O USO DE CÂMERAS DE RECONHECIMENTO FACIAL EM CONTEXTO DE PÓS DEMOCRACIA – UMA FERRAMENTA CONTRA O INIMIGO NO DIREITO PENAL?

Débora Freitas Mendes Pereira[1]

Resumo: Artigo apresentado para avaliação do semestre 2020/2, do Curso de Pós-Graduação Lata Sensu em Direito Digital, do ITS Rio em parceria com a UERJ. Analisamos aqui o uso das câmeras de reconhecimento facial como ferramenta de tecnologia dentro do espectro da repressão criminal, que coletam dados biométricos, observando-se a necessidade de uma forte regulamentação que possa ser eficaz para a proteção ao direito à privacidade e intimidade, diante de um quadro de fragilização da democracia, conforme análise de Rubens Casara, observando se os usos de tais máquinas podem servir de instrumentos que reforçam a criminalização dos grupos sociais já tradicionalmente alvos de repressão criminal, conforme a concepção de Raúl Zaffaroni do "inimigo no Direito Penal".

Palavras-chaves: Tecnologia de Vigilância; Repressão Criminal; Democracia; Direitos Fundamentais.

Introdução

Analisamos no presente artigo a influência do conceito de "pós democracia", expressão cunhada pelo cientista político Colin Crouch, da *Warwick University*, em 2000, e inserida no contexto nacional pelo professor Rubens Casara (2018)[2] diante da fragilização dos direitos fundamentais, observados a partir da realidade da efetivação destes direitos, em ambiente no qual a tecnologia pode ser utilizada para aprofundamento desta crise, amparando esta análise no estudo do professor Raúl Zaffaroni (2007)[3] quando avalia o indivíduo apontado como "inimigo no direito penal".

O foco da análise é direcionado às câmeras de reconhecimento facial que se tornaram, no Brasil, uma ferramenta importante no âmbito da segurança pública, propagadas como *cases* de sucesso, sobretudo, no cumprimento de mandados de prisão em aberto. Contudo, após estudo dirigido pelo Instituto Igarapé e pelo *Data PrivacyBR Research*[4], de junho de 2020 é possível se ter uma noção do tamanho do problema que

[1] Pós-graduada em Direito Público e Inteligência de Segurança Pública. Pós-Graduanda em Direito Digital. Delegada de Polícia Civil da Bahia.

[2] CASARA, Rubens. Estado Pós Democrático – Neo - Obscurantismo e Gestão dos Indesejáveis. Editora Civilização Brasileira. Rio de Janeiro. 2018.

[3] ZAFFARONI, Raúl. O Inimigo no Direito Penal. Editora Revan. Rio de Janeiro. 2007.

[4] Instituto Igarapé, Data Privacy BR Research. (junho de 2020). Fonte: https://igarape.org.br/: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/

tais câmeras podem causar para os direitos fundamentais. Alertas são dados ao contexto do cenário nacional, verificando-se que tanto na Europa quanto nos Estados Unidos a ferramenta de reconhecimento facial tem sido bastante contestada e até proibida, e, no caso da China, o uso tem se voltado, com frequência, para identificar e reprimir ativistas, como é o caso de movimentos pela democracia em Hong Kong.

Diante do cenário de início de vigência da Lei Geral de Proteção de Dados (LGPD), existe o desafio de que, no âmbito da segurança pública e da investigação criminal, será preciso aprovação pelo Congresso Nacional de lei específica sobre estes temas (conforme artigo 4.º, III e parágrafo 1.º da LGPD). No caso das câmeras de reconhecimento facial a legislação ainda deverá ser mais cuidadosa porque lidam com dados biométricos, que são extraídos quando da coleta algorítmica e são considerados **dados sensíveis** do indivíduo.

A lei específica de proteção de dados na seara penal deverá se orientar pelos mesmos princípios da LGPD que são: finalidade, necessidade, transparência, segurança e não discriminação. Em face deste princípio da "não discriminação", os procedimentos relacionados ao reconhecimento facial estarão sob o regramento do artigo 20 da LGPD, no que diz respeito às "decisões automatizadas", sendo direito do titular dos dados solicitar revisão de decisões "tomadas única e exclusivamente com base em tratamento automatizado de dados pessoais"[5].

Em relação aos direitos fundamentais, vemos o nascimento em nossa doutrina e jurisprudência de um novo direito dentro desta categoria, como é o da proteção dos dados pessoais. E esta proteção deverá ainda ser maior dentro do quadro de dados sigilosos e sensíveis. Buscaremos neste artigo analisar o problema da utilização dos dados pessoais, especificamente os da biometria coletados pelas câmeras de reconhecimento facial dentro de um contexto de segurança pública e investigação criminal, levando em consideração a ausência de regulamentação que possa dar limites ao uso desta ferramenta de forma a

[5] Lei Geral de Proteção de Dados. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

evitar que possa ser utilizada contra "os que incomodam o poder", dentro da concepção de Zaffaroni (2007:22)[6] e da própria criminologia crítica, conforme Barata (2002)[7]

A Lei Geral de Proteção de Dados Pessoais (LGPD) e a Proteção de Dados Penais:

A Lei Geral de Proteção de Dados Pessoais (LGPD), n.º 13.709, de 14 de agosto de 2018, entrou em vigor em setembro de 2020, vindo para proteger o tratamento de dados dos indivíduos por entidades públicas e privadas. Com a velocidade do desenvolvimento da *internet* temos visto coleta de dados pessoais em níveis nunca antes observados, sejam através de mecanismos de inteligência artificial que estruturam a *Internet* das Coisas (IOT) e conforme Magrani (2018:20) tenta-se conceituar o tema[8]:

> Existem fortes divergências em relação ao conceito de IOT, não havendo, portanto, um conceito único que possa ser considerado pacífico ou unânime. De maneira geral pode ser entendido como um ambiente de objetos físicos interconectados com a *internet* por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia. O que todas as definições de IOT têm em comum é que elas se concentram em como computadores, sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de hiperconctividade.

A Lei Geral de Proteção de Dados (LGPD), é fundamental para a proteção da intimidade e privacidade do indivíduo. Em nosso país o seu texto teve forte influência da lei geral europeia, conhecida como GDPR - *General Data Protetion Regulation*. Seus princípios estão contidos no artigo 2.º da LGPD. O dado pessoal só poderá ser fornecido com o consentimento do titular (artigo 5.º, I e XII da LGPD). O arcabouço de proteção aos direitos da personalidade, como observamos, na LGPD, são pontos fundamentais dessa nova era da informação. O dado pessoal faz parte do arcabouço de direitos individuais e seu fornecimento só poderá ser oportunizado em uma relação de consentimento entre o titular deste e o seu tomador. De acordo com Bioni (2020:12):

> Com a inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (*marketing*) e a sua promoção (publicidade), os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação. E, com a possibilidade de organizar tais dados de maneira mais escalável (e.g., *Big Data*), criou-se um (novo) mercado cuja base de sustentação é a sua extração e comodificação. Há uma 'economia de vigilância' que tende a posicionar o cidadão como um mero expectador das suas informações. Esse é um diagnóstico necessário, sem o qual não se poderia avançar na investigação do papel

[6] ZAFFARONI, Raúl. O Inimigo no Direito Penal. Editora Revan. Rio de Janeiro. 2007.
[7] BARATTA, Alessandro. Criminologia Crítica e Crítica do Direito Penal. Editora Revan. Rio de Janeiro. 2002.
[8] MAGRANI, Eduardo, A Internet das Coisas. Editora FGV. Rio de Janeiro. 2018, pág 20.

> do consentimento na proteção dos dados pessoais, especialmente, por rivalizar com tal condição de passividade atribuída ao cidadão quanto ao fluxo de suas informações pessoais".

No mesmo sentido, temos o estudo de Shoshana Zuboff (2018:17)[9], no qual a mesma analisa os efeitos do capitalismo de vigilância dentro da sociedade de informação, citando um trabalho produzido pela Casa Branca, de 2015, que diz: "a trajetória tecnológica é bastante clara: mais dados serão produzidos sobre indivíduos; a manutenção desses dados, porém, ficará sob o controle de outros". Restando claro que a proteção de dados pessoais se tornou vital para a humanidade.

No caso da área de coleta de dados para a área penal, não obstante a LGPD se destine, também, ao setor público, o artigo 4.º da lei, inciso III, informa que não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de: **"segurança pública**; defesa nacional; segurança do Estado **e atividades de investigação e repressão de infrações penais" (grifos)**. Para tanto o parágrafo 1.º deste dispositivo legal exige que "o tratamento de dados pessoais previsto no inciso III, será regido por **legislação específica,** que deverá **prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público**, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta lei" (Grifos). Para efeitos desta análise, específica, é preciso focar nas necessidades ao atendimento do **interesse público** nas atividades de investigação e repressão de infrações penais por parte dos órgãos da persecução penal.

Em 2019, o presidente de Câmara dos Deputados Rodrigo Maia, instituiu uma Comissão de Juristas para propor ao Parlamento brasileiro um anteprojeto de lei sobre o tema em questão, e neste ano de 2020, a comissão realizou um seminário internacional para discutir o tema. O Instituto de Tecnologia e Sociedade (ITS Rio), analisou o seminário e as pesquisadoras Ana Lara Mangoth e Giovana Carneiro avaliaram as discussões. Quanto ao reconhecimento facial destacam a posição do professor Eric Hilgendorf, tratando da abordagem europeia quanto ao tema:

> Segundo o professor Eric Hilgendorf, a abordagem europeia da regulação de Inteligência Artificial, especialmente quando se trata da atividade policial e processos criminais, está voltada para a ideia de que todas as **medidas estatais devem ser baseadas nos direitos fundamentais dos cidadãos**. Isso decorre justamente do direito

[9] *Big Other*: Capitalismo de Vigilância e Perspectivas Para uma Civilização de Informação. Tecnopolíticas de Vigilância. 2018.

> à autodeterminação informacional, anteriormente mencionado. Em paralelo, na concepção europeia e alemã, principalmente, o Estado é obrigado a proteger os direitos dos cidadãos, o que inclui a segurança pública, a luta contra o crime e a investigação criminal, a favor dos quais devem ser usados os melhores e mais atualizados métodos. Isso inclui, ainda, o uso de Inteligência Artificial para reconhecimento facial e análise de DNA. Em suma, dois direitos precisam ser sopesados: a **privacidade e direitos fundamentais dos cidadãos**, por um lado, e o **interesse da sociedade na ordem e segurança pública**, de outro. **Esses usos são legalmente possíveis, mas a interferência no direito deve ser proporcional, adequada, necessária e apropriada.** Na Alemanha, há o uso de câmeras de vigilância e reconhecimento facial para prevenir situações de violência. Entretanto, sublinha Hilgendorf, o uso de câmeras de vigilância também significa que cidadãos inocentes estão sendo vigiados e isto tem um impacto no comportamento dos cidadãos: a ampla implementação desses dispositivos coloca uma pressão nos indivíduos sobre a detecção do que pode ser considerado anormal, então eles tendem a se comportar da forma mais regular possível, o que não é uma boa tendência para a democracia. Além das questões da privacidade, há também riscos relacionados a possíveis falhas desses dispositivos e internalização de vieses, o que vem sendo muito discutido na União Europeia e nos Estados Unidos. Pesquisas demonstram que *softwares* utilizados para análise e reconhecimento facial executam de forma distinta de acordo com idade, gênero e raça da pessoa identificada. Algoritmos executados dessa forma podem reforçar preconceitos na sociedade, razão pela qual controladores de dados devem garantir que dados biométricos derivados de vigilância por câmeras sejam objeto de avaliação regular com relação a sua relevância e também sobre a eficiência das garantias fornecidas — tópico muito discutido pelo *EU High Level Expert Group on AI*. Na Alemanha, **câmeras de vigilância com reconhecimento facial em locais públicos**, em geral, são permitidas, mesmo que estejam em aparente conflito com o direito à autodeterminação informacional. Muitos cidadãos alemães solicitam informações às autoridades sobre os dados coletados e o uso dessas informações, o que é positivo e faz com que a atividade seja mais transparente. O cenário atual encontra-se longe de banir o reconhecimento facial, porém ainda não há uma regulação específica de tal atividade na Alemanha, o que é passível de ser feito no próximo governo.

Em 05 de novembro de 2020, a Comissão Juristas, acima citada, entregou ao Presidente da Câmara dos Deputados, o anteprojeto de lei sobre tratamento de dados pessoais na área criminal. Em relação ao tratamento de dados relacionados às decisões automatizadas, que se relacionam com a atuação das câmeras de reconhecimento facial, o anteprojeto indicou um capítulo para tratar do assunto: "Tecnologias de Monitoramento e Tratamento de Dados de Elevado Risco". O artigo 42 do anteprojeto estabelece: "A utilização de tecnologias de monitoramento ou o tratamento de dados pessoais que representem **elevado risco** para direitos, liberdades e garantias dos titulares dos dados por autoridades competentes **dependerá de previsão legal específica**, que estabeleça garantias aos direitos dos titulares e seja precedida de **relatório de impacto de vigilância"**, com critérios previstos no parágrafo único deste artigo 42. (Grifos).

O artigo 43 do anteprojeto se preocupada com **a utilização dos dados de forma indeterminada, em tempo real e de forma continuada dos indivíduos, sem que haja conexão com a atividade de persecução penal individualizada e autorizada por lei e**

decisão judicial. Este ponto é relevante a ser observado quando se sabe que as máquinas de reconhecimento facial possuem tecnologia para obtenção de informação para além das questões de natureza criminal, como é possível se perceber da matéria veiculada no programa "Fantástico"[10], da rede Globo, onde o jornalista Murilo Salviano, obtém informações preocupantes vindas dos gestores da ferramenta da Secretaria de Segurança Pública da Bahia, quando demonstram que em suas bases de dados, não existem apenas fotografias de pessoas com mandados de prisão em aberto, mas que podem identificar qualquer pessoa para objetivos não regulados e disciplinados, através do cruzamento de dados com redes sociais. O indivíduo se torna um número, que é sua identidade biométrica, e que este número são informações de algoritmos extraídos das características do rosto do indivíduo: distância entre os olhos, tamanho da boca e nariz, linha da mandíbula. Na matéria, o Secretário da Segurança da Bahia aponta que possíveis erros das máquinas estão dentro de uma margem esperada e não demonstra ver problemas nisto; ainda sendo registrado que o sistema teria sido comprado de uma empresa chinesa pelo valor de dezoito milhões de reais.

Bauman e Lyon (2013:98), em reflexão acerca do controle social exercido pela tecnologia de vigilância, avaliam o que denominam de um crescente "medo do Outro", que acaba por dar carta branca aos detentores do poder para o uso indiscriminado de câmeras de reconhecimento facial:

> ...O Outro é um vizinho, um transeunte, um vadio, um espreitador, em última instância, qualquer estranho. Mas, então, como todos sabemos, os moradores das cidades são estranhos entre si, e todos somos suspeitos de portar o perigo; assim, todos nós, em algum grau, queremos que as ameaças flutuantes, difusas e incontroladas sejam condensadas e acumuladas num 'conjunto de suspeitos habituais'. Espera-se que essa condensação mantenha a ameaça afastada e também, simultaneamente, nos proteja do perigo de sermos classificados como parte dela.

Ocorre que, tanto no Brasil como ao redor do mundo, casos de erros na identificação por reconhecimento facial, têm colocado o sistema sob suspeita, a exemplo da prisão de Robert Williams[11], na cidade de Detroit, em janeiro de 2020, pela prática do crime de roubo de cinco relógios, ao valor de US$ 3.800,00 (três mil e oitocentos dólares), na cidade de Shinola, em outubro de 2018. Williams foi identificado erroneamente, pela ferramenta de reconhecimento facial do Departamento de Polícia de Detroit, sendo

[10] http://g1.globo.com/bahia/bahia-meio-dia/videos/t/edicoes/v/fantastico-mostra-como-funciona-o-reconhecimento-facial-nas-cameras-de-seguranca/7445951/

[11]https://www.uol.com.br/tilt/noticias/redacao/2020/06/25/homem-e-preso-apos-erro-de-tecnologia-de-reconhecimento-facial-nos-eua.htm

utilizada as imagens da cena do crime cruzadas com a imagem da carteira de motorista de Robert Williams. Um outro caso que ganhou matérias jornalísticas[12] ocorreu em 2019, quando uma mulher foi presa erroneamente em Copacabana, sendo confundida com uma outra que teria um mandado de prisão em aberto, em erro da captura das imagens.

Discute-se também acerca dos problemas associados à leitura dos algoritmos quando se está diante da relação comparativa entre o alvo que se busca e a pessoa que está sendo identificada. Nesse sentido, Fernanda Bruno (2018:242)[13] alerta:

> Tecnicamente um algoritmo é uma sequência de regras ou de instruções voltadas para a execução automatizada de uma tarefa. O problema não é essa mediação em particular, mas o modo como ela vem sendo construída: **encapsulada nas caixas-pretas dos Estados ou corporações**, torna-se extremamente difícil tanto a compreensão como a negociação dos habitantes da cidade com tais mediadores. Em suma, **o problema é o fato de certas experiências coletivas da cidade tornarem-se prioritariamente mediadas por algoritmos privados ou estatais extremamente opacos.** (Grifos).

Diante do "novo brinquedo" Panótico[14], no sentido proposto pelo jurista e filósofo Jeremy Bentham, preocupa a possibilidade de controle social com uso de tecnologia de vigilância, conforme fora estabelecido para o domínio de prisioneiros, cujo modelo pode atravessar as fronteiras da prisão:

> Você ficará satisfeito em observar que, embora o ponto mais importante seja, talvez, o de que as pessoas a serem inspecionadas sempre **sentir-se-ão como se estivessem sob inspeção ou, pelo menos, como tendo uma grande possibilidade de estarem sob inspeção**, essa não é, de forma alguma, a única possibilidade. Se fosse, a mesma vantagem poderia ser atribuída a edifícios de praticamente qualquer forma. O que é também de importância é que, para a máxima proporção de tempo possível, **cada homem deve realmente estar sob inspeção. É importante, em todos os casos, que o inspetor possa ter a satisfação de saber que a disciplina realmente tenha o efeito para o qual é planejada:** e é mais particularmente importante naqueles casos em que o inspetor, além de ver que eles se conformam às regras em vigor, tem que lhes fornecer aquelas instruções transientes e incidentais que são necessárias no início de qualquer tipo de atividade. E penso que não é necessária muita argumentação para provar que a atividade de inspeção, como qualquer outra, será exercida a um grau maior de perfeição na medida em que menores forem os problemas causados por seu exercício. (Grifos).

O anteprojeto dos juristas da lei de dados penal, escolheu o Conselho Nacional de Justiça (CNJ) para ser o órgão máximo que emitirá opiniões técnicas ou

[12]https://canaltech.com.br/governo/mulher-e-detida-por-engano-apos-erro-em-sistema-de-reconhecimento-facial-no-rj-143761/

[13] BRUNO, Fernanda. Visões Maquínicas da Cidade Maravilhosa: Do Centro de Operações do Rio à Vila Autódromo. Tecnopolíticas da Vigilância, Perspectivas da Margem. Boitempo. São Paulo. 2018. Pág 242.

[14] Pan- ótico, aqui no sentido dado por Jeremy Bentham, como prisão ideal que permite, por meio de seu formato físico, que apenas um vigilante cuide dos prisioneiros, sugerindo aos mesmos um comportamento desejado. Nesse sentido, O Panóptico – JEREMY BENTHAM.

recomendações e publicará relatório anual acerca do uso das tecnologias de monitoramento, bem como auditoria em face de denúncias de descumprimento da Lei. Vide artigos 10 e 11, do anteprojeto. Tais exigências legais deverão estar, a nosso sentir relacionados a uma condição de responsabilização acerca da coleta e do uso de tais dados, gerando ampla implicação de natureza civil, administrativa e penal, quando da identificação de desvios funcionais e governamentais. Tudo isto em clara consonância com a carta Magna e a proteção dos direitos individuais.

O uso de Tecnologia de Vigilância em Hong Kong:

A cidade autônoma de Hong Kong voltou ao controle da China em 1997, após 156 anos sob o domínio Inglês, na condição de colônia, que ocorreu após a primeira guerra do ópio em 1842. Contudo, desde o ano de 2012, temos acompanhado uma série de conflitos entre a população de Hong Kong e o governo central de *Beijing*[15], numa clara demonstração que objetivo da China é impor seu regime político. Esse choque se reflete na relação com Hong Kong, que tem forte influência de valores democráticos. A diferença entre a cultura dos dois povos é tão marcante que reportagem da BBC News destaca 5 (cinco) pontos de diferença entre as duas comunidades[16]: do sistema político, administrativo, do sistema judicial, em relação aos direitos civis, e na economia. Vige o sistema chamado de "um país, dois sistemas", onde se permite que a região conviva com o comunismo e capitalismo ao mesmo tempo.

No documentário "Joshua: Adolescente vs. Superpotência", do catálogo da Netflix[17], é retratado o movimento liderado por um estudante de 14 (quatorze) anos em 2012, quando criou o movimento "Escolarismo", para combater a implantação de um programa de educação nacional imposto pelo governo chinês para o povo de Hong Kong, e mostra com clareza o conflito político e cultural entre as duas regiões. O jovem Joshua Wong, escreveu o relato de sua luta de ativista pela democracia em Hong Kong[18], e apela pela defesa de direitos democráticos, explicando que qualquer sociedade pode vir a sofrer o que seu povo sofre, atualmente:

[15] Beijing ou Pequim, são a mesma coisa. Capital da China.
[16]https://noticias.uol.com.br/ultimas-noticias/bbc/2019/07/05/as-5-principais-diferencas-da-vida-em-hong-kong-e-na-china.htm
[17] https://www.netflix.com/br/title/80169348
[18] WONG, Joshua. Democracia Ameaçada. Faro Editora. Barueri. 2020

> O livro termina com um apelo urgente para todos nós defendermos os nossos direitos democráticos. Incidentes recentes, desde a polêmica nas redes sociais envolvendo a China e a NBA, principal liga de basquete profissional dos Estados Unidos, até a retirada de um aplicativo de rastreamento policial em Hong Kong pela Apple, mostraram que a erosão das liberdades que assolou Hong Kong está se espalhando pelo resto do mundo. Se as multinacionais, os governos internacionais e, sem dúvidas, os cidadãos comuns não começarem a prestar atenção em Hong Kong e a tratarem nossa história como um sinal de alerta, não demorará muito para que todo mundo sinta a mesma violação das liberdades civis que os honcongueses sofreram, não sem resistência, todos os dias nas últimas duas décadas.[19]

Em 2013, Xi Jinping, foi eleito pelo partido comunista chinês e passou a ser o líder máximo da China e a ofensiva pelo controle de Hong Kong se tornou mais agressiva, sobretudo em face da luta histórica da unidade autônoma em relação ao voto universal, como era a promessa quando da devolução de Hong Kong, pelos ingleses em 1997, como uma questão fundamental para a defesa da soberania da Ilha. O movimento ativista se chamou: "Occupy". A ofensiva de Pequim foi tentar negociar com o movimento a eleição de lideranças através de uma lista de candidatos previamente escolhidos pelo governo central chinês e ofertá-los para os cidadãos de Hong Kong. Ou seja: o povo de Hong Kong poderia escolher seus líderes, desde que fossem da lista chinesa ofertada. O movimento recrudesceu e a violência por parte do governo de Hong Kong, controlado pela China, passou a ser violento contra os manifestantes. O movimento ativista aumentou em participação popular, passando a ser denominado pela mídia de "Revolução dos Guarda-chuvas", porque o povo começou a usar guarda-chuvas para se defenderem do *spray* de pimenta jogado pelos policiais contra os manifestantes.

Em 2019, matéria da revista "Olhar Digital"[20], reporta novo movimento em Hong Kong contra a China em face de projeto de lei que autoriza cidadãos desta cidade serem extraditados por suspeita de crime contra a China. Na repressão a este movimento caracterizou-se **o uso massivo do reconhecimento facial por câmeras, equipadas com avançadas tecnologias de inteligência artificial.** Uma forma interessante dos manifestantes buscarem evitar serem identificados pelas câmeras de tecnológica foi a utilização de *lasers*, o que acabou por se tornar uma verdadeira "guerra cibernética". A ideia era enfrentar o sistema de vigilância massiva e avançado do sistema chinês contra os manifestantes, evitando a identificação dos participantes e consequentes prisões.

[19] WONG, Joshua. Democracia Ameaçada. Faro Editorial. Barueri. 2020. Pág 14
[20] https://olhardigital.com.br/noticia/manifestantes-usam-laser-contra-cameras-de-reconhecimento-facial/88677

A Fragilização dos Direitos Fundamentais no Brasil. O uso de Tecnologia de Vigilância e seu possível uso policial contra os inimigos do Poder:

Para Zaffaroni (2007:21)[21], a essência do conceito inimigo no direito penal está associada a aqueles que são inimigos do poder. E a repressão contra estes "inimigos" pode variar a depender do etiquetamento criminoso que lhes possa atribuir:

> De todo modo e para concluir, o que se discute em doutrina penal é a admissibilidade do conceito de inimigo no direito penal (ou no direito em geral) do Estado de Direito, considerando como tal aquele que é punido só em razão de sua condição de ente perigoso ou daninho para a sociedade, sem que seja relevante saber se a privação dos direitos mais elementares à qual é submetido (sobretudo, a sua liberdade) seja praticada com qualquer outro diferente do de pena, e sem prejuízo, tampouco, de que se lhe reconheça um resíduo de direitos mais ou menos amplo.

A aplicação do direito penal é seletiva, sobretudo, diante da estratificação social e econômica em nosso país. E nem todos possuem o mesmo tratamento dado pelo sistema de justiça criminal, não sendo difícil esta constatação diante da simples análise daqueles que compõe o quadro majoritário dos presos no Brasil e são alvos preferenciais da polícia, conforme os diversos estudos anuais do atlas da violência no Brasil, produzido pelo Instituto de Pesquisa Econômica Aplicada (IPEA)[22]

Para o exercício da análise deste fenômeno, de populismo penal, em nosso país são relevantes os ensinamentos de Casara (2018)[23] em relação ao nascimento, por assim dizer da construção de um "estado pós democrático", onde a fragilizalização dos direitos fundamentais é real em nosso país. Casara (2018:20) explicita:

> ...A opção política que levou ao Estado Democrático de Direito, construída após a Segunda Guerra Mundial, é a de que **o poder deve ser limitado,** a fim de evitar novos holocaustos e permitir o exercício da máxima liberdade (vida plena), compatível com igual liberdade dos demais (vida plena dos outros). Não por acaso, os direitos e as garantias fundamentais previstos na Constituição da República tornaram-se os principais limites ao exercício do poder...O que há de novo na atual quadra histórica, e que sinaliza a superação do Estado Democrático de Direito, não é a violação dos limites ao exercício do poder, **mas o desaparecimento de qualquer pretensão de fazer valer esses limites.** Isso equivale a dizer que não existe mais uma preocupação democrática, ou melhor, **que os valores do Estado Democrático de Direito não produzem mais o efeito de limitar o exercício do poder em concreto.** Em uma primeira aproximação, pode-se afirmar que na pós-democracia desaparecem, mais do que a fachada democrática do Estado, os valores democráticos.[24] (Grifos).

[21] ZAFFARONI, Raúl. O Inimigo no Direito Penal. Editora Revan. Rio de Janeiro. 2007. Pág 21.
[22]https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=36488&Itemid=432
[23] CASARA. Rubens R.R. Estado Pós Democrático. Neo-Obscurantismo e Gestão dos Indesejáveis. Editora Civilização Brasileira. Rio de Janeiro. 2018.
[24] Idem. Pág 20 a 22.

A teoria do *labeling approach* (etiquetamento social), também nos ajuda a compreender que o sistema penal não é neutro, conforme ensina Barata (2002:86)[25], quando da análise de quem é o sujeito criminoso: "...depende menos de uma atitude interior intrinsecamente boa ou má, social ou antissocial, valorável positiva ou negativa pelos indivíduos, do que da definição legal **que, em dado momento distingue, em determina sociedade, o comportamento criminoso do comportamento lícito**". (Grifos).

Temos diversos exemplos deste fenômeno na aplicação do sistema penal brasileiro. Em 2016 tivemos o caso em São Paulo, quando da manifestação de ativistas contra o governo Temer e o Capitão do Exército Willian Pina Botelho[26] se infiltrou em aplicativo de encontros, via *internet* conhecido como *Tinder* e no *WhatsApp*, para se aproximar dos ativistas e de seus diálogos. Registre-se que realizou estes atos sem autorização judicial em atividade de inteligência estatal. Outro caso que vemos acontecer em nosso país e que chega a ser teratológico é a discussão no Congresso Nacional e no Supremo Tribunal Federal, acerca da prisão em segunda instância nascida do gérmem autoritário chamado "Operação Lava Jato", e também defendida no bojo do "`Pacote Anticrime", que resultou na Lei 13.964/2019, à revelia da cláusula pétrea estabelecido na Constituição Federal, no artigo 5.º, LVII.

Em estudo do Instituto Igarapé e o Data Privacy BR[27], foram analisadas questões relacionadas à questão do videomonitoramento[28], em análise em três cidades brasileiras: Campinas; Salvador e São Paulo. O estudo tratou de avaliar o uso das câmeras de circuito fechado de televisão (CFTV), Câmeras com softwares de reconhecimento facial e de placas de veículos. Em relação ao reconhecimento facial, o estudo aponta as seguintes conclusões:

> **Privacidade:** diferentemente do reconhecimento por íris ou de impressão digital, o reconhecimento facial é um método de identificação biométrica que opera mesmo sem o conhecimento da pessoa que tem o seu rosto analisado. O sistema permite fazer varreduras em massa de pessoas que passaram apenas segundos diante de uma câmera. Ao redor do mundo, empresas têm construído grandes bases de dados de rostos para

[25] BARATTA, Alessandro. Criminologia Crítica e Crítica do Direito Penal. Editora Revan. Rio de Janeiro. 2002. Pág 86.
[26] https://brasil.elpais.com/brasil/2019/05/17/politica/1558119752_973399.html
[27]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.pdf
[28] https://igarape.org.br/videomonitoramento-webreport

> testes desses sistemas. Entretanto, há o risco de essas bases serem comercializadas ou mesmo acessadas indevidamente por terceiros, se não forem armazenadas adequadamente ou se *hackeadas*. Além disso, outra preocupação que surge com o uso do reconhecimento facial é não se poder verificar a prática de coleta e o armazenamento das imagens captadas, devido à ausência de mecanismos de transparência adequados. **Bases de dados:** riscos distintos surgem com o uso de bases de dados distintas. Por exemplo, um sistema que utiliza bases de treinamento formadas primordialmente por pessoas brancas irá ter dificuldades em identificar rostos negros. O cruzamento entre diferentes bases de dados pode ampliar o risco de se produzir "caixas-pretas" em que não seja possível explicar um falso positivo, se não acompanhado de mecanismos de compliance adequados. No caso específico do uso de bases de dados de procurados pela justiça e pessoas desaparecidas, o principal risco decorre da falta de atualização das informações ali presentes. **Confiança nas instituições**: A falta de mecanismos de transparência que permitam avaliar, de modo independente, a eficácia e o uso adequado do reconhecimento facial, assim como garantir o respeito à legislação de proteção de dados pessoais, gera incerteza sobre como esses sistemas são efetivamente utilizados. Além disso, a **ineficiência** desses sistemas, devido ao alto número de falsos positivos, pode afetar a confiança nas instituições que o utilizam. É fundamental, portanto, que o setor público seja transparente sobre o uso e a implementação do reconhecimento facial e que trabalhe de modo que a sociedade civil e a comunidade técnica possam avaliar possíveis violações aos direitos humanos, se o investimento compensa e colaborar com sugestões e mecanismos para se remediar erros e abusos. **Ampliação do uso**: À medida que o reconhecimento facial se torna uma ferramenta popular, o risco é que passe a ser utilizado como critério para acesso a um serviço – por exemplo, como condição para matricular um filho na escola, utilizar serviços de saúde, declarar imposto de renda ou mesmo para acesso ao crédito. Esse cenário amplia o horizonte do reconhecimento facial para além do monitoramento em massa, abrindo espaço para uma série de injustiças e abusos.

Portanto, se faz necessária forte regulação em face da questão da utilização das máquinas de reconhecimento facial, posto que tomam decisões automatizadas, e, sobretudo, no campo da segurança pública e da investigação criminal, o rigor deve ser ainda maior, a fim de que seus detentores e executores sejam responsabilizados diante de um sistema que possa ser usado contra os indivíduos e de possível instrumentalização para perseguição e de criminalização, em atuação desviada da prevista em lei.

Conclusão:

Concluímos pela necessidade de que as futuras regulações relacionadas às ferramentas de câmeras de reconhecimento facial estejam atentas aos direitos fundamentais, não se constituindo em máquinas a serviço de perseguição política e policial, como vemos acontecer na China, posto que, não obstante o Brasil possuir uma Carta Magna, com dispositivos que protegem os cidadãos dos abusos do poder estatal; a verdade é que temos visto o esgarçamento desta proteção diante do fenômeno da fragilização da democracia, aliada a uma conjuntura de desigualdade social e de forte repressão criminal, já próprias do Brasil, onde determinados sujeitos, pela sua condição

socioeconômica e posição política podem sofrer os efeitos de controle persecutório facilitado por tecnologias de vigilância, a exemplo das câmeras de reconhecimento facial.

A condição das câmeras de reconhecimento facial recolherem dados biométricos dos indivíduos, e levando-se em consideração que os dados pessoais vem ganhando *status* de direito humano fundamental, exige daqueles que manipulam estes dados um nível elevado de responsabilidade e de responsabilização, quando descumprirem a LGPD, e as futuras legislações de proteção de dados penal. Como vimos no estudo do Instituto Igarapé e do *Data PrivacyBR Reserch*, especificamente em relação às câmeras de reconhecimento facial, percebemos que se tratam de uma espécie de "caixa preta", na atual situação de uso pela segurança pública, sendo, absolutamente necessário, que sejam fiscalizadas e que prestem *accountability* para a sociedade.

Com a real existência de casos de "falsos positivos", no campo do reconhecimento facial criminal, além da coleta de dados biométricos de forma indiscriminada, de todo e qualquer indivíduo que passe por local de monitoramento, gera, uma afetação ao direito à intimidade e privacidade, de cidadãos que sequer são investigados criminalmente.

Para além disto, conforme a teoria de Montesquieu[29] sabemos que quem possui muito poder costuma abusar deste (fundamento para a teoria tripartite do poder e dos freios e contrapesos, nas democracias). É preciso cuidar para que mesmo em sociedades democráticas como a brasileira, não se aceite a utilização deste tipo de ferramenta de vigilância tecnológica para controle e perseguição política e policial, haja vista a fragilização dos direitos fundamentais, norteados pela realidade de violência social, no qual o uso do direito penal como instrumento persecutório de excluídos de direitos básicos, onde a utilização da ideia de "dano colateral" (utilizado na doutrina militar para justificar a morte de civis em combate, de forma acidental, em erro justificável, dentro de uma lógica de guerra), acaba sendo normalizada em nosso país. Que, esta lógica perversa não vigore dentro da tecnopolítica de vigilância voltada para a segurança pública e investigação criminal, que deve preservar direitos e proteger vidas, sempre.

[29]MONTESQUIEU. O Espírito das Leis. Editora Martin Claret. 2010. São Paulo.

REFERÊNCIAS:

BARATA, A. (2002). *Criminologia Crítica e Crítica do Direito Penal.* Rio de Janeiro: Revan.

BAUMAN, Z. L. (2014). *Vigilância Líquida.* Rio de Janeiro: Zahar.

Câmara dos Deputados. (11 de novembro de 2019). Dispoível em: https://www.camara.leg.br/: https://www.camara.leg.br/noticias/618483-maia-cria-comissao-de-juristas-para-propor-lei-sobre-uso-de-dados-pessoais-em-investigacoes/Acesso em 12 de outubro de 2020.

Câmara dos Deputados. (10 de julho de 2020). Disponível em: https://www.camara.leg.br/: https://www.camara.leg.br/noticias/675204-seminario-internacional-sobre-protecao-de-dados-pessoais-termina-hoje/Acesso em: 30 de outubro de 2020.

Canaltch. (10 de julho de 2019). Disponível em: https://canaltech.com.br/: https://canaltech.com.br/governo/mulher-e-detida-por-engano-apos-erro-em-sistema-de-reconhecimento-facial-no-rj-143761/Acesso em 30 de outubro de 2020.

Carneiro, A. L. (11 de agosto de 2020). Disponível em: *https://feed.itsrio.org/caminhos-para-a-prote%C3%A7%C3%A3o-de-dados-pessoais-na-seguran%C3%A7a-p%C3%BAblica-e-investiga%C3%A7%C3%A3o-criminal-li%C3%A7%C3%B5es-do-595027052636*. Fonte: https://itsrio.org/pt/home/: https://feed.itsrio.org/caminhos-para-a-prote%C3%A7%C3%A3o-de-dados-pessoais-na-seguran%C3%A7a-p%C3%BAblica-e-investiga%C3%A7%C3%A3o-criminal-li%C3%A7%C3%B5es-do-595027052636. Acesso em: 20 de agosto de 2020.

CASARA, R. (2018). *Estado Pós Democrático - Neo-Obscurantismo e Gestão dos Indesejáveis.* Rio de Janeiro: Civilização Brasileira.

El País. (17 de maio de 2019). Disponível em: https://brasil.elpais.com/: https://brasil.elpais.com/brasil/2019/05/17/politica/1558119752_973399.html. Acesso em 18 de novembro de 2020.

G1 - Globo - Bahia. (11 de março de 2019). Disponível em: https://g1.globo.com/ba/bahia/: http://g1.globo.com/bahia/bahia-meio-dia/videos/t/edicoes/v/fantastico-mostra-como-funciona-o-reconhecimento-facial-nas-cameras-de-seguranca/7445951/?trk=organization-update-content_share-video-embed_share-article_title. Acesso em 05 de novembro de 2020.

http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. (24 de abril de 2020). Disponível em: www.stf.jus.br: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em 10 de junho de 2020.

Instituto Igarapé. (2020). *Videomonitoramento - Mais Câmeras, Mais Segurança?* Disponível em: https://igarape.org.br/videomonitoramento-webreport. Acesso em 02 de novembro de 2020.

Instituto Igarapé, Data Privacy BR Research. (junho de 2020). Disponível em: https://igarape.org.br/: https://igarape.org.br/infografico-reconhecimento-facial-no-brasil/Acesso em: 02 de novembro de 2020.

IPEA. (2020). Disponível em: www.ipea.gov.br: https://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=36488&Itemid=432. Acesso em 02 de novembro de 2020.

Istoé Independente. (15 de abril de 2004). Disponível em: *https://istoe.com.br/10629_PEQUIM+OU+BEIJING+/#:~:text=Como%20%C3%A9%20que%20%C3%A9%3F,Beijing%20s%C3%A3o%20a%20mesma%20coisa%3F&text=No%20caso%20da%20China%2C%20Pequim,chinesa%20para%20o%20alfabeto%20romano.* Fonte: https://istoe.com.br/. Acesso em 05 de novembro de 2020.

LYON, Z. B. (2013). *Vigilância Líquida.* Rio de Janeiro: Zahar.

MAGRANI, E. (2018). *A Internet das Coisas.* Rio de Janeiro: FGV.

MANGOTE, A. L. (11 de 08 de 2020). Disponível em: https://feed.itsrio.org/: https://feed.itsrio.org/caminhos-para-a-prote%C3%A7%C3%A3o-de-dados-pessoais-na-seguran%C3%A7a-p%C3%BAblica-e-investiga%C3%A7%C3%A3o-criminal-li%C3%A7%C3%B5es-do-595027052636. Acesso em: 10 de outubro de 2020.

MONTESQUIEU. (2010). *O Espírito das Leis.* São Paulo: Martin Claret.

Olhar Digital. (01 de agosto de 2019). Disponível em: https://olhardigital.com.br/: https://olhardigital.com.br/2019/08/01/noticias/manifestantes-usam-laser-contra-cameras-de-reconhecimento-facial/. Acesso em: 05 de novembro de 2020.

Piscatella, J. (Diretor). (2017). *Joshua: Adolescente Vs Superpotência* [Filme Cinematográfico].

Poder 360. (novembro de 2020). Disponível em: https://www.poder360.com.br/: https://static.poder360.com.br/2020/11/DADOS-Anteprojeto-comissao-protecao-dados-seguranca-persecucao-FINAL.pdf. Acesso em 05 de dezembro de 2020.

PRESIDÊNCIA DA REPÚBLICA. (14 de Agosto de 2018). Disponível em: https://www.gov.br/planalto/pt-br: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 16 de setembro de 2020.

RIZZOTO, A. (08 de junho de 2020). Disponível em: www.conjur.com.br: https://www.conjur.com.br/2020-jun-08/adriana-rizzotto-protecao-dados-pessoais-persecucao-penal. Acesso em 05 de dezembro de 2020.

STJ. (05 de novembro de 2020). Disponível em: https://www.stj.jus.br/sites/portalp/Inicio: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Comissao-entrega-a-Camara-anteprojeto-sobre-tratamento-de-dados-pessoais-na-area-criminal.aspx. Acesso em 10 de novembro de 2020.

TADEU, T. (2000). *O Panóptico - JEREMY BENTHAM.* Belo Horizonte: Autêntica.

TEIXEIRA, T., & ARMELIN, R. M. (2019). *Lei Geral de Proteção de Dados Pesoais - Comentada Artigo por Artigo.* Salvador: JusPodium.

TOMAZ, T. (2000). *O Panóptico - Jeremy Bentham.* Belo Horizonte: Autêntica.

UOL - tilt. (25 de junho de 2020). Disponível em: https://www.uol.com.br/tilt: https://www.uol.com.br/tilt/noticias/redacao/2020/06/25/homem-e-preso-apos-erro-de-tecnologia-de-reconhecimento-facial-nos-eua.htm. Acesso em 05 de dezembro de 2020.

UOL. (05 de julho de 2019). Disponível em: https://noticias.uol.com.br/: https://noticias.uol.com.br/ultimas-noticias/bbc/2019/07/05/as-5-principais-diferencas-da-vida-em-hong-kong-e-na-china.htm. Acesso em 05 de outubro de 2020.

WONG, J. (2020). *Democracia Ameaçada.* São Paulo: Faro Editorial.

www.ambitojuridico.com.br. (01 de junho de 2010). Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/movimento-da-lei-e-ordem-sua-relacao-com-a-lei-dos-crimes-hediondos/#:~:text=%E2%80%9CUm%20dos%20princ%C3%ADpios%20do%20%E2%80%9C Movimento,e%20severidade%20da%20lei%20penal. Acesso em 05 de novembro de 2020.

ZAFFARONI, E. R. (2007). *O Inimigo no Direito Penal.* Rio de Janeiro: Revan.

ZUBOFF, S. (2018). Big Other: Capitalismo de Vigilância e Perspectivas para uma Civilização de Informação. Em B. C. FERNANDA Bruno, *Tecnopolíticas da Vigilância* (p. 411). São Paulo: Boitempo.