em um contexto de vigilância massiva da sociedade, todos os indivíduos passam a ser suspeitos até que se prove o contrário, transformando-se toda a sociedade em vigilantes e suspeitos em potencial (Bruno, 2009). Contudo, destaco que uns são mais visíveis que outros e que são muitas as camadas de visibilidade ou de invisibilidade possíveis.

Em diversas cidades, ferramentas tecnológicas têm aumentado a preocupação de autoridades e da Sociedade Civil. Todos os sistemas de monitoramento e vigilância têm desafiado o direito fundamental relativo à privacidade. Tais sistemas baseiam-se na utilização e extração massiva de dados que representam dinâmicas sociais. (Aguirre; Badran, Mugah, 2019).

Como é cada vez mais barato coletar e manter dados, eles agora podem ser capturados com cada vez menos esforço, sendo inseridos em contextos de pouca ou nenhuma regulação legal, o que faz com que se justifique guardar tanto dado quanto for possível em detrimento de seu descarte. Em um mundo cuja norma é a vigilância, o próprio fato de existir indica a presença em estruturas e sistemas que fazem parte de muitas esferas da vida em sociedade. Contudo, para a utilização de dados de forma massiva, é necessária a dataficação do mundo (Kalpokas, 2019).

Frank Pasquale (2015) argumenta que um estado de vigilância que não se pode explicar representa uma ameaça maior à liberdade do que o medo da insegurança ou do terrorismo. É o que o autor chama de “erosão de uma série de liberdades” (Pasquale, 2015, p. 52, tradução nossa). A crítica do autor prossegue ao afirmar que aqueles que vigiam possuem o poder de classificar os críticos do sistema como inimigos do estado, vigiando-os ainda mais. Para ele, o principal dano da vigilância massiva é sua capacidade de calar as vozes dissonantes. Tal preocupação aparece também em autores como Oliveira (2020), Ĉas *et al* (2017), Solove (2008) e Véliz (2021).

Rafael Capurro (2016) aponta para a transformação do mundo em panóptico, com a vigilância ampliada, pois a economia digital perdeu a consciência sobre a liberdade humana e as interações entre os mundos físico e digital. Os pensadores devem, então, assumir certa responsabilidade e devem perguntar-se sobre quem são os excluídos e os beneficiários neste processo. É preciso questionar quem explora indivíduos tanto no mundo físico quanto no cibernético no modo como o capitalismo manifesta-se atualmente. A Sociedade Civil deve se perguntar que tipos de mecanismos serão úteis para manter a civilidade nos dois mundos que são, afinal, o mesmo.

A privacidade não se constitui apenas em um direito fundamental, mas atua também na garantia de outros direitos e liberdades fundamentais, no equilíbrio entre o Estado e os cidadãos, no desenvolvimento da democracia, na inovação social e econômica e no exercício da autonomia individual, conforme indica Daniel Solove (2008). Ela é uma das condições para que o indivíduo se expresse livremente. O exercício da vigilância de massas é por si só um sintoma de desrespeito por princípios democráticos (Ĉas *et al*, 2017). Para Frank Pasquale (2015), um estado de vigilância irresponsável pode significar ameaça maior à liberdade do que certas

ameaças à segurança, pois erodem uma série de direitos, como os anteriormente citados.

Carissa Véliz (2021) defende que um mundo sem privacidade é um mundo perigoso, pois essa consiste também em não compartilhar com as demais questões que são íntimas, como os pensamentos, as experiências, as conversas e os planos – eu acrescento nossos hábitos, nossos afetos, nossas manias, nossos medos. Os seres humanos precisam de privacidade para conseguirem relaxar da dificuldade que é viver em sociedade; para explorar ideias novas de forma libertária; para formar suas próprias opiniões. A privacidade ajuda a nos proteger das pressões indesejadas e dos abusos de poder.

Indivíduos têm colaborado com a própria vigilância e coleta de seus próprios dados à medida que utilizam determinados serviços disponíveis em redes sociotécnicas (Zuboff, 2018; Crary, 2016). O direito à privacidade é submetido por vontade própria em troca dos "benefícios" recebidos (Bauman, 2013). Segundo Jonathan Crary,

> A televisão havia colonizado arenas importantes do tempo vivido[6], mas o neoliberalismo exigia que houvesse uma extração de valor muito mais metódica do tempo de televisão e a princípio de toda hora de vigília. Nesse sentido, o capitalismo 24/7 não é simplesmente a apreensão contínua ou sequencial da atenção, mas também uma composição densa do tempo em camadas, na qual múltiplas operações ou atrações podem ser atendidas quase simultaneamente, independente de onde estamos ou do que mais estamos fazendo. Os assim chamados aparelhos smart recebem esse nome menos pelas vantagens que podem oferecer para um indivíduo do que por sua capacidade de integrar seu usuário de forma mais completa a rotinas 24/7. (Crary, 2016)

Por trás de acordos de confidencialidade e formatos proprietários, agências governamentais e instituições privadas escondem seus atos enquanto tudo aquilo que o cidadão faz nas redes sociotécnicas é capturado em um mundo ausente ou quase ausente no que concerne às regulamentações legais no campo da proteção da privacidade dos indivíduos. Progressivamente, os dados de seus utilizadores são recolhidos, mas ainda são poucos os regulamentos que protegem usuários, permitindo que exerçam controle sobre seus dossiês digitais.

[6] Inevitável não pensar na canção Televisão, dos Titãs. Disponível: https://www.youtube.com/watch?v=7psItZeHmqU. Acesso em 18 de dezembro de 2023.

As pressões mercadológicas avançam em relação aos consumidores que viram matéria-prima para a extração de dados. Câmeras de vigilância tornam-se cada vez mais baratas e incorporadas a um número de locais que só aumenta, acrescidas de mais tipos de sensores. A informação que resulta de tais operações, além de uma grande quantidade de dados, dá origem a perfis detalhados dos usuários. Tudo isso em um processo de diluição das fronteiras entre o setor público e o setor privado (Pasquale, 2015).

A partir da extração massiva de dados, ocorre seu processamento por modelos matemáticos que acabam por gerenciar diversos aspectos da economia, publicidade, segurança social, etc. São obscuros, difíceis de contestar e responsabilizar, operando em larga escala para otimizar a vida de milhões de pessoas. São, portanto, armas de destruição matemática. (O'Neil, 2020). Espalhados por diversos campos da vida humana, sistemas automatizados baseiam-se em lógicas algorítmicas que aplicam inteligência artificial em processos preexistentes que eram transformados por causa da digitalização como, por exemplo, a televisão, o mercado financeiro, a segurança pública e todas as esferas em que a coleta de dados serve de matéria de extração para o capital da informação (Silva, 2022). A vida traduzida em dados é a matéria-prima da economia da vigilância que tem transformado cidadãos em usuários e sujeitos em dados (Véliz, 2021). Ou, nas palavras de Garcia Canclini (2019), cidadãos são substituídos por algoritmos.

Tecnologias orientadas para a vigilância têm sido implementadas de forma ostensiva para prevenir o crime, localizar suspeitos, vítimas e testemunhas, além de gerir o sistema penal e penitenciário com base no argumento de proteção social. Tal tendência deve ser criticada por, ao menos, duas razões. Primeiramente, as sociedades têm evoluído para estados superprotegidos, com base na cultura do medo e implementação difusa de tecnologias de vigilância apenas porque estão disponíveis. Em segundo lugar, residem as preocupações com a erosão do direito à privacidade derivada da utilização de tecnologias de vigilância por empresas privadas e instituições públicas. (Vermeersch; De Pauw, 2017)

Contudo, Ruth Cardoso e Alexandre Barbosa Pereira (*apud* Nemer, 2023) argumentam que este medo dos criminosos significa, na realidade, o medo dos

pobres, o que justifica a violência policial, mas também todas as formas de vigilância sobre aqueles vistos como indesejados.

A vigilância estatal para fins de segurança e a espionagem empresarial não são tão semelhantes, se examinadas superficialmente. As corporações privadas podem argumentar que regulamentações reduzem os lucros e a capacidade de inovação enquanto o Estado alega que, sem acesso total à informação, a sociedade está em perigo. Com base no argumento da segurança, é mais difícil reprimir a vigilância de Estado do que a corporativa. Contudo, sua estrutura opaca e a inseparável colaboração entre o público e o privado têm demonstrado que os dois estão intrinsecamente relacionados (Pasquale, 2015).

Há uma lógica por trás da ideia de segurança baseada em dados que entende que a coleta de dados pessoais e metadados seria capaz de permitir uma intervenção direcionada e orientada, de modo a concentrar a atenção e os recursos em ameaças, possibilitando que sejam impedidas (Ĉas *et al*, 2017). Assume-se também que cidadãos valorizam mais a segurança do que a privacidade, pois aqueles que não devem coisa alguma também não temem o aumento da vigilância (Vermeersch; De Pauw, 2017).

A racionalidade tecnológica tornou-se política em um cenário que se utiliza da privatização para a redução de custos e maximização do lucro. Soluções tecnológicas são vistas como necessárias para redução dos custos e terceirização das decisões para máquinas supostamente inteligentes (Benjamin, 2019). Presente em diversas esferas da vida, a vigilância é, segundo Morozov e Bria (2019), uma das piores dimensões das *smart city.* Para combater tal problema, a privacidade deve ser percebida como um direito e não como um serviço, pois, como aponta Cathy O'Neil (2020), aqueles que detém privilégios "são processados mais pelas pessoas; as massas, pelas máquinas", já que a privacidade se torna um luxo restrito aos ricos que podem pagar por ela.

Nas palavras de Bauman (Bauman; Lyon, 2013, p. 27), "os drones da próxima geração poderão ver tudo, ao mesmo tempo que permanecem confortavelmente invisíveis – em termos literais e metafóricos". É nesse contexto que o cidadão se torna muito visível enquanto outros agentes tentam se invisibilizar, pois governos classificam mais documentos como secretos e delegam mais funções a empresas

terceirizadas com maior facilidade para fugir do escrutínio da população (Morozov, 2020)[7].

A vigilância não é um fenômeno novo, mas tem sido aperfeiçoada pelo desenvolvimento tecnológico. As torres de observação do panóptico de Bentham (Foucault, 1977) dão lugar a sistemas de câmeras interligadas com cada vez mais capacidades. Atualmente, fornecem imagens de alta resolução, registram ruídos, reconhecem faces e alertam operadores para atividades suspeitas (Vermeersch; De Pauw, 2017). A fronteira entre o público e o privado se dissipa com a presença de câmeras privadas em local público (Firmino, 2018).

A vigilância não é formada apenas pelo videomonitoramento, mas a associação entre os dois é inevitável. Isso ocorre pela presença maciça de câmeras e pela incorporação de tecnologias de reconhecimento facial nos dispositivos (Oliveira, 2021). Tal correlação leva também à necessidade de compreender as tecnologias de reconhecimento facial como "tecnologias carcerárias algorítmicas" porque são muito imprecisas (Silva, 2022). Contudo, algumas das questões referentes ao reconhecimento facial serão melhor abordadas no próximo capítulo.

O videomonitoramento tem sido utilizado como uma das principais formas de enfrentamento à violência urbana na América Latina. Acredita-se que as câmeras "podem servir como mecanismo de prevenção ao crime quando empregadas em conjunto com processos e práticas eficientes de policiamento, proporcionando apoio em um ambiente de recursos limitados" (Francisco; Hurel; Rielli, 2020, p. 2).

Contudo, a multiplicação de "projetos de vigilância governamental altamente tecnófilos" é, segundo Graham, uma demonstração da "militarização da sociedade civil", ou seja, "a extensão das ideias militares de rastreamento, identificação e seleção nos espaços e meios de circulação da vida cotidiana" (Graham, 2016, p. 24).

A coleta e o processamento de dados biométricos no espaço urbano são normalizados com base na ideia de que oferecem benefícios e de que seus custos são inofensivos (Silva, 2022). A adoção deste tipo de ferramentas torna o cidadão transparente e manipulável enquanto permite que governos e empresas possuam a

[7]Um bom exemplo disso é o governo Bolsonaro e os esforços para aquisição do Pegasus, *software* espião de origem israelense. Mais pode ser visto em https://Brasil.elpais.com/opiniao/2021-08-02/pegasus-a-ponta-do-iceberg-da-fragilidade-no-controle-de-atividades-de-inteligencia-e-uso-de-tecnologias-de-vigilancia.html. Por outro lado, o mesmo governo ficou famoso pela frequência com que usou da prerrogativa do sigilo em documentos públicos. Veja mais em https://noticias.uol.com.br/politica/ultimas-noticias/2022/08/30/bolsonaro-poe-sigilo-de-100-anos-sobre-seu-cartao-de-vacinacao-veja-casos.htm. Acesso em 03 nov. 2022.

liberdade para perseguirem seus próprios projetos (Morozov, 2020). David Lyon (2018) acrescenta que a cultura de vigilância não reside apenas em aspectos técnicos e políticos, mas também no entusiasmo, na ignorância, na cooperação e na proatividade dos vigiados.

A internet, as redes sociodigitais e a análise de dados algorítmicos possibilitam a construção de novos saberes, combinando diferentes áreas do conhecimento. Isso pode potencializar os recursos para o exercício da cidadania. No entanto, é preciso lembrar que as grandes corporações e governos muitas vezes têm escondido dados e informações que parecem relevantes para a tomada de decisão (Garcia Canclini, 2019).

Capurro (2016) alerta que o mais difícil do aumento da conectividade não está relacionado à grande capacidade de conexão, mas ao modo que esta conectividade deve ser gerida. O autor faz perguntas fundamentais para o momento histórico em que vivemos:

> Todos devem estar permanentemente conectados a tudo? Quem possui quais dados, e como a informação deve ser tornada pública? O uso dos dados pode e deve ser regulamentado, e, se sim, como? E que papel devem desempenhar os usuários comuns, os governamentais e os empresariais na resposta a estas questões? (Capurro, 2016, p. 7)

Faz-se necessário que os cidadãos se protejam do excesso de regulamentação ou controle por parte dos governos e de corporações, sem que isso signifique abandonar a importância do Estado no processo.

Mais do que soluções, as reflexões trazidas ajudam a repensar a centralidade do humano diante da tecnologia, no capitalismo atualmente. A humanidade parece perdida, angustiada, em um ambiente de incerteza, cercada pelas novas e velhas formas de opressão. A globalização financeira permanece descontrolada, bem como as atividades de empresas transnacionais de tecnologia da informação e de grupos ideológicos. Perspectivas emancipatórias, como as propostas pelo materialismo histórico-dialético, parecem cada vez mais distantes.

Diante do desinteresse e da incapacidade de fundar valores e um projeto ético-político que se destine a mudanças conjunturais e a construção de uma sociedade com mais justiça e felicidade (Baratta, 1995, p. 122), é difícil não ceder ao pessimismo, parecendo cada vez mais penoso produzir resistência diante deste

modo de ser-no-mundo e ao modo como o capitalismo molda nossas relações sociais, políticas e afetivas. No horizonte, distanciam-se as resistências que provocam tensões e que abrem espaço para rupturas. Ainda assim, é preciso continuar a tentar, pois "estruturas políticas como a democracia podem garantir que a sociedade não se encaixe em um mero jogo de poder (o direito do mais forte) ou se torne objeto de ideologias/doutrinas que pregam a 'verdade'" (Bezerra; Capurro; Schneider, 2017, p. 378).

É preciso estabelecer um projeto de aliança fundador de "um Estado mais rico, alimentado por todas as distintas cidadanias, pelas experiências, projetos, visões de mundo através das quais as diferenças" podem exprimir-se (Baratta, 1995, p. 125). Ou seja, um Estado cuja reflexão ética pense o universal sem abandonar as singularidades e as idiossincrasias locais. Tal pluralismo deve evitar relativismos e pragmatismos (Capurro, 2010). Para fundarmos esse Estado, restam pelo menos três tarefas para o pleno exercício da cidadania: a reconstrução do sentido da heterogeneidade para que sejamos solidários; o reconhecimento de que é preciso esperançar[8]; e a reflexão de que há diversas maneiras de construir uma nova cidadania em andamento. É preciso que nos reinventemos e assumamos nossa responsabilidade diante dos usos sociais dos algoritmos. Aí reside a importância do debate ético em torno dos valores e de seus reflexos nas ações humanas.

Conforme Charles Ess (*apud* Capurro, 2017), o ocidente percebe a privacidade como um valor intrínseco e as tradições budistas e confuncianas percebem o sujeito como algo que tem valor negativo em si mesmo, pois há primazia da comunidade sobre o indivíduo. Por isso, uma ética intercultural da informação, conforme debaterei melhor no capítulo seis, é muito necessária nos dias atuais, pois é capaz de considerar as diferenças, desequilíbrios e dissonâncias de nível político e social. Portanto, essa ética precisa tomar com seriedade os diferentes contextos culturais e históricos entre o extremo Oriente e extremo Ocidente (Capurro, 2017).

A emergência de uma "nova civilização" requer "um diálogo intercultural arejado" que "conceda mais liberdade de informação e comunicação" (Capurro, 2016, p. 1). A liberdade de pensamento é o que está no núcleo de uma ética intercultural da informação futura. E essa ética deve considerar as diferentes

[8]Para Paulo Freire (1992), "é preciso ter esperança, mas esperança do verbo esperançar; porque tem gente que tem esperança do verbo esperar. E esperança do verbo esperar não é esperança, é espera. Esperançar é se levantar, esperançar é ir atrás, esperançar é construir, esperançar é não desistir! Esperançar é levar adiante, esperançar é juntar-se com outros para fazer de outro modo".

realidades impostas pelo e no capital. Primeiro, acredito ser importante destacar que o valor da privacidade é percebido de forma bastante diferente por ocidentais e orientais[9].

Assim, encerro a apresentação dos marcos teóricos deste estudo para, então, analisar leis, projetos de lei e algumas indicações legislativas relacionadas às ferramentas de reconhecimento facial no Brasil.

[9]Talvez você esteja se perguntando sobre o fato da China não ter sido abordada até então. Esta tese trata do problema da extração massiva de dados e da vigilância dentro de um contexto ocidental de uma perspectiva do Sul Global na qual se enquadra a realidade Brasileira. Por isso, as análises mais complexas sobre o país ficarão de fora. Ainda assim, reconheço que a China tem sido uma questão difícil de explicar. Muitas vezes, é difícil separar o que é propaganda anticomunista das análises sobre a realidade chinesa. Ao mesmo tempo, também é complicado encontrar textos sobre o que acontece no país que não pareçam propaganda pró-governo. O fato é que esse é, realmente, um país muito vigiado, cheio de câmeras e outras tecnologias de vigilância e controle. Isso posto, é importante relembrar que o tema da privacidade não é um valor universal para todas as culturas do modo como o ocidente a vê.

3 O RECONHECIMENTO FACIAL PELA ÓTICA DA POLÍTICA

De vez em quando todos os olhos se voltam pra mim /
De lá de dentro da escuridão /
Esperando e querendo que eu seja um herói
Todos os Olhos – Tom Zé

O surgimento e a disseminação de tecnologias em diversas áreas implicam a necessidade de regulamentação dessas práticas e a maior parte da responsabilidade para fazê-lo recai no setor público. Isso decorre tanto do desejo de implementá-las quanto do de proibi-las. Além do mais, pessoas legisladoras também buscam demonstrar, por meio de suas atuações nas câmaras legislativas, que fazem parte do debate público, conhecem os problemas do momento e são capazes de responder às questões sociais das mais diversas ordens. Muitas vezes, tais necessidades refletem na elaboração de projetos diversos, como os que analisarei ao longo deste capítulo.

A lógica de militarização da vida cotidiana (Graham, 2016) tem demonstrado que o desejo político de implementação de tecnologias de vigilância é uma tendência ininterrupta, o que pode ser visto no aumento de propostas legislativas em cada ciclo. As autoridades públicas, os governos e as instituições supranacionais têm defendido abertamente a necessidade de implantar tecnologias de vigilância em prol da segurança (Amoore; De Goede *apud* Čas *et al*, 2017).

Uma narrativa comum, que é bastante utilizada para convencer comunidades do uso de ferramentas de reconhecimento facial, é a de que elas reduzirão crimes, melhorarão a segurança pública e são supostamente mais imparciais e sem vieses, se comparadas aos humanos (Bell, 2023), o que também poderá ser visto frequentemente nos discursos políticos refletidos nesse capítulo.

É nesse contexto que se torna impossível separar dados e política. Os dados não têm apenas delineado as relações sociais, as preferências pessoais e as oportunidades, mas também têm influenciado fortemente as democracias (Bigo, 2019). Do mesmo modo, ferramentas, como o reconhecimento facial, são influenciadas politicamente e impactam a política em sociedade, podendo gerar discussões éticas e jurídicas, nem sempre previsíveis no momento do desenvolvimento das ferramentas (Oliveira, 2021).

As disputas sobre a coleta e a guarda de dados, repletas de conflitos e de mudanças bruscas nas políticas, têm mostrado evidências da interação entre o desenvolvimento tecnológico e os recursos de vigilância, por um lado, e entre as políticas de regulamentação e de segurança, por outro. Assim, há uma disputa no que se refere aos marcos regulatórios da inteligência artificial e ao desenvolvimento de ferramentas baseadas em IA (Čas *et al*, 2017), como as TRFs, e que apresentarei ao longo do texto.

Em relação à metodologia desta pesquisa, as estratégias usadas para o recolhimento dos dados apresentados neste capítulo foram diferentes para cada portal de câmara legislativa, de acordo com as especificidades de apresentação das informações nas páginas da autoridade legislativa em questão. Ao *corpus,* somam-se também a lei de acesso à informação, 12.527/2011, a Lei Geral de Proteção de Dados, 13.709/2018, além das leis e proposições específicas que versam sobre tecnologias de reconhecimento facial no país.

A busca pela expressão “reconhecimento facial” recuperou 58 resultados, entre projetos de lei, requerimentos de diversos tipos, pareceres, votos em separados, emendas na comissão, etc. Foram mantidos apenas os projetos de lei que também passaram por análise, restando 44 itens, apresentados na tabela 1, a seguir, do mais recente para o mais antigo.

Tabela 1: Leis ou proposições legislativas federais.

Lei ou Proposição Legislativa	Ementa
PL 284/2023	Dispõe sobre regras de segurança para os motoristas por aplicativos, e dá outras providências.
PL 2.606/2023	Institui a identificação biométrica e ou facial para ingresso nas escolas da rede pública ou privada da educação básica de ensino, a submissão dos ingressantes à verificação por equipamentos detectores de metais e sobre a obrigatoriedade de aquisição de equipamentos de detecção de metais, porta giratória com detecção de metais e outros equipamentos.
PL 2.714/2023	Regulamenta o uso, instalação e implementação de tecnologia de reconhecimento facial em câmeras e sistemas de videomonitoramento, e dá outras providências.
PL 2.745/2023	Institui obrigatoriedade a todos os estádios de futebol, ginásios, arenas e demais locais de competições de esportes profissionais, credenciados para realização de jogos/competições oficiais a implementação de tecnologia de câmeras e sistemas de videomonitoramento com reconhecimento facial ou não.
PL 4.073/2023	Altera o art. 69 da Lei nº 8.212, de 24 de julho de 1991, que dispõe sobre os

	Planos de Benefícios da Previdência Social, para tratar da prova de vida do beneficiário do Instituto Nacional do Seguro Social – INSS.
PL 3.839/2023	Autoriza o uso de fotografia de identificação com elemento de indumentária tradicional que exprime a identidade da pessoa, bem como altera as leis nº 7.116, de 29 de agosto de 1983, nº 9.503, de 23 de setembro de 1997 (Código de Trânsito Brasileiro) e o Decreto-Lei nº 5.452, de 1º de maio de 1943 (Consolidação das Leis do Trabalho).
PL 4.179/2023	Dispõe sobre a confirmação facial no comércio de bens e serviços pela internet.
PL 3.047/2023	Altera a Lei nº 9.394, de 20 de dezembro de 1996, que estabelece as diretrizes e bases da educação nacional (LDB), para dispor sobre a instalação de software de reconhecimento facial nas instituições de nível superior.
PL 2.028/2023	Dispõe sobre o endurecimento da fiscalização e o cumprimento da faixa etária para jogos eletrônicos.
PL 1.921/2023	Altera a Lei no 9.394, de 20 de dezembro de 1996, que estabelece as diretrizes e bases da educação nacional, para dispor sobre a instalação de detectores de metais, câmeras nos arredores das escolas; software de reconhecimento facial, instalação de internet 5G e iluminação em volta das ruas circunvizinhas.
PL 1.828/2023	Autoriza a instalação, em todo o território nacional, de câmeras de reconhecimento facial nas estações ferroviárias e rodoviárias, no interior dos vagões das composições, em vias públicas e repartições públicas; e dá outras providências.
PL 243/2023	Dispõe sobre o emprego de tecnologia de reconhecimento facial de crianças e adolescentes desaparecidos.
PL 3.069/2022	Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências.
PL 807/2022	Estabelece medidas de prevenção e combate ao trabalho infantil em empresas de aplicativos de entregas ou transporte e dá outras providências.
PL 2.392/2022	Dispõe sobre o uso de tecnologias de reconhecimento facial nos setores público e privado.
PL 1.756/2022	Dispõe sobre a obrigatoriedade de instalação de câmeras para reconhecimento facial em hospitais públicos.
PL 572/2021	Altera a Lei nº 13.812, de 16 de março de 2019, e cria o Banco Nacional de Dados de Reconhecimento Facial e Digital.
PL 3.714/2021	Dispõe sobre o reconhecimento facial em todas as fases da persecução penal.
PL 3.307/2021	Altera a Lei no 10.703, de 18 de julho de 2003, que dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos, para tornar obrigatório o uso de sistema de verificação das informações dos usuários.
PL 1.969/2021	Dispõe sobre os princípios, direitos e obrigações na utilização de sistemas de inteligência artificial.
PLP 245/2020	Altera a redação do art. 3º da Lei Complementar nº 79, de 7 de janeiro de 1994, que cria o Fundo Penitenciário Nacional – FUNPEN, e do art. 64 da Lei nº 7.210, de 11 de julho de 1984, que institui a Lei de Execução Penal – LEP.
PL 4.768/2020	Altera a Lei nº 12.587, de 2012, para estabelecer diretrizes para a prestação do serviço de transporte remunerado privado individual de passageiros, e a Lei nº 8.989, de 1995, para instituir isenção do Imposto sobre Produtos Industrializados – IPI –, na aquisição de automóveis por motoristas que prestem esse serviço.
PL 329/2020	Dispõe sobre a obrigatoriedade de identificação facial ou biométrica e pagamento por meios eletrônicos em veículos particulares que exerçam transporte de passageiros via aplicativos.
PL 1.786/2020	Altera a Lei nº 13.982, de 02 de abril de 2010, para possibilitar a substituição do Cadastro de Pessoa Física - CPF por outro documento oficial ou por outras formas de identificação dos beneficiários do auxílio emergencial, e dá outras providências.
PL 6.163/2019	Institui o Plano Regional de Desenvolvimento do Nordeste para o período de

	2020-2023.
PL 4.828/2019	Dispõe sobre a obrigatoriedade de empresas fabricantes de aparelhos celulares introduzirem aplicativo permanente nos aparelhos celulares que saem de fábrica e nos antigos para acionar a polícia em caso de violência contra a mulher.
PL 4.827/2019	Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), para dispor sobre o uso de dispositivo móvel de segurança para conferir maior efetividade às medidas protetivas de urgência.
PL 4.612/2019	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.
PL 2.537/2019	Obriga o aviso sobre o reconhecimento facial em estabelecimentos comerciais.
PL 1.745/2019	Altera a Lei nº 12.527, de 18 novembro de 2011 - Lei de Acesso à Informação, para ampliar as hipóteses de acesso a dados públicos pelos administrados.
PDL 6.75/2019	Susta os efeitos do Decreto 10.046, de 09 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.
PDL 674/2019	Susta os efeitos do Decreto 10.047, de 09 de outubro de 2019, que dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais.
PL 9.414/2017	Obriga a instalação da leitura de impressão digital e facial nos meios de transportes públicos coletivos.
PL 5.699/2016	Obriga a instalação de equipamentos de identificação biométrica em aeroportos.
PL 6.154/2016	Institui a destinação 2% do total dos Recursos do Pré-sal destinados à Educação, nos termos da Lei Nº 12.351, de 22 de dezembro de 2010, para implantação de Sistema de Frequência Digital Escolar - controle de frequência de alunos em escolas públicas.
PL 4.413/2016	Torna obrigatória a implantação de sistema de controle de frequência de alunos em escolas públicas – Frequência Digital Escolar.
PL 7.461/2014	Altera a Lei nº 9.454, de 7 de abril de 1997, para vincular o Cadastro Nacional de Registro de Identificação Civil ao sistema biométrico, previsto na Lei nº 12.034, de 29 de setembro de 2009, e dá outras providências.
PL 7.759/2014	Altera a Lei nº 9.454/1997, que institui o número único de Registro de Identidade Civil e dá outras providências, tornando obrigatória a identificação biométrica para a emissão de documento de identidade.
PL 7.902/2010	Modifica o art. 1º da Lei nº 9.454, de 7 de abril de 1997, que "Institui o número único de Registro de Identidade Civil e dá outras providências."
PL 1.230/2007	Estabelece que o credenciamento e autenticação de usuário para proceder alterações de informações em sistemas e bancos de dados nos setores de arrecadação de tributos, pagamentos diversos e de pessoal na Administração Pública Federal será dotado de características biométricas (impressão digital, reconhecimento facial ou da íris) ou outro mecanismo tecnológico.
PL 5.034/2005	Inclui dados na carteira de identidade e dá outras providências.
PL 3.372/2004	Dispõe sobre mecanismos de segurança para acesso aos sistemas e bancos de dados da Administração Pública Federal.
PL 1.877/2003	Dá nova redação ao art. 3º, letra "e" da Lei nº 7.116 de 09 de agosto de 1983.
PL 879/2003	Obriga as empresas de ônibus a terem GPS e câmeras de vídeo.

Fonte: Elaboração própria, 2024.

A seguir, a tabela 2 apresenta o mapeamento de projetos, leis, indicações legislativas e moções apresentados nos estados brasileiros e no Distrito Federal. Tais documentos ajudam a compreender o que tem sido discutido em nível estadual.

Tabela 2: Mapeamento dos projetos de lei a favor da implementação do reconhecimento facial nos estados brasileiros.

Estado	Proposição legislativa	Ementa
AM	Projeto de Lei 2/2019	Determina o uso de ferramentas de biometria digital nas viaturas policiais de todo o estado do Amazonas.
AM	Projeto de Lei 196/2018	Determina o uso de ferramentas de biometria digital nas viaturas policiais de todo o estado do Amazonas.
AP	Projeto de Lei 0091/2019	Institui o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos no estado do Amapá.
PE	Projeto de Lei 1.466/2020	Dispõe sobre a realização de prova de vida por meio eletrônico ou virtual no âmbito do Estado de Pernambuco, dos aposentados e pensionistas, cujos benefícios previdenciários são geridos pela Fundação de Aposentadorias e Pensões dos Servidores do Estado de Pernambuco – FUNAPE.
PE	Indicação Legislativa Nº 6.102/2021	Automatização da identificação civil e criminal de pessoas naturais no âmbito do Estado de Pernambuco, mediante biometria, com a coleta e o armazenamento de dados em meio digital.
PE	Projeto de Lei 669/2023	Institui o protocolo de acesso, para visitantes, nas unidades de ensino da Rede Pública Estadual de Pernambuco.
PE	Projeto de Lei 1.220/2023	Estabelece diretrizes para a criação do dispositivo “Escola Protegida” no âmbito do Estado de Pernambuco e dá outras providências.
MA	Projeto de Lei 75/2021	Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes e dá outras providências.
PB	Lei 11.858/2021 (origem: PLO 1331/2019)	Obriga o aviso sobre o reconhecimento facial em estabelecimentos comerciais.
PB	Projeto de Lei 2.453/2021	Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes e dá outras providências.
CE	Indicação Legislativa 202/2020	Dispõe acerca da instituição de banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos, na forma que indica. – (CIA, CDS, CTASP, COFT)
CE	Indicação	Dispõe sobre a obrigatoriedade de Concessionárias do Serviço

	legislativa 411/2019Indicação Legislativa 411/2019	Público de Administração de Terminais Rodoviários, instalação de câmeras de segurança com tecnologia de reconhecimento facial de suspeitos e procurados da justiça nos locais que determina e dá outras providências. (CCJR, CICTS, CDS, CTASP, COFT)
CE	Projeto de Lei 146/2023	Dispõe sobre a autorização, no âmbito do Estado do Ceará, para implantação da tecnologia de reconhecimento facial (TRF) nos dispositivos de vigilância por vídeo, na forma que indica.
AL	Indicação Legislativa 546/2017	Solicitando a instalação de catracas com controle de biometria para acesso a estádios de futebol com capacidade de mais de 10 mil pessoas.
AL	Lei nº 8.113/2019Lei nº 8.113/2019	Dispõe sobre a autorização e a regulamentação da venda e do consumo de bebidas alcoólicas em eventos desportivos no Estado de Alagoas e no art. 5º fica autorizada a instalação de sistemas de reconhecimento facial nos estádios localizados no Estado.
AL	Lei nº 7.333/2012	Desenvolver ações preventivas e agilidade no combate à criminalidade, através de tecnologia capaz de realizar reconhecimento facial, identificação de movimentos e placas de veículos, diminuindo o índice de criminalidade, utilizando uma moderna ferramenta tecnológica.
BA	Projeto de Lei 22.451/2017	Obriga a utilização de sistema de identificação biométrica nas entradas de estádios com capacidade superior a 10.000 (dez mil) pessoas, nos dias de jogos de futebol e dá outras providências.
BA	Moção 22.283/2019	Moção de Aplausos ao Poder Executivo Estadual pela iniciativa do Governador e do Secretário de Segurança Pública de ampliar os investimentos em tecnologia para segurança com implantação de video-monitoramento e Identificação Facial em eventos públicos.
BA	Indicação Legislativa 18.790/2011	Indica ao Governador, que determine a implantação de controle eletrônico de frequência, por identificação biométrica, dos servidores e funcionários que prestam serviços em unidades públicas de saúde.
BA	Indicação Legislativa 16.057/2007	Indica ao Secretário de Segurança do Estado, a implantação de sistema de reconhecimento facial para identificação de criminosos
TO	Lei 4.058/2022	Dispõe sobre o Banco de Dados de Reconhecimento Facial e Digital para a Prevenção ao Desaparecimento de Pessoas no Estado do Tocantins, e dá outras providências.
GO	Projeto de Lei 2019001893/2019	Dispõe sobre a obrigatoriedade de instalação de câmeras inteligentes pelas empresas concessionárias de transporte coletivo urbano do estado de Goiás, que permitem detectar o reconhecimento facial de suspeitos de crime e procurados da justiça.
GO	Projeto de Lei 2021005741	Cria o banco estadual de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes, e dá outras providências.
GO	Projeto de Lei 298/2023	Altera a lei n° 16.499, de 10 de fevereiro de 2009 para prever a disponibilização de reconhecimento facial de pessoas desaparecidas no cadastro de pessoas desaparecidas do estado de Goiás.
DF	Indicação Legislativa 8.929/2010	Sugere providências ao excelentíssimo senhor Governador do Distrito Federal para a implementação de sistema biométrico facial, de campanhas de conscientização do uso do benefício de gratuidade do

		transporte e de uma fiscalização eficiente para a prevenção de fraudes e o consequente escoamento de dinheiro público no sistema de transportes coletivo integrado do Distrito Federal.
DF	Projeto de Lei 1.649/2020	Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes e dá outras providências.
DF	Lei 6.712/2020 (PLO 936/20)	PUBLICAÇÃO DA LEI Nº 6.712/2020, EM 11/11/2020, NO DODF. (VETO AO ART. 8º) Dispõe sobre o uso de tecnologia de reconhecimento facial – TRF[10] na segurança pública e dá outras providências.
DF	Projeto de Lei 459/2023	Altera a Lei nº 6.390, de 25 de setembro de 2019, que cria o Programa Cidade Segura – PCS e dá outras providências, para dispor sobre videomonitoramento de segurança em praças públicas.
MT	Projeto de Lei 12/2023	Institui o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos, no âmbito do estado de Mato Grosso.
MT	Projeto de Lei 734/2023	Cria o Sistema Integrado de Vigilância Comunitária de Segurança Pública e dispõe sobre a obrigatoriedade de padrões mínimos de implantação de um sistema de videovigilância comunitária nos municípios.
MT	Projeto de Lei 140/2021	Cria o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos, no âmbito do estado de Mato Grosso.
MT	Projeto de Lei 53/2020	Institui o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos, no âmbito do estado de Mato Grosso.
MT	Indicação Legislativa 4063/2020	Indica ao exmo. Senhor governador do estado, Mauro Mendes, com cópia a secretaria estadual de segurança pública – SESP, a necessidade de implantação de sistema de monitoramento eletrônico (câmeras de segurança) em todas as pontes do estado do Mato Grosso.
MT	Projeto de Lei 84/2019	Obriga a utilização de sistema de identificação biométrica nas entradas e de sistema de monitoramento por imagem em toda a área de uso comum de estádios com capacidade superior a 10.000 (Dez mil) pessoas, nos dias de jogos de futebol, no âmbito do estado de Mato Grosso, e dá outras providências.
MT	Projeto de Lei 387/2015	Dispõe sobre a instalação de câmeras de vigilância nas áreas externas dos estabelecimentos bancários de crédito, financiamento e investimentos e de estabelecimentos congêneres.
MS	Projeto de Lei 00244/2023	Institui o Banco de Dados de Reconhecimento Facial e Digital de Crianças e Adolescentes Desaparecidos, no âmbito do Estado de Mato Grosso do Sul, e dá outras providências.
MS	Projeto de Lei 152/21	Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes, e dá outras providências.
MS	Projeto de Lei 84/2019	Obriga a utilização de sistema de identificação biométrica nas entradas e de sistema de monitoramento por imagem em toda a área de uso comum de estádios com capacidade superior a 10.000 (Dez mil) pessoas, nos dias de jogos de futebol, no âmbito do estado de Mato Grosso, e dá outras providências.

[10]É possível observar muitos erros de ortografia, gramática e concordância nos textos das leis e projetos de lei. Optei por mantê-los no original. As exceções são apenas quando a manutenção do texto impossibilita a compreensão do mesmo.

MS	Projeto de Lei 152/21	Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes, e dá outras providências.
MG	Projeto de Lei 391/2019	Dispõe sobre a obrigatoriedade de implantação de tecnologia de reconhecimento facial em locais públicos, no âmbito do Estado.
ES	Projeto de Lei n° 207/2020	Ficam as operadoras de celular obrigadas a possuir um banco de dados dos clientes com terminal de reconhecimento facial e biometria digital, no âmbito do estado do Espírito Santo.
ES	Indicação n° 293/2020	solicitar, em conjunto com a secretaria de estado da segurança pública e defesa social – SESP, a instalação de tecnologias de reconhecimento facial por aplicativo e por sistema de videomonitoramentos no estado do Espírito Santo.
ES	Indicação n° 2.896/2019	seja sugerido ao senhor governador do estado do Espírito Santo integração e ampliação do sistema de segurança e monitoramento adotado no transporte coletivo urbano em tempo real, incluindo reconhecimento facial e dispositivo do tipo “botão do pânico” de forma a garantir a segurança sem prejuízos à integridade física dos motoristas e cobradores.
ES	Indicação n° 1.715/2019	Indica ao Poder Executivo que, por intermédio da Secretaria de Estado da Segurança Pública e Defesa Social (SESP) e outros entes públicos, elabore o projeto e promova a implantação do sistema de videomonitoramento de acessos rodoviários ao estado do Espírito Santo, em vias estaduais e federais limítrofes a outros estados, com capacidade de detecção de placas de veículos com restrição e em reconhecimento facial de criminosos.
ES	Indicação Legislativa 7.556/2021	Para que o Governo do Estado do Espírito Santo possa criar o Banco de dados de reconhecimento facial e digital para prevenção ao desaparecimento de crianças e adolescentes.
RJ	Projeto de Lei 607/2019	Torna obrigatória a instalação de câmeras de monitoramento com reconhecimento facial em todas as praças de pedágios, no âmbito do estado do Rio de Janeiro.
RJ	Projeto de Lei 2.548/2020	Dispõe sobre a obrigatoriedade da carteira de identidade para todos os cidadãos com idade inferior a 18 (dezoito) anos a ser emitida pelos órgãos de identificação competentes, do estado do Rio de Janeiro. E no Art. 1º inciso 1º No ato deverá ser realizadas as imagens para reconhecimento facial e digital de todos os cidadãos com idade inferior a 18 (dezoito) anos.
RJ	Projeto de Lei 318/2019	Dispõe sobre a obrigatoriedade da implantação de tecnologia de reconhecimento facial em toda a área de uso comum, incluindo eventos públicos e privados, com capacidade superior a 10.000 (Dez mil) pessoas, no âmbito do estado do Rio de Janeiro.
RJ	Lei 9.167/2021	Dispõe sobre o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos.
RJ	Projeto de Lei 1.505/2019	Institui o banco estadual de dados de reconhecimento facial de crianças e adolescentes desaparecidos.
RJ	Projeto de Lei 1.372/2019	Dispõe sobre a instalação obrigatória de câmeras de reconhecimento facial em todas as estações do metrô-rio e da supervia, bem como no interior dos vagões das composições e dá outras providências.
RJ	Projeto de Lei 1.097/2019	Dispõe sobre a instalação de sistema de dispositivo de reconhecimento facial em edificações públicas e privadas no âmbito do estado do Rio de Janeiro e dá outras providências.
RJ	Projeto de Lei	Dispõe sobre a obrigatoriedade de concessionários do serviço público

	342/2019	de metrô, trens e barcas, instalação de câmeras de segurança com tecnologia de reconhecimento facial de suspeitos e procurados da justiça nos locais que determina e dá outras providências
RJ	Projeto de Lei 665/2019	Cria o Sistema de Identificação Biométrica no estado do Rio de Janeiro. O Sistema de Identificação Biométrica abrangerá todos os bancos de dados biométricos existentes no Serviço Público Estadual, podendo compreender também, através de parcerias, as concessionárias ou permissionárias de serviços públicos concedidos, ou delegatárias a elas vinculadas, bem como entidades privadas.
RJ	Projeto de Lei 853/2019	Veda a negociação e comercialização de produtos e serviços no interior dos vagões e embarcações dos transportes públicos do estado do Rio de Janeiro na forma que menciona. E fica o Poder Executivo autorizado a implantar equipamentos de reconhecimento facial ou tecnologia similar, com o intuito de aperfeiçoar a integração da segurança nas estações com os órgãos de segurança pública.
RJ	Projeto de lei 4493/2021Projeto de Lei 4.493/2021	Institui a carteira de identidade funcional em formato digital para policiais militares, policiais civis, policiais penais, e demais agentes de segurança pública do estado do Rio de Janeiro (autorizado no formato online e digital) e determinando a coleta da foto digital a ser em qualidade para ser usada em reconhecimento facial.
RJ	Projeto de Lei 341/2019	Dispõe sobre a obrigatoriedade de concessionários do serviço público de administração de terminais rodoviários, instalação de câmeras de segurança com tecnologia de reconhecimento facial de suspeitos e procurados da justiça nos locais que determina e dá outras providências.
RJ	Projeto de Lei 1.833/2020	Institui o banco estadual de dados multibiométricos no sistema de segurança pública, conjugando impressões papilares, impressões palmares, imagens de face, assinatura, íris e fala, bem como dá outras providências.
RJ	Projeto de Lei 2.946/2020	Dispõe sobre a flexibilização dos serviços para obtenção da carteira nacional de habilitação. Art. 3º – Os exames de direção veicular, teóricos, serão realizados via online, por entidades privadas credenciadas pelo Detran do Estado do Rio de Janeiro, por plataformas digitais, que utilizem captura da imagem e reconhecimento facial do candidato, colheita da biometria e controle do tempo de realização do exame teórico.
RJ	Projeto de Lei 1.101/2019	Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes no estado do Rio de Janeiro.
RJ	Requerimento 40/2019	Requer informações ao sr. Governador Wilson Witzel sobre o sistema de investigação e inteligência ultra.
RJ	Projeto de Lei 274/2023	Dispõe sobre a instalação de dispositivo de reconhecimento facial de suspeitos e procurados da justiça em terminas rodoviários, portos e aeroportos no âmbito do estado do Rio de Janeiro e dá outras providências.
RJ	Projeto de Lei 384/2023	Dispõe sobre a instalação de dispositivo de reconhecimento facial de suspeitos e procurados da justiça em shoppings centers no âmbito do Estado do Rio de Janeiro e dá outras providências.
RJ	Projeto de Lei 550/2023	Autoriza o poder executivo a utilizar tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública, no Estado do Rio de Janeiro, e dá outras providências.
SP	Projeto de Lei 739 / 2023	Institui o porte eletrônico de identificação funcional para os integrantes da Polícia Militar do Estado.
SP	Projeto de Lei 580 / 2023	Autoriza o Poder Executivo a implementar sistema de câmeras de reconhecimento facial nas unidades de ensino da rede pública do Estado.

SP	Projeto de Lei 579 / 2023	Institui o protocolo de acesso para visitantes nas unidades de ensino do Estado.
SP	Projeto de Lei 865 / 2019	Torna obrigatória a instalação de câmeras de reconhecimento facial em todas as estações do Metrô e da CPTM, bem como no interior dos vagões das composições.
SP	Indicação Legislativa 2.287/2019	Indica que todas as estações do Metrô e da CPTM deverão contar com câmeras de reconhecimento facial em suas dependências, bem como no interior dos vagões das composições.
SP	Requerimento 696/2020	Requer ao Sr. Secretário da Segurança Pública informações sobre a utilização das imagens colhidas pelas “bodycams” nas investigações de violência policial.
PR	Indicação Legislativa 429/2012	Realização de estudos para adoção de sistemas de identificação biométrica dos apenados e o monitoramento eletrônico da população carcerária no Estado do Paraná, conforme especifica.
PR	Projeto de Lei 75/2021	Institui o banco de dados de reconhecimento facial e digital de pessoas desaparecidas. Lei do reencontro.
PR	Projeto de Lei 148/2019	Dispõe sobre a permissão de implantação de tecnologia de reconhecimento facial em locais públicos.
SC	Projeto de Lei 0027.1/2021	Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes e adota outras providências.
SC	Indicação Legislativa 0104.6/2021	Sugere a criação de um Banco de Dados de Reconhecimento Facial e Digital para a Prevenção ao Desaparecimento de Crianças e Adolescentes.
SC	Indicação Legislativa 2142.9/2020	Sugere a aquisição de softwares, a serem utilizados em câmeras de segurança com tecnologia OCR, bem como de câmeras de reconhecimento facial, a fim de identificar criminosos, coibir condutas ilícitas e auxiliar na resolução de crimes.
SC	Projeto de Lei 0299.1/2018	Dispõe sobre a possibilidade de convênio entre a secretaria de estado da segurança pública e os tabelionatos de notas para o compartilhamento de dados de identificação civil.
SC	Projeto de lei 0592.3/2013Projeto de lei 0592.3/2013Projeto de lei 0592.3/2013Projeto de Lei 0592.3/2013	Obriga a utilização de sistema de identificação biométrica nas entradas e de sistema de monitoramento por imagem em toda a área de uso comum de estádios com capacidade superior a 10.000 (dez mil) pessoas, nos dias de jogos de futebol, e adota outras providências.
RS	Projeto de Lei 73/2019	Institui o Banco de Dados de Reconhecimento Facial e Digital de Crianças e Adolescentes Desaparecidos.
RS	Projeto de Lei 15460/2020	Cria o Banco de Dados de Reconhecimento Facial e Digital para a Prevenção ao Desaparecimento de Crianças e Adolescentes.

Fonte: Elaboração própria, 2023.

A tabela 3 apresenta o mapeamento dos projetos de lei contrários à implementação do reconhecimento facial nos estados brasileiros.

Tabela 3: Mapeamento dos projetos de lei contrários à implementação do reconhecimento facial nos estados brasileiros

Estado	Proposição Legislativa	Ementa
BA	Projeto de Lei 2.4579/2022	Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo Poder Público no Estado da Bahia.
CE	Projeto de Lei 251/2022	Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo poder público no estado do Ceará.
DF	Projeto de Lei 629/2023	Estabelece diretrizes para política de instalação de câmeras corporais nos uniformes dos policiais penais no sistema prisional do Distrito Federal.
DF	Projeto de Lei 595/2023	Estabelece diretrizes para política de videomonitoramento no sistema prisional do Distrito Federal.
MG	Projeto de Lei 3812/2022	Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo poder público no Estado.
PE	Projeto de Lei 402/2023	Proíbe a utilização de tecnologia de reconhecimento facial automatizado no âmbito dos sistemas de segurança do Estado de Pernambuco e dá outras providências.
RJ	Projeto de Lei 5240/2021	Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo poder público no Estado do Rio de Janeiro.
RS	Projeto de Lei 16/2023	Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo Poder Público no Estado do Rio Grande do Sul.
SE	Projeto de Lei 470/2023	Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo poder público no estado de Sergipe.
SP	Projeto de Lei 385/2022	Restringe o uso de tecnologias de reconhecimento facial pelo Poder Público.

Fonte: Elaboração própria, 2024.

Até dezembro de 2023, nos estados do Acre, Rondônia, Roraima, Piauí e Rio Grande do Norte não foram identificadas proposições legislativas contrárias ou a favor da adoção de ferramentas de reconhecimento facial. Na página do *Tire meu rosto da sua mira* não constavam os estados do Pará e Tocantins. A busca realizada por mim nas leis e proposições legislativas nos dois estados não encontrou resultados no Pará. Contudo, em dezembro de 2022, foi aprovada lei que trata de tecnologias de reconhecimento facial no Tocantins, o que já consta na tabela anteriormente apresentada[11].

Não farão parte da análise as proposições legislativas municipais a respeito do reconhecimento facial, por reconhecer que o universo de análise ficaria muito grande, impossibilitando a execução do estudo.

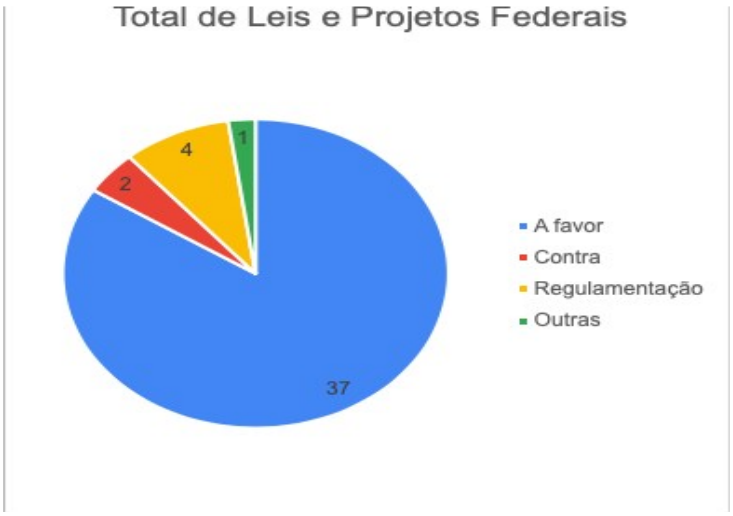
[11]A busca foi realizada em fevereiro de 2023 e refeita pela última vez no dia 07 de dezembro de 2023.

Este capítulo divide-se em duas partes. Na primeira delas, eu apresento os dados extraídos do levantamento de matérias legislativas – para este fim, considerei apenas projetos e leis – federais, estaduais e do DF. Depois, a partir da metodologia da análise do discurso, busco apresentar e debater as leis que estão relacionadas ao uso (ou não) de ferramentas de reconhecimento facial no Brasil. Então, vamos aos números.

3.1 Dados sobre regulamentação de ferramentas de reconhecimento facial no Brasil

Na Câmara dos Deputados, ou seja, em nível federal, foram 37 projetos a favor e dois contrários. Os projetos com o objetivo de regulamentar a tecnologia foram quatro e um projeto classificado como outras, conforme pode ser visto na figura 1 a seguir.

Figura 1: Projetos e Leis Federais



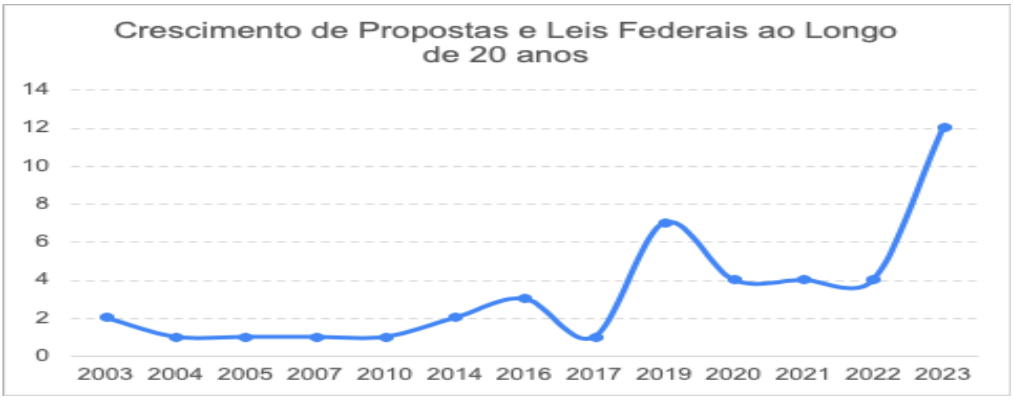
Fonte: Elaboração própria

Entendo que projetos de regulamentação são, em certa medida, a favor de ferramentas de reconhecimento facial. Contudo, creio ser importante diferenciá-los dos demais, pois representam características próprias, como a apresentação de limites para o uso das tecnologias e informações mais específicas sobre o que os sistemas devem conter, como analisarei mais adiante, ao discutir os projetos de lei

com maior profundidade. Nesse sentido, parece-me que partem do pressuposto de que tecnologias de reconhecimento facial são uma realidade e, por isso, precisam de regulamentação. A categoria “outros” aqui serve para enquadrar projetos de lei que não são exatamente sobre o reconhecimento facial como tecnologia, mas a tecnologia é citada no texto, como no projeto que permite indumentárias em carteiras de identificação. É o exemplo do PL 3.839/2023.

A figura 2 apresenta o crescimento das proposições que envolvem TRFs entre 2003 e 2023. Os anos com o maior número de matérias legislativas são aqueles que correspondem ao início de mandato parlamentar, como os de 2019 e 2023. Contudo, em 2023, foram apresentados 13 projetos, enquanto em 2019 foram sete, quase o dobro de 2019. É o que pode ser visto na figura 2.

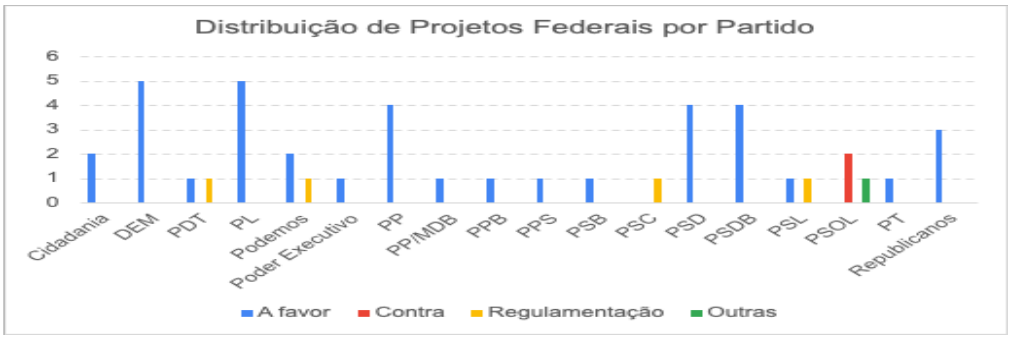
Figura 2: Crescimentos de Propostas e Leis Federais em 20 anos



Fonte: Elaboração própria, 2024.

Este gráfico mostra apenas o crescimento dos projetos na Câmara dos Deputados sem diferenciá-los em a favor, contra, regulamentação ou em outra situação. O gráfico 3, a seguir, mostra a distribuição de projetos de nível federal, por partido político.

Figura 3: Distribuição de Projetos Federais por Partido

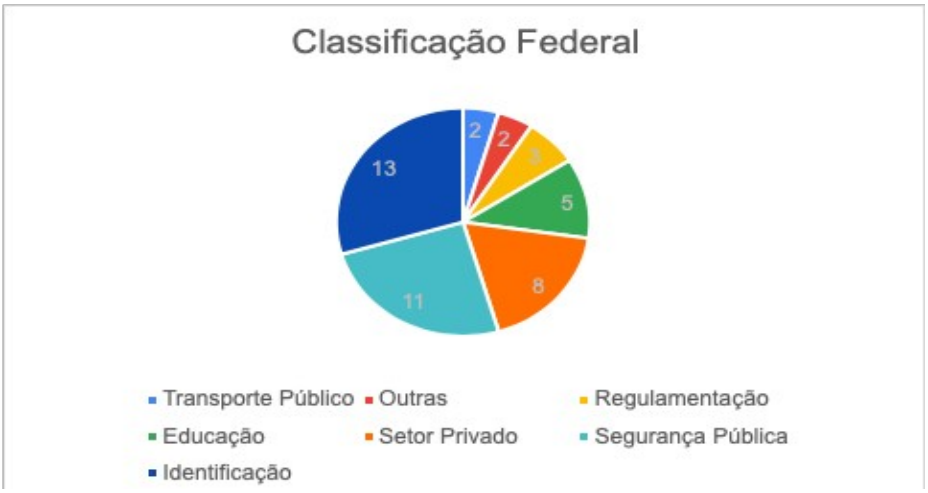


Fonte: Elaboração própria (2024)

O partido que mais submeteu projetos foi o PL, seguido pelo DEM e, em terceiro, PP, PSD e PSDB. Em quinto, o Republicanos. O único partido a submeter propostas contrárias ao uso de TRFs foi o PSOL.

A seguir, na figura 4, apresento os projetos classificados por temática.

Figura 4: Classificação Federal



Fonte: Elaboração própria, 2024.

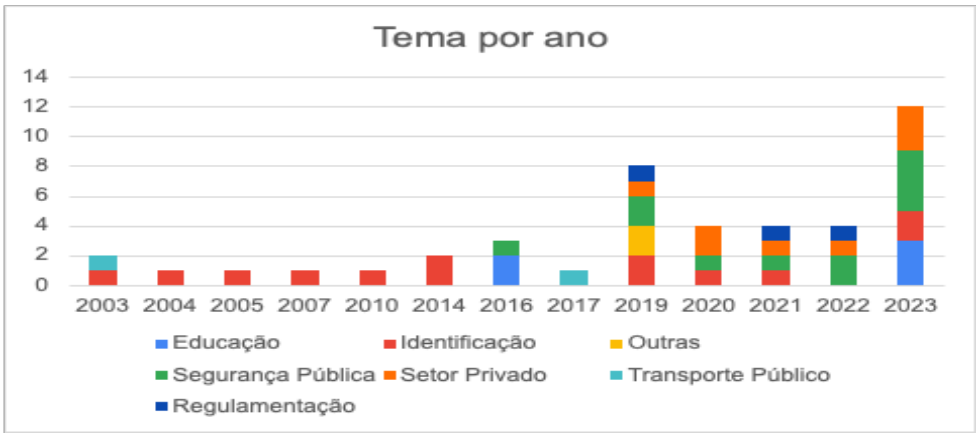
Em nível federal, as matérias legislativas que mais têm sido submetidas são aquelas que relacionam TRFs à identificação de pessoas, correspondendo a 13. Em segundo lugar, aparecem 11 matérias voltadas à segurança pública. Depois, em terceiro lugar, temos oito matérias que objetivam regular o uso de TRFs no setor privado, como aplicativos de transporte de passageiros. Em quarto lugar, há cinco matérias voltadas para o uso de TRFs na educação. Em quinto lugar, aparecem três projetos de regulamentação da tecnologia. Em sexto lugar, temos duas matérias voltadas para o uso de TRFs no transporte público. Em sétimo e último lugar, na categoria outras, existem dois projetos que não se enquadravam nas demais categorias. A categoria segurança pública contém projetos em diversas áreas, o que pode ser visto na figura 5, a seguir.

Figura 5: Divisões dentro da Segurança Pública - Federal

Fonte: Elaboração própria (2024).

Ao analisar o crescimento dos temas por ano, é possível perceber que os primeiros projetos eram sobre transportes e identificação, conforme pode ser visto na figura 6 adiante. No caso da identificação, é possível afirmar que eles estão direcionados à coleta de dados dos cidadãos, por meio das carteiras de identidade, e à criação de bancos de dados com essas informações.

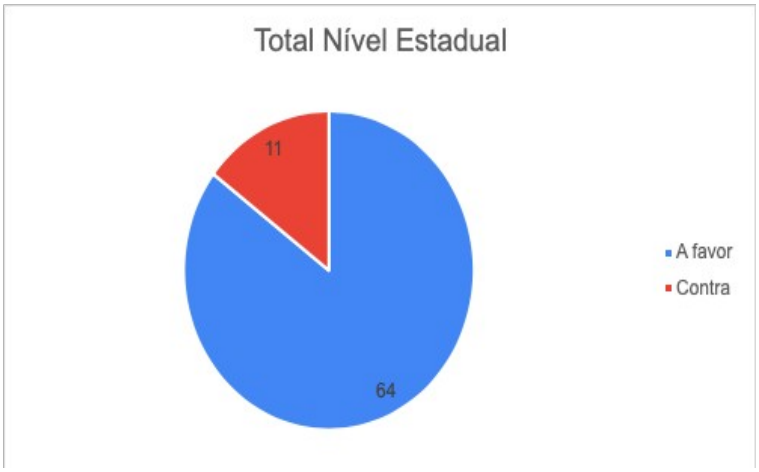
Figura 6: Temas por Ano



Fonte: Elaboração própria (2024).

No ano de maior crescimento, 2023, é possível observar que a educação e a segurança pública foram as áreas que chamaram mais a atenção de legisladores. Os projetos para regulamentação da tecnologia encontram-se nos anos de 2019, 2021 e 2022. Em nível estadual, os números podem ser vistos na figura 7, a seguir:

Figura 7: Projetos e Leis Estaduais



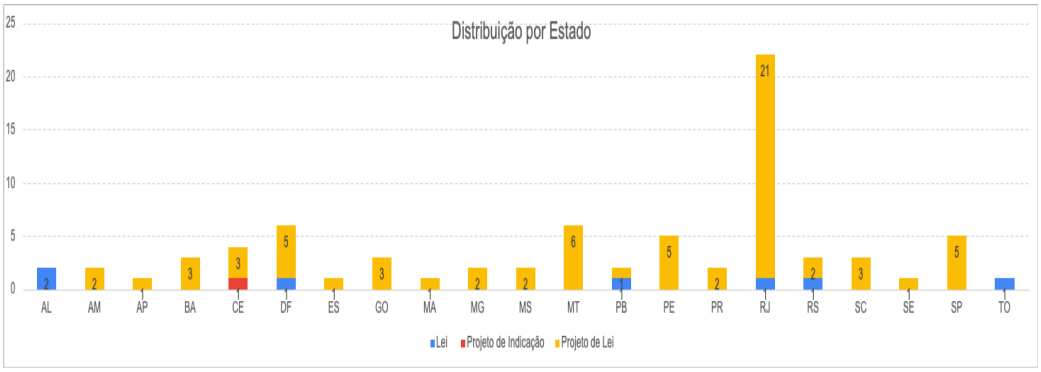
Fonte: Elaboração própria (2024).

Foram 11 projetos direcionados ao banimento de TRFs, propostos entre 2021 e dezembro de 2023. A favor deste tipo de tecnologia, foram 66, entre projetos e leis já promulgadas.

As discussões nos estados funcionam de outra maneira. Nesse caso, não fazia sentido adicionar as categorias *outros* e *regulamentação* porque os tipos de propostas nas casas legislativas estaduais tinham um perfil diferente. Ainda assim, é possível observar que projetos a favor de TRFs ganharam contorno de regulamentação com a atuação de parlamentares de esquerda, como ocorreu no Distrito Federal.

Na figura 8, a seguir, é possível observar as leis, projetos de lei e projetos de indicação distribuídos por estados.

Figura 8: Distribuição de Projetos e Leis por estado



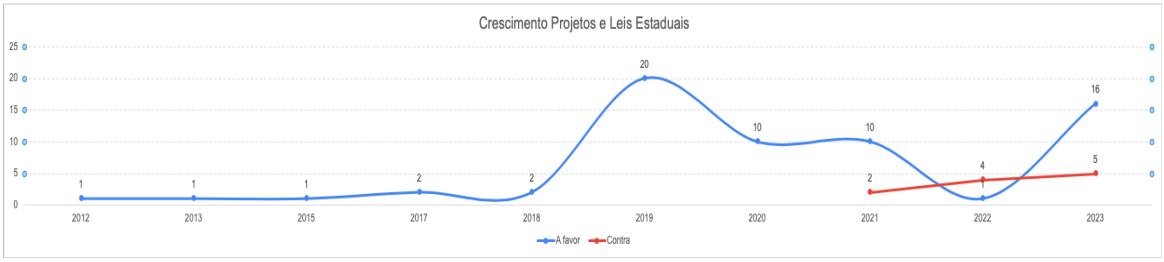
Fonte: Elaboração própria (2024).

O Rio de Janeiro ocupa papel de destaque, no que se refere ao uso de tecnologias de controle e vigilância, como o videomonitoramento e o reconhecimento facial. O maior número de projetos pertence ao estado, conforme pode ser visto na figura 8, anteriormente apresentada. O pioneirismo do RJ era bastante evidente com relação à videovigilância, o que já foi analisado por Bruno Cardoso (2013), e agora se mantém no que se refere à adoção de TRFs. Apesar dos muitos projetos, ainda são poucas as leis aprovadas.

A figura 9, adiante, apresenta o crescimento dos projetos e leis ao longo dos anos. O primeiro ano é o de 2012 e o último é o de 2023, fim do levantamento. Assim como no crescimento das propostas de nível federal, os anos com mais propostas são os de início de mandatos parlamentares, como os de 2019 e 2023. Contudo, nos estados, os parlamentares apresentam um número maior de projetos em 2019, porém a diferença é bem pequena. Foram apenas mais dois projetos. Quanto aos projetos contrários, que podem ser vistos na linha vermelha, os primeiros foram propostos em 2021.

Os PLs contrários ao reconhecimento facial têm crescido ao longo do tempo de maneira estável, mas ainda é cedo para afirmar que tal crescimento permanecerá do mesmo modo. Além disso, o número de projetos a favor sempre vai se sobrepor ao número de contrários. Afinal, eles estão direcionados a diversos setores, enquanto os contrários são quase todos com o objetivo de banir TRFs pelo setor público ou na segurança pública.

Figura 9: Crescimento Projetos e Leis Estaduais

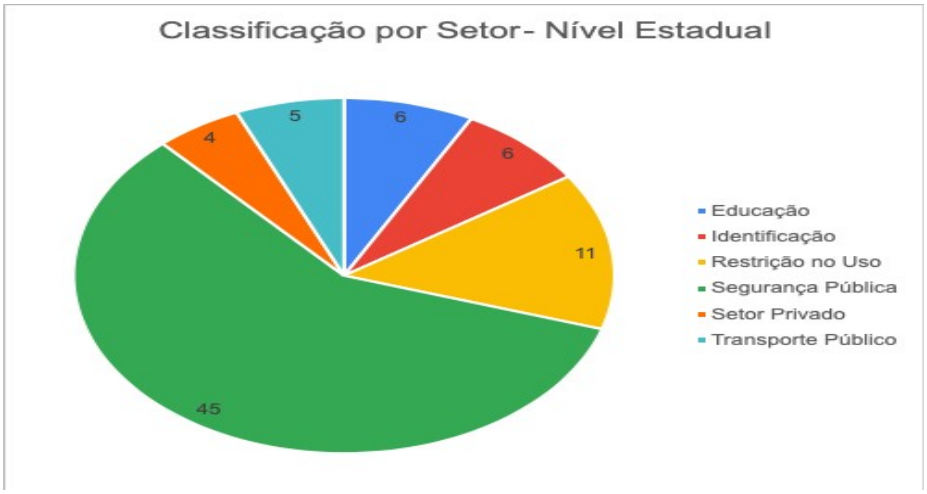


Fonte: Elaboração própria (2024).

Quase todos os projetos de nível estadual, com o objetivo de banir TRFs, foram propostos por partidos identificados com a esquerda ou centro-esquerda. O PSOL foi o que mais submeteu proposições nesse sentido. O único estado em que o Partido Socialismo e Liberdade não esteve envolvido com essas iniciativas foi Minas Gerais. Em São Paulo e no Rio de Janeiro, os projetos foram em coautoria. Em SP, foram coautores o PSOL e o PCdoB. No RJ, PSOL, PSB, PSD e PCdoB são coautores do projeto. O Rio de Janeiro é o único cujo projeto tem coautoria de um partido de centro-direita, como o PSD.

As iniciativas foram classificadas em nível estadual em educação, identificação, segurança pública, transporte público, setor privado e outras, o que pode ser visto na figura 10, a seguir.

Figura 10: Classificação Temática - Estaduais



Fonte: Elaboração própria (2024).

Observa-se que a segurança pública é o setor com o maior número de matérias legislativas no âmbito dos estados. Em segundo lugar, os projetos que

envolvem a restrição no uso de TRFs. Em terceiro, ficam os projetos que envolvem TRFs na educação e na identificação de pessoas. Em quarto lugar, os projetos com o objetivo de estabelecer regras sobre o uso de TRFs no transporte público. Em quinto e último lugar, projetos que envolvem legislar sobre TRFs no setor privado, como nas empresas de telefonia ou nos transportes de passageiros.

Embora eu não tenha ficado muito satisfeita com a categoria “outras”, ela foi necessária para enquadrar os projetos de regulamentação que não consegui enquadrar nas demais. A categoria “segurança pública” inclui também projetos voltados para setores distintos, como estádios; vias e espaços públicos; regulação do uso de TRFs, em espaços públicos e privados; busca de desaparecidos; busca de suspeitos e procurados da justiça; identificação e proibição do uso na segurança pública; totalizando 48 projetos, o que pode ser visto na figura 11, adiante.

O maior número de matérias legislativas na segurança pública está voltado para a busca de pessoas desaparecidas, com 21. Em seguida, matérias para implementação de TRFs em vias e espaços públicos, com 8 projetos. Em terceiro lugar, estão as matérias voltadas para a implementação de TRFs em estádios, com 6. Em quarto lugar, encontram-se 5 matérias voltadas para a utilização de TRFs em atividade policial, como policiamento ostensivo ou em viaturas, por exemplo. Em quinto lugar, com 4, estão as matérias com o objetivo de proibir a utilização de tais tecnologias na segurança pública. Em sexto lugar, estão duas matérias legislativas voltadas para a adoção de TRFs na busca por suspeitos e procurados. Em sétimo e oitavo, ambos com uma, temos matérias voltadas para a regulamentação de TRFs em espaços públicos e privados e de identificação de pessoas.

Figura 11: Classificação Segurança Pública

Fonte: Elaboração própria (2024).

O total de matérias aqui consideradas foi de 48, ou seja, as 44 matérias de segurança pública e mais quatro projetos que, no gráfico anterior, apareciam classificados como restrição no uso. Como objetivam restringir o uso de TRFs na segurança pública, achei importante incluí-los no grupo.

Na próxima seção, apresentarei, de maneira mais aprofundada, os projetos e leis que envolvem a utilização de ferramentas de reconhecimento facial, propostos na Câmara dos Deputados e nas Assembleias Legislativas do Brasil. Porém, antes de passar a ela, quero fazer algumas considerações sobre os dados federais e estaduais.

Os temas de interesse de legisladores federais e estaduais estão relativamente dentro do mesmo espectro. Contudo, nas matérias legislativas estaduais, o tema da segurança pública aparece em primeiro lugar. Já nas matérias legislativas federais, o tema da identificação e da criação de bancos de dados de pessoas é o que tem mais destaque. No caso das divisões dentro da segurança pública, o tema que mais recebe a atenção de parlamentares nos estados é a questão dos bancos de dados e tecnologias de reconhecimento facial para pessoas desaparecidas. No âmbito federal, são os atos voltados para a adoção de TRFs nas atividades policiais e de justiça criminal.

A seguir, analiso o texto dos projetos de leis e das leis, tanto no federal quanto estadual.

3.2 Discussão nas Casas Legislativas

Depois de demonstrar os dados sobre o crescimento de proposições legislativas federais e estaduais, apresento de que maneira a questão das TRFs têm aparecido no conteúdo das matérias legislativas.

3.2.1 A legislação Federal

Nesta seção, apresento projetos, leis e debates que tramitam ou tramitaram na Câmara dos Deputados. As matérias legislativas são dispostas aqui de acordo com a classificação anteriormente apresentada, que divide os projetos nas áreas de transporte público, segurança pública, identificação e educação.

O primeiro projeto federal que se relaciona com TRFs é o PL 879/2003 que "obriga as empresas de ônibus a terem GPS e câmeras de vídeo" (Brasil, 2003a) e é de autoria do deputado Eduardo Cunha (PPB/RJ). O texto do projeto não apresenta menção ao reconhecimento facial. Contudo, sua tramitação e apensação do PL 685/2022 fez com que fosse incorporado ao grupo, ao ser recuperado na base de dados da Câmara dos Deputados com o termo reconhecimento facial. A incorporação de tecnologias de reconhecimento facial em projetos já existentes sobre câmeras de vigilância demonstra como muitos membros da sociedade têm visto TRFs como a evolução natural do videomonitoramento.

O projeto de Lei 9.914/2017, de autoria da deputada Mariana Carvalho (PSDB/RO), tem como objetivo obrigar "a instalação da leitura de impressão digital e facial nos meios de transporte coletivos" (Brasil, 2017). A lei objetiva obrigar "os veículos e estações do transporte público coletivo a adotarem políticas de segurança contra fraude nas concessões de benefícios públicos com a instalação de equipamentos de leitura de impressão digital ou facial" (Brasil, 2017). As medidas incluem a adoção de equipamentos de leitura de impressão facial ou digital. O objetivo da instalação de tais ferramentas é coibir fraudes nos benefícios nos sistemas de transporte. A justificativa da lei é que as fraudes custam R$50 milhões por ano. Contudo, não se apresenta a fonte de tal afirmativa. Utiliza-se ainda, como exemplo de sistema de reconhecimento facial, o utilizado em Brasília para fiscalizar

usuários do Passe Livre Estudantil. Ainda segundo o PL, a conta da adoção será paga pelos operadores de ônibus e não haverá custo para os cofres públicos. Vale questionar com que interesse as operadoras de ônibus farão tal benesse.

O projeto de lei 329/2020, do parlamentar Julio Cesar Ribeiro (Republicanos/DF), objetiva tornar obrigatória a "identificação facial ou biométrica e o pagamento por meios eletrônicos em veículos particulares que exerçam transporte de passageiros via aplicativos" (Brasil, 2020b). O projeto responsabiliza os aplicativos de transporte pela identificação biométrica ou facial de passageiros. Além disso, os passageiros terão que encaminhar documentos comprobatórios relativos aos seus antecedentes criminais.

Na mesma direção, há o projeto de lei 4.768/2020, de autoria do deputado Claudio Cajado (PP/BA), que objetiva alterar a Lei 12.587/2012 "para estabelecer diretrizes para a prestação do serviço de transporte remunerado privado individual de passageiros", e a Lei nº 8.989/1995, "para instituir isenção do Imposto sobre Produtos Industrializados – IPI –, na aquisição de automóveis por motoristas que prestem esse serviço" (Brasil, 2020c). O projeto pretende que seja exigido documento com foto e comprovante de residência para o cadastro de passageiros por parte das empresas e o uso de aplicativo com reconhecimento facial no momento da solicitação da viagem. Não fica explícito nos projetos se pessoas serão discriminadas de acordo com a informação sensível constante em seus antecedentes criminais ou comprovantes de residência.

O projeto de lei 1.828/2023, de autoria do deputado Rodrigo Gambale (Podemos/SP), tem como objetivo dar autorização para que sejam instaladas câmeras de reconhecimento facial nas estações ferroviárias e rodoviárias, no interior dos vagões das composições e em vias e repartições públicas, em todo o território nacional (Brasil, 2023b). Ou seja, o projeto significaria permitir que sejam instaladas câmeras de reconhecimento facial em praticamente todos os lugares públicos. Segundo a proposta,

> É indubitável que a instalação de câmeras de reconhecimento facial nesses locais inibirá a ação criminosa, pois o delinquente saberá que será reconhecido, e, se, ainda assim, praticar o crime, as câmeras o identificarão.
> Não bastasse, as câmeras também facilitarão a localização de eventuais criminosos foragidos e de pessoas desaparecidas,

> prestando, desse modo, um serviço de incalculável importância para todo o País.
> Outrossim, vale lembrar que atualmente é possível implantar no sistema de vigilância por câmeras, programas decodificadores que irão proteger os dados dos usuários, tudo em acordo com a previsão da Lei Geral de Proteção de Dados (LGPD), que foi sancionada em agosto de 2018 e entrou em vigor em agosto de 2020. (Brasil, 2023b)

Em primeiro lugar, gostaria de destacar a confiança com que o parlamentar argumenta que é indubitável e ele o faz, apesar das pesquisas que apontam as altas taxas de erro da tecnologia (Buolamwini, 2023; Nunes; Silva; Oliveira, 2022; Buolamwini; Gebru, 2018). Depois, a desproporcionalidade da ação, que envolve colocar todos os usuários de transportes e serviços públicos sob vigilância para que, eventualmente, sejam encontrados foragidos e desaparecidos. E, em terceiro lugar, a forma como a Lei Geral de Proteção de Dados (LGPD) é acionada. Propõe-se um projeto de vigilância massiva, mas afirma-se que tudo será conforme a LGPD, sem que se dê garantia alguma de como isso ocorrerá.

Promulgada em 2019, a Lei 13.709 é também conhecida como LGPD e apareceu como preocupação de outros legisladores, como poderá ser visto ao longo deste trabalho.

Ainda que as menções à LGPD pareçam recurso retórico, o pesquisador e advogado Samuel de Oliveira (2021) acredita que instrumentos regulatórios que considerem regras jurídicas rígidas podem impor algum desestímulo ao desenvolvimento tecnológico. Na conciliação entre a regra e a ética, o autor acredita que a Lei Geral de Proteção de Dados tem potencial para ser um instrumento normativo apropriado que permite, mas limita, o uso de sistemas de reconhecimento facial, pois a LGPD admite, por intermédio “da aplicação dos princípios previstos em seu artigo 6º, a regulação da atividade de tratamento de dados que, em última instância demarca a forma por meio da qual os sistemas de reconhecimento facial atuam” (Oliveira, 2021, p. 11).

O projeto de lei 5.699/2016 objetiva obrigar “a instalação de equipamentos de identificação biométrica em aeroportos” (Brasil, 2016c). O PL de autoria do Deputado Marcos Rogério, do DEM/RO, foi arquivado. Contudo, há iniciativas em andamento no país com uso de TRFs em aeroportos, o que prova que nem sempre a falta de legislação é garantia de que o Poder Executivo esperará pela existência de regulamentação para adotar medidas. Na realidade, o que tem sido observado, no

que se refere à diversas tecnologias, incluindo TRFs, é que são colocadas em uso para posterior regulamentação.

Embora alguns projetos envolvam a proteção das operadoras de transporte para coibir fraudes, é possível observar que os que tratam do uso de TRFs em transportes estão na tênue fronteira entre a segurança pública e o transporte público. Quero dizer que eles são implementados com o objetivo de diminuir fraudes, ou seja, proteger empresas de transporte, mas muitas vezes argumenta-se que protegerão também passageiros. Nem sempre fica explicado de que maneira a proteção de passageiros ocorrerá. Na relação entre identificação e reconhecimento facial, o projeto de lei 1.877/2003 “dá nova redação ao art. 3º, letra “e” da Lei nº 7.116 de 09 de agosto de 1983” (Brasil, 2003). O projeto de Colbert Martins (PPS/BA) pretende modificar a carteira de identidade feita no Brasil para incluir dados biométricos. Possui o mesmo objetivo do PL 5.034/2005, do deputado Carlos Nades (PL/RJ), ou seja, incluir “dados na carteira de identidade” e dar outras providências (Brasil, 2005).

No mesmo caminho, há o projeto de lei 7.902/2010, do deputado Lira Maia (DEM/PA), que objetiva modificar a Lei 9.454/1997, “que institui o número único de Registro de Identidade Civil” ao tornar “obrigatória a identificação biométrica para a emissão de documento de identidade” (Brasil, 2010). O PL 7.902/2010 foi apensado ao PL 5.034/2005. O projeto de lei 7.461/2014, sob autoria de Nelson Marchesan Junior (PSDB/RS), também tem o objetivo de alterar a Lei 9.594/1997 e “vincular o Cadastro Nacional de Registro de Identificação Civil, ao sistema biométrico, previsto na Lei nº 12.034, de 29 de setembro de 2009”, e dar outras providências (Brasil, 2014b).

O projeto de lei 1.786/2020, de Júnior Ferrari (PSD/PA), objetiva alterar a Lei nº 13.982/2010, “para possibilitar a substituição do Cadastro de Pessoa Física – CPF por outro documento oficial ou por outras formas de identificação dos beneficiários do auxílio emergencial” (Brasil, 2020a). Relacionado ao auxílio emergencial oferecido pelo Governo Federal durante a pandemia de Covid-19, o PL propunha ampliar as formas de acesso ao direito, ao utilizar outras formas de identificação, como as biométricas e o cadastro eleitoral. O legislador argumentou que não se podia excluir pessoas por meio do uso do CPF. Contudo, ele não disse exatamente que base de dados seria utilizada para se conferir as informações

biométricas e como o banco de dados do cadastro eleitoral diferiria do usado pelo CPF, na medida em que um cidadão precisa do CPF para fazer o título de eleitor.

Do mesmo modo que aconteceu no PL que objetivava a instalação de câmeras no transporte público, os projetos de leis com o objetivo de alterar as carteiras de identidade são gradualmente apensados uns aos outros até que um deles se relacione ao reconhecimento facial, de modo a criar uma base de dados com a face dos indivíduos no Brasil.

O projeto de lei 3.372/2004 objetiva dispor “sobre mecanismos de segurança para acesso aos sistemas e bancos de dados da Administração Pública Federal”. Já arquivado, o texto da matéria indica que os mecanismos de credenciamento de servidores ocorrerão por meio de “características biométricas (impressão digital, reconhecimento facial ou da íris) e os bancos de dados deverão ser dotados de sistema de LOG” (Brasil, 2004). O PL foi proposto por Eduardo Paes, na época no PSDB/RJ. Atualmente prefeito do Rio de Janeiro, o autor é um conhecido entusiasta das tecnologias para gestão, como pode ser visto na conferência TED, realizada em 2012[12]. O Art. 3º autorizava o Poder Executivo

> a firmar convênios com universidades, entidades estatais, inclusive com o Supremo Tribunal Federal, para o intercâmbio administrativo de aprimoramento tecnológico dos recursos de segurança no acesso e administração de bancos de dados sigilosos ou restritos (Brasil, 2004).

O PL foi arquivado com o fim da legislatura, de acordo com o Artigo 105 do Regimento Interno da Câmara dos Deputados. Se tivesse permanecido em tramitação, é possível que tivesse sido visto com cada vez mais entusiasmo. Afirmo-o com base no gráfico que demonstra um crescimento das propostas que envolvem as características biométricas dos cidadãos.

O projeto de lei 1.230/2007

> estabelece que o credenciamento e autenticação de usuário para proceder alterações de informações em sistemas e bancos de dados nos setores de arrecadação de tributos, pagamentos diversos e de pessoal na Administração Pública Federal será dotado de

[12]Os quatro mandamentos das cidades, Eduardo Paes: Disponível em https://www.ted.com/talks/eduardo_paes_the_4_commandments_of_cities?language=pt acesso em 17 dezembro de 2023.

> características biométricas (impressão digital, reconhecimento facial ou íris) ou outro mecanismo tecnológico (Brasil, 2007, p. 1).

Sob autoria de Eduardo Gomes (PSDB/TO), o projeto é igual ao apresentado por Eduardo Paes, arquivado no fim da legislatura. Seu fim foi o mesmo, ao ser arquivado em 2008 por parecer contrário da Comissão de Trabalho, de Administração e Serviço Público.

O projeto de decreto legislativo 674/2019, dos Parlamentares da então Bancada do PSOL, Ivan Valente (SP), Fernanda Melchionna (RS), Luiza Erundina (SP), Sâmia Bomfim (SP), Glauber Braga (RJ) e Marcelo Freixo - PSOL/RJ objetiva sustar “os efeitos do Decreto 10.047, de 09 de outubro de 2019, que dispõe sobre a governança do Cadastro Nacional de Informações Sociais” que “institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais” (Brasil, 2019a, p. 1).

O PL tem um perfil mais protecionista, diante dos dados dos cidadãos, e argumenta que a existência de uma base de dados, como o Cadastro Base do Cidadão. Esta base seria composta por informações como “nome, inscrição no CPF, filiação, sexo, data de nascimento e naturalidade. A norma prevê a possibilidade da inclusão de qualquer dado das bases temáticas” (Brasil, 2019a, p. 1), o que institucionalizaria um cadastro unificado.

> Os dados cadastrais seriam compostos por, entre outras coisas, atributos “biográficos” (“dados de pessoa natural relativos aos fatos da sua vida, tais como nome civil ou social, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço e vínculos empregatícios) e “biométricos” (características biológicas e comportamentais mensuráveis da pessoa natural que podem ser coletadas para reconhecimento automatizado, tais como a palma da mão, as digitais dos dedos, a retina ou a íris dos olhos, o formato da face, a voz e a maneira de andar). Ambos incluem informações “sensíveis”, de cunho estritamente privado, como religião, orientação sexual, filiação a sindicatos, movimentos sociais, que podem ser utilizadas para controle político típico de regimes totalitários (Brasil, 2019a).

Segundo os deputados,

> Uma base de dados dessa dimensão pode se tornar um instrumento perigoso sob a administração de uma gestão de viés autoritário ou que busca vigiar ou reprimir opositores. Para além disso, a centralização também traz problemas no tocante à segurança das

> informações dos cidadãos, que poderão ter verdadeiros dossiês sobre a sua vida privada. Diversos casos de vazamento por órgãos públicos evidenciam as limitações do armazenamento de informações importantes dos indivíduos. Uma base centralizada amplia os focos de vulnerabilidade para invasões e outros incidentes deste tipo (Brasil, 2019a).

Conforme poderá ser visto, o PSOL tem uma atuação mais defensiva quanto ao uso de tecnologias que envolvam dados biométricos. O partido também foi o que mais propôs leis pelo banimento total ou parcial de TRFs, o que será melhor abordado ao longo deste capítulo.

Outro projeto de decreto legislativo é o 675/2019, também de autoria dos parlamentares do PSOL acima citados. Seu objetivo é sustar os efeitos do Decreto 10.046/2019 “que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados” (Brasil, 2019b). O teor do projeto é o mesmo ao do projeto 674/2019, o que pode demonstrar que os deputados tentaram atuar de diversos modos contra os efeitos dos Decretos 10.046/2019 e 10.047/2019. Ainda assim, esses projetos não são exatamente contrários à utilização de TRFs e sim à criação das bases de dados que poderão alimentar a Tecnologia de Reconhecimento Facial.

O PL 3.839/2023, da Deputada do PSOL mineiro, Célia Xakriabá, objetiva autorizar “o uso de fotografia de identificação com elemento de indumentária tradicional que exprime a identidade da pessoa” e alterar “as leis nº 7.116, de 29 de agosto de 1983, nº 9.503, de 23 de setembro de 1997 (Código de Trânsito Brasileiro) e o Decreto-Lei nº 5.452, de 1º de maio de 1943 (Consolidação das Leis do Trabalho)” (Brasil, 2023g). No PL, a indumentária tradicional poderá ser utilizada “desde que esses elementos não impeçam o reconhecimento da fisionomia da pessoa”.

Na justificativa, a expressão fisionomia da pessoa é tratada como sinônimo de reconhecimento facial. O problema, a meu ver, é que o termo reconhecimento facial já está carregado dos significados que envolvem o reconhecimento facial feito por modelos algorítmicos. Usá-lo de maneira pouco cuidadosa acaba por deixar aberturas em aspectos sensíveis, acredito. Além disso, se TRFs são notadamente conhecidas pelos erros na identificação de minorias, é provável que fossem capazes de errar ainda mais com a adição de mais elementos da indumentária tradicional.

Além disso, o uso de indumentária tradicional adiciona mais um elemento a ser considerado em qualquer algoritmo de TRF, de modo a salvaguardar o direito das pessoas de autoidentificação e valorização de identidades.

O PL 4.073/2023, dos deputados Bebeto (PP/RJ) e Gutemberg Reis (MDB/RJ), objetiva alterar “o art. 69 da Lei nº 8.212, de 24 de julho de 1991, que dispõe sobre os Planos de Benefícios da Previdência Social, para tratar da prova de vida do beneficiário do Instituto Nacional do Seguro Social” (Brasil, 2023h). De acordo com a proposta, o reconhecimento facial seria uma das possibilidades para a realização de prova de vida de segurados do INSS. Dessa maneira, creio não ser o pior cenário. Afinal, mesmo que TRFs sejam utilizadas, há outras maneiras de garantir também que segurados do INSS tenham acesso ao direito, fazendo com que permaneça acessível ou seja ampliado. A utilização de tecnologias para a prova de vida também facilitaria o cotidiano de pessoas com dificuldade de locomoção, seja por questões físicas ou de transporte. O problema maior seria se o reconhecimento facial fosse a única maneira de autenticação, fazendo com que pessoas que não fossem reconhecidas pelos *softwares* perdessem benefícios.

Em 2016, começam a surgir propostas que envolvem educação e controle biométrico, como pode ser visto com os projetos a seguir.

O projeto de lei de autoria de Marcelo Aguiar (DEM/SP), sob o número 4.413/2016, objetiva tornar “obrigatória a implantação de sistema de controle de frequência de alunos em escolas públicas – Frequência Digital Escolar”. Do mesmo ano é o projeto de lei 6.154/2016, de Ildon Marques, que

> institui a destinação de 2% do total dos recursos do Pré Sal destinados à Educação, nos termos da Lei nº 12.351, de 22 de setembro de 2010, para implantação de Sistema de Frequência Digital Escolar – controle de frequência de alunos em escolas públicas (Brasil, 2016a, p. 1).

Na justificativa do PL 4.413, o deputado Marcelo Aguiar indica que a iniciativa atenderá “a realidade das escolas públicas através da web, podendo ser acessado de qualquer lugar pela internet, em tempo real, sem a necessidade de que as escolas tenham que arcar com computadores e servidores de última geração” (Brasil, 2016a, p. 1). Como mágica, “assim que os portões do colégio são fechados, o sistema realiza o envio automático de e-mail e SMS (mensagem de texto) para o

celular dos pais ou responsáveis dos alunos que não compareceram na escola", garantindo "maior tranquilidade às famílias" (Brasil, 2016). A propósito, os mesmos trechos podem ser vistos no PL 6.154/2016.

A repetição de trechos, de justificativas e de PLs inteiros foi algo que observei com frequência nos documentos analisados neste trabalho, o que ficará demonstrado ao longo do texto.

O projeto de lei 1.921/2023 objetiva alterar a Lei 9.394/1996, que estabelece as diretrizes e bases da educação nacional. As mudanças são no sentido de "dispor sobre a instalação de detectores de metais, câmeras nos arredores das escolas; software de reconhecimento facial, instalação de internet 5g e iluminação em volta das ruas circunvizinhas" (Brasil, 2023c). De autoria do deputado Júnior Mano (PL/CE), o projeto se soma aos demais que visam alterar a LDB. Dessa vez, o objetivo é obrigar que instituições públicas e privadas de ensino instalem detectores de metais, câmeras de videovigilância, *software* de reconhecimento facial, internet 5G e iluminação. As despesas ficam sob responsabilidade da União e podem ser suplementadas com recursos do Fundo Nacional de Educação.

O PL 3.047/2023 objetiva alterar a Lei 9.394/1996 (Lei de Diretrizes e Bases da Educação Nacional) "para dispor sobre a instalação de software de reconhecimento facial nas instituições de nível superior" (Brasil, 2023e). Ficam obrigadas as instituições públicas e privadas a instalarem tecnologias de reconhecimento facial em suas instalações. Os softwares deverão respeitar a LGPD, com o objetivo de proteger os "direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada estudante" (Brasil, 2023e). Além disso,

> o presente projeto de lei prevê a implantação do reconhecimento facial nas instituições públicas e privadas do ensino superior, tendo como objetivo **coibir o acesso de pessoas estranhas à comunidade bem como monitorar o acesso e presença de estudantes. (**Brasil, 2023e, grifo nosso)

O projeto de lei 2.606/2023, de autoria do deputado Sargento Gonçalves, objetiva instituir "a identificação biométrica e ou facial para ingresso nas escolas da rede pública ou privada da educação básica de ensino, a submissão dos ingressantes à verificação por equipamentos detectores de metais," além de tornar obrigatória a "aquisição de equipamentos de detecção de metais, porta giratória com

detecção de metais e outros equipamentos” (Brasil, 2023k).

Primeiramente, no caso das instituições de ensino superior públicas, vale perguntar quem é a comunidade da qual fala o legislador, pois essas entidades são responsáveis – a partir do tripé ensino, pesquisa e extensão – por oferecerem diversos serviços à população como, por exemplo, hospitais públicos. Em segundo lugar, a ideia de que tecnologias de reconhecimento facial vão monitorar o acesso e a presença de estudantes remete aos estudos de Michel Foucault (1977) sobre o controle e a vigilância.

É importante destacar que muitas proposições sobre o reconhecimento facial nas escolas são de 2023, conforme pôde ser visto nas figuras anteriormente apresentadas, o que foi muito provavelmente motivado pela onda de medo de ataques a instituições de ensino, ocorrida na primeira metade daquele ano[13]. Isso teve reflexo tanto na ação de deputados federais quanto na dos estaduais, como poderá ser visto.

Há um conflito contínuo que opõe o político aos imperativos da administração e à necessidade de responder os assuntos cotidianos (Sadin, 2020), o que pode ser percebido nas matérias legislativas, no que se refere à quantidade de proposições do ano de 2023 com o objetivo de, supostamente, promover a segurança nas escolas por meio de tecnologias de reconhecimento facial. Aliás, a justificativa do PL 3.047/2023 apresenta o seguinte texto:

> No esteio dos fatos recentes de violência, levantamento do jornal Folha de São Paulo, de abril de 2023, aponta que foram propostos ao menos 102 projetos de lei nas Assembleias Legislativas dos 26 estados e na Câmara Legislativa do Distrito Federal nos últimos 90 dias, relacionados à segurança em unidades de ensino. Na Câmara dos Deputados também foram apresentados diversos Projetos com o mesmo teor. A maioria dos projetos, no entanto, são direcionados à educação básica, deixando uma lacuna no que se refere à educação superior. (Brasil, 2023e)

O PL 2.028/2023, sob autoria do deputado Adriano do Baldy (PP/GO), tem o objetivo de dispor “sobre o endurecimento da fiscalização e o cumprimento da faixa etária para jogos eletrônicos” (Brasil, 2023d). Nesse caso, tecnologias de

[13]As escolas brasileiras sofreram diversos ataques na primeira metade de 2023, conforme a reportagem da CNN Brasil. Disponível em https://www.cnnBrasil.com.br/nacional/Brasil-registra-9-ataques-em-escolas-neste-ano-e-atinge-patamar-recorde-relembre-casos/. Acesso em 18 dez 2023.

reconhecimento facial serão uma forma de verificação da idade dos compradores de jogos para fazer cumprir a faixa etária indicativa para cada tipo de *game*. O projeto também está inserido no contexto do aumento de ataques a escolas. Com frequência, a correlação entre jogos violentos e ataques executados por jovens aparece.

O projeto de lei 1.745/2019, de autoria de Luiz Philippe de Orleans e Bragança (PSL/[14]SP) objetiva alterar a Lei nº 12.527/2011, a "Lei de Acesso à Informação, para ampliar as hipóteses de acesso à dados públicos pelos administrados" (Brasil, 2019c). Ao alterar a LAI, o deputado pretende inserir, no seu Art. 3°, o seguinte texto

> VI - Vedação absoluta ao poder público da prática de classificação, listagem, ranqueamento ou estabelecimento de qualquer processo de posicionamento ou comparação de dados pessoais compilados de indivíduos, de grupos de indivíduos ou de dados comerciais, uns em relação aos outros, na escala ordinal (Brasil, 2019c).

Dentre as muitas mudanças na Lei de Acesso, o autor também está preocupado com práticas de classificação ou ranqueamento de cidadãos. A inquietação do legislador, ao justificar o projeto, está na implementação, no Brasil, de um sistema semelhante ao Crédito Social Chinês. Nesse sentido, segundo o texto, o legislador deve vedar antecipadamente violações de privacidade e a geração de um sistema de castas baseado em ranqueamento de pessoas. Nesse sentido, o projeto de um deputado de direita tem também um perfil protecionista dos direitos de privacidade e intimidade.

O projeto de lei 2.537/2019, de autoria do deputado Juninho do Pneu (DEM/RJ), tem como objetivo "obrigar o aviso sobre o reconhecimento facial em estabelecimentos comerciais". Assim como acontece com as câmeras de vigilância, os estabelecimentos comerciais ficam obrigados a avisarem aos clientes da utilização de ferramentas de reconhecimento facial. O projeto

> visa alertar aos consumidores da utilização do programa de reconhecimento facial realizado pelos estabelecimentos comerciais que usam a imagem de consumidores para fazer identificação de consumo e de situação restritiva de crédito por órgãos específicos (Brasil, 2019d).

[14]O PSL fundiu-se com o Democratas para fundar o União Brasil, em 2022. Portanto, toda a legislação proposta por políticos da legenda é anterior ao ano de 2022.

A justificativa demonstra preocupação com a análise de sentimentos que também pode ser adotada em sistemas de reconhecimento facial. Segundo o texto “mais do que apenas reconhecimento de pessoas, o sistema também identifica emoções e reações por meio das expressões monitoradas. O que fere os direitos humanos fundamentais, como privacidade e liberdade de expressão” (Brasil, 2019d). Acho curioso que o projeto indique que a análise de sentimentos fere direitos fundamentais, mas objetive apenas “regular” o uso deste tipo de tecnologia com um aviso. Portanto, o cidadão pode ter seu direito violado desde que dê seu consentimento, ao entrar em um determinado estabelecimento comercial. E aqui o legislador manifesta a sua preocupação com não querer “calar a tecnologia e os avanços cada vez mais rápidos da sociedade” (Brasil, 2019d).

O projeto de lei 4.612/2019, de autoria de Bibo Nunes (PSL/RS), objetiva dispor “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, 2019e). Este PL é o primeiro com o objetivo de regulamentar o desenvolvimento de ferramentas de identificação biométricas e preditivas ou analíticas comportamentais. Aplica-se a “todas as atividades da cadeia de suprimento das tecnologias”, o que inclui “concepção de produto ou serviço, origem e uso de dados, dispositivos e aplicações desenvolvidos para uso da tecnologia” (Brasil, 2019e). Dentre os artigos da lei, consta que

> Art. 2º Esta Lei tem como fundamento o avanço das tecnologias digitais como fator estratégico para o desenvolvimento econômico e social sustentável e inclusivo, além dos seguintes pressupostos:
> I. uso da tecnologia para fins benéficos e dentro de padrões razoáveis e aceitáveis, proibido o tratamento discriminatório;
> II. proibição do uso das tecnologias de que trata o art. 1º para estabelecimento de regime de contínua vigilância massiva;
> III. incentivo à inovação e à difusão de novas tecnologias em prol dos direitos e garantias dos cidadãos;
> [...]
>
> IX. definição multissetorial de boas práticas e padrões técnicos, éticos, de segurança garantidores dos direitos dos cidadãos, especialmente quando as consequências do uso da tecnologia de que trata esta Lei no longo prazo forem desconhecidas (Brasil, 2019e).

O PL possui um capítulo inteiro dedicado a regulamentar o uso e a aplicação de TRFs. Nele, o legislador argumenta que “as informações utilizadas para o desenvolvimento, aplicação e uso de tecnologias de reconhecimento facial e emocional são dados pessoais sensíveis”. Por isso, estão submetidas ao tratamento baseado na Lei Geral de Proteção de Dados. Dentro deste capítulo do projeto de lei, na Seção I, podem ser encontrados os direitos e obrigações dos desenvolvedores e usuários de TRFs. Os direitos são:

> Art. 5º São garantias dos agentes que desenvolvem, aplicam ou utilizam as tecnologias de que trata esta Lei, sem prejuízo de outros previstos pela Constituição e demais legislação:
> I. **tratamento diferenciado** a microempresas e empresas de pequeno porte; a novas iniciativas empresariais; bem como à pesquisa voltada para a inovação; e
> II. incentivo a bens e serviços com tecnologia desenvolvida no País.
> Parágrafo único. O **tratamento diferenciado de que trata do inciso I inclui a flexibilização temporária de normas regulatórias voltadas para a abertura e funcionamento das empresas, assim como para o desenvolvimento tecnológico (**Brasil, 2019e, grifo nosso).

Observa-se que, em nome do suposto progresso da tecnologia, as normas regulatórias podem ser flexíveis. Na mesma seção, podem ser encontrados os deveres.

> Art. 6º São obrigações dos agentes que desenvolvem, aplicam ou utilizam tecnologias de que trata esta Lei:
> I. garantia de mecanismos que permitam a **supervisão e controle humano** nos casos definidos em regulamentação;
> II. **transparência quanto aos parâmetros para a tomada de decisão automatizada, observados os segredos comercial e industrial;**
> III. manutenção de estruturas técnica e administrativa aptas a garantir as exigências desta Lei; da Lei nº 13.709, de 14 de agosto de 2018; da regulamentação definida pela Autoridade de que trata o art. 4º e demais normas aplicáveis;
> IV. **uso e aplicação da tecnologia mediante padrões mínimos de desempenho de precisão,** a serem definidos pela Autoridade de que trata o art. 4º; e
> V. **garantia de processo simplificado e sumário aos cidadãos para a defesa de eventuais direitos afetados e questionamentos de decisões tomadas com base em quaisquer das tecnologias de que trata esta Lei.**
> §1º **Os segredos comercial e industrial não poderão servir de justificativa para a violação de direitos, padrões éticos e demais normas definidas nesta Lei e sua regulamentação.**

> §2º O agente que não se enquadrar nas disposições do §1º deverá dispor de outros mecanismos de transparência que viabilizem a supervisão dos critérios utilizados para a tomada de decisões que afetem a esfera de direitos de outrem (Brasil, 2019e, grifo nosso).

Dentre as obrigações, consta a garantia da supervisão e controle humano, da transparência, padrões mínimos de desempenho de precisão, processo simplificado de defesa e questionamento por parte dos afetados. Além disso, aponta que os segredos comerciais e industriais não poderão ser utilizados como justificativas para violações de direitos. É interessante que o legislador trate de tal aspecto, pois esses segredos têm servido para justificar a falta de transparência das decisões algorítmicas, por parte de empresas. Inclusive, é do que trata Frank Pasquale (2015), ao discutir a caixa-preta dos dados. O autor afirma que muitas vezes segredos de propriedade industrial são utilizados para esconder ações governamentais e institucionais, enquanto a vida do cidadão é cada vez mais um "livro aberto" (Pasquale, 2015).

Assim como o PL 2.537/2019, anteriormente apresentado, o PL 4.612/2019 indica que ficam os agentes que utilizem TRFs obrigados a sinalizarem seu uso ou aplicação, de modo claro e visível (Brasil, 2019e). O projeto tenta proteger cidadãos da vigilância massiva, garantir os direitos humanos e a defesa dos consumidos, além do respeito à privacidade, à autodeterminação informativa e à liberdade de expressão, de informação, de comunicação e de opinião (Brasil, 2019e). O PL tenta ainda regular o uso compartilhado dos dados, vedando, inclusive, "a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores, com objetivo de obter vantagem econômica" (Brasil, 2019e).

Observa-se que o projeto tenta equilibrar os direitos das pessoas afetadas e os interesses dos demais envolvidos, como os comerciais, dos desenvolvedores, e os de controle, por parte do Estado. A proposta também indica a criação do Banco Nacional de Reconhecimento Facial e Emocional, a ser controlado pelo Poder Executivo Federal, embora pareça ter boas intenções, conforme pode ser visto na sua justificativa:

> Assim, 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, 2019e).

Contudo, quem pode garantir que os interesses do Estado serão sempre os da população e que um Banco Nacional de Reconhecimento Facial e Emocional não seja utilizado para perseguir opositores, conforme pode ser visto em diversos casos que envolvem ferramentas de vigilância e que têm sido alvo da preocupação de diversos autores? (Véliz, 2021; Lyon, 2013; Pasquale, 2015).

A autoridade de que trata o projeto é a Autoridade Nacional de Proteção de Dados, estabelecida pela Lei 13.079, a LGPD. O projeto de lei 1.969/2021, de autoria do deputado Gustavo Fruet (PDT/PR), “dispõe sobre os princípios, direitos e obrigações na utilização de sistemas de inteligência artificial”, A proposta define o dado biométrico como o “dado pessoal resultante de técnicas específicas de tratamento relacionadas a características físicas, psicológicas ou comportamentais da pessoa natural, que permitem a identificação dessa pessoa” (Brasil, 2021a). Segundo o PL, os sistemas de IA devem observar princípios, como responsabilidade e prestação de contas; explicabilidade; auditabilidade; precisão; e equidade.

> (i) responsabilidade e prestação de contas, que aloca o dever de adoção de medidas eficazes e capazes de cumprir as normas atinentes ao mercado de IA; (ii) explicabilidade, que procura evitar a opacidade do provedor em oferecer explicações e justificar os resultados advindos da decisão algorítmica do sistema de IA; (iii) auditabilidade, que torna obrigatória a validação ou averiguação dos passos tomados pelo sistema de IA para alcançar os resultados pretendidos, inclusive para fins de fiscalização pelo Poder Público; (iv) precisão, de modo a evitar-se o falseamento de informações inseridas ou conclusões resultantes de sistemas de IA; e (v) equidade, a fim de se proibir tratamentos com vieses discriminatórios (Brasil, 2021a).

O projeto veda que IAs:

> I – empreguem técnicas subliminares que distorçam o comportamento de uma pessoa natural, de maneira a causar nelas ou em terceiros danos físicos ou psicológicos;
> II - explorem as vulnerabilidades de grupos específicos de pessoas, seja em função da idade ou da condição física ou mental; III – sejam usados, por parte do Poder Público, para aferir ou classificar a confiabilidade de pessoa natural baseando-se em seu comportamento social ou em práticas preditivas e que resultem em sistema de escore social de recompensas e punições;
> IV – utilizem sistemas de identificação remota por meio de dados biométricos em tempo real e em espaços públicos para fins de segurança pública e atividades de investigação e repressão de infrações penais, a não ser:

> a) que vítimas de crimes em potencial sejam o alvo do sistema de IA, incluindo crianças perdidas;
> b) para a prevenção de uma ameaça específica, substancial e iminente para a vida ou segurança de pessoas naturais;
> c) para a prevenção de ações de terrorismo;
> d) para a identificação, localização e persecução de suspeito de ofensa criminal punível com, no mínimo, pena de reclusão (Brasil, 2021a).

Primeiramente, o inciso III de vedação parece se referir ao Crédito Social Chinês, o que vai ao encontro da proposição 1.745/2019, anteriormente apresentada. O inciso IV e suas alíneas apontam que sistemas que sistemas de identificação remota poderão ser utilizados em casos relacionados à segurança pública. Isso coloca tais sistemas em um limbo em que tudo passa a ser mais permitido, pois como será visto, a segurança é também uma das exceções da Lei Geral de Proteção de Dados. O próprio legislador reconhece o problema e afirma que

> O objetivo é impedir que, sob o pretexto de garantir a segurança pública à população, o Estado simplesmente promova a disseminação de câmeras de reconhecimento facial ou de sistemas que tratem dados biométricos em espaços públicos, de forma abusiva. Muitas vezes o Poder Público pode praticar monitoramento remoto para causas menores ou insignificantes, que não justificam a devassidão que essas tecnologias invasivas podem causar na vida do cidadão (Brasil, 2021a).

Para proteger cidadãos, o PL 1.969/2021 propunha a criação, por parte da União, de uma lista de sistemas de IA de alto risco e aplicação de multa aos provedores de IA, em caso de infração da lei. A justificativa da lei aponta que algumas Inteligências Artificiais, tais como o reconhecimento facial e o policiamento preditivo, atentam contra os direitos humanos. O legislador também reconhece que se baseou no regulamento europeu[15] para propor a lei.

Proposto pelo deputado Guiga Peixoto (PSC/SP), o projeto de lei 2.392/2022 objetiva dispor “sobre o uso de tecnologias de reconhecimento facial nos setores público e privado” (Brasil, 2022b). Segundo o PL, o tratamento de dados pessoais provenientes de TRFs deve ser feito de acordo com a LGPD e fica vedado o repasse

[15]O Parlamento Europeu tem debatido questões sobre inteligência artificial e tentado avançar na legislação sobre o tema. Disponível em: https://www.europarl.europa.eu/news/pt/headlines/society/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial. Acesso em: 23 dez 2023.

das informações a terceiros, excetuando-se o “poder público para casos exclusivos de segurança pública, defesa nacional e atividades de investigação e repressão de infrações penais”, além de que “não poderão ser utilizados como forma de identificação sem realização prévia de relatório de impacto à privacidade” (Brasil, 2022b).

Outro ponto que merece destaque no PL 2.392/2022 é a indicação de que TRFs não poderão ser utilizadas como único meio de identificação para a utilização de serviços públicos, ficando obrigatório o oferecimento imediato de modo alternativo de reconhecimento, em caso de não reconhecimento de um indivíduo. As instituições públicas ou privadas que utilizarem TRFs deverão elaborar anualmente relatório de acesso público em que conste a avaliação da tecnologia, as reclamações dos usuários, as soluções dadas para cada caso e os processos administrativos e judiciais em que os responsáveis pela TRF tenham sido réus. O PL 2.392/2022 demonstra preocupação com o “uso indiscriminado dessas tecnologias”, pois “pode incorrer em abusos do ponto de vista de consumidores, ou ainda mais graves, do ponto de vista dos cidadãos” (Brasil, 2022b). O projeto também se preocupa com comercialização dos dados, proibindo-a como uma maneira de dar maior proteção ao cidadão e promover a restrição da circulação de informações sensíveis.

Os projetos de regulamentação atuam dentro da lógica da sociedade da caixa-preta em que vivemos, movida pela crença de que as informações são úteis apenas na medida de sua exclusividade. Assim, Frank Pasquale (2015) afirma que é possível que a sociedade não consiga mais impedir a coleta de informações, mas ainda é possível que possa regular seus usos, o que projetos de lei como o PL 2.392/2022, o PL 1.969/2021 e o PL 4.612/2019 tentam fazer.

O projeto de lei 4.827/2019, de autoria de Carmen Zanotto (Cidadania/SC), objetiva alterar “a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), para dispor sobre o uso de dispositivo móvel de segurança para conferir maior efetividade às medidas protetivas de urgência” (Brasil, 2019f). O projeto prevê que o agressor, nos termos da Lei Maria da Penha, instale aplicativo em seu telefone celular que não poderá ser desligado. Dentre diversas funções, deve servir para conferir sua identidade “através de reconhecimento facial com selfies de segurança em horários alternados várias vezes por dia” como parte da medida protetiva, pois

> um aplicativo, que possua ampla capacidade de gerir uma rede preventiva de ações visando a proteção de mulheres vítimas de violência, certamente contribuirá para resultados positivos no combate a esses crimes (Brasil, 2019f).

De autoria da mesma deputada, o projeto de lei 4.828/2019

> dispõe sobre a obrigatoriedade de empresas fabricantes de aparelhos celulares introduzirem aplicativo permanente nos aparelhos celulares que saem de fábrica e nos antigos para acionar a polícia em caso de violência contra a mulher" (Brasil, 2019g).

No caso do segundo projeto, a legisladora pretende obrigar fabricantes a instalarem aplicativos que permitam o acionamento policial em caso de violência contra mulher. Os aplicativos teriam a função de reconhecimento facial, por meio de selfies dos agressores, anteriormente citadas no projeto 4827/2019. Esse é um caso em que se deposita nas ferramentas tecnológicas a resolução de problemas sociais absolutamente complexos, como a violência de gênero.

O projeto de lei 6.163/2019, do Poder Executivo, "institui o Plano Regional de Desenvolvimento do Nordeste para o período de 2020-2023" (Brasil, 2019h). No Plano, consta como uma das ações indicativas a implementação do Sistema ABIS para reconhecimento facial. O ABIS é uma ferramenta utilizada pela Polícia Federal que armazena dados biométricos (Augusto, 2021).

Sob autoria de Capitão Alberto Neto (Republicanos/AM), o projeto de lei 3.307/2021 objetiva alterar "a Lei nº 10.703, de 18 de julho de 2003, que dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos, para tornar obrigatório o uso de sistema de verificação das informações dos usuários" (Brasil, 2021b). O PL objetiva reduzir golpes que envolvem linhas telefônicas, por meio da digitalização de documentos de identificação e de tecnologias de reconhecimento facial.

Na segurança pública, o projeto de lei complementar 245/2020 objetiva alterar a redação do art. 3º da Lei Complementar nº 79/1994, "que cria o Fundo Penitenciário Nacional – FUNPEN, e do art. 64 da Lei" nº 7.210/1984, "que institui a Lei de Execução Penal – LEP" (Brasil, 2020d). O PDL, de autoria da Policial Katia Sastre (PL/SP), tem como objetivo permitir a utilização dos recursos do FUNPEN na instalação de equipamentos de videomonitoramento nas imediações de

estabelecimentos prisionais. Nesse sentido, municípios com estabelecimentos prisionais teriam mais verba para investir em videovigilância e câmeras integradas com ferramentas de reconhecimento facial, usando recursos do Fundo Penitenciário Nacional.

O PL 3.714/2021, de autoria de Julio Lopes (PP/RJ), pretende dispor “sobre o reconhecimento facial em todas as fases da persecução penal” (Brasil, 2021c). Este projeto não trata exatamente das tecnologias de reconhecimento facial, mas do reconhecimento fotográfico. Esse tipo de reconhecimento também tem se demonstrado problemático, conforme pode ser visto nos trabalhos da Defensoria Pública (O Reconhecimento..., 2022) e na matéria da Agência Brasil (Tokarnia, 2022). Ainda assim, o projeto não visa proibir tal prática, mas regulamentá-la. A mistura dos dois temas é bastante comum. Isso decorre também do fato de que há uma preocupação de que TRFs sejam contaminadas pelas práticas ruins que envolvem o reconhecimento fotográfico.

O projeto de lei 1.756/2022, de José Nelto (PP/GO), “dispõe sobre a obrigatoriedade de instalação de câmeras para reconhecimento facial em hospitais públicos” com capacidade para “coletar os padrões de face, de íris e de voz” (Brasil, 2022a). Segundo a justificativa do PL, a necessidade de instalação de câmeras com reconhecimento facial justifica-se pela crise na segurança pública e estes dispositivos poderiam identificar foragidos e criminosos que se utilizem de estabelecimentos públicos de saúde. Novamente, a apresentação de soluções simples para problemas complexos.

O projeto de lei 572/2021, do deputado Igor Kannário (DEM/BA), “altera a Lei nº 13.812, de 16 de março de 2019 e cria o Banco Nacional de Dados de Reconhecimento Facial e Digital” (Brasil, 2021d). Esta base de dados seria criada com o objetivo “de auxiliar na prevenção e localização de crianças e adolescentes desaparecidos” (Brasil, 2021d) e pretende criar uma base com o rosto de milhares de crianças e jovens brasileiros. Os projetos de lei que envolvem bases de dados de crianças e adolescentes estão bastante presentes nas casas legislativas estaduais, contudo esse é o primeiro, em nível estadual, nesse sentido.

O projeto de lei 3.069/2022 objetiva dispor “sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública” (Brasil, 2022d) e dar outras providências, sendo de autoria do deputado Subtenente

Gonzaga, do PSD de Minas Gerais. Segundo a proposta, o reconhecimento facial deve ser utilizado em investigações criminais e na busca de pessoas desaparecidas. As forças policiais poderão utilizar de TRFs instaladas em locais públicos ou oriundas de terceiros, ficando necessária a fixação de placas informativas sobre o uso de TRF.

A lei acrescenta que “nenhuma ação ou diligência policial de restrição da liberdade de ir e vir de qualquer cidadão poderá ser efetuada a partir do RF sem a confirmação de Revisor e/ou Perito Papiloscopista especialista em Identificação Facial” (Brasil, 2022d). Na justificativa da lei consta que ela foi redigida por um papiloscopista policial da PCDF. O legislador/papiloscopista policial menciona que, “embora saibamos que o seu uso foi afastado em alguns países, entendemos que essas restrições decorrem do seu uso equivocado e do desconhecimento de alguns para com a tecnologia de reconhecimento facial”. O problema seria, então, da falta de conhecimento a respeito do tema e não oriundo dos diversos casos de falsos positivos e de falsos negativos. Portanto, para resolver o problema do desconhecimento, a justificativa passa a explicar o funcionamento de TRFs. Como solução para os erros da tecnologia, propõe-se

> que sistemas de reconhecimento facial aplicados a programas de segurança pública sejam sempre supervisionados por operadores humanos treinados em análise facial ou que operem conforme protocolos multibiométricos, como os Peritos Papiloscopistas lotados nos Institutos de Identificação (Brasil, 2022d).

Esse perito deve ter algumas características como

> aptidão para identificar faces, boa memória fotográfica, além de capacitação específica em reconhecimento facial. Ademais, a literatura internacional recomenda treinamentos periódicos a fim de avaliar a capacidade do operador para identificar corretamente uma face e melhorar suas habilidades para operar sistemas biométricos faciais (Brasil, 2022).

O perito atuaria como o revisor das decisões automatizadas. Esse é um critério bastante comum em legislações que envolvem a regulação de IAs e tem o objetivo de reduzir erros. Contudo, esse perfil de perito (alguém com aptidão para identificar faces e boa memória fotográfica) parece caminhar para o lado oposto ao que se preconiza com a utilização de ferramentas automatizadas, ficando a decisão na mão de alguém cujas características pessoais e sagacidade podem se sobrepor

aos procedimentos. Afirma-se ainda que “o objeto da lei é técnico, inovador e complexo”, recorrendo ao recurso da tecnologia como algo que, por ser técnico, é automaticamente bom.

O projeto de lei 807/2022, da deputada Maria do Rosário (PT/RS) tem como objetivo estabelecer “medidas de prevenção e combate ao trabalho infantil em empresas de aplicativos de entregas ou transporte” (Brasil, 2022c, p. 1), além de dar outras providências. Para prevenir e combater o trabalho infantil, ficam as empresas de aplicativos obrigadas a exigir cadastro biométrico ou identificação facial e a promover a checagem periódica. Nesse sentido, a checagem periódica, por meio do reconhecimento facial, funcionaria como uma maneira de coibir o trabalho infantil.

O projeto de lei 243/2023 é de autoria do deputado Tenente Coronel Zucco (Republicanos/RS), o mesmo cujo PL foi apropriado pelo Executivo gaúcho e aprovado como lei. Ele será também discutido na seção sobre a legislação estadual. O PL “dispõe sobre o emprego de tecnologia de reconhecimento facial de crianças e adolescentes desaparecidos” (Brasil, 2023a, p. 1) que responsabilizará o Poder Executivo pela instalação e operação de sistemas com emprego de reconhecimento facial para buscar crianças e adolescentes desaparecidos.

O projeto prevê a possibilidade de integração entre os entes da federação, a revisão por agente público antes das ações decorrentes de identificação positiva, o tratamento segundo a LGPD e a manutenção das imagens por prazo indeterminado ou até a localização da pessoa desaparecida. Justifica-se, ao apresentar dados sobre o problema do desaparecimento de crianças e adolescentes, e alegar que “um sistema de reconhecimento facial, **indubitavelmente,** será de grande valia aos órgãos de segurança pública na busca das crianças e adolescentes desaparecidos”, pois aumentará “de forma considerável a possibilidade de suas localizações e resgate” (Brasil, 2023a, grifo nosso).

A proposta cita ainda que legislação de mesma natureza foi aprovada no Rio Grande do Sul, conforme poderá ser visto na próxima seção, e afirma estar relacionado com o Decreto no 10.622, de 9 de fevereiro de 2021, que objetiva designar “a autoridade central federal de que trata a Lei nº 13.812, de 16 de março de 2019”, e instituir “o Comitê Gestor da Política Nacional de Busca de Pessoas Desaparecidas e dispõe sobre a Política Nacional de Busca de Pessoas Desaparecidas e o Cadastro Nacional de Pessoas Desaparecidas” (Brasil, 2021).

Acrescento aqui dois comentários. O primeiro é que, ao que parece, os legisladores não costumam apresentar dados efetivos sobre o modo como determinadas políticas realmente possuem resultado. Com base em que o legislador afirma que “indubitavelmente” TRFs auxiliam na busca de crianças e desaparecidos? É possível que auxiliem em algumas situações, mas acho que carece de pesquisa para tal afirmativa. O outro ponto é a relação com o Decreto 10.622/2021 que não apresenta a expressão reconhecimento facial em parte alguma. A única correlação envolve a criação do Cadastro Nacional de Pessoas Desaparecidas com bancos de informações públicas (sigilosas e ostensivas) que envolvem também informações biométricas.

O projeto de lei 4.179/2023 tem como objetivo a disposição “sobre a confirmação facial no comércio de bens e serviços pela internet” (Brasil, 2023f). A partir do dia 01 de janeiro de 2024, todas as vendas de bens e serviços realizadas pela internet passariam a exigir a confirmação facial para coibir fraudes em compras. A confirmação facial é “o procedimento de verificação da identidade do cliente por meio de leitura e comparação de características faciais, utilizando tecnologias seguras e reconhecidas” (Brasil, 2023f). As empresas não poderão armazenar os dados biométricos de compradores após a conclusão da transação. Apesar de não citar a LGPD diretamente, a justificativa do projeto diz estar

> em conformidade com a legislação de proteção de dados pessoais, garantindo que as informações biométricas dos clientes sejam tratadas de forma adequada e em conformidade com os princípios de privacidade e segurança (Brasil, 2023f).

Destaco o otimismo do legislador, ao submeter um projeto de lei em 25 de agosto de 2023 para que a lei esteja em vigor no dia 01 de janeiro de 2024. O trâmite das câmaras costuma ser bastante demorado para matérias não votadas em regime de urgência. Outro ponto que acredito que deva ser destacado é que o PL não pontua que tipo de crimes pretende coibir e de que maneira TRFs realmente ajudariam a impedir tais atos criminosos.

O PL 284/2023 objetiva dispor sobre regras de segurança para motoristas de aplicativos. O projeto pretende legislar sobre formas de assegurar motoristas de aplicativos física e economicamente. Tecnologias de reconhecimento facial serão utilizadas em corridas solicitadas e pagas em dinheiro para confirmar a identidade

do usuário que solicita o veículo. Não fica explícito porque as corridas em dinheiro precisariam dessa garantia e as corridas em outras formas de pagamento não.

O PL 2.745/2023, do deputado Rodrigo Gambale (Podemos/SP), objetiva Instituir que, em “todos os estádios de futebol, ginásios, arenas e demais locais de competições de esportes profissionais”, sejam “credenciados para realização de jogos/competições oficiais a implementação de tecnologia de câmeras e sistemas de videomonitoramento com reconhecimento facial ou não” (Brasil, 2023i). Apesar de obrigar a instalação de videomonitoramento, o PL propõe que

> O sistema de reconhecimento facial citado é facultativo, a sua implementação aos sistemas de videomonitoramento e câmeras será feita de acordo com a necessidade de cada estádio, ginásios, arenas e demais locais de competições de esportes profissionais, credenciados para realização de jogos/competições oficiais (Brasil, 2023i).

Segundo o PL, “fica proibido o uso indiscriminado da tecnologia de reconhecimento facial em locais onde o usuário deve ter a sua privacidade garantida, como banheiros, vestiários, salas de café e refeitórios”. O emprego de câmeras de vigilância fica obrigatório, mas a indicação da localização das câmeras não é obrigatória, se a finalidade for a segurança pública ou a segurança nacional. Segundo a justificativa do PL, casos de racismo e vandalismo teriam “uma resolução simples através da implantação das câmeras com a tecnologia de reconhecimento facial” e “é indubitável que a instalação de câmeras de reconhecimento facial nesses locais inibirá a ação criminosa, pois o delinquente saberá que será reconhecido, e, se, ainda assim, praticar o crime, as câmeras o identificarão”, além de facilitar “a localização de eventuais criminosos foragidos e de pessoas desaparecidas, prestando, desse modo, um serviço de incalculável importância para todo o País” (Brasil, 2023i). Ainda segundo a justificativa, a implementação de programas decodificadores garante que os dados serão protegidos, de acordo com a LGPD.

No mesmo caminho, o Governo Federal assinou com a Confederação Brasileira de Futebol o projeto Estádio Seguro que “prevê ações de combate ao racismo e à violência nos estádios Brasileiros”, por meio da “aplicação do uso de tecnologias que permitam identificar torcedores que tenham se envolvido em casos de violência e possam, porventura, causar problemas nas praças esportivas” e coibir a ação de cambistas (Magalhães, 2023). A ANPD (2023) publicou a Nota Técnica

175/2023 que discorre sobre a legalidade do reconhecimento facial em estabelecimentos esportivos.

Sob a lógica da regulamentação, o projeto de lei do deputado Rodrigo Gambale, sob o número 2.714/2023, objetiva regulamentar “o uso, instalação e implementação de tecnologia de reconhecimento facial em câmeras e sistemas de videomonitoramento”, e dar “outras providências” (Brasil, 2023j). Autorizadas em todo o território nacional, em vias públicas, repartições públicas e espaços públicos de uso comum, as TRFs em câmeras ficam restritas aos seguintes casos:

> I - Investigações criminais, atividades de segurança pública, utilização judicial e a localização de eventuais criminosos foragidos;
> II - Controle de acesso a locais de acesso restrito, desde que haja prévio consentimento dos indivíduos envolvidos;
> III - Prevenção e investigação de fraudes em instituições financeiras e de crédito, com autorização judicial.
> IV - Contribuição para investigações de pessoas desaparecidas que constem nos bancos de dados.
> V - Reconhecimento de pessoas em porte de armas de fogo ou armas brancas.
> VI - Prevenção de atentados através da inspeção de mochilas, malas e grandes objetos deixados em área de cobertura do monitoramento (Brasil, 2023j).

Segundo o PL 2.714/2023, fica proibido o repasse de dados oriundos de terceiros e a adoção de tecnologias de reconhecimento facial em equipamentos de videomonitoramento deve seguir a LGPD. Proíbe-se o uso indiscriminado de câmeras com TRFs em banheiros, vestiários, refeitórios e salas de café. Acredito que vale perguntar o que o legislador entende por uso indiscriminado. O aviso em locais públicos sobre a utilização de câmeras de vigilância é obrigatório, apesar de não ser necessário revelar a localização de câmeras cuja finalidade é a segurança pública ou a segurança nacional. Um canal para reclamações deve ser ofertado, indivíduos gravados terão o direito de acesso ao material e esses pedidos devem ser respondidos em um prazo de até 40 dias.

Ainda segundo o PL, os aspectos éticos do uso de dados biométricos devem ser avaliados, o que incluiria avaliações semestrais de impacto. Agentes de tratamento de dados que descumprirem a lei estão sujeitos à advertência; multa simples; multa diária; publicação da infração depois de apurada; ao bloqueio de dados pessoais referentes à infração; suspensão parcial do banco de dados por até

seis meses, prorrogável por igual período, até a regulação da atividade de tratamento de dados pessoais pelo controlador; suspensão da atividade de tratamento de dados pessoais por até seis meses, passível de prorrogação por igual período; e à proibição parcial ou total de atividades de tratamento de dados.

Os §2 e §3 do Art. 8º do PL 2.714/2023 preconizam que

> §2o - Após uma prisão, a polícia pode registrar uma foto do indivíduo e mantê-la sob custódia e armazená-la em sistemas locais, bem como em sua base de dados, contudo, indivíduos absolvidos ou cujas acusações foram retiradas podem requisitar a remoção de suas imagens do sistema. As imagens e informações coletada por câmeras não podem ser armazenadas por mais tempo do que seja necessário para sua finalidade.
> §3o - Todos os dados coletados serão eliminados automaticamente, quando não houver nenhum tipo de alerta do sistema. Na ocasião em que ocorre um alerta, os dados são deletados o mais rápido possível após a tomada de decisão, dentro de um limite máximo de 31 dias (Brasil, 2023j).

A justificativa do PL 2.714/2023 é igual à do PL 1.828/2023, do mesmo deputado, Rodrigo Gambale (Podemos/SP). O parlamentar submeteu alguns projetos que envolvem TRFs em 2023 cujos trechos são bastante parecidos ou iguais.

A partir da legislação federal anteriormente exposta, é possível observar alguns elementos:

Os primeiros projetos relacionados ao reconhecimento facial estão, em sua maioria, ligados ao seu uso para a identificação de indivíduos, apesar do PL sobre câmeras no transporte público. Depois, surgem os projetos sobre regulamentação de TRFs, seguidos pelos mais relacionados com a segurança pública. Os últimos projetos relacionam-se com a adoção de TRFs em estabelecimentos de ensino ou direcionados ao controle de crianças e adolescentes.

Destaca-se a atuação do deputado de São Paulo, Rodrigo Gambale (Podemos). Eleito por São Paulo, o parlamentar foi o que mais submeteu projetos sobre tecnologias de reconhecimento facial em nível federal, sendo três só no ano de 2023, além dos que apresentou durante a sua atuação como deputado estadual, o que poderá ser visto na próxima seção.

3.2.2 Nas Assembleias Legislativas

Nesta seção serão discutidos projetos, leis, indicações legislativas e pareceres em comissões dos estados e do Distrito Federal. Para fins da análise, foram considerados os projetos que se encontram em tramitação ou arquivados, pois acredito que são importantes para compreender o processo legislativo e as intenções dos legisladores, principalmente no que pode ser observado a partir das justificativas das propostas. O objetivo da análise não foi apresentar projeto a projeto exaustivamente, mas articulá-los e agrupá-los.

Foram analisados projetos entre 2012 e dezembro de 2023. Quando apresentados, foram considerados os partidos aos quais os deputados estavam filiados no momento da submissão do PL. Por isso, pode ser que deputados tenham mudado de legenda ou partidos tenham sido extintos.

Em Alagoas, em 2012, o Plano Plurianual, para o período de 2012 a 2015, direcionou R$22.456.000,00 para ações de implantação de videomonitoramento. A finalidade do programa consistia no desenvolvimento de ações de prevenção e "agilidade no combate à criminalidade através de tecnologia capaz de realizar reconhecimento facial, identificação de movimentos e placas de veículos, diminuindo o índice de criminalidade, utilizando uma moderna ferramenta tecnológica" (Alagoas, 2012). O que aparece na Lei 7.333/2012, que aprovou o Plano Plurianual, é mais uma vez a crença de que a implementação de "modernas ferramentas tecnológicas" será capaz de reduzir o índice de criminalidade.

Diversas proposições legislativas, dentre as quais incluem-se leis e indicações legislativas, versam sobre a instalação de equipamentos com capacidade de reconhecimento facial em estádios. Em geral, as proposições são direcionadas a estádios com capacidade acima de 10.000 pessoas. Em um documento de 2017, elaborado pela deputada estadual de Alagoas, Thaise Guedes, o reconhecimento biométrico aparece como um "sistema de baixo custo, benefício inestimável e associado ao registro de imagens de torcedores, pode facilitar a identificação de pessoas no caso de brigas e cenas de violência" (Alagoas, 2017).

Posteriormente, em 2023, os deputados de Alagoas indicaram ao governador do Estado, Paulo Suruagy do Amaral Dantas, a instalação de câmeras de monitoramento com reconhecimento facial nos dois principais estádios alagoanos, o

Estádio Rei Pelé, de propriedade do Governo Estadual, e o Estádio Municipal Coaracy da Mata Fonseca, na cidade de Arapiraca.

Em outros estados, como a Bahia, Rio de Janeiro e Santa Catarina, os projetos de lei objetivam obrigar a adoção de ferramentas de reconhecimento biométrico em estádios. Nesse caso, é preciso destacar uma diferença sútil que reside entre a autorização e a obrigatoriedade. Estes projetos baseiam-se no Estatuto do Torcedor, Lei Federal 10.671/2003, que permite a identificação biométrica de torcedores em estádios.

Nesse sentido, a utilização deste tipo de tecnologia objetiva constituir um banco de dados de pessoas com histórico de violência, dentro e no entorno dos estádios, e o cruzamento com outros bancos de dados que envolvem pessoas impedidas de comparecimento às suas proximidades; foragidos; pessoas com mandados de prisão; associados e torcedores membros de torcidas organizadas; e outros bancos de dados de segurança pública e do Poder Judiciário. Em 2023, o Governo Federal e a Confederação Brasileira de Futebol lançaram o projeto Estádio Seguro com o objetivo de coibir crimes no entorno e dentro dos estádios, por meio do uso de tecnologias de videomonitoramento (Magalhães, 2023), o que já foi anteriormente citado.

No Rio de Janeiro, duas pessoas foram detidas em 2019 por meio da utilização de câmeras com tecnologia de reconhecimento facial, no entorno e nos portões de acesso do Maracanã (PM..., 2019), demonstrando que a tecnologia tem sido utilizada há algum tempo em estádios. Aliás, o PL 318/2019, de autoria de Gil Viana (PSL), “dispõe sobre a obrigatoriedade da implantação de tecnologia de reconhecimento facial em toda a área de uso comum, incluindo eventos públicos e privados, com capacidade superior a 10.000 (dez mil) pessoas, no âmbito do Estado” (Rio de Janeiro, 2019g). O RJ vem utilizando TRFs em estádios sem que legislação específica tenha sido aprovada.

Em diversos estados, como no do Amazonas, o reconhecimento facial aparece nas câmaras legislativas como parte de programas que envolvem a identificação de indivíduos.

A partir das matérias legislativas, é possível observar que muitos projetos são arquivados porque invadem as atribuições do Executivo. Para solucionar tal questão, muitas vezes, deputados e deputadas utilizam-se de requerimentos e solicitações

aos chefes do Executivo. Essa seria uma forma de contornar as limitações que envolvem esses dois poderes. Inclusive, casas legislativas estaduais fazem indicações para o Executivo Municipal, como pode ser visto no Requerimento 494, de 2018 do estado do Amazonas (Amazonas, 2018).

Neste documento, o deputado Ricardo Nicolau requer que seja enviada indicação ao então prefeito de Manaus, Arthur Virgílio Neto, e ao superintendente municipal de transportes urbano, Franclide Corrêa Ribeiro, para solicitar a instalação de câmeras de reconhecimento facial nos ônibus municipais de Manaus, capital do estado, para combater assaltos nos coletivos. A justificativa do documento aponta que seriam tiradas 10 fotos em sequência, com uma distância de até um metro. Em seguida, ele explica de que maneira o reconhecimento facial em coletivos de transporte público funcionaria.

> A medida tem como objetivo combater as fraudes nas gratuidades, ou seja, os casos de pessoas que utilizam o cartão de terceiros para não pagar a tarifa, ao mesmo tempo em que evita ou combate os assaltos nos coletivos.
> A partir do momento que você adquire o cartão, passa a usar o reconhecimento facial para fazer com que acabe com esse uso de bilhetes que circulam por aí como isentos. Com isso, ele diminui o número de passageiros que circulam gratuitamente de forma ilegal, evita assaltos dentro dos ônibus porque não tem mais dinheiro e com isso, você traz mais segurança, agilidade e conforto para o usuário (Amazonas, 2018).

Contudo, o requerimento não aponta estudos que indiquem que a adoção de ferramentas de reconhecimento facial seja capaz de coibir crimes ou fraudes nos transportes. Outros estados já permitem a utilização de ferramentas de reconhecimento facial no transporte público.

Os requerimentos e indicações funcionam também como uma forma do legislativo fiscalizar e/ou pressionar outros órgãos ou entidades.

Em São Paulo, o PL 865/2019 “dispõe sobre a instalação obrigatória de câmeras de reconhecimento facial em todas as estações do Metrô e da CPTM, bem como no interior dos vagões das composições” (São Paulo, 2019). O projeto, de autoria do deputado Rodrigo Gambale, então PSL, justifica-se por supostos atos de vandalismo promovidos por torcidas organizadas; brigas entre vendedores ambulantes e seguranças das estações; assaltos e homicídios. Segundo o

legislador, a presença de câmeras “inibe a ação criminosa, pois o praticante saberá que será reconhecido. E, ainda que o crime seja praticado, essas câmeras identificarão os possíveis responsáveis” (São Paulo, 2019). Ao ser eleito deputado federal, Gambale submeteu o projeto de teor similar, anteriormente citado.

O parlamentar submeteu, também em 2019, a Indicação Legislativa 2.287 para tratar do mesmo tema e solicitar ao governador que instalasse equipamentos com reconhecimento facial em metrôs e trens de São Paulo. Vale destacar que as câmeras com TRF, instaladas no metrô em São Paulo, têm sido objeto de disputa judicial.

A Indicação Legislativa 8.929/2010 solicitava ao governador do Distrito Federal a implementação de TRFs no transporte público, aliadas às campanhas de conscientização contra fraudes.

O Rio de Janeiro, pioneiro em leis sobre videomonitoramento e também sobre reconhecimento facial, possui alguns projetos arquivados ou tramitandos sobre a utilização de TRFs no transporte público. O PL 341/2019 objetiva dispor a respeito da “obrigatoriedade de concessionários do serviço público de administração de terminais rodoviários, instalação de câmeras de segurança com tecnologia de reconhecimento facial de suspeitos e procurados da justiça” (Rio de Janeiro, 2019h). O PL 342/2019 “dispõe sobre a obrigatoriedade de concessionários do serviço público de metrô, trens e barcas, instalação de câmeras de segurança com tecnologia de reconhecimento facial de suspeitos e procurados da justiça” (Rio de Janeiro, 2019i). No metrô, o PL 1.372/2019, de autoria de Marcelo do Seu Dino (PSL), objetiva dispor “sobre a instalação obrigatória de câmeras de reconhecimento facial em todas as estações do metrô-rio e da supervia, bem como no interior dos vagões das composições” (Rio de Janeiro, 2019)e. Um detalhe interessante é a similaridade entre estes PLs do Rio de Janeiro e o PL 865/2019. Os projetos justificam-se da mesma maneira, trocando apenas algumas palavras.

Já o PL 274/2023 dispõe sobre a instalação de dispositivos “de reconhecimento facial de suspeitos e procurados da justiça em terminais rodoviários, portos e aeroportos no âmbito do Estado do Rio de Janeiro” (Rio de Janeiro, 2023, p. 1). O projeto determina que sejam instalados em terminas rodoviários, portos e

aeroportos, por parte de empresas públicas ou privadas e concessionárias, câmeras com monitoramento “on-line e tecnologia de reconhecimento facial de suspeitos e procurados da justiça” (Rio de Janeiro, 2023a).

Segundo o seu artigo 1º, as câmeras, interligadas ao Centro Integrado de Controle de Comando, serão instaladas em plataformas, entradas e saídas, e no embarque e desembarque. Ao detectarem pessoa suspeita, um alerta será emitido à Polícia Militar e aos seguranças privados do local. A base de dados será composta por imagens e dados de suspeitos e procurados da Justiça, fornecidos pelo Disque-Denúncia e pela Secretaria Estadual da Polícia Civil.

Segundo a justificativa do projeto de Thiago Rangel (Podemos), a lei objetiva “Integrar o sistema privado de segurança com o sistema dos órgãos de segurança pública” para “capturar suspeitos e procurados com mandados de prisão em aberto, que utilizem para qualquer finalidade nas rodoviárias, portos e aeroportos do Estado do Rio de Janeiro” (Rio de Janeiro, 2023a). As leis que objetivam dispor sobre a adoção de TRFs no transporte público, terminais de ônibus, estações e portos são iguais, alterando-se apenas a localidade. Apresento uma delas adiante.

> Ressalta se que a busca de suspeitos por meio de câmeras com programa de reconhecimento facial, já está sendo implantada por um projeto-piloto do poder executivo estadual, porém sem abarcar os locais indicados no presente projeto.
> Resta claro que a instalação dos dispositivos de identificação facial nestes locais, trará mais segurança para todos usuários do sistema, pois é fato público e notório que ao longo dos anos, ocorre o aumento de casos de assaltos nas imediações dos terminais rodoviários e dentro dos ônibus. Além de evitar a fuga dos suspeitos e procurados para outros Estados e Municípios.
> Acrescenta-se ainda que existem câmeras de reconhecimento facial em três shoppings da capital do RJ, além de edifícios comerciais.
> Salienta-se que o Governo do Estado do Rio de Janeiro, em pronunciamento em uma de suas redes sociais, informou que o teste de programa de reconhecimento facial tem sido um sucesso, com 8 (oito) mandados de prisão cumpridos em apenas 10 dias, o que demonstra a real importância da expansão do referido projeto para os locais aqui indicados (Rio de Janeiro, 2023a).

Mais uma vez, a instalação de câmeras com reconhecimento facial é colocada como solução para a segurança pública. Contudo, vale relembrar o estudo de Bruno Cardoso (2014) sobre a instalação de câmeras no Rio de Janeiro e a forma como seus operadores atuavam. Mais câmeras exigirão cada vez mais pessoal capacitado, o que implica em custo com recursos tecnológicos e humanos.

Nota-se, ainda, o interesse do legislador de ligar-se à política de implementação de TRFs por parte do Executivo estadual. Por último, penso ser interessante que conste na justificativa que câmeras com reconhecimento facial sejam utilizadas em três *shoppings*, sem que tais estabelecimentos sejam explicitamente citados. Isso demonstra que tecnologias de reconhecimento facial têm sido adotadas antes de legislação que as regulamente, considerando que ainda são poucas as leis aprovadas sobre o tema.

Ainda no Rio de Janeiro, o PL 607/2019 objetiva tornar **"**obrigatória a instalação de câmeras de monitoramento com reconhecimento facial em todas as praças de pedágios" no Estado (Rio de Janeiro, 2019). Ao analisar a Lei 4.917/2006, sobre a instalação de câmeras de videovigilância em pedágios, Bruno Cardoso (2013) comenta que há

> a ideia recorrente de que a instalação de câmeras passaria imediatamente a significar a realização de um trabalho vasto, tecnicamente complicado e extenuante, de monitoramento completo de todo o fluxo de veículos circulando pela malha rodoviária estadual do Rio de Janeiro. Contrabando, sequestro, tráfico, organização em quadrilha, todos esses crimes seriam mais bem prevenidos ou investigados com o simples artifício da câmera de vigilância nas praças de pedágio, ignorando todas as outras etapas do monitoramento em si, da manutenção diária dos computadores ao efetivo humano que lidaria com essas câmeras (Cardoso, 2013, p. 53).

Acredito que o mesmo pode ser aplicado aos diversos projetos que envolvem a utilização de TRFs em locais como transportes públicos, hospitais, escolas, repartições públicas e até mesmo vias urbanas.

Outro projeto, o PL 853/2019, cujo objetivo é vedar "a negociação e comercialização de produtos e serviços no interior dos vagões e embarcações dos transportes públicos do Estado", autoriza, em seu artigo 6º, a implementação de dispositivos de reconhecimento facial (Rio de Janeiro, 2019k, p. 1). O objetivo de TRFs passa por reconhecer os trabalhadores ambulantes que atuam nos transportes. Penso ser desproporcional colocar sob vigília tantos usuários de transporte público para coibir o trabalho, em um país profundamente desigual, com tanta gente atuando profissionalmente na informalidade. Não será o medo dos pobres e das suas práticas?

Projeto de lei de 2019, de Goiás, de número 299 e de autoria do deputado Paulo Trabalho (PSL), versa sobre a obrigatoriedade de instalação de câmeras inteligentes pelas empresas concessionárias de transporte coletivo urbano do estado de Goiás, que permitam realizar reconhecimento facial de suspeitos de crimes e procurados da justiça. Como justificativa, o projeto aponta a prisão de uma pessoa no carnaval de Salvador, ao ser identificada pela tecnologia. Vale ainda o destaque para a forma como o legislador acredita que vá acontecer o reconhecimento:

> Por fim, caberá a Polícia Civil fornecer o banco de dados, com imagens de procurados, **bandidos perigosos e principais alvos** do nosso estado, para o sistema de monitoramento on-line. Estas informações serão utilizadas nas câmeras, para fazer o reconhecimento facial. Se um desses procurados entrar em algum veículo que esteja monitorado, ele poderá ser imediatamente reconhecido. Ao fazer uma identificação positiva, um alarme é disparado de forma silenciosa para as autoridades policiais mais próximas do local, aumentando a possibilidade de uma abordagem (Goiás, 2019, grifo nosso).

Ressalto a expressão “bandidos perigosos e principais alvos”, pois parece-me um certo tipo de ato falho. Quem são os principais alvos? Os bandidos perigosos ou aqueles que sempre são o alvo de políticas públicas ineficientes na segurança, como as pessoas pobres e negras?

Os projetos voltados para a adoção de TRFs no transporte público dividem-se em dois grupos. O primeiro é o que pretende utilizar a tecnologia como uma forma de coibir fraudes nos transportes e o segundo o que quer usar essa tecnologia nos transportes por razões de segurança pública, para buscar foragidos ou pessoas desaparecidas.

Na segurança pública, são diversos os projetos, a exemplo do PL 196/2018, de Ricardo Nicolau, que “determina o uso de ferramentas de biometria digital nas viaturas policiais de todo o Estado do Amazonas”. Consta na sua justificativa:

> A cada dia que passa, a biometria vem se tornando um recurso valioso para identificação humana, pois se trata de uma técnica acessível, segura e confiável. Várias entidades de segurança, por todo o mundo, públicas e privadas, estão empenhadas na utilização da biometria na área de segurança, tanto no controle de acesso, quanto para identificação de investigados. Além disso, diversos crimes podem ser evitados com ferramentas que possibilitam o cruzamento de dados biométricos, tendo em vista o intercâmbio de dados entre aplicações biométricas distintas e independentes, com um nível reduzido de acoplamento e com interoperabilidade entre

> sistemas de diferentes plataformas e tecnologias, de modo que seja possível agregar ao serviço o uso de várias funcionalidades biométricas tais como: o reconhecimento de face, a voz, as impressões digitais, a geometria da mão, a íris, ou mesmo a combinação destas, dentre outras, para executar a tarefa de identificação pessoal (Amazonas, 2018).

Novamente, a adoção de ferramentas de identificação biométrica, dentre as quais figura o reconhecimento facial, é acionada como uma forma de se evitar crimes, como se a tecnologia, por si só, fosse capaz de resolver problemas complexos. Esse é um discurso usado com frequência pelos legisladores, mas também pela imprensa e por muitos cidadãos, conforme pode ser visto na fala de um cidadão, a favor do reconhecimento facial, proferida em audiência pública no Senado, que cito a seguir. Para Renato Alencar (2022), “a utilização do reconhecimento facial seria um grande benefício para a sociedade por ser uma ferramenta que irá facilitar a identificação e captura de pessoas procuradas pela justiça”[16].

Em Minas Gerais, o projeto 391/2019, do deputado Carlos Henrique (PRB), “dispõe sobre a obrigatoriedade da implantação de tecnologia de reconhecimento facial em locais públicos no âmbito do Estado de Minas Gerais”. Seu artigo 1º “declara obrigatória a implantação de tecnologia de reconhecimento facial em locais públicos” (Minas Gerais, 2019) e indica que a danificação de equipamentos de reconhecimento facial acarretará multa de um salário-mínimo vigente. Creio que a justificativa é bastante interessante. Primeiramente, é composta pelo recurso discursivo do apelo ao combate à violência, como em muitos outros projetos.

Para o legislador, a implementação de TRFs fará com que as pessoas possam “ir trabalhar, estudar, passear com sua família mais tranquila, sabendo que mesmo em uma rua perigosa há um equipamento que reconhecerá um suspeito ou foragido, fazendo com que os criminosos repensem antes de cometer uma ação ilegal” (Minas Gerais, 2019). Afinal, o que é uma rua perigosa? É uma rua pouco iluminada? Uma rua onde ocorrem muitos crimes? Ou é mais uma maneira de reforçar preconceitos em determinadas áreas da cidade? Restam ainda outras

[16]O Relatório Final da Comissão de Juristas Responsável por Subsidiar Elaboração de Substitutivo sobre Inteligência Artificial no Brasil tem uma seção sobre o reconhecimento facial. Diversos são os atores que participaram dos debates sobre regulação de IA no país. Na parte sobre reconhecimento facial, diversas organizações da Sociedade Civil pedem o banimento da tecnologia enquanto a Polícia Federal se posicionou contrária ao banimento e a Microsoft pediu regulação adequada. Disponível em: https://static.poder360.com.br/2023/02/comissao-senado-IA-relatorio-final-dez-2022.pdf. Acesso em 20 jan 2024.

perguntas, como: de que maneira esses equipamentos reconhecerão os suspeitos e por que isso significa dissuadi-los instantaneamente? Ainda hoje faltam estudos que comprovem correlação entre a presença de câmeras de vigilância e a diminuição da criminalidade. Em segundo lugar, o legislador explica que “essa tecnologia será trazida da China para a instalação aqui no Brasil, o custo não será muito alto, levando em conta os gastos com as reformas e reconstrução de ambientes públicos depredados” (Minas Gerais, 2019). Por que a tecnologia adotada será a chinesa? Com base em que o legislador afirma que o custo de instalação e manutenção não será alto? Ele está considerando todo o aparato por trás das câmeras e o pessoal necessário para lidar com elas? Parece-me que não. Outro destaque a ser feito envolve o trecho “o avanço tecnológico é inevitável, pois o mundo está em constante movimento. Com os investimentos da China no Brasil e vice-versa esse sistema poderá chegar mais rápido e com fácil acessibilidade e garantir um bem-estar social” (Minas Gerais, 2019).

A justificativa da proposição também envolve a noção de que a tecnologia é capaz de garantir o bem-estar social, o que remete ao último destaque a ser feito na justificativa do PL 391/2021. O texto da justificativa é encerrado com o seguinte parágrafo: “com este projeto de lei, pretendo tranquilizar as famílias que desejam passear com segurança para parques, praças e evitar ações que contrariam a moral e os bons costumes da nossa sociedade” (Minas Gerais, 2019). Aqui, o comportamento suspeito não se restringe ao comportamento criminoso. Parece ser ampliado para todo e qualquer comportamento que seja capaz de contrariar a moral e os bons costumes, ou seja, aquele percebido como desviante. Como resposta, deputados de esquerda, na Assembleia Legislativa de Minas Gerais, propuseram projeto contrário com o objetivo de banir a adoção de TRFs no estado de MG, que será analisado na próxima seção.

O PL 1.097/2019 dispõe sobre a instalação de dispositivos com reconhecimento facial em edificações públicas e privadas no Estado do Rio de Janeiro.

> **Art. 1o -** Todas as edificações públicas e privadas no âmbito do estado do Rio de Janeiro devem possuir, na entrada, sistema de câmeras de vigilância com dispositivos de reconhecimento facial.
> **Parágrafo único -** Apenas as edificações privadas com mais de 20 câmeras instaladas deverão seguir esta lei.

> **Art. 2o-** Deverá ser criado um sistema de monitoramento interligado com órgãos públicos de segurança e o CICC (Centro Interligado de Comando e Controle).
> **§1o-** Uma pessoa capacitada deve ficar responsável por analisar as imagens, para o caso de alguma identificação positiva poder acionar as autoridades.
> **§2o-** As câmeras de vigilância deverão funcionar ininterruptamente durante o horário de funcionamento da edificação pública (Rio de Janeiro, 2019d).

Se aprovada, a proposta significaria a verdadeira instalação de um estado de vigilância e controle e o número de indivíduos trabalhando 24 horas no CICC seria bastante alto para assegurar que as câmeras realmente estivessem sendo visualizadas. Segundo a justificativa do projeto, ele foi apresentado devido ao "cuidado com a população de nosso estado, sua segurança e tranquilidade. Essa seria uma forma de procurar inibir qualquer tipo de ação de marginais ou atitudes que não condizem com a moral, ética e respeito" (Rio de Janeiro, 2019d, p. 2), ou seja, com os bons costumes do cidadão de bem. Afirma ainda que as gravações são capazes de coibir crimes, pois os "meliantes" sentem-se "inibidos" (Rio de Janeiro, 2019d).

Agora, na fronteira entre a identificação e a segurança pública, o PL 739/2023, de autoria de Dani Alonso (PL), objetiva dispor "sobre a criação do porte eletrônico de identificação funcional para os integrantes da Polícia Militar do Estado de São Paulo" (São Paulo, 2023c, p. 1), permitindo que policiais militares possuam documentos de identificação digitais, o que envolve o reconhecimento facial. No Rio de Janeiro, o PL 4.493/2021, de Rodrigo Amorim (PSL), objetiva instituir "a carteira de identidade funcional em formato digital para policiais militares, policiais civis, policiais penais, e demais agentes de segurança pública do estado do Rio de Janeiro" (Rio de Janeiro, 2021a).

Na identificação civil e do funcionalismo público, o RJ toma mais uma vez a frente. O projeto de lei 862/2003, do deputado Otávio Leite (PSDB), "dispõe sobre os mecanismos de segurança para acesso aos sistemas e bancos de dados da administração pública do Estado", permitindo o credenciamento e a autenticação de usuários em sistemas da administração pública direta por meio de "características biométricas, tais quais impressão digital, reconhecimento facial, reconhecimento da íris ou outro mecanismo tecnológico destinado a este fim" (Rio de Janeiro, 2003, p.

1). Justifica-se pela suposta fragilidade de senhas alfanuméricas. Portanto, a solução estaria na utilização de dados biométricos para a confirmação de identidade.

O projeto de lei 2.548/2020, de autoria de Gil Vianna (PSL), objetiva criar a "obrigatoriedade da carteira de identidade para todos os cidadãos com idade inferior a 18 (dezoito) anos a ser emitida pelos órgãos de identificação competentes, do Estado" do RJ (Rio de Janeiro, 2020b, p. 1). A obrigatoriedade de documentos de identificação se restringe aos maiores de 18 anos. Com isso, busca-se fornecer subsídios para o Banco de Dados de Reconhecimento Facial e Digital de Crianças e Adolescentes Desaparecidos, em caso de desaparecimento de pessoa menor de 18 anos, no Estado do Rio de Janeiro.

O projeto de lei 1.833/2020, de Rodrigo Amorim (PSL), objetiva instituir "o banco estadual de dados multibiométricos no sistema de segurança pública, conjugando impressões papilares, impressões palmares, imagens de face, assinatura, íris e fala", como meio de "dar maior celeridade a identificação criminal e autoria de delitos" (Rio de Janeiro, 2020a, p. 1).

Outro projeto fluminense, o 2.946/2020, de autoria de Alexandre Knoploch (PSL), tinha o objetivo de flexibilizar os "serviços para obtenção da carteira nacional de habilitação do Estado do Rio de Janeiro, enquanto vigorar o estado de calamidade pública em virtude da pandemia do novo coronavírus (covid-19)" (Rio de Janeiro, 2020c, p. 1). Nesse sentido, os exames seriam feitos em plataformas digitais com capacidade para a realização de "captura da imagem e reconhecimento facial do candidato, colheita da biometria e controle do tempo de realização do exame teórico" (Rio de Janeiro, 2020c, p. 1). Nesse caso, o uso de TRFs objetivava evitar fraudes nos exames para habilitação de condutores.

Tema que recebe bastante atenção dos adeptos de ferramentas de reconhecimento facial é o que concerne aos desaparecidos. As primeiras leis que autorizavam a adoção de TRFs estavam direcionadas para a instituição de bancos de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos. Tais bancos de dados estão intrinsecamente relacionados com a coleta de dados biométricos, no momento da confecção de documentos de identificação. É o que pode ser percebido em projetos e leis dos estados do Amapá, Ceará, Distrito Federal, Goiás, Maranhão, Mato Grosso, Mato Grosso do Sul, Paraíba, Paraná, Rio de Janeiro, Rio Grande do Sul e Santa Catarina. Rio de

Janeiro, Rio Grande do Sul e Tocantins são os estados que já possuem leis relacionadas à criação de banco de dados para reconhecimento facial e digital de desaparecidos.

No Ceará, no projeto de indicação legislativa que justifica a adoção de bancos de dados para reconhecimento facial de crianças e adolescentes desaparecidos, consta:

> A presente proposição tem por objetivo indicar ao Governo do Estado que seja providenciado a instituição de banco de dados com reconhecimento facial e digital de crianças e adolescente desaparecidos, a cargo da Secretaria da Segurança e Defesa Social, que coletará as informações e imagens quando da confecção da carteira de identidade.
> Destaca-se ainda que, as informações constantes no mencionado banco de dados deverão ser compartilhadas com os demais órgãos com atuação no sentido de localização dos desaparecidos.
> Assim, demonstrada a relevância da matéria, e na certeza da aprovação, inclusive quanto ao regime de tramitação, submetemos o presente projeto de indicação a apreciação desta Augusta Casa Legislativa (Ceará, 2020).

O breve texto da justificativa, apresentado anteriormente, não explica de que maneira as TRFs são realmente eficientes na busca de pessoas desaparecidas. Ele parte do pressuposto de que a matéria é relevante e que será aprovada. O projeto foi aprovado, mas consiste em uma Indicação, o que pode significar sua adoção ou não pelo executivo. Isso também vale para o projeto de mesmo objetivo, de autoria do deputado Hermeto, de número 1.649/2020. Nele, o parlamentar justifica o projeto ao discorrer sobre o problema do tráfico internacional de pessoas. E aqui já não se trata de uma indicação legislativa, mas de um projeto de lei. Posteriormente, em 2021, o projeto do Distrito Federal recebeu emenda para adaptar-se à LGPD, atendendo ao "princípio da proporcionalidade, finalidade e transparência e também algumas questões relativas PPP[17] para tratar dados de segurança pública que a lei proíbe". (Distrito Federal, 2020). No Maranhão, projeto de lei de autoria de Wellington do Curso, de 2021, apela à sensibilidade dos legisladores para justificar-se e retoma a ideia de que novas tecnologias ajudarão a buscar pessoas desaparecidas, como pode ser visto no trecho a seguir.

[17]Parceria Público Privada.

> O desaparecimento de um ente querido, naturalmente, é um acontecimento que afeta profundamente toda a família, que a partir de então passa a realizar inúmeras ações com o objetivo de localizar o parente desaparecido, porém, nem sempre as buscas obtêm sucesso.
> Por essa razão, os serviços de auxílio a essa busca devem atualizar constantemente suas ferramentas de trabalho, adequando-se também as novas possibilidades tecnológicas, que podem oferecer um importante auxílio no cruzamento de dados entre os estados e também com sistemas que permitam reconstruir a imagem do desaparecido após algum tempo, oferecendo maiores chances de êxito a partir da veiculação da imagem atualizada (Maranhão, 2021).

O projeto de lei 2.453/2021, da Paraíba, apresenta justificativa bastante parecida com a anteriormente apresentada, além de abordar uma outra questão relativa à inteligência artificial, que é a criação de projeções de imagem atualizada da pessoa desaparecida.

> Por essa razão, os serviços de auxílio a essa busca devem atualizar constantemente suas ferramentas de trabalho, adequando-se também as novas possibilidades tecnológicas, que podem oferecer um importante auxílio no cruzamento de dados entre os estados e também com sistemas que permitam reconstruir a imagem do desaparecido após algum tempo, oferecendo maiores chances de êxito a partir da veiculação da imagem atualizada. (Paraíba, 2021)

Os projetos relacionados à criação de bancos de dados de crianças e adolescentes desaparecidos de diversos estados possuem essa mesma tônica: remetem ao problema do desaparecimento de pessoas e a tristeza que isso causa, ignorando quase que completamente em suas justificativas porque a utilização de TRFs pode ajudar na resolução do problema. As TRFs são tratadas como algo que basta ser implementado para que ocorra a diminuição dos desaparecimentos, como pode ser percebido nos demais exemplos explorados adiante. E é verdade que ter uma pessoa desaparecida é desesperador e é possível que TRFs ajudem, mas faltam evidências. O PL anteriormente apresentado, redigido pelo papiloscopista da PCDF, dizia que as críticas à TRF eram feitas por falta de conhecimento da tecnologia. Nesse sentido, parece que o exacerbado encantamento por ela também o é.

No Mato Grosso, na justificativa do projeto de autoria do deputado Silvio Fávero, consta que a proposta “permite que seja potencializado Sistema de Videomonitoramentos Eletrônico do Estado” e que serve para “impedir o

desaparecimento de crianças e jovens que na maioria das vezes, são vítimas do tráfico ou de organizações criminosas envolvidas com exploração sexual" (Mato Grosso, 2020). O autor cita também a estrutura de videomonitoramento urbano já implementada no Estado, demonstrando mais uma vez a forte relação entre os sistemas de reconhecimento facial e câmeras de videovigilância.

Já a justificativa do PL 75/2021, do deputado paranaense Do Carmo, apresenta que a tecnologia de reconhecimento facial representa uma realidade em diversas cidades do Brasil e vem sendo utilizada pela Receita Federal desde 2016. Além disso, o deputado argumenta que TRFs já são adotadas pela telefonia móvel "e em breve a maioria das cidades contará com câmeras com este tipo de tecnologia" (Paraná, 2021) – o Paraná já adota TRFs em escolas, como poderá ser visto no próximo capítulo. Em Santa Catarina, na justificativa do PL 0027.1/2021, de autoria da deputada Paulinha (PDT), já arquivado, consta que "é de conhecimento" que

> as câmeras de monitoramento facial atualmente são utilizadas no auxílio a segurança pública pois reconhecem pessoas muitos anos depois de terem cometido algo errado que determine sua procura, inclusive com severas alterações em sua face (Santa Catarina, 2021, p. 3).

Na justificativa, também consta que matéria similar obteve aprovação no Rio Grande do Sul, o que demonstra que parlamentares a favor (e contra) a adoção de TRFs se articulam de alguma maneira.

No Tocantins, a Lei 4.058/2022 "dispõe sobre o banco de dados de reconhecimento facial e digital de pessoas no Estado do Tocantins" (Tocantins, 2022). Algo que difere a lei tocantinense de outras é que ela não se restringe às crianças e adolescentes desaparecidos. No texto da lei, consta que serão observados os limites fixados pela Lei Geral de Proteção de Dados.

No Rio Grande do Sul, a Lei 15.460/2020 "cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes" (Rio Grande do Sul, 2020, p. 1). Essa é a lei citada anteriormente pela deputada Paulinha como parte de sua justificativa para a adoção de matéria similar em SC. A lei foi uma iniciativa do Executivo gaúcho e baseou-se em PL do deputado Tenente Coronel Zucco que depois, ao ser eleito deputado federal, submeteu o projeto de lei que apresentei na seção anterior.

No Rio de Janeiro, são três projetos e uma lei que objetivam adotar o reconhecimento facial para lidar com o problema de pessoas desaparecidas. O primeiro deles, o PL 1.033/2019, aprovado sob o número de lei 9.167/2021, de autoria dos deputados Gustavo Schmidt (PSL) e André Ceciliano (PT), objetiva instituir “o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos” (Rio de Janeiro, 2019b). As imagens para o banco de dados seriam extraídas no momento de confecção de documentos de identidade, o que poderia ser um problema, pois a identificação civil de menores de 18 anos não é obrigatória. Tal questão ficaria resolvida com a criação da obrigatoriedade, o que é objeto do PL 2.548/2020, que será discutido com maior profundidade em momento oportuno. Com o mesmo objetivo, há ainda os projetos de lei 1.101/2019, do deputado Renato Cozzolino (PRP), e 1.505/2019, do deputado Rodrigo Amorim (PSL).

Acredito que é possível que TRFs sejam capazes de auxiliar a busca por crianças e adolescentes desaparecidos. Contudo, é preciso que tais ferramentas façam parte de política pública mais ampla, envolvendo diversos órgãos.

Ainda na segurança pública, no Paraná, a indicação legislativa 477/2012, do deputado Ney Leprevost, atualmente do União Brasil, já sugeria a adoção de sistemas de identificação biométrica de pessoas apenadas e monitoramento eletrônica da população carcerária no Paraná. No mesmo estado, o projeto de lei 148/2019, de autoria do deputado Subtenente Everton, do bloco PSL/PTB, “dispõe sobre a permissão de implantação de tecnologia de reconhecimento facial em locais públicos” (Paraná, 2019).

O art. 1° do PL estabelece que aos órgãos da administração direta permite-se implementar tecnologia de reconhecimento facial em espaços públicos. Justifica-se pela ideia de que a instalação de tecnologias de reconhecimento facial geraria mais segurança e contribuiria para o reconhecimento de suspeitos. A proposta indica que o sistema de câmeras de alta tecnologia poderia “ser instalado em rodoviárias, aeroportos, vias públicas, comunidades e demais locais públicos nos quais o Estado entender necessário” (Paraná, 2019). Trata também a tecnologia como algo impossível de ser evitado, o que aparecerá em outros projetos, conforme poderá ser visto adiante. Para o legislador, “o avanço tecnológico é inevitável e o mundo está em constante desenvolvimento, por isto com intuito de ajudar na segurança e

garantir o bem-estar social, este projeto permitirá uma ampliação no modo de fazer segurança pública" (Paraná, 2019).

No Rio de Janeiro, o projeto 550/2023, do deputado Rodrigo Amorim (então PSL), objetiva autorizar "o poder executivo a utilizar tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública, no Estado" (Rio de Janeiro, 2023c). Segundo o PL, poderão ser utilizados equipamentos públicos ou imagens fornecidas por terceiros, o que abre espaço para empresas terceirizadas que oferecem serviços de segurança que incluem reconhecimento facial. O projeto indica que placas informativas devem ser fixadas para avisar que há captura de imagem para fins de reconhecimento facial e que identificações positivas devem ser confirmadas por agente público responsável. Reconhece ainda as controvérsias que envolvem TRFs, mas insiste na sua capacidade para combater a criminalidade, afirmando que a "taxa de sucesso é crescente devido ao desenvolvimento de tecnologias de reconhecimento 3D e de câmeras infravermelhas" (Rio de Janeiro, 2023c).

Na educação em nível estadual, os projetos começam a surgir em 2023. Na Bahia, o deputado Estadual Hassan propôs, em abril de 2023, lei que objetiva autorizar "a inclusão do reconhecimento facial como forma de acesso e controle de presença nas Escolas Públicas Estaduais", além de dar outras proposições:

> Art. 1o. Fica autorizada a inclusão do reconhecimento facial como forma de acesso e controle de presença nas Escolas Públicas Estaduais.
> Parágrafo único. O **reconhecimento facial fica estabelecido como um dos meios oficiais de garantia da segurança pública e repressão de infrações penais no acesso à escola pública.**
> Art. 2o. **No momento da matrícula do estudante deve ser incluído, em formulário próprio, autorização expressa do responsável legal para a captação de imagens do estudante, contendo no referido documento o motivo da captura de imagens e o tempo que as informações pessoais ficarão salvas.**
> Art. 3o. **O reconhecimento facial também se torna o modo oficial de comprovação da presença do aluno, para todos as finalidades.**
> Art. 4o. Por ocasião do acesso e saída do estudante, poderá ser estabelecido sistema de controle em que o responsável receba notificação imediata do acesso e saída do aluno da instituição de ensino.
> Art. 5o. **Os recursos para a execução das determinações desta lei não serão advindos do Poder Público, salvo quando existir previsão orçamentária, devendo ser obtidos por meio de**

> **convênios, parcerias, doações e instrumentos correlatos, em face do notório interesse público do reconhecimento facial para a proteção da segurança pública e repressão de infrações penais** (Bahia, 2023, grifo nosso).

Em primeiro lugar, destaco a forma como o deputado tenta contornar o fato de que as leis que representam gastos para o Executivo precisam de fonte de custeio. No artigo 5º, grifado acima, é indicado que os recursos não virão do Poder Público, mas de parcerias, convênios, doações e documentos correlatos. Essas benfeitorias ocorrerão devido ao "notório interesse público para a proteção da segurança pública e repressão de infrações penais" (Bahia, 2023), o que demonstra a vulnerabilidade do Poder Público diante do ideal neoliberal de que o mercado e o privado resolverão os problemas do Estado.

O segundo ponto que gostaria de destacar é a utilização de TRFs para aferir presença aos alunos. Isso faz parecer que passar a catraca e ter a face reconhecida, ao entrar no ambiente escolar, significa necessariamente estar em sala de aula. O terceiro ponto a ser destacado é que, no momento da matrícula, deve haver a inclusão de formulário que autoriza a captação de imagens de estudantes. Pergunto o que acontecerá na educação pública se algum responsável legal não quiser assinar tal documento. O estudante fica impedido de prosseguir os estudos ou a adoção de TRFs ficará restrita a poucas escolas? Haverá uma escola que ficará sem reconhecimento facial para garantir o direito daqueles com responsáveis contrários?

Por último, o quarto destaque que gostaria de fazer sobre o projeto de lei 24813/2023. Aparentemente, essa não é uma lei sobre educação, mas uma lei de segurança pública. Ela está direcionada para tornar o reconhecimento facial uma das formas oficiais de garantir a segurança pública e reprimir ações penais no âmbito escolar. Tal afirmativa é corroborada pela justificativa da proposição, na qual se indica que a Lei Geral de Proteção de Dados não é aplicável neste caso, pois trata-se de uma questão de segurança pública, o que aparece na LGPD como uma exceção à lei.

Em Pernambuco, o projeto de lei 669/2023 dispõe sobre a instituição de protocolo de acesso para visitantes em escolas da rede estadual de ensino. Dentre as medidas, autoriza-se a utilização de "câmeras de identificação ou reconhecimento facial nos acessos das unidades de ensino" (Pernambuco, 2023). Em sua

justificativa pela disseminação de ferramentas de controle em prédios comerciais, o projeto argumenta:

> Atualmente, para se ter acesso em prédios comerciais ou condomínios, seja na recepção ou na portaria, a regra mínima de segurança exige a identificação pessoal, o setor ou unidade autônoma a ser visitada e ainda, a coleta compulsória da imagem do visitante, para a liberação de sua entrada naquele empreendimento. Todavia, essas medidas de cautela e segurança, tão usuais no dia a dia da sociedade, precisa ser aplicada também nas unidades de ensino.
>
> As unidades de ensino, durante todo período letivo, mantêm elevado número de alunos, professores e demais profissionais da educação nas dependências da escola. Todo esse público tem o direito de conviver num ambiente protegido e seguro. Nesse sentido, os cuidados devem ser permanentes, com adoção de medidas de prevenção, em especial, com rígido controle de acesso de visitantes, como forma de inibir e evitar que uma pessoa estranha ou não autorizada frequente, mesmo que ocasionalmente, as dependências da escola. Portanto, o presente Projeto de Lei visa implantar protocolo de acesso nas unidades de ensino da Rede Pública Estadual de Pernambuco como forma de proteger toda comunidade escolar (Pernambuco, 2023, p. 1).

Os legisladores parecem acreditar que a comunidade escolar precisa ser protegida de ameaça externa que será resolvida com controle rígido dos visitantes. Contudo, o argumento parece-me precipitado, pois muitos dos ataques recentemente promovidos em escolas foram provocados por ex-alunos, ou seja, indivíduos que são, de alguma maneira, membros da comunidade escolar.

Na justificativa do projeto de lei 2.4813/2023, da Bahia, uma lista de ataques a escolas aparece como argumentos para sua aprovação. Indicação legislativa de 2023, de autoria do deputado do Mato Grosso, Wilson Santos, pede ao governador do Estado a implementação de tecnologias de reconhecimento facial em unidades de ensino públicas para coibir ataques violentos em escolas.

O PL 579/2023 “institui o protocolo de acesso, para visitantes, nas unidades de ensino do Estado de São Paulo” (São Paulo, 2023a). Aqui, o projeto de lei não está restrito apenas aos estabelecimentos de ensino da rede estadual, como acontece no projeto da Bahia, por exemplo, mas dirige-se à totalidade de estabelecimentos de ensino no estado de São Paulo, autorizando “o uso de Câmeras de Identificação ou Reconhecimento Facial nos acessos das unidades de ensino do Estado” (São Paulo, 2023a). Contudo, Carla Morando (PSDB), a mesma deputada do projeto anterior, elaborou o PL 580/2023 que objetiva autorizar o “Poder

Executivo a implementar sistema de câmeras de reconhecimento facial nas unidades de ensino da rede pública do Estado" (São Paulo, 2023b).

A preocupação com a violência no ambiente escolar fez com o que o presidente da República, Luiz Inácio Lula da Silva (PT), desse uma declaração em que defendeu que a escola não pode virar prisão de segurança máxima, alegando que não há verba para isso e "nem é politicamente correto, humanamente correto, socialmente correto" (Soares, 2023).

Terry Eagleton (2013) lembra que o ato de "formar alguém é dar a esta pessoa as ferramentas necessárias para ela compreender melhor o mundo em que vive e poder, no mínimo, sofrer nomeando as razões de seu sofrimento". Projetos de TRFs em escolas podem ter um aspecto muito nocivo, pois são uma transposição dos parâmetros da segurança para o ambiente escolar.

No DF, o projeto de lei 936/2020, que virou a Lei 6.712/2020, de autoria do deputado do MDB, Hermeto, merece ser analisado com calma. Tal proposta objetiva não a implementação de tecnologias de reconhecimento facial, o que aparece com frequência, mas a sua regulação. A seguir, apresento sua justificativa.

> A tecnologia de reconhecimento facial tem sido adotada pela sociedade em diversas áreas, principalmente na de segurança pública. **Todavia, a escassez de legislação sobre o tema permite a ocorrência de abusos.**
> A tecnologia pode ser uma ferramenta importante no combate ao crime, mas é preciso **estabelecer limites quanto ao monitoramento de pessoas. Imperioso garantir que sua utilização não gere parcialidade racial ou de gênero, sob o risco de, sem a devida proteção jurídica, tornar-se um mecanismo de controle social.**
> Em todo o mundo, câmeras de segurança com reconhecimento facial já são utilizadas para identificar criminosos entre milhares de pessoas e dar **maior efetividade ao combate à criminalidade e ao terrorismo.** (Distrito Federal, 2020, grifo nosso).

A justificativa reconhece a lacuna na legislação e os abusos decorrentes da utilização de TRFs. O projeto manifesta a importância da proteção jurídica para evitar vieses raciais ou de gênero, de modo a evitar que este tipo de tecnologia seja utilizado como mecanismo de controle social.

Considero particularmente interessante que o deputado tenha indicado que as TRFs podem dar maior efetividade ao combate à criminalidade e ao terrorismo. Em diversos países, o terrorismo aparece como uma justificativa regular para a adoção

de tecnologias de vigilância e controle, mas não é exatamente a principal razão para o uso desse tipo de tecnologia no Brasil.

Muito da atividade legislativa relacionada ao reconhecimento facial está ligada à segurança, conforme apontam Johann Čas, Rocco Bellanova, J. Peter Burgess, Michael Friedewald e Walter Peissel (2017, p. 3). Além disso, tem sido possível constatar, até aqui, que o papel cada vez mais importante da segurança nos debates políticos é paralelo ao estreitamento do próprio significado de segurança.

A complexidade do conceito de segurança, que envolve componentes como condições sociais e econômicas, de saúde, nutrição, o ambiente político, natural ou as liberdades individuais fundamentais, muitas vezes é ignorada nos debates sobre a temática na política e na mídia. A adoção de tecnologias de vigilância massiva por parte das autoridades estatais caminha lado a lado com uma reformulação mais ou menos explícita da noção clássica de segurança nacional, agora menos centrada na defesa de um determinado território e mais na definição de perfis.

A Lei 6.712/2020, antigo Pl 936/2020, que dispõe sobre o uso de tecnologias de reconhecimento facial na segurança pública do DF, apresenta limitações para o uso de TRFs, a necessidade de revisão das informações e parâmetros sobre a custódia das informações. O PL proíbe a utilização de TRF “em vigilância contínua de um indivíduo ou grupo de indivíduos, exceto quando autorizada judicialmente”. Vigilância contínua é definida como

> a utilização da tecnologia de reconhecimento facial para envolver-se em um esforço contínuo de rastreamento dos movimentos físicos de um indivíduo identificado em um ou mais locais públicos onde esses movimentos ocorrem durante um período de tempo superior a 72 horas, seja em tempo real ou através da aplicação de essa tecnologia para registros históricos (Distrito Federal, 2020).

O PL indica ainda a necessidade de validação da identificação positiva, por meio de revisão realizada por agente público antes de ação decorrente, e aponta que o agente público que descumprir os limites estabelecidos pela lei comete infração disciplinar grave.

O projeto 936/2020, do DF, parece-me mais realista do que a maior parte da legislação analisada que, com frequência, aparenta tratar tecnologias de reconhecimento facial como uma solução milagrosa. E, pensando de maneira mais

pragmática, conseguir diminuir os riscos do uso dessas tecnologias deve ser feito enquanto não se consegue bani-lo totalmente.

Vale destacar que os documentos que apresentam os pareceres do projeto nas comissões ajudam a compreender o processo parlamentar e as disputas políticas em torno do tema. Nas comissões, o debate envolveu a preocupação com a garantia de direitos fundamentais e também alguns clichês sobre o uso de tecnologias de vigilância e controle, girando em torno até mesmo de afirmações de que os defensores dos direitos humanos seriam aqueles que defendem bandido, conforme pode ser visto na seguinte fala do deputado Hermeto:

> Quem tem que ter medo de ser reconhecido é vagabundo. Quem não deve não teme. Quem não está devendo nada... Eu passo cinquenta, cem vezes com minha cara em frente à câmera. Quem está preocupado é o vagabundo que está na rua, que está matando, que está roubando, que está destruindo as vidas, Deputado Fábio Felix. V.Exa. se preocupa muito com os direitos humanos. Eu me preocupo muito com a segurança pública. Na hora que alguém morre, os direitos humanos não aparecem para ver a família que está lá. Não aparecem. Se vagabundo e corrupto que o Ministro Marco Aurélio colocou na rua... Esse vagabundo, esse cara que está condenado há mais de 25 anos de prisão e o nosso eminente Ministro Marco Aurélio colocou na rua, se ele tivesse passado em uma câmera que tivesse reconhecimento
> Então, Deputado, V.Exa. está certo com os direitos humanos. Pois eu vou cuidar dos direitos das pessoas com vida e que os vagabundos têm matado (Distrito Federal, 2020).

Após o comentário anterior, a deputada Arlete Sampaio, do PT, pede a palavra para reforçar que as alterações propostas não objetivam impedir a utilização de tecnologias de reconhecimento facial, mas garantir o direito à privacidade. Outro deputado do PSB, Roosevelt Vilela, ao elogiar o projeto, indica como o efetivo da Polícia Militar não cresceu proporcionalmente à população. Portanto, a adoção de ferramentas de controle e vigilância seria capaz de auxiliar na efetivação da justiça. O deputado Roosevelt Vilela prossegue, ao lembrar algo que remete à cultura da vigilância, analisada por David Lyon (2002; 2018; 2019). Em tal cultura, o monitoramento, por meio de tecnologias digitais, é percebido como inevitável na rotina dos indivíduos.

> Ninguém vai usar essas imagens para denegrir ou invadir a privacidade de ninguém, até porque todo mundo na rua hoje anda com celular e a nossa privacidade já está sendo invadida de qualquer

> forma. Então, não vai ser o Estado que vai reprimir isso (Distrito Federal, 2020).

A fala do deputado acima demonstra como a tecnologia é percebida como algo que não se pode evitar, corroborando com a cultura da vigilância.

Essas dinâmicas de disputa dentro das comissões e no plenário devem ser vistas como algo que auxilia o aprimoramento das leis. Por isso, é tão importante que os parlamentos sejam efetivamente representativos da população brasileira. Percebe-se, pelo resultado final do projeto aprovado na Comissão de Constituição e Justiça do Distrito Federal, que o debate parlamentar e as emendas ao projeto foram capazes de adicionar preocupações com a privacidade e os direitos humanos.

O projeto 207/2020, que tramita no Espírito Santo, foge um pouco às principais justificativas para a adoção de TRFs. Dirige-se às operadoras de telefonia que ficam “obrigadas a possuir um banco de dados dos clientes com terminal de reconhecimento facial e biometria digital, no âmbito do Estado do Espírito Santo” (Espírito Santo, 2020). O projeto de lei, proposto pelo deputado Capitão Assumção, objetiva coibir golpes que se utilizam de linhas telefônicas e números de Wh*atsapp.* A Câmara do ES solicitou parecer sobre a constitucionalidade do projeto à Procuradoria Geral do Estado que apontou sua inconstitucionalidade. A Comissão de Constituição e Justiça também considerou o projeto inconstitucional. Contudo, os deputados resolveram ignorar os pareceres e mantiveram a tramitação do projeto, como pode ser visto no Diário do Poder Legislativo do dia 24 de agosto de 2020. A proposta foi desarquivada em 2023, com o início de nova magistratura, conforme exige o regimento da assembleia. Agora, o projeto volta a tramitar nas comissões.

Outro projeto, agora da Paraíba, dispõe sobre a utilização de tecnologia de reconhecimento facial em estabelecimentos comerciais. A Lei 11.858/2021, de autoria do deputado Melchior Naelson Batista da Silva (Rede Sustentabilidade), objetiva obrigar que estabelecimentos comerciais que utilizem TRFs informem, com aviso, sobre a utilização destas tecnologias, tal qual é feito com o videomonitoramento. A justificativa aponta que TRFs têm o potencial de ferir direitos, como privacidade, intimidade e liberdade de expressão, demonstrando preocupação com a capacidade de análise de sentimentos de ferramentas de IA.

No Rio de Janeiro, o PL 384/2023 “dispõe sobre a instalação do sistema de dispositivo de reconhecimento facial de suspeitos e procurados da justiça em

shopping centers" (Rio de Janeiro, 2023, p. 1). Os *shopping centers* do Estado ficam obrigados a instalar câmeras com reconhecimento facial em todas as entradas e saídas dos estabelecimentos para identificar suspeitos e procurados da justiça. O PL proposto por Thiago Rangel (Podemos) é bastante similar ao outro projeto sobre reconhecimento facial do mesmo deputado, anteriormente citado.

O PL 0299.1/2018, de Santa Catarina, "dispõe sobre a possibilidade de convênio entre a Secretaria de Estado de Segurança Pública e os tabelionatos de notas para o compartilhamento de dados de identificação civil" (Santa Catarina, 2018). O texto de seu artigo 1º apresenta que o poder público "poderá firmar convênio com os notários". O projeto versa sobre a possibilidade de convênio entre a Secretaria de Segurança Pública e cartórios para a interoperabilidade de sistemas e o compartilhamento de informações. Segundo a justificativa, a troca de informações permite a correção e atualização de dados:

> os cadastros dos tabelionatos capturam e documentam as mudanças de feições naturais ao longo da vida e que não são devidamente apropriadas para o uso no banco de dados dos órgãos de segura, pois estes dependem da emissão de novos documentos de identificação (RG ou CNH) para a coleta da biometria, enquanto as bases dos cartórios são constantemente alimentadas com novas fotografias e imagens (Santa Catarina, 2018).

Nesse sentido, os cartórios e tabelionatos funcionariam como mais um órgão para o controle biométrico da população. O próprio legislador aponta a capilaridade dos tabelionatos. O deputado João Amin (PP) indica ainda que o projeto não onera os cofres públicos, não implicando em novos investimentos estatais porque prevê o aproveitamento da infraestrutura tecnológica que já existe na SSP. Mais uma vez, o discurso do custo zero aparece baseado em ideia que desconsidera os custos de visualização, tratamento e armazenamento de imagens, entre outros.

Primeiramente, é possível observar, nas casas legislativas e no Parlamento brasileiro, a crença no solucionismo tecnológico. A adoção de ferramentas de reconhecimento facial é percebida como algo que será capaz de resolver o problema das fraudes nos transportes públicos, trazer segurança para escolas e baratear custos com merendas ao evitar o desperdício alimentar e proporcionar melhoria na segurança pública. Os deputados e deputadas não parecem considerar os custos financeiros e práticos da utilização de tais ferramentas: privacidade aparece como

uma questão de menor gravidade, a logística que envolve a implementação é tratada como algo simples e o custo é desconsiderado. A questão da despesa é também o que faz com que muitos projetos sejam arquivados. Afinal, o Legislativo não pode criar despesas para o Executivo sem fonte de custeio e nem pode invadir suas atribuições. Apesar disso, as demais externalidades negativas nem sempre são levadas em conta.

Muitos dos projetos a favor do reconhecimento facial foram vetados ou arquivados porque criam uma despesa para o Executivo, sem que a fonte de custeio seja determinada, ou porque criam atribuições para órgãos e secretarias do Executivo, o que vai contra a separação de poderes.

Além disso, frequentemente, os debates ficam reduzidos ao equilíbrio entre privacidade e segurança, o que parte do pressuposto de que a vigilância massiva promovida pela dataficação da vida é a única solução para todo o tipo de ameaças. Isso faz com que o discurso em torno da tentação de adotar vigilância em massa seja difícil de resistir para diversos atores, dentro os quais os políticos eleitos (Čas *et al*, 2017).

Os relatórios das comissões nas quais os projetos tramitam são interessantes para observar de que maneira os deputados percebem o reconhecimento facial e as discussões em torno das TRFs, como pode ser observado nos debates em torno do PL 148/2019.

É observável nos discursos dos parlamentares a supervalorização do potencial das tecnologias de reconhecimento facial, no que parece ser um curto-circuito entre a promessa e a realidade concreta.

Também é possível perceber o aumento de leis propostas no sentido de implementar, regulamentar ou banir TRFs, o que se explica pelo avanço tecnológico nesse sentido e pela vontade dos parlamentares de participarem do debate público. Na próxima seção, apresentarei as propostas de banimento.

3.3 “Pare agora”! ou projetos contrários ao uso de tecnologias de reconhecimento facial

Nos estados da Bahia, Ceará, Minas Gerais, Pernambuco, Rio de Janeiro, São Paulo e no Distrito Federal deputados identificados com o campo da esquerda propuseram leis com o objetivo de proibir o reconhecimento facial em uma área ou em todo o setor público.

Na Bahia, o projeto de lei 2.4579/2022, de autoria do deputado Hilton Coelho (PSOL), “dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo Poder Público no Estado da Bahia” (Bahia, 2022). No corpo da justificativa, aparecem preocupações com a insegurança jurídica e a ineficiência de gastos públicos; com direitos fundamentais; racismo e transfobia; a preocupação com a privacidade de crianças e adolescentes e se aponta o reconhecimento facial como uma medida ineficaz, inadequada e onerosa, apresentando-se dados de estudos a respeito da baixa acurácia de tais tecnologias.

As justificativas dos projetos contrários ao uso de TRFs possuíam fundamentação muito mais extensa para justificar as proposições, quando comparadas às de projetos a favor do reconhecimento facial. Tenho a impressão de que isso se dá porque as tecnologias são tão difundidas no cotidiano que as proibir exige muito mais argumentos por parte dos legisladores. Sei que o número de páginas não representa por si só muita coisa, mas demonstra, nesse caso, uma preocupação com argumentos.

Vale destacar que os projetos de lei da Bahia e do Ceará são praticamente iguais: as fontes são as mesmas, as preocupações também e o texto é praticamente igual, o que pode ser explicado pela iniciativa que envolve parlamentares e será melhor vista adiante. O texto igual não é uma exclusividade dos projetos contrários ao reconhecimento facial, mas acontece em projetos a favor, inclusive, do mesmo Estado, como já foi visto. É interessante destacar que os textos são similares, mesmo quando seus objetivos são um pouco diferentes. Bahia, Ceará, Minas Gerais, Rio de Janeiro e São Paulo possuem projetos de lei que objetivam banir o uso de tecnologias de reconhecimento facial no setor público. Já em Pernambuco, o PL visa restringir o uso de TRFs apenas na segurança pública. No DF, os projetos visam restringir o uso de tecnologias de reconhecimento facial em câmeras corporais de policiais penais e no sistema penitenciário.

Os projetos para banir TRFs apresentam estudos a respeito do tema, apontam cidades que já baniram essas tecnologias, citam outros instrumentos e

entidades que pedem a proibição de seu uso, situações que envolvem falsos positivos e empresas que indicaram a paralisação ou fim da comercialização de tecnologias de reconhecimento facial. Contudo, vale destacar que o PL de autoria de Dani Portela (PSOL) objetiva proibir o uso de tecnologias de reconhecimento facial na segurança de Pernambuco. Seu texto aponta que o projeto está inserido em um quadro nacional de iniciativa de larga escala, envolvendo mais de 50 parlamentares de 13 estados, o que inclui legislativos municipais e estaduais.

> O Projeto de Lei em questão, por sua vez, tem como origem iniciativa legislativa de escala nacional sobre o tema do reconhecimento facial reunindo mais de 50 (cinquenta) parlamentares atuando em legislativos municipais e estaduais de 13 estados, tendo sido denominada a iniciativa “Sai da Minha Cara” (1). A campanha expressou uma preocupação ao revelar que a tecnologia é falha, com baixa eficiência em suas intenções de combater o crime ao apresentar dados e resultados discriminatórios. A utilização de tecnologias de reconhecimento facial para a segurança pública é uma questão que suscita preocupação em relação à proteção dos direitos fundamentais e à discriminação racial. É importante destacar que esses sistemas não são infalíveis e podem gerar resultados imprecisos ou discriminatórios (Pernambuco, 2023).

O PL baseia-se no PLO nº 249/22, da Câmara Municipal do Recife, sob autoria de Dani Portela e Ivan Moraes, e indica a presença de legislação similar em 13 estados. Em levantamento nas Assembleias Legislativas, somente identifiquei 9 – inclusive com as leis do DF que não são propriamente sobre a proibição de TRF, mas sobre sua incorporação em câmeras de policiais – e alguns são posteriores. Provavelmente, o levantamento considera também as propostas nas câmaras de vereadores.

Na legislação baiana para banir TRFs, a privacidade de menores de idade aparece como uma preocupação explícita, o que pode ser visto no trecho a seguir:

> Quanto à violação dos direitos de crianças e adolescentes, podemos frisar que a privacidade da população infantojuvenil é garantida pelo ordenamento jurídico Brasileiro tanto no que diz respeito ao direito de imagem quanto ao tratamento de seus dados pessoais em prol do seu melhor interesse, sendo necessário o consentimento específico por seu responsável para tanto. Pela impossibilidade de sistemas de tecnologias de reconhecimento facial serem utilizados em espaços públicos sem coletar dados de menores e incapazes, eles representam uma ameaça aos direitos de indivíduos dessa faixa etária. (Bahia, 2022)

Na proposta que objetiva implementar TRFs em escolas, a solução para o problema apontado acima está na assinatura de autorização expressa do responsável legal. Entretanto, restam as questões anteriormente apontadas.

No Rio de Janeiro, o PL 5.240/2021 foi o primeiro com o objetivo de banir o reconhecimento facial na segurança pública. A proposta foi feita sob autoria de Dani Monteiro (PSOL), Waldeck Carneiro (PT), Luiz Paulo (Cidadania), Flavio Serafini (PSOL), Mônica Francisco (PSOL), Enfermeira Rejane (PCdoB), Carlos Minc (PSB), Renata Souza (PSOL) e Eliomar Coelho (PSOL). Na justificativa do projeto, consta que a proposição foi elaborada a partir da ponderação de um grupo de pesquisadores. Nela também se discorre brevemente sobre a adoção de ferramentas de reconhecimento facial pelas polícias Militar e Civil do Estado e sobre o trabalho em conjunto das corporações com empresas como a operadora telefônica Oi, a empresa britânica de tecnologia *Staff of Technology Solutions* e a chinesa *Huawei* para disseminar TRFs em cidades fluminenses.

Segundo a justificativa, tais tecnologias têm sido espalhadas acriticamente e exibidas “como a solução para a diminuição da criminalidade e para maior controle de multidões” enquanto “já existem levantamentos de dados e evidências científicas de que o uso destas tecnologias além de caras e ineficientes para esta finalidade, ainda contribuem para o aprofundamento de desigualdades históricas” (Rio de Janeiro, 2021b, p. 3). Cita ainda inquérito do Ministério Público para investigar o programa de reconhecimento facial, no que se refere à violação ao direito à privacidade e à possível utilização das imagens coletadas com objetivos comerciais e publicitários.

O PL 5.240/2021 apresenta o debate sobre os problemas relacionados ao reconhecimento facial, do mesmo modo que os projetos de lei apresentados anteriormente. Parece-me também que sua fundamentação serviu de apoio para a elaboração dos demais. A justificativa do PL tenta ainda responder por que banir TRFs:

> O reconhecimento facial tem falhas técnicas significativas em suas formas atuais, incluindo, por exemplo, sistemas que refletem vieses raciais e são menos acurados para pessoas com tons de pele mais escuros. Entretanto, as melhorias técnicas desses sistemas não evitarão a ameaça que representam aos nossos direitos humanos.
> Embora dados de treinamento mais diversificados ou outras medidas para melhorar a precisão possam resolver alguns problemas atuais com esses sistemas, tais medidas apenas os aperfeiçoarão como

> instrumentos de vigilância e os tornarão mais eficazes em minar nossos direitos.
> Essas tecnologias representam uma ameaça aos nossos direitos de duas formas principais:
> Primeiro, os dados de treinamento - o banco de dados de rostos com o qual os dados de entrada são comparados e os dados biométricos tratados por esses sistemas - são geralmente obtidos sem o conhecimento, consentimento ou escolha genuinamente livre daqueles que estão incluídos neles, o que significa que essas tecnologias incentivam a vigilância em massa e discriminatória desde sua concepção.
> Em segundo lugar, enquanto as pessoas em espaços acessíveis ao público puderem ser instantaneamente identificadas, destacadas ou rastreadas, seus direitos humanos serão minados. Até a ideia de que essas tecnologias poderiam estar em operação em espaços acessíveis ao público cria um efeito inibitório que mina a capacidade das pessoas de exercerem seus direitos.
> Apesar de alegações questionáveis de que essas tecnologias aprimoram a segurança pública, quaisquer benefícios serão sempre ultrapassados pelas sistemáticas violações aos nossos direitos. Nós vemos cada vez mais provas de como essas tecnologias são usadas de modo abusivo e implementadas com pouca ou nenhuma transparência.
> Qualquer pesquisa e análise de como o policiamento foi historicamente conduzido mostra que o uso experimental de tecnologias de vigilância comumente criminaliza comunidades marginalizadas e de baixa renda, as mesmas comunidades que tradicionalmente enfrentam o racismo estrutural e a discriminação. O uso de reconhecimento facial não é uma exceção a isso e, por esse motivo, deve ser impedido antes que uma infraestrutura de vigilância ainda mais perigosa seja criada ou operacionalizada de modo permanente.
> A mera existência dessas ferramentas, seja nas mãos das instituições policiais ou de empresas privadas (ou em parcerias público-privadas), sempre criará incentivos para que sejam utilizadas de modo a desvirtuar sua função e para aumentar a vigilância em espaços públicos, levando a um efeito inibidor na liberdade de expressão. Como sua própria existência mina nossos direitos e a supervisão efetiva dessas tecnologias não é possível de modo a impedir abusos, não há outra opção a não ser bani-las totalmente em seu uso em espaços publicamente acessíveis (Rio de Janeiro, 2021b).

Segundo a justificativa do PL 5.240/2021, anteriormente apresentada, a disseminação de TRFs fere direitos, como à liberdade de expressão, à privacidade e à intimidade. Esse argumento vai ao encontro dos debates já abordados sobre dados pessoais e o problema da privacidade, discutido por autores como Pasquale (2015) e Véliz (2021).

No Rio Grande do Sul, o PL 16/2023, de autoria dos deputados do PSOL, Matheus Gomes e Luciana Genro, objetiva restringir “uso de tecnologias de reconhecimento facial pelo Poder Público no Estado” (Rio Grande do Sul, 2023, p. 1). O texto da lei é parecido com os demais e tem o mesmo objetivo. Isso ocorre porque a proposição faz parte da iniciativa citada anteriormente, que reúne parlamentares em torno da proibição de TRFs.

> A proposição visa fazer um chamamento à sociedade e ao Parlamento gaúcho para o desafio de legislar sobre o meio virtual e a captura de dados sensíveis do cidadão antes que as câmeras instaladas nas vias públicas e prédios da Administração Estatal passem a constituir um banco de dados sem nenhum controle social e com a tendência a perpetuar preconceitos, discriminações e injustiças (Rio Grande do Sul, 2023).

Linda Brasil, deputada estadual do PSOL de Sergipe, apresentou o projeto de lei 470/2023, que dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo poder público no Estado. A parlamentar já havia apresentado projeto similar em âmbito municipal, quando submeteu projeto contrário ao uso de TRFs em Sergipe, logo depois que uma pessoa foi erroneamente identificada no Pré-Caju, em Aracaju. Ainda assim, o PL não foi exatamente uma novidade na carreira da deputada, pois ela tinha protocolado projeto de teor similar na Câmara de Vereadores de Aracaju, durante seu mandato de vereadora.

O PL 16/2023, do Rio Grande do Sul, termina ao convidar a sociedade sobre os desafios a respeito da legislação sobre a dataficação da vida e a captura de dados sensíveis dos indivíduos. E é com esse apelo que passo às considerações elaboradas a partir da análise dos documentos e dados anteriormente apresentados.

Há um debate relativo à TRF entre parlamentares ligados à direita e à esquerda. Os deputados de esquerda demonstram ser mais receosos com o uso desse tipo de tecnologia, enquanto os deputados de direita depositam maior esperança nele. Esse mesmo debate aparece nas comissões e nos exemplos apresentados anteriormente.

Um dos problemas da democracia é que não se pode afirmar que ela é efetivamente representativa, se os cidadãos não pensam que são representados. O rompimento do vínculo subjetivo entre o que os cidadãos desejam e pensam e os atos daqueles eleitos pode produzir uma crise de legitimidade política, causando a

impressão de que os atores do sistema político não representam o cidadão (Castells, 2011). E, por isso, é tão importante que as pessoas eleitas realmente sejam capazes de representar os interesses dos cidadãos e não de empresas.

Foi possível observar que vereadores, deputados estaduais e deputados federais apresentam projetos similares, ao assumirem mandatos em outras esferas, conforme os exemplos de Dani Portela (PSOL) que, ao deixar o cargo de vereadora em Recife e assumir como deputada estadual, submeteu projeto contrário ao reconhecimento na Câmara Legislativa de Pernambuco. Também há o exemplo de Linda Brazil, de Sergipe, e do Deputado Coronel Zucco (na época PSL e atualmente Republicanos) que, ao assumirem outros cargos, levaram projetos similares.

Acredito que o debate legislativo, nos âmbitos federal e estadual, ganharia muito, se acrescido de análise da legislação municipal. Os municípios possuem bastante impacto na adoção de TRFs e ainda são mais difíceis de serem fiscalizados do que os estados, por causa de seu número. Afinal, o país possui 5.568 municípios.

Parece que os projetos de lei que objetivam restringir o uso de tecnologias de reconhecimento facial funcionam como tentativas de fomentar o debate público a respeito dos problemas provocados por TRFs. Contudo, o debate começa muito tardiamente, se comparado com os projetos a favor do uso. Além disso, muitos projetos objetivam proibir a adoção de tais tecnologias em contextos em que elas já se encontram implementadas em diversos estados, conforme poderá ser visto no próximo capítulo. Nesse sentido, uma opção que parece viável aos parlamentares contrários ao uso do reconhecimento facial é o trabalho em comissões, como o do exemplo brasiliense, para diminuir os danos de leis relacionados às TRFs, ampliando o debate e tentando garantir direitos e um melhor controle do uso de tais ferramentas. E aí vale pensar que a política é o espaço das negociações.

Algo que merece ser destacado é que a presença de legislação não significa necessariamente que tecnologias de reconhecimento facial estejam em uso. O contrário também é verdadeiro: a ausência de legislação não garante que TRFs não sejam adotadas pelo Executivo dos estados analisados. Isso será melhor abordado no próximo capítulo.

Muitas vezes, os parlamentares parecem utilizar ferramentas de reconhecimento facial como um dispositivo mágico que resolverá problemas multifacetados, ao serem colocadas em estabelecimentos comerciais, em garantias

de compras, no uso de aplicativos de transporte, em unidades de ensino. Também não se apresenta o modo como tais tecnologias serão implementadas ou quem arcará com seus custos.

Observa-se que o desejo de utilizar TRFs em diversos setores da vida também já tem reflexos na política feita nas câmaras legislativas, o que reflete na diversidade de setores em que há matérias legislativas.

Carissa Véliz (2021) destaca que parte importante de regulações positivas é conseguir impedir que um determinado tipo de poder seja convertido em outro, como a transformação do poder econômico em poder político.

Para concluir, gostaria de lembrar que a política nas câmaras legislativas é algo complexo e é impossível encerrar completamente o debate por aqui, mas essa também não é a única forma de fazer política. Abordarei esse outro modo no capítulo intitulado *Para Imaginar o Novo*.

A política nas câmaras legislativas é algo complexo e seria impossível encerrar o debate por aqui. Contudo, busquei apresentar e apontar elementos da legislação vigente e proposta. A partir dela, creio ser possível destacar alguns elementos que vão ao encontro dos debates teóricos apresentados neste estudo.

No próximo capítulo, abordo a economia por trás da utilização de ferramentas de reconhecimento facial.

4 USOS E CUSTOS DE FERRAMENTAS DE RECONHECIMENTO FACIAL

Em nossas terras, os numerinhos têm melhor sorte que as pessoas.
Quantos vão bem quando a economia vai bem?
Quantos se desenvolvem com o desenvolvimento?
O livro dos Abraços - Eduardo Galeano

Apesar das muitas críticas à adoção de ferramentas de reconhecimento facial e de extração de dados biométricos, tem crescido sua utilização em muitos setores da vida humana. TRFs têm sido propagandeadas como solução para problemas sociais muito complexos, em diversos lugares do mundo, assim como ocorreu com o videomonitoramento, o que pôde ser observado na legislação apresentada no capítulo anterior.

Neste capítulo, abordo a economia envolvida na utilização de ferramentas de reconhecimento facial no mundo e no Brasil. Primeiramente, apresento um panorama da questão. Depois, busco demonstrar como o uso de tecnologias de reconhecimento facial tem se espalhado por estados brasileiros. Para verificar iniciativas e seus custos estaduais, foram utilizados pedidos de acesso à informação, realizados entre março e junho de 2023, com respostas obtidas entre março e setembro do mesmo ano.

4.1 A videovigilância e o reconhecimento facial no mundo

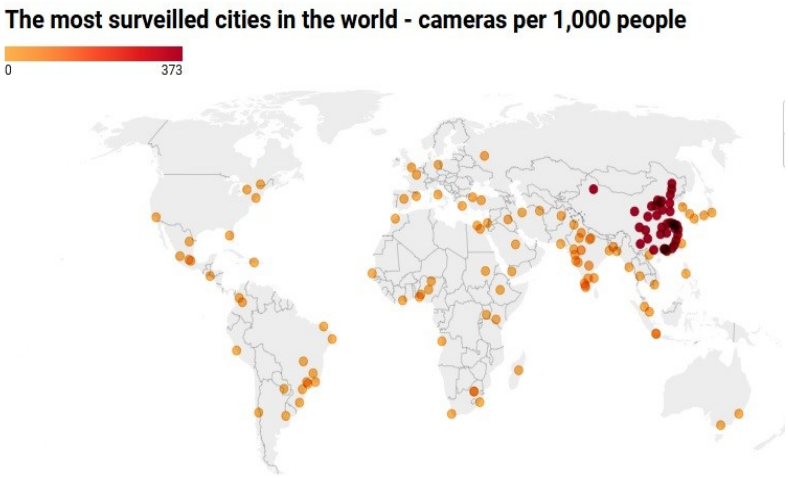
Como dito anteriormente, videomonitoramento e reconhecimento facial caminham lado a lado, em muitos casos. Mundialmente, a videovigilância já é bastante disseminada. Estimativa realizada pela IHS Markit, em 2019, indicava que o mundo teria, em 2021, mais de um bilhão de câmeras (Cosgroove, 2019). A China, por exemplo, é o país com o maior número de câmeras ligadas a circuitos fechados de televisão. As cidades com as maiores taxas baseadas no número de câmeras por 1.000 pessoas são Indore, Haiderabade, Delhi e Chennai, na Índia; Singapura, em Singapura; Moscou e São Petesburgo, na Rússia; Bagdá, no Iraque; Londres, no Reino Unido; e Los Angeles, nos Estados Unidos da América (Bischoff, 2022).

Países como China, Emirados Árabes Unidos, Japão, Singapura e Estados Unidos da América foram pioneiros na adoção do reconhecimento facial, em diversos setores do cotidiano (Prakash, 2018).

Na China, 200 milhões de câmeras constituem um sistema de vigilância com a capacidade de identificação de 1,4 bilhões de cidadãos do país. No aeroporto em Dubai, nos Emirados Árabes, mais de 80 câmeras escaneiam as faces dos indivíduos que circulam pelo local. A partir disso, o sistema indica se as pessoas podem entrar livremente no país ou alerta a necessidade de análise de segurança mais profunda. Estima-se que, em 2016, pelo menos 50% dos cidadãos estado-unidenses adultos já tinham seus rostos em bases de dados de reconhecimento facial governamental (Oliveira, 2021).

A seguir, na figura 12, é possível ver a presença de câmeras de vigilância ao redor do globo.

Figura 12: Cidades mais vigiadas do mundo



Fonte: Bischoff (2022)[18]

O estudo *The Facial Recognition World Map,* realizado em 2020, apontou que 109 países adotavam ou haviam aprovado a utilização de tecnologias de reconhecimento facial para fins de vigilância (Surfshark, 2022). A pesquisa reuniu dados coletados em 194 países, conforme pode ser visto na figura 13 a seguir.

[18] Pode ser consultado de forma interativa em https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/. Acesso em 01 nov. 2022.

Figura 13: Mapa do reconhecimento facial no mundo

Fonte: Surfshark, 2020.

Os países foram divididos em cinco categorias: em uso, aprovado para uso (mas não implementada), em consideração, banida ou sem evidência de uso. As cores no mapa significam:

a) rosa escuro – em uso;

b) rosa claro – aprovado para uso, mas não implementada;

c) amarelo – em consideração;

d) azul – sem evidência de uso;

e) verde – banida.

No momento da realização da figura, em 2020, somente a Bélgica havia banido o uso de reconhecimento facial. Contudo, a mesma pesquisa aponta que, posteriormente, Bélgica, Luxemburgo e Marrocos baniram o uso da tecnologia de alguma maneira[19] (Surfshark, 2022).

[19]Os dados utilizados pela pesquisa podem ser consultados aqui: https://docs.google.com/spreadsheets/d/157mTA67QAMxb0N4e7tO755r9uw2wsaT1z2rcCO1hPIU/edit#gid=689675349. Acesso em: 13 nov. 2022.

No conflito armado entre Ucrânia e Rússia, em 2022, a Ucrânia reconheceu utilizar tecnologias de reconhecimento facial para identificar mortos, combater desinformação e identificar russos acusados de crimes de guerra. A tecnologia utilizada foi oferecida pela empresa *Clearview AI's*, que forma sua base de dados a partir de imagens recolhidas de redes sociais (Dave; Dastin; 2022) e que tem oferecido seus serviços para diversos países e estados, incluindo-se o Brasil, como poderá ser visto adiante na figura 14.

O mercado de tecnologias de reconhecimento facial tem crescido.

Figura 14: Crescimento do mercado de reconhecimento facial

Fonte: Mordor Intelligence, 2020.

Segundo estudo da consultoria Mordor Intelligence (2020), o mercado global de tecnologias de reconhecimento facial estava avaliado em $3,72 bilhões de dólares, em 2020. A projeção de crescimento, no período compreendido entre 2021 e 2026, era 21.71%, o que significa $11,62 bilhões de dólares, conforme pode ser visto na figura 13, acima.

Já outra consultoria, a Allied Market Research, estimou em 2021 que a movimentação do mercado seria de US$ 9,6 bilhões, ou seja, R$ 53 bilhões em 2022 (Góis, 2021).

Pesquisa da Emergen Research (2022) indica as 10 companhias que estão no topo dos negócios de reconhecimento facial no mundo, conforme pode ser visto na tabela 4 abaixo.

Tabela 4: 10 companhias com maior valor de mercado na área de reconhecimento facial

Companhia	Valor de	Descrição

	Mercado	
Megvii [20]	US$193.6 milhões	Empresa de tecnologia de software de reconhecimento de imagem e aprendizado profundo, sediada em Pequim, China. A companhia é a maior fornecedora de software de autenticação de terceiros em todo o mundo. O principal produto da empresa, Face++, é mundialmente a maior plataforma de visão computacional de código aberto. Com tecnologia biométrica avançada, o Face++ é capaz de detectar e analisar 106 pontos de dados no rosto. Suporta um grande número de kits de desenvolvimento de software (SDKs) para PHP, Java, Python, iOS e Ruby e é amplamente utilizado na aplicação da lei para capturar criminosos e analisar redes de videomonitoramento nas cidades.
Clear Secure, Inc.[21]	US$189 milhões	Empresa de tecnologia biométrica que oferece uma solução de verificação e identidade segura. O produto líder da Clear Secure, CLEAR é uma plataforma de identidade segura, amplamente utilizada em aeroportos e estádios que promete celeridade nas filas. Tem sede em Nova Iorque, EUA.
AnyVision[22]	US$22.9 milhões	Startup israelense que é uma das principais plataformas de IA visual do mundo, desenvolvendo software de reconhecimento corporal, digital e facial. Utiliza tecnologia de reconhecimento facial para abrir locais protegidos para indivíduos autorizados. A AnyVision usa mapas de calor gerados por IA para análises inteligentes em lojas para aprimorar a experiência do usuário.
Clarifai, Inc.[23]	US$15.8 milhões	Empresa de inteligência artificial localizada em Nova York, Estados Unidos, especializada em visão computacional e aprendizado de máquina automatizado. Objetiva melhorar a segurança das pessoas e reduzir o risco do negócio, utilizando tecnologia de reconhecimento facial. Este software é amplamente utilizado por diversos setores como financeiro, varejo, organizações governamentais para coibir furtos e roubos.
Sensory, Inc.[24]	US$15 milhões	Empresa de desenvolvimento de Inteligência Artificial localizada na Califórnia, EUA. Desenvolve tecnologias de

[20] Acesso em: https://en.megvii.com. Acesso em: 12 set 2022.
[21] Disponível em: https://ir.clearme.com/. Acesso em: 12 set. 2022.
[22] Disponível em: https://oosto.com/. Acesso em: 12 set. 2022.
[23] Disponível em: https://www.clarifai.com/models/ai-face-detection. Acesso em: 12 set. 2022.
[24] Disponível em: https://www.sensory.com/ Acesso em: 12 set. 2022.

		reconhecimento de fala e biometria e plataformas de software, possuindo alta demanda por produtos no setor de eletrônicos de consumo e automotivo. O *Truly Secure* é uma solução de autenticação de voz e rosto segura e flexível que, supostamente, oferece maior conveniência e autenticação do que os métodos tradicionais. A solução atualizada é capaz de reconhecer usuários enquanto o anúncio de uso de máscaras também pode detectar espirros e tosses.
Cognitec Systems GmbH[25]	US$13.64 milhões	Empresa com sede na Alemanha que lida com soluções de software e hardware biométricos. É uma das principais empresas de reconhecimento facial, oferecendo aplicativos e tecnologias de reconhecimento facial em todo o mundo. Oferecem sistemas de reconhecimento facial personalizáveis e fáceis de usar baseados na tecnologia FaceVACS.
iProov[26]	US$10.3 milhões	Empresa de segurança cibernética com sede em Londres, Reino Unido, que, supostamente, oferece autenticação biométrica para usuários online com alta segurança, privacidade e usabilidade. É amplamente utilizado em diversos setores públicos e governamentais, serviços financeiros, provedores de identidade digital, provedores de viagens entre outros. O *iProov Face Verifier* é um aplicativo de autenticação de verificação facial remota que permite que as organizações verifiquem o rosto de um usuário em relação a um modelo biométrico pré-registrado.
TrueFace[27]	US$4.9 milhões	Empresa estadounidense de visão computacional fundada por Shaun Moore e Nezare Chafni em 2013. Usa técnicas de IA e aprendizado de máquina, além de ser especializada em tecnologias de reconhecimento facial, detecção de ameaças, análise de emoções e idade e detecção de etnia. A TrueFace assinou um acordo com a Força Aérea dos EUA para fornecer serviços de reconhecimento facial e detecção de armas. Em novembro de 2020, a TrueFace fez parceria com a Modzy para desenvolver soluções faciais biométricas com inteligência artificial e ferramentas de detecção de falsificação. Em 2 de junho de 2021, a TrueFace foi adquirida pela Pangiam, apoiada pela AEI, uma provedora de serviços

[25] Disponível em: https://www.cognitec.com/ Acesso em: 12 set. 2022.
[26] Disponível em: https://www.iproov.com/ Acesso em: 12 set. 2022.
[27] Disponível em: https://www.trueface.ai/ Acesso em: 12 set 2022.

		de segurança e viagens.
CaraCom Group[28]	US$4 milhões	Empresa de software finlandesa, com foco em segurança especialmente nos setores de aplicação da lei, construção e industrial. CaraCom oferece proteção de dados pessoais e segurança de dados. CaraID é uma carteira de identidade que utiliza tecnologia de reconhecimento facial para identificar e autenticar a pessoa com o objetivo de reduzir problemas relacionados ao controle de acesso.
Kairos AR Inc. [29]	US$1.4 milhões	Empresa de biometria facial que oferece ferramentas de análise emocional e reconhecimento facial. Permite que as organizações integrem o reconhecimento facial por meio de sua API de nuvem Kairos, oferecendo segurança e privacidade de dados. Oferece identificação de rosto, detecção de rosto, detecção anti-spoof. Kairos oferece SDKs para linguagens JS, .net e Python. Foi fundada em 2012 em Miami, EUA. A empresa promete uma abordagem ética no desenvolvimento de tecnologias de reconhecimento facial.

Fonte: Emergen Research (2022)

Na tabela 4 acima, é possível observar que a maior parte das empresas de reconhecimento facial, dentre as 10 com maior valor de mercado, segundo levantamento da Emergen Research (2022), é dos EUA, apesar de o primeiro lugar ser de uma empresa chinesa. São estadunidenses a *Kairos AR Inc*., *TrueFace*, *Sensory*, *Inc*., *Clarifai*, *Inc*. e a *Clear Secure, Inc*.. São europeias a *CaraCom Group*, *Iproov e a Cognitec System GmbH*. Fora do eixo Europa-Estados Unidos da América, encontra-se a israelense *AnyVision* e a Chinesa *Megvii* que ocupam o terceiro e o primeiro lugar, respectivamente.

É interessante lembrar que Estados Unidos e Reino Unido compõem a aliança chamada de *Five Eyes* (cinco olhos), formada ainda pela Nova Zelândia, Austrália e Canadá, com o objetivo de facilitar a troca de Inteligência, constituindo um acordo multilateral entre tais países, mas não apenas. Eles também possuem intensa colaboração com outros países, como Dinamarca, França, Holanda, Noruega, Alemanha, Bélgica, Itália, Espanha e Suécia. Em termos práticos, uma comunidade de segurança, formada por 14 olhos (Deibert; Pauly, 2019).

[28] Disponível em: http://www.caracom.fi. Acesso em: 26 mai. 2024.
[29] Disponível em: https://www.kairos.com. Acesso em: 26 mai. 2024.

O crescimento do mercado em valor econômico vem acompanhado de uma série de polêmicas a respeito desse tipo de tecnologia, algumas das quais apresento no próximo capítulo, ao discutir os problemas éticos das tecnologias de reconhecimento facial. Para entender como a adoção dessas mesmas tecnologias tem crescido no Brasil, eu apresento estudos e o levantamento feito por mim por meio da Lei de Acesso à Informação. Os dados foram solicitados aos estados brasileiros, na educação e na segurança pública.

4.2 O reconhecimento facial no Brasil

Os exemplos apresentados aqui não pretendem ser exaustivos, mas ilustrativos, de modo a apresentar um panorama do que tem sido implementado no Brasil, onde crescem as empresas que desenvolvem soluções tecnológicas de reconhecimento facial. Alguns exemplos são as ferramentas desenvolvidas por companhias como a *Payface, Winker, Stoque, PontoID* e a Gabriel.

A *Payface*, startup brasileira, fornece ferramenta para pagamento de compras em lojas e redes de supermercado[30]. Por meio de um aplicativo próprio, os clientes podem pagar os itens consumidos em lojas diretamente por meio do celular e do reconhecimento biométrico. O serviço oferecido pela empresa é gratuito para os usuários e o seu objetivo é diminuir as filas nas lojas. Fundada em 2018 em Florianópolis, a empresa já recebeu mais de R$3 milhões em investimentos (Startupi, 2022).

Outra empresa, a Winker, oferece soluções tecnológicas para condomínios. Dentre elas, o reconhecimento facial. O acesso ao local ocorre por meio de aplicativo próprio que envolve cadastro de moradores e visitantes (Winker, 202-). Já a Stoque oferece serviços de automação digital para processos e documentos que agora envolvem o recolhimento e tratamento de dados biométricos.

Nem a fé é deixada de fora das tecnologias de reconhecimento facial. Em 2019, a empresa Kuzzma lançou na 15ª ExpoCristão um aplicativo para a utilização de reconhecimento facial em igrejas. A tecnologia funciona a partir de imagens extraídas de uma câmera panorâmica de alta resolução. O dispositivo identifica

[30]Disponível em: https://payface.com.br/para-o-seu-negocio/. Acesso em: 12 set. 2022.

informações pessoais e a assiduidade dos indivíduos nos cultos. Depois disso, são gerados relatórios para cada pessoa (Kuzzma, 201-)

O mercado do reconhecimento facial movimenta bastante a economia e faz circular tecnologias que envolvem imagens em 2D e 3D, para usos privados e públicos, em diversas localidades do globo.

Na segurança pública, existe Gabriel. Com nome de anjo, a empresa oferece soluções de vigilância para locais privados, como condomínios, prédios, empresas e casas. Foi fundada no Rio de Janeiro em 2020 e chegou a São Paulo em 2021, tendo levantado R$66 milhões em rodada de investimento do Softbank (Ribeiro, 2023).

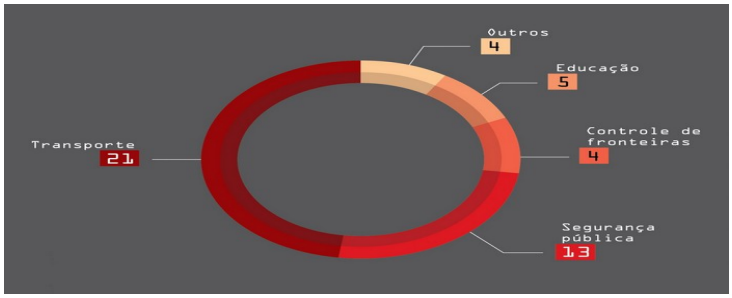
Os exemplos anteriores demonstram que a proteção da privacidade é algo bastante desafiador, diante dos progressos das tecnologias da informação e comunicação em andamento. Como alertam Bigo, Isin e Ruppert (2019), as tecnologias não tornam apenas a vigilância mais eficiente e intrusiva, mas diluem as fronteiras entre os dispositivos de vigilância tradicionais e os aparelhos eletrônicos utilizados no cotidiano, além de ocuparem espaços diversos, como escolas, igrejas e transportes, ocorrendo uma diluição das fronteiras.

Cabe aqui comentar que muitas dessas empresas são mais promessas para o mercado do que efetivamente lucrativas, o que remete ao comentário da jornalista Kashmir Hill (2023) sobre ser cética diante das promessas de *startups*, pois frequentemente não se cumprem. Ainda assim, estas empresas têm movimentado a economia em rodadas de investimentos, como as que participam a Payface e a Único (Souza, 2023).

Estudo realizado pelo Instituto Igarapé (2022), intitulado *Reconhecimento facial no Brasil,* indica que esse tipo de ferramenta tem sido usado no país desde 2011, contudo, em 2019, observou-se um aumento de sua popularidade.

A pesquisa do Instituto Igarapé indica que, entre 2011 e 2019, ao menos, 47 casos foram publicamente reportados sobre o uso do reconhecimento facial, pelo setor público e por seus parceiros no setor privado. A figura 15, adiante, mostra as áreas em que o reconhecimento facial é adotado no Brasil pelo setor público.

Figura 15: Reconhecimento facial no Setor Público brasileiro



Fonte: Instituto Igarapé (2022).

O mesmo estudo aponta que tecnologias de reconhecimento facial são frequentemente implementadas pelo Poder Público em quatro setores: 1) educação; 2) transporte; 3) controle de fronteiras; e 4) segurança pública, conforme pôde ser visto na figura 15, anteriormente apresentada.

Pesquisa de Mariah Rafaela Silva e Joana Varon (2021) realizou mapeamento em órgãos federais, por meio de pedidos de acesso para o Ministério da Economia, ao Serviço Federal de Processamento de Dados - SERPRO, ao Instituto Nacional de Seguro Social - INSS e à Secretaria de Governo Digital do Ministério da Economia, Receita Federal, Dataprev e Banco do Brasil, para verificar a adoção de TRFs por esses órgãos e instituições.

Como apontam as autoras, o Brasil tem adotado, com a desculpa da "promoção da segurança", o reconhecimento facial como meio para autenticar identidades e permitir o acesso a serviços governamentais. O SERPRO oferece diversos serviços que usam TRF, como Datavalid, o Biovalid, CDT, CPF-Digital, Acesso Gov Br, ID Estudantil, Embarque Seguro. Inclusive, Biovalid e Datavalid são vendidos para o mercado.

> Tais tecnologias operam na interconexão entre nome, sexo e dados biométricos (no caso dessa tecnologia em específico, a imagem do rosto) configurando deste modo uma política de massa de identificação civil, através dos velhos paradigmas de classificação das diferenças entre homens e mulheres e, principalmente, no agenciamento dos discursos sobre "segurança jurídica" (Silva; Varon, 2021, p. 14).

Na fronteira entre a segurança e o controle de fronteiras, em março de 2021, o Governo Federal iniciou testes de embarque aéreo 100% digital no Aeroporto

Santos Dumont, no Rio de Janeiro. O projeto Embarque + Seguro conta com a tecnologia do Serpro e foi criado pela Secretaria Nacional de Aviação Civil, do Ministério da Infraestrutura. Os passageiros não precisam de cartão de embarque ou documentos para embarcar nos voos (Gandra, 2021). Meses depois, em maio, foi a vez do Aeroporto Internacional de Belo Horizonte receber a tecnologia para testes.

Os passageiros foram voluntários na operação cujo funcionamento inicia na hora do *check-in* no aeroporto. Nesse momento, o passageiro recebe, no aparelho celular, uma mensagem a solicitar autorização para o registro de uma foto. Com o consentimento do indivíduo, a pessoa atendente da empresa aérea executa a validação biométrica do passageiro, realizando uma comparação entre os dados fornecidos e a foto tirada na hora com as bases de dado governamentais. Depois disso, os passageiros ficam autorizados para ingresso na sala de embarque e na aeronave somente ao passar pelos pontos de controle biométricos que os identificam por meio de câmeras, sem que seja preciso apresentar documento ou cartão de embarque novamente (Embarque..., 2021).

Segundo o Serpro, o Embarque + Seguro[31]

> é um sistema de reconhecimento por biometria, que valida a identidade do viajante por selfies tirados na hora comparados com os dados do Senatran e do Barramento SGD (TSE). O objetivo é tornar o processo de embarque nos aeroportos mais eficiente e as viagens aéreas mais seguras.
> A solução encontra-se alinhada com as principais iniciativas e projetos internacionais do setor, tais como: Programa de Identificação de Viajantes (Traveller Identification Programme – TRIP) da Organização da Aviação Civil Internacional (OACI) e o One ID da Associação Internacional do Transporte Aéreo (IATA). (Brasil, 202?-)

Atualmente, o Serpro indica que o sistema vem sendo utilizado nos aeroportos Santos Dumont e Congonhas (SP). Aponta também que a utilização das informações alinha-se à Lei Geral de Proteção de Dados, pois “atende às necessidades de segurança pública e defesa nacional e o compartilhamento de informações só é possível mediante convênio prévio entre os órgãos” [32]. O que o Serpro não diz na página do projeto é que a tecnologia é desenvolvida em parceria

[31]Disponível em https://campanhas.serpro.gov.br/embarque-mais-seguro/#menu Acesso em: 20 out. 2022.

[32]A segurança pública e o controle fronteiriço configuram algumas das exceções da LGPD.

com uma outra empresa, a IDEMIA. Em sua página web, a IDEMIA[33] (202-) aponta que sua missão é abrir o mundo e fazer dele um lugar mais seguro, a partir de suas tecnologias para verificação de identidade. Segundo a companhia, são utilizadas por governos em mais de 180 países. No caso das tecnologias que envolvem biometria, a companhia oferece soluções com reconhecimento facial, de íris e digitais. Segundo a empresa,

> Em 2021, nosso algoritmo 1:N de reconhecimento facial obteve os melhores resultados de precisão entre 75 sistemas testados e 281 participantes durante o Teste de Fornecedor de Reconhecimento Facial ("FRVT", que mede a precisão de algoritmos de identificação um para muitos pesquisando galerias inscritas contendo pelo menos 10 milhões de identidades). O relatório também observa que os vieses demográficos são indetectáveis em nossos algoritmos de identificação facial (Idemia, 202-, tradução nossa).

Vale ressaltar que o uso de tecnologias de identificação biométrica pelo setor público faz muitas vezes com que as pessoas não possam recusar a coleta de dados pessoais, por dependerem dessas tecnologias para acessar seus direitos ou porque essas ferramentas fazem parte da política de segurança estatal.

> Além disso, e talvez o mais importante de tudo, é que, quando essas tecnologias são utilizadas pelo setor público, na maioria das vezes, as pessoas simplesmente não têm a opção de recusar a coleta de seus dados biométricos, nem tão pouco de recusar o escrutínio das câmeras de vigilância por se tratar de uma política de segurança de Estado, mesmo quando se trata, por exemplo, dos termos de uso das plataformas e aplicativos produzidos pelo governo, ou seja, os termos de aplicativos como meugov.br, e outros, são compulsórios. Caso o usuário se negue a aceitá-los, o uso da plataforma é negado, não havendo outra possibilidade a não ser entregar os dados pessoais para acessar os mais variados serviços públicos. Nesse sentido, a própria cidadania fica restrita à obrigatoriedade dos termos de uso destas plataformas, não se tem o poder de dizer não, portanto, não há consentimento real. Em outras palavras, trata-se de condicionalidade na promoção da cidadania, onde se tem pouca ou nenhuma opção de receber um determinado serviço público (Silva; Varon, 2021, p. 34)

Além do uso para autenticação de usuários, as TRFs têm sido usadas em outros tipos de serviços públicos, como a educação e a segurança.

Empresas que oferecem tecnologias de segurança, como demonstrarei adiante, têm se tornado cada vez mais importantes na operacionalização de

[33] Disponível em https://www.idemia.com/our-technologies. Acesso em: 20 out. 2022.

atividades estatais e uma normatividade da lógica neoliberal acaba por ser incorporada aos *softwares*, mapas georreferenciados e metadados (Cardoso, 2018). Contudo, vale destacar que essa lógica não afeta apenas a segurança pública, mas também outros setores, como a educação. A adoção de ferramentas de reconhecimento facial em diversas áreas, para supostamente otimizar processos e baratear custos, parte dessa lógica.

Na educação, diversas cidades têm adotado tecnologias de reconhecimento facial para controle de frequência de estudantes. Segundo matéria de 2017 do jornal O Estado de São Paulo, a Escola Politécnica da Universidade de São Paulo testava um novo sistema de câmeras com capacidade para reconhecer rostos e objetos. Trata-se de uma pesquisa acadêmica da universidade, realizada pelo professor Moacyr Martucci Jr em parceria com a Huawei. O projeto tinha a ambição de, em até dois anos, integrar o sistema às demais câmeras de todas as unidades do campus universitário (Toledo, 2017).

Outra matéria, agora da jornalista Charlotte Peet (2021), aponta que a PontoID é pioneira no desenvolvimento de tecnologias de reconhecimento facial para a educação e está presente em 19 dos 26 estados brasileiros. A prefeitura de Mata de São João, na Bahia, adotou tecnologia de reconhecimento facial oferecida pela empresa PontoID em, inicialmente, duas escolas, por meio de contrato celebrado no valor de R$900.000,00. Segundo a companhia, trata-se de um sistema de controle da frequência dos alunos, sem que seja necessária a realização de chamadas em sala de aula. Promete diminuir a evasão escolar; reduzir o uso de papel; controlar, de modo mais eficiente, a merenda; centralizar informações e tranquilizar os pais. A mesma empresa também oferece outras soluções voltadas para o controle de ponto de funcionários públicos. Oriunda de Goiânia, a empresa também tem escritório na Flórida, EUA (PontoID, 2022). Nova Venécia, no Espírito Santo, testou o reconhecimento facial em escolas públicas, em 2018. Os pais eram comunicados a respeito da presença dos filhos por mensagens de SMS (Sena; Borges, 2018).

Já em Goiás, em agosto de 2021, o governo estadual celebrou o que seria a primeira escola pública do país com reconhecimento facial[34]. A inauguração do Colégio Estadual Rocha Leal, em Águas Lindas, contou com a presença do

[34]Aparentemente, o governador não estava muito atualizado a respeito do tema e da difusão da empresa PontoID no país.

presidente do Fundo Nacional de Desenvolvimento da Educação, Marcelo Ponte; representante do ministro da Educação, Milton Ribeiro; governador do estado, Ronaldo Caiado; do deputado federal José Nelto; do prefeito de Águas Lindas, Lucas Antonietti; e da secretária estadual de Educação, professora Aparecida Gavioli (Brasil, 2021). Segundo Caiado,

> Os estudantes chegam na escola, já são identificados, é verificada a temperatura e os pais recebem no celular a informação de que os alunos estão na escola. A informação também vai, imediatamente, para o refeitório da escola, para não haver desperdício nenhum de alimentação escolar (Caiado *apud* Brasil, 2021).

No setor público, é bastante difícil dissociar a presença de câmeras de videovigilância e o reconhecimento facial. A tabela 5 apresenta o número de câmeras de vigilância, o cálculo de câmeras per capita, tamanho da cidade em km e o *crime index*[35] de 10 cidades brasileiras.

Tabela 5: Quantitativo de câmeras em 10 cidades brasileiras

Cidade	Nº de câmeras	Cidadãos (2022)	Nº de câmeras por 1000 pessoas	Tamanho da cidade em milhas	Câmeras por milha² aproximadamente	Crime Index (2022)
Rio de Janeiro	45,571	13.63M	3.34	2,057	22	78
São Paulo	23,415	22.43M	1.04	3,068	8	70
Salvador	5,710	3.92M	1.46	1,681	3	75
Recife	2,080	4.22M	0.49	1,071	2	76
Brasília	3,832	4.8M	0.80	2,240	2	60
Fortaleza	3,033	4.16M	0.73	2,237	1	78
Porto Alegre	2,871	4.19M	0.69	3,785	1	74
Belo Horizonte	3,655	6.19M	0.59	5,568	1	64
Curitiba	3,260	3.77M	0.86	5,953	1	62
Campinas	769	3.77M	0.23	1,407	1	67

Fonte: Bischoff (2022)

[35]Indicador baseado em taxa de criminalidade por 1000 habitantes. O índice vai de 0 a 100, em que 0 é mais seguro e 100 significa maior ocorrência de crimes.

Em 2018, o governo do Estado da Bahia utilizou câmeras de reconhecimento facial no carnaval de Salvador, parcialmente compradas da Huawei por cerca de 18 milhões de Reais. Em 2021, um contrato no valor de 131 milhões de Dólares foi assinado com a empresa de telefonia Oi para operar as câmeras da Huawei, depois dos testes realizados na Capital do Estado da Bahia. O plano era estender a utilização da tecnologia para 77 cidades do estado (Peet, 2021), o que já foi feito (Bahia, 2023). Voltarei neste contrato em breve.

O Rio de Janeiro começou a usar o reconhecimento facial em 2019, em um programa experimental que espalhou 28 câmeras no bairro de Copacabana, com o objetivo de identificar veículos roubados e indivíduos foragidos. A Praia de Copacabana, um dos pontos turísticos mais visitados do país, já havia sido objeto de programa de videomonitoramento (Cardoso, 2013). O banco de dados estava conectado com os registros do Detran e da Polícia Civil (Bom Dia Rio, 2019).

Ainda na Segurança Pública, levantamento realizado pelo Centro de Estudo de Segurança [illegible] nhecimento facial foi usada na Se[illegible]btidos em outubro de 2022

Figura 16: Reconhecimento facial na Segurança Pública

Fonte: Centro de Estudo de Segurança e Cidadania (2022).

A figura 5, apresentada anteriormente, mostra os casos apresentados no *Panóptico*[36], projeto do CESec que objetiva monitorar a adoção de tecnologias de reconhecimento facial na Segurança Pública.

[36] Disponível em https://opanoptico.com.br/sobre/. Acesso em: 18 out. 2022.

Com base no argumento de que cabe aos governantes a garantia da proteção física e da propriedade dos cidadãos (Cardoso, 2013), tecnologias de reconhecimento facial têm sido adotadas na Segurança Pública em muitas esferas. Bruno Cardoso (2014) indica a existência de um modelo gerencial-militarizado e Graham (2016) aponta que esse modelo é implementado em ações de militarização do cotidiano.

O Estado e o mercado têm estabelecido uma relação simbiótica (Bauman, 2012). Nela, há uma série de externalidades, ou seja, “custos (ou benefícios) que não oneram (ou não favorecem) o agente que os causa, mas sim a economia e a sociedade como um todo” (Carvalho, 2018). Dentre elas, pode haver externalidades positivas ou negativas. As atividades que provocam externalidades positivas, entretanto, compreendem ganhos sociais que suplantam a soma dos ganhos privados envolvidos.

Companhias que oferecem soluções tecnológicas de segurança são parceiras indispensáveis dos “órgãos públicos responsáveis pela construção e coordenação tanto dos centros locais quanto do sistema integrado” (Cardoso, 2018) de videovigilância que posteriormente serão usados para reconhecimento facial. Em 2023, a empresa Gabriel, que oferece soluções de tecnologias com reconhecimento facial para condomínios, empresas e casas anteriormente citada foi alvo de reportagem do veículo jornalístico Intercept, pois a empresa tinha uma “rede de informações clandestinas pelo whatsapp com a polícia do Rio” (Ribeiro, 2023). Segundo a reportagem de Paulo Victor Ribeiro (2023) para o Intercept, a iniciativa da colaboração entre a Gabriel e a polícia partiu da própria PM do Rio de Janeiro e a relação localiza-se em um obscuro lugar com relações ambíguas entre empresas privadas e corporações e de difícil fiscalização.

Outra reportagem do Intercept, de Laís Martins (2023), mostrou como a ClearView AI tem tentado vender seu sistema de reconhecimento facial para autoridades brasileiras. Kashmir Hill (2023) demonstra como a empresa tem se espalhado pelo mundo, ao oferecer bases de dados com faces coletadas de redes sociais. Para a autora, a Clearview AI representa os piores medos, mas também uma oportunidade para encarar o problema do reconhecimento facial no mundo.

Empresas de tecnologia têm operado um estado de bem-estar social paralelo e privatizado em diversos países, em uma lógica de racionalidade neoliberal

(Morozov; Bria, 2019). Isto está inserido na percepção de que a gestão estatal é similar à de uma empresa em doutrina chamada de *new public management* (Hood; Dardot; Laval; *apud* Cardoso, 2018). Esses discursos funcionam como uma estratégia para a norma neoliberal de reestruturação do Estado no Brasil, o que, na segurança, ganha contornos próprios que envolvem diferentes tipos de órgãos públicos e privados em relações complexas que também envolvem tensões e ambiguidades (Cardoso, 2018).

No transporte público, o estado de São Paulo oferece uma diversidade de exemplos. Aponta-se que a utilização do reconhecimento facial em ônibus ajudou a coibir fraudes, o que gerou o bloqueio de 331.000 bilhetes únicos que eram usados por terceiros para acessar os benefícios da gratuidade de idosos e pessoas com deficiência, além dos descontos de tarifa estudantis.

No metrô paulista, a tecnologia de reconhecimento facial foi implementada em 2018. As expressões faciais detectadas eram reconhecidas e os anúncios exibidos adaptavam-se ao humor dos passageiros identificados, sendo o sistema capaz de reconhecer idade e gênero, além de classificação das emoções em quatro categorias: feliz; insatisfeito; surpreso; ou neutro. A empresa responsável era a Via Quatro,[37] que implementou o sistema em parceria com a LG, multinacional do ramo de eletrônicos, e a Hypera Pharma, farmacêutica Brasileira. A ação de publicidade foi interrompida após ação civil do Instituto Brasileiro de Defesa do Consumidor, que alegou falta de consentimento dos passageiros.

Em 2019, a Via Quatro quis instalar um novo sistema de monitoramento com reconhecimento facial na linha amarela do metrô de São Paulo. O número de câmeras instaladas aumentou exponencialmente e havia a opção de vincular com o sistema aos bancos de dados da Secretaria de Segurança Pública de SP. A companhia alegou que o sistema auxilia na busca de foragidos e de crianças perdidas que estejam a circular pela linha, além de compor a segurança antiterrorista, por detectar objetos suspeitos (Taute, 2020).

No mesmo ano, ocorreu a licitação realizada pelo Governo de São Paulo para a expansão do sistema de monitoramento de estações, trens e áreas de operação, de 2,2 mil para 5,2 mil câmeras nas linhas 1 – azul, 2 – vermelha e 3 – verde. O objetivo era eliminar câmeras analógicas e adicionar o reconhecimento facial. O

[37] A Via Quatro é a concessionária responsável pela linha amarela do metrô de São Paulo, a primeira sob o modelo parceria público-privado no país. A empresa detém a concessão por 30 anos.

consórcio vencedor, Engie Ineo Johnson, apresentou proposta no valor de R$58,6 milhões, mas um grupo formado pela Defensoria Pública e por associações entrou com uma ação judicial para exigir maior transparência quanto à segurança dos dados de cerca de 3,7 milhões de passageiros do metrô paulistano (Ortega, 2020).

A Secretaria de Estado da Assistência e Desenvolvimento Social de Alagoas, em parceria com os municípios do estado, implementou um sistema de reconhecimento facial no programa de entrega de cestas nutricionais, com o objetivo de dar maior transparência e agilidade ao Programa de Complementação Alimentar e Nutricional das Gestantes e Nutrizes (Sobral, 2018).

Na gestão de dados de utilizadores com objetivos comerciais, políticos e sociais de tecnologias que envolvem algoritmos, é possível observar o *lobby* de grandes corporações e os interesses políticos do neoliberalismo, arriscando democracias, as possibilidades de autogestão e até mesmo a autodeterminação de gênero e de sexualidade no Brasil (Silva; Varon, 2021).

A instrumentalização de dados pessoais e de tecnologias de IA por parte de governos, atualmente, também está relacionada com a desapropriação de dados (Pereira; Couldry, 2023).

Para buscar melhor conhecer a implementação de sistemas de reconhecimento facial por estados brasileiros, realizei uma série de perguntas via 85 pedidos de dados pela Lei de Acesso à Informação, entregues aos 26 estados e ao DF nas pastas de Educação e Segurança pública. Na segurança pública, dirigi os pedidos para secretarias e polícias, a depender da configuração administrativa do ente da federação. O modelo utilizado para os pedidos de acesso pode ser visto no anexo A.

Apresento, nas figuras 17 e 18, um resumo a partir dos pedidos de acesso realizados em 2023. A figura 17 é o mapa do uso de ferramentas de reconhecimento facial na educação.

Figura 17: Mapa do reconhecimento facial na Educação

Fonte: Elaboração própria (2024).

Legenda da Figura 17:
Verde – Tem reconhecimento facial.
Vermelho – Não tem reconhecimento facial.
Amarelo – Projeto de implementação de reconhecimento facial em estudo.
Laranja – Resposta inconclusiva.

A seguir, na figura 18, apresento o mapa feito a partir dos pedidos de acesso para órgãos de Segurança Pública.

Figura 18: Mapa do reconhecimento facial na Segurança Pública

Fonte: Elaboração própria (2024).

Legenda da Figura 18:
Verde – Tem reconhecimento facial.
Vermelho – Não tem reconhecimento facial.
Amarelo – Projeto de implementação de reconhecimento facial em estudo.
Laranja – Resposta inconclusiva.

Foram inconclusivas as respostas da Educação do Amapá, Bahia, Maranhão, Pará, Pernambuco, Piauí e Santa Catarina. Na Segurança Pública, obtivemos esse resultado inconcluso no Maranhão, Minas Gerais, Piauí e Santa Catarina. Considerei inconclusivos aqueles estados cuja resposta foi incompreensível ou ocorreu a negativa de acesso; onde não houve resposta ao pedido ou quando não consegui solicitar a informação.

Foram 13 os estados que afirmaram, por meio dos pedidos de acesso, utilizar tecnologias de reconhecimento facial na Educação e/ou Segurança Pública, até 2023. Na Educação, foram quatro estados: Goiás, Mato Grosso, Paraná e Tocantins. Na Segurança Pública, confirmaram o uso Bahia, Ceará, Goiás, Pará, Paraíba, Rio de Janeiro, Rio Grande do Norte, Rio Grande do Sul e o Distrito Federal.

São Paulo utiliza a ferramenta para produção de identidades, que é responsabilidade da Polícia Civil. O Rio Grande do Norte informou que tem a tecnologia, mas que está fora de uso.

São oito os estados que afirmaram estar estudando a adoção de TRFs. Na educação: Acre, Espírito Santo, Mato Grosso do Sul, Rondônia, São Paulo e Sergipe. Na segurança pública: Espírito Santo, Mato Grosso e Roraima.

Meu objetivo, ao realizar os pedidos de acesso, era tentar identificar se há projetos de reconhecimento facial em andamento; a quantidade de câmeras em uso; qual é o custo mensal da tecnologia; que empresa prestou e presta serviço na instalação e manutenção das câmeras em funcionamento; ter informações sobre contratos e informações; além disso, quem desenvolveu o sistema de reconhecimento facial e que bases de dados são utilizadas para que o sistema realize o cruzamento de informações; nos casos em que não há, perguntei também sobre se há estudos para sua adoção.

Dos órgãos que responderam “sim” para o uso de ferramentas de reconhecimento facial, foram poucos os que responderam integralmente ao pedido de informação. Alguns pedidos foram absolutamente evasivos, ficando até mesmo difícil compreender se há ou não ferramentas de reconhecimento facial em utilização. Houve também estado que negou ter uso ou estudo, mas implementou TRFs meses depois da resposta, como o Estado de Sergipe. O pedido respondido em abril de 2023 dizia não ter uso ou projeto para a adoção, contudo, em novembro de 2023, 27 câmeras foram utilizadas com o objetivo de identificar pessoas com mandados de prisão e medidas cautelares por cumprir (Reconhecimento..., 2023).

Além disso, vale destacar que diversos estados recebem os pedidos de acesso pelas Ouvidorias que marcam o pedido como encerrado, após o encaminhamento para o órgão competente. Dessa maneira, eles “cumprem” a lei por terem supostamente respondido no prazo, enquanto as respostas dos pedidos não chegam.

Aliás, os pedidos de acesso à informação são, por si só, um tema interessante. As páginas são pouco amigáveis, cadastros complexos, dificuldade de saber para qual órgão mandar a demanda em muitos casos. Também há respostas negadas por motivos diversos, como segurança pública ou falta de pessoal para responder, o que remete ao arbítrio de quem é responsável pela resposta. Tive pedidos parcialmente negados ou completamente negados, enquanto obtive a resposta de pedido com o mesmo teor de outros estados.

Segurança pública não é, necessariamente, um motivo para negar pedidos de acesso. Na realidade, ele deveria ser a norma e o sigilo a exceção. Ao menos, isso é o que preconiza a lei. Sem contar o desrespeito ao prazo de resposta, que é frequente, sem que o solicitante seja avisado. A resposta de alguns pedidos não chegou após sete meses. Encontrei problemas também com a migração de sites para pedidos de acesso, o que deixou as páginas antigas indisponíveis; com isso, meus pedidos de acesso se tornaram inacessíveis.

A seguir, apresento os custos da adoção de TRFs nos estados. Os dados foram obtidos por meio dos pedidos de acesso à informação ou na imprensa.

4.2.1 Quanto vale ou é por quilo? Gastos estaduais com ferramentas de reconhecimento facial

Do mesmo modo que não foi fácil identificar se órgãos estão ou não utilizando tecnologias de reconhecimento facial, foi difícil conhecer os custos desses projetos. Para o levantamento dessas informações, a principal fonte foi a imprensa, pois representantes do Executivo a usam como forma de propaganda dos investimentos feitos. Ainda assim, foi árduo rastrear os contratos relacionados ao uso de TRFs e verificar se os valores foram mesmo empenhados ou eram só publicidade. Nos pedidos de acesso à informação, apenas Bahia, Goiás, DF, Paraná e Tocantins informaram-me sobre os custos ou contratos sob os quais estão regidos os gastos.

Solicitei aos estados os valores gastos com as tecnologias de reconhecimento facial. Alguns poucos, como a Segurança Pública da Bahia e a do Rio Grande do Sul, informaram os custos da tecnologia. Outros, como a Educação de Goiás e a do Paraná, responderam com os números de contratos que eu poderia encontrar no Portal da Transparência, o que me levou à busca seguinte, feita para localizar contratos nos portais da transparência estaduais.

A falta de transparência nos contratos remete às ideias de Rafael Zanatta (2019) sobre a necessidade de transformar contratos públicos que envolvam tecnologia para “favorecer o uso mais estratégico, eficiente e transparente de recursos públicos e de investimentos no governo” (Zanatta, 2019).

Conseguir informações sobre a adoção de TRFs nem sempre é uma tarefa fácil, conforme pode ser visto nas negativas de pedidos de acesso à informação feitas por mim (negadas duas vezes pelo Maranhão) ou pela reportagem do G1 da Bahia, cuja solicitação de dados sobre a quantidade de falsos positivos (Alencar, 2023) não foi respondida pela Secretaria de Segurança Pública estadual. A Bahia tem sido pioneira no uso de TRFs. Em funcionamento desde 2018, o sistema que custou R$665 milhões prendeu 1011 pessoas (Franco, 2023). Como o estado não divulgou a proporção de falsos positivos, não é possível saber quantas dessas prisões foram injustas. É aí que a caixa-preta dos dados se encontra com outra caixa-preta, que é a da segurança pública, que encontra a outra caixa-preta, que é a da transparência governamental.

Assumo aqui o fracasso[38]: eu não consegui obter acesso aos dados de todos os estados. Por isso, tentarei apresentar adiante os poucos dados coletados por mim nos pedidos de acesso à informação e também obtidos na base de dados do Panóptico (2024).

Recebi respostas evasivas, que afirmam que a tecnologia não tem custo, como nos casos dos estados do Ceará e do Rio de Janeiro. No Ceará, a resposta ao meu pedido de acesso afirma que foi desenvolvida em parceria com a Universidade Federal do Ceará e é sem custo. Honestamente, eu não consigo compreender como uma ferramenta do gênero pode ser utilizada pelo estado sem custo de manutenção ou instalação.

No Rio de Janeiro, segundo a resposta obtida por meio da Lei de Acesso à Informação, os equipamentos foram doados “pelo Gabinete de Intervenção Federal para a SEAP-RJ - Termo de Doação no 65 GIFRJ, de 03 de março de 2020 - Processo Administrativo no 00144.003762/2018-61. Portanto, não há custo mensal”. A empresa responsável pelo desenvolvimento do sistema foi Hikvision Digital Technology Co. A empresa responsável pela instalação e manutenção das câmeras é a Empresa Emive Patrulha 24 Horas LTDA. São 1.734 câmeras em 54 locais. Contudo, a Polícia Militar do Rio de Janeiro realizou, em setembro de 2023, pregão para contratação de empresa especializada em videomonitoramento. Venceu a licitação o L8 *GROUP* S/A. A licitação objetivava contratar empresa especializada para a Solução Integrada e Equipamentos para Videomonitoramento Analítico Centralizado no Centro Integrado de Comando e Controle. Criado em 2014, o L8 *Group* oferece tecnologias voltadas para segurança pública e cidades inteligentes e o valor final do lance foi R$ 4.700.000,00. A empresa tem filial em diversas cidades brasileiras e na Flórida (L8 *Group*, 2024)[39].

O pedido de acesso à informação, feito para a Secretaria de Segurança Pública da Bahia, obteve a informação de que o valor gasto na tecnologia de reconhecimento facial é de R$665 milhões por cinco anos, no Projeto Vídeo Polícia Expansão. Em abril de 2023, eram 2.974 pontos de imagens (reconhecimento facial, reconhecimento de placas de veículos e de análise situacional) que atendiam a Capital, a região metropolitana de Salvador e 77 municípios baianos. O consórcio OI

[38] Será meu ou do Estado brasileiro que falha em garantir o acesso à informação? De todo modo, vale o Poema em Linha Reta, de Álvaro de Campos (pseudônimo de Fernando Pessoa): Nunca conheci quem tivesse levado porrada./ Todos os meus conhecidos têm sido campeões em tudo.
[39] L8 Group: https://www.l8group.net/l8-group/

e Avantia ganhou e a fabricante da solução (câmeras e *software* de reconhecimento facial) foi a empresa Huawei.

Em Goiás, o projeto em andamento é na Educação, sob um contrato de R$9.532.300,00 e envolve o uso de 680/689 câmeras em escolas estaduais. O dinheiro utilizado é oriundo de recursos do FUNDEB, o Fundo de Manutenção e Desenvolvimento da Educação Básica e de Valorização dos Profissionais da Educação.

Na Segurança Pública do Rio Grande do Sul, são pagos R$886,00 mensais pela licença de cada uma das 20 câmeras. Em um mês, o somatório das licenças representa R$17.720,00. Se multiplicado por 12 meses, são R$ 212.640,00 pela licença anual das câmeras. Em cinco anos, são R$1.063.200,00.

No Tocantins, por meio da LAI, fui informada que na educação há uso de TRF no valor de R$19.064.600 por 12 meses. Na Segurança Pública, a página do Governo Estadual anunciou projeto de R$15,8 milhões O prazo de vigência da contratação é de 48 meses e a empresa tem um ano para implantação (Cardoso, 2023).

A Polícia Civil do DF contratou desenvolvimento de sistema ABIS da empresa Gemalto do Brasil Cartões e Terminais LTDA, sob o contrato 00052-0000002218/2016-00 no valor de R$ 11.229.924,19. Contudo, a empresa informada pelo pedido de acesso tinha outro nome. Segundo a pessoa responsável por responder a solicitação, a empresa fornecedora era a Thales Dis Brasil Cartões e Soluções de Tecnologia Ltda.

Os contratos para implementação de reconhecimento facial são firmados com empresas de pequeno e médio porte ou com as grandes corporações, como a IBM, que também fazem parte do aparato de vigilância, a exemplo do que ocorre no Comando de Controle Integrado da Prefeitura do Rio de Janeiro, analisado por Lalita Kraus, Fabiola de Cássia Freitas Neves e Adenilson dos Santos Vitorino Costa (2022). Já o Estado da Bahia utiliza a tecnologia da Huawei, conforme pôde ser visto no pedido de aceso à informação realizado em março e respondido em abril de 2023. O oferecimento de serviços relacionados às ferramentas de reconhecimento facial acaba por ficar concentrado em grupo relativamente pequeno de empresas, como alerta a economista Laura Carvalho (2018).

> O poder de monopólio existe por diversos fatores, entre os quais o alto volume de investimentos necessários para a prestação do serviço (como no caso da construção da rede de distribuição de energia elétrica) e as economias e ganhos de produtividade gerados quando a mesma empresa oferece o serviço para uma grande parcela do mercado. Tudo isso acaba fazendo com que o mercado seja dominado por uma única empresa ou por um pequeno número de empresas que, na ausência de controle ou regulação, teriam o poder de cobrar o preço que quisessem. (Carvalho, 2018)

Ladislau Dowbor (2022) argumenta que a dominação do jogo econômico na atualidade está nos sistemas de controle financeiro e tecnológico com empresas como o Google, a Apple, a Meta, a Amazon, a Microsoft nos Estados Unidos; e Baidu, Alibaba e Tencent na China e nas Instituições Financeiras de Importância Sistêmica, colocando no centro da economia as plataformas, os gestores de fortunas e os controladores das tecnologias que envolvem a comunicação e as informações pessoais.

A tendência é que cada vez mais tecnologias orientadas para a vigilância ocupem os espaços públicos e privados, conforme pôde ser visto por meio dos dados apresentados. Seus custos também são cada vez mais elevados, sem que seja possível comprovar sua eficácia. Além disso, no caso do reconhecimento facial, é possível observar que muitos projetos acontecem nos municípios (Nunes; Lima; Rodrigues, 2023), tornando sua fiscalização mais difícil.

Nesse contexto, como resistir coletivamente para pensar em futuros alternativos? É uma pergunta que tentarei responder no sexto capítulo, depois de apresentar, a seguir, considerações a respeito dos problemas éticos do uso de ferramentas de reconhecimento facial.

5 PROBLEMAS ÉTICOS DO RECONHECIMENTO FACIAL NO MUNDO REAL

Thais Santos, 31 anos, foi abordada pela polícia, após a ferramenta de reconhecimento facial utilizada em uma micareta, em Aracaju, errar ao reconhecê-la como foragida da justiça. Aliás, foi duas vezes erroneamente abordada. Na segunda, os policiais a levaram. Thais, muito nervosa, relata ter urinado em si e que nunca se sentiu tão humilhada na vida. No evento, foram utilizadas 27 câmeras com reconhecimento facial. Segundo a PM, elas auxiliaram na prisão de três outras pessoas[40]. No caso das prisões realizadas no evento em Aracaju, a tecnologia teve 25% de erro. Pouco ou muito, isso certamente marcará a vida de Thais, que era inocente.

Ao utilizar discursos que disseminamo medo da violência, a indústria de segurança passa a investir em inovações tecnológicas "para criar e comercializar sistemas cada vez mais sofisticados e, em teoria, menos custosos", cujas promessas seduzem rapidamente os consumidores e cidadãos (Cardoso, 2014, p. 40). O videomonitoramento se consolidou e tecnologias de reconhecimento facial têm aparecido, com frequência, como uma proposta de solução para a segurança pública.

Algumas das utilizações são vistas com otimismo por alguns, apesar de ser cedo para classificar sua adoção em algumas localidades. Por exemplo, o uso de câmeras em uniformes por parte de agentes policiais, o que supostamente favorece a fiscalização de suas condutas (Gortázar, 2021; Preite Sobrinho, 2022). Contudo, o otimismo tem dado lugar à descrença, pois crescem as denúncias de que policiais vêm burlando as câmeras corporais (Nascimento, 2023; Adorno, 2023). Além disso, a incorporação de reconhecimento facial às câmeras corporais também é fator de preocupação.

Desde 2011, o reconhecimento facial tem sido adotado no Brasil. Até 2019, ferramentas de reconhecimento facial já haviam sido implementadas em 47 casos, em 37 cidades diferentes no setor público, conforme estudo do Instituto Igarapé (2022), que pôde ser visto melhor no capítulo que apresentou o panorama do reconhecimento facial no Brasil e no mundo. Em 2023, estudo do Panóptico (2023) indica que 165 projetos que utilizam técnicas de reconhecimento facial estiveram ou

[40] Para mais informações, acessar a matéria do Uol. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2023/11/15/erro-camera-reconhecimento-facial.htm. Acesso em: 14 jan. 2023.

estão em uso ou em estudo no país. Destes, 155 estão ativos. Isso significa dizer que 47.589.925 pessoas são potencialmente vigiadas por esse tipo de tecnologia.

Apesar de muitas preocupações estarem dirigidas ao modo como o reconhecimento facial é utilizado na segurança pública, é possível observar que ele também é adotado na educação, nos transportes e nos controles fronteiriços. Até 2019, era no setor de transportes que a tecnologia tinha maior força, objetivando combater fraudes nos transportes públicos (Instituto Igarapé, 2022), o que tem mudado, pois têm crescido os projetos na educação.

A questão que envolve a utilização do reconhecimento facial em setores diversos esbarra no que é denominado "*control creep" (*Kelleher; Tierney, 2018, p. 197), ou seja, a transferência de dados para outros fins que não os originais. A lei 1.3709/2018, também conhecida como Lei Geral de Proteção de Dados Pessoais, preconiza que os fundamentos da proteção de dados pessoais envolvem o respeito à privacidade; à autodeterminação informativa; à liberdade de expressão, de informação, de comunicação e de opinião; à inviolabilidade da intimidade, da honra e da imagem; ao desenvolvimento econômico e tecnológico e à inovação; à livre iniciativa, à livre concorrência e à defesa do consumidor; aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania pelas pessoas naturais. Contudo, o Artigo 4º diz que a lei não é aplicável ao tratamento de dados pessoais em quatro casos: a) segurança pública; b) segurança nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais (Brasil, 2018).

São muitos os exemplos que têm demonstrado erros derivados da adoção de ferramentas de reconhecimento facial no Brasil e no mundo. No Rio de Janeiro, durante uma partida no Maracanã, foram realizadas 11 detenções com o uso do reconhecimento biométrico. Em 63% delas, ou seja, sete delas, ocorreram falsos positivos, conforme pode ser visto em levantamento realizado por Pablo Nunes, Mariah Silva e Samuel Oliveira (2022), por meio da Lei de Acesso à Informação. Outro caso é o de uma mulher que foi levada para a delegacia após ter sido identificada pelas câmeras, no bairro de Copacabana. Na delegacia, sua identidade foi confirmada e provou-se que se tratava de um falso positivo (Sistema..., 2019).

Em Londres, Grã-Bretanha, o sistema de reconhecimento facial errava em 81% dos casos (Jee, 2019). Esses não são os únicos exemplos e é importante destacar que uma prisão errada afeta profundamente a vida da pessoa envolvida.

Essa é uma das razões que realça a importância do debate a respeito das implicações da adoção do reconhecimento facial na contemporaneidade.

A adoção de ferramentas de reconhecimento biométrico no país tem lugar em um cenário com um número grande de problemas preexistentes. Portanto, os resultados podem não ser os prometidos, mas, ao contrário, ampliar as desigualdades que já existem em nossa sociedade. Por exemplo, em 2019, cerca de 90% dos presos por reconhecimento facial no país eram negros (Nunes, 2019). Estatística apenas um pouco superior ao reconhecimento por foto resultante em falhas, que acontece em delegacias brasileiras: 83% dos presos injustamente por reconhecimento fotográfico, mediante catálogos de pessoas identificadas, são negros (Exclusivo..., 2021).

Outro problema a ser destacado é a desproporcionalidade da vigilância para o resultado modesto. Por exemplo, 1,3 milhões de rostos foram mapeados para o cumprimento de apenas 18 mandados de prisão, na Micareta de Feira de Santana, na Bahia. Deve-se considerar a capacidade dos fornecedores desse tipo de tecnologia para promover a auditoria de seus próprios sistemas, delimitar a aceitação de taxas de erro e os meios de instalação e venda. Além disso, a forma como os compradores do governo analisam ou aceitam esses erros deve ser percebida como tão ou mais importante que os índices métricos de acurácia ou erro das ferramentas (Silva, 2021). Afinal, a sociedade brasileira, estruturalmente racista e marcada pela seletividade penal, acabará por servir à ampliação do encarceramento de grupos sociais específicos já submetidos a esse processo, conforme alerta Tarcízio Silva (2021). Na era do *big data*, muitos continuam monitorados. O fato de as estratégias terem mudado não quer dizer que os problemas tenham desaparecido (Benjamin, 2019).

Observa-se, no Brasil, a ausência de regulamentação que considere princípios como proporcionalidade, finalidade, consentimento e transparência para orientar a implementação e promover a salvaguarda do exercício de direitos democráticos, como os de ir e vir, da liberdade de expressão, privacidade e liberdades das pessoas (Instituto Igarapé, 2022). As leis e projetos em andamento direcionam-se mais no sentido de regularizar ou implementar o que já está em andamento do que necessariamente regulamentar o uso da tecnologia de reconhecimento facial, o que se expressa na presença de apenas três propostas federais nesse sentido.

O uso de tecnologias de reconhecimento facial é marcado por críticas. A ausência de transparência pode ser identificada em diversos aspectos: por trás dos algoritmos utilizados nas ferramentas e até mesmo a respeito dos resultados obtidos com sua implementação. A falta de transparência que “pode ser identificada em diversos aspectos: por trás dos algoritmos utilizados nas ferramentas e até mesmo a respeito dos resultados obtidos com sua implementação (Silva, 2022).

Para Samuel de Oliveira (2021), o uso da tecnologia de reconhecimento facial pode levar à violação do direito fundamental à privacidade e a decisões algorítmicas enviesadas. Duas questões devem ser consideradas, durante o desenvolvimento dessas tecnologias: primeiramente, as demandas sociais no que tange à segurança, pois o reconhecimento facial tem aparecido como uma forma de reconhecer suspeitos e/ou foragidos; a segunda remete aos dados utilizados por essas ferramentas, devendo-se questionar a sua forma de coleta. Ainda assim, o autor reconhece os benefícios da tecnologia, pois tem o potencial de “acessar serviços, tanto públicos, quanto privados, atendendo a interesses dos próprios sujeitos, em decorrência de uma comodidade e eficiência” (Oliveira, 2021, p. 9).

> Inicialmente como instrumentos de vigilância que retiram das pessoas a capacidade de manter seu direito à privacidade plenamente resguardado, os sistemas de reconhecimento facial apresentam, outrossim, uma ameaça à liberdade individual, por criar um efeito inibitório - chilling effect - no exercício de determinados direitos. […] investigar quais os efeitos que o uso de tais tecnologias invasivas e omnipresentes impõem no pleno exercício de direitos de natureza fundamental, sendo o direito de proteção de dados pessoais incluído nessa categoria (Oliveira, 2021, p. 10).

Apesar de seus aspectos negativos, reconheço que as tecnologias não são boas ou más, mas servem a propósitos determinados dentro de contextos específicos. Contudo, apesar das tecnologias serem defendidas com base na ideia de que podem ser usadas para o bem ou para o mal, isso não faz delas neutras e menos complexas, conforme lembra Kashmir Hill (2023). Não se trata, portanto, de apenas demonizar a utilização do reconhecimento facial, mas de aferir seus impactos para compreender se o uso desse tipo de ferramenta faz sentido no Brasil, quiçá, no mundo, porque é apenas a partir das experiências concretas que seus impactos podem ser medidos. E isso só pode ser feito a partir de uma análise que considere contextos específicos, conforme preconiza a ética intercultural da informação.

Quando o assunto é reconhecimento facial, há dois tipos de erros: os falsos positivos e os falsos negativos. Os falsos positivos são aqueles cujo reconhecimento é de uma pessoa que não é. Ou seja, um rosto é erroneamente identificado como outro que consta em uma base de dados determinada. Já os falsos negativos são aqueles em que uma pessoa que é não tem seu rosto identificado com a face presente em uma base de dados determinada. Um exemplo de falso positivo pode ser encontrado na história de Thais apresentada neste capítulo. Já um falso negativo é o que acontece quando Maria Eduarda, estudante do DF, é impedida de pegar o ônibus porque seu cartão está bloqueado, pois o sistema de reconhecimento facial implementado no transporte público não reconheceu sua foto. Ambos os casos significam um prejuízo para as pessoas envolvidas (Silva; Varon, 2021).

Muitos podem dizer que são pequenos erros, dentre um total de muitos sucessos da tecnologia. Contudo, o número de erros não para de crescer e a pouca divulgação dos relatórios de impacto e erros aumenta ainda mais a descrença dos críticos da tecnologia.

Thais não passou dia algum detida, mas o mesmo não pode ser dito do homem negro que foi preso em uma festa junina em Salvador, em 2002. Depois da prisão na frente do filho, o vigilante passou 26 dias injustos na cadeia (Alencar, 2023). Os dias perdidos por ele não voltarão. Também não deixarão de existir os traumas provocados pelo cárcere. É por isso que o uso de reconhecimento facial na Segurança Pública precisa ser banido.

Apesar dessas iniciativas para contornar os problemas do reconhecimento facial, é preciso destacar que as questões que envolvem IAs não afetam negativamente apenas TRFs. São parte de um todo maior de processos baseados na suposta neutralidade da máquina, na ideologia capitalista do Norte Global de que todo avanço tecnológico é automaticamente progresso, e em dinâmicas inerentes ao modo de produção capitalista, que necessita do racismo, do colonialismo e das opressões de gênero para perpetuar-se, produzindo reconhecimentos e irreconhecimentos.

Estar entre os reconhecíveis e os irreconhecíveis significa que os mesmos sujeitos estão inseridos em processos absolutamente distintos. O mesmo indivíduo hipervigiado pela cultura da vigilância (Lyon, 2018) é aquele submetido a processos mediados por inteligência algorítmica que o penaliza porque erram muito para

identificá-lo. Os erros não são um acidente, mas um projeto (Buolamwini, 2023; Faustino; Lippold, 2023).

Os sistemas que envolvem a inteligência artificial estão embutidos de valores políticos, estéticos racializados, manifestados na invisibilização, na hiper-visiblização e na esterotipização dos sujeitos (Silva, 2022). Esses valores representam desigualdades que são inerentes ao capitalismo (Gilmore *apud* Benjamin, 2022).

Conforme já dito, o sistema capitalista precisa encontrar organismos não explorados para manter-se vivo. Ele o faz destruindo as condições de prosperidade ou de sobrevivência de seu hospedeiro (Bauman, 2012). Além disso, a onipresença das redes sociotécnicas tem modificado percepções e capacidades sensoriais para que os indivíduos se conheçam e se conectem (Crary, 2023).

Semelhantemente ao poder colonial, tecnologias de vigilância operam para fazer com que indivíduos brancos cisgêneros sejam o modelo. Sua presença e seus comportamentos são percebidos como o padrão enquanto minorias ficam hiper-visíveis e constantemente vigiadas (Bell, 2023).

Aquilo que os modelos algorítmicos ignoram, ou seja, seus pontos cegos, reproduzem os julgamentos e as prioridades de quem os criou. Apesar de sua reputação de imparciais, modelos algorítmicos refletem objetivos e ideologias (O'Neil, 2020) que ficam ocultas na ideia de que as tecnologias são neutras. No caso das redes sociotécnicas, a invisibilidade dos processos com frequência oferece imunidade para a manutenção das desigualdades (Benjamin, 2019).

O processo de mascaramento das relações socioeconômicas por trás da tecnologia pode ser chamado de fetiche da tecnologia.

Segundo Henrique Novaes (*apud* Faustino; Lippold, 2023), o fetiche da tecnologia reside na confiança depositada na neutralidade e na linearidade do desenvolvimento das forças produtivas do capitalismo. Ele ofusca as relações sociais por trás das tecnologias.

> Para Marx, o fetichismo ocorre quando a mercadoria e as leis econômicas deixam de ser vistas como produtos das relações sociais e passam a ser encaradas como entidades universais e a-históricas ou dotadas de vida e intencionalidade próprias. Ocorre que o fetiche não se reduz à naturalização da exploração; expressa-se, também, pela aceitação do mito da neutralidade ou da incontrolabilidade – seja salvadora, seja amaldiçoada – da tecnologia, como se ela própria não fosse fruto de relações sociais historicamente determinadas que a projetam de acordo com certas finalidades políticas, culturais e econômicas (Faustino; Lippold, 2023, p. 44).

Ou seja, o fetichismo da tecnologia mascara as relações sociais e econômicas que acontecem antes, durante e depois do desenvolvimento e adoção de tecnologias diversas, dentre as quais incluo as de vigilância e controle e de processamento algorítmico. Um dos componentes dessa ofuscação está na ideologia do Vale do Silício, que propaga a ideia de que as *big techs* espalharão a salvação dos problemas do mundo como anjos[41]. A IA não se configura apenas como tecnologia, mas encarna tecno-ideologia, que autoriza que sejam confundidos os processos cerebrais e as lógicas econômicas e sociais (Sadin, 2020).

Uma margem de erro maior para pessoas negras aumenta a probabilidade de que sejam confundidas com pessoas procuradas e detidas, de alguma maneira, como o caso de Thais Silva, do início desse capítulo. Ou seja, um falso positivo. Contudo, esse não é o único impacto. Há também os falsos negativos, ou seja, os casos em que os sistemas não reconhecem o indivíduo e o acesso a um serviço público que necessite de verificação de identidade, por meio de reconhecimento facial, fica prejudicado (Silva; Varon, 2021).

A pluralidade semântica do termo reconhecimento coloca um lugar duplo. De um lado, o reconhecimento em seu sentido positivo. Ou seja, como aquele que percebe as diferenças e é capaz de atender demandas de grupos sociais diferentes. Vindo da filosofia de Hegel, o reconhecimento refere-se ao ideal de relação recíproca entre sujeitos que se percebem como iguais e ao mesmo tempo diferentes. Assim, tonar-se sujeito na medida em que se reconhece e é reconhecido pelo outro (Fraser, 2003). Há em outra ponta o reconhecimento negativo, ou seja, aquele que individualiza não a partir de seu todo, mas apenas de suas características físicas, para que o sujeito seja processado por máquina. É no reconhecimento negativo que processos algorítmicos, como o racismo (Silva, 2022; Noble, 2021; Bezerra; Costa, 2022), a acumulação primitiva de dados (Faustino; Lippold, 2022; Lippold; Faustino, 2023), a transfobia (Silva; Varon, 2021) e o machismo (Buolamwini, 2023; Buolamwini; Gebru, 2018) se reproduzem.

Com frequência, o conceito de identidade é percebido pela sua capacidade de individualizar as pessoas, por meio de suas características físicas e biométricas e de seus traços de personalidade. (Silva; Varon, 2021, p. 9). O reconhecimento facial

[41] Anjos Tronchos, de Caetano Veloso. Disponível em: https://www.youtube.com/watch?v=22gCVzU9WUY. Acesso em: 17 dez. 2023.

subverte a lógica do reconhecimento como aquilo que torna o indivíduo único, pois torna o sujeito métrica quantificável.

Paulo Freire (1987) lembra que, em contextos de opressão, os oprimidos são, então, percebidos como coisas cuja finalidade é aquela prescrita pela racionalidade opressora que conta com a tecnologia para a manutenção da ordem. É nesse contexto de injustiça distributiva que se torna tão necessário falar da relação entre reconhecimento e redistribuição (Fraser; Honneth, 2003)

Ao apresentar o PL 9914/2017, expus que a sua justificativa dizia que o projeto se baseava na iniciativa de reconhecimento facial nos ônibus do DF. Foi esse mesmo sistema que deixou a estudante Maria Eduarda sem poder acessar o direito ao Passe Livre Estudantil. Maria Eduarda é uma mulher trans e sua imagem, após a transição, não seria, então, igual à cadastrada no banco de dados (Silva, Varon, 2021), o que acarretou um falso negativo.

Estudos, como o Mariah Rafaela Silva e Joana Varon (2021) e o de Sasha Costanza-Chock (2020) demonstram de que maneira a perspectiva de gênero binária de mundo, que classifica pessoas como homens e mulheres, afeta pessoas trans em suas experiências do cotidiano. A classificação automatizada fez renascer técnicas lombrosianas, como o Reconhecimento Automático de Gênero, que objetiva identificar, por meio de algoritmos, o gênero de indivíduos (Pasquinelli; Joler, 2020), pois “classificam imagens e determinam que rostos são de ‘homem’ ou ‘mulheres’, ao fazer isso, estabelecem um falso link (representacional) físico das características do rosto” (Silva; Varon, 2021, p. 15).

Iniciativas voltadas para a adoção de ferramentas de reconhecimento facial têm a capacidade de exemplificar o colonialismo de dados porque demonstram a desigualdade na balança entre estados e parcerias público-privadas e a população, na implementação de ferramentas de vigilância com a capacidade de monitorar cidadãos e pela habilidade de extrair dados da população, sem seu conhecimento, em nome do lucro, de acordo com Kainem Bell (2023). Isso remete aos comentários de Morozov e Bria (2019) que apontam que as cidades precisam se manter capazes de implementar políticas públicas de modo independente e eficiente.

Cidades, estados e países precisam de novos vocabulários e de novos conceitos para repensar suas relações com ferramentas tecnológicas, com os dados e com as infraestruturas. Ainda assim, é importante destacar que

> Quando dados, sensores e algoritmos – os ingredientes principais da dinâmica smart oferecida pelo neoliberalismo – são mediadores do fornecimento de serviços em domínios que vão de utilidades públicas a transporte, educação e saúde, é evidente que a discussão não pode se restringir a questões de infraestrutura (Zanatta, 2019).

De que modo é possível haver espaços de criação, de contestação e de anonimato, se tecnologias algorítmicas objetivam resolver todos os problemas em tempo real enquanto medidas econômicas de austeridade estão em andamento (Zanatta, 2019)? De que maneira a cidadania não será substituída por algoritmos (Garcia Canclini, 2019)?

As cidades, estados e países possuem cada vez mais dados, mas isso não significa que eles estão disponíveis ou facilmente acessíveis para o interesse público (Zanatta, 2019).

A presença das tecnologias da informação e comunicação está tão espalhada, e com tanta complexidade, que companhias têm conseguido escapar das pressões por transparência e *accountability* (Pasquale, 2015). Algumas tecnologias podem, por concepção, ofuscar questões éticas e a justificativa das escolhas feitas em suas elaborações, afastando-as da compreensão da maior parte das pessoas (Dratwa, 2017). Companhias têm se esforçado para esconder seus modelos e os resultados sob o argumento da propriedade intelectual, dificultando que se responda perguntas como: esse modelo é capaz de danificar ou destruir vidas? É justo? (O'Neil, 2020).

Apesar da aura de neutralidade, ainda assim questionamentos sobre os vieses presentes em tecnologias algorítmicas, como o reconhecimento facial, têm sido colocados (Pasquale, 2015).

Mariah Rafaela Silva e Joana Varon (2021) afirmam que a utilização de estratégias tecnopolíticas de implementação de TRFs, como meio para verificar identidades sem transparência e/ou salvaguardas, pode significar ameaças a conquistas que, inclusive, estão relacionadas à autodeterminação de gênero. Outro estudo, *Gender Shade* (2018) demonstrou que softwares de reconhecimento exibem mais erros ao processarem fotos de mulheres e, em especial, de negras.

> Esses erros na identificação de gênero e raça acontecem porque os bancos de dados são produzidos a partir de um referencial branco, conferindo à tecnologia um caráter profundamente enviesado tanto no que diz respeito às políticas raciais, quanto no que diz respeito às políticas de gênero. Isso apresenta um grande desafio ao

> treinamento desses algoritmos, uma vez que, se a base de dados parte de uma prerrogativa masculinista e branca, as taxas de erros tendem a ser grandes, apresentando ameaças à direitos fundamentais. (Silva; Varon, 2021, p. 41).

De acordo com Joy Buolamwini e Timmit Gebru (2018), algoritmos treinados com dados enviesados resultaram em discriminação algorítmica. Falsos positivos e buscas e apreensões errôneas significam uma ameaça aos direitos humanos.

Já os exemplos que envolvem a dimensão racista das redes sociotécnicas, que tem recebido o nome de racismo algorítmico, pode ser vista nos estudos de Safyia Noble (2021), Ruha Benjamin (2019), Tarcízio Silva (2022) Bianca Kemmer (2023).

O racismo algorítmico é definido por Tarcízio Silva (2022) como

> o modo pelo qual a disposição de tecnologias e imaginários sociotécnicos em um mundo moldado pela supremacia branca realiza a ordenação algorítmica racializada de classificação social, recursos e violência em detrimento de grupos minorizados. Tal ordenação pode ser vista como uma camada adicional do racismo estrutural, que, além do mais, molda o futuro e os horizontes de relações de poder, adicionando mais opacidade sobre a exploração e a opressão global que já ocorriam desde o projeto colonial do século XVI (Silva, 2022).

O capitalismo moderno sustenta-se em processos imperialistas e de racialização – uma tecnologia de poder – para justificar as diferentes relações econômicas que envolvem a expropriação e a exploração. O capitalismo moderno está intrinsecamente conectado com processos de racialização, conforme argumenta Nai Lee Kalema (2023).

Deivison Faustino e Walter Lippold (2023) propõem a categoria racialização digital. Essa seria uma tendência de materialização e subjetivação do racismo, não apenas no que se refere ao desenvolvimento da técnica, inerente ao que compõe organicamente o capital, mas, acima de tudo, na desigualdade de distribuição do caráter destrutivo do sistema capitalista. O racismo não foi eliminado pela digitalização e dataficação, mas reproduzido e até mesmo expandido em diversos casos (Silveira *apud* Faustino; Lippold, 2023) e muitos exemplos podem ser encontrados nos casos que envolvem a baixa taxa de acurácia de tecnologias de reconhecimento facial, diante da face de pessoas negras.

As transformações digitais globais do sistema econômico têm dado espaço para a emergência de um capitalismo racial digital, o que ocorre no encontro de

práticas das transformações digitais, do capitalismo racial e do colonialismo de dados e digital, resultando em formas mediadas por dados de racialização, violência estrutural e necropolítica de dados. Essa se refere ao modo como formas de governança algorítmica expõem indivíduos a desigualdades no acesso à saúde, na exposição à violência social e à morte (literalmente e metaforicamente) e ao modo como dados são instrumentalizados por governos para normalizar desigualdades sociais.

O capitalismo racial digital cria hierarquias racializadas de risco e vulnerabilidade dentro do colonialismo de dados, ao usar dados e tecnologias digitais para reconfigurar, criar e fortalecer categorias de racialização como, por exemplo, migrantes, terroristas. Os dados obtidos por meio do colonialismo de dados são usados para criar modos de categorização, estratificação e racialização, que colocam pessoas em diferentes categorias de despossessão e descartabalidade (Kalema, 2023). Sistemas de vigilância massiva geram necessariamente um número alto de pessoas suspeitas (Dratwa, 2017). Nesse sentido, vale lembrar que tal geração é baseada na ordem que criminaliza a pobreza e o comportamento dissonante percebido como subversivo da moral e dos bons costumes, como foi visto nos discursos de parlamentares.

O racismo algorítmico é um fenômeno que está diretamente ligado ao problema da dupla opacidade, ou seja, a forma pela qual grupos hegemônicos procuram tanto apresentar a ideia de “neutralidade” tecnológica quanto apagar o debate sobre racismo e supremacismo branco no Ocidente. Um dos maiores perigos do racismo algorítmico é a diluição da responsabilidade, verificada no ato de atribuir à tecnologia a agência de abordagens policiais; a identificação de pessoas; a tipificação ou condenação de comportamentos que ocorre por meio de ferramentas tecnológicas, como o reconhecimento facial; o policiamento preditivo e o ranqueamento em escores de risco. Socialmente, não se deve consentir que a reunião de ações discriminatórias cotidianas seja transformada em dados que alimentam sistemas de aprendizado de máquina, tal qual acontece nos processos que envolvem a justiça criminal (Silva, 2022).

Pessoas racializadas e grupos étnicos estão mais vulneráveis à hiper-vigilância, aos danos digitais e à desapropriação de dados. Os tipos de crenças usados para justificar a exploração e a expropriação predatórias de dados estão ligados à racialização necessárias à reprodução do capitalismo que necessita de

disciplina e gerenciamento (Kalema, 2023), conforme indicam os estudos de Michel Foucault (1977). Segundo Nai Lee Kalema (2023), o colonialismo de dados e o capitalismo racial digital são co-constitutivos um do outro e facilitam a dominação digital global, o que diminui o poder de ação das pessoas (por exemplo, a sua capacidade de contestar decisões), alienando-as dos seus dados.

Apresentei alguns exemplos de problemas relacionados às diversas formas de discriminação algorítmica, apenas uma parte de um fenômeno muito mais abrangente que envolve o resgate do significado de humano. Afinal, o que significará livre-arbítrio e autonomia em um mundo em que algoritmos rastreiam, predizem e persuadem os indivíduos a todo momento? (Benjamin, 2019).

Joana Varon (2023) aponta a necessidade de compreender o papel que sistemas sociotécnicos possuem na reprodução da violência epistêmica colonial e do controle social em sociedades dataficadas. Em muitos casos, a adoção de tecnologias acaba por automatizar e massificar preconceitos e estigmas sociais já enraizados, o que alimenta

> estruturas de dominação de um cishétero patriarcado racista, capitalista e colonial, e como tal, apresentando riscos principalmente às populações historicamente vulnerabilizadas e estigmatizadas, em especial pessoas negras, LGBTI e pobres (Silva; Varon, 2021, p. 6).

Diversas companhias relacionadas ao reconhecimento facial buscam solucionar o problema dos vieses algoritmos, apoiando-se na ideia de que maior diversidade das bases de dados solucionaria a questão. Contudo, Ruha Benjamin (2019) lembra que a criação de bancos de dados com informações étnico-raciais também traz possíveis efeitos negativos, no que se refere à privacidade, à vigilância e à discriminação. Além disso, como lembram Matteo Pasquinelli e Vladan Joler (2020), os problemas das IAs não se restringem ao viés da informação. Ferramentas baseadas em IA não são apenas aparelhos de controle, mas também aparelhos produtivos.

Ao longo deste texto, foi frequente a menção às tecnologias de grandes corporações do Norte Global. É possível observar que as *big techs* não são as únicas a participarem de projetos que envolvam tecnologias de vigilância massiva. Na realidade, pudemos observar que há muitos envolvidos no fenômeno, no caso brasileiro. Contudo, acredito que também vale a pena observar que, apesar de nem sempre ser uma *big tech* que instala tecnologias do gênero, esses projetos estão

imbuídos da ideologia que sustenta o Vale do Silício e percebe a tecnologia como salvadora de mazelas sociais. São “os mecanismos de sustentação ideológica desse novo colonialismo a partir do novo fetichismo da técnica, da ilusão da neutralidade tecnológica e de ingênuas crenças na libertação pelos dispositivos” (Silveira *apud* Faustino; Lippold, 2023, p. 16).

Mariah Rafaela Silva e Joana Varon (2021) lembram que as tecnologias não têm caráter neutro. São traduções da ordem social e sua manutenção ocorre a partir de interações sociais desenvolvidas ao longo da história. Elas “carregam consigo a sombra de um modelo de sociedade que é reproduzido nos mundos digitais e tecnológicos” (Silva; Varon, 2021, p. 41).

Com frequência, agendas que envolvem a liberdade nas redes sociotécnicas estão muito mais ligadas aos interesses econômicos e políticos do que aos valores éticos (Bigo, 2019).

Ainda assim, os vieses e a falta de neutralidade presentes em ferramentas algorítmicas não são o único problema. São diversas as questões que envolvem direitos à privacidade e à intimidade. Privacidade e intimidade, conforme debatido anteriormente na seção sobre a China, são valores muito ligados às lógicas de pensamento e organização social ocidentais. Ainda assim, eles podem chamar a atenção para os muitos problemas causados pelas redes sociotécnicas, pelos processos diversos de comodificação da vida e pelo aprofundamento das contradições provocadas pelas tecnologias da informação e comunicação em muitas esferas da existência (Faustino; Lippold, 2023)

Diferenças na percepção do que é privacidade e na importância de proteger este direito são importantes fatores que complicam a balança entre a proteção da privacidade e a segurança. A privacidade não está nos mais altos lugares no *ranking* das necessidades humanas. Portanto, sacrificar privacidade por mais segurança acaba por parecer uma consequência lógica (Dratwa, 2017). Os dados pessoais não devem ser percebidos como algo passível de compra, venda ou compartilhamento, visando o lucro. As oportunidades para a ocorrência de abusos de muitas ordens são muitas e não param de aumentar. No que se refere à privacidade, a pior combinação possível é a que envolve o fato de que os dados pessoais são extremamente valiosos e simultaneamente muito baratos (Véliz, 2021).

Acidentes de segurança costumam receber mais atenção do que acidentes que envolvem a violação da privacidade das pessoas, exceto quando a percepção

da violação é de cidadãos chineses. Nesse caso, a privacidade é colocada como um valor importante. Alguns parlamentares brasileiros demonstraram preocupação com o modelo de vigilância e controle de massas da China, expresso no Crédito Social Chinês, mas em sua maioria não tentaram impedir o modelo de negócios de empresas de reconhecimento facial ocidentais, o que se expressa na quantidade de leis pela implementação de TRFs ou no fato de não haver nenhuma menção à intervenção israelense na Palestina e seus muitos aparatos tecnológicos de segurança dentro dos quais se inclui o reconhecimento facial (Amnesty International, 2023).

O desenvolvimento e adoção de ferramentas tecnológicas de vigilância em massa nos convida a questionar se o argumento da segurança às custas das liberdades individuais é aceitável. É preciso tensionar para, então, considerá-las a partir de uma pesquisa de justiça e de solidariedade, também em termos de acesso, desigualdade e equidade. Aqui a dialética reside nas tensões entre individual e coletivo, nacional e transnacional, público e privado (Dratwa, 2017).

Ao falar de coletividade, é importante lembrar de outra dimensão do colonialismo digital, que envolve a necessidade predatória de recursos naturais. No caso brasileiro, não é possível dissociar a tecnologia digital da extração ilegal de ouro em terras indígenas, como nas reservas do povo Ianomâmi, pois *softwares* necessitam de *hardware* e estes são produzidos com o ouro oriundo de terras indígenas no Brasil, a columbita e a tantalita do Congo e o lítio da Bolívia, por exemplo. Os dados, a informação, as nuvens e os *softwares* precisam ainda de matéria orgânica, de água e energia para existirem. Desse modo, o extrativismo predatório de matérias-primas é uma das faces do colonialismo digital, assim como era do colonialismo clássico (Faustino; Lippold, 2023). Outro ponto é a necessidade de *data centers* e seus impactos ambientais, pois consomem muita energia e água (Silveira *apud* Faustino; Lippold, 2023). Segundo Jess Ciacci (2023), um modelo de desenvolvimento baseado nesta concepção extrativista implica necessariamente em impactos sociais e ambientais.

A ideologia capitalista e a ideologia da lógica científica ocidental somente puderam sobreviver a partir do progressivo crescimento da exploração, da apropriação contínua de recursos, do infinito processo de criação de conhecimento e do desenvolvimento de ferramentas tecnológicas cada vez mais poderosas. A atitude diante da apropriação ilimitada de recursos aliada à ideologia, que categoriza

e hierarquiza objetos e suas características, não é imprescindível para a ciência, mas o é para a exploração capitalista. (Numerico, 2023).

Tecnologias de vigilância e controle estão ancoradas e recriam visões coloniais de determinismo tecnológico e controle social. O crescimento de arquiteturas de vigilância não apenas normaliza o monitoramento das atividades diárias dos cidadãos, mas também monopoliza os dados sobre minorias sociais, de forma que silenciam e privam a criação de soluções orientadas e lideradas pela comunidade como respostas alternativas aos problemas locais, conforme apontam Chamee Yang, Gowri Balasubramaniam, Clara Belitz e Anita Say Chan (2023).

Para além do extrativismo predatório e da expropriação de territórios, a colonização também tenta dominar corpos e mentes. Ela se sustenta como uma ordem epistemológica capaz de definir o que e quem tem valor, em detrimento do que e de quem é descartável. Mascarada pela ideia de neutralidade, a colonização de dados atua sob a invisibilidade epistêmica de formas alternativas de ser e estar no mundo (Varon, 2023). Ela ultrapassa o controle das terras e recursos naturais, estendendo-se para controlar as narrativas sobre as pessoas, suas identidades, culturas e histórias e sobre como elas devem se comportar, o que inclui normas de gênero e sexualidade (Mayoral Baños, 2023).

Jonathan Crary (2016) argumenta que o problema do envolvimento em redes sociotécnicas, que atualmente acontece 24 horas em sete dias da semana, é que ele faz com que as pessoas percam a capacidade de sonharem acordadas que ocorre no ócio, pois o tempo também foi colonizado. Os diversos dispositivos que nos cercam atraem também por causa de sua velocidade ou, ao menos, da impressão de velocidade. Para o autor, daí deriva “uma incompatibilidade profunda entre qualquer coisa que se assemelhe ao devaneio e as prioridades de eficiência, funcionalidade e velocidade” (Crary, 2016), o que prejudica o ócio que permite a criação e a conexão com os demais. E é das possibilidades de imaginação transformadora que tratarei no próximo capítulo.

6 PARA IMAGINAR O NOVO

Se oriente, rapaz/ Pela constelação do Cruzeiro do Sul/
Se oriente, rapaz/ Pela constatação de que a aranha
Vive do que tece/ Vê se não se esquece
Pela simples razão de que tudo merece / Consideração
Oriente - Gilberto Gil

Ao longo deste trabalho, abordei o modo pelo qual o capitalismo tem domado sociabilidades na atualidade. Os tentáculos do sistema de produção capitalista demonstram sua força por meio do colonialismo digital, no que se refere tanto à dimensão relativa de suas infraestruturas quanto ao colonialismo de dados. Para isso, usa ferramentas algorítmicas, cada vez mais complexas e presentes no cotidiano das pessoas, como as tecnologias de reconhecimento facial, cujos aspectos políticos, econômicos e éticos de sua adoção no Brasil tentei demonstrar ao longo desta pesquisa.

A publicação *Resisting Data Colonialism: a Practical Intervention* (The Tierra Común Network, 2023) chama à desobediência[42] – que aqui tem o sentido de propor novos caminhos e outras e perturbadoras questões para favorecer a idealização de alternativas para a criação de novas realidades – e apresenta uma lista com 10 possibilidades para resistir ao colonialismo de dados. São elas:

1. Identificar maneiras nas quais a dataficação está operando na sua rotina diária;

2. Adotar a ideia de comunalidade digital e da gestão de dados como bem-comum;

3. Prevenir e diminuir as muitas formas de opressão estrutural que acabam por serem incorporadas aos dados e às arquiteturas digitais, incluindo o dever de exigir reparação pelos danos causados pelo uso de dados e de redes sociotécnicas;

4. Organizar sua própria comunidade e apoiar comunidades mais afetadas pelo colonialismo de dados, buscando, de modo simultâneo, a sua proteção de dados dentro do possível;

[42] *É nunca fazer/ nada que o mestre mandar / sempre desobedecer/ nunca reverenciar* – Como o Diabo Gosta, Belchior. Disponível em: https://www.youtube.com/watch?v=tDWEdRo6mA4. Acesso em: 25 jan. 2024.

5. Dar apoio a uma legislação forte e quadros políticos aliados da promoção da justiça de dados e limitar o abuso de plataformas digitais e a concentração de mercado, em especial no dito “Sul Global”;

6. Promover modos alternativos de governança de dados. Comunidades e países podem desenvolver seus próprios modelos de dados;

7. Promover uma abordagem de permacultura de dados e das tecnologias, ou seja, promover políticas capazes de assumir a responsabilidade pelos impactos ambientas da economia digital;

8. Desenvolver outros modelos e ferramentas de saber/produzir dados permeados por valores alternativos que objetivem a justiça de dados;

9. Lutar por justiça para aqueles trabalhadores explorados pela economia de dados;

10. Acrescentem suas próprias ações (The Tierra Común Network, 2023, p. 93, tradução nossa)

Este trabalho foi feito na tentativa de acrescentar as minhas e as nossas próprias ações. Além disso, apresento alguns caminhos possíveis para resistir aos diversos aspectos do capitalismo que foram abordados neste estudo, tais como o colonialismo digital, o colonialismo de dados, o racismo algorítmico, as violências de gênero e as agressões da lógica do sistema punitivo que envolvem tecnologias de vigilância e controle.

As discussões sobre colonialismo de dados devem levar à práxis, ou seja, à resistência (Couldry, 2023). O colonialismo de dados se perpetua a partir da automação de processos de classificação social. Para combater tais aspectos, as assimetrias, os vieses e os limites das IAs e do *big data,* derivados dos problemas de abstração e classificação, devem ser substituídos por uma visão que coloque os conhecimentos em perspectiva (Numerico, 2023).

E é para fomentar a capacidade de colocar os conhecimentos em perspectiva que a ética intercultural da informação tem lugar.

A abordagem ético-metodológica proposta por Rafael Capurro (2017) é a da reflexão crítica comparativa intercultural, ou seja, a ética intercultural da informação, que parte do pressuposto de que há diferenças tanto nas tradições morais, a saber, nos diferentes valores e modos de vida, bem como em sua codificação na forma de leis e normas como expressão de um ideal ou de uma ideologia. Para a realização de tal reflexão comparativa é preciso paciência, o que não significa perder de vista o

senso crítico. Não se trata de somente descrever as diversidades culturais, mas também de problematizar as normas subjacentes aos interesses e poderes locais e/ou globais, além de buscar valores e princípios comuns e formas de organizar a vida comunitária. Uma reflexão ética deve pensar o universal sem descuidar da singularidade das formas de vida e dos fatos históricos e geográficos. Como uma reflexão crítica, ela tem de problematizar, por exemplo, aspectos de justiça, participação política e social, bem como de proteção ambiental.

Primeiramente, a desigualdade é uma construção histórica, social e política (Piketty *apud* Dowbor, 2022). Em outras palavras, para níveis de desenvolvimento tecnológico e/ou econômico iguais há diversas formas de organização dos sistemas de propriedade ou fronteira, do sistema sociopolítico, e de organizar regimes fiscais e educativos. Todas essas são escolhas políticas (Dowbor, 2022).

Vale nos perguntarmos de que forma os direitos são reivindicados não apenas por meio de regulamentos, leis e protocolos, mas pelos cidadãos que fazem suas próprias reivindicações e, por sua vez, executam o que é política relativa aos dados por meio de seus atos digitais cotidianos? (Bigo, 2019)

Por isso, reflexões éticas possuem também o papel de despertar e preservar a sensibilidade ética. Por isso, faz-se necessária a abertura de espaços locais e globais para reflexões éticas acerca das tecnologias da informação e comunicação e das redes sociotécnicas. Isso presume reflexões éticas que não se limitem apenas ao fundamento de determinadas normas morais, mas incluem a problematização a partir de sua interação com outras dimensões da vida social. Corresponde também à busca por formas de vida em comum que comportem a variedade e a riqueza da experiência humana (Capurro, 2017).

As tecnologias digitais de informação e comunicação têm tido profunda influência nas normas morais e legais, ou seja, nas formas de vida no século XXI. A ética, em geral, e a ética da informação, particularmente, são confrontadas com os desafios teóricos e práticos surgidos na diversidade de valores morais e éticos em culturas diferentes e em relação com as TICs (Capurro, 2017), alguns dos quais já abordados anteriormente nesse estudo.

O reconhecimento facial é a promessa do inalcançável que utiliza a neutralidade do discurso tecnológico. É sempre o horizonte da tecnologia que poderá responder aos problemas do hoje. Quando câmeras de vigilância foram espalhadas, a ideia era de que seriam capazes de coibir a criminalidade. Agora,

adicionar mais tecnologia aos dispositivos instalados será capaz de resolver um problema para o qual esses mesmos dispositivos foram pouco expressivos na resolução: o problema da violência é complexo e absolutamente multifatorial, como lembra Bruno Cardoso (2013).

A escolha entre segurança e liberdade dá-se mais em um padrão pendular (Bauman, 2012). Não há uma resposta simples sobre se devemos valorizar mais a segurança ou a liberdade porque não há liberdade sem segurança e também não acredito que seja possível haver segurança real sem liberdade. Contudo, precisamos tomar consciência e fazer parte das decisões que envolvem projetos que restringem a liberdade das pessoas em muitas dimensões da vida cotidiana. E é nesse sentido que se deve falar em privacidade. Do ponto de vista da privacidade, a ideia de que os dados coletados precisam ser aprovados pelos usuários e a proibição do reuso dessas informações são interessantes (O'Neil, 2020). Contudo, é preciso reconhecer as limitações disso, pois usuários têm cada vez menos escolha de não optarem pela coleta, pois ela faz parte das exigências dos serviços públicos e das infraestruturas urbanas.

A privacidade deve ser percebida como um direito que ajuda a garantir o reconhecimento em seu sentido positivo, ou seja, auxilia na garantia do respeito à diferença e à individualidade.

Além disso, deve haver uma mudança no regime de propriedade dos dados, o que pode ser uma opção com menos custo. Nesse sentido, cidadãos e cidades precisam ser donos dos dados que são produzidos no ambiente urbano e conseguir utilizá-los para promover melhoras nos serviços públicos e o impulsionar políticas públicas (Zanatta, 2019).

Para Zanatta, é preciso favorecer a construção de modelos econômicos baseados em dados que permitam o fortalecimento da democracia participativa em decisões complexas. Além disso, deve-se dar preferência para organizações colaborativas, criar condições para a instituição de mecanismo de renda básica universal para combater a pobreza e a exclusão social, implementar dados abertos nas cidades e impedir que dados gerados a partir da prestação de serviços públicos sejam apropriados pelos prestadores.

Rafael Zanatta (2019) reconhece a complexidade dos dados pessoais serem tratados como um recurso coletivo, o que faz com que a governança coletiva de dados seja um assunto complexo. Ainda assim, para o mesmo autor

> As cidades precisam se apoderar de dados coletivos sobre pessoas, sobre o ambiente, sobre objetos conectados, sobre o transporte público e sobre sistemas de energia e precisam fazê-los circular como bens de uso comum. Infraestruturas de dados para captura, visualização e análise que se ocupam principalmente de alimentar centros operacionais municipais de propriedade de grandes comerciantes de TI (como o Centro de Operações Inteligentes da IBM no Rio de Janeiro) podem ser aproveitadas pelos cidadãos para atingir seus próprios interesses, para trazer à tona questões ligadas à corrupção, à igualdade na distribuição de recursos municipais e a outras matérias ligadas ao poder e ao acesso em defesa de um autogoverno autônomo (Zanatta, 2019).

Os algoritmos, assim como os outros *designs* tecnológicos, são capazes de expressar, recolocar e intensificar contradições das sociedades nas quais estão inseridos (Faustino; Lippold, 2023). Por isso, a criação de tecnologias mundanas deve fazer parte do processo de libertação das diversas formas de opressão. Segundo David Nemer (2021), as tecnologias mundanas envolvem o processo de apropriação dos oprimidos das tecnologias presentes no cotidiano. como artefatos, espaços e operações, de modo a utilizá-las para promover o alívio da opressão em suas rotinas (Nemer, 2021).

Pessoas ao redor do globo sempre desenvolveram suas próprias estratégias de resistência diante de sistemas violentos. Elas podem ser consideradas como desobediência epistêmica que batalha para se afastar da colonialidade de poder exercida por meio da colonização de conhecimentos e dos modos de ser e sentir. O valor da resistência reside na possibilidade da produção de fissuras nesses sistemas de violência, tornando a existência possível. Diversos grupos têm buscado autonomia, dignidade e seu direito ao futuro baseados em práticas que não sucumbiram à lógica aniquiladora do modelo capitalista colonial e patriarcal do mundo (Ricaurte Quijano, 2023).

Solidariedade em vez de caridade. Faz-se necessária a destruição de sistemas nocivos, o suprimento das necessidades imediatas dos indivíduos e a criação de estruturas alternativas capazes de atender tais necessidades baseadas em valores de cuidado, participação democrática e solidariedade (Benjamin, 2022). Trata-se de buscar regras de solidariedade que sejam baseadas em respeito mútuo (Capurro, 2017). Nos nossos modos de apresentação no mundo diante dos outros reside a fundação para um mundo mais junto e colaborativo entre humanos.

A subordinação compulsória e passiva às redes sociotécnicas digitais é primordial para o alcance da meta neoliberal de tornar invisível ou inconcebível a

abertura para modos não opressivos de ser e estar no mundo. Contudo, há a resistência continuada em localidades diversas no Sul Global, pois seria o local em que “o espírito de revolta nunca foi derrotado, que os caminhos mais relevantes para um mundo pós-capitalista estão sendo forjados” (Crary, 2023, p. 6).

A ética intercultural da informação tem mostrado sua relevância para analisar a relação entre o público e o privado na América Latina, que também tem sido lugar fértil para que as redes sociotécnicas sejam vistas a partir de uma lógica primariamente social, baseada em valores comuns. As análises éticas precisam considerar as relações complexas entre as tradições ocidentais, epistemologias indígenas e afrodiaspóricas, além dos encontros violentos ou não entre essas tradições de pensamento.

A extração massiva de dados é um tipo de desapropriação que gera injustiças econômicas, raciais, epistêmicas, ambientais, entre outras. Por isso, a resistência deve ser vista como uma forma de reinventar o mundo em que se vive para redefinir e ressignificar as condições de vida, tornando-as mais dignas (Alban *apud* Ricaurte Quijano, 2023). Resistir, nesse sentido, é explorar alternativas diante daquilo que subtrai a humanidade.

A dataficação, quando instituída sob a lógica da racionalidade dominante governada pelo mercado, torna-se um processo que reduz, quantifica, redefine a ordem social de classificação e cria sistemas de conhecimento, além de reforçar injustiças, retirar autonomia e a capacidade para a tomada de decisões. A resistência, então, exige retomar a autonomia, a soberania, a comunalidade, a convivência e o direito ao futuro e a formas de coletividade que ultrapassem atores que buscam a apropriação da vida (Ricaurte Quijano, 2023).

Gerhard Dilger (2016) aponta que visões de mundo, como o bien-vivir, o movimento social para decrescimento sustentável e a filosofia humanista do ubuntu compartilham alternativas ao desenvolvimento em torno de ideias de

> colaboração em vez da concorrência que o capitalismo promove; a valorização da convivencialidade; a importância da autonomia, da autogestão e dos processos construídos localmente a partir de baixo; o respeito à diversidade e o valor central da deliberação; a democratização da economia e da tecnologia; a transformação da propriedade privada em propriedade social (que não é o mesmo que propriedade estatal) ou em comuns; a soberania alimentar; a solidariedade e a reciprocidade (Dilger, 2016).

Desse modo, a ética intercultural da informação deve ser hospitaleira, não apenas ao respeitar culturas e formas de vida, mas também com aqueles que se encontram marginalizados e esquecidos pelas redes sociotécnicas dentro de um mundo globalizado (Capurro, 2005). Acrescento que esta ética também deve ser solidária com aqueles que são hiper-visíveis e invisíveis dentro do sistema capitalista, ou seja, aqueles a quem estou chamando de irreconhecíveis e reconhecíveis.

Em resumo, os desafios teóricos e práticos da ética intercultural da informação são vastos e muitos. Por isso, precisam de apoio de instituições de educação e pesquisa que realizem um esforço para criar redes locais e globais que permitam a troca de conhecimento. A busca por princípios comuns deve considerar a complexidade e a variedade das culturas e ter em conta a interdependência que permite transformações (Capurro, 2010).

É preciso admitir que o processo tecnológico não será revertido. Por isso, faz-se necessário que seu sentido político seja modificado para que esteja a serviço da sociedade como um todo e não de plataformas (Dowbor, 2022, p. 62) inseridas no capitalismo. A partir disso, pode-se definir qual é o tipo de infraestrutura necessária. Suas características devem envolver o livre acesso e possibilitar usos subversivos (Morozov, 2020).

Não se pode ser contrário ao capitalismo enquanto se valida seus “aparatos constitutivos de funcionamento” (Crary, 2023, p. 4). Os debates sobre tipos alternativos de intervenções políticas e pragmáticas que podem vir a ser implementados precisa ser inserido dentro de um contexto mais amplo de “lutas contra a austeridade, contra o neoliberalismo predatório e contra a corporização de todas as coisas” (Zanatta, 2019).

Morozov e Bria (2019) aponta nove necessidades para o momento histórico em que vivemos. São elas:

> 1. Incentivo a regimes alternativos de propriedade de dados. 2. Realocação de serviços de informação para plataformas de código e padrão abertos e adoção de soluções ágeis de entrega. 3. Transformação das contratações públicas a fim de torná-las éticas, sustentáveis e geradoras de inovação. 4. Controle das plataformas digitais. 5. Construção e expansão das infraestruturas digitais alternativas. 6. Desenvolvimento de modelos cooperativos de fornecimento de serviços. 7. Potencialização de inovações com valor social. 8. Reavaliação de esquemas de bem-estar social e sistemas

> monetários complementares locais. 9. Incentivo à democracia e à soberania digitais (Morozov; Bria, 2019).

Todos os recursos devem ser aproveitados para a inclusão produtiva, o que envolve mecanismos de mercado, o planejamento e a regulação do público e os sistemas participativos da sociedade civil (Dowbor, 2022). E é nesse último que a moral subjacente à ética do bem-viver pode mostrar-se útil no que concerne a modelos mais participativos de democracia, inclusive, a respeito da utilização de tecnologias de vigilância e controle.

Conhecimento e imaginação são elementos centrais na construção de sociedades e na economia (Numerico, 2023). Conforme lembra Sérgio Amadeu Silveira (2023), “o mundo é formado não apenas pelo que já existe, mas pelo que pode efetivamente existir”.

O conhecimento é construção social. Por isso, o retorno que oferece também deve ser oferecido à sociedade. O objetivo não é o controle do conhecimento, mas a possibilidade de sua libertação (Dowbor, 2022), de modo a ser empregado socialmente.

Retomo Faustino e Lippold (2023), anteriormente citados, para destacar que é preciso atentar-se para o fetiche da tecnologia que a percebe como salvadora ou como totalmente destruidora. E mais uma vez repito que tecnologias por si sós não são boas ou más, mas reflexos das sociedades que as idealizam. Ainda assim, é preciso reconhecer sua complexidade, como lembra Kashmir Hill (2023), e a capacidade de extensão de seus danos. É por isso que pensar novas relações com a tecnologia que tenham potencial emancipatório é tão importante no estágio atual do capitalismo.

Nesse sentido, Johann Čas, Rocco Bellanova, J. Peter Burgess, Michael Friedewald e Walter Peissel (2017) levantam uma questão bastante importante: como podemos modificar a economia da vigilância em prol da construção de futuros que ainda podem ser imaginados coletivamente? Pois não se trata apenas tecer críticas, mas de imaginar e construir novos futuros alternativos – embora eu reconheça a importância da crítica e dos críticos. Por isso, deve-se rejeitar ideias falsas que tratam as tecnologias, bases de dados e representações algorítmicas como neutras, o que se configura como um esforço permanente contra diversas formas de opressão nas redes sociotécnicas (Silva, 2022). É também necessário imaginar novos tipos de ferramentas emancipatórias, como lembra Ruha Benjamin

(2019) ou, nas palavras de Jonathan Crary (2016), o “caráter indispensável da imaginação para a sobrevivência coletiva”[43].

É preciso admitir que, no capitalismo, sonhar tem se mostrado um luxo. Os indivíduos que almejam a construção de uma realidade social diferente, baseada na justiça e na felicidade, não devem apenas criticar o mundo do jeito que é, mas também construir o que o mundo deve ser (Benjamin, 2022). Ou, para citar Karl Marx (1982), agora é (continua sendo) importante transformar o mundo e não mais apenas interpretá-lo.

As tecnologias possuem a capacidade de representação e reprodução dos valores de seus criadores. Por isso, o reconhecimento de tais valores permite imaginar e construir alternativas e novas formas de relacionamento com tais aparatos tecnológicos. Reimaginar a tecnologia é necessário para que seja possível reagir e remediar os problemas causados por ela (Silva, 2022). Ganhar consciência da opressão possibilita ações transformadoras (Freire, 1987).

Antonio Gramsci (2020) lembra que a ordem vigente se apresenta como estável, harmoniosa e coordenada, amedrontando cidadãos diante da incerteza das consequências das mudanças radicais. Para Alain Badiou (*apud* Crary, 2023), “a política emancipatória consiste sempre em fazer parecer possível justamente aquilo que, visto de dentro da situação, é declarado impossível”, ou seja, é no momento das impossibilidades que surgem as condições para insurgir. Para Jonathan Crary (2023), aqueles que mais declaram a impossibilidade também são seus maiores beneficiários. Antonio Gramsci (2020) argumenta que o programa liberal criou a ideia de Estado Ético superior às disputas de classe, o que constitui mais uma aspiração da política do que uma realidade de fato, mas a ideia de sua existência faz-se força de sua conservação e afasta a luta pela substituição do Estado Liberal.

Contudo, sobre as utopias, Gramsci (2020) diz que seu defeito reside na crença de que é possível prever os fatos. Para o autor, é possível apenas prever princípios ou máximas jurídicas (o direito, a jurisprudência e a moralidade implementada) que são criações humanas enquanto vontade. Por isso, precisam estar no escopo do que podem ser para não murcharem depois do primeiro entusiasmo. Faz-se cada vez mais necessário pensarmos em deixar nascer o novo, pois é verdadeiro que permanecemos no mesmo capitalismo que expropria mais-

[43] El Derecho ao Delirio, de Eduardo Galeano. Disponível em https://www.youtube.com/watch?v=Z3A9NybYZj8. Acesso em 23 dez 2023.

valor e reifica subjetividades e que esse encontra novos modos de explorar e apropriar-se da existência (Faustino; Lippold, 2023).

Para sonhar, é preciso ter espaços vazios. Segundo Zygmunt Bauman (2012), esses espaços são capazes de estimular a curiosidade, incitar à ação e dão coragem, confiança e determinação. Contudo, o conhecimento e a informação acumulados são uma ameaça à autoconfiança. Diante de todo o processo de comodificação da vida, ainda restam algumas atitudes possíveis. Dentre elas, figura a esperança e a "confiança que o ser humano tem de ser sensato e digno", tornando o mundo um lugar mais amigável e "mais hospitaleiro para a dignidade humana" (Bauman, 2012).

Cidadãos precisam retomar seu lugar de modo que deixem de permitir que suas decisões sejam tomadas por processos algorítmicos (Garcia Canclini, 2019). A desesperança precisa dar lugar ao desejo de lutar por melhores condições. Como lembra Bauman (2012), as condições materiais não tornam as escolhas inevitáveis, pois o ser humano é, por definição, um ser que escolhe.

> Em todas as línguas humanas existe uma partícula "não" que nos permite negar e rejeitar "a realidade da evidência"; e um tempo verbal futuro que nos permite imaginar uma gama de diferentes situações diversas das normalmente tidas como "óbvias" (Bauman, 2012).[44]

Segundo Matteo Pasquinelli e Vladan Joler (2020), nós devemos desafiar o misticismo frente à inteligência artificial, o que envolve a definição técnica de inteligência e a forma política de sua pretensa autonomia diante da sociedade e do humano. Ainda segundo os autores, a expressão inteligência artificial carrega em si o mito da autonomia da tecnologia, pois "mistifica dois processos de alienação: a crescente autonomia geopolítica das empresas de alta tecnologia e a invisibilização da autonomia dos trabalhadores" ao redor do mundo, tornando, no século XXI, o projeto moderno de mecanizar a razão humana "em um regime corporativo extrativista do conhecimento e um colonialismo epistêmico" (Pasquinelli; Joler, 2020).

Reconhecer o modo como o colonialismo de dados opera permite que seus danos e consequências sejam respondidos. O conceito de colonialismo de dados

[44] A canção Trova do Vento que Passa de Adriano Correia de Oliveira, composta por Manuel Alegre, cuja letra diz que "Mesmo na noite mais triste/ em tempo de servidão/ há sempre alguém que resiste/ há sempre alguém que diz não". Está disponível em: https://www.youtube.com/watch?v=McRqaiBmIT4. Acesso em: 03 jan. 2024.

permite compreender as opressões promovidas pela dataficação na atualidade, o que inclui os impactos materiais da extração massiva de dados no bem-estar das pessoas (Pereira; Couldry, 2023).

Uma parte importante da luta por igualdade precisa da criação de arranjos comunitários e individuais que se afastem da dominação mercadológica sobre as vidas humanas em coletivo. Uma parte fundamental da luta por uma sociedade mais igualitária no futuro próximo envolve “a criação de arranjos sociais e pessoais que abandonem a dominância do mercado e do dinheiro sobre nossas vidas em coletividade” (Crary, 2023, p. 10). Em sociedades “em que o principal fator de produção é o conhecimento, os processos colaborativos são simplesmente muito mais produtivos do que a competição” (Dowbor, 2022, p. 62).

Segundo Tarcízio Silva (2022), algumas diretrizes podem auxiliar para que lidemos com tecnologias emergentes. Elas incluem medidas no âmbito do Estado e das instituições privadas:

> • estados devem tomar medidas imediatas e efetivas, particularmente nos campos de ensino, educação, cultura e informação, com o objetivo de combater preconceitos que levam a discriminação racial;
> • prevenir e eliminar discriminação racial no desenho e uso de tecnologias digitais emergentes requer adereçar esforços para resolver a “crise de diversidade”;
> • deve-se tornar avaliações de impactos em direitos humanos, igualdade racial e não discriminação um prerrequisito para a adoção de sistemas baseados em tais tecnologias por autoridades públicas;
> • estados devem garantir transparência e prestação de contas sobre o uso de tecnologias digitais emergentes pelo setor público e permitir análise e supervisão independente, utilizando apenas sistemas que sejam auditáveis;
> • frameworks e regras de conduta desenvolvidas para permitir regulação e governança flexíveis, práticas efetivas de tecnologias digitais emergentes devem ser fundamentadas em princípios internacionais vinculativos de direitos humanos (Silva, 2022).

Cathy O'Neil (2020) lembra-nos que os modelos matemáticos presentes nos algoritmos devem ser ferramentas e não mestres das atividades humanas. Cinco princípios devem nortear a ética diante dos algoritmos. São eles: a beneficência, a não maleficência, a autonomia, a justiça e a explicabilidade (Floridi; Cowls *apud* Silva, 2022)

Para reduzir os danos provocados por algoritmos de destruição em massa (O'Neil, 2020), é preciso mensurar o impacto das ferramentas e promover auditorias dos algoritmos. Tarcízio Silva (2022) destaca que a reunião de evidências sobre os

pontos frágeis de sistemas algoritmos é multidisciplinar, pois essas não devem ser apenas computacionais ou baseadas em auditorias de código, mas fundamentadas em relatos, pesquisas etnográficas e investigações científicas e de jornalistas. Esses elementos acabam por ter impactos diferentes em contextos políticos, econômicos e sociais diversos.

A implementação de regulamentações justas e de transparência dos algoritmos é necessária, mas não é o suficiente (Morozov; Bria, 2019). Por isso, é preciso reconhecer que alguns problemas não poderão ser consertados por algoritmos. Antes de pensar na melhora dos modelos, é preciso reconhecer suas limitações para a resolução de problemas sociais complexos. Alguns algoritmos não poderão ser consertados, então devem ser descartados ou adiados (O'Neil, 2020). Nessa categoria, incluo TRFs.

Matteo Pasquinelli e Vladan Joler (2020) propõem que não se estude apenas o funcionamento da tecnologia, mas também como “quebram”, ou seja, “como os sujeitos se rebelam contra seu controle normativo e os trabalhadores sabotam suas engrenagens”. Destacam para isso a observação de práticas de *hacking* como um método importante de produção de conhecimento. Os autores o exemplificam com formas de ativismo de contra-vigilância feitas para sistemas de reconhecimento facial, como a proposta pelo artista e pesquisador de IA Adam Harvey que

> inventou um tecido de camuflagem chamado HyperFace que engana os algoritmos de visão de computador para ver vários rostos humanos onde não há nenhum. O trabalho de Harvey provoca a pergunta: o que constitui uma face para um olho humano, por um lado, e para um algoritmo de visão computacional, por outro? As falhas neurais do HyperFace exploram essa lacuna cognitiva e revelam qual é a aparência de um rosto humano para uma máquina. Essa lacuna entre a percepção humana e da máquina ajuda a introduzir o crescente campo de ataques adversariais (Pasquinelli; Joler, 2020).

Acrescento que a pirataria de livros, músicas e artigos científicos tem sido instrumento importante de acesso à informação e cultura para diversos grupos. Além disso, é inegável a participação da importância das práticas *hacking* no Wikileaks, que demonstrou como a espionagem tornou-se parte do cotidiano, após 11 de setembro de 2001 (Assange, 2015). É nas contradições do capitalismo que surgem novas formas de resistência (Faustino; Lippold, 2023).

> Descolonizar a tecnologia e confrontar a *mission civilizatrice* em noves moldes *high-tech* é, antes de qualquer coisa, colocar em xeque o caráter destrutivo do modo de produção capitalista em todas as suas dimensões sutis e declaradas. Essa crítica radical, no entanto, não nos isenta de nos posicionarmos diante de um campo que ainda está em construção e, portanto, permeável a uma série de disputas (Faustino; Lippold, 2023, p. 189).

De que maneira comunidades e ativistas têm resistido à implementação de ferramentas de vigilância e controle e, em especial, de reconhecimento facial?

Uma das maneiras de lutar contra os danos potenciais ou não das redes sociotécnicas é a arte, conforme lembrou Pasquinelli e Joller (2020) e como também citei logo no início deste trabalho, ao referenciar os artistas Banksy e Weiwei. Pamela Ramirez M. (2023) lembra que o artivismo é uma forma de resistência com raízes históricas na América Latina, e que utiliza a arte para combater desigualdades.

Além de expressões artísticas, movimentos contrários ao uso de reconhecimento facial têm a ganhar com a aproximação das comunidades mais afetadas por projetos de TRFs, com o entendimento de suas necessidades e com a capacidade de demonstrar de que maneira esse tipo de projeto pode impactar suas vidas. Isso pode fortalecer movimentos de resistência e criar alternativas futuras com maior impacto, conforme lembra Kainen Bell (2023).

Em Recife, na campanha *Sem Câmera na Minha Cara*, movimentos comunitários e organizações voltadas para a defesa dos direitos humanos assinaram uma Carta Aberta para que fosse retirado de um projeto da prefeitura da cidade a presença de câmeras com tecnologia de reconhecimento facial. Suas preocupações incluíam a fragilidade dos protocolos de controle de dados, a falta de transparência sobre o acesso dos dados por parte de companhias privadas e a possibilidade de discriminação algorítmica de raça e/ou gênero (Bell, 2023). A carta não foi a única forma de atuação: ativistas fizeram campanha nas ruas e participaram de audiências públicas sobre o uso de TRFs na cidade. A Defensoria Pública do Estado publicou notícia que trazia que a tecnologia não seria implementada “enquanto não forem realizadas discussões amplas com a sociedade civil e com técnicos da área a fim de aperfeiçoar as ferramentas” (Tecnologia..., 2023).

No campo das mediadas paliativas, é preciso ampliar a rede de indivíduos interessados em fiscalizar projetos de reconhecimento facial e de inteligência

algorítmica. O aumento dessa rede vai permitir que os projetos possam ser conhecidos e fiscalizados em um número maior de cidades, estados e países.

É necessária a nutrição de uma cultura de transparência que coloque fim à corrupção (Morozov; Bria, 2019). Nesse sentido, projetos de implementação de TRFs devem ser transparentes quanto aos objetivos, custos, taxas de falsos positivos e de falsos negativos. Além disso, comunidades devem ser consultadas quanto ao uso desse tipo de tecnologias em escolas, estádios, cidades inteiras e no acesso a serviços públicos.

Perceber algoritmos como forças neutras e inevitáveis é uma forma de abdicar da responsabilidade humana (O'Neil, 2020). É preciso reconhecer que mais serviços oferecidos em e por meio de redes sociotécnicas não serão capazes de consertar problemas sociais complexos (Nemer, 2023). Por isso, sua utilização precisa ser colocada no cerne do debate político, ampliada socialmente e a decisão sobre o uso coletivizada. E aí fica evidente a importância do papel das cidades no processo.

Rafael Zanatta (2019) destaca a proposta de Eugeny Morozov e Francesca Bria (2019) diante do grande desafio da construção de “cidades rebeldes” e “soberania tecnológica”. O autor destaca quatro intervenções propostas em políticas de cidades inteligentes:

> A primeira é a possibilidade de que contratos com empresas privadas deem ênfase ao software livre e a alternativas open source, garantindo que os códigos sejam reutilizados, auditados e aproveitados pela comunidade. A segunda é a demonstração de que o interesse local é de fato atingido por esses projetos, evitando processos de captura por parte de agentes decisórios no nível executivo. A terceira é a possibilidade de múltiplas experimentações em escalas menores, permitindo que projetos que não gerem valor aos cidadãos sejam descartados. A quarta – e mais ousada – é a criação de regimes de governança coletiva de dados sobre pessoas, ambientes, objetos conectados, transporte e sistemas de energia. No limite, o que se defende nesse quarto ponto é a mudança do regime de propriedade dos dados, criando mecanismos jurídicos, econômicos e de governança para fortalecer o controle coletivo aos “bens comuns digitais” gerados pelos próprios cidadãos (Zanatta, 2019, posição 94-98).

É preciso reforçar o debate sobre soberania digital para combater o colonialismo digital. Deivison Faustino e Walter Lippold (2023, p. 13) apontam que a

“descolonização da tecnologia passa pela compreensão, pela ação e pelo controle dos meios tecnológicos por parte dos trabalhadores da periferia do capitalismo”.

Muitos projetos de TRFs estão inclusos na ideia de que as cidades devem se tornar inteligentes. Nesse sentido, é preciso desmistificar a ideia de *smart*, de modo a demonstrar que projetos de smart *cities* são uma continuação expandida e potencializada de pautas neoliberais de privatização e terceirização. O esforço para se opor ao paradigma neoliberal das *smart cities* depende da capacidade de organização de cidades corajosas para ousar desafiá-lo.

O acesso ao conhecimento comum, a dados abertos e infraestruturas urbanas deve ser visto como um modo de garantir qualidade de vida e melhores serviços públicos, o que depende do resgate de conhecimentos, dados e infraestruturas de tecnologia que são primordiais e frequentemente estão sob o controle de poucos prestadores de serviços. A soberania digital – o que inclui a utilização de softwares e estruturas livres – deve ser percebida como pré-requisito para a promoção de uma pauta tecnológica que seja efetivamente democrática e tenha potencial para constituir economias produtivas novas e possibilitar que o conhecimento seja compartilhado (Zanatta, 2019).

Serão os cidadãos capazes de reconquistar a soberania popular sobre a tecnologia? Para Eygene Morozov (2020), isso somente ocorrerá se antes formos capazes de reconquistar a soberania no campo da economia e da política. Se a maior parte das pessoas se encontra incapaz ou indisposta para buscar “uma alternativa genuína tanto ao capitalismo global como ao predomínio do mercado na vida social” (Morozov, 2020), então, não restará esperanças. A subjetividade neoliberal acabaria por destruir todos os novos valores embutidos nas redes sociotécnicas.

Sem um esforço conjunto a favor da soberania tecnológica, a luta pelo direito às cidades perde muito de sua força. Por isso, a aliança entre movimentos sociais é tão importante e deve ser fortalecida ao elaborar políticas públicas sobre soberania tecnológica e digital. São alianças preciosas aqueles movimentos que buscam a transformação dos recursos em bem comum e que fazem a defesa da administração dos “recursos públicos, como a água, o ar e a energia elétrica, e o fornecimento de moradia e de saúde pública sob a categoria mais geral do “direito à cidade”” (Silveira, 2019), conforme demonstrou Bell (2023) ao evidenciar a união de movimentos sociais em Recife.

O significado de soberania tecnológica também deve incluir a capacidade de organização de seus próprios interesses por parte de cidades e cidadãos distantes da lógica de pensamento neoliberal que reside por trás de mecanismos de métrica e quantificação. Na construção da soberania digital, destaca-se a importância do movimento de dados abertos, pois podem ajudar comunidades a desenvolverem alternativas de plataformas com demandas predatórias. (Zanatta, 2019). O movimento de dados abertos pode se relacionar com o movimento já existente na ciência, que é o Ciência Cidadã ou Ciência Aaberta. Outro movimento que tem muito a oferecer nesse sentido é a Geração Cidadão de Dados (Mota; Vieira, 201-; Silva, 2017), como o Cocozap[45] e o Fogo Cruzado[46], por exemplo.

Vale destacar que o Brasil possui uma tradição estabelecida de uso de *software* livre e de políticas de dados abertos, o que advém dos diferentes movimentos sociais e de experiências de governo e da política.

Instituições públicas devem participar de processos que estimulem a cultura colaborativa entre cidadãos e comunidades, pois o setor público é capaz de auxiliar a sustentação e fortalecimento de redes e movimentos de comunidade, entregando mais ferramentas e instrumentos legais que favoreçam a auto-organização para mudanças sociais (Zanatta, 2019). Por isso, movimentos para a construção de alternativas ao desenvolvimento, como os citados, são importantes, pois carregam em si ideais de bem-estar comum e construção de redes.

Apesar da importância da discussão sobre soberania tecnológica e das ações de resistência do cotidiano, essas são formas de ganhar tempo enquanto a articulação de pautas políticas e econômicas mais ambiciosas sejam capazes de causar uma reversão nos danos das políticas neoliberais.

São diversas as formas de resistência às redes sociotécnicas, em uma multiplicidade de níveis. Há formas de resistência aos processos de datafication, algoritmização e automação; resistências nos níveis macro e micro da política; e, por último, resistências em vários domínios que vão do material ao imaterial como infraestruturas, práticas, imaginários (Ricaurte Quijano, 2023). A descolonização da tecnologia precisa passar por uma radical transformação do mundo e das formas de sociabilidade que nele existem (Faustino; Lippold, 2023). Deve-se questionar a ideia de que a tecnologia é capaz de promover grandes mudanças sociais para que seja

[45] Projeto do Datalabe: Disponível em: https://cocozap.datalabe.org. Acesso em: 17 jan. 2024.
[46] Fogo Cruzado: Disponível em: https://fogocruzado.org.br. Acesso em: 17 jan. 2024.

possível criar o entendimento de sociedade menos opressora, conforme lembra David Nemer (2023).

Alguns podem pensar que resistir à dataficação significa aprovar leis ou realizar ajustes técnicos. O que se propõe é que resistir à colonialidade de dados não acontece apenas ao mudar as tecnologias por trás dela. É preciso modificar as relações que governam a sociedade e a economia (Ricaurte Quijano, 2023).

Reconheço também que a palavra resistir pode transmitir a ideia de uma reação aos acontecimentos. Em parte, é verdade. A resistência acontece diante de algo. Contudo, para mim (e muitos outros, pois resistência é uma palavra importante nos movimentos sociais) resistir tem um sentido amplo: resistir é manter-se firme. Nesse sentido, a resistência é um dos mecanismos da práxis transformadora. A resistência também, ainda assim, deve ser acompanhada de outras ações para que seja possível transformar o mundo radicalmente.

As ações que apresentei aqui fazem parte da luta por justiça. Justiça hoje requer tanto reconhecimento quanto redistribuição (Fraser, 2003). Reconhecimento não no sentido de individuação neoliberal e/ou algorítmica, mas no sentido de aceitação do outro e de suas diferenças. A redistribuição deve atuar no sentido de reduzir as desigualdades existentes no capitalismo e inerentes a esse modo produção.

Apesar de reconhecer minha incapacidade de abordar todas ações e possibilidades, acredito que este estudo faz parte do processo comunitário para deixar que o novo possa, então, florescer[47]. Espero também que ele funcione como um convite para fazer parte das muitas formas de resistência que acontecem no cotidiano de cada um, pois, para citar a filósofa negra abolicionista Angela Davis (2015), “a liberdade é uma luta constante”.

[47] Traduzo muito humildemente as palavras de Octavia E. Butler, escritora negra estadounidense que, ao tentar responder “o que se pode fazer” disse “Eu quero dizer que não há uma resposta única que resolverá todos os nossos problemas do futuro. Não há pílula mágica. Em vez disso, há milhares de respostas, no mínimo. Você pode ser parte de uma delas, se você o quiser ser”. O ensaio completo de Octavia E. Butler está disponível em https://commongood.cc/reader/a-few-rules-for-predicting-the-future-by-octavia-e-butler/. Acesso em: 30 dez. 2023.

7 CONSIDERAÇÕES PARA ADIAR O FIM DO MUNDO

A liberdade é uma luta constante.
Angela Davis

Ailton Krenak, ambientalista, filósofo e líder indígena brasileiro, da etnia Krenak, escreveu em 2019 o livro *Ideias para Adiar o Fim do Mundo,* com provocações sobre a abstração civilizatória que nos distancia da Terra e dos demais seres viventes.

> Nosso tempo é especialista em criar ausências: do sentido de viver em sociedade, do próprio sentido da experiência da vida. Isso gera uma intolerância muito grande com relação a quem ainda é capaz de experimentar o prazer de estar vivo, de dançar, de cantar. E está cheio de pequenas constelações de gente espalhada pelo mundo que dança, canta, faz chover. O tipo de humanidade zumbi que estamos sendo convocados a integrar não tolera tanto prazer, tanta fruição de vida. Então, pregam o fim do mundo como uma possibilidade de fazer a gente desistir dos nossos próprios sonhos. E a minha provocação sobre adiar o fim do mundo é exatamente sempre poder contar mais uma história. Se pudermos fazer isso, estaremos adiando o fim. (Krenak, 2019)

Eu sei que, em geral, as considerações finais não contam com citações, mas acredito que Krenak vale o risco, pois também quero acreditar no potencial transformador desse trabalho e na desobediência epistemológica, ainda que tímida. Ainda assim, é preciso considerar ou concluir alguma coisa a partir dos muitos ditos anteriormente apresentados.

Primeiramente, gostaria de começar por retomar as hipóteses apresentadas: reafirmo que o videomonitoramento e o reconhecimento facial estão intrinsecamente ligados ao processo de terceirização da Segurança Pública, mas agora acrescento que da Educação também. Isso ocorre a partir de uma visão neoliberal de mundo – e o neoliberalismo visto também como aquilo que penetra o desejo e as projeções do que somos capazes. Contudo, é difícil provar porque os contratos ficam perdidos nas amarras da burocracia e em uma política generalizada de segredo. É difícil obter acesso à informação e mais difícil ainda navegar nos portais da transparência, depois de obter a informação solicitada por meio de pedidos de acesso. Além disso, a lógica neoliberal já está tão arraigada na sociedade que é difícil separar neoliberalismo de eficiência estatal, porque todo o discurso gira em torno da eficiência e os críticos são percebidos como críticos do progresso.

Acredito ter sido possível demonstrar que há, sim, diferenças consideráveis no discurso, diante da adoção de ferramentas de reconhecimento facial no que se refere aos espectros políticos da direita e da esquerda. Isso pode ser observado na dicotomia expressa em direitos individuais de intimidade, privacidade e proteção do patrimônio. As propostas legislativas que objetivam banir o reconhecimento facial no setor público por completo, ou na segurança pública, foram de partidos identificados com a esquerda (PSOL e PT, por exemplo), enquanto a maior parte das propostas a favor do reconhecimento facial, seja pela exigência de sua utilização seja pela regulamentação, foram provenientes de partidos identificados com a direita (PSL, DEM, PL e PMDB, por exemplo). Além disso, é também possível observar que a esquerda tem tentado amenizar o impacto de leis a favor de TRFs, durante o seu processo de aprovação, o que é uma dinâmica comum da política.

Acredito que a quantidade de erros provenientes do uso de TRFs no dia a dia faz com que os gastos com a adoção dessas ferramentas não compensem o resultado obtido. Contudo, apesar de tentar demonstrar o custo da utilização das ferramentas, é difícil afirmar que todas as pessoas chegarão à conclusão de que não compensam. Além disso, os poucos dados financeiros aos quais tive acesso dificultam ainda mais a missão de provar que essas tecnologias têm custo muito alto para o Estado enquanto oferecem muito pouco benefício, o que nos leva à última hipótese.

Definitivamente, há dilemas éticos que não são superados por uma forma global, mas sempre aparecerão em perspectiva. Por exemplo, a avaliação do que é mais importante entre privacidade e segurança, apesar da privacidade parecer levemente derrotada neste momento. Realmente, a privacidade tem perdido, mas não dá para dizer que a segurança tem alcançado alguma vitória para além do discurso. O aumento de tecnologias orientadas para vigilância ainda não tem conseguido diminuir crimes, como sua propaganda defende. Talvez nunca consiga. Por isso, é tão importante que as perspectivas diante do problema sejam colocadas. É proporcional colocar toda a população de 77 cidades da Bahia sob ferramentas de reconhecimento facial para prender cerca de duas mil pessoas em dois anos e ainda gastar R$665 milhões para isso? Eu espero ter conseguido mostrar que não é.

As questões relacionadas ao reconhecimento facial, à inteligência artificial, à datafication da vida, ao colonialismo de dados, ao colonialismo digital e ao

capitalismo não se encerram aqui. Já é possível pensar que caminhos gostaria de ter abordado com maior profundidade e que há sempre espaço em trabalhos futuros.

O primeiro deles está relacionado aos autores que gostaria de ter abordado melhor. Apesar de ter me aproximado de suas obras, acredito que elas têm muito a acrescentar nos debates sobre colonialismo de dados, colonialismo digital, soberania digital e inteligência algorítmica. Um deles é Eric Sadin e a noção de inteligência artificial como tecno-ideologia. Outro é Luciano Floridi que tem discutido ética da informação e inteligência artificial. Pretendo também me reaproximar da filosofia para, a partir dos escritos de Emmanuel Levinas, discutir a ética do eu e do outro que envolve a detecção de faces e de comportamentos automatizados, e da obra de Baruch Espinoza, para abordar a imaginação como emoção transformadora.

O segundo se refere à articulação entre os debates éticos do bem-viver, da ética feminista e da ética do cuidado, para aproximá-los da ética intercultural da informação. Acredito que estas aproximações podem fomentar o debate dentro daquilo que se define por ética intercultural da informação, ampliando suas perspectivas e olhares diante do mundo.

O último deles envolve aproximar a teoria crítica e a ciência da informação, no que podemos chamar de teoria crítica da informação. Acredito que os trabalhos de autores clássicos da teoria crítica, como Theodor Adorno, Max Horkheimer para, então, chegar em Axel Honneth, podem ser úteis para interpretar o tempo histórico em que vivemos atualmente e eu ainda quero poder me debruçar sobre suas obras com calma.

Certamente, há muito trabalho para ser feito ainda e eu espero que esta pesquisa sirva como um diagnóstico de nosso tempo sobre ferramentas de reconhecimento facial ou de um mundo em que elas não são uma realidade absoluta. Busquei analisar o regime de informação dominante de modo a evidenciar seus aspectos como atores, além de seus recursos preferenciais, seus dispositivos, regras e instituições.

Talvez em algum momento essas ferramentas estejam tão disseminadas que esta tese pareça uma história obsoleta de muito tempo atrás. Nos meus sonhos, ela terá sido um retrato de um caminho que percorríamos, mas mudamos de rota: chegaremos juntos na conclusão de que ferramentas de reconhecimento facial não valem os riscos. Sei que é utópico, mas, para citar Eduardo Galeano novamente, a utopia serve para que a gente não deixe de caminhar.

Ao longo deste texto, trouxe autores como Paola Ricaurte Quijano, Deivison Faustino, Walter Lippold, Ruha Benjamin, Nicky Couldry, Ulisses Mejias, Sygmund Bauman, David Lyon, Tarcízio Silva, Johnathan Crary, entre tantos outros para debater as configurações do capitalismo atualmente. A escolha por um predicado (de vigilância, datacêntrico ou de plataforma, por exemplo) baseia-se bastante nos aspectos que se pretende ressaltar do sistema. Contudo, o mais importante ainda reside nas consequências do sistema capitalista: desigualdades de gênero e raciais, exploração das pessoas e do meio-ambiente, de modo predatório. O reconhecimento facial é mais uma das ferramentas, ao fazer parte dos processos de extração massiva de dados do colonialismo digital. Não é o único, mas um elemento de um fenômeno muito maior de comodificação da vida humana, depois que diversos outros aspectos da existência já viraram *commodities*.

No capítulo *Da Informação no Capital*, busquei demonstrar o papel que a informação tem no capitalismo atualmente e ressaltar aspectos da vigilância massiva presente em nossas vidas. A vigilância é cada vez mais presente nos dispositivos que usamos de modo rotineiro, mas também nos serviços públicos. O modelo de negócio das redes sociotécnicas depende da extração e do processamento de dados massivamente realizados. O processo de comodificação da vida remete ao colonialismo de dados e tem consequências diferentes no Norte e no Sul Globais. Por sua vez, o colonialismo de dados remete ao colonialismo digital e à acumulação primitiva de dados. Os impactos dessa lógica de acumulação não param de crescer e afetam democracias, comunidades e modos de ser e estar no mundo. Ao moldar sociabilidades, a vigilância e a extração massiva de dados fazem sujeitos mais conformados dentro do regime capitalista. Será, então, a realização do sonho do controle e da disciplina do capital?

No capítulo *O Reconhecimento Facial pela Ótica da Política*, analisei a legislação proposta sobre o uso de ferramentas de reconhecimento facial no Brasil. Acredito ser possível concluir que o reconhecimento facial tem ganhado cada vez mais destaque no país, o que pode ser observado com o crescimento da legislação e do debate sobre o tema em todas as esferas, além do aumento de projetos em andamento com o uso dessas tecnologias. Busquei demonstrar o crescimento de projetos tanto federais quanto estaduais e a que setores as proposições são direcionadas. Nas câmaras legislativas, o debate ético tem aparecido como algo de solução simples, a partir da confiança da maior parte dos legisladores de que

tecnologias de reconhecimento facial são benéficas. Ainda assim, são muitos os exemplos que envolvem pessoas erroneamente identificadas, em casos de falsos positivos ou falsos negativos que foram abordados ao longo deste trabalho. Ainda são poucos os projetos voltados para a regulamentação da tecnologia. Contudo, crescem os que buscam seu banimento total ou parcial pelo setor público. Acredito que projetos contrários ao uso de TRFs também ajudam a fomentar o debate para, de alguma forma, criar mais consciência sobre o dano provocado por essas tecnologias.

No capítulo *Usos e Custos de Ferramentas de Reconhecimento Facial,* busquei demonstrar o mercado movimentado do TRFs no Brasil e no mundo. Tem sido crescente a utilização de ferramentas e o valor de mercado das empresas que oferecem *softwares* e câmeras têm crescido em igual medida. Empresas que oferecem soluções de reconhecimento facial estão na Segurança Pública, na educação, nas compras, no varejo, nos transportes. No setor público, TRFs têm se espalhado e ganham cada vez mais destaque. Neste trabalho, busquei evidenciar os estados que as adotam na Educação e na Segurança pública. Foi possível observar que elas já são uma realidade nessas áreas com uma tendência de crescimento. Se forem considerados os estados cuja tecnologia está em estudo, é possível que passemos de 4 estados para 10 na Educação e de 10 para 13 na Segurança Pública. Nesse sentido, a Educação dobraria e quase se igualaria ao número de projetos ligado à Segurança Pública. Tudo isso sem contar os estados "inconclusivos", que nada indicam que não tenham projetos de TRFs em andamento.

No capítulo *Problemas do Reconhecimento Facial no Mundo Real*, busquei tratar da questão ética da adoção de TRFs tanto pela quantidade de erros, como falsos negativos e falsos positivos, quanto por suas dimensões racistas, misóginas e transfóbicas. Às minorias oferece-se menos reconhecimento de seus problemas reais, de sua individualidade e das suas formas de comportamento. Seus prejuízos pelos erros da tecnologia são minimizados, pois são apenas um efeito colateral menor ou, para usar uma expressão da economia, uma externalidade.

Contudo, a vida das pessoas afetadas não deve ser vista como um problema pequeno, pois também é amplamente divulgada a truculência das polícias brasileiras e a violência do cárcere. Qualquer ferramenta que sirva não para humanizar a Segurança Pública e a Educação, mas para corroborar desigualdades, enquanto mascara suas determinações de modo fetichista, deve ser vista com desconfiança.

O reconhecimento facial tem problemas que não podem ser vistos apenas da perspectiva de melhora de bases de dados: uma melhor oferta de bases e algoritmos mais bem feitos e melhor treinados não será capaz de resolver os problemas complexos da Educação e da Segurança Pública no Brasil. Também vale destacar que a mediação algorítmica para acessar direitos pode prejudicar indivíduos que não se enquadram dentro da lógica binária que é própria dos algoritmos. Esses só são problemas insolúveis na medida em que se insiste neles. Sempre é tempo de parar o que está sendo feito e seguir em outra direção.

No capítulo Para Imaginar o Novo, busquei evidenciar formas de combater o colonialismo digital e o colonialismo de dados, o reconhecimento facial e criar possibilidades para que seja possível vislumbrar o novo. Mostrei ações, como as campanhas nacionais pelo banimento do reconhecimento facial, *Tire o meu Rosto da sua Mira* e *Sem Câmera na Minha Cara,* do Recife. Aliás, a vitoriosa campanha recifense, que recebeu do poder público o compromisso de não usar TRFs antes de debate. Por isso, é também importante celebrar as vitórias. Aliás, as pequenas vitórias são motor poderoso para a imaginação.

A verdade é que tenho poucas respostas sobre o que usaremos, se não usarmos reconhecimento facial. Defendo que possamos imaginar juntos um novo mundo com menos tecnologias orientadas para a vigilância, invadindo nossas casas e corpos. Estou de acordo com Paola Ricaurte Quijano, ao lembrar que a tomada de consciência sobre o modo como o colonialismo de dados afeta nossa vida já é uma forma de combatê-lo. A tomada de consciência é uma ferramenta poderosa para a transformação. Depois disso, a construção e o fortalecimento de redes comunitárias com o objetivo de transformação do *status quo*. E essas redes podem ser construídas a partir de políticas de distribuição e reconhecimento aliadas à ampliação de perspectivas éticas, como a ética intercultural da informação, mas não apenas. É preciso reconhecer e incorporar novas tradições de pensamento que sejam mais coletivistas e com objetivo de oferecer alternativas ao modelo de desenvolvimento da atualidade. Nesse ritmo, o fim do mundo não poderá mais ser adiado.

Algumas considerações precisam ainda ser feitas:

Tenho muitas vezes a sensação de que os dados já nasceram obsoletos, porque os projetos de implementação de TRFs são muitos. Por exemplo, o caso do estado de Sergipe: fui informada por meio do pedido de acesso à informação que

não havia TRF em uso ou em estudo em março. Contudo, poucos meses depois, em novembro, a tecnologia de reconhecimento facial foi utilizada. Ainda assim, acho importante ter tentado mapear esses projetos para, de algum modo, conseguirmos perceber o seu crescimento e acompanhá-los.

Foi possível observar a lentidão com que projetos de lei sobre o tema são aprovados, enquanto os Poderes Executivos parecem correr para colocar TRFs em uso. Tecnologias de reconhecimento facial também têm servido como propaganda de eficiência governamental e modernidade dos serviços públicos.

Esbarrei na dificuldade do acesso à informação no Brasil, conforme apontado anteriormente. Foram muitos pedidos negados, pedidos não respondidos, acessos que não funcionavam corretamente. Assumo que fui otimista sobre os dados que conseguiria obter. Fui também audaciosa demais ao querer abarcar aspectos políticos, éticos e econômicos. Ainda assim, acredito ter sido importante para conseguir realizar um diagnóstico da adoção de TRFs no Brasil hoje. Reconheço que incompleto, como todos os diagnósticos da realidade o são.

Assumo a dificuldade de criar comparações econômicas e o desejo de evitar sensacionalismos para deixar que as pessoas cheguem às suas próprias conclusões, a partir dos dados e análises apresentados. Afinal de contas, R$665 milhões investidos em Segurança Pública é diferente do mesmo valor investido em Educação. É difícil comparar valores e afirmar quantos professores ou policiais isso vale. Inclusive, porque os salários de professores e policiais são baixos e nem eles valem o quanto realmente valem. Ainda assim, gostaria de ter podido trazer uma maior quantidade de dados nesse sentido. Acredito que a economia e sua pretensa objetividade ajudam a colocar os debates em terreno comum, que era um dos meus principais objetivos com este trabalho.

Tenho o desejo de permanecer acompanhando a tramitação de projetos de lei, principalmente nos estados que já utilizam a tecnologia. É interessante perceber o tempo entre o uso de determinada tecnologia e a sua regulamentação. Além disso, quero continuar a acompanhar a adoção de ferramentas pelos estados brasileiros e me aventurar a identificar sua adoção por municípios. Por sorte, não estou sozinha na missão e outros também têm observado o modo como ferramentas de reconhecimento facial têm se espalhado pelo Brasil.

Busquei, ao longo deste trabalho, apontar discursos políticos, além de impactos econômicos e éticos da adoção de ferramentas de reconhecimento facial

no Brasil. Fiz isso de maneira ampla de modo a abranger os três aspectos e espero ter cumprido o objetivo de promover um diagnóstico de época a respeito da utilização de um tipo de tecnologia que também servirá para que outros explorem e analisem outros tipos. Quis contar uma parte da história do reconhecimento facial no Brasil.

Para adiar o fim do mundo é preciso contar mais histórias de modo a construir um novo mundo com relações baseadas em solidariedade e respeito mútuo. Para adiar o fim do mundo é preciso construir todos os dias esse novo mundo.

REFERÊNCIAS

ADORNO, Luis. Como PMs de São Paulo manipulam o sistema de câmeras corporais. **Tab Uol**, São Paulo, 20 dez. 2023. Disponível em: https://tab.uol.com.br/noticias/redacao/2023/12/20/como-pms-de-sao-paulo-manipulam-o-sistema-de-cameras-corporais.htm. Acesso em: 22 jan. 2024.

AGUIRRE, Katherine; BADRAN, Emile; MUGGAH, Robert. **Future Crime**: assessing twenty first century crime prediction. [S./.]: Igarapé Institute, 2019. Disponível em: https://igarape.org.br/wp-content/uploads/2019/07/2019-07-12-NE_33_Future_Crime.pdf. Acesso em: 12 nov. 2022.

ALAGOAS. Assembleia Legislativa. **Indicação Legislativa 546/2017**. Solicitando a instalação de catracas com controle de biometria para acesso a estádios de futebol com capacidade de mais de 10 mil pessoas. Maceió, 2017. Disponível em: https://sapl.al.al.leg.br/media/sapl/public/materialegislativa/2017/3439/3439_texto_integral.pdf. Acesso em: 16 ago 2024.

ALAGOAS. **Lei nº 8.113/2019, de 29 de maio de 2019.** Dispõe sobre a autorização e a regulamentação da venda e do consumo de bebidas alcoólicas em eventos desportivos no Estado de Alagoas E no art. 5º fica autorizada a instalação de sistemas de reconhecimento facial nos estádios localizados no Estado. Maceió, 2019. Disponível em: https://sapl.al.al.leg.br/media/sapl/public/normajuridica/2019/1594/lei_no_8.113_de_29.05.2019.pdf. Acesso em: 5 jun. 2024.

ALAGOAS. **Lei nº 7.333/2012, de 05 de janeiro de 2012.** Desenvolver ações preventivas e agilidade no combate a criminalidade, através de tecnologia capaz de realizar reconhecimento facial, identificação de movimentos e placas de veículos, diminuindo o índice de criminalidade, utilizando uma moderna ferramenta tecnológica. Maceió, 2012. Disponível em: https://sapl.al.al.leg.br/media/sapl/public/normajuridica/2012/686/686_texto_integral.pdf. Acesso em: 5 jun. 2024.

ALENCAR, Itana. Com mais de mil prisões na BA, sistema de reconhecimento facial é criticado por 'racismo algorítmico'; inocente ficou preso por 26 dias. **G1,** Bahia, 01 set. 2023. Disponível em: https://g1.globo.com/ba/bahia/noticia/2023/09/01/com-mais-de-mil-prisoes-na-ba-sistema-de-reconhecimento-facial-e-criticado-por-racismo-algoritmico-inocente-ficou-preso-por-26-dias.ghtml. Acesso em: 22 jan. 2024.

ALVES, Thiara dos Santos; BEZERRA, Arthur Coelho. INFORMAÇÃO, POLÍTICA E PODER: 20 anos do conceito de ⁖regime de informação⁖ em maria nélida gonzález de gómez. In: ENCONTRO NACIONAL DE PESQUISA E PÓS-GRADUAÇÃO EM CIêNCIA DA INFORMAÇÃO, Não use números Romanos ou letras, use somente números Arábicos., 2019, Florianópolis. **Anais [...]** . Florianópolis: Ufsc, 2019. p. 1-20. Disponível em: https://brapci.inf.br/#/v/122938. Acesso em: 14 ago. 2024.

AMÂNCIO, Thiago. Plano de Doria para interligar 10 mil câmeras de segurança em SP empaca: a 1 ano do prazo, sistema na capital tem 2.940 equipamentos e baixa

adesão de condomínios. **Folha de São Paulo**. São Paulo. 15 nov. 2019. Disponível em: https://www1.folha.uol.com.br/cotidiano/2019/11/plano-de-doria-para-interligar-10-mil-cameras-de-seguranca-em-sp-empaca.shtml. Acesso em: 19 maio 2021.

AMAPÁ. Assembleia Legislativa. **Projeto de Lei nº 0091/2019.** Institui o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos no estado do Amapá. Macapá, 2019.

AMAZONAS. Assembleia Legislativa. **Indicação Legislativa 7494/2018.** Instalação de câmeras de reconhecimento facial nos ônibus do Município de Manaus/AM, para combater assaltos. Manaus, 2018. Disponível em: https://sapl.al.am.leg.br/materia/131628. Acesso em: 16 ago 2024.

AMAZONAS. Assembleia Legislativa. **Projeto de Lei nº 02/2019.** Determina o uso de ferramentas de biometria digital nas viaturas policiais de todo o estado do Amazonas. Manaus, 2019. Disponível em: https://sapl.al.am.leg.br/materia/132099. Acesso em: 5 jun. 2024.

AMAZONAS. Assembleia Legislativa. **Projeto de Lei nº 196/2018.** Determina o uso de ferramentas de biometria digital nas viaturas policiais de todo o estado do Amazonas. Manaus, 2018. Disponível em: https://sapl.al.am.leg.br/materia/131690. Acesso em: 5 jun. 2024.

AMNESTY INTERNATIONAL. **Automated Apartheid**: how facial recognition fragments, segregates and controls palestinians in the opt**.** Londres: Amnesty International, 2023. Disponível em: https://banthescan.amnesty.org/opt/wp-assets/Automated_Apartheid.pdf. Acesso em: 22 jan. 2024.

ANTUNES, Ricardo. **O privilégio da servidão:** o novo proletariado de serviços na era digital. São Paulo: Boitempo, 2018.

ARRUDA, Wellington. Oi anuncia expansão de projeto de vigilância e segurança que começou no RJ. **Canal Tech.** [S.l.], 22 mar. 2019. Disponível em: https://canaltech.com.br/infra/oi-anuncia-expansao-de-projeto-de-vigilancia-e-seguranca-que-comecou-no-rj-135343/. Acesso em: 21 maio 2021.

ASSANGE, Julian. **Quando o Google encontrou o WikiLeaks**. São Paulo: Boitempo, 2015.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Nota Técnica no 175/2023/CGF/ANPD. S.L: Anpd, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf. Acesso em: 22 jan. 2024.

BAHIA. Assembleia Legislativa. **Projeto de Lei nº 22.451/2017.** Obriga a utilização de sistema de identificação biométrica nas entradas de estádios com capacidade superior a 10.000(dez mil) pessoas, nos dias de jogos de futebol e dá outras providências. Salvador, 2017. Disponível em: https://www.al.ba.gov.br/atividade-legislativa/proposicao/PL.-22.451-2017. Acesso em: 5 jun. 2024.

BAHIA. Assembleia Legislativa. **Projeto de Lei nº 24813/2023.** Autoriza a inclusão do reconhecimento facial como forma de acesso e controle de presença nas Escolas Públicas Estaduais, e dá outras providências. Salvador, 2023.

BARATTA, Alessandro. Ética e pós-modernidade. *IN:* Kosovosky, Ester (org.). **Ética e comunicação**. Rio de Janeiro: Mauad, 1995, p. 113-131.

BARDIN, Laurence. **Análise de Conteúdo**. Lisboa: Edições 70, 1977.

BAUMAN, Zygmunt; LYON, David. **Vigilância Líquida**. Rio de Janeiro: Editora Zahar, 2013.

BAUMAN, Zygmunt. **Capitalismo Parasitário**: e outros temas contemporâneos. Rio de Janeiro: Editora Zahar, 2012.

BAYLEY, David. **Padrões de Policiamento.** São Paulo: Editora da Universidade de São Paulo, 2017.

BELL, Kainen. Resistance storytelling: Anti-Surveillance campaign in Recife, Brazil. In: THE TIERRA COMÚN NETWORK. **Resisting Data Colonialism :** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023. p. 63-68. Disponível em: https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

BENJAMIN, Ruha. **Race After Technology:** Abolitionist Tools for the New Jim Code. Medford, MA: Polity, 2019.

BENJAMIN, Ruha. **Viral Justice:** how we grow the world we want. Princeton: Princeton University Press, 2022.

BEZERRA, A. C.; COSTA, C. M. da. Pele negra, algoritmos brancos: informação e racismo nas redes sociotécnicas. **Liinc em Revista**, *[S. l.]*, v. 18, n. 2, p. 01-14, 2022. DOI: 10.18617/liinc.v18i2.6043. Disponível em: https://revista.ibict.br/liinc/article/view/6043. Acesso em: 9 dez. 2022.

BEZERRA, Arthur Coelho. Da teoria matemática para uma proposta de teoria crítica da informação: a integração dos conceitos de regime de informação e competência crítica em informação. **Perspectivas em Ciência da Informação**, [S.l.], v. 25, n. 3, p. 182-201, jul. 2020.

BEZERRA, Arthur Coelho. Teoria Crítica da Informação: proposta teórico-metodológica de integração entre os conceitos de regime de informação e competência crítica em informação. In: BEZERRA, Arthur Coelho; SCHNEIDER, Marco; PIMENTA, Ricardo M.; SALDANHA, Gustavo Silva. **IKRITIKA**: estudos críticos em informação. Rio de Janeiro: Garamond, 2019. p. 15-72. Disponível em: https://www.garamond.com.br/wp-content/uploads/2020/06/iKr%C3%ADtika_Livro.pdf?thwepof_product_fields=. Acesso em: 11 nov. 2022.

BEZERRA, Artur Coelho; CAPURRO, Rafael; SCHNEIDER, Marco. Regimes de verdade e poder: dos tempos modernos à era digital. **Liinc em Revista**, Rio de Janeiro, v.13, n.2, p. 371-380, nov. 2017. Disponível em: http://revista.ibict.br/liinc/article/view/4073. Acesso em 22 nov. 2020. Acesso em 11 nov. 2022.

BIGO, Didier; ISIN, Engin; RUPPERT, Evelyn. Data Politics. IN: Bigo, Didier; ISIN, Engin; RUPPERT, Evelyn. **Data Politics**: worlds, subjects, rights. Nova York: Routledge, 2019. p. 1-16.

BISCHOFF, Paul. **Surveillance camera statistics**: which cities have the most CCTV cameras? 2022. Disponível em: https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/. Acesso em: 12 set. 2022.

BOBBIO, Norberto. **Democracia e Segredo.** São Paulo: Editora Unesp, 2015.

BRAGA, Giampaollo Morgado; ARAÚJO, Vera. Câmeras em uniformes de PMs não reduzem mortes em primeiro mês de uso. **Extra.** Rio de Janeiro. 01, ago. 2022. Disponível em: https://extra.globo.com/casos-de-policia/cameras-em-uniformes-de-pms-nao-reduzem-mortes-em-primeiro-mes-de-uso-25549673.html. Acesso em: 06 set. 2022.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 879/2003.** Obriga as empresas de ônibus a terem GPS e câmeras de vídeo. Brasília, 2003a Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=113531. Acesso em: 09 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 1877/2003.** Dá nova redação ao art. 3º, letra "e" da Lei nº 7.116 de 09 de agosto de 1983. Brasília, 2003b. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=131430&fichaAmigavel=nao. Acesso em: 09 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 3372/2004.** Dispõe sobre mecanismos de segurança para acesso aos sistemas e bancos de dados da Administração Pública Federal. Brasília, 2004. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=249679. Acesso em: 09 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 5034/2005.** Inclui dados na carteira de identidade e dá outras providências. Brasília, 2005. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=281181. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 1230/2007.** Estabelece que o credenciamento e autenticação de usuário para proceder alterações de informações em sistemas e bancos de dados nos setores de arrecadação de tributos, pagamentos diversos e de pessoal na Administração Pública Federal será dotado de características biométricas (impressão digital, reconhecimento facial ou da íris) ou outro mecanismo tecnológico. Brasília, 2007. Disponível em:

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=353978. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 7902/2010.** Modifica o art. 1º da Lei nº 9.454, de 7 de abril de 1997, que "Institui o número único de Registro de Identidade Civil e dá outras providências.". Brasília, 2010. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=node01om9hjfe299tpnpexqp87tgek9397651.node0?codteor=823113&filename=Avulso+-PL+7902/2010. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 7759/2014.** Altera a Lei nº 9.454/1997, que institui o número único de Registro de Identidade Civil e dá outras providências, tornando obrigatória a identificação biométrica para a emissão de documento de identidade. Brasília, 2014b. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=619449. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 7461/2014.** Altera a Lei nº 9.454, de 7 de abril de 1997, para vincular o Cadastro Nacional de Registro de Identificação Civil, ao sistema biométrico, previsto na Lei nº 12.034, de 29 de setembro de 2009, e dá outras providências. Brasília, 2014a. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=613390. Acesso em: 11 jan. 2014.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº PL 4413/2016.** Torna obrigatória a implantação de sistema de controle de freqüência de alunos em escolas públicas - Frequência Digital Escolar. Brasília, 2016c. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2077399. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº PL 6154/2016.** Institui a destinação 2% do total dos Recursos do Pré Sal destinados à Educação, nos termos da Lei Nº 12.351, de 22 de dezembro de 2010, para implantação de Sistema de Frequência Digital Escolar - controle de freqüência de alunos em escolas públicas. Brasília, 2016b. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1492438&filename=Despacho-PL+6154/2016-22/09/2016. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº PL 5699/2016.** Obriga a instalação de equipamentos de identificação biométrica em aeroportos. Brasília, 2016a. Disponível em: https://www.camara.leg.br/propostas-legislativas/2089587. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº PL 9414/2017.** Obriga a instalação da leitura de impressão digital e facial nos meios de transportes públicos coletivos. Brasília, 2017. Disponível em: https://www.camara.leg.br/propostas-legislativas/2166846. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Decreto Legislativo nº 674/2019.** Susta os efeitos do Decreto 10.047, de 09 de outubro de 2019, que dispõe sobre a governança do Cadastro Nacional de Informações Sociais e institui o programa Observatório de Previdência e Informações, no âmbito do Cadastro Nacional de Informações Sociais. Brasília, 2019a. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2226412. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Decreto Legislativo nº 675/2019.** Susta os efeitos do Decreto 10.046, de 09 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados. Brasília, 2019b. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2226413. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 1745/2019.** Altera a Lei nº 12.527, de 18 novembro de 2011 - Lei de Acesso à Informação, para ampliar as hipóteses de acesso a dados públicos pelos administrados. Brasília, 2019c. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2195396. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 2537/2019.** Obriga o aviso sobre o reconhecimento facial em estabelecimentos comerciais. Brasília, 2019d. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2199418. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 4612/2019.** 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, 2019e. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2216455. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 4827/2019.** Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), para dispor sobre o uso de dispositivo móvel de segurança para conferir maior efetividade às medidas protetivas de urgência. Brasília, 2019f. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2218307. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 4828/2019.** Dispõe sobre a obrigatoriedade de empresas fabricantes de aparelhos celulares introduzirem aplicativo permanente nos aparelhos celulares que saem de fábrica e nos antigos para acionar a polícia em caso de violência contra a mulher. Brasília, 2019g. Disponível em: https://www.camara.leg.br/propostas-legislativas/2218309. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 6163/2019.** Institui o Plano Regional de Desenvolvimento do Nordeste para o período de 2020-2023. Brasília,

2019h. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2230650. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 1786/2020.** Altera a Lei nº 13.982, de 02 de abril de 2010, para possibilitar a substituição do Cadastro de Pessoa Física - CPF por outro documento oficial ou por outras formas de identificação dos beneficiários do auxílio emergencial, e da outras providências. Brasília, 2020c. Disponível em: https://www.camara.leg.br/propostas-legislativas/2247368. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 329/2020.** Dispõe sobre a obrigatoriedade de identificação facial ou biométrica e pagamento por meios eletrônicos em veículos particulares que exerçam transporte de passageiros via aplicativos. Brasilia, 2020a. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2237590. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 4768/2020.** Altera a Lei nº 12.587, de 2012, para estabelecer diretrizes para a prestação do serviço de transporte remunerado privado individual de passageiros, e a Lei nº 8.989, de 1995, para instituir isenção do Imposto sobre Produtos Industrializados – IPI –, na aquisição de automóveis por motoristas que prestem esse serviço. Brasília, 2020b. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2263604. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei Complementar nº 245/2020.** Altera a redação do art. 3º da Lei Complementar nº 79, de 7 de janeiro de 1994, que cria o Fundo Penitenciário Nacional – FUNPEN, e do art. 64 da Lei nº 7.210, de 11 de julho de 1984, que institui a Lei de Execução Penal – LEP. Brasília, 2020d. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2263658. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 1969/2021.** Dispõe sobre os princípios, direitos e obrigações na utilização de sistemas de inteligência artificial. Brasília, 2021a. Disponível em: https://www.camara.leg.br/propostas-legislativas/2284814. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 3307/2021.** Altera a Lei no 10.703, de 18 de julho de 2003, que dispõe sobre o cadastramento de usuários de telefones celulares pré-pagos, para tornar obrigatório o uso de sistema de verificação das informações dos usuários. Brasília, 2021d. Disponível em: https://www.camara.leg.br/propostas-legislativas/2300297. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 3714/2021.** Dispõe sobre o reconhecimento facial em todas as fases da persecução penal. Brasília, 2021c. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2303912. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 572/2021.** Altera a Lei nº 13.812, de 16 de março de 2019 e cria o Banco Nacional de Dados de Reconhecimento Facial e Digital. Brasília, 2021f. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2270809. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 1756/2022.** Dispõe sobre a obrigatoriedade de instalação de câmeras para reconhecimento facial em hospitais públicos. Brasília, 2022a. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2330234. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 2392/2022.** Dispõe sobre o uso de tecnologias de reconhecimento facial nos setores público e privado. Brasília, 2022b. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2334803. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 807/2022.** Estabelece medidas de prevenção e combate ao trabalho infantil em empresas de aplicativos de entregas ou transporte e dá outras providências. Brasília, 2022d. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2319143. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 3069/2022.** Dispõe sobre o uso de tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública e dá outras providências. Brasília, 2022c. Disponível em: https://www.camara.leg.br/propostas-legislativas/2345261. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei Complementar nº PL 243/2023.** Dispõe sobre o emprego de tecnologia de reconhecimento facial de crianças e adolescentes desaparecidos. Brasília, 2023g. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2409076. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 1828/2023.** Autoriza a instalação, em todo o território nacional, de câmeras de reconhecimento facial nas estações ferroviárias e rodoviárias, no interior dos vagões das composições, em vias públicas e repartições públicas; e dá outras providências. Brasília, 2023a. Disponível em: https://www.camara.leg.br/propostas-legislativas/2355883. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 1921/2023.** Altera a Lei no 9.394, de 20 de dezembro de 1996, que estabelece as diretrizes e bases da educação nacional, para dispor sobre a instalação de detectores de metais, câmeras nos arredores das escolas; software de reconhecimento facial, instalação de internet 5G e iluminação em volta das ruas circunvizinhas. Brasília, 2023c. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2356527. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 2028/2023.** Dispõe sobre o endurecimento da fiscalização e o cumprimento da faixa etária para jogos eletrônicos. Brasília, 2023f. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2357500. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 3047/2023.** Altera a Lei nº 9.394, de 20 de dezembro de 1996, que estabelece as diretrizes e bases da educação nacional (LDB), para dispor sobre a instalação de software de reconhecimento facial nas instituições de nível superior. Brasília, 2023d. Disponível em: https://www.camara.leg.br/propostas-legislativas/2368864. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 4179/2023.** Dispõe sobre a confirmação facial no comércio de bens e serviços pela internet. Brasília, 2023h. Disponível em: https://www.camara.leg.br/propostas-legislativas/2383389. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 3839/2023.** Autoriza o uso de fotografia de identificação com elemento de indumentária tradicional que exprime a identidade da pessoa, bem como altera altera as leis nº 7.116, de 29 de agosto de 1983, nº 9.503, de 23 de setembro de 1997 (Código de Trânsito Brasileiro) e o Decreto-Lei nº 5.452, de 1º de maio de 1943 (Consolidação das Leis do Trabalho). Brasília, 2023a. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2377163. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 4073/2023.** Altera o art. 69 da Lei nº 8.212, de 24 de julho de 1991, que dispõe sobre os Planos de Benefícios da Previdência Social, para tratar da prova de vida do beneficiário do Instituto Nacional do Seguro Social – INSS. Brasília, 2023b. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2382074. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 2745/2023.** Institui obrigatoriedade a todos os estádios de futebol, ginásios, arenas e demais locais de competições de esportes profissionais, credenciados para realização de jogos/competições oficiais a implementação de tecnologia de câmeras e sistemas de videomonitoramento com reconhecimento facial ou não. Brasília, 2023i. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2364455. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 2714/2023.** Regulamenta o uso, instalação e implementação de tecnologia de reconhecimento facial em câmeras e sistemas de videomonitoramento, e dá outras providências. Brasília, 2023j. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2364072. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 2606/2023.** Institui a identificação biométrica e ou facial para ingresso nas escolas da rede pública ou privada da educação básica de ensino, a submissão dos ingressantes à verificação

por equipamentos detectores de metais e sobre a obrigatoriedade de aquisição de equipamentos de detecção de metais, porta giratória com detecção de metais e outros equipamentos. Brasília, 2023e. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao/?idProposicao=2362562. Acesso em: 11 jan. 2024.

BRASIL. Assembleia Legislativa. **Projeto de Lei nº 284/2023.** Dispõe sobre regras de segurança para os motoristas por aplicativos, e dá outras providências. Brasília, 2023l. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2347089. Acesso em: 11 jan. 2024.

BRASIL. **Decreto n° 7.724, de 16 de maio de 2012.** Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5°, no inciso II do § 3° do art. 37 e no § 2° do art. 216 da Constituição. Brasília, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm. Acesso em: 11 nov. 2022.

BRASIL. Assembleia Legislativa. **Projeto de Lei 21/2020.** Estabelece princípios, direitos e deveres para o uso de inteligência artificial no Brasil, e dá outras providências. Brasília, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1853928. Acesso em: 11 nov. 2022.

BRASIL. **Decreto nº 10046, de 9 de outubro de 2019.** Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados [...] Brasília, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 11 nov. 2022.

BRASIL. **Lei n° 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5°, no inciso II do § 3° do art. 37 e no § 2° do art.216 da Constituição Federal; altera a Lei n° 8.112, de 11 de dezembro de 1990; revoga a Lei n° 11.111, de 5 de maio de 2005, e dispositivos da Lei n° 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, 18 nov.2011 (Edição Extra). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 11 nov. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil [...] Brasília, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 nov. 2022.

BRASIL. **Lei nº 13709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 nov. 2022.

BRASIL. Ministério da Educação. **Inaugurada a primeira escola pública Brasileira com sistema de reconhecimento facial dos estudantes**. [S./.]. 2021. Disponível em: https://www.gov.br/fnde/pt-br/assuntos/noticias/inaugurada-a-primeira-escola-publica-Brasileira-com-sistema-de-reconhecimento-facial-dos-estudantes. Acesso em: 21 out. 2022.

BRASIL. Serpro. **Embarque + Seguro**: uma nova forma de viajar. Uma nova forma de viajar. [202-]. Disponível em: https://campanhas.serpro.gov.br/embarque-mais-seguro/#menu. Acesso em: 20 out. 2022.

BRASIL. Câmara Legislativa. CPI - Violência Contra Jovens Negros E Pobres. Brasília, 2015.Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-morte-e-desaparecimento-de-jovens/conheca-a-comissao/historico-de-reunioes. Acesso em: 11 nov. 2022.

BRUNO, Fernanda *et. al*. (orgs.). **Tecnopolíticas da vigilância**: perspectivas da margem. São Paulo: Boitempo, 2018.

BRUNO, Fernanda. Mapas de crime: vigilância distribuída e participação na cibercultura. **Revista da Associação Nacional dos Programas de Pós-Graduação em Comunicação** | *E-compós.* Brasília, v.12, n.2, maio/ago. 2009, p. 01-16. Disponível em: https://www.e-compos.org.br/e-compos/article/view/409. Acesso em: 2 de jun. de 2022

BRUNO, Fernanda. Rastrear, classificar, performar. **Ciência e Cultura,** São Paulo, v. 68, p. 34-39, 2016.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: intersectional accuracy disparities in commercial gender classification. In: CONFERENCE ON FAIRNESS, ACCOUNTABILITY AND TRANSPARENCY., 1., 2018, New York. **Proceedings of Machine Learning Research.** [S. L.]: Mlr Press, 2018. p. 1-15.

BUOLAMWINI, Joy. **Unmasking AI:** my mission to protect what is human in a world of machines. S.L: Random House, 2023.

CÂMERAS com reconhecimento facial são instaladas em Copacabana durante o Carnaval. **G1.** Rio de Janeiro. 01 mar. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/03/01/cameras-com-reconhecimento-facial-sao-instaladas-em-copacabana-durante-o-carnaval.ghtml. Acesso em: 20 out. 2022.

CEARÁ. Assembleia Legislativa. **Projeto de Lei nº 202/2020.** Dispõe instituição dados de facial e digital de crianças e adolescentes desaparecidos, na forma que indica. Fortaleza, 2020.

CEARÁ. Assembleia Legislativa. **Projeto de Lei nº 251/2022.** Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo poder público no Estado do Ceará. Fortaleza, 2022.

CEARÁ. Assembleia Legislativa. **Projeto de Lei nº 146/2023.** Dispõe sobre a autorização, no âmbito do Estado do Ceará, para implantação da tecnologia de reconhecimento facial (TRF) nos dispositivos de vigilância por vídeo, na forma que indica. Fortaleza, 2023.

CAPURRO, Rafael. Cidadania na era digital. Tradução Marco Schneider e Arthur Bezerra). In: CABRAL, Adilson; CABRAL, Eula (org.). **Comunicação, Cultura, Informação e Democracia**: tensões e contradições. 1ed. Lisboa: MEDIA XXI - Publishing, Research & Consulting, v. 1, 2016. Livro do V Encontro da Ulepicc-Brasil.

CAPURRO, Rafael. Desafíos teóricos y prácticos de la ética intercultural de la información. In: SIMPÓSIO BRASILEIRO DE ÉTICA DA INFORMAÇÃO, Não use números Romanos ou letras, use somente números Arábicos., 2010, João Pessoa. **Simpósio.** João Pessoa: Ideia, 2010. p. 11-51. Disponível em: https://lti.pro.br/uploads/posts_files/148/5174bcdc63b1722a7b0a923f3f8fe63f.pdf. Acesso em: 15 ago. 2024.

CAPURRO, Rafael. Ética para provedores e usuários da informação. In: KALB, Anton; ESTERBAUER, Reinhold; RUCKENBAUER, Hans-Walber. **Cibernética – Responsabilidade em mundo interligado pela rede digital**. São Paulo: Loyola, 2001.

CAPURRO, Rafael. Information Ethics. in: KALDIS, Byron. **Encyclopedia of Philosophy and the Social Sciences.** Londres: Sage Publ, 2013, Vol. 1, p. 471-473.

CAPURRO, Rafael. **Desafios Teóricos Y Prácticos de la Ética Intercultural de la Información**. 2017. Disponível em: http://www.capurro.de/paraiba.html. Acesso em: 24 jan. 2024.

CARDIA, N. O medo da polícia e as graves violações dos direitos humanos. **Tempo Social**, [*S. l.*], v. 9, n. 1, p. 249-266, 1997.

CARDOSO, Bruno. Câmeras Legislativas: videovigilância e leis no Rio de Janeiro. **Revista Brasileira de Ciências Sociais**, Rio de Janeiro, v. 28, n. 81, p. 49-62, fev. 2013. Disponível em: https://www.scielo.br/j/rbcsoc/a/GxLv9QpQckNRx5vFHYTMvLr/?format=pdf&lang=pt. Acesso em: 24 jan. 2024.

CARDOSO, Bruno. Estado, tecnologias de segurança e normatividade neoliberal. In: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas. **Tecnopolíticas da Vigilância:** perspectivas da margem. São Paulo: Boitempo, 2018. p. 91-106.

CARDOSO, Bruno. **Todos os Olhos**: videovigilâncias, voyeurismos e (re)produção imagética. Rio de Janeiro: Editora UFRJ, 2014.

CARDOSO, Sara. Governo do Tocantins investe R$ 15,8 milhões em sistema de monitoramento para identificar e prender suspeitos. **Governo do Tocantins.** Palmas. 30 ago. 2023. Disponível em: https://www.to.gov.br/secom/noticias/governo-

do-tocantins-investe-r-158-milhoes-em-sistema-de-monitoramento-para-identificar-e-prender-suspeitos/5boea9vl52qe. Acesso em: 24 jan. 2024.

CARTA Soberania Digital. 2022. Disponível em: https://cartasoberaniadigital.lablivre.wiki.br/carta/. Acesso em: 22 jan. 2024.

ČAS, Johann *et al*. Introduction: surveillance, privacy and security. In: FRIEDWALD, Michael *et al*. **Surveillance, Privacy and Security**: citizen's perspectives. New York: Routledge, 2017. p. 1-12.

CASTELLS, Manuel. **A sociedade em rede.** São Paulo: Paz e Terra, 1999.

CELLARD, André. A análise documental. In: POUPART, Jean *et al*. **A pesquisa qualitativa:** enfoques epistemológicos e metodológicos. Petrópolis: Vozes, 2012, p. 295-316.

CENTRO DE ESTUDO DE SEGURANÇA E CIDADANIA. **O Panóptico**: monitor do reconhecimento facial no Brasil. Disponível em: https://opanoptico.com.br/. Acesso em: 07 set. 2022.

CIACCI (SURSIENDO), Jes.'We are struggling to survive': Resistance against mining in Acacoyagua, Chiapas. In: THE TIERRA COMÚN NETWORK. **Resisting Data Colonialism:** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023, p. 51-56. Disponível em: https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

CITY Câmeras: São Paulo. São Paulo. 201-. Disponível em: https://www.citycameras.prefeitura.sp.gov.br/howworks. Acesso em: 21 mai. 2021.

BRASIL. Senado Federal. Comissão de Juristas. **Relatório Final.** Brasília: Senado Federal, 2022. Disponível em: https://static.poder360.com.br/2023/02/comissao-senado-IA-relatorio-final-dez-2022.pdf. Acesso em: 24 jan. 2024.

COSGROVE, Elly. One billion surveillance cameras will be watching around the world in 2021, a new study says. **Cnbc.** [S.L]. 06 dez. 2019. Disponível em: https://www.cnbc.com/2019/12/06/one-billion-surveillance-cameras-will-be-watching-globally-in-2021.html. Acesso em: 01 nov. 2022.

COSTANZA-CHOCK, Sasha. **Design Justice:** community-led practices to build the worlds we need. SI: The Mit Press, 2020.

COULDRY, N.; MEJIAS, U. A. Data colonialism: Rethinking big data's relation to the contemporary subject. **Television and New Media. [***S. l.***],** v. 20, n. 4, p. 336–349, 2019.

COULDRY, Nick. There is something wrong with data extraction. The Tierra Común Network. **Resisting Data Colonialism:** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023, p. 8-11. Disponível em: https://networkcultures.org/wp-

content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

CRARY, Jonathan. **24/7:** Capitalismo tardio e os fins do sono. São Paulo: Ubu Editora, 2016.

CRARY, Jonathan. **Terra arrasada:** além da era digital, rumo a um mundo pós-capitalista. São Paulo: Ubu, 2023.

DAVE, Paresh; DASTIN, Jeffrey. Exclusive: Ukraine has started using Clearview AI's facial recognition during war. **Reuters.** [S. l.]. 14 mar. 2022. Disponível em: https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/. Acesso em: 12 set. 2022.

DEIBERT, Ronald J.; PAULY, Louis W. Mutual Entanglement and Complex Sovereignty in Cyberspace. In: BIGO, Didier; ISIN, Engin; RUPPERT, Evelyn. **Data Politics**: worlds, subjects, rights. Nova York: Routledge, 2019, p. 81-99.

DELEUZE, Gilles. Post-sciptum sobre as sociedades de controle. In: DELEUZE, Gilles. **Conversações:** *1972-1990.* Rio de Janeiro: Editora 34, 1992.

DEPOIS do investimento de US$ 100 milhões, para onde vai a Unico? **Exame**. [S. l.]. 02 maio 2022. Disponível em: https://exame.com/insight/depois-do-investimento-de-us-100-milhoes-para-onde-vai-a-unico/p. Acesso em: 22 jan. 2024.

DISTRITO FEDERAL. Assembleia Legislativa. **Projeto de Lei nº 1649/2020.** Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes e dá outras providências. Brasília, 2020. Disponível em: https://legislacao.cl.df.gov.br/Legislacao/consultaProposicao-1!1649!2020!visualizar.action. Acesso em: 5 jun. 2024.

DISTRITO FEDERAL. Assembleia Legislativa. **Projeto de Lei nº 2336/2021.** Dispõe sobre a instalação de câmera de vídeo nos uniformes dos policiais civis e militares e nas viaturas de polícia do Distrito Federal e dá outras providências. Brasília, 2021.

DISTRITO FEDERAL. Assembleia Legislativa. **Projeto de Lei nº 629/2023.** Estabelece diretrizes para política de instalação de câmeras corporais nos uniformes dos policiais penais no sistema prisional do Distrito Federal. Brasília, 2023a.

DISTRITO FEDERAL. Assembleia Legislativa. **Projeto de Lei nº 595/2023.** Estabelece diretrizes para política de videomonitoramento no sistema prisional do Distrito Federal. Brasília, 2023b.

DISTRITO FEDERAL. Assembleia Legislativa. **Projeto de Lei nº 459/2023.** Altera a Lei nº 6.390, de 25 de setembro de 2019, que cria o Programa Cidade Segura – PCS e dá outras providências, para dispor sobre videomonitoramento de segurança em praças públicas. Brasília, 2023c.

DISTRITO FEDERAL. **Lei nº 6712/2020, de 10 de novembro de 2020.** Dispõe sobre o uso de tecnologia de reconhecimento facial trf na segurança pública e dá

outras providências. Brasília, 2020. Disponível em: https://legislacao.cl.df.gov.br/Legislacao/buscarLeiPeloLegis-31818!buscarNormaJuridicaPeloLegis.action. Acesso em: 5 jun. 2024.

DOWBOR, Ladislau. **Resgatar a Função Social da Economia**. São Paulo: Editora Elefante, 2022.

DRATWA, Jim. Foreword: Ethical Experimentations of Security and Surveillance as an Inquiry into the Open Beta Society. In: FRIEDWALD, Michael *et al*. **Surveillance, Privacy and Security**: citizen's perspectives. Nova York: Routledge, 2017. Prefácio.

EMBARQUE 100% digital é testado no Aeroporto Internacional de BH. **Belo Horizonte.** Belo Horizonte, maio 2021. Disponível em: https://www.belohorizonte.com.br/embarque-100-digital-e-testado-no-aeroporto-internacional-de-bh/. Acesso em: 20 out. 2022.

EMERGEN RESEARCH. **Top 10 leading Facial Recognition Companies in the World**. 2022. Disponível em: https://www.emergenresearch.com/blog/top-10-leading-facial-recognition-companies-in-the-world. Acesso em: 12 set. 2022.

EMPRESAS lançam serviço de reconhecimento facial para igrejas no Brasil. **Carta Capital,** São Paulo, 14 nov. 2019. Disponível em: https://www.cartacapital.com.br/sociedade/empresas-lancam-servico-de-reconhecimento-facial-para-igrejas-no-Brasil/. Acesso em: 02 nov. 2022.

ESPÍRITO SANTO. Assembleia Legislativa. **Projeto de Lei nº 207/2020.** Ficam as operadoras de celular obrigadas a possuir um banco de dados dos clientes com terminal de reconhecimento facial e biometria digital, no âmbito do estado do espírito santo. Vitória, 2020.

EXCLUSIVO: 83% dos presos injustamente por reconhecimento fotográfico no Brasil são negros: um levantamento inédito feito pelo CONDEGE, entidade que reúne defensores públicos de todo país, e também pela defensoria pública do Rio de Janeiro mostra que os negros são, de longe, as maiores vítimas desse tipo de erro.. **G1**. Rio de Janeiro. 21 fev. 2021. Disponível em: https://g1.globo.com/fantastico/noticia/2021/02/21/exclusivo-83percent-dos-presos-injustamente-por-reconhecimento-fotografico-no-Brasil-sao-negros.ghtml. Acesso em: 07 mai. 2021.

FAUSTINO, Deivison; LIPPOLDI, Walter. **Colonialismo de Digital**. São Paulo: Boitempo 2023.

FIRMINO, Rodrigo. Securitização, Vigilância E Territorialização Em Espaços Públicos Na Cidade Neoliberal. In: BRUNO, Fernanda. **Tecnopolítica da vigilância: perspectivas da margem**. São Paulo: Boitempo, 2018, p. 69-89.

FOUCAULT, Michel. **Segurança, Território, População:** curso dado no Collège de France (1977-1978). São Paulo: Martins Fontes, 2008.

FOUCAULT, Michel. ***V*igiar e Punir:** História da Violência nas Prisões. Petrópolis: Editora Vozes, 1977.

FRANCISCO, Pedro Augusto P.; HUREL, Louise Marie; RIELLI, Mariana Marques. **Regulação do Reconhecimento Facial no Setor Público:** avaliação de experiências internacionais. Rio de Janeiro: Instituto Igarapé; Data Privacy Brasil Research, 2020. Disponível em: https://igarape.org.br/wp-content/uploads/2020/06/2020-06-09-Regula%C3%A7%C3%A3o-do-reconhecimento-facial-no-setor-p%C3%BAblico.pdfhttps://igarape.org.br/videomonitoramento-webreport/. Acesso em: 21 maio 2021.

FRASER, N.; JAEGGI, R. **O capitalismo em debate:** uma conversa na teoria crítica. São Paulo: Boitempo, 2020.

FRASER, Nancy; HONNETH, Axel. **Redistribution or Recognition? A Political-philosophical Exchange**. Londres: Verso, 2003.

FRASER, Nancy. Social Justice in the Age of Identity Politics: redistribution, recognition, and participation. In: FRASER, Nancy; HONNETH, Axel. **Redistribution or Recognition?** A Political-philosophical Exchange. Londres: Verso, 2003. p. 07-109.

FREIRE, Paulo. **Pedagogia da Esperança:** um reencontro com a Pedagogia do Oprimido. Rio de Janeiro: Paz e Terra, 1992.

FREIRE, Paulo. **Pedagogia do Oprimido**. Rio de Janeiro: Paz e Terra, 1987.

FROHMANN, Bernd. Taking information policy beyond Information Science: applying the actor network theory for connectedness: information, systems, people, organizations, 1995. Disponível em: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=40176306291e2cf81caecb4b6c9412853ae54031> Acesso em: 15 ago 2024.

GANDRA, Alana. Governo inicia teste de embarque aéreo 100% digital: o projeto embarque + seguro foi desenvolvido pelo serpro. **Agência Brasil.** Rio de Janeiro. 11 mar. 2021. Disponível em: https://agenciaBrasil.ebc.com.br/geral/noticia/2021-03/governo-inicia-teste-de-embarque-aereo-100-digital. Acesso em: 20 out. 2022.

GARCIA CANCLINI, Nestor. **Ciudadanos reemplazados por algoritmos.** Alemanha: Bielefeld University Press, 2019.

GOIÁS. Assembleia Legislativa. **Projeto de Lei nº 298/2023.** Altera a lei n° 16.499, de 10 de fevereiro de 2009 para prever a disponibilização de reconhecimento facial de pessoas desaparecidas no cadastro de pessoas desaparecidas do estado de Goiás. Goiânia, 2023.

GOIÁS. Assembleia Legislativa. **Projeto de Lei nº 2021005741/2021.** Cria o banco estadual de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes, e dá outras providências. Goiânia,

2021. Disponível em: https://opine.al.go.leg.br/proposicoes/2021005741. Acesso em: 5 jun. 2024.

GOIÁS. Assembleia Legislativa. **Projeto de Lei nº 2019001893/2019.** Dispõe sobre a obrigatoriedade de instalação de câmeras inteligentes pelas empresas concessionárias de transporte coletivo urbano do estado de Goiás, que permitem detectar o reconhecimento facial de suspeitos de crime e procurados da justiça. Goiânia, 2019. Disponível em: https://opine.al.go.leg.br/proposicoes/2019001893. Acesso em: 5 jun. 2024.

GÓIS, Aléxis Cerqueira. Reconhecimento facial deve movimentar R$ 50 bilhões em 2022. **Techmundo.** [S. *l.*]. 06 nov. 2021. Disponível em: https://www.tecmundo.com.br/mercado/228271-reconhecimento-facial-deve-movimentar-r-50-bilhoes-2022.htm. Acesso em: 12 set. 2022.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Para uma reflexão epistemológica acerca da ciência da informação. **Perspectivas em Ciência da Informação**, Rio de Janeiro, v. 6, n. 1, p. 5–18, 2001.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Novos cenários políticos para a informação. **Ciência da Informação**, Brasília, v.31, n.1, p.27- 40, 2002. Disponível em: https://revista.ibict.br/ciinf/article/view/975. Acesso em: 06 set 2022.

GONZÁLEZ DE GÓMEZ, Maria Nélida. O caráter seletivo das ações de informação. **Informare**, Rio de Janeiro, v.5, n.2, p.7-31, 1999.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Reflexões sobre a genealogia dos regimes de informação. **Informação e Sociedade**: Estudos, João Pessoa, v.29, n.1, p.137-158, jan./mar., 2019.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Regime de informação: construção de um conceito. **Informação & sociedade:** estudos, João Pessoa, v. 22, n. 3, p.43-60, set/dez, 2012. Disponível em: https://www.brapci.inf.br/_repositorio/2015/12/pdf_3c42553162_0000011948.pdf. Acesso em: 20 jul. 2022.

GORTÁZAR, Naiara Galarraga. Câmeras no uniforme para travar o gatilho fácil da polícia Brasileira. **El País.** São Paulo. 07 dez. 2021. Disponível em: https://Brasil.elpais.com/Brasil/2021-12-07/cameras-no-uniforme-para-travar-o-gatilho-facil-da-policia-Brasileira.html. Acesso em: 06 set. 2022.

GRAHAM, S. **Cidades sitiadas**. São Paulo: Boitempo Editorial, 2016.

HAN, Byung-Chu. **Infocracia**: digitalização e a crise da democracia. Petrópolis: Vozes, 2022.

HARVEY, David. **Condição pós-moderna**: uma pesquisa sobre as origens da mudança cultural. São Paulo: Ed. Loyola, 1998.

HILL, David W. The injuries of platform logistics. **Media, Culture & Society**, [S.L.], v. 42, n. 4, p. 521-536, 21 jul. 2019. Disponível em: http://dx.doi.org/10.1177/0163443719861840. Acesso em: 12 nov. 2022.

HILL, Kashmir. **Your Face Belongs to Us:** the secretive startup dismantling your privacy. S.L: Simon & Schuster UK, 2023.

IBM CLOUD EDUCATION. **Machine Learning**. Disponível em: https://www.ibm.com/br-pt/cloud/learn/machine-learning. Acesso em: 02 nov. 2022.

IDEMIA. **Our technologies**: idemia puts its unique suite of identity technologies at the service of a simpler and safer world. Disponível em: https://www.idemia.com/our-technologies. Acesso em: 12 nov. 2022.

INOCENTE preso por erro de reconhecimento facial vive traumas. **R7.** Brasília. 15 dez. 2021. Disponível em: https://noticias.r7.com/brasilia/videos/inocente-preso-por-erro-de-reconhecimento-facial-vive-traumas-15122021. Acesso em: 22 jan. 2024.

INSTITUTO IGARAPÉ. **Reconhecimento Facial no Brasil**. [S. l.]. 2022. Disponível em: https://igarape.org.br/infografico-reconhecimento-facial-no-Brasil/. Acesso em: 07 set. 2022.

JEE, Charlotte. London police's face recognition system gets it wrong 81% of the time. **MIT Technology Review**. Massachusetts. 4 julho 2019. Disponível em: https://www.technologyreview.com/2019/07/04/134296/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time/. Acesso em: 13 junho 2022.

KALEMA, Nai Lee. Intersections of Data Power: Unmasking the Nexus of Data Colonialism and Digital Racial Capitalism. In: THE TIERRA COMÚN NETWORK. **Resisting Data Colonialism:** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023, p. 21-28. Disponível em: https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

KALPOKAS, Ignas. **Algorithmic Governance:** politics and law in the post-human era. Palgrave Pivot, 2019.

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

KRAUS, Lalita; NEVES, Fabiola de Cássia Freitas; COSTA, Aldenilson dos Santos Vitorino. Unequal smart spaces: the command and control centre of rio de janeiro. **Espaço e Economia:** Revista Brasileira de Geografia Econômica, S. *l.*]. v. 23, p. 01-18, 2022,. Disponível em: https://journals.openedition.org/espacoeconomia/21619. Acesso em: 26 jan. 2024.

KRENAK, Ailton. **Ideias para Adiar o Fim do Mundo.** São Paulo: Companhia das Letras, 2019.

KUZZMA. **Inteligência Artificial para Igrejas**. 201-. Disponível em: https://site.kuzzma.com/pt/. Acesso em: 02 nov. 2022.

L8. **Segurança Pública é um seguimento do Grupo L8.** 2024. Disponível em: https://www.l8group.net/seguranca-publica/. Acesso em: 24 jan. 2024.

LEVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

LYON, D. Situating surveillance: history, technology, culture. In: KEES, B.; VAN BRAKEL, R.; FONIO, C.; WAGENAAR, P. (Org.) **Histories of State Surveillance in Europe and Beyond**. New York; London: Routledge, 2014. p. 32-46.

LYON, D. **Surveillance studies: an overview**. Cambridge: Polity Press, 2007.

LYON, David. Surveillance capitalism, surveillance culture and data politics. In: BIGO, Didier; ISIN, Engin; RUPPERT, Evelyn. **Data Politics**: worlds, subjects, rights. New York: Routledge, 2019. p. 64-76.

LYON, David. Surveillance studies: understanding visibility, mobility and the phenetic fix. **Surveillance & Society**, [S.L], v. 1, n. 1, p. 1-7, set. 2002. Disponível em: https://www.researchgate.net/publication/229031385_Surveillance_studies_Understanding_visibility_mobility_and_the_phenetic_fix. Acesso em: 11 nov. 2022.

MAGALHÃES, Lucas. Governo Federal e CBF anunciam o lançamento do Projeto Estádio Seguro. **Globo Esporte.** Brasília. 20 set. 2023. Disponível em: https://ge.globo.com/df/noticia/2023/09/20/governo-federal-e-cbf-anunciam-o-lancamento-do-projeto-estadio-seguro.ghtml. Acesso em: 22 jan. 2024.

MARANHÃO. Assembleia Legislativa. **Projeto de Lei nº 75/2021.** Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes e dá outras providências.São Luís, 2021. Disponível em: http://sapl.al.ma.leg.br:8080/sapl/consultas/materia/materia_mostrar_proc?cod_materia=20487. Acesso em 6 jun. 2024.

MARCONI, Marina; LAKATOS, Eva. Metodologia da pesquisa científica. São Paulo: Editora Atlas, 2003.

MARTINS, Carlos Eduardo. **Globalização, dependência e neoliberalismo na América Latina**. São Paulo: Boitempo, 2011.

MARTINS, Laís. **Exclusivo:** em reuniões secretas, Clearview ofereceu 3 bilhões de imagens de brasileiros para polícias e Ministério da Justiça. **Intercept Brasil.** [S.l.]. 16 maio 2023. Disponível em: https://www.intercept.com.br/2023/05/16/em-reunioes-secretas-clearview-policias-ministerio-da-justica/. Acesso em: 22 jan. 2024.

MARX, Karl. **Teses sobre Feuerbach.** Lisboa: Editorial Avante, 1982. Disponível em: https://lisboa.pcp.pt/wp-content/uploads/2007/04/teses-fuerb.pdf. Acesso em: 22 jan. 2024.

MATO GROSSO. Assembleia Legislativa. **Projeto de Lei nº 387/2015.** Dispõe sobre a instalação de câmeras de vigilância nas áreas externas dos estabelecimentos bancários de crédito, financiamento e investimentos e de estabelecimentos congêneres. Cuiabá, 2015.

MATO GROSSO. Assembleia Legislativa. **Projeto de Lei nº 84/2019.** Obriga a utilização de sistema de identificação biométrica nas entradas e de sistema de monitoramento por imagem em toda a área de uso comum de estádios com capacidade superior a 10.000 (Dez mil) pessoas, nos dias de jogos de futebol, no âmbito do estado de mato grosso, e dá outras providências. Cuiabá, 2019.

MATO GROSSO. Assembleia Legislativa. **Projeto de Lei nº 53/2020.** Institui o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos, no âmbito do estado de Mato Grosso. Cuiabá, 2020.

MATO GROSSO. Assembleia Legislativa. **Projeto de Lei nº 140/2021**. Cria o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos, no âmbito do estado de Mato Grosso. Cuiabá, 2021.

MATO GROSSO. Assembleia Legislativa. **Projeto de Lei nº 12/2023.** Institui o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos, no âmbito do estado de Mato Grosso. Cuiabá, 2023a.

MATO GROSSO. Assembleia Legislativa. **Projeto de Lei nº 734/2023.** Cria o Sistema Integrado de Vigilância Comunitária de Segurança Pública e dispõe sobre a obrigatoriedade de padrões mínimos de implantação de um sistema de videovigilância comunitária nos municípios. Cuiabá, 2023b.

MATO GROSSO DO SUL. Assembleia Legislativa. **Projeto de Lei nº 152/21.** Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes, e dá outras providências. Campo Grande, 2021.

MATO GROSSO DO SUL. Assembleia Legislativa. **Projeto de Lei nº 00244/2023.** Institui o Banco de Dados de Reconhecimento Facial e Digital de Crianças e Adolescentes Desaparecidos, no âmbito do Estado de Mato Grosso do Sul, e dá outras providências. Campo Grande, 2023.

MAYORAL BANOS, Alejandro. Data colonialism is not a metaphor: Remembering colonialism and why it matters in the digital ecosystem. In: THE TIERRA COMÚN NETWORK. **Resisting Data Colonialism:** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023, p. 12-20. Disponível em: https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

MELO, R. Teoria crítica e os sentidos da emancipação. **Caderno CRH**, Salvador, v. 24, n. 62, p. 249–262, 2011.

METRÔ de SP: reconhecimento facial enfrenta resistência. **O Estadão.** São Paulo. 27 abr. 2021. Disponível em: https://summitmobilidade.estadao.com.br/compartilhando-o-caminho/metro-de-sp-reconhecimento-facial-enfrenta-resistencia/. Acesso em: 20 out. 2022.

MEU RECIFE (Recife). SEM Câmera na Minha Cara. 2023. Disponível em: https://www.semcameranaminhacara.meurecife.org.br/. Acesso em: 22 jan. 2024.

MINAS GERAIS. Assembleia Legislativa. **Projeto de Lei nº 3812/2022.** Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo poder público do Estado. Belo Horizonte, 2022.

MINAS GERAIS. Assembleia Legislativa. **Projeto de Lei nº 391/2019.** Dispõe sobre a obrigatoriedade de implantação de tecnologia de reconhecimento facial em locais públicos, no âmbito do Estado. Belo Horizonte, 2019. Disponível em: https://www.almg.gov.br/projetos-de-lei/PL/391/2019. Acesso em 6 jun. 2024.

MORDOR INTELLIGENCE. **Global Facial Recognition Market (2021 - 2026)**. [S.l.]: Mordor Intelligence, 2020. Disponível em: https://samples.mordorintelligence.com/64785/Sample%20-%20Global%20Facial%20Recognition%20Market%20(2021%20-%202026)%20-%20Mordor%20Intelligence1617732105320.pdf. Acesso em: 12 set. 2022.

MOROZOV, Eygene. **Digital Technologies And The Future Of Data Capitalism**. Social Europe. 23 junho 2015. Disponível em: https://socialeurope.eu/digital-technologies-and-the-future-of-data-capitalism. Acesso em 20 julho 2022

MOROZOV, Evgene; BRIA, Francesca. **A cidade inteligente**: tecnologias urbanas e democracia. São Paulo: Ubu Editora, 2019.

MOROZOV, Evgene. **Big Tech**: a ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018.

MOROZOV, Evgene. **Big Tech**: a ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2020.

NASCIMENTO, Rafael. Corregedoria da PM identifica 39 policiais que burlaram câmeras corporais da corporação. **G1**. Rio de Janeiro. 01 set. 2023. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2023/09/01/corregedoria-da-pm-identifica-39-policiais-que-burlaram-cameras-corporais-da-corporacao.ghtml. Acesso em: 22 jan. 2024.

NASCIMENTO, Stephany. **Violência Policial**: letalidade e vitimização. Letalidade e vitimização. [S.l.]. 2022. Disponível em: https://www.politize.com.br/violencia-policial/. Acesso em: 11 nov. 2022.

NEMER, David. **Tecnologia do Oprimido**: desigualdades e o mundano digital nas favelas do Brasil. Vitória: Editora Milfontes, 2021.

NOBLE, Safyia Umoja. **Algoritmos da Opressão:** como o Google fomenta e lucra com o racismo. Santo André: Editora Rua do Sabão, 2021.

NUMERICO, Teresa. Science and colonialism: The violence of abstraction. In: THE TIERRA COMÚN NETWORK. **Resisting Data Colonialism:** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023, p. 29-37. Disponível em: https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

NUNES, Pablo; SILVA, Mariah Rafaela; OLIVEIRA, Samuel de. **Um Rio de câmeras com olhos seletivos: uso de reconhecimento facial pela polícia fluminense.** Rio de Janeiro: CESeC, 2022. Disponível em: https://opanoptico.com.br/wp-content/uploads/2022/05/PANOPT_riodecameras_mar22_0404b.pdf. Acesso em: 14 jun. 2022.

NUNES, Pablo. Exclusivo: Levantamento revela que 90,5% dos presos por Monitoramento Facial no Brasil são Negros: rede de observatórios de segurança monitorou a tecnologia de reconhecimento facial em cinco estados. resultado: além de ineficiente, sistema agrava o encarceramento de negros. **The Intercept: Brasil.** [S.l.]. 21 nov. 2019. Disponível em: https://theintercept.com/2019/11/21/presos-monitoramento-facial-Brasil-negros/. Acesso em: 07 maio 2021.

O RECONHECIMENTO fotográfico nos processos criminais no Rio de Janeiro. Rio de Janeiro: **Defensoria Pública do Estado do Rio de Janeiro**, 2022. Disponível em: https://static.poder360.com.br/2022/05/reconhecimento-fotografico-processos-criminais-mai-2022.pdf. Acesso em: 22 jan. 2024.

O'NEIL, Cathy. **Algoritmos de destruição em massa:** como o big data aumenta a desigualdade e ameaça a democracia. Santo André: Editora Rua do Sabão, 2020.

OI aposta em soluções de vigilância para Cidades Inteligentes. **Segurança Eletrônica,** [S.l.]. 201?-. Disponível em: https://revistasegurancaeletronica.com.br/oi-aposta-em-solucoes-de-vigilancia-para-cidades-inteligentes/. Acesso em: 21 mai. 2021.

OLIVEIRA, Samuel R. **Sorria! Você está sendo filmado!**: repensando direitos na era do reconhecimento facial. São Paulo: Thomson Reuters Brasil, 2021.

ORLANDI, Eni Puccinelli. **Análise de Discurso**: princípios & procedimentos. 8. ed.Campinas: Pontes, 2009.

ORTEGA, Pepita. Defensorias pedem à Justiça que obrigue Metrô a informar sobre licitação de R$ 58 mi para reconhecimento facial. **O Estadão.** São Paulo.11 fev. 2020. Disponível em: https://12ft.io/proxy?q=https%3A%2F%2Fpolitica.estadao.com.br%2Fblogs%2Ffausto-macedo%2Fdefensorias-pedem-a-justica-que-obrigue-metro-a-informar-sobre-licitacao-de-r-58-mi-para-reconhecimento-facial%2F. Acesso em: 13 nov. 2022.

ORWELL, George. **1984**. São Paulo: Companhia Editora Nacional, 1978.

PARAÍBA. Assembleia Legislativa. **Projeto de Lei nº 2453/2021.** Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes e dá outras providências. João Pessoa, 2021a.

PARAÍBA. **Lei nº 11858/2021, de 25 de março de 2021.** Obriga o aviso sobre o reconhecimento facial em estabelecimentos comerciais. João Pessoa, 2021b. Disponível em: https://leisestaduais.com.br/pb/lei-ordinaria-n-11858-2021-paraiba-obriga-o-aviso-sobre-o-reconhecimento-facial-em-estabelecimentos-comerciais. Acesso em 22 jul. 2024.

PARANÁ. Assembleia Legislativa. **Projeto de Lei nº 148/2019.** Dispõe sobre a permissão de implantação de tecnologia de reconhecimento facial em locais públicos. Curitiba, 2019.

PARANÁ. Assembleia Legislativa. **Projeto de Lei nº 75/2021.** Institui o banco de dados de reconhecimento facial e digital de pessoas desaparecidas. Lei do reencontro. Curitiba, 2021.

PASQUALE, F. **The Black Box Society: The Secr*et al*gorithms that Control Money and Information**. Harvard Un ed. Cambridge: Harvard, 2015.

PASQUINELLI, Matteo; JOLER, Vladan. **O Manifesto Nooscópio: inteligência artificial como instrumento de extrativismo do conhecimento**. 2020. Disponível em: https://lavits.org/o-manifesto-nooscopio-inteligencia-artificial-como-instrumento-de-extrativismo-do-conhecimento/?lang=pt. Acesso em: 22 jan. 2024.

PAYFACE. **Payface**. [202-]. Disponível em: https://payface.com.br/#. Acesso em: 12 set. 2022.

PEET, Charlotte. Brazil's embrace of facial recognition worries Black communities: activists are concerned that using biometric tools on people with no say over the decision risks reinforcing racist practices. **Rest Of The World.** Rio de Janeiro. 22 out. 2021. Disponível em: https://restofworld.org/2021/brazil-facial-recognition-surveillance-black-communities/. Acesso em: 20 out. 2022.

PEREIRA, Gabriel; COULDRY, Nick. Data Colonialism Now: Harms and Consequences. In: THE TIERRA COMÚN NETWORK. **Resisting Data Colonialism:** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023, p. 38-44. Disponível em: https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

PM prende dois foragidos no entorno do Maracanã usando sistema de reconhecimento facial. **G1.** Rio de Janeiro. 01 set. 2019. Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/09/01/mulher-e-presa-na-entrada-do-estadio-do-maracana-apos-ser-flagrada-por-sistema-de-reconhecimento-facial.ghtml. Acesso em: 24 jan. 2024.

PERNAMBUCO. Assembleia Legislativa. **Projeto de Lei nº 1466/2020.** Dispõe sobre a realização de prova de vida por meio eletrônico ou virtual no âmbito do Estado de Pernambuco, dos aposentados e pensionistas, cujos benefícios previdenciários são geridos pela Fundação de Aposentadorias e Pensões dos Servidores do Estado de Pernambuco – FUNAPE. Recife, 2020. Disponível em https://www.alepe.pe.gov.br/proposicao-texto-completo/?docid=6351&tipoprop=p. Acesso em 6 jun. 2024.

PERNAMBUCO. Assembleia Legislativa. **Projeto de Lei nº 402/2023.** Proíbe a utilização de tecnologia de reconhecimento facial automatizado no âmbito dos sistemas de segurança do Estado de Pernambuco e dá outras providências. Recife, 2023a.

PERNAMBUCO. Assembleia Legislativa. **Projeto de Lei nº 669/2023.** Institui o protocolo de acesso, para visitantes, nas unidades de ensino da Rede Pública Estadual de Pernambuco. Recife, 2023b.

PERNAMBUCO. Assembleia Legislativa. **Projeto de Lei nº 1220/2023.** Estabelece diretrizes para a criação do dispositivo “Escola Protegida” no âmbito do Estado de Pernambuco e dá outras providências. Recife, 2023c.

PONTOID. **A Ponto iD**. 2022. Disponível em: https://www.pontoid.com.br/empresa/. Acesso em: 20 out. 2022.

PRAKASH, Abishur. **Facial Recognition Cameras and AI**: 5 countries with the fastest adoption. 2018. Disponível em: https://abishurprakash.com/facial-recognition-cameras-and-ai-5-countries-with-the-fastest-adoption/. Acesso em: 11 nov. 2022.

PREITE SOBRINHO, Wanderley. Após um ano de uso de câmeras em uniformes, mortes por policiais caem 80%. **Uol.** São Paulo. 05 jul. 2022. Disponível em: Após um ano de uso de câmeras em uniformes, mortes por policiais caem 80%... - Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2022/07/05/cameras-no-uniforme-da-pm-letalidade-policial-intervencao-lesao-corporal.htm?cmpid=copiaecola. Acesso em: 06 set. 2022.

PREITE SOBRINHO, Wanderley. Letalidade policial cai com câmeras; especialistas pedem "mudança cultural". **Uol.** São Paulo. 29 jan. 2022. Disponível em: https://noticias.uol.com.br/cotidiano/ultimas-noticias/2022/01/29/cameras-no-unifome-da-pm-letalidade-policial-intervencao-lesao-corporal.htm. Acesso em: 06 set. 2022.

RAMÍREZ M., Pamela. No to the Data Center! Resistance and Artivism Against Google in Cerrillos. In: THE TIERRA COMÚN NETWORK. **Resisting Data Colonialism:** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023. p. 57-62. Disponível em: https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

RECONHECIMENTO facial é reforçado com 27 câmeras para evitar entrada de foragidos da Justiça no Pré-Caju 2023. **Portal do Governo do Estado De Sergipe**. Disponível em: https://www.se.gov.br/noticias/seguranca-publica/reconhecimento_facial_e_reforcado_com_27_cameras_para_evitar_entrada_de_foragidos_da_justica_no_pre_caju_2023. Acesso em: 22 jan. 2024.

RICAURTE QUIJANO, Paola. Resisting data colonialism: What lies ahead. In: THE TIERRA COMÚN NETWORK. **Resisting Data Colonialism:** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023. p. 95-96. Disponível em: https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

RICAURTE, Paola. Data Epistemologies, The Coloniality of Power, and Resistance. **Television & New Media**, [S.L.], v. 20, n. 4, p. 350-365, 7 mar. 2019.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 862/2003.** Dispõe sobre os mecanismos de segurança para acesso aos sistemas e bancos de dados da administração pública do Estado". Rio de Janeiro, 2017.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 3261/2017.** Dispõe sobre a utilização de sistema de identificação biométrica nas entradas e de sistema de monitoramento por imagem em toda a área de uso comum de estádios com capacidade superior a 10.000 (dez mil) pessoas, nos dias de jogos de futebol, no âmbito do estado do Rio de Janeiro, e dá outras providências. Rio de Janeiro, 2017.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 318/2019.** Dispõe sobre a obrigatoriedade da implantação de tecnologia de reconhecimento facial em toda a área de uso comum, incluindo eventos públicos e privados, com capacidade superior a 10.000 (Dez mil) pessoas, no âmbito do estado do rio de janeiro. Rio de Janeiro, 2019a.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 341/2019.** Dispõe sobre a obrigatoriedade de concessionários do serviço público de administração de terminais rodoviários, instalação de câmeras de segurança com tecnologia de reconhecimento facial de suspeitos e procurados da justiça nos locais que determina e dá outras providências. Rio de Janeiro, 2019b.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 1372/2019.** Dispõe sobre a instalação obrigatória de câmeras de reconhecimento facial em todas as estações do metrô-rio e da supervia, bem como no interior dos vagões das composições e dá outras providências. Rio de Janeiro, 2019c.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 607/2019.** Torna obrigatória a instalação de câmeras de monitoramento com reconhecimento facial em todas as praças de pedágios, no âmbito do estado do Rio de Janeiro. Rio de Janeiro, 2019d.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 853/2019.** Veda a negociação e comercialização de produtos e serviços no interior dos vagões e

embarcações dos transportes públicos do estado do rio de janeiro na forma, na forma que menciona. E fica o Poder Executivo autorizado a implantar equipamentos de reconhecimento facial ou tecnologia similar, com o intuito de aperfeiçoar a integração da segurança nas estações com os órgãos de segurança pública. Rio de Janeiro, 2019e.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 1097/2019.** Dispõe sobre a instalação de sistema de dispositivo de reconhecimento facial em edificações públicas e privadas no âmbito do estado do rio de janeiro e dá outras providências. Rio de Janeiro, 2019f.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 1033/2019.** Institui o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos. Rio de Janeiro, 2019g.
RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 1101/2019.** Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes no estado do rio de janeiro. Rio de Janeiro, 2019a.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 1505/2019.** Institui o banco estadual de dados de reconhecimento facial de crianças e adolescentes desaparecidos. Rio de Janeiro, 2019f.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 342/2019.** Dispõe sobre a obrigatoriedade de concessionários do serviço público de metrô, trens e barcas, instalação de câmeras de segurança com tecnologia de reconhecimento facial de suspeitos e procurados da justiça nos locais que determina e dá outras providências. Rio de Janeiro, 2019i.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 665/2019.** Cria o sistema de identificação biométrica no estado do Rio de Janeiro. O Sistema de Identificação Biométrica abrangerá todos os bancos de dados biométricos existentes no Serviço Público Estadual, podendo compreender também, através de parcerias, as concessionárias ou permissionárias de serviços públicos concedidos, ou delegatárias a elas vinculadas, bem como entidades privadas. Rio de Janeiro, 2019j.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 2548/2020.** Dispõe sobre a obrigatoriedade da carteira de identidade para todos os cidadãos com idade inferior a 18 (dezoito) anos a ser emitida pelos órgãos de identificação competentes, do estado do rio de janeiro. E no Art. 1º inciso 1º No ato deverá ser realizadas as imagens para reconhecimento facial e digital de todos os cidadãos com idade inferior a 18 (dezoito) anos. Rio de Janeiro, 2020a.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 1833/2020.** Institui o banco estadual de dados multibiométricos no sistema de segurança pública, conjugando impressões papilares, impressões palmares, imagens de face, assinatura, iris e fala, bem como dá outras providências. Rio de Janeiro, 2020b.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 2946/2020.** Dispõe sobre a flexibilização dos serviços para obtenção da carteira nacional de habilitação.

Art. 3º – Os exames de direção veicular, teóricos, serão realizados via on line, por entidades privadas credenciadas pelo Detran do Estado do Rio de Janeiro, por plataformas digitais, que utilizem captura da imagem e reconhecimento facial do candidato, colheita da biometria e controle do tempo de realização do exame teórico. Rio de Janeiro, 2020c.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 4493/2021.** Institui a carteira de identidade funcional em formato digital para policiais militares, policiais civis, policiais penais, e demais agentes de segurança pública do estado do Rio de Janeiro. (autorizado no formato online e digital) e determinando a coleta da foto digital a ser em qualidade para ser usada em reconhecimento facial. Rio de Janeiro, 2021a.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 5240/2021.** Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo poder público no Estado do Rio de Janeiro. Rio de Janeiro, 2021b.

RIO DE JANEIRO. **Lei nº 9167/2021, de 06 de janeiro de 2021.** Dispõe sobre o banco de dados de reconhecimento facial e digital de crianças e adolescentes desaparecidos. Rio de Janeiro, 2021c. Disponível em: https://gov-rj.jusbrasil.com.br/legislacao/1157629067/lei-9167-21-rio-de-janeiro-rj. Acesso em 7 jun. 2024.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 274/2023.** Dispõe sobre a instalação de dispositivo de reconhecimento facial de suspeitos e procurados da justiça em terminas rodoviários, portos e aeroportos no âmbito do estado do Rio de Janeiro e dá outras providências. Rio de Janeiro, 2023a.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 384/2023.** Dispõe sobre a instalação de dispositivo de reconhecimento facial de suspeitos e procurados da justiça em shoppings centers no âmbito do Estado do Rio de Janeiro e dá outras providências. Rio de Janeiro, 2023b.

RIO DE JANEIRO. Assembleia Legislativa. **Projeto de Lei nº 550/2023.** Autoriza o poder executivo a utilizar tecnologia de reconhecimento facial automatizado no âmbito das forças de segurança pública, no Estado do Rio de Janeiro, e dá outras providências. Rio de Janeiro, 2023c.

RIO GRANDE DO SUL. Assembleia Legislativa. **Projeto de Lei nº 73/2019.** Institui o Banco de Dados de Reconhecimento Facial e Digital de Crianças e Adolescentes Desaparecidos. Porto Alegre, 2019.

RIO GRANDE DO SUL. Assembleia Legislativa. **Projeto de Lei nº 15460/2020.** Cria o Banco de Dados de Reconhecimento Facial e Digital para a Prevenção ao Desaparecimento de Crianças e Adolescentes. Porto Alegre, 2020.

RIO GRANDE DO SUL. Assembleia Legislativa. **Projeto de Lei nº 16/2023.** Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo Poder Público no Estado do Rio Grande do Sul. Porto Alegre, 2023.

SADIN, Eric. **La inteligencia artificial o el desafío del siglo:** anatomía de un antihumanismo radical. Madrid: Caja Negra, 2020.

SANTA CATARINA. Assembleia Legislativa. **Projeto de Lei nº 0592.3/2013.** Obriga a utilização de sistema de identificação biométrica nas entradas e de sistema de monitoramento por imagem em toda a área de uso comum de estádios com capacidade superior a 10.000 (dez mil) pessoas, nos dias de jogos de futebol, e adota outras providências. Disponível em: https://www.alesc.sc.gov.br/legislativo/tramitacao-de-materia/PL./0592.3/2013. Acesso em 7 jun. 2024.

SANTA CATARINA. Assembleia Legislativa. **Projeto de Lei nº 0299.1/2018.** Dispõe sobre a possibilidade de convênio entre a secretaria de estado da segurança pública e os tabelionatos de notas para o compartilhamento de dados de identificação civil. Florianópolis, 2018. Disponível em: https://www.alesc.sc.gov.br/legislativo/tramitacao-de-materia/PL./0299.1/2018. Acesso em 7 jun. 2024.

SANTA CATARINA. Assembleia Legislativa. **Projeto de Lei nº 0027.1/2021.** Cria o banco de dados de reconhecimento facial e digital para a prevenção ao desaparecimento de crianças e adolescentes e adota outras providências. Florianópolis, 2021. Disponível em: https://www.alesc.sc.gov.br/legislativo/tramitacao-de-materia/PL./0027.1/2021. Acesso em 7 jun. 2024.

SÃO PAULO. Assembleia Legislativa. **Projeto de Lei nº 865/2019.** Torna obrigatória a instalação de câmeras de reconhecimento facial em todas as estações do Metrô e da CPTM, bem como no interior dos vagões das composições. São Paulo, 2019.

SÃO PAULO. Assembleia Legislativa. **Projeto de Lei nº 385/2022.** Restringe o uso de tecnologias de reconhecimento facial pelo Poder Público. São Paulo, 2022.

SÃO PAULO. Assembleia Legislativa. **Projeto de Lei nº 579/2023.** Institui o protocolo de acesso para visitantes nas unidades de ensino do Estado. São Paulo, 2023a.

SÃO PAULO. Assembleia Legislativa. **Projeto de Lei nº 580/2023.** Autoriza o Poder Executivo a implementar sistema de câmeras de reconhecimento facial nas unidades de ensino da rede pública do Estado. São Paulo, 2023b.SÃO PAULO. Assembleia Legislativa. Projeto de Lei nº 739/2023. Institui o porte eletrônico de identificação funcional para os integrantes da Polícia Militar do Estado. São Paulo, 2023c.

SEM Câmera na Minha Cara. 2023. **Meu recife**. Disponível em: https://www.semcameranaminhacara.meurecife.org.br/. Acesso em: 22 jan. 2024.

SENA, Anelice; BORGES, Juliana. Escolas de Nova Venécia usam reconhecimento facial para controlar frequência e desperdício de merenda. **G1.** Espírito Santo. 03 abr. 2018. Disponível em: https://g1.globo.com/es/espirito-santo/noticia/escolas-de-

nova-venecia-usam-reconhecimento-facial-para-controlar-frequencia-e-desperdicio-de-merenda.ghtml. Acesso em: 21 out. 2022.

SERGIPE. **Governo Do Estado De Sergipe.** Reconhecimento facial é reforçado com 27 câmeras para evitar entrada de foragidos da Justiça no Pré-Caju 2023. Sergipe, 2023. Disponível em: https://www.se.gov.br/noticias/seguranca-publica/reconhecimento_facial_e_reforcado_com_27_cameras_para_evitar_entrada_de_foragidos_da_justica_no_pre_caju_2023. Acesso em: 22 jan. 2024.

SERGIPE. Assembleia Legislativa. **Projeto de Lei nº 470/2023.** Dispõe sobre a restrição do uso de tecnologias de reconhecimento facial pelo poder público no estado de Sergipe. Aracaju, 2023.

SILVA, Mariah Rafaela; VARON, Joana. **Reconhecimento Facial no Setor Público e Identidades Trans:** tecnopolíticas de controle e ameaça à diversidade de gênero em suas interseccionalidades de raça, classe e território. Rio de Janeiro: Coding Rights, 2021. Disponível em: https://codingrights.org/docs/rec-facial-id-trans.pdf. Acesso em: 24 jan. 2024.

SILVA, Tarcizio da. **Racismo algorítmico**: inteligência artificial e discriminação nas redes digitais. São Paulo: Edições Sesc SP, 2022.

SILVEIRA, Sérgio Amadeu da; SOUZA, Joyce; CASSINO; João Francisco. Colonialismo de Dados: como opera a trincheira da guerra neoliberal. São Paulo: Autonomia Literaria, 2021.

SILVEIRA, Sérgio Amadeu da. Não haverá soberania digital sem o Estado. **Outras Palavras.** São Paulo. 06 set. 2023. Disponível em: https://outraspalavras.net/tecnologiaemdisputa/nao-havera-soberania-digital-sem-o-estado/. Acesso em: 22 jan. 2024.

SISTEMA de reconhecimento racial da PM do RJ falha, e Mulher é detida por engano. **G1.** Rio de Janeiro. 11 julho 2019 . Disponível em: https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml. Acesso em 13 junho 2022

SOARES, Ingrid. Lula diz que escolas não podem virar "prisão de segurança máxima". **Correio Brasiliense.** Brasília. 18 abr. 2023. Disponível em: https://www.correiobraziliense.com.br/politica/2023/04/5088168-lula-diz-que-escolas-nao-podem-virar-prisao-de-seguranca-maxima.html. Acesso em: 22 jan. 2024.

SOBRAL, Thiago. Tecnologia de reconhecimento facial para gestantes e nutrizes do programa de cestas nutricionais é implantada em Penedo**. Prefeitura de Penedo,** 2018. Disponível em: https://penedo.al.gov.br/2018/04/18/tecnologia-de-reconhecimento-facial-para-gestantes-e-nutrizes-do-programa-de-cestas-nutricionais-e-implantada-em-penedo/. Acesso em: 21 out. 2022.

SOLOVE, Daniel J., Data Mining and the Security-Liberty Debate. **University of Chicago Law Review**, Chicago, Vol. 74, p. 343, 2008, GWU Law School Public Law Research Paper v 278. Disponível em: https://ssrn.com/abstract=990030. Acesso em: 12 nov. 2022.

STOQUE. **Stoque**. [202-]. Disponível em: https://stoque.com.br. Acesso em: 12 set. 2022.

SOUZA, Leandro Miguel. Payface levanta R$ 15 mi e traz investidor de peso ao captable. **Startups.Com.Br.** 07 jul. 2023. Disponível em: https://startups.com.br/rodada-de-investimento/payface-levanta-r-45-mi-e-traz-investidor-de-peso-ao-captable/. Acesso em: 22 jan. 2024.

SURFSHARK. **The facial recognition world map**. [S.l.]. 2022. Disponível em: https://surfshark.com/facial-recognition-map. Acesso em: 07 set. 2022.

TAUTE, Fabian. Reconhecimento Facial e suas controvérsias. **Heinrich-Böll-Stiftung.** Rio de Janeiro. 07 fev. 2020. Disponível em: https://br.boell.org/pt-br/2020/02/05/reconhecimento-facial-e-suas-controversias. Acesso em: 21 out. 2022.

TECNOLOGIA de reconhecimento facial não será implantada pela Prefeitura do Recife e pelo Governo do Estado de Pernambuco. **Portal da Defensoria Pública de Pernambuco,** 2023. Disponível em: https://www.defensoria.pe.def.br/tecnologia-de-reconhecimento-facial-nao-sera-implantada-pela-prefeitura-do-recife-e-pelo-governo-do-estado-de-pernambuco/. Acesso em: 22 jan. 2024.

THE TIERRA COMÚN NETWORK. **Resisting Data Colonialism:** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023. Disponível em: https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

TIREMEUROSTODASUAMIRA. **Mapeamento dos projetos de lei sobre reconhecimento facial nos estados Brasileiros**. 2022. Disponível em: https://tiremeurostodasuamira.org.br/mapeamento/. Acesso em: 06 set. 2022.

TOCANTINS. **Lei nº 4058/2022, de 21 de dezembro de 2022.** Dispõe sobre o Banco de Dados de Reconhecimento Facial e Digital para a Prevenção ao Desaparecimento de Pessoas no Estado do Tocantins, e dá outras providências. Palmas, 2022. Disponível em: https://www.legisweb.com.br/legislacao/?id=440090. Acesso em 22 jul. 2024.

TOKARNIA, Mariana. Reconhecimento fotográfico de réu pode levar a erro, diz relatório. **EBC.** Rio de Janeiro. 05 maio 2022. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2022-05/reconhecimento-fotografico-de-reu-pode-levar-erro-diz-relatorio. Acesso em: 22 jan. 2024.

TOLEDO, Luiz Fernando. Poli-USP testa câmera de monitoramento facial. **O Estadão.** São Paulo. 23 jul. 2017. Disponível em: https://noticias.uol.com.br/ultimas-

noticias/agencia-estado/2017/07/23/poli-usp-testa-camera-de-monitoramento-facial.htm. Acesso em: 21 out. 2022.

TOLEDO, Mario. Câmeras de reconhecimento facial começam a funcionar em Copacabana: patrulhamento será feito durante o carnaval. **Agência Brasil**. Rio de Janeiro. 27 fev. 2019. Disponível em: https://agenciaBrasil.ebc.com.br/geral/noticia/2019-02/cameras-de-reconhecimento-facial-comecam-funcionar-em-copacabana. Acesso em: 21 maio 2021.

TRINDADE, A. Estado, governança e segurança pública no Brasil: Uma análise das secretarias estaduais de Segurança Pública. **Dilemas - Revista de Estudos de Conflito e Controle Social.** Rio de Janeiro, v. 8, n. 4, p. 607–632, 2015.

UNIÃO EUROPEIA. Parlamento Europeu. **Lei da UE sobre IA:** primeira regulamentação de inteligência artificial, 2023. Disponível em: https://www.europarl.europa.eu/news/pt/headlines/society/20230601STO93804/lei-da-ue-sobre-ia-primeira-regulamentacao-de-inteligencia-artificial. Acesso em: 23 jan. 2024.

VAN DIJCK, José; POELL, Thomas; WAAL, Martijn de. **The Platform Society:** Public Values in a Connective World. Oxford: Oxford University Press, 2018.

VAN DIJCK, José. Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. **Surveillance & Society**, [S.l.], v. 12, n. 2, p. 197-208, 2014.. Disponível em: https://www.academia.edu/26648535/Datafication_dataism_and_dataveillance_Big_Data_between_scientific_paradigm_and_ideology. Acesso em: 20 jul. 2022

VARON, Joana. Coloniality as an Attempt to Erase Other Ways of Living and Forms of Relating to our Bodies and Territories. In: THE TIERRA COMÚN NETWORK. **Resisting Data Colonialism:** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023, p. 45-50. Disponível em: https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

VÉLIZ, Carissa. **Privacidad es poder.** Datos, vigilância y libertad em la era digital. Madrid: Debates, 2021.

VERMEERSCH, Hans; DE PAUW, Evelien. The Acceptance of New Security Oriented Technologies: a ‘framing’ experiment. In: FRIEDWALD, Michael *et al*. **Surveillance, Privacy and Security**: citizen's perspectives. Nova York: Routledge, 2017. p. 52-71.

WINKER. **Controle de Acesso Winker**: segurança para o condomínio, autonomia e simplicidade para síndicos e moradores. [202-]. Disponível em: https://www.winker.com.br/lp-controle-acesso/. Acesso em: 12 set. 2022.

YANG, Chamee; BALASUBRAMANIAM, Gowri; BELITZ, Clara; CHAN, Anita Say. Resisting Data Colonialism and Digital Surveillance in a Midwestern Classroom: Exploring Community-driven Alternatives to Automated License Plate Readers. In:

THE TIERRA COMÚN NETWORK. **Resisting Data Colonialism:** a practical intervention. Amsterdam: Institute Of Network Cultures, 2023. p. 81-85. Disponível em: https://networkcultures.org/wp-content/uploads/2023/12/ResistingDataColonialism_INC2023_TOD50.pdf. Acesso em: 25 jan. 2024.

YESHIMABEIT, M.; TRAUB, A., 2021. **Data capitalism and Algorithmic Racism**. Paper Knowledge. Toward a Media History of Documents. . Disponível em: https://www.demos.org/sites/default/files/2021-05/Demos_%20D4BL_Data_Capitalism_Algorithmic_Racism.pdf. Acesso em: 14 jun. 2022.

ZANATTA, Rafael. Prefácio. In: MOROZOV Evgeny; BRIA, Francesca. **A cidade inteligente**: tecnologias urbanas e democracia. São Paulo: Ubu Editora, 2019.

ZUBOFF, Shoshana. **A Era do Capitalismo de Vigilância**: a luta por um futuro humano na nova fronteira de poder. Rio de Janeiro: Intrínseca, 2021.

ZUBOFF, Shoshana. Big other: capitalismo de vigilância e perspectivas para uma civilização de informação. In: BRUNO, Fernanda. **Tecnopolítica da vigilância: perspectivas da margem**. São Paulo: Boitempo, 2018, p.17-68.

ANEXO A – MODELO DE PEDIDO DE ACESSO À INFORMAÇÃO

Prezados,

Espero que esta mensagem encontre todos bem. Escrevo para solicitar informações sobre a adoção de reconhecimento facial na [segurança pública/educação] no [Estado].

Gostaria de solicitar informações detalhadas sobre a implementação de tecnologias de reconhecimento facial na segurança pública do estado, incluindo os objetivos dessa implementação. Há sistemas de reconhecimento facial em uso pela [inserir nome do órgão]? Se sim, estou interessada em saber como o sistema funciona na prática e como as informações são coletadas e armazenadas. Qual é o número de câmeras em funcionamento? Qual é o custo mensal dessas câmeras? Que empresa prestou e presta serviço na instalação e manutenção das câmeras em funcionamento? Sob que contrato ou contratos? Houve licitação?

Além disso, quem desenvolveu o sistema de reconhecimento facial? Que bases de dados são utilizadas para que o sistema realize o cruzamento de informações?

Em caso negativo, há previsão de implementação de sistema de reconhecimento facial por parte [inserir nome do órgão]?

Agradeço antecipadamente por sua ajuda. Aguardo ansiosamente sua resposta.

Atenciosamente,

ANEXO B – PEDIDO DE ACESSO À INFORMAÇÃO – SEGURANÇA PÚBLICA BAHIA

Gmail Camila Costa <camilamcta@gmail.com>

Resposta da sua demanda junto a Ouvidoria do(a) SSP

1 mensagem

Ouvidoria Geral do Estado da Bahia <sgo_oge@ouvidoria.ba.gov.br> 28 de abril de 2023 às 12:24
Para: camilamcta@gmail.com

==========
NAO RESPONDA ESTE E-MAIL. SUA RESPOSTA NAO SERA RECEBIDA.
==========

Senhora Camila,
A Ouvidoria Geral de Policia/SSP retorna na manifestacao no 2779136, cadastrada sob o no 4266 para enviar resposta fornecida pela Assessoria Tecnica - SSP/GAB/SGTO/ASTEC a seguir:
1) Ha sistemas de reconhecimento facial em uso por esta secretaria? Se sim, estou interessada em saber como o sistema funciona na pratica e como as informacoes sao coletadas e armazenadas.
Resposta: Sim. A solucao de video analitico avancado, implantada em sua fase inicial em 2018, possui uma arquitetura flexivel e que permite o uso de algoritmos de analises em cameras IP, com condicoes para que o usuario defina os gatilhos de eventos para um alarme, o que contribuiu para a automatizacao de diversos processos realizados anteriormente de forma manual, otimizando seus resultados. Essa solucao foi desenhada visando a alta disponibilidade dos servicos, com configuracao em modo Cluster ativo-ativo, instalada no Data Center do Centro de Operacoes e Inteligencia (COI), com acesso restrito ao ambiente, seguindo os principios estabelecidos nas melhores praticas de seguranca da informacao, com utilizacao dos dados estrita e exclusivamente paras as atividades de seguranca publica.
O uso das licencas do reconhecimento facial e feita de acordo com pontos de interesse de monitoramento por parte da Seguranca Publica, visto que esses analiticos podem ser direcionados, a qualquer momento, para qualquer camera da SSP, desde que atendam aos requisitos tecnicos de configuracao.
Registra-se que o uso dessa tecnologia pela Seguranca Publica visa apoia-la no exercicio das atribuicoes legais das forcas policiais como a protecao da vida e da propriedade, prevencao e deteccao de crimes e garantia da seguranca publica, tornando-se um instrumento salutar para o combate a criminalidade e passando a ser um instrumento agregador no mecanismo de prevencao ao crime quando empregadas em conjunto com processos e praticas eficientes de policiamento.

2) Qual e o numero de cameras em funcionamento?
Resposta: Atualmente a SSP/BA ja instalou 2.974 pontos de imagens (Reconhecimento Facial, Reconhecimento de Placas Veiculares e de analise situacional), atendendo a Capital, RMS e 77 Municipios da Bahia.

3) Qual e o custo mensal dessas cameras?
Resposta: O Governo da Bahia investiu R$ 665 milhoes para a implantacao do Projeto Video Policia Expansao, contratados nos moldes servicos por um periodo de 05 anos.

4) Que empresa prestou e presta servico na instalacao e manutencao das cameras em funcionamento? Sob que contrato ou contratos? Houve licitacao? Alem disso, quem desenvolveu o sistema de reconhecimento facial?
Resposta: A contratacao da tecnologia de reconhecimento facial foi feita atraves de licitacao publica, nos moldes de servico, e precedeu de realizacao de audiencia publica, com divulgacao de avisos e resumos dos editais de licitacao no Diario Oficial do Estado - DOE e em jornais de grande circulacao, conforme preceitua a Lei de no 9.433, no seu artigo 54. A ganhadora do certame foi o consorcio OI e Avantia. A fabricante da solucao (cameras e software de reconhecimento facial) e a empresa Huawei.

5) Que bases de dados sao utilizadas para que o sistema realize o cruzamento de informacoes?
Resposta: As bases de dados utilizadas para aplicacao do comparativo para o reconhecimento facial sao os bancos de dados de procurados com mandado de prisao e desaparecidos.

Atenciosamente,
OUVIDORIA GERAL DE POLICIA/SSP