UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

MARIANA RAMOS CARLOS DE CAMPOS REIS

O USO DE RECONHECIMENTO FACIAL PARA FINS DE VIGILÂNCIA PÚBLICA: ANÁLISE DO CASO BRITÂNICO À LUZ DA CRIMINOLOGIA CRÍTICA

BRASÍLIA

2022

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE DIREITO

MARIANA RAMOS CARLOS DE CAMPOS REIS

O USO DE RECONHECIMENTO FACIAL PARA FINS DE VIGILÂNCIA PÚBLICA: ANÁLISE DO CASO BRITÂNICO À LUZ DA CRIMINOLOGIA CRÍTICA

Trabalho de conclusão de curso de graduação apresentado à Faculdade de Direito da Universidade de Brasília, como requisito parcial para a obtenção do grau de Bacharel em Direito.

Orientadora: Professora Doutora Cristina Maria Zackseski

BRASÍLIA

2022

MARIANA RAMOS CARLOS DE CAMPOS REIS

O USO DE RECONHECIMENTO FACIAL PARA FINS DE VIGILÂNCIA PÚBLICA: ANÁLISE DO CASO BRITÂNICO À LUZ DA CRIMINOLOGIA CRÍTICA

Monografia apresentada à Banca Examinadora da Faculdade de Direito da Universidade de Brasília, campus Darcy Ribeiro, como requisito parcial para a obtenção do grau de Bacharel em Direito.

Data da defesa: 05/05/2022.

Resultado: Aprovado.

BANCA EXAMINADORA

_____

Professora Doutora Cristina Maria Zackseski

Orientadora

_____

Professor Mestre Welliton Caixeta Maciel

Examinador

_____

Professor Mestre Vinícius de Souza Assumpção

Examinador

BRASÍLIA

2022

AGRADECIMENTOS

A meus avós, Ana Maria e Daladier Carlos, que me ensinaram desde cedo o valor dos estudos e do trabalho. Vocês são os meus principais pilares de amor e cuidado e, juntos, por meio de livros, poesias e incessantes reflexões, me mostraram que a educação é o principal veículo de transformação de vidas, e, com ela, eu poderia ir mais longe. Obrigada por me ensinarem a ser uma mulher ambiciosa e a não medir esforços pelos meus objetivos.

À minha família, em especial a meus pais Bianca, Saulo e Marcello, irmãos Bernardo e Matheus e cunhada Alessandra, por fornecerem um canal de compreensão e amor mesmo nos tempos difíceis e por me proporcionarem mais alegria. Obrigada por constituírem a minha base.

A meu companheiro de vida, Mathews, por ter aceitado viver esse desafio comigo até aqui. Não tenho palavras para descrever o quanto o seu apoio incondicional foi fundamental para mim, especialmente com o cenário de incertezas e ansiedades que a pandemia trouxe. Você foi parte fundamental disso. Obrigada por ter me amparado, compreendido minhas dores e ausências e ter permanecido ao meu lado a todo momento.

Aos amigos que a UnB me trouxe: Brennda, Jullia, Natália, Rafaela, Carol e André. Obrigada por terem feito a minha graduação mais leve, pelas conversas, reflexões, grupos de trabalho compartilhados, e por terem compreendido a minha ausência.

À minha orientadora, Prof. Cristina Zackseski, por ter aceitado me orientar e por ter me auxiliado ao longo de todo o processo, com cuidadosos apontamentos e interessantíssimas conversas, que muito me ensinaram. Obrigada pela confiança e paciência depositadas em mim, e por ter expandido o meu olhar dentro do estudo da criminologia.

Por fim, à minha banca, que singelamente aceitou avaliar o presente trabalho, e a todo o corpo docente da Faculdade de Direito da UnB, pelos ensinamentos recebidos.

RESUMO

O presente trabalho buscou analisar a evolução do uso da tecnologia de reconhecimento facial no contexto da sociedade britânica para fins de segurança pública, utilizando, para esse objetivo, uma base teórica fundada na perspectiva da criminologia crítica. Como ponto de partida, busca-se desenvolver uma revisão bibliográfica dos autores Jeremy Bentham e Michel Foucault, a partir de suas análises críticas sobre o modelo panóptico, vigilância e controle social. Em seguida, busca-se elucidar o que é e como funciona a tecnologia de reconhecimento facial, bem como seu contexto histórico e principais desafios, como o problema da acurácia e dos vieses algorítmicos. Posteriormente, o estudo tem como fim analisar o contexto de desenvolvimento da vigilância no Reino Unido, os principais usos da tecnologia de reconhecimento facial e as principais bases legais utilizadas para fundamentar o uso dessa tecnologia pelas instituições policiais britânicas. Observa-se que o Reino Unido, apesar de possuir recomendações, guias de condutas e legislações utilizadas para justificar o uso da ferramenta de vigilância, não possui uma base legal clara e robusta que regule o uso de sistemas de reconhecimento facial por parte de suas forças policiais sem a ocorrência de possíveis violações aos direitos fundamentais dos cidadãos.

Palavras-chave: tecnologia; reconhecimento facial; panóptico; criminologia crítica; controle social; vigilância pública.

ABSTRACT

The present work aims to analyze the evolution of the use of facial recognition technology in the context of British society for public security, using, for this purpose, a theoretical basis founded on critical criminology perspective. As a starting point, we seek to develop a literature review by the authors Jeremy Bentham and Michel Foucault, based on their critical analysis of the panoptic model, surveillance and social control. Then, it seeks to elucidate what facial recognition technology is and how it works, as well as its historical context and main challenges, such as the problem of accuracy and algorithmic biases. Subsequently, the study aims to analyze the context of surveillance development in the United Kingdom, the main uses of facial recognition technology and the main legal bases used to support the use of this technology by British police institutions. It is observed that the United Kingdom, despite having recommendations, conduct guidelines and legislation used to justify the use of the surveillance tool, does not have a clear and robust legal basis that regulates the use of facial recognition systems by its police forces without the occurrence of possible violations of fundamental rights of the citizens.

Keywords: technology; facial recognition; panopticon; critical criminology; social control; public surveillance.

LISTA DE ABREVIATURAS E SIGLAS

ACLU	União Americana por Liberdades Civis
ANPD	Agência Nacional de Proteção de Dados
CFTV	Circuito Fechado de Televisão
EUA	Estados Unidos da América
GDPR	*General Data Protection Regulation*
G.R.E.A.T	*Gang, Reporting, Evaluation and Tracking System*
IA	Inteligência Artificial
IoT	Internet das coisas
IBM	*International Business Machines Corporation*
LAPIN	Laboratório de Políticas Públicas e Internet
LECN	*Law Enforcement Communication Network*
MIT	*Massachussets Institute of Technology*
MPS/ MET	Polícia Metropolitana de Londres
NIST	*National Institute of Standards and Technology*
ONU	Organização das Nações Unidas
RGPD	Regulamento Geral sobre a Proteção de Dados
SWP	Polícia de South Wales
TRF	Tecnologia de Reconhecimento Facial

INTRODUÇÃO

Os mecanismos de poder, atrelados à dispositivos de controle, tiveram um intenso crescimento ao longo das últimas décadas. Câmeras de vigilância se fazem presentes em todos os lugares, públicos ou privados, expondo o comportamento dos indivíduos ao escrutínio das instituições de poder e à decisão de quem entra, sai ou permanece. A decisão, que antes era manual, agora conta com o auxílio de sistemas de inteligência artificial que, mediante sua suposta áurea de neutralidade, retiram do detentor de poder o fardo do juízo.

Com a tecnologia de reconhecimento facial, no entanto, as câmeras ganharam o poder de enxergar além do comportamento manifestável e exposto, pois os diversos pontos que conectam os traços faciais do indivíduo passaram a revelar o seu dado mais valioso: a sua identidade. Com essa informação em mãos, tornou-se possível deliberar sobre questões mais complexas, que vão além da visão corpórea captada pelas câmeras, como a decisão sobre quem é inocente ou culpado.

A partir desse contexto, o presente trabalho tem como foco analisar como as ferramentas de vigilância pública, em especial a tecnologia de reconhecimento facial, reforça uma lógica de controle perpetrada pelas instituições de poder, partindo para isso, de uma perspectiva advinda da criminologia crítica. Nesse sentido, supõe-se que a prova da inocência de um indivíduo por meio da tecnologia de reconhecimento facial é travada a partir de um raciocínio seletivo e eficientista, dado que se atribui à tecnologia uma lógica messiânica, que ignora os meios e fatores sociais.

Nesse percurso, buscou-se empregar, como marco teórico inicial, o modelo panóptico de Jeremy Bentham do século XVIII e a posterior revisita de Michael Foucault ao termo no século XX, visando compreender de que forma as ferramentas de controle, em especial a tecnologia do reconhecimento facial, foram utilizadas para fins de controle disciplinar e se esse processo de transformação do panóptico ainda é observado nos dias atuais.

Posteriormente, após a compreensão do funcionamento da ferramenta e da análise de seus principais desafios, como a falta de acurácia e os vieses algoritmos, objetivou-se observar como o Reino Unido – uma das nações mais desenvolvidas economicamente e, ao mesmo tempo, uma das nações mais vigiadas do mundo – travou o uso de câmeras de vigilância e de sistemas de reconhecimento facial, em especial pelas forças policiais britânicas, como suposto método de segurança dos seus cidadãos, analisando, para isso, se os resultados foram positivos ou negativos, se trouxeram mais eficiência no combate à criminalidade, e, ainda, se as bases legais britânicas são

suficientes para justificar o uso na esfera da segurança pública e garantir a prevenção de violações aos direitos fundamentais dos cidadãos. Nesse sentido, a presente pesquisa justifica-se pela relevância do olhar da criminologia crítica para a compreensão dos métodos de vigilância na sociedade atual, especialmente no contexto britânico, pioneiro no uso da tecnologia de reconhecimento facial e primeiro país a levar o debate para as vias judiciais, através do caso Ed Bridges vs. Polícia de South Wales.

Para concluir tal análise, buscou-se elencar, de maneira cronológica, os principais casos práticos de utilização da tecnologia de reconhecimento facial no contexto da vigilância pública no Reino Unido e os principais estudos e pesquisas realizados com o uso de dados fornecidos pelas próprias instituições policiais, a partir de relatórios de acesso à informação solicitados por organizações de direitos civis.

O estudo, por sua vez, não é de todo modo conclusivo, abrindo margem para que o contexto de vigilância pública do Reino Unido continue a ser estudado, de modo a observar se a decisão judicial Ed Bridges v. Polícia de South Wales, que concluiu pela ilegalidade da ferramenta, resultou em mudanças nas bases legais e no desenvolvimento de políticas que observem o cumprimento das garantias legais.

1. VIGILÂNCIA NA ABORDAGEM CRIMINOLÓGICA

1.1. DO PANÓPTICO DE BENTHAM AO "PANOPTISMO" MODERNO: A EVOLUÇÃO DOS MECANISMOS DE VIGILÂNCIA E CONTROLE DISCIPLINAR

> O que você diria, se, pela gradual adoção e diversificada aplicação desse único princípio, você visse um novo estado de coisas difundir-se pela sociedade civilizada? Se você visse a moral reformada; a saúde preservada; a indústria revigorada; a instrução difundida; os encargos públicos aliviados; a economia assentada, como deve ser, sobre uma rocha; o nó górdio das Leis sobre os Pobres não cortado, mas desfeito – tudo por uma simples ideia de arquitetura? (BENTHAM, 2008, p. 84)

Com essa provocação, Jeremy Bentham concluía a última carta do compilado de ideias que revelou ao mundo seu audacioso projeto, *O Panóptico* (1791), que traduzia muito mais do que "uma simples ideia de arquitetura", ou uma minuciosa estruturação prática de um modelo idealizado de controle social e disciplinar.

O famoso modelo arquitetônico do século XVIII é representado por duas construções que se complementam: uma construção periférica, com estrutura em formato circular, é dividida em celas que atravessam toda a espessura da construção, com janelas que permitem que a luminosidade atravesse a cela de fora para dentro; por outro lado, há no centro uma construção em forma de torre, com amplas janelas que permitem enxergar a face interna do anel. Nesta, assenta-se um único indivíduo que cumpre o papel de vigia, enquanto naquela residem os prisioneiros em suas celas (BENTHAM, 2018). No entanto, apesar de chamar atenção pelo visual inovador para a época, a essência dessa inovação tecnológica não está em sua construção de geometria curvilínea, mas, em diferentes aspectos, no contraste entre luz e "escuridão". As sombras e lacunas, antes inacessíveis, que o Panóptico passa a revelar são tanto físicas quanto abstratas.

No decorrer da ascensão das monarquias europeias, o regime dos suplícios despontou como solução visceral para o que Foucault conveio chamar de "espetáculo punitivo" (1999, p. 12), quando os transgressores da ordem social vigente, que detinha forte justificação moral e política, eram punidos por meio da tortura e do derramamento de sangue em massacres públicos e coletivos. Tais rituais demonstravam a ligação entre o agir delituoso e a punição pouco indulgente como resultado, de forma que o criminoso servia de exemplo para que a população, controlada pelo medo, evitasse sair dos trilhos da tirania e, consequentemente, amargar o mesmo doloroso destino. Os

suplícios representavam, portanto, a mecânica do poder de punir do regime monárquico (FOUCAULT, 1999). Ausente um controle incessante sobre a locomoção de todos os corpos purgantes, renovava-se, a cada suplício, a manifestação e a ostentação do poder pelos que o detinham vigente.

O cenário começou a mudar a partir da segunda metade do século XVIII, quando o período de grandes transformações e desenvolvimento tecnológico da Revolução Industrial, germinada na Inglaterra, fez urgir o aumento da capacidade produtiva e a consolidação gradativa do capitalismo ao redor do mundo. A ascensão da sociedade burguesa também refletiu em novas demandas sociais, entre elas, a necessidade de uma população operária com vigor para preencher as exaustivas jornadas de trabalho atravancada à maquinofatura e aos aparatos de produção e a necessidade de não somente punir criminosos, mas também evitar que tais punições fossem imperativas. Vigiar, portanto, passa a ser mais produtivo e vantajoso do que punir. Atrelado a isso estavam os ideais trazidos pela Revolução Francesa no decênio final do século XVIII que, junto aos inúmeros projetos de reformas do século XIX, geraram uma nova jurisdição moral e política do direito de punir. Após uma era marcada pela concepção de penas primitivas e excruciantes, a tirania do poder, o excesso de brutalidade física e o "cruel prazer de punir" passaram por uma perspectiva de irracionalidade e intolerância do ponto de vista do fortalecimento de ideais iluministas. Dessa forma, a "punição generalizada" não deveria mais possuir espaço dentro de um imaginário racional de humanidade (FOUCAULT, 1999, p. 94).

Segundo Foucault, "a prisão, peça essencial no conjunto das punições, marca certamente um momento importante na história da justiça penal: seu acesso à 'humanidade'" (1999, p.260). No entanto, a crença na "humanização" dos métodos punitivos em face da evolução da consciência societária como "sociedade civilizada" não é, por si só, justificativa párea para tamanha mudança. A punição se afasta dos olhos do público, exclui-se majoritariamente o suplício, desaparece a encenação da dor e da violência, porém, o que verdadeiramente ocorre é um deslocamento do objeto ao qual se aplica a façanha punitiva. O corpo já não é mais o alvo preeminente da punição. Em seu lugar, o indivíduo tem condenado tudo aquilo considerado incorpóreo – sua alma, espírito

e liberdade – cessando gradativamente[1] o espetáculo sangrento do processo punitivo. Nas palavras de Foucault:

> Se não é mais ao corpo que se dirige a punição, em suas formas mais duras, sobre o que, então, se exerce? A resposta dos teóricos — daqueles que abriram, por volta de 1780, o período que ainda não se encerrou — é simples, quase evidente. Dir-se-ia inscrita na própria indagação. Pois não é mais o corpo, é a alma. À expiação que tripudia sobre o corpo deve suceder um castigo que atue, profundamente, sobre o coração, o intelecto, a vontade, as disposições. Mably formulou o princípio decisivo: "Que o castigo, se assim posso exprimir, fira mais a alma do que o corpo" (FOUCAULT 1999, p. 20).

Nesse contexto está inserido o modelo de prisão panóptica de Bentham (2008). Sua essência, afastada do castigo físico, paira primordialmente na ideia de que um vigia, no interior de uma torre central opaca, é contemplado com uma visão panorâmica e integral dos prisioneiros das celas que o cercam, ao passo que estes convivem entre a dúvida e a certeza de estarem sendo observados. Uma vez que os presos não conseguem enxergar o interior da torre, não há como afirmar se o vigia está ou não presente. O efeito de maior relevância do Panóptico se expressa no ato de impelir no ser disciplinado um estado de "consciente e permanente visibilidade", de forma a ratificar o funcionamento automático do poder (FOUCAULT, 1999, p.224).

A eficiência do sistema decorre, portanto, da garantia da ordem e de uma autorregulação das condutas, pois, ao não saber em que momento os olhos vigilantes pairam sobre si, gera-se a necessidade da manutenção contínua de um padrão de bom comportamento, disciplina e obediência: os ingredientes perfeitos para a receita dos "corpos dóceis"[2] foucaultianos. Sob o aspecto psicológico, transmite-se uma sensação imutável de vigilância, tornando o detento prisioneiro não somente de um espaço físico limitado, mas do atormento de seus próprios pensamentos, o que Bentham exprime como um "novo modo de garantir o poder da mente sobre a mente" (2008, p.17); do homem como vigia de si mesmo. O princípio da masmorra, caracterizado pelo trancamento e privação de luz já não cabe neste plano: a sombra que escondia os doentes e

[1] Conforme ilustrou Foucault: "O poder sobre o corpo, por outro lado, tampouco deixou de existir totalmente até meados do século XIX. Sem dúvida, a pena não mais se centralizava no suplício como técnica de sofrimento; tomou como objeto a perda de um bem ou de um direito. Porém castigos como trabalhos forçados ou prisão — privação pura e simples da liberdade — nunca funcionaram sem certos complementos punitivos referentes ao corpo: redução alimentar, privação sexual, expiação física, masmorra" (1999, p. 19).

[2] "É dócil um corpo que pode ser submetido, que pode ser utilizado, que pode ser transformado e aperfeiçoado". (...) "A disciplina fabrica assim corpos submissos e exercitados, corpos 'dóceis'. A disciplina aumenta as forças do corpo (em termos econômicos de utilidade) e diminui essas mesmas forças (em termos políticos de obediência)" (FOUCAULT, 1999, p. 162-165).

leprosos é substituída pela claridade e pelo olhar atento do vigia. “No edifício opaco e circular, é a luz que aprisiona” (MILLER, 2008, p. 90).

Apesar do conhecido modelo de estrutura concreta desenvolvido por Bentham no fim do século XVIII e posteriormente esmiuçado por Foucault no século XX, a existência de prédios e torres circulares que guardem proximidade ao arquétipo idealizado n’O Panóptico pouco importa no contexto analisado. Este é apenas o representante; o exemplar maior da utopia *benthamiana* de um poder disciplinar que não pode ser limitado por paredes físicas ou uma realidade ontológica, pois a consolidação do poder disciplinar e vigilante se encontra nas relações entre dominante e dominado, cuja ferramenta maior é a disciplina (FOUCAULT, 1999, p. 195).

Tal modelo surge como uma nova perspectiva de controle sobre os corpos. A vigilância generalizada, contínua e iluminada dos corpos detentos exime a necessidade da dor do castigo físico. Por consequência, tudo deverá ser assistido, catalogado e revertido em dados. Assim, o Panóptico pode ser definido como o “dispositivo polivalente da vigilância, a máquina óptica universal das concentrações humanas” (MILLER, 2008, p.89); ou, ainda, compreendido como “um modelo generalizável de funcionamento; uma maneira de definir as relações de poder com a vida cotidiana dos homens” (FOUCAULT, 1999, p.228), contanto que tais relações não se limitem à instituições físicas, na medida que não mais é necessário que um indivíduo esteja trancado em uma cela para ser alvo da vigilância do poder disciplinador.

Outra característica importante e definidora da configuração do dispositivo panóptico de poder está retratada no fato de pouco importar quem o exerce. O poder disciplinar não reside na figura de um soberano e seu direito dicotômico de ‘fazer morrer’ ou ‘deixar viver’ (FOUCAULT, 2005, p. 287), se não justamente na anonimização fragmentada, onipresente e onisciente da detenção do poder. Quanto mais substancial o número de observadores, a despeito de suas motivações heterogêneas, mais amplificado para o apenado da máquina óptica o risco de ser surpreendido e a inquietude de estar sendo observado (FOUCAULT, 1999, p. 225). Assim, as engrenagens do poder disciplinar são rotacionadas por suas próprias razões.

Ao longo de sua analítica do poder, Michel Foucault analisa três mecanismos de poder: os suplícios, as disciplinas e a biopolítica, tendo as duas últimas surgido em oposição ao mecanismo punitivo dos suplícios, formando os dois eixos do biopoder. Se à época de “Vigiar e Punir”, escrito

em 1975, Foucault ainda não havia tecido uma análise aprofundada sobre o nascimento da biopolítica (1979), hoje pode-se afirmar que a disciplina (o governo do corpo de cada indivíduo) e o biopoder (o governo da população) não se anulam, mas pelo contrário, se articulam e complementam[3]. Enquanto a disciplina age sobre o indivíduo ao fixar procedimentos de adestramento e de controle, padronizando o indivíduo e seus comportamentos, o biopoder age não sobre um único indivíduo, mas a um conjunto de pessoas. O que consente essa articulação do poder disciplinar e regulamentador é a norma, posto que ela "é o que pode tanto se aplicar a um corpo que se quer disciplinar quanto a uma população que se quer regulamentar" (FOUCAULT, 2005, p. 302).

Dada uma população homogênea e devidamente disciplinada pelos mecanismos disciplinares, a biopolítica visa responder como conduzir a vida desse agrupamento de indivíduos de forma a cuidar de suas necessidades como sociedade e, simultaneamente, satisfazer interesses políticos e econômicos e o *status quo* do poder. A partir da descoberta do indivíduo como um corpo adestrável, os mecanismos de gestão biológica e social da sociedade (saúde, educação, trabalho, produção, natalidade e longevidade), passam a se inserir nas estratégias políticas e na regulação societária, gerando a biopolítica (FOUCAULT, 2005, p.288-290). Assim, da governabilidade e da regulamentação geradas pelo poder sobre a vida resulta-se, por meio da ação ou omissão de políticas públicas, o poder de "fazer viver" ou "deixar morrer" (FOUCAULT, 2005, p.287).

Essa mudança da "anátomo-política do corpo humano" para o que Foucault (2005, p.289) chamaria de "biopolítica da espécie humana" é considerada uma nova tecnologia do poder que não exclui o poder disciplinar, mas o modifica, evoluindo-o, e o implementa a si próprio. Assim, as técnicas de racionalização que outrora existiam mediante os sistemas de controle, disciplina e vigilância no século XVIII se integram, na passagem para o século XIX, sob um ponto de vista mais político-econômico, que se instala e se dirige à multiplicidade dos homens, a massa global. Atualmente, é possível dizer que o homem disciplinado passa a ser visto também como o que Foucault intitula *homo oeconomicus*, pois toda a sua vida é regulada a partir de uma análise

[3] Com base na relação entre os diferentes mecanismos de poder, Castro (2014, p. 109) afirma: "não se trata de identificá-los com determinadas épocas históricas, como se houvesse uma época arcaica, a da soberania; outra moderna, a das disciplinas; e outra contemporânea, a da segurança e da biopolítica. Historicamente, não há uma sucessão desses diferentes dispositivos, mas uma simultaneidade. O que muda de uma época a outra é o modo em que essas diferentes formas de exercício do poder se relacionam entre si e, no contexto desse jogo, qual desses dispositivos cumpre a função dominante".

econômica: quantos filhos tem, os lugares que frequenta, quanto ganha, quantas horas labora, entre outros fatores marcados por uma sociedade neoliberal. Apesar de livre de suplícios, cárceres ou prisões panópticas, o homem econômico, acreditando possuir uma liberdade incondicional, aprisiona-se na construção de liberdade de uma governabilidade reguladora.

Não obstante, como esperado, alguns autores teceram críticas aos desdobramentos da racionalização e a 'precificação' da alma dos indivíduos por meio dos mecanismos de poder foucaultianos, principalmente aqueles cujo a máxima do panoptismo bem ilustrou. ADORNO e HORKHEIMER (1985), expoentes da Escola de Frankfurt, recriminaram o conceito de razão proveniente do Iluminismo, denominada "razão instrumental", sendo esta, segundo eles, utilizado como artifício de dominação travestida de instrumento de libertação. O uso da razão de modo instrumentalizado, para esses autores, é um meio para alcançar determinado fim – que é o interesse próprio – condicionado a uma lógica de mercado:

> O preço da dominação não é meramente a alienação dos homens com relação aos objetos dominados; com a coisificação do espírito, as próprias relações dos homens foram enfeitiçadas, inclusive as relações de cada indivíduo consigo mesmo (…) O animismo havia dotado a coisa de uma alma, o industrialismo coisifica as almas. O aparelho econômico, antes mesmo do planejamento total, já provê espontaneamente as mercadorias dos valores que decidem sobre o comportamento dos homens. (…) As inúmeras agências da produção em massa e da cultura por ela criada servem para inculcar no indivíduo os comportamentos normalizados como os únicos naturais, decentes, racionais. (ADORNO; HORKHEIMER, 1985, p. 40).

Adverte-se que o panoptismo, ao passo que não deve ser categorizado como o único modelo de repressão do vasto sistema de controle social e disciplinar moderno, de igual maneira não deve ser descartado como se descrevesse um modelo de controle social europeu ultrapassado e improfícuo. Pelo contrário, o modelo de panóptico idealizado por Bentham e intensamente abordado por Foucault como uma metáfora da moderna redistribuição dos poderes de controle social é retomado por Zygmunt Bauman na obra *Globalização: as consequências humanas* (1998), livro que, ao preceder o famoso *Modernidade Líquida* (2000), já explorava as raízes e

consequências sociais do processo globalizador e da modificação das relações sociais, econômicas e políticas ocorridas no período pós-moderno[4].

Conforme explicita Bauman (1998, p. 3), a globalização é um processo irreversível e o destino irremediável do mundo, que afeta a todos na mesma medida e da mesma maneira. Estamos todos sendo "globalizados". Todavia, o fato de toda a sociedade ser simultaneamente afetada, não quer dizer, por conseguinte, que seus efeitos e suas consequências sejam sentidos de forma igualitária: esse é o núcleo central de sua natureza ambivalente. A globalização "tanto divide como une; divide enquanto une", integra e desintegra, insere e segrega, e as causas dessa divisão são as mesmas que promovem a uniformidade do mundo. Dessa maneira, Bauman diferencia os conceitos de *globalização* e *localização*: coloca-se, em movimento, um processo "localizador" de fixação no espaço que distingue as condições existenciais de populações inteiras, bem como os segmentos existentes em cada uma.

O fenômeno de anulação das distâncias espaciais/temporais produzida pela tecnologia, ao invés de promover uma condição humana mais homogênea, tende a polarizá-la. Enquanto parte da humanidade, mormente privilegiada, emancipa-se das restrições territoriais e desfruta uma "liberdade sem precedentes face aos obstáculos físicos e uma capacidade inaudita de se mover e agir a distância", a outra parte presencia a "impossibilidade de domesticar e se apropriar da localidade da qual tem pouca chance de se libertar para mudar-se para outro lugar" (BAUMAN, 1998, p. 19). Como um símbolo de poder, a mobilidade tornou-se o fator de estratificação mais cobiçado e poderoso dessa sociedade moderna, onde reafirma-se diariamente as novas hierarquias sociais, políticas, econômicas e culturais. (TREVISOL, 2000).

Essa libertação da "elite móvel" de limitações físicas, conceituada por Bauman como a elite da mobilidade, resulta em uma nova imponderabilidade do poder. No século XVIII, a mão de obra e a força de trabalho eram imprescindíveis para que a sociedade produzisse. Era preciso o controle operante e disciplinar de corpos para integrá-los ao ritmo monótono do trabalho fabril. A ascensão do modelo econômico capitalista propiciou o êxodo rural e o deslocamento dos trabalhadores rurais para os grandes centros urbanos, ocupando as regiões periféricas e subdesenvolvidas que

[4] Para Bauman, não há uma pós-modernidade no sentido de ruptura ou superação, mas sim uma continuação do período histórico moderno, no qual a solidez da época anterior é substituída, entre outras, pela volatilidade das relações, pelo individualismo, pela insegurança e pela exaltação do consumo.

"rodeavam" os detentores do poderio econômico em busca de melhores oportunidades e acesso à necessidades como saúde, saneamento e especialização da mão de obra. Com o desenvolvimento industrial e o avanço da tecnologia, no entanto, a necessidade de mão de obra foi perdendo seu caráter de essencialidade, de forma que o poder disciplinar não mais poderia se limitar às fábricas e às prisões como principal fonte de controle: a globalização e a ascensão de tecnologias no final do século XX, como celulares móveis, computadores de uso doméstico e a rede mundial de computadores (*internet*) transmuta o controle para a vida privada de cada indivíduo, de forma a mantê-lo *dentro dos eixos*, não ousando ir além do comportamento esperado ou das regiões onde não são bem-vindos: "o que para alguns é sinal de liberdade, para muitos outros é um destino indesejado e cruel" (BAUMAN, 1998).

Nesse contexto, pode-se dizer que os efeitos de um mundo considerado "líquido" também revertem na segurança pública e privada, cuja sensação é de insegurança e volatilidade. Segundo Bauman (2011), há dois valores indispensáveis para uma vida satisfatória e relativamente feliz: a segurança e a liberdade. Não é possível ter uma vida digna na ausência de um desses fatores, uma vez que "a segurança sem liberdade é escravidão, e liberdade sem segurança é um completo caos". O problema, no entanto, é que ninguém na história da humanidade encontrou a "fórmula de ouro" com o equilíbrio perfeito entre os dois cobiçados fatores, uma vez que a existência de parte de um torna compulsória a ausência de parte do outro. Cada vez que mais segurança é adquirida por um indivíduo, entrega-se, em contramão, também um pouco de sua liberdade, e vice-versa. Para uma de suas referências está o psicanalista Sigmund Freud, que em sua famosa obra *O Mal-Estar na Civilização* (1930) reflete como a civilização é pautada na ideia de uma troca, onde o indivíduo troca parte de seu bem-estar individual pelo bem da civilização. A partir dessa reflexão, Freud conclui que a angústia e o sofrimento psicológico dos indivíduos partem, no geral, dessa renúncia de valores essenciais, como a liberdade – a principal vítima do processo civilizatório – em prol do acréscimo na proteção e resguardo dos perigos externos. Em parte, toda essa conjuntura explica por que a segurança é um tema tão caro para a elite financeira (embora essa conta acabe sendo paga pelas classes menos favorecidas – onde não há uma escolha). Para as classes mais privilegiadas, o espaço possui pouca relevância: são livres para explorar e usufruir, sobretudo financeiramente, e, logo após, negligenciar e abandonar as consequências dessa exploração. No entanto, essa "*incorporeidade*" do poder é responsável pela estruturação cada vez mais estrita do território: no mundo físico, constroem suas casas, escritórios e consultórios em regiões muradas e supervigiadas,

cujo alto nível de controle é necessário para a proteção da interferência de vizinhos inoportunos e da comunidade local, tornando-se inacessíveis a aqueles confinados nos arredores físicos. Bauman consubstancia em suas palavras:

> Como diz Steven Flusty, os tradicionais espaços públicos são cada vez mais suplantados por espaços de produção privada (embora muitas vezes com subsídios públicos), de propriedade e administração privadas, para reunião pública, isto é, espaços de consumo... O acesso é facultado pela capacidade de pagar... Aí reina a exclusividade, garantindo os altos níveis de controle necessários para impedir que a irregularidade, a imprevisibilidade e a ineficiência interfiram com o fluxo ordenado do comércio. As elites escolheram o isolamento e pagam por ele prodigamente e de boa vontade. O resto da população se vê afastado e forçado a pagar o pesado preço cultural, psicológico e político do seu novo isolamento. Aqueles incapazes de fazer de sua vida separada uma questão de opção e de pagar os custos de sua segurança estão na ponta receptora do equivalente contemporâneo dos guetos do início dos tempos modernos; são pura e simplesmente postos para "fora da cerca" sem que se pergunte a sua opinião, têm o acesso barrado aos "comuns" de ontem, são presos, desviados e levam um choque curto e grosso quando perambulam às tontas fora dos seus limites, sem notar os sinais indicadores de "propriedade privada" ou sem perceber o significado de indicações não verbalizadas mas nem por isso menos decididas de "não ultrapasse"(BAUMAN, 1998, p. 21-22).

É sob essas dicotomias do poder de vigiar *versus* ser vigiado e da mobilidade *versus* isolamento que reside, para Bauman, a transmutação do conceito *limitado* de Panóptico para a natureza global do Sinóptico e da modernização do poder disciplinar no advir da sociedade contemporânea. Como anteriormente citado, no século XVIII a disciplinarização de corpos demonstrou-se de grande valia para atingir determinados interesses, principalmente em ambientes – que iam desde o chão de fábrica das crescentes indústrias até os exércitos de recrutamento em massa e campos de treinamento – em que o sentimento de se sentir constantemente vigiado impedia o desmantelamento da regulação da disciplina altamente producente, o que tornava o panóptico uma ideia factível e atraente. No entanto, na contemporaneidade, os desafios não são mais os mesmos, de forma que as estratégias panópticas ortodoxas não mais se mostrariam suficientes para conter e disciplinar uma sociedade pós-moderna, globalizada e hiperconectada.

Nesse sentido, antes de adentrar o conceito de sinóptico em si, Bauman (1998) analisa uma versão mais atualizada e *ciberespacial* do Panóptico: os bancos de dados eletrônicos. A cada uso, transação ou compra no cartão de crédito, ida a aeroportos ou outros locais hipervigiados, uso de aparelhos eletrônicos ou realização de quaisquer interações virtuais resultam no armazenamento de centenas de dados, utilizados para fins diversos, que, trazendo mais para a atualidade, vão da criação do perfil de risco do indivíduo com uma análise da confiabilidade para concessão de

créditos, empréstimos e vistos internacionais até casos mais extremos, como políticas antiterroristas governamentais e cálculo de proporcionalidade do risco de reincidência. Esse fenômeno de dados tão observado no presente, cunhado por Mark Poster como "superpanóptico" (apud. Bentham, 1998), pode ser considerado menos uma superação e mais uma modernização do conceito de Bentham. Sua principal diferença do panóptico padrão – observa – reside no fato de que os indivíduos vigiados, ao fornecerem seus principais ativos (dados) nas atividades propostas pela civilização moderna e romperem a sua privacidade, tornam-se, voluntariamente, ativos de sua própria vigilância. Com efeito, o panóptico é um instrumento de imobilização, ao passo que os bancos de dados são um veículo de mobilidade. No entanto, a mobilidade aqui descrita não significa liberdade ou inclusão: pelo contrário, os bancos de dados servem como instrumento de seleção, separação e exclusão, pois, como Bauman (1998, p. 49) explicita, "quanto mais informação sobre você contenha o banco de dados, mais livremente você poderá se movimentar", isto é, tal "liberdade" só é admitida caso você esteja apto a portar as credenciais necessárias, como um alto nível de "confiabilidade" e "credibilidade" confirmado pelos bancos de dados. Se a principal função do Panóptico era não permitir *escapar* da vigilância, a principal função do "superpanóptico" é delimitar o acesso, impedindo que indivíduos indesejados possam *entrar* – seja em locais físicos, virtuais ou simbólicos – como os espaços de poder.

Posto o conceito de superpanótico, Bauman introduz outra perspectiva de destino histórico para o modelo panóptico, pelo qual mais advoga: o Sinóptico. O termo, assinalado por Thomas Mathiesen (1997), é revisitado pelo autor polonês para ilustrar o que considera ser o modelo de vigilância e controle social em atual exercício, apontando os motivos para tal. Um dos principais fatores reside numa crítica ao modelo panóptico foucaultiano não ter dado atenção ao processo moderno de desenvolvimento de novas técnicas de poder, onde ao invés de poucos vigiarem muitos – tal como na prisão de edifício circular – muitos observam poucos. O segundo fator constitui no Panóptico possuir natureza *local*, mesmo quando sua aplicação era universal: seus efeitos consistiam na *imobilização* física, mental e territorial dos indivíduos vigiados. O Sinóptico, por sua vez, apresenta caráter *global*; a vigilância não está mais submetida a confinamentos territoriais, como nas escolas e prisões. O ato de vigiar está em todo lugar, auxiliada pelos aparelhos de comunicação em massa, pois "não importa mais se os alvos do Sinóptico, que agora deixaram de ser os vigiados e passaram a ser os vigilantes, se movam ou fiquem parados. Onde quer que estejam

e onde quer que vão, eles podem ligar-se – e se ligam – na rede extraterritorial que faz muitos vigiarem poucos" (BAUMAN, 1998, p. 50).

Em terceiro lugar, tal como observado no "superpanóptico" de Poster (apud. Bauman, 2008) é constatado por Bauman um caráter de voluntariedade na adesão ao Sinóptico. Isso porque diferentemente do Panóptico, cuja principal ferramenta consistia em forçar os indivíduos à posição passiva de possivelmente estarem sendo vigiados, o Sinóptico não utiliza a coerção, se não outra ferramenta igualmente poderosa: a sedução dos indivíduos à vigilância. Essa técnica de controle, portanto, revela um perfil paradoxal: ao passe que tanto o Poder Público quanto o Privado se beneficiam do acúmulo arbitrário de dados e informações dos indivíduos, esses indivíduos aceitam contribuir com a entrega dos seus direitos de imagem e informações em prol de sua inclusão, identificação e credibilidade, pois, ainda que não estejam totalmente conscientes dos fins que esses dados levarão ou suas possíveis consequências, estes já se tornaram, em maior ou menor proporção, imprescindíveis para a vida em sociedade. (ZIMMER, 2009). Bauman cita Germaine Greer, que cirurgicamente pontua: "na era da informação, a invisibilidade é equivalente à morte" (2008, p. 21).

Ante o exposto, apesar de reconhecer a evolução dos mecanismos de controle social e disciplinar em acordo com as mudanças da sociedade e suas maneiras de controlar, vigiar e punir, que foram dos suplícios da Idade Média à sociedade disciplinar e panóptica de Foucault, passando também pelo 'superpanóptico' de Poster; e apesar de advogar pela existência de um modelo Sinóptico de controle que teria surgido no final do século XX, onde a vigilância é menos coercitiva e mais voluntária e persuasiva, num distanciamento entre os "locais" – a maioria – e os "globais" – a minoria –, a teoria apresentada por Mathiesen e Bauman não mais consegue contemplar as nuances e complexidades do fluxo de informações da sociedade do século XXI, considerado multidirecional, multissemiotizado e multifacetado.

Em tese, a ideia principal do Sinóptico, ainda que relevante no estudo e na compreensão da evolução panóptica, apresenta um caráter unilateral e unidimensional, onde os meios de comunicação em massa, como as televisões, seriam responsáveis pela condução e acessibilidade da vigilância de muitos contra poucos, conscientes dos olhares que os vigiam. No entanto, a tese sinóptica falha ao não considerar – ou melhor – ao subestimar a força e a relevância do crescimento da *internet* e da *Word Wide Web* (rede mundial de computadores, em tradução livre), capaz de não

só potencializar as questões observadas no modelo sinóptico e a dicotomia entre segurança e liberdade, mas de levar a vigilância para uma nova dimensão. Bauman deixa claro, inclusive, sua convicção de que a "elogiadíssima 'interatividade'" (1998, p. 50-51) que se anunciava, à época, que a internet traria, era "um grande exagero", visto que a *internet* e a *Web* estariam acessíveis apenas uma a elite global, enquanto o demais, abandonados em frente à meios de comunicação unilaterais, como a rede de TV por satélite ou a cabo, jamais atingiriam "qualquer pretensão de simetria entre os dois lados da tela", sendo fadados à observação contínua. A crença de Bauman, no entanto, se revelaria com o tempo como uma meia-verdade: por um lado, a interatividade da Web revelou ser de uma força sem precedentes, capaz de mudar permanentemente as relações humanas, sociais, políticas e econômicas em todos os seus níveis e contextos, além de gerar e impulsionar uma indústria bilionária; por outro lado, não se pode fechar os olhos para a visível desigualdade econômica no acesso à essas ferramentas. Apesar de parecer, dentro da "bolha" dos países mais desenvolvidos, que "todo mundo" está na internet, foi somente em 2018 que o mundo ultrapassou a marca de mais de 50% da população conectada; no final de 2021, esse número aumentou para 63%, no entanto, esse acesso está desigualmente distribuído, visto que em países classificados pela ONU como desenvolvidos, o acesso à internet é de cerca de 90% da população, já nos países em desenvolvimento, essa taxa cai pra 57% da população, enquanto que nos países mais vulneráveis ou classificados como menos desenvolvidos, a média é de apenas 27% da população. Sendo assim, dos 37% da população (cerca de 2,9 bilhões de pessoas) que ainda estão fora da *internet*, 96% vivem em países em desenvolvimento[5], o que demonstra que a Web e as suas funcionalidades podem funcionar como ferramentas tanto de inclusão quanto de exclusão, afinal, a quem interessa *conectar* a população mais desenvolvida e *isolar* a população de menor desenvolvimento? A imobilização dos corpos não é mais física, tal como o panóptico padrão, mas virtualizada: estejam, consumam, observem e sejam observados somente até onde queremos.

Outro fenômeno responsável por conferir mais modernidade à teoria panóptica é a evolução da Web 1.0 para a Web 2.0, termo utilizado por O'Reilly (2005) para designar a segunda fase da rede mundial de computadores. Se o maior propósito do uso doméstico da Web 1.0, a primeira geração da Web, era a busca por informação, sendo a interação, ainda precária, resumida a e-mails e fóruns, a Web 2.0, por sua vez, foi responsável pela era do compartilhamento, das redes sociais

[5] International Communication Union - ITU/UN

e das comunidades virtuais, revolucionando a maneira como a Web era utilizada até então. A exemplo disso, é possível citar, preliminarmente, os flogs, o Facebook, o Twitter, o Youtube, o Skype, o Podcast, entre outros. Com apenas um clique, tornou-se possível traçar os gostos e os interesses de um indivíduo; onde vive; o que consome; sua rotina diária; suas amizades e conexões em comum; além da facilidade no acesso à criação de conteúdo online, como textos, imagens e vídeos, processo que não só possibilitou uma maior hiperconectividade, interatividade e ampliação global das práticas comunicativas no mundo digital, mas, por outro lado, também proporcionou o desenvolvimento de novas técnicas de controle (ou a repaginação de técnicas já conhecidas).

Nesse sentido, o compartilhamento estratosférico de dados e a capacidade quase ilimitada de interatividade dos usuários inaugurou um novo olhar sob o controle sinóptico defendido por Bauman: o indivíduo, agora conectado, não mais pode ser considerado mero observador passivo, onde o "privilégio" ou o "prejuízo" de ser observado, visto, vigiado é exclusivo de indivíduos notáveis, públicos ou globais: os poucos vigiados por muitos. Na atual era, onde qualquer indivíduo é capaz de produzir conteúdo e onde a circulação de informações não mais reside exclusivamente aos veículos oficiais de informação, insta considerar uma nova dinâmica de poder: o multissinóptico, onde muitos observam muitos.

O indivíduo torna-se elemento ativo e essencial na criação, divulgação e compartilhamento de dados, substituindo a passividade do sofá em frente às telas de televisão pela interatividade das redes de dados, trazendo também parte do que outrora foi observado na teoria 'superpanóptica': a necessidade de ser visto é uma escolha necessária para a convivência em sociedade, onde o não compartilhamento de seus dados individuais implica numa "morte virtual". Quem não é visto não só não é lembrado, como é barrado do acesso à bancos, serviços, consumo, crédito financeiro, planos de saúde, imóveis, viagens, entre outros. O compartilhamento de dados pessoais, inclusive biométricos, torna-se requisito para uma sobrevivência digna na sociedade contemporânea. O mais perigoso, no entanto, é observar que os indivíduos cujos dados antropológicos (gênero, idade, raça, classe social, bairro onde mora, escolaridade etc.) são etiquetados como mais "perigosos" ou "problemáticos", numa herança do positivismo criminológico e do determinismo atávico – observado no tópico a seguir –, podem ser barrados não somente de uma esfera física, cujo isolamento territorial já foi observado na teoria sinóptica, mas postos como alvos dos novos e dos repaginados mecanismos disciplinares.

Insta salientar, ainda, que a observada transferência das limitações físicas da vigilância do modelo panóptico tradicional para um universo multissinóptico e hiperconectado não gera – e nem tem a pretensão de gerar – a exclusão do controle exercido em espaços de disciplinaridade física total ou parcial, tal como prisões, quartéis, instituições educacionais, entre outros; pelo contrário, tal modelo de controle social, mesmo com a evolução da sociedade e suas maneiras de vigiar e punir, encontra-se ainda extremamente atual, havendo poucas mudanças na maneira de gerir o controle físico dos corpos disciplináveis. Assim, o panoptismo da presente modernidade não é responsável por uma possível superação dos métodos de controle tradicionais, substituindo-os completamente por métodos mais avançados, eis que, na verdade, trabalham de forma colaborativa e sincronizada com estes últimos, apresentando-lhes novas ferramentas para manter a perpetuação do controle. As inovações tecnológicas possuem destaque nesse sentido, visto que, por mais que em sua maioria não tenham sido criadas com propósitos maléficos, funcionam perfeitamente para a atualização e perpetuação dos objetivos citados. A impressão digital biométrica, as câmeras instaladas em pontos estratégicos públicos e privados com o uso de tecnologia de reconhecimento facial, a leitura de retina e de voz, entre outros; são inovações que possuem uma característica elementar em comum: a possibilidade de armazenamento em bancos de dados para finalidades que ultrapassam colossalmente o uso ético da ferramenta ou o pressuposto consentimento do indivíduo. Prevalece no panóptico moderno, com a manutenção do olhar vigilante, a mesma função e implicações observadas nos métodos panópticos antigos, mas agora, no entanto, opera de maneira mais sofisticada, e seus efeitos, ao menor sinal de transgressão, podem ser observados para muito além das torres circulares.

1.2. PERCURSO DO PENSAMENTO CRIMINOLÓGICO

Para compreender o problema do panoptismo moderno, representado e limitado, neste trabalho, pelo uso da tecnologia de reconhecimento facial como mecanismo tecnológico de controle social e disciplinar, é necessário retomar, o que Vera Malaguti Batista (2011) convencionou chamar de "genealogia da criminologia", amparada pelos fundamentos da criminologia crítica e pelas principais ideias que percorrem o percurso histórico do estudo criminológico pré-científico às Escolas criminológicas italianas, de forma a compreender como o

discurso criminológico evoluiu ao longo dos séculos e como culminou no enraizamento de uma percepção eficientista da criminalidade na sociedade.

Apesar de, formalmente, a criminologia ter se consolidado como ciência autônoma apenas no século XIX, não se pode dizer que tenha nascido no berço do iluminismo, mas, muito antes, no berço da Inquisição (BATISTA, 2011). Seus esboços remetem ao século XIII, quando a centralização do Estado e da Igreja Católica como monopólio de poder, as estruturas nascentes do Estado e o processo de acumulação de capital situaram a criminologia como uma resposta política ao carecimento de ordem (ZAFFARONI, 2017). Na questão político-religiosa, o combate à heresia, blasfêmia, bruxaria e qualquer comportamento considerado desviante pela Igreja Católica tornava-se o pressuposto perfeito para a "busca da verdade" por meio de técnicas inquisitórias de domínio, sendo as confissões, as penas públicas e a demonização de ritos e costumes pagãos formas de manutenção e reafirmação de seu poder punitivo, afinal, "se a criminologia corre o risco de ser 'saber e arte de despejar discursos perigosistas', conhecer o eixo dos medos é traçar o caminho das criminalizações e identificar os criminalizáveis" (BATISTA, 2011, p. 24).

Entre os séculos XIII e XVII, é possível contemplar as teorias mais primitivas do escopo pré-científico do estudo criminológico, num esforço de seus precursores de questionar e tentar compreender as origens do comportamento criminoso como objeto de análise. Em comum, tais teses possuíam o conhecimento pseudocientífico como principal embasamento, sobrevindo respostas inerentemente ligadas à etiologia do crime ou a crenças e superstições populares. Destaca-se, entre elas, três das chamadas 'ciências ocultas': a demonologia, a fisiognomia e a frenologia. Conforme Zaffaroni explicita: "O Martelo das Feiticeiras seria o primeiro livro de criminologia, os demonólogos seriam os primeiros teóricos e os exorcistas, os primeiros clínicos" (2000, apud. BATISTA, 2011, p.18).

Por meio da Demonologia, buscava-se comprovar a natureza do mal mediante a existência de demônios como entidades sobrenaturais opositoras ao bem divino. Mediante essa crença, os comportamentos considerados desviantes pela Igreja eram muitas vezes associados à possessão demoníaca, devendo ser controlados e expurgados pelos Tribunais de Inquisição, detentores da graça divina (ZAFFARONI, 2017). Hoje, sabe-se que muitos dos considerados "possuídos" no período inquisitório possuíam transtornos mentais tais como a esquizofrenia, vindo os sanatórios e hospitais psiquiátricos a se tornar uma sombria herança da Inquisição.

Por sua vez, a Fisiognomia baseava-se na interpretação de que a leitura de características do rosto e corpo do indivíduo poderia revelar traços profundos de sua personalidade, virtudes e inclinação para o mal, vindo a ser considerada um esboço da noção antropobiológica e do método indutivo ou experimental no estudo criminológico de Lombroso, na Escola Positiva do século XIX, convertendo o criminoso no objeto central do estudo criminológico. Mais tarde, essa noção antropobiológica foi reforçada pela Frenologia, cujos adeptos acreditavam que o comportamento delitivo, assim como doenças e outras aptidões mentais e psicológicas do indivíduo, poderiam ser explicados por meio do desdobramento da forma anatômica craniana e da localização física de cada função cerebral.

A correlação das faculdades mentais do ser-objeto investigado às elevações e depressões na superfície, no formato e nas dimensões do crânio foi o escopo principal dos estudos do médico austríaco Franz Joseph Gall (1758-1828), precursor da Frenologia, crença que determinou, à época, que determinados formatos cranianos eram mais voltados à perversidade humana em detrimento de outros, mais justos e íntegros, justificando a utilização dessa como "método científico" para resolução de dilemas cotidianos quanto à escolha de indivíduos na contratação para atividades laborais, na escolha de parceiros para contrair matrimônio e procriar até o julgamento de indivíduos como portadores de uma determinista inclinação criminosa. A máquina frenológica, um equipamento experimental onde um capacete de metal conectava sensores ao topo da cabeça e registrava, através de uma impressora, um diagnóstico impresso das funções mentais do indivíduo, exemplifica como a tecnologia, ainda que não comprometida com rígidos valores científicos, pode vir a servir erroneamente como método comprobatório de questões medicinais, sociológicas e até criminológicas por meio de uma falsa aura de transparência e respeitabilidade teórica (SABBATINI, 1997).

Avançando para a questão político-econômica, tem-se o já citado processo de acúmulo de capital como proveniente sobretudo do contexto mercantilista da Idade Moderna, consolidando o aumento da produção, das exportações e das relações comerciais mundo afora. Evidente, contudo, que o crescimento econômico dos principais países da Europa ocidental não teria sido possível sem o amparo da exploração colonial, que, com o auxílio da manufatura (e posteriormente da maquinofatura trazida pela Revolução Industrial), fortaleceu a sociedade de classes por meio de

suas relações de dominação e subordinação do colonizado, tal como a geração de riqueza por meio da extração de contingentes de mão de obra.

No contexto de crise das monarquias absolutistas e do enfraquecimento da Igreja a partir da metade do século XVII, o fortalecimento dos conceitos filosóficos e políticos trazidos pelos principais filósofos da Era Moderna por meio de suas obras, como *Leviatã* (1651), de Thomas Hobbes, *Dois Tratados sobre o Governo Civil* (1689), de John Locke, e *Do Contrato Social* (1762), de Jean-Jacques Rousseau, contribuíram para uma série de mudanças sociopolíticas que, com a interferência do humanismo, do liberalismo e do contratualismo, influenciaram diretamente o estudo criminológico primordialmente pré-iluminista. Entre elas, destaca-se o desmantelamento dos governos absolutistas e das penas excruciantes, a evolução dos conceitos principiológicos da legalidade e da dignidade da pessoa humana e a individualização e proporcionalidade da pena.

Dessa maneira, o fim do século XVIII ficou reconhecido não somente pelo nascimento das prisões[6] como forma de humanização do método punitivo do Estado em alternativa às cruéis penas do regime absolutista, mas por uma série de mudanças originadas pela *iluminação* dos ideais sociopolíticos e econômicos da época. No século XVIII, os preceitos iluministas propunham não mais um grande poder absoluto representado pelo Clero e cercado de luxo exploratório, mas um Estado laico que melhor representasse os anseios do insatisfeito povo diante da fome, da miséria, dos atrozes métodos punitivos e pesadas cargas tributárias. A fusão dos ideais utilitaristas (tais como os defendidos por Jeremy Bentham, Rousseau etc.), com a influência dos princípios consagrados pelo iluminismo (como contemplados por Cesare Beccaria, Voltaire etc.) entre o final do século XVIII e a metade do século XIX favoreceram a construção do pilar doutrinário da Criminologia por meio da que, posteriormente, denominou-se Escola Clássica, a primeira escola do estudo criminológico moderno, apesar deste ainda não ostentar autonomia e rigor científico.

Considerada a "época dos pioneiros"[7], a Escola Clássica da criminologia foi essencial no processo de formação do preâmbulo do pensamento criminológico moderno menos por representar

[6] Termo utilizado por Foucault em seu livro "Vigiar e Punir: Nascimento da Prisão" (1975). Apesar do conceito de prisão como conhecemos hoje ter se desenvolvido a partir do Século XVIII, junto com os sistemas penais modernos, há diversos registros de Casas de Correção e instituições penais de encarceramento anteriores ao século XVIII, como as denominadas "*tuchthuis*" ou prisões de Amsterdã, como a *Rasphuis* (1596) e a *Spinhuis* (1597); e as *London House of Correction*, construídas entre o século XVI e XVIII na Inglaterra (ARTIACH, 2006; INNES, 1987).

[7] "Quando se fala da escola liberal clássica como um antecedente ou como a 'época dos pioneiros' da moderna criminologia, se faz referência a teorias sobre o crime, sobre o direito penal e sobre a pena, desenvolvidas em diversos

a unificação de uma linha de pensamento homogênea e mais por configurar um rompimento ideológico com as interpretações místicas, esotéricas e religiosas que fundamentavam o ato delituoso até então, consolidando-se como ferrenha instância crítica ao Antigo Regime e às práticas penais que o norteavam, como a tortura e a pena de morte, na defesa da proporcionalidade entre a pena e o dano social causado pelo delito.

Nesse sentido, Cesare Beccaria, com o desenvolvimento do tratado *Dos Delitos e das Penas*, de 1764, foi imprescindível para a consolidação e consagração não apenas da teoria criminológica clássica, na qual representou indiscutível égide, mas também da tradição italiana de cunho legalista da ciência penal, orientando o controle penal não somente como ferramenta de punição do criminoso, mas como delimitação do ius puniendi por parte do Estado. Dessa forma, Beccaria proclamou, pela primeira vez, a formação de limites legais entre a justiça divina e a justiça humana, entre o pecado e o crime, e entre a sanção e a pena capital com base em fundamentos legais.

A frente do período filosófico/teórico da corrente classicista, Beccaria (2003, pp. 19-20) desenvolveu o ideal de um sistema penal baseado não apenas nos princípios humanitários iluministas que pervadiam a sua época, mas também em princípios liberais, utilitaristas e contratualistas, ao defender que são as pequenas parcelas de liberdade que, unidas, constituem o fundamento do direito de punir (BECCARIA, 1983)[8], ao passe que o pacto social firmado entre os indivíduos e o Estado se encarrega da usurpação de interesses individuais em prol do estabelecimento da ordem social e da máxima felicidade do maior número. Para Beccaria, portanto, a justiça humana tem como base a máxima da utilidade comum (BARATTA, 2011, p. 29-34).

Por sua vez, inspirado por autores como Beccaria, do qual obteve notável influência, Carmignani e Mori, cuja cadeira sucedeu como professor de direito penal na Universidade de Pisa[9],

países europeus no século XVIII e princípios do século XIX, no âmbito da filosofia política liberal clássica. Faz-se referência, particularmente, à obra de Jeremy Bentham na Inglaterra, de Alsem von Feurbach na Alemanha, de Cesare Beccaria e da escola clássica de direito penal na Itália." (BARATTA, 2011, p. 32).

[8] "Assim sendo, somente a necessidade obriga os homens a ceder uma parcela de sua liberdade; disso advém que cada qual apenas concorda em pôr no depósito comum a menor porção possível dela, quer dizer, exatamente o necessário para empenhar os outros em mantê-lo na posse do restante" (BECCARIA, 1983, p.15).

[9] Segundo Francisco Laplaza (1950, p. 19-20), é muito difundida a ideia de que Carrara seria sucessor direto de Carmignani e que este teria sido seu professor, no entanto, ambas as informações são inexatas. Em 9 de novembro de 1859, Carrara foi designado professor de Direito Penal da Universidade de Pisa para suceder a Francesco Antonio Mori, que por sua vez sucedeu Carmignani em 1840. No entanto, o autor do Programa do Curso de Direito Penal não nega que Carmignani teria sido uma de suas grandes inspirações, tendo inclusive indicado que sua obra foi disposta

Francesco Carrara consagrou-se como o principal expoente do período jurídico/prático da teoria criminológica clássica. Com a publicação do *Programa do Curso de Direito Criminal*, entre os anos de 1859 e 1870, o mestre de Piza foi basilar no processo de sistematização da teoria do direito penal e da evolução do pensamento legalista italiano que sobrevinha o Antigo Regime desde o século XVIII, estabelecendo às leis penais caráter absoluto. Ao reconhecer o homem como um ser moralmente imputável e dotado de livre-arbítrio, Carrara designa a concepção de delito não como ente de fato, mas como ente jurídico, composto essencialmente por duas vertentes: a física (movimento corpóreo e dano provocado pelo crime) e a moral (vontade livre e consciente do infrator), cuja correspondência se assemelha aos elementos objetivos e subjetivos do tipo legal moderno.

Além disso, não basta que o ato considerado criminoso seja moralmente repreensivo ou perverso, devendo ser legalmente imputável e socialmente danoso. Com isso, Carrara foca seu objeto de estudo não na pessoa do criminoso, se não no crime como resultado do homem como detentor de conscientes liberdade, desejos e anseios e — por que não, possivelmente — idoneidade ou perversidade moral, sendo estes fatores necessários para a imputação de uma legítima e prevista responsabilidade penal, porém não deterministas quanto a sua evolução mental e psíquica. A citação a seguir sintetiza, por bem, os pensamentos de Carrara como profundo defensor da sistematização da lei penal, promulgada para proteger a segurança dos cidadãos, a partir de princípios e garantias penais, tendo a codificação penal italiana do século XIX inspirado reformas jurídicas no restante da Europa e do mundo. O grande feito de Carrara — e, pode-se dizer, de formal geral, da Escola Clássica — é, pois, "entender a ciência penal ao dispor da liberdade humana" (ZAFFARONI; PIERANGELI, 2021):

> Deve, pois, o direito ter existência e critérios anteriores às inclinações dos legisladores terrenos: critérios absolutos, constantes, e independentes dos seus caprichos e da utilidade avidamente anelada a eles. Assim, como primeiro postulado, a Ciência do Direito Criminal vem a ser reconhecida como ordem racional que emana da Lei mora-jurídica, e preexiste a todas as Leis humanas, tendo autoridade sobre os próprios legisladores. O direito é a liberdade. Bem entendida, a Ciência Penal é, pois, o código supremo da liberdade, que tem como escopo subtrair o homem à tirania e ajudá-lo a subtrair-se à sua própria, bem como a de suas paixões (CARRARA, 1956, p.11).

segundo a ordem lógica proposta por Carmignani, a quem retrata como mestre: "A mis alunos/ Al componer este livro – dispuesto según el orden eminentemente lógico que trazó Carmignani, nuestro gran maestro – no busqué gloria para mí, sino utilidad para vosotros; (...)". (Carrara, 2000).

Cerca de duas décadas após a publicação da principal obra de Carrara, no final do século XIX, urge um momento histórico de notável prestígio das ciências naturais. Esse entusiasmo científico é causado por uma série de mudanças no contexto político e social do pensamento europeu ocidental, entre elas, em síntese: (i) o otimismo econômico que pairava em face do progresso capitalista e dos benefícios trazidos pela industrialização; (ii) o apogeu da teoria positivista de Augusto Comte (1798-1857), corrente filosófica que concede idealmente às ciências experimentais (baseada em experiências e análise de dados) o título de padrão por excelência e natureza de conhecimento "real", acima de qualquer especulação; e (iii) aliado ao positivismo filosófico, outra importante mudança ocorre com a publicação da célebre obra "A Origem das Espécies", de Charles Darwin, um marco não só para a biologia evolutiva como para a expansão da divulgação científica, fomentando ainda mais o fascínio pela ciência e a sacralização dos métodos científicos.

É nesse contexto de inspiração fronte o positivismo filosófico e o intelectualismo científico que é inaugurada a Escola Positivista, marcada por intensas críticas aos teóricos antecessores do estudo criminal, que, ante a ausência de rigor científico e unificação teórica, convencionaram chamar — com conotação pejorativa — de "*clássicos*"[10], e, a si próprios, de "*críticos*". Entre as críticas realizadas à Escola Clássica, destaca-se a descrença na eficácia das concepções clássicas de crime, pena e responsabilidade penal com relação à diminuição da criminalidade e da manutenção da segurança pública ante a crescente taxa de criminalidade na Europa ocidental. Além disso, urgia por parte dos juristas e estudiosos sociais do crime um grande interesse na aplicação de métodos mais experimentais e indutivos no estudo criminológico, tanto no aspecto físico quanto psíquico, tendo em vista o crescente corpo de estudos médicos, clínicos e psiquiátricos que já lidavam direta ou indiretamente com aspectos do criminoso e da conduta criminosa[11], de forma a incentivar, nos estudos sociais e criminológico, uma busca pela mesma confiabilidade e certeza

[10] Conforme elucida BITENCOURT (2011, p.81): "Não houve uma Escola Clássica propriamente, entendida como um corpo de doutrina comum, relativamente ao direito de punir e aos problemas fundamentais apresentados pelo crime e pela sanção penal. Com efeito, a denominação Escola Clássica foi dada pelos positivistas, com conotação pejorativa. Na verdade, é praticamente impossível reunir os diversos juristas, representantes dessa corrente, que pudessem apresentar um conteúdo homogêneo.". ZAFFARONI e PIERANGELI (2021, p. 354) complementam ao dizer que: "Semelhante 'escola' seria mais condizente com um congresso pluripartidarista. Ocorre que para Ferri foi conveniente classificar sob um mesmo rótulo todos os penalistas que não compartilhavam de seus pontos de vista".

[11] Consoante Anitua (2008, p. 302), a Criminologia do século XIX possuía uma conexão mais relacionada à influência proveniente de médicos, psicólogos e frenólogos do que com a sociologia, como é possível observar na Criminologia contemporânea.

cometida aos postulados do método científico em voga, com o desígnio da eficaz proteção da ordem jurídico-social. Conforme se observa:

> Enfim, creio que essa vontade de verdade assim apoiada sobre um suporte e uma distribuição institucional tende a exercer sobre os outros discursos — estou sempre falando de nossa sociedade — uma espécie de pressão e como que um poder de coerção. […] penso ainda na maneira como um conjunto tão prescritivo quanto o sistema penal procurou seus suportes ou sua justificação, primeiro, é certo, em uma teoria do direito, depois, a partir do século XIX, em um saber sociológico, psicológico, médico, psiquiátrico: como se a própria palavra da lei não pudesse mais ser autorizada, em nossa sociedade, senão por um discurso de verdade (FOUCAULT, 1996, p. 18-19).

Em face dos aspectos citados, o positivismo jurídico põe fim ao período pré-científico do estudo criminológico cuja interpretação do crime partia majoritariamente de métodos dedutivos e metafísicos para inaugurar uma corrente que dá a ciência o papel maior de identificar, a partir do princípio da causalidade, como o determinismo se manifesta na realidade factual do crime. Nasce, enfim, a Criminologia como ciência empírica[12], tendo a Escola Positivista especial importância para a gênese do caráter científico do estudo criminológico. Conforme leciona BARATTA (2014, p.41-44), as diferenças da Escola Positivista para a Escola Clássica não residem tanto no conteúdo da ideologia da defesa social, de forma que o objetivo de ambas, em sua essência, pode ser considerado o mesmo: o estudo do fenômeno crime[13] para fins de promoção da defesa social[14]. Residem, na verdade, na disposição metodológica utilizada com o fim de explicar a criminalidade. Dentro dessa seara, a Escola Positivista italiana postula não mais o delito como ente jurídico, tal como visto em sua escola antecessora, mas na existência do delito natural, e seu objeto de estudo ganha uma nova ótica ao retirar o foco da responsabilidade moral e do livre-arbítrio do indivíduo na conduta criminosa e atribuí-lo às características biológicas e psicológicas do indivíduo reputadas

[12] Importante destacar a diferença de nascimento científico com nascimento ideológico, afinal, conforme se pontua: "A nosso ver, sua história ideológica é anterior, porque sempre houve exigências de sistemas de respostas justificantes por parte da política criminal, só que em outros tempos eram dirigidas à teologia e à filosofia e apenas mais recentemente foram formuladas à biologia, à psicologia ou à sociologia" (ZAFFARONI; PIERANGELI, 2021, p. 190).
[13] Nesse sentido, pode-se dizer que "os clássicos focaram seus olhares no fenômeno e encontraram o crime; positivistas fincaram suas reflexões nos autores desse fenômeno, encontrando o criminoso", sendo ambos, portanto, faces distintas de uma mesma moeda (SHECAIRA, 2011, P. 89-90).
[14] " Seja qual for a tese aceita, um fato é certo: tanto a Escola clássica quanto as escolas positivistas realizam um modelo de ciência penal integrada, ou seja, um modelo no qual ciência jurídica e concepção geral do homem e da sociedade estão estreitamente ligadas. Ainda que suas respectivas concepções do homem e da sociedade sejam profundamente diferentes, em ambos os casos nos encontramos, salvo exceções, em presença da afirmação de uma ideologia da defesa social, como nó teórico e político fundamental do sistema científico." (BARATTA, 2014, p. 41). No mesmo sentido: BATISTA, 2011, p.46.

como desviantes, fortalecendo a noção de periculosidade, insígnia de predisposição individual ao delito (BATISTA, 2011).

Nesse contexto, é concebido a Cesare Lombroso, pela literatura criminológica contemporânea, o título hegemônico de pai da antropologia criminal. Apesar de ter publicado diversos livros posteriormente[15], é em sua obra *O Homem Delinquente*, de 1876, que o criminólogo e médico italiano realiza um compêndio de seus estudos e teses mais relevantes, parte do que posteriormente ficou conhecido como teoria lombrosiana, tendo o ganho de notabilidade de sua teoria sido tanto amplamente reproduzida por uns quanto criticada por outros. Isso ocorre porque, por meio do estudo de indivíduos considerados delinquentes — cujo ofício psiquiátrico lhe concedeu amplo acesso — Lombroso buscou identificar e classificar as suas características fisionômicas, biológicas e estéticas, posteriormente reunindo e rotulando as características que julgou possuírem em comum, entre elas: o formato do crânio, deformidades ósseas, assimetria facial, mandíbula proeminente, tamanho dos membros, presença de tatuagens, além de pele, olhos e cabelos escuros. Já nas características psicológicas elencadas por Lombroso, destaca-se, entre outras, a preguiça, a vaidade, a falta de fetio ao trabalho (vadiagem), a ausência de sensibilidade tanto à dor física quanto à sensibilidade afetiva e o uso de gírias e jargões (LOMBROSO, 2010).

Concebe, portanto, por meio das semelhanças e divergências entre as categorias de delinquentes elencadas — ladrões, assassinos, estelionatários, pederastas, inconstantes mentais até os considerados 'ociosos e vagabundos'[16] — o perfil do criminoso nato[17]: indivíduo cuja aparência humana esconde sua essência selvagem e irracional. Os nascidos com essa essência seriam criminosos natos, por definição, mesmo que jamais tivessem delinquido. (LOMBROSO, 2010). Sendo assim, em razão de sua natureza atavista e pré-determinada, a aplicação de uma pena é simplesmente ineficaz: "é inerente à sua constituição orgânica e/ou psíquica a existência de

[15] Oficialmente, Lombroso teria escrito nove obras, tendo sido "O Homem Delinquente" sua segunda obra publicada, atrás apenas de "Gênio e Loucura", de 1874 (CESARE, 2010, p. 6).

[16] Lombroso (2010, p. 140-141) classifica, por exemplo, os estupradores, em geral, como indivíduos de "lábios grossos, cabelos abundantes e negros". Já os pederastas "de ombros descobertos e cabelos encaracolados, se ligam aos maus hábitos", se forem de classe alta, e "amam a vida de baixo nível e preferem odores fortes" os que provém de classe baixa.

[17] Ressalta-se que o criminoso nato não é a única categoria de indivíduos considerados inclinados à delinquência que Lombroso analisa em suas obras, sendo, no entanto, a categoria que mais desenvolveu e dissecou em seus estudos, sendo também a mais elementar para fins da presente pesquisa. A título de complementação, destaca-se a categorização dos criminosos ocasionais, habituais, passionais e os loucos, além de abordar, junto com Guglielmo Ferrero, a análise da mulher delinquente, que, por conta de seu perfil débil, infantil e de inteligência menos desenvolvida, ocupava um lugar de inferioridade na escala evolutiva até para cometer delitos (ANITUA, 2008, p.306-307).

potência criminosa que, cedo ou tarde, quer queira ou não, será transformada em ato, revelando sua natureza hostil, bestial, pré-civilizada, animalesca" (CARVALHO in LIMA; CASARA, 2010, p. 926). Além do delinquente nato, Lombroso distinguia e classificava outros grupos, como os 'dementes morais', e os 'selvagens'. Aqueles não expõem a habilidade ou a tenacidade do delinquente nato, tampouco teriam nascido maldosos ou imorais, mas, em uma determinada época da vida, adquirem semelhança ao criminoso nato. Já os selvagens, para Lombroso, são provenientes de tribos e reminiscentes de 'raças primitivas', sendo a antropofagia e a ausência de remorso fatores que os definem (LOMBROSO, 2010).

A solução para tais indivíduos, considerados incorrigíveis e incapazes de atingir a civilidade e o pleno exercício de suas faculdades mentais, portanto, seria o isolamento indeterminado[18]. Tal pensamento reforça o afastamento tanto da responsabilidade moral do indivíduo quanto de circunstâncias sociais com relação a origem positivista-etiológica do crime, visto que o indivíduo criminoso, por mais que fossem empregados esforços de reinserção social, melhoria econômica ou penas alternativas, seria incapaz de remover o estigma social ou dissipar a natureza transgressora em si presente. Justifica-se, por meio do uso de uma armadura de neutralidade científica, construída a partir do fomento do cientificismo positivista vigente no século XX e de um atavismo biológico e social, um certo preditivismo com relação ao destino dos indivíduos cujas características se destacam na teoria lombrosiana, tendo em vista a crença na possibilidade de identificação do criminoso nato antes mesmo que este pratique o crime.

Juntamente com Lombroso, os autores Enrico Ferri e Raffaele Garófalo, a despeito de outros criminólogos positivistas e suas divergências ideológicas[19], destacaram-se como a *trindade* do positivismo criminal italiano. Ferri, o principal representante e difusor da diretriz sociológica da Escola Positivista, foi responsável por influir na que viria a ser uma versão mais elaborada e

[18] Conforme expressa Lombroso no ensaio denominado *As mais recentes descobertas e aplicações da psiquiatria e antropologia criminal*: "Na realidade, para os delinquentes-natos adultos não há muitos remédios; é necessário isolá-los para sempre, nos casos incorrigíveis, e suprimi-los quando a incorrigibilidade os torna demasiado perigosos" (LOMBROSO, 2010, p. 8).

[19] Anitua destaca que "embora os três fossem conhecidos como as cabeças visíveis desse movimento, as diferenças entre eles – entre outras, ideológicas – eram muito significativas. "O "corpo" do positivismo seria o de um Lombroso mais idoso e bastante conservador. Ferri e Garófalo representariam as duas "asas" de um mesmo "pássaro", lastreado por sua suposta cientificidade e consubstanciação com os aparelhos de Estado. Ser bem que a esquerda mais revolucionária se tenha identificado com Ferri e a direito mais reacionária com Garófalo, o "lastro" comum seria o que os fizera derivar seu voo comum para posições claramente autoritárias quando o século XX chegou" (2008, p. 308).

acolhida[20] do positivismo criminal italiano ao estabelecer uma melhor estruturação e refinamento da teoria criminológica elaborada inicialmente por Lombroso. Um dos pontos de convergência de Ferri com a teoria lombrosiana está na ideia de livre-arbítrio como mera ficção e no reforço da utilização de métodos científicos como principal mecanismo de defesa do organismo social – a criminologia, para ele, seria o instrumento para "salvar as derivações metafísicas do direito penal por intermédio dos dados empíricos da biologia e da sociologia" (ANITUA, 2008, p. 310-312).

Por outro aspecto, uma de suas principais contribuições e pontos de divergência[21] com relação à teoria mais famosa do psiquiatra italiano está na estruturação do delito a partir de um trinômio causal, isto é, além do coeficiente antropológico (características físicas e psíquicas do indivíduo, além de sexo, raça, idade etc.) e do coeficiente físico ou telúrico (aspectos climáticos, ambiente, estações do ano etc.), seria imprescindível analisar também a incidência de fatores sociais (família, educação, segurança pública, moral, densidade populacional, cultura, crenças, etc.) que influenciam diretamente numa composição multifatorial do indivíduo criminoso e da etiologia delinquencial. Dessa forma, um dos principais feitos de Ferri foi elucidar uma teoria da gênese criminológica a partir da criminalidade como fenômeno social, de forma que, assim como outros fenômenos dessa espécie, acreditava ser possível antever a criminalidade em uma determinada sociedade e período concreto (meio socialmente determinável) caso pudesse quantificar a incidência de cada fator individual, físico e social conflitante – como um diagnóstico estatístico do problema criminal – articulando-se, então, estratégias preventivas para neutralizar a criminalidade.

Por sua vez, Raffaele Garófalo, o precursor do positivismo jurídico, representa a que talvez seja uma das ideias mais polêmicas do direito positivista, ao partir do conceito radical, inspirado no darwinismo social e numa busca pelo 'delito natural', que assim como a natureza elimina a espécie que não se adapta ao meio, também o Estado deve eliminar o indivíduo considerado

[20] Apesar da teoria determinista e antropológica criminal da Escola Positiva, comumente vinculada a lembrança de Lombroso, ter sido muito repercutida e discutida por críticos mundo afora, a diretriz sociológica de Ferri foi, em verdade, recebida com maior acolhida em alguns países, em especial os da América do Sul (GOMES, 2007, p. 99).

[21] Isso porque, apesar de Lombroso ter se tornado famoso principalmente por conta do simplismo de suas primeiras teorias como em "O Homem Delinquente", onde teria abordado apenas os fatores biológicos e psicológicos para explicar a causalidade criminal, o autor teria recebido duras críticas ao seu monocausalismo, tendo, no final de seus dias, ampliado sua teoria em obra póstuma chamada *O delito, suas causas e seus remédios* (1911), a fatores físicos, ambientais e sociais que influenciam o problema criminal (ANITUA, 2008, p. 305-306; GOMES, 2007, p. 104).

delinquente, visto esse ser incapaz de se adaptar à sociedade e à convivência que seu meio exige (ZAFFARONI, 2021).

Um dos grandes problemas da teoria positivista que foi ignorado por Lombroso e seus sucessores, no entanto, reside no fato de que a análise psiquiátrica e criminológica dos indivíduos que estudou trata-se de um panorama estatístico não do indivíduo criminoso, mas, na verdade, de indivíduos inseridos e criminalizados dentro de um sistema penal formal, cujos dados oficiais de criminalidade não levam em consideração a cifra oculta existente dentro de qualquer sistema criminal. Pune-se mais, portanto, não quem comete mais crimes, dado que muitos não chegam ao conhecimento das instituições de justiça, mas quem é mais criminalizado pelas máquinas de poder.

Nesse sentido, a antropologia lombrosiana pressupunha uma hierarquia moral na evolução da vida terrestre, com os seres animais e os fenótipos humanos não-europeus nos degraus inferiores de uma escada evolutiva no qual o homem europeu ocupava o topo. Os “estigmas lombrosianos”, de modo pouco surpreendente, confundiam-se com as características fisionômicas comuns nas raças consideradas “selvagens” e “inferiores” e até mesmo de animais não-humanos.

Nessa esteira de ideias incongruentes, insta concluir que, dentro de uma perspectiva crítica, não há um criminoso nato, tampouco delitos considerados naturais: o que existe são indivíduos criminalizados pela máquina de seletividade penal. Dentro desse contexto é que se insere uma concepção de etiquetamento social, isto é, a teoria criminológica marcada pela ideia de que não há uma noção de crime ou de delinquente natural: estas são construídas socialmente, a partir de definições legais e jurídicas desenvolvidas por meio das instâncias oficiais de controle social com relação aos indivíduos e ao comportamento considerado criminoso.

Por fim, a criminologia crítica reconhece a existência de um processo político, isto é, o reconhecimento de que a existência do crime depende de um processo de interpretação de ações e comportamentos e a atribuição de um significado - político, arbitrário e subjetivo. Assim, diferentemente dos conceitos trazidos pelo positivismo criminológico, a criminologia crítica reconhece a existência de componentes ideológicos e tendenciosos na definição do crime e do criminoso que precisam ser considerados para uma compreensão efetiva do fato-social crime (BARATTA, 2014).

2. A TECNOLOGIA DE RECONHECIMENTO FACIAL: SURGIMENTO, EMPREGO E PRINCIPAIS DESAFIOS

2.1. INTRODUÇÃO HISTÓRICA DA TECNOLOGIA DO RECONHECIMENTO FACIAL

O desenvolvimento da sociedade sempre esteve atrelado a uma capacidade ímpar da espécie humana: a de imaginar. Júlio Verne[22], na literatura, e George Méliès[23], no cinema, já imaginavam a ida do homem à lua muito antes do primeiro indivíduo pousar no satélite natural. Na medida que novas tecnologias surgem, o cérebro humano é capaz de imaginar infinitas possibilidades – positivas ou não - do impacto que elas trarão para as nossas vidas. A ideia de ciborgues, carros autônomos e robôs inteligentes foi exaustivamente utilizada em obras da ficção científica, alimentando o desejo do desenvolvimento da tecnologia com o fim de solucionar e facilitar problemas naturalmente humanos, como a cura de doenças, o adiamento da morte e a transformação da condição humana por meio da simbiose entre o cérebro humano e as máquinas, como defende a corrente transhumanista.

Tal como as máquinas a vapor foram para a primeira revolução industrial, a inteligência artificial é perpetuada como uma das protagonistas da chamada Quarta Revolução Industrial, podendo ser considerada uma tecnologia disruptiva e exponencial.

O conceito de disrupção foi criado em 1995 para definir as tecnologias capazes de romper o antigo *modus operandi* e revolucionar, de maneira significativa, soluções anteriormente empregadas a determinado desafio global, gerando um novo mercado, tais como a inteligência artificial, a internet das coisas (IoT) e a realidade virtual e aumentada (BOWER; CHRISTENSEN, 1995).

Por sua vez, o que define uma tecnologia exponencial é que, ao contrário de uma evolução tecnológica predominantemente linear, sua evolução se desenvolve geometricamente, multiplicando-se em uma curva exponencial (DIAMANDIS; KOTLER, 2012), como pode ser observado nos crescentes desafios trazidos pelo aprendizado de máquina. Segundo Ray Kurzweil, "na década de 1960, quando Arthur C. Clarke concebeu HAL[24], tratava-se de ficção científica.

[22] O autor escreveu "Da Terra à Lua - Viagem Direta em 97 Horas e 20 Minutos", romance de 1865.
[23] Le voyage dans la Lune, 1902, curta-metragem dirigido pelo cineasta.
[24] HAL, computador de bordo da espaçonave Discovery One, do filme 2001: Uma Odisseia no Espaço, dirigido por Stanley Kubrick e escrito por Stanley Kubrick e Arthur C. Clarke. A máquina foi considerada o auge da inteligência

Cinquenta anos atrás sabíamos bem pouco sobre IA. Hoje a história é outra. Muitos aspectos de Jarvis[25] já existem ou estão na prancheta". (apud DIAMANDIS; KOTLER, 2015).

Nesse contexto, o avanço da computação e a busca de modelos complexos que pudessem reproduzir ou até mesmo compreender racionalmente o funcionamento da mente humana possibilitaram o surgimento e o desenvolvimento da tecnologia da inteligência artificial em escalas ainda maiores do que poderia imaginar Alan Turing (1950) quando propôs seu famoso teste[26], tendo a denominação "*artificial intelligence*" (AI) sido cunhada seis anos depois, por John McCarthy (1956), que a definiu como a ciência e a engenharia de fazer máquinas com a capacidade de realizar funções que, se fossem realizadas pelo ser humano, seriam consideradas inteligentes (MCCARTHY, 2007).

No entanto, ainda conforme a visão do autor, a inteligência artificial não se trata usualmente de uma mera simulação da inteligência humana, afinal, uma máquina pode aprender a resolver problemas através da observação do comportamento humano, mas o estudo e o trabalho no desenvolvimento da inteligência artificial envolve majoritariamente a observação dos problemas que o mundo apresenta (MCCARTHY, 2007).

De modo geral, apesar de não haver uma única forma de conceituar a inteligência artificial, é possível dividir suas definições em duas dimensões: as que definem o sucesso da IA comparando o seu desempenho à fidelidade que possui com o desempenho humano, e as que a comparam a chamada racionalidade, que seria um conceito ideal de inteligência, "onde um sistema é racional se faz a coisa certa, dado o que ela sabe" (RUSSEL; NORVIG, 2013). Ainda, há divisões conceituais entre o "pensar" (raciocínio) e o "agir" (comportamento) da máquina.

---

artificial na ficção científica por quase 50 anos e foi retratada fisicamente como um grande olho vermelho nos painéis da famosa nave.

[25] Jarvis, acrônimo de "Just Another Rather Very Intelligent System", é um sistema de inteligência artificial fictício que ficou mundialmente famoso ao ser introduzido como o assistente pessoal de Tony Stark, o "Homem de Ferro", no filme homônimo de 2008. O sistema possui avançado processamento de linguagem natural e é capaz de coletar dados de bilhões de sensores, possibilitando sua ação por meio de qualquer sistema dispositivo robótico. (DIAMANDIS; KOTLER, 2018)

[26]. Observa-se que Turing não denomina sua pesquisa como 'Teste de Turing", mas "Jogo da Imitação"; no entanto, posteriormente a literatura reservou esta denominação para uma fase específica do teste. "Vamos fixar nossa atenção um computador digital em particular, vamos chamá-lo de C. É possível que, modificando o computador para que tenha uma capacidade de armazenamento adequado, aumento substancial de velocidade e dando a programação adequada, C possa realizar a parte A do jogo da imitação, se a parte B for feita por um humano?" (TURING, 1950, p. 442)

A partir do conceito de racionalidade, é possível dizer que uma tecnologia de inteligência artificial não é à "imagem e semelhança" do ser humano, como impera na cultura popular, mas é, na verdade, indivisivelmente atrelada a uma manifestação racional onde um agente-inteligente adota a melhor ação possível em uma determinada situação pré-estabelecida, portando, para isso, do auxílio de amplas pesquisas, investimento em estudos multidisciplinares e uma diversificada e robusta base de dados algorítmica.

Já no âmbito das ciências criminais, insta considerar que as ciências criminais tendem a ser, ao redor do mundo, uma ciência de lenta evolução, evidentemente porque as mudanças culturais também o são, desse modo, apenas transformações culturais já estabelecidas podem ser ratificadas pela lei, tendo em vista que o progresso científico sempre precederá as mudanças na seara legal. Sendo assim, se a regulação nas ciências criminais tende a surgir após as mudanças sociais e tecnológicas, a evolução digital ocorreu anteriormente a marcos jurídicos específicos e a pesquisas aprofundadas sobre os riscos que tais avanços podem acarretar para os direitos valorados em nossa sociedade, geralmente protegidos pelo direito penal. (QUATTROCOLO, 2019, p. 1519-1554).

Dessa forma, o avanço científico e tecnológico experienciado nas últimas décadas com o *'boom'* de tecnologias como, por exemplo, um poder computacional barato e sem precedentes, a inteligência artificial e a praticamente ilimitada disponibilidade e armazenamento de dados reflete uma virada cultural cada vez mais ágil, tendo as ciências criminais o dever de acompanhar e regular essas mudanças, tanto no contexto em que atos criminosos podem ocorrer, suas novas ferramentas e métodos probatórios, como na forma como as investigações criminais podem ser conduzidas (QUATTROCOLO, 2019, p. 1519-1554).

Um dos principais avanços tecnológicos que merecem um amplo e cauteloso olhar pelas ciências criminais é a tecnologia do reconhecimento facial. Apesar dessa tecnologia ter sido notada pela população em geral somente após a sua utilização massiva em grandes eventos e no surgimento de novas funcionalidades em aplicativos[27] e dispositivos móveis[28], a detecção

[27] https://forbes.com.br/colunas/2019/09/facebook-leva-reconhecimento-facial-a-todos-os-usuarios/

[28] Apesar do uso de reconhecimento facial para desbloquear dispositivos celulares ter sido popularizado pela Apple, em 2017, ao implementar a tecnologia no seu modelo Iphone X, em outubro de 2011 a Samsung já havia testado a implementação de reconhecimento facial em uma nova versão de seu sistema operacional como opção de desbloqueio de tela. No entanto, testes mostraram que a tecnologia podia ser enganada facilmente por fotos. https://exame.com/tecnologia/android-4-0-leva-reconhecimento-facial-ao-celular/

automatizada de rostos não é uma tecnologia recente. Nos anos sessenta, o cientista da computação Woodrow W. Bledsoe, em parceria com Helen Chan e Charles Bisson, realizava experimentos na tentativa ambiciosa de que computadores reconhecessem rostos humanos (BLEDSOE; CHAN, 1965; BLEDSOE, 1966a, 1966b;). Seu primeiro experimento se chamou "*man-machine facial recognition*", onde com o auxílio de uma máquina rudimentar, denominada RAND Tablet, Bledsoe registrava manualmente as coordenadas de características faciais como linha do cabelo, nariz e olhos, associando-as a dados numéricos. A partir de uma fotografia de um rosto desconhecido, a máquina baseava-se nos dados numéricos e na distância entre as características faciais para recuperar, num banco de dados, a imagem mais próxima da fotografia fornecida (LYDICK, 2007).

Apesar dos experimentos de Bledsoe terem sido severamente prejudicados pela tecnologia da época, que necessitava de trabalho manual para funcionar, suas pesquisas foram fundamentais por enxergar na máquina a viabilidade de uma característica até então considerada específica e hereditária, que é a capacidade de identificar rostos (WILMER et. al., 2010). Além disso, a necessidade de cálculos manuais por parte de um operador de sistemas não durou muito, pois em 1969 os pesquisadores Sakai, Nagao e Fujibayashi desenvolveram o primeiro computador apto a confirmar a existência ou não de um rosto em uma imagem sem a intervenção humana (GATES, 2004), o que hoje seria equivalente à tecnologia de "detecção de faces".

O sistema de reconhecimento facial calculado manualmente por Bledsoe também se tornou um pouco mais preciso na década de 1970, onde Harmon, Lesk e Goldstein realizaram pesquisas utilizando vinte e um marcadores em diferentes pontos do rosto, permitindo a identificação de uma maior variedade de características faciais até então não identificáveis, que incluíam desde a espessura dos lábios até o tom do cabelo do indivíduo.

Já no fim dos anos 80, os cientistas da computação Kirby e Sirovich desenvolveram um famoso método de reconhecimento facial denominado Eigenface (PCA), com a aplicação de álgebra linear para estabelecer características faciais básicas (TISTARELLI, 2009, apud. KIRBY; SIROVICH, 1990). Com a virada dos anos 90, Matthew Turk e Alex Pentland deram continuidade à abordagem criada por Kirby e Sirovich, levando aos primeiros casos de reconhecimento facial automático (KPCA). (TISTARELLI, 2009, apud. TURK; PENTLAND, 1991).

Fato é que entre a década de 1960 até a década de 1990, muitos pesquisadores além dos citados, como M. D. Kelly (1970), Takeo Kanade (1973), Belhumeur (1997) e Moghaddam (1998), auxiliaram no desenvolvimento de significantes melhorias à sistemas de reconhecimento facial, porém, embora empregassem esforços para tornar o processo de identificação e detecção de rostos cada vez mais fácil e automatizado, as máquinas ainda estavam longe de possuir o status de "inteligente" (GATES, 2004), como é discutido a partir do crescimento contínuo da inteligência artificial e do aprendizado de máquina.

2.2. RECONHECIMENTO FACIAL: O QUE É E COMO FUNCIONA?

Utilizada atualmente em bancos, aeroportos, lojas, sistemas de circuito interno de televisão e difundida por parte das contas digitais, redes sociais e aparelhos móveis, é possível dizer que grande parte da população mundial já teve o rosto detectado ou identificado por sistemas de reconhecimento facial pelo menos uma vez na vida, seja por câmeras públicas, privadas, ou fotos compartilhadas na internet. No entanto, após analisar o histórico, é necessário compreender por que etapas e procedimentos os sistemas de reconhecimento facial passam para tornar o rosto humano um dado biométrico calculável, sensível e potencialmente perigoso.

Segundo o grupo de trabalho instituído pelo artigo 29º da Diretiva 95/46 da Comissão Europeia, órgão consultivo europeu independente sobre proteção de dados e privacidade, o reconhecimento facial pode ser definido como "o processamento automático de imagens digitais que contêm rostos de indivíduos para efeitos de identificação, autenticação/verificação ou categorização desses indivíduos" (DATA PROTECTION WORKING PARTY, 2012).

Diferente da tecnologia de detecção facial, que detecta apenas a existência de um rosto em uma imagem ou vídeo, o reconhecimento facial é capaz de responder de quem é aquele rosto e diferenciar um rosto ao vivo de uma imagem digital. Além dos três processos principais citados, o parecer também define que o processo de reconhecimento facial é composto por uma série de subprocessos distintos, analisados a seguir.

Primeiramente, o processo de obtenção ou captação de imagem (*image acquisition*) se inicia ao captar o rosto de um indivíduo e convertê-lo ao formato digital, tornando-se uma imagem digital. Essa captação pode ser realizada por meio da digitalização de uma fotografia pré-existente ou com

a utilização de uma câmera eletro-óptica para adquirir uma imagem ou vídeo em tempo real. (WOODWARD JR et al, 2003). Em seguida, o sistema detecta a presença de um rosto na imagem *(face detection*), delimitando a zona onde o rosto aparece. Após detectado e delimitado, os rostos passam por um processo de normalização de recursos (*normalisation*), isto é, as variações na imagem são reduzidas, de forma a padronizar a escala, dimensão, resolução, brilho e distribuição de cores na imagem. A quarta etapa é a extração de características (f*eature extraction*) ou codificação. Nela, as características do rosto detectável como olhos, nariz e boca são isoladas e são produzidas distintas leituras da imagem digital de um indivíduo. Dessa forma, o conjunto de características essenciais de uma determinada pessoa pode ser armazenado para posterior comparação. (DATA PROTECTION WORKING PARTY, 2012)

Esses subprocessos de extração e armazenamento de características faciais de um indivíduo possibilitam o registro (*enrolment*) de seu rosto, caso seja a primeira vez em que ele é encontrado pelo sistema. Prontamente, o padrão único e específico de seu rosto é remetido a um dono, tal como o padrão biométrico único de cada digital. Por fim, ocorre o processo de comparação (*comparison*), onde são medidas as semelhanças entre um conjunto de características de um indivíduo a outros padrões previamente registrados em um banco de dados (DATA PROTECTION WORKING PARTY, 2012).

Do processo de comparação se resulta um sistema de pontuação (*score*) que busca no banco de dados atrelado ao sistema de reconhecimento facial utilizado o modelo que possui a pontuação mais semelhante àquele que se quer identificar, de forma a declarar uma correspondência (WOODWARD JR et al, 2003). É nessa etapa que muitos erros de identificação ocorrem, pois ao utilizar esse sistema de pontuação de probabilidade, em vez de retornar um único e melhor resultado, o algoritmo pode oferecer uma gama de potenciais correspondências, como num "cardápio" de prováveis identificações em ordem de maior probabilidade de correspondência entre os rostos.

Cabe ressaltar que nem todo sistema de reconhecimento facial é necessariamente igual. Diferentes sistemas podem conter algumas alterações com relação à maneira como as etapas e subetapas ocorrem. Como relatado por Woodward Jr. e outros (2003, p. 8), "diferentes fornecedores usam métodos diferentes para extrair as características de identificação de um rosto". Sendo assim, cada método possui suas particularidades e características, que podem ser patenteadas

ou amplamente disponibilizadas para desenvolvedores em bibliotecas de software gratuitas, como a OpenCV. Entre os métodos mais famosos de reconhecimento facial de código aberto utilizado por desenvolvedores e fornecedores estão a Análise de Componentes Principais (PCA), também conhecido por método E*igenface,* o método *Fisherfaces* e o método *Local Binary Pattern* (LBP) (OPENCV, 2016).

Além disso, no decorrer dessas etapas existem questões difíceis de serem superadas pela normalização de recursos e que moldam a eficiência dos sistemas de reconhecimento facial, como problemas na qualidade da imagem, iluminação, ângulo, idade do indivíduo e a oclusão de características faciais (como pelos faciais e o uso de acessórios), podendo comprometer seus resultados. Dessa forma, o uso de variados tipos de tecnologia (inteligência artificial e o aprendizado de máquina, redes neurais, modelagem 3D, criptografia de dados, luz infravermelha etc.) e a qualidade e robustez do banco de dados utilizado são atributos que podem diferenciar os sistemas de reconhecimento facial empregados e a qualidade dos seus resultados.

Para avaliar e classificar os resultados encontrados pelos sistemas de reconhecimento facial, uma importante forma de medição é a taxa de erros, isto é, além da taxa de resultados verdadeiros, que deve ser a mais alta possível, busca-se medir percentualmente o número de resultados falso positivos (também chamado de "taxa de aceitação falsa" ou FAR) e falsos negativos ("taxa de rejeição falsa" ou FRR) do sistema (LYNCH, 2018).

Tem-se um falso positivo quando o instrumento de reconhecimento facial faz a correspondência incorreta do rosto de um indivíduo com uma imagem em um banco de dados (LYNCH, 2018). Isso ocorre, por exemplo, quando Ana posta uma foto ao lado de seu amigo José em uma rede social e o aplicativo erroneamente identifica o rosto de José como sendo de João, sugerindo a marcação do perfil de João na foto. Infelizmente, os falsos positivos podem trazer problemas muito maiores do que uma marcação imprecisa, o que pode ocorrer se Marcos, ao assistir uma partida de futebol em um estádio, for erroneamente identificado pelo sistema de reconhecimento facial da polícia local como sendo Marcelo[29], um indivíduo procurado por ser supostamente membro de um grupo terrorista.

[29] Nomes fictícios, a título de exemplo.

Já no resultado falso negativo ocorre o procedimento inverso: o sistema não encontra resultados ou não consegue fazer a correspondência correta entre o rosto de um indivíduo e o seu perfil já existente em um banco de dados. É o que ocorre toda vez que um indivíduo tenta desbloquear o seu próprio aparelho celular com dispositivo de reconhecimento facial e o sistema não o reconhece, negando o desbloqueio do dispositivo. (LYNCH, 2018). Por outro lado, a falha do falso negativo também pode ser prejudicial em casos como a de uma pessoa sequestrada ou desaparecida há anos que deixa de ser identificada por um sistema de reconhecimento facial ligado a um banco de dados de pessoas desaparecidas devido à questões como mudanças faciais decorrentes dos efeitos da passagem do tempo.

2.3. A (NÃO) NEUTRALIDADE DA TECNOLOGIA DE RECONHECIMENTO FACIAL E SEUS PRINCIPAIS RISCOS

Ensinar um computador a ver "estímulos visuais complexos, multidimensionais e significativos" como o rosto humano não é uma tarefa simples (GATES, 2009, apud. TURK; PENTLAND, 1991, 71-86). Para isso, foi necessário o trabalho incessante de pesquisadores, cientistas da computação, engenheiros de software, matemáticos, analistas de sistema, entre outros profissionais ao longo de mais de cinco décadas para se chegar aos sistemas atuais: mais ágeis, automatizados e tecnológicos. No entanto, ainda é possível observar um longo caminho a respeito de outras matérias que foram pouco apreciadas no contexto científico computacional do desenvolvimento do reconhecimento facial, como questionamentos éticos, morais, sociológicos e criminológicos, principalmente no que concerne à sua aplicação na segurança pública.

De um modo geral, as inovações tecnológicas costumam ser recebidas com positividade e otimismo pelo público, pois seus objetivos costumam ser trazer melhorias à problemas sociais, ambientais, de saúde, segurança pública e outros aspectos de impacto global, além de muito auxiliar no cotidiano individual. No entanto, nem toda inovação tecnológica é inerentemente positiva, tampouco são carregadas de imparcialidade. Melvin Kranzberg, professor e historiador americano, assinalou a Primeira Lei da Tecnologia de Kranzberg ao declarar que "a tecnologia não é boa, nem má, e também não é neutra" (KRANZBERG, 1986, p. 544), ou seja, compreender a não neutralidade da tecnologia não significa cunhar uma visão pessimista à esta, mas compreender que

a aplicação de um determinado sistema algorítmico, a depender de quem e por qual razão é aplicado, pode resultar em impactos positivos ou negativos.

Em seu livro "(Des)inteligência Artificial", a pesquisadora Meredith Broussard cunhou a expressão Tecnochauvinismo (*technochauvinism*) como:

> Technochauvinism is often accompanied by fellow-traveler beliefs such as Ayn Randian meritocracy; technolibertarian political values; celebrating free speech to the extent of denying that online harassment is a problem; the notion that computers are more "objective" or "unbiased" because they distill questions and answers down to mathematical evaluation; and an unwavering faith that if the world just used more computers, and used them properly, social problems would disappear and we'd create a digitally enabled utopia. (BROUSSARD, 2018, p. 12)

Essa crença da tecnologia como uma utópica solução dos problemas inerentes à natureza humana e a noção de que algoritmos podem ser considerados neutros porque são programados a partir de estimativas matemáticas (como se, em face disso, fossem à prova de falhas humanas) ocultam um problema maior: o de que algoritmos, tal como os seres humanos, ou inerentemente em razão destes, também erram.

Em linguagem irreverente, Broussard (2018, p.22) brinca que, se não pensarmos muito a respeito, podemos talvez acreditar na ideia de que dados "surgem" no mundo totalmente formulados da cabeça de Zeus, isto é, sem interferência humana, o que aproximaria a tecnologia a uma concepção de singularidade tecnológica que, apesar de muito presente em ficções científicas futuristas, não possui compromisso com a realidade tangível atual.

Nesse sentido, a autora afronta a imprecisão linguística contida no termo '*machine learning*' ou, em português, aprendizado de máquina, pois leva muitos indivíduos a acreditar que os sistemas algorítmicos são de certa forma autoconscientes por realizarem a atividade de "aprender", tarefa geralmente realizada por seres dotados de sensibilidade e inteligência, tais como seres humanos e animais. Na verdade, o termo atribuído pela ciência da computação funciona mais como uma metáfora, no sentido de que esses sistemas podem realizar tarefas programadas e automatizadas a partir de bases de dados desenvolvidas por seres humanos, adquirindo constantes melhorias quanto a maneira de realizá-las (BROUSSARD, 2018, p. 87).

Tal ambiguidade linguística também remete ao termo *'mathwashing',* criado para denominar a tendência de profissionais da tecnologia e do jornalismo de utilizar conotações

objetivas de termos matemáticos para descrever ferramentas que possuem uma realidade mais subjetiva do que acreditam os seus usuários. Segundo Benenson (2018), desde os primórdios da computação essa tendência já ocorria com a inserção dos computadores nas empresas nas décadas de 1960 e 1970, na medida que todos esperavam que as máquinas lhes fornecessem respostas mais verdadeiras do que as fornecidas pelos humanos, mas eventualmente perceberam que os computadores eram apenas tão bons quanto seus programadores. Dessa forma, crer que a tecnologia, em virtude de sua capacidade de adquirir melhorias, é neutra ou que de certa forma é apenas resultado de pontuações e estimativas matemáticas minimiza a responsabilidade dos seres humanos que não somente desenvolvem tais tecnologias, mas principalmente àqueles que a utilizam com más intenções revestidas de precisão estatística.

Com foco na tecnologia do reconhecimento facial, o mecanismo matemático que está por trás de seu sistema pode incluir milhões de variáveis que são otimizadas no processo de treinamento do algoritmo. É essa complexidade que torna muito mais difícil para um ser humano examinar um algoritmo e compreender como ele funciona. Até mesmo seus designers e desenvolvedores não podem explicar com exatidão como a autoaprendizagem da máquina toma suas decisões finais (GARVIE, BEDOYA, FRANKLE, 2016), o que proporciona um fácil acesso ao esquivo de responsabilidades.

Sendo assim, é preciso considerar que apesar das diferentes maneiras de se desenvolver uma base algorítmica — seja ela utilizada para reconhecimento facial ou não — e da robustez tecnológica desenvolvida por meio de avanços na inteligência artificial e no aprendizado de máquina, os dados que constituem suas bases possuem uma coisa em comum: são constituídos socialmente (BROUSSARD, 2018), e, por isso, carregam questões sociais que nasceram bem antes da tecnologia como a conhecemos. É essencial, portanto, uma melhor compreensão de nossas condutas e interações com os algoritmos, em face da "aura de objetividade e infalibilidade" que a nossa cultura incorpora aos algoritmos (OSOBA; WELSER IV, 2017).

2.3.1. (IN)ACURÁCIA

Os sistemas de reconhecimento facial são fruto de mãos humanas e, portanto, refletem tanto nossas aspirações quanto nossas limitações. Um sistema forte, ainda que não infalível, é construído

a partir de bases de dados fortes, robustas e diversificadas, pois a performance e os resultados desses sistemas são fortemente ligados à qualidade do conjunto de dados utilizado, reduzindo erros. Uma base de dados limitada e um sistema de baixa apuração de erros podem resultar em vieses, imprecisões e equívocos desde as etapas de detecção e coleta de dados até o processo de atribuir um rosto detectado à identidade de uma pessoa em particular.

Como destacado anteriormente, a variação dos sistemas de reconhecimento facial em sua capacidade de identificar pessoas corretamente são identificadas por meio de taxas de erros que demonstram, além dos casos identificados acertadamente, o número de falsos positivos e falsos negativos encontrados, que devem ser relatados por esses sistemas visando uma melhor acurácia (LYNCH, 2018, p.6).

Conforme as diretrizes "*Ethics guidelines for trustworthy AI"*, produzido pelo grupo independente de peritos em IA criado pela Comissão Europeia, todas as técnicas de aprendizado de máquina possuem uma certa porcentagem de erros, ainda que pequena (AI HLEG, 2019, p.6). Como efeito, a acurácia (*accuracy*) é um conceito essencial, que no reconhecimento facial pode ser sintetizada na porcentagem de amostras corretas em detrimento de falsos positivos e negativos encontrados. Quanto menor for a taxa de acurácia de um determinado sistema de reconhecimento facial, mais riscos ele pode trazer.

Nota-se que a acurácia não é a única métrica existente para analisar os resultados de um modelo de aprendizado de máquina. Outras métricas, como as chamadas "curva ROC' e "recall", também são utilizados no campo de desenvolvimento de sistemas, no entanto, no campo de classificação de amostras de dados a acurácia é a métrica mais utilizada para avaliar a necessidade de investimento de mais recursos em soluções até a chegada do sistema ao mercado.

Nesse sentido, são vários os fatores responsáveis por influenciar a acurácia de um sistema de reconhecimento facial. Elementos como (a) a resolução e nitidez do retrato, o (b) plano de fundo, as (c) expressões faciais e o (d) ângulo em que a imagem foi capturada são determinantes para indicar a qualidade da imagem que passará pelo crivo do processo de identificação de rostos; além disso, as condições ambientais da captura da imagem, como a (e) iluminação do ambiente e a (f) posição e distância da câmera com relação ao "alvo", também são capazes de influenciar no número de falsos positivos e falsos negativos (HAMANN; SMITH, 2019).

Em 2018, um teste realizado com 127 algoritmos e 45 desenvolvedores constatou que quando as imagens utilizadas para comparação eram de alta qualidade, os algoritmos mais precisos falhavam em apenas 0,2% das vezes, um resultado vinte vezes melhor do que no mesmo teste realizado em 2014 (NIST, 2018, p.4). No entanto, há diferenças significativas entre ambientes controlados, muito utilizados em treinamentos de algoritmos, e ambientes não controlados. Quando uma fotografia é tirada sob um ambiente orientado em que há o controle do ângulo e da distância da câmera, da iluminação do local além do controle da expressão facial e do posicionamento físico frontal do indivíduo, como ocorre nas circunstâncias de uma foto posada e nas famosas 'mug shots[30]' (LYNCH, 2018, p.7), minimiza-se o número de variáveis, de forma que o software opere em condições quase ideais, impulsionando significativamente sua precisão.

No entanto, quando uma imagem é capturada em movimento, como ocorre na extração de imagem de filmagens em tempo real ou em condições de ambiente ou qualidade de imagem não ideais, o reconhecimento de faces pode ser extremamente desafiador. Dessa maneira, o desbloqueio de tela de um dispositivo móvel mediante o rosto de seu proprietário requer menos precisão algorítmica do que esse mesmo rosto ser corretamente identificado entre uma multidão de pessoas em movimento por meio de câmeras de vídeo de vigilância pública.

Nas palavras de Garvie, Bedoya e Frankle:

> Real-time, continuous video surveillance systems tend to combine the worst of these traits, rendering them less accurate than many other deployments. Unlike mug shot-based systems, which use photos captured in controlled settings according to strict standards, real-time systems must contend with people going about their daily lives. Subjects rarely face the camera straight on, and video stills are often poorly or unevenly lit. The security cameras themselves vary in quality and are often mounted on ceilings. They often capture only the tops of people's heads (GARVIE, BEDOYA, FRANKLE, 2016. p.26)

Somado a isso, o tamanho da lista de observação do banco de dados também desempenha importante papel na acurácia sistêmica. Estudos afirmam que sistemas de reconhecimento facial apresentam pior desempenho geral conforme o tamanho do conjunto de dados – isto é, a quantidade de rostos armazenados – aumenta. À medida que o tamanho de um banco de dados aumenta para uma escala nacional ou até mesmo internacional, um algoritmo inevitavelmente encontrará faces

[30] Consiste num registro fotográfico duplo, da perspectiva frontal e da perspectiva lateral, de uma pessoa do busto para cima, normalmente tirado depois que a pessoa é presa para fins de registro policial, possibilitando a identificação pelas vítimas, testemunhas e investigadores. O termo, em tradição livre, também pode ser utilizado para definir pequenas fotografias de rosto em geral.

congêneres (GARVIE, BEDOYA, FRANKLE, 2016). Em parte, isso ocorre porque muitas pessoas de uma determinada população ou etnia possuem características em comum, assemelhando-se umas com as outras (LYNCH, 2018, p.7). Banco de dados maiores também são mais prováveis de conter mais imagens antigas, o que também pode reduzir a acurácia (BEST-ROWDEN; JAIN, 2015).

Como seres biológicos, somos condicionados ao decurso do tempo e às mudanças fisiológicas e anatômicas trazidas por ele, que podem ser mais ou menos severas em cada indivíduo a depender de fatores genéticos. No entanto, o envelhecimento não é o único fator anatômico a modificar a aparência de um indivíduo e tornar as fotos armazenadas, consequentemente, datadas. Fatores como o estilo de vida que o indivíduo leva e o ambiente onde está inserido também possuem um significante impacto na aparência facial ao passar dos anos. Fumar, exposição prolongada ao sol, uso de entorpecentes e níveis elevados de estresse explicam mudanças visíveis no padrão de envelhecimento do rosto de gêmeos idênticos. O uso de metanfetamina, por exemplo, pode alterar drasticamente o perfil de um indivíduo em um curto espaço-temporal. Tais fatores, portanto, podem ser responsáveis por abalar a acurácia de um sistema de reconhecimento facial, que não leva em consideração as mudanças trazidas pelo tempo e espaço.

Os problemas ligados à opacidade dos algoritmos poderiam ser inofensivos se os algoritmos fossem "quase" infalíveis, no entanto, segundo Osoba (2018) a maioria dos algoritmos possui apenas garantias probabilísticas de precisão. E isso ocorre nos melhores cenários possíveis, nos quais os modelos e algoritmos certos são aplicados de forma adequada, com a melhor intenção de "aperfeiçoar" os dados. Os usuários e designers de algoritmos raramente têm o luxo de tais cenários perfeitos. Estes, portanto, devem se basear em suposições que podem falhar e levar a resultados inesperados (OSOBA, 2018).

Cientes dos problemas que uma identificação facial imprecisa pode proporcionar, alguns indivíduos - pesquisadores, ativistas, designers e artistas - de diversas partes do mundo têm arriscado a suposta imacularidade e a reputação desses sistemas ao desenvolver produtos com intuito comercial, artístico ou acadêmico que prometem enganar softwares de reconhecimento facial, atacando diretamente a acurácia de tais sistemas ao aumentar o índice de erros. Um dos projetos precursores desenvolvidos com essa finalidade ocorreu em 2010 pelo artista e tecnólogo Adam Harvey. Com uma junção de maquiagem e penteados de estética ousada inspirados na

camuflagem utilizada em navios de guerra britânicos para confundir ataques de submarinos germânicos na Primeira Guerra Mundial[31], Harvey descreve sua criação, denominada "Computer Vision Dazzle Camouflage" (ou apenas "CV Dazzle")[32] não como um produto, mas como um conceito ou estratégia cujo design foi projetado para expor as vulnerabilidades da tecnologia de detecção e reconhecimento facial existente. (HARVEY, 2010-2020).

Harvey explica que uma vez que os algoritmos de reconhecimento facial costumam depender da relação espacial das principais características do rosto, dos padrões faciais e dos contornos tonais, é possível bloquear a detecção criando uma espécie de "anti-face", que funciona a partir da quebra ou neutralização de padrões do rosto de forma a bloquear a detecção facial, ou, caso detectado o rosto, dificultar a identificação do indivíduo (HARVEY, 2010-2020). O artista também é responsável pela co-criação do protótipo Hyperface, em parceria com a Hyphen-Labs. Diferente do primeiro projeto, que visa gerar um falso negativo, o Hyperface foi desenvolvido de forma que sua famosa estampa, de propositalsemelhança com características que lembram um rosto humano, seja interpretada como se rostos de fato, gerando múltiplas detecções falsamente positivas no sistema de reconhecimento facial utilizado à época. Embora tecnicamente desatualizado para os sistemas de reconhecimento facial atuais, o projeto possuía um objetivo maior: "reduzir a pontuação de confiança da detecção e reconhecimento facial, fornecendo faces falsas que distraem os algoritmos de visão de computador" (HARVEY, 2017). Dessa forma, o projeto reconhece que a estampa não é capaz de tornar pessoas invisíveis aos olhos do algoritmo, mas, por sua vez, é capaz de apontar para as brechas da acurácia dos sistemas de LFR utilizados.

Há também outros exemplos de projetos que buscam testar a assertividade de sistemas de reconhecimento facial. Em 2016, um grupo de pesquisadores da universidade americana Carnegie Mellon idealizaram um modelo de óculos fabricado via impressão 3D cuja estampa, que lembra o casco de uma tartaruga, é suficiente para obscurecer cerca de 6,5% dos pixels e confundir determinados sistemas de reconhecimento facial, gerando falsas identificações[33] (SHARIF, et al., 2016, p.5). Por sua vez, o professor do Instituto Nacional de Informática do Japão - INII, Isao Echizen, conjuntamente com outros pesquisadores, elaboraram um visor equipado com onze lâmpadas LED de luz infravermelha localizadas nas áreas dos olhos e do nariz que são

[31] https://www.history.com/news/dazzle-camouflage-world-war-1
[32] https://cvdazzle.com/
[33] https://www.theguardian.com/technology/2016/nov/03/how-funky-tortoiseshell-glasses-can-beat-facial-recognition

aparentemente invisíveis a olho humano, mas brilhante aos olhos ”mecânicos”, isto é, o sistema de reconhecimento facial, ao absorver e refletir a luz, é cegado pelas luzes que escondem a visão de grande parte do rosto humano, fazendo com que o usuário do visor passe despercebido (NII Press Release, 2012; YAMADA, T. GOHSHI, S. ECHIZEN, I, 2013).

Atualmente, os sistemas de reconhecimento facial mais modernos contam com algoritmos cada vez mais precisos e inteligentes, com soluções baseadas em sensores infravermelhos (aptos a enxergar em baixa iluminação), redes neurais profundas e em modelos que escaneiam dados tridimensionais do rosto[34], tornando-se cada vez mais difícil passar ileso dos registros dos bancos de dados faciais mundo afora. No entanto, as manifestações políticas de Hong Kong, em 2019, nos quais manifestantes utilizaram lasers para impedir o reconhecimento de seus rostos pela inteligência artificial do distópico governo local revelam que a ascensão de tais projetos, cunhados pelo termo ‘antivigilância’, apesar de não possuírem o condão de se tornarem soluções definitivas às questões controversas da tecnologia do reconhecimento facial, são extremamente relevantes para demonstrar as brechas que a acurácia de tais sistemas possuem, além de se apresentarem como uma espécie de protesto e resistência à utilização vertinosa e indiscriminada dos sistemas de reconhecimento facial por governos autoritários para identificar e inibir manifestantes, pois tais dados dificilmente podem ser controlados por aqueles cujos rostos são coletados.

2.3.2. VIESES E DISCRIMINAÇÃO ALGORÍTMICA

Até aqui, buscou-se demonstrar que os sistemas de reconhecimento facial estão abertos a riscos, em especial a não neutralidade dos algoritmos e uma acurácia condicionada por fatores externos e de difícil controle, gerando resultados não confiáveis e que podem pôr em risco direitos fundamentais do ser humano, tais como o direito à privacidade e proteção de dados e a dignidade da pessoa humana. Somado a isso, a tecnologia enfrenta uma questão que gera uma notável sensação de desconfiança por organizações de direitos civis do mundo todo: os vieses e a discriminação algorítmica. Quando se parte da premissa ingênua de que a tecnologia é revestida de neutralidade e imparcialidade, abre-se um leque de possibilidades de espelhamento nos algoritmos

[34] O TrueDepth, utilizado pela Apple, por exemplo, identifica variados níveis de profundidade ao invés do contraste, o que torna maquiagens e pinturas menos eficazes contra o LFR.

das tendências mais reprováveis do comportamento humano, cujo resultado é a perpetuação de preconceitos já existentes em nossa sociedade.

No ano de 2016, um caso em particular gerou considerável repercussão: a gigante Microsoft Corporation desenvolveu uma chatbot cunhada Tay por meio do uso de Processamento de Linguagem Natural (PLN), uma vertente da inteligência artificial que ajuda computadores a processar, entender e interpretar a linguagem humana. O objetivo era que Tay interagisse com seres humanos por meio da rede social Twitter, aprendendo com os interesses e comportamentos destes e tornando-se cada vez mais "inteligente" e personalizada. Incapaz de discernir os conceitos éticos de "certo" ou "errado", ou, ao menos, sem ter sido projetada para isso, o resultado foi que, em menos de 24 horas de interação social com os usuários, passou a reproduzir ideias de cunho nazista e eugenista e endossar piadas e mensagens de ódio a negros, mulheres e judeus, precisando ser imediatamente retirada do ar.

Ao contrário do que possa parecer, ante a suposta "onisciência" das gigantes da tecnologia, tal resultado não foi pré-programado ou previsto pela corporação. Não obstante, levando em consideração a falta de transparência e previsibilidade dos algoritmos quando confrontados por pessoas reais, não há motivos para se surpreender. Segundo Miguel Paz (apud. GARCIA, 2016, p.112), a Tay é um bom ponto de partida para entender o problema de os algoritmos da inteligência artificial serem testados, para fins de pesquisa, em um ambiente isolado e controlado, quando a realidade, por si só, não está inserida dentro de um laboratório, mas em um mundo real de alta diversidade e complexidade.

A fim de desmitificar o algoritmo, Osonde Osoba e William Welser IV, autores de "A*n Intelligence in Our Image*", enfatizam o entendimento de que agentes artificiais, tal como a inteligência artificial, são desprovidos de elementos essencialmente humanos, como a moral e a empatia; além de apresentarem o termo "*misbehaving algorithm*", cujas consequências podem levar a resultados "incorretos, injustos e perigosos":

> Artificial agents are, by definition, not human. Moral judgment typically requires an element of choice, empathy, or agency in the actor. There can be no meaningful morality associated with artificial agents; their behavior is causally determined by human specification. The term *misbehaving algorithm* is only a metaphor for referring to artificial agents whose results lead to incorrect, inequitable, or dangerous consequences (2017, p. 7-8).

Nesse sentido, os vieses algorítmicos podem ser definidos como uma discriminação sistemática contra certos indivíduos ou grupos baseados no uso inapropriado de determinados traços, características ou particularidades. Entre os principais alvos dos vieses discriminatórios do algoritmo estão pessoas cuja raça, identidade de gênero, nacionalidade, deficiências físicas ou mentais ou outras características ímpares sejam divergentes do padrão pelo qual a base de dados é ensinada e está, portanto, habituada. (SILBERG; MANYIKA, 2019).

Tais vieses, no entanto, não nascem de uma subjetividade crítica e intencional da máquina, mas por uma construção que envolve desde seu nascimento – como os desenvolvedores e operadores que projetam os seus algoritmos - até o banco de dados utilizado para treinar o sistema (GARVIE, FRANKLE, 2016). Na esfera da tecnologia de reconhecimento facial, como já mencionado anteriormente, os bancos de imagens desempenham papel de suma importância para a qualidade de seus resultados.

No campo da estatística e da ciência de dados, há muito já se fala dos vieses nos modelos preditivos de aprendizado de máquina. Nessa seara, o viés (*bias*) é considerado um erro sistemático resultado do processo de amostragem, isto é, uma distorção aleatória de um estimador estatístico que muito ocorre, por exemplo, nas análises preditivas do aprendizado de máquina, que buscam entender o passado de seus dados para tentar "prever" uma resposta futura. Para que o estimador de um determinado parâmetro seja considerado não viesado, é esperado que seu valor, na média, seja igual ao valor real. Além disso, é preferível que a variância seja a mínima viável, o que nem sempre é possível. Tanto um alto viés quanto uma alta variância podem causar falhas na precisão do sistema.

Há 25 anos, Friedman e Nissenbaum (1996) já relatavam comportamentos injustos ou tendenciosos de sistemas computacionais utilizados em tarefas diversas, como na assistência jurídica automatizada para imigração, e propunham uma estrutura sistemática para pensar sobre tais vieses. Naquela época, a discussão dos autores não englobava termos de ciência da computação mais avançados, porém suas críticas eram dirigidas aos procedimentos que esses sistemas usavam para chegar até os seus resultados, isto é, os algoritmos (OSOBA, 2017).

Se, naquela época, os vieses na tecnologia eram reportados em sistemas de escala industrial, quando o computador pessoal e a internet ainda engatinhavam, atualmente o crescimento

exponencial da tecnologia e sua multipotencialidade garantem a expansão desses problemas a alcances antes inimagináveis. (OSOBA, 2017) Hoje, é difícil pensar em interações virtuais que não envolvam o crivo de algoritmos, que, com base no perfil e interesses do indivíduo, definem o que este deve comprar, ler, assistir e pensar, o que Eli Pariser (2011) define como "filtro-bolha". Essas ações escondem por trás um conjunto de instruções que foram idealizadas por pessoas reais, treinadas por máquinas e executadas em diferentes níveis. O risco de ter sua visão de mundo orientada por algoritmos foi bem observado no escândalo da *Cambridge Analytica*. A partir do uso ilegal de dados pessoais de cerca de 50 milhões de usuários do Facebook, a empresa de marketing político traçou perfis demográficos e comportamentais dos eleitores norte-americanos para oferecer-lhes tendenciosamente publicidades políticas da campanha pró-Trump que possuíam mais chances de êxito, tornando-se um fator determinante no resultado das últimas eleições presidenciais norte-americanas (KAISER, 2019).

Atualmente, é possível constatar que a implementação de modelos preditivos baseados em algoritmos de inteligência artificial em diferentes áreas está aumentando em proporções globais, visando a busca estratégica pela melhor resposta para uma demanda com base na análise dos dados anteriores, gerando, consequentemente, um certo padrão de resposta. Entre algumas de suas implementações, está o *'match'* entre vagas de emprego e determinado perfil de profissional buscado por uma empresa, a concessão de empréstimos e créditos financeiros à indivíduos avaliados positivamente e a concessão de pontos que determinam a taxa de periculosidade e reincidência de indivíduos presos, com base na probabilidade calculada a partir do perfil do indivíduo.

De maneira geral, a implementação de sistemas algorítmicos pode trazer relevantes aprimoramentos em determinados setores, como na área da saúde, que pode se beneficiar da agilidade e capacidade de realização de cálculos n-dimensionais dos algoritmos disponíveis para a predição de riscos cardiovasculares e de outras doenças (BATISTA; CHIAVEGATTO FILHO, 2019). No entanto, o problema mais agravante e que merece especial atenção dos programadores, desenvolvedores de softwares e da sociedade como um todo urge quando a tecnologia, ante sua áurea *technochauvinista* de "imparcialidade", é capaz de determinar o valor (e o destino) de determinados indivíduos, principalmente quando implementada na esfera criminal.

Batizados de “avaliadores de risco”, softwares responsáveis por estipular, por meio de algoritmos, se o acusado é ou não digno de ser libertado sob fiança ou liberdade condicional baseado na probabilidade de reincidir, além de determinar o tipo mais apropriado de supervisão e encarceramento se tornaram cada vez mais utilizados sobretudo nos EUA, embora cada estado tenha implementado sistemas próprios - alguns deles licenciados por empresas com fins lucrativos, como a Northpointe (BARRY-JESTER, CASSELMAN, GOLDSTEIN, 2015). Um dos casos mais emblemáticos de discriminação algorítmica na esfera criminal manifestou-se com o COMPAS, ferramenta de avaliação de risco desenvolvida pela empresa Northpointe Inc. e utilizada no sistema judiciário e penitenciário norte-americano, cujo principal objetivo concernia em calcular o risco de reincidência criminal de indivíduos presos atribuindo-os pontuações de 1 a 10 com base em mais de 100 fatores (como idade, sexo e histórico criminal), determinando se estes eram considerados de menor ou maior risco de cometerem novos crimes.

Em conferência, o então procurador-geral dos Estados Unidos, Eric Holder, alertou publicamente que as pontuações de risco poderiam injetar preconceitos e vieses nos julgamentos:

> Legislators have introduced the concept of “risk assessments” that seek to assign a probability to an individual’s likelihood of committing future crimes and, based on those risk assessments, make sentencing determinations. Although these measures were crafted with the best of intentions, I am concerned that they may inadvertently undermine our efforts to ensure individualized and equal justice. By basing sentencing decisions on static factors and immutable characteristics – like the defendant’s education level, socioeconomic background, or neighborhood – they may exacerbate unwarranted and unjust disparities that are already far too common in our criminal justice system and in our society (HOLDER, 2014)

Segundo a ProPublica, empresa de jornalismo sem fins lucrativos, a preocupação de Holder se mostrou verdadeira. Pesquisas mostraram que, no geral, o sistema de avaliação COMPAS previa corretamente a reincidência em 61% dos casos, mas estava correta em suas previsões de reincidência violenta em apenas 20% das vezes (ANGWIN et al., 2016). Contudo, com quem o sistema mais errava? Uma análise investigativa criteriosa feita pela ProPublica com mais de 10.000 réus criminais em Broward County, Flórida, em um período de dois anos, descobriu que réus negros eram muito mais prováveis do que réus brancos de serem incorretamente classificados como de maior risco (ANGWIN et al., 2016).

Dos indivíduos rotulados erroneamente como de maior risco (não reincidiram), a maioria (44,9%) eram afro-americanos, ao passe que 23,5% eram brancos. Já dos indivíduos classificados erroneamente como de menor risco potencial (voltaram a cometer algum crime), 28,0% eram afro-americanos, enquanto 47,7% eram brancos. Além disso, a pesquisa também demonstrou que réus negros eram 58% mais propensos a serem classificados (erroneamente ou não) como de médio ou alto risco, versus 33% dos réus brancos. Os réus negros, portanto, foram rotulados mais vezes como futuro criminosos, enquanto os réus brancos eram mais comumente rotulados como de baixo risco (ANGWIN et al., 2016).

Apesar da raça não estar entre as 137 perguntas respondidas pelos réus ou extraídas de registros criminais para gerar a predição algorítmica do COMPAS, não há evidências suficientes para sugerir que a inclusão da raça tenha um impacto significativo na precisão ou justiça dos dados. Isso porque a exclusão da raça não leva necessariamente à eliminação das disparidades raciais na previsão algorítmica de reincidência (DRESSEL, FARID, 2018).

Além disso, ao contrário do que imaginavam as empresas e licenciadoras de softwares (e os governos que as implementaram), que buscavam utilizar algoritmos como uma forma de encontrar respostas precisas que gerassem mais segurança e garantia ao sistema penal, pesquisas mostraram que o mecanismo de risco COMPAS não é mais preciso ou justo do que as previsões de participantes da pesquisa com pouco ou nenhum conhecimento em justiça criminal, girando em cerca de 65% de precisão (DRESSEL, FARID, 2018). Reforça-se, aqui, uma constante: os sistemas algorítmicos, ainda que fortemente treinados, são incapazes de agir com total imparcialidade, visto que apenas reforçam os vieses já existentes no sistema penal e na sociedade como um todo.

Para além das análises preditivas observadas em sistemas de pontuação de risco de reincidência criminal, outra aplicação de algoritmos de reconhecimento facial que possui riscos de gerar discriminação algorítmica é bem observada na esfera criminal. Em diversos países, agências policiais e órgãos de segurança pública têm buscado implementar sistemas de policiamento preditivo visando identificar a possível ocorrência de crimes que possam ser prevenidos com o uso de previsões estatísticas.

Os vieses discriminatórios contidos no ramo das atuações policiais e da segurança pública não são novidade em nossa sociedade, tampouco a análise de dados para esse fim. Na França

monárquica do século XVI, os patrulhamentos policiais já eram realizados a partir da análise de dados dos locais que apresentavam mais ocorrências criminais, e regiões mais periféricas e marginalizadas "sofriam o revés de um patrulhamento mais ostensivo, com maior violência, muito provocado pela forma de criminalização da época, de preconceitos estruturados, e nas legislações penais da época" (LUCENA, 2019). Hodiernamente, a combinação da voluptuosidade da big data com sistemas de reconhecimento facial, inteligência artificial e aprendizado de máquina como formas de aprimorar o serviço policial trazem uma sensação de maior combatividade ao crime e menos enviesamento de dados nos patrulhamentos policiais, no entanto, não é o que estudos demonstram.

Se determinado software de policiamento preditivo é desenvolvido para reproduzir padrões de policiamento, logo, não preverá crimes futuros, mas policiamentos futuros (LUM; ISAAC, 2016), ampliando, consigo, o enviesamento discriminatório contido nas atividades policiais rotineiras – desde os bairros onde o policiamento é mais agressivo até os tipos de crimes que mais geram atenção policial, como crimes de drogas e contra o patrimônio, passando pelas características raciais que são mais tendenciosamente atribuídas a imagem de um infrator criminal. Em pesquisa, aponta-se que apesar do uso de drogas possuir praticamente o mesmo nível entre pessoas de diferentes raças, se o sistema preditivo PredPol fosse utilizado na cidade de Oakland, no estado da Califórnia, nos EUA, indivíduos negros possuiriam duas vezes mais chances de serem alvo de policiamento preditivo se comparado às pessoas brancas. O resultado se repete quando a análise é feita a partir de classes sociais, com um nível maior de policiamento em regiões de baixa renda se confrontado com os dados de outras regiões. Fica evidente, portanto, que o resultado de um policiamento baseado em dados algorítmicos reforça não a queda de atos criminosos, mas sim um policiamento desmedido e ostensivo nas regiões onde indivíduos de baixa renda e de maioria negra ou imigrante predominam (LUM; ISAAC, 2016).

Quando tais sistemas de policiamento e segurança pública incluem o uso de reconhecimento facial para identificar supostos criminosos, o enviesamento algorítmico de torna-se ainda mais evidente. São muitos os estudos que demonstram que os algoritmos de sistemas de reconhecimento facial contêm vieses desde a sua concepção (*by design*), o que, no entanto, não impediu que algumas das maiores empresas de tecnologia do mundo as desenvolvessem e comercializassem para outras empresas de segurança pública e privada nos últimos anos.

Em 2019, pesquisadores do MIT Media Lab testaram o Amazon Rekognition, programa de classificação de rostos com base na raça e no gênero do indivíduo vendido para autoridades policiais norte-americanas pela gigante varejista, e concluíram que este era 92,9% preciso no reconhecimento de mulheres brancas, mas apenas 68,6% quando se tratava de mulheres negras. A taxa de acerto quanto ao rosto de homens brancos foi 100% precisa.

Se a classificação de indivíduos pelo gênero e cor da pele não parece perigosa o suficiente, uma investigação do jornal independente The Intercept revelou que a IBM utilizou filmagens confidenciais das câmeras de vigilância do Departamento de Polícia da cidade de Nova Iorque como uma forma de "teste" para o desenvolvimento de software que permite à polícia pesquisar pessoas por vídeo com base no seu gênero, tom de pele e cor de cabelo (JOSEPH, LIPP, 2018). Essas capacidades levantam amplas discussões sobre os riscos trazidos pela automação de perfil raciais pela polícia.

Já a pesquisadora e cientista da computação Joy Buolamwini (2016), gerou repercussão internacional ao usar uma máscara inteiramente branca que era instantaneamente detectada quando utilizada em frente a um software de reconhecimento facial. Quando retirava a máscara e revelava seu rosto de pele negra, tornava-se invisível: a máquina era incapaz de identificar a sua presença. No MIT, a pesquisadora co-produziu o projeto Gender Shades, que tinha como objetivo medir a proporção de erros dos sistemas de reconhecimento facial quanto ao gênero. Com um banco de dados de 1.270 imagens selecionadas do rosto de parlamentares de diferentes países africanos e europeus, divididos em grupos por gênero e tons de pele, a pesquisa demonstrou que as três empresas participantes (IBM, Microsoft e Face++) obtiveram melhor performance ao identificar rostos masculinos, com apenas 8,1% de erros, enquanto errava 20,6% dos rostos femininos. As empresas participantes também foram mais precisas na identificação do rosto de indivíduos de pele clara em detrimento dos indivíduos de pele escura (11.8% − 19.2% de erros, respectivamente). A precisão era ainda pior quando se tratavam de mulheres negras, com uma taxa de erros que variava entre 20.8% e 34.7%. A taxa de erros na identificação de homens brancos variou entre 0,0% e 0,7%, a depender da empresa (BUOLAMWINI; GEBRU, 2018).

Klare et al. (2012) tiveram resultados semelhantes. Em pesquisa que examinou a influência da demografia no desempenho de algoritmos de reconhecimento facial de seis diferentes sistemas, calculadas a partir de bancos de dados de grande escala (mais de cem mil rostos), o resultado foi

que grupos de mulheres, jovens e negros eram mais difíceis de serem reconhecidos em todas as combinações realizadas (algoritmos comerciais, treináveis e não treináveis). Quanto aos algoritmos treináveis, concluiu que as taxas de precisão quanto a idade e raça/etnia podem ser melhoradas se treinados especificamente para essas questões.

É importante observar, como já descrito, que os sistemas algorítmicos são tão bons quanto a robustez e variedade de dados que os compõem. No entanto, não é errado acrescentar que tais sistemas complexos são tão inclusivos ou discriminatórios quanto os indivíduos que o desenvolvem. Segundos estudos psicológicos, seres humanos possuem mais facilidade em reconhecer rostos da sua própria raça do que rostos de raças distintas da sua. Com os algoritmos, não é diferente. Phillips et al. (2011) descrevem o chamado '*other-race effect*": Em um teste realizado com a taxa de falsos positivos mais baixa requisitada, os algoritmos ocidentais reconheceram rostos caucasianos mais precisamente do que rostos asiáticos, enquanto algoritmos da Ásia Oriental (China, Japão, Coreia do Sul etc.) tiveram maior performance em reconhecer rostos do leste asiático em detrimento de rostos caucasianos. No entanto, quando o teste abrangia todas as taxas de falsos positivos, ambos os algoritmos performaram melhor com rostos caucasianos, visto que eram a maioria na base de dados. Ainda assim, as taxas de precisão nos rostos caucasianos eram mais vantajosas se comparadas as do algoritmo do leste asiático.

Tarcízio Silva (2019) também traz dois relevantes pontos para essa discussão. Em primeiro lugar, os problemas causados pelos vieses algorítmicos revelam a dificuldade de se discutir a chamada "dupla opacidade', descrita como "o caráter difuso tanto da tecnologia, vista erroneamente como neutra, quanto das relações étnico-raciais na sociedade e, por consequente, na tecnologia" (SILVA, 2019). Nesse sentido, a falta de transparência dentro da tecnologia e da forma como ela é elaborada impedem a expansão dos aspectos sociais da tecnologia dos debates raciais na sociedade na medida que os tornam invisíveis. Em segundo lugar, o autor demonstra que a inviabilização de questões raciais na tecnologia é trazida a partir de uma visão computacional definida por práticas da branquitude, enquanto "definidora da sociedade e das tecnologias de produção e controle" (SILVA, 2019).

Identificar vieses e desvios sistêmicos em sistemas algorítmicos não é uma tarefa fácil. Para isso, conhecimentos matemáticos, estatísticos e computacionais não são o suficiente. Mais do que isso, é latente a necessidade de se expor a reflexões sociais, éticas, sociológicas e políticas, além

de compreender aspectos embutidos nas raízes da sociedade, como o racismo estrutural (ALMEIDA, 2015) e questões de gênero (BUOLOWMINI, 2018), das quais o algoritmo está inerentemente veiculado.

Com tamanho crescimento de possibilidades trazidas pela tecnologia e o risco do desmantelamento de direitos, impõe-se a urgência de entender a justiça a partir de uma lógica manual e individualizada, observada “a dedo” as circunstâncias que a cercam de forma a não reforçar a desumanização e a automação de um sistema penal já desumano e sistemático, onde os indivíduos de grupos minoritários são os mais comprometidos.

Acrescenta-se que, para questões tanto sociais quanto técnicas, inúmeras organizações sem fins lucrativos e de defesa aos direitos humanos e às liberdades civis têm se tornado porta-vozes de questões como o banimento do uso de reconhecimento facial e outros sistemas algorítmicos - principalmente quando utilizados para fins de policiamento preditivo e segurança pública - e o emprego de práticas de programação e desenvolvimento de algoritmos mais transparentes e inclusivos. Como Buolowmini (2016) afirma, três princípios são de suma importância: quem programa, como programa e para que fins. Por meio desses três princípios, é possível pensar em times mais abrangentes e diversos, de forma que os pontos cegos da “caixa preta” dos algoritmos possam se tornar, enfim, mais visíveis.

3. O RECONHECIMENTO FACIAL NO REINO UNIDO

3.1. CONTEXTO HISTÓRICO DE VIGILÂNCIA NO REINO UNIDO

Seja pela forte influência econômica mercantilista, pela potência marítima e bélica ou pela posição geográfica estratégica, além de diversos outros fatores, fato é que a nação insular hoje conhecida como Reino Unido sempre esteve no centro dos principais conflitos históricos ocidentais, como método de manutenção e gerenciamento de sua soberania política. Nesse sentido, busca-se, nesse tópico revisar brevemente, sem a pretensão de esgotar o tema, o contexto histórico de controle, vigilância e manutenção de poder dentro do Reino Unido, de maneira a explicar, aliado ao desenvolvimento de novos métodos tecnológicos de controle, como o Reino Unido foi de maior potência econômica mundial para um dos países mais vigiados do mundo.

Desde o século II, quando o Império Romano se encontrava em um processo de larga expansão e a região de Britânia, hoje conhecida como o centro-sul da ilha da Grã-Bretanha, era uma província romana, já havia uma certa preocupação na elaboração de estruturas defensivas físicas contra as investidas militares de tribos originárias próximas, como os Pictos e os Escotos, tendo o imperador antonino Adriano ordenado a construção da Muralha de Adriano (em latim, *Vallum Aelium*), que foi não somente uma das primeiras e mais extensas barreiras extensivas da Grã-Bretanha, como também uma separação simbólica do mundo civilizado (romano) com o mundo bárbaro (nativo). Na posse do controle sobre quem tinha permissão de entrar e sair do império, a divisória não servia apenas como barreira física, mas também como uma espécie de ponto de observação e vigilância, sendo um dos primeiros alertas do povo romano quanto à aproximação de um possível ataque, de forma a retardar a travessia de invasores ou saqueadores. (MILAZZO, 2008, p. 9-14). Da Idade Média até o início da Era Contemporânea, as Ilhas Britânicas estiveram envolvidas em diversos conflitos, como A Guerra dos Cem Anos (1337-1453), a Guerra das Rosas (1455-1487) e a Batalha de Waterloo (1815), com a vitória da Inglaterra e da Prússia contra as invasões napoleônicas. Somadas as vitórias belicosas à exploração colonial, a dominação do comércio internacional e às Revoluções Industriais, o Reino Unido[35], em suas diferentes

[35] Elucida-se que a história do Reino Unido foi marcada por diferentes composições, entre elas, os marcados pelo Tratado da União de 1707, com a criação do Reino da Grã-Bretanha, junção política do Reino da Inglaterra (incluso o País de Gales) e o Reino da Escócia e o Ato de União de 1801, que uniu politicamente o Reino Unido da Grã-Bretanha com o Reino da Irlanda. Enfim, a formação do Reino Unido como atualmente conhecemos surgiu apenas em 1922, com o surgimento do Estado Livre Irlandês, que se tornou independe da coroa britânica.

composições e, em especial, a Inglaterra, colecionava motivos para se consolidar, então, como a principal potência econômica mundial entre os séculos XVII e XIX.

No meio das constantes inovações tecnológicas proporcionadas pela intensiva industrialização britânica e sua consequente soberania econômica, novas estratégias para além dos métodos de guerra defensivos e ofensivos tradicionais foram sendo desenvolvidos, de forma a acompanhar a evolução da sociedade. No contexto da Segunda Guerra Mundial, urgia a necessidade não mais dos fronts e trincheiras da Primeira Grande Guerra, mas de observar e decifrar o inimigo para além das barreiras físicas, de forma a utilizar a computação e os primórdios da inteligência artificial para traçar estratégias de inteligência. No início da década de 1940, o matemático britânico e pioneiro da tecnologia da informação Alan Turing (1912-1954) desenvolveu uma máquina capaz de decifrar o "Enigma", código amplamente utilizado pelos nazistas para enviar mensagens secretas entre seus agentes, além de um método de criptografia de conversas telefônicas. A espionagem da comunicação alemã representou uma grande vantagem a Inglaterra e seus aliados, permitindo derrotar mais depressa a Alemanha. Além disso, outros sistemas de contraespionagem e controle social foram utilizados pelos britânicos durante a Segunda Guerra, como o Sistema Double Cross[36] ou XX, travado pela M5, serviço doméstico de inteligência militar britânica (MASTERMAN, 1972).

A despeito do decurso do tempo, duas representações de controle social habitam frequentemente o imaginário social coletivo britânico e inspiram análises, críticas, teses e revisões, ascendendo o debate sobre vigilância e controle social mundo afora, seja no pilar acadêmico ou na esfera da cultura e do entretenimento. A primeira consiste no modelo panóptico do final do século XVIII, que como anteriormente analisado, transformou-se, para além de seus rascunhos iniciais de arquitetura circular física, num ideal de disciplinamento de corpos, posteriormente abordado por Foucault. A outra representação é a figura do Grande Irmão ("*Big Brother*"), personagem que ultrapassa os limites literários do romance "*1984",* vindo a se tornar uma das referências mais importantes da cultura de vigilância do século XX e uma feroz crítica a governos autoritários.

[36] Conforme MASTERMAN (1972) explicita, o sistema de dupla espionagem (*Double Cross*) foi um notável aparato por meio do qual os agentes alemães capturados na Grã-Bretanha foram induzidos a servir à causa aliada, fornecendo aos oficiais alemães informações elaboradas e manipuladas pela inteligência britânica. Esse dispositivo contribuiu substancialmente para o sucesso militar dos Aliados. Por meio desse sistema, por exemplo, se explica como Hitler e o exército alemão foram levados a acreditar que os desembarques dos Aliados no Dia D seriam feitos na região francesa Passo de Calais, e não na Normandia.

Ausente a pretensão de conceder total paridade a ambas as representações, fato é que possuem uma interessante característica em comum para além de suas características distópicas: ambas foram escritas e elaboradas por autores de nacionalidade britânica, quais sejam, Jeremy Bentham e George Orwell (pseudônimo do autor Eric Arthur Blair). A partir de seus diferentes contextos e épocas, esses autores nos ajudam a ilustrar brevemente a evolução histórica da vigilância no Reino Unido e nos dão pistas quanto ao cenário atual.

No contexto de Bentham, o projeto foi idealizado a partir de uma série de cartas escritas no ano de 1787 durante uma visita do autor a seu irmão em *Crecheff*, na Rússia Branca. Com a influência do positivismo inglês de Stuart Mill e James Mill, o modelo panóptico de vigilância nasce de uma radical intenção de buscar soluções utilitaristas para a sociedade de forma a proporcionar o seu bem-estar. Dois anos depois, em 1789, a queda da Bastilha e, consequentemente, a aprovação da Declaração dos Direitos do Homem e do Cidadão, que passou a definir, pela primeira vez, os direitos individuais e coletivos do homem como universais, inauguraram um novo período histórico em que a pena corpórea, não mais totalmente aceita pelos ideais iluministas, é comutada pelas prisões e instituições disciplinares. Por sua vez, o inglês George Orwell escreve uma de suas obras mais relevantes, *1984*, sob o contexto do fim da Segunda Guerra Mundial. Em 1948, ano em que a obra foi publicada, a nação britânica vinha tornando-se consciente tanto de seu triunfo na Guerra quanto do declínio de sua era como potência imperialista.

A nação insular, que até então sustentava o título de maior potência bélica e econômica do mundo, era então ofuscada pela crescente supremacia política dos Estados Unidos da América e da União Soviética, bem como pelo início da Guerra Fria travada por estas duas superpotências. Na corrida pela liderança do poder e influência mundial e com a expansão da globalização trazida pelas duas Guerras Mundiais e pela Guerra Fria, o Reino Unido contou com o desenvolvimento de novas tecnologias e a coleta de informações internacionais para promover o aumento de sua segurança nacional e internacional, como a assinatura, em 1946, do Tratado de Segurança entre os Estados Unidos e o Reino Unido, um pacto de cooperação de inteligências que mais tarde viria a se tornar a aliança ‘Five Eyes’, uma rede de espionagem multinacional em parceria com Canadá, Austrália e Nova Zelândia.

A partir de seus contextos e épocas completamente diferentes, esses autores nos ajudam a ilustrar brevemente a evolução histórica da vigilância no Reino Unido e nos dão pistas quanto ao

cenário atual. Nesse contexto, um elemento fundamental para a vigilância britânica foi a ascensão da utilização de câmeras de circuito fechado. Em 1953, de acordo com Francisco, Hurel e Rielli (2020), o governo britânico instalou câmeras na cidade de Londres para constituir o seu primeiro circuito fechado de televisão (CFTV), visando garantir a segurança da cerimônia de coroação da Rainha Elizabeth II. Segundo Williams (2003), esses sistemas foram introduzidos principalmente para detectar e prevenir o crime, a desordem e o comportamento antissocial, mas também para ajudar a reduzir o "medo do crime". Para este fim, esses sistemas provaram ser muito populares na época, recendo o amplo apoio de políticos, formuladores de políticas e cidadãos.

No começo do século XXI, em frente aos atentados de 11 de setembro de 2001, o *Anti-Terrorism, Crime and Security Act (2001)* foi publicado como uma tentativa de preparar o país para lidar com a ameaça do terrorismo internacional, incluindo medidas rígidas e sem precedentes que ajudam a detectar, investigar e a processar terroristas (CHIRINOS, 2005). Entre estas novas medidas, estão o poder do governo de deter cidadãos estrangeiros suspeitos de terrorismo por um período indefinido sem acusação formal ou julgamento, o poder da polícia de congelar os bens de indivíduos suspeitos de terrorismo, e a possibilidade de os provedores dos serviços de comunicação reterem informação, para que a polícia possa acessar as informações quando investigar casos de terrorismo.

Um importante marco para o Reino Unido com relação à vigilância e terrorismo ocorreu, no entanto, em 7 de julho de 2005, quando a cidade de Londres sofreu uma série de ataques terroristas que resultaram na morte de 52 pessoas e no ferimento de mais de 700. Em decorrência disso, no dia 21 de julho, quatro extremistas islamistas buscaram reproduzir os ataques de 7 de julho e detonar quatro bombas no sistema de transporte metroviário londrino. Essa série de ataques falhou e as bombas nunca chegaram a explodir, no entanto, durante a busca intensa pelos criminosos responsáveis pelos ataques, a polícia londrina cometeu um erro e, no dia seguinte à tentativa de ataque, matou o brasileiro Jean Charles de Menezes com sete tiros na cabeça e no ombro, após este ser identificado por meio de câmeras de vigilância e confundido com um dos membros terroristas.

Em decorrência desses recentes fatos, o *Terrorism Act 2006* foi publicado como uma legislação de emergência que introduz novas medidas de segurança, como o poder do governo em processar indivíduos ou organizações que glorificarem ou divulgarem publicações terroristas. No

entanto, a medida mais controversa introduzida no *Terrorism Act 2006* é a que autoriza a polícia a deter indivíduos suspeitos de terrorismo sem acusação durante 28 dias (um aumento de 14 dias em relação ao que estava estipulado na última legislação).

Segundo Eijkman e Weggemans (2011), o uso de câmeras de vigilância como medida antiterrorista aumentou desde os atentados terroristas de 2005, tendo esse controverso instrumento de prevenção se difundido rapidamente no país. Nesse contexto, a organização de liberdades civis Liberty critica o impacto dos sistemas de vigilância na privacidade dos indivíduos e solicita uma regulação mais rígida, "dado o risco que as câmeras de vigilância ilimitadas representam para a intrusão injustificável da privacidade" (MOITA, 2016). Já de acordo com Eijkman (2011), as câmeras de vigilância têm se demonstrado um problema que vai além de apenas questões de privacidade dos cidadãos, pois também podem contribuir para a discriminação de grupos minoritários. Isso é demonstrado pelo autor no caso da cidade de Birmingham, na Inglaterra, onde as câmaras foram colocadas majoritariamente em áreas com populações de origem muçulmana, o que resultou numa tensão entre a polícia e as comunidades locais.

Nesse sentido, a política antiterrorista que prosperou com o *onze de setembro* e a instituição da Guerra ao Terror, principalmente nos Estados Unidos e na Europa, elegeu a tecnologia do poder panóptico como elemento fundamental na vigilância e controle não somente do inimigo, mas também do que Zygmunt Bauman (2017) intitulou como o "estranho". Os "estranhos à nossa porta" (BAUMAN, 2017) são aqueles que se situam na zona entre o amigo e o inimigo: seus rostos não são familiares como o do considerado amigo, cidadão, mas não são necessariamente caracterizados como o "inimigo" descrito pela teoria antigarantista de Jakobs.

Dos imigrantes, refugiados e outros grupos minoritários deve-se valer da desconfiança e da vigilância para embutir controle sobre cada um de seus passos, de forma que não preencham os espaços e tampouco os direitos do cidadão legítimo. Se um crime for cometido, também são esses – fora os inimigos declarados – os primeiros a serem apontados como suspeitos, a partir de uma premissa tanto de Soberania Nacional quanto de superioridade moral, dado que do estranho espera-se valores e princípios éticos inferiores e maior propensão ao cometimento de crimes.

3.2. O USO DE RECONHECIMENTO FACIAL NO REINO UNIDO PARA FINS DE VIGILÂNCIA PÚBLICA

Como observado no capítulo anterior, sistemas de reconhecimento facial vêm sendo desenvolvidos desde a década de 1960. Os primeiros, mais rudimentares e em época de pouca força computacional, permitiam apenas pequenas amostras em espaços controlados e com bases de dados evidentemente limitadas. Alguns sistemas antigos, inclusive, são até hoje erroneamente classificados como de reconhecimento facial, quando na verdade permitiam apenas a detecção de faces, sem a combinação dos rostos detectados com a base de dados existente. Com a evolução da tecnologia e da ciência da computação, o desenvolvimento de sistemas de reconhecimento facial passou a possibilitar o reconhecimento quase instantâneo e em tempo real de milhares de rostos, sendo estes combinados com as informações de diferentes bases de dados de tamanhos estratosféricos. Não é preciso dizer que, de pequenas amostragens, o reconhecimento facial passou a ser um interessante e viável método de controle em espaços públicos, com a coleta de grandes amostragens que permitem abastecer os bancos de instituições públicas e privadas. Nesse sentido, o presente tópico busca elucidar o uso de sistemas de reconhecimento facial no Reino Unido para fins de vigilância em massa, isto é, grandes proporções de dados biométricos faciais coletados em espaços públicos por instituições governamentais, em especial as polícias britânicas, visto que a utilização para fins criminais é a maior representação do perigo existente quanto ao cerceamento de direitos e liberdades.

A utilização de bancos de dados por organizações policiais não é recente. Segundo Atick, Griffin e Redlich (1997), desde 1985 o banco de dados chamado G.R.E.A.T. (*Gang, Reporting, Evaluation and Tracking System*), foi desenvolvido e adotado pela *Law Enforcement Communication Network* (LECN), um consórcio de mais de 650 departamentos de polícia locais, estaduais e federais nos Estados Unidos. O sistema possibilitou o registro automatizado, a pesquisa e a conexão de milhares de dados de indivíduos considerados de gangues locais, contendo cada registro até 150 campos possíveis para entrada de dados, tais como fotos faciais, fotos coletivas de ‘gangues’ e quadrilhas, antecedentes, tatuagens, apelidos, afiliações, entre outros, de forma a facilitar a identificação, a abordagem e a acusação e/ou execução penal desses indivíduos. As informações contidas no sistema eram obtidas diretamente de agências policiais e departamentos de segurança pública que se inscrevessem no sistema, fomentando-o a nível nacional. Em fato, o sistema G.R.E.A.T. não era capaz de identificar o conteúdo das fotografias, bem como a detecção e identificação facial automatizada dos indivíduos, no entanto, Atick, Griffin e Redlich (1997),

membros do Laboratório de Neurociência Computacional da Universidade de Rockefeller, defendiam a implementação do sistema de reconhecimento facial FaceIt, tecnologia de reconhecimento facial criada em 1994 e a primeira comercialmente viável no mundo, à base de dados G.R.E.A.T. para trazer mais precisão e confiabilidade à identificação policial. Curioso notar que a pesquisa foi realizada em parceria com a Visionics Corporation, empresa responsável pelo desenvolvimento do FaceIt, do qual Atick assumia o cargo de presidente e CEO.

Somado a isso, antes mesmo da que é considerada uma das primeiras utilizações de reconhecimento facial em um evento público de grandes proporções, qual seja, o Super Bowl XXXV, que ocorreu na cidade de Tampa, na Flórida, EUA, em janeiro de 2001, Londres, no Reino Unido, já ostentava o título de primeira região a adotar um sistema de reconhecimento facial para fins de vigilância pública, ao adotar, em 1998, o sistema FaceIt no bairro de Newham. Em 2001, o sistema já contava com 300 câmeras de circuito fechado de televisão (CFTV ou CCTV, em inglês) no bairro em questão, ligadas à uma sala de controle central operada pela Polícia Metropolitana de Londres. Em abril de 2001, o sistema FaceIt também foi implantado em Birmingham City Center, onde foi integrado ao sistema de CFTV já existente. Após a estreia britânica, o sistema passou a ser utilizado pelo Departamento de Polícia de Tampa, Flórida em junho de 2001, a primeira cidade estadunidense a aderir o uso, após a Visionics oferecer o software gratuitamente por um ano. Após esse período de teste, a compra do software pela polícia custaria na faixa de 33 mil euros, na cotação da época (POWER, 2001). Nas três regiões citadas, o propósito principal da adesão era monitorar pedestres e transeuntes para identificar, deter e prender terroristas, suspeitos ou foragidos com mandado de prisão em aberto, reduzindo a criminalidade (BREY, 2004).

Depois do 11 de setembro de 2001, quando as ações da Visionics dispararam em Wall Street, a empresa tornou Newham, bairro até então pouco conhecido de Londres, famoso por "ter vencido e tido a ousadia de compreender o futuro da tecnologia de combate ao crime" (MEEK, 2002). Isso porque, inicialmente, creditou-se ao sistema uma queda de 40% na criminalidade (DEVLIN, 2019). Entretanto, em pouco tempo foram encontradas falhas no sistema, que revelaram que ele só funcionava de maneira confiável em experimentos realizados em laboratórios, dado que, até a adoção por agências policiais inglesas, o sistema nunca havia detectado um alvo vivo sequer. Essa informação foi revelada por James Meek (2002), jornalista do The Guardian que, no ano de 2002, tentou em vão ser descoberto pelo FaceIt no bairro de Newham, após a polícia concordar em

adicionar seu rosto à lista de observação. Após duas tentativas de locomoção em regiões movimentadas e sem a utilização de artifícios que afetassem a detecção de seu rosto, o sistema não o reconheceu.

O jornalista finaliza afirmando que o suposto sucesso do FaceIt na redução da criminalidade em Newham não resiste a uma análise detalhada, pois, apesar de entre 1999 e 2002 os crimes com uso de violência terem tido um aumento menor quando comparado aos bairros vizinhos, o número de roubos em Newtam aumentaram 38%, comparado a 33% em Tower Hamlets, e enquanto nesta última os roubos com arrombamento diminuíram em 12% no período, em Newham eles aumentam ligeiramente. Nesse sentido, a adesão ao sistema de reconhecimento facial foi comparada por Meek (2002) a um sistema de segurança falso instalado na frente de uma casa: a redução no crime se deu porque pela crença nos indivíduos que o sistema funcionava, não em face dos resultados reais apresentados pelo sistema, que havia falhado em seu propósito.

A ascensão do sistema FaceIt não durou muito. Após alguns protestos, a organização estadunidense de direitos civis *American Civil Liberties Union* (ACLU) pressionou a polícia de Tampa, na Flórida, a disponibilizar registros diários do funcionamento do sistema FaceIt nas câmeras de circuito fechado de televisão da cidade. Os resultados dos registros mostraram que em quatro dias do mês de julho de 2001 o sistema soou o alarme 14 vezes. No entanto, cada um desses alarmes revelou ser um falso positivo, isto é, 14 indivíduos inocentes tiveram seus rostos erroneamente expostos à escrutínio policial por um serviço de segurança (MEEK, 2002). Tais registros representaram um golpe na credibilidade da Visionics Corporation no uso de seu software para fins de vigilância pública e, em agosto de 2003, a polícia de Tampa decidiu suspender a utilização do sistema, com um saldo de dois anos de uso e nenhuma prisão ou identificação positiva.

Posteriormente, outras regiões que também não obtiveram resultados positivos, como Virginia Beach, seguiram essa decisão. Ressalta-se que o desligamento do sistema FaceIt para fins policiais nas cidades abordadas não significou o fim do uso de câmeras de circuito fechado de televisão (CFTV) no Reino Unido, que só cresceu ao longo dos anos sob supervisão policial constante e mediada, tampouco o fim de novas tentativas de utilização de reconhecimento facial para fins de vigilância pública nos anos seguintes, no entanto, a atenção negativa que o experimento tecnológico recebeu e o término definitivo do projeto não obteve outro resultado senão o de retardar

durante anos os esforços para pôr a tecnologia de reconhecimento facial como uma opção viável de ferramenta policial na vigilância pública (GATES, 2011).

Ante o exposto, o uso de sistemas de reconhecimento facial na vigilância pública voltou a ganhar os holofotes no Reino Unido a partir do ano de 2015. Alguns anos antes, em 2011, a TRF havia sido utilizada para ajuda a confirmar a identidade de Osama Bin Laden, morto em um ataque dos EUA, o que fomentou a ideia de que a tecnologia era uma boa ferramenta na luta contra o "inimigo" terrorista ou criminoso por policiais e profissionais militares. No Reino Unido, as principais representantes desse rápido crescimento foram três forças policiais britânicas: a Polícia Metropolitana de Londres (*Metropolitan Police Service* – Met), da Grande Londres, na Inglaterra; a Polícia de South Wales (*South Wales Police* – SWP), do País de Gales; e a Polícia de Leicestershire, das regiões de Leicester, Leicestershire e Rutland, na Inglaterra, que passaram a implementar o uso reconhecimento facial automatizado com câmeras de CFTV em espaços e eventos públicos.

Em junho de 2015, os participantes do Download Festival, festival de rock britânico com duração de três dias no Donington Park, em Derby, na Inglaterra, foram submetidos, em pontos estratégicos, ao sistema de reconhecimento facial aderido pela Polícia de Leicestershire. Os indivíduos tiveram seus rostos escaneados e comparados com um banco de imagens de custódia legalmente mantidas em toda a Europa junto a parceiros da Europol. Acredita-se ter sido a primeira vez que o software de TRF foi usado em um evento ao ar livre no Reino Unido. O lançamento da tecnologia era para ser discreta, no entanto, a informação foi vazada por uma entrevista da Police Oracle publicada antes do previsto, onde gabava-se que os mais de 90.000 frequentadores esperados seriam as primeiras pessoas na Grã-Bretanha monitoradas ao vivo em um festival de música dessas proporções. Na conferência Security Twenty 15, o Comissário da Câmara de Vigilância do governo britânico Tony Porter (2015), reconheceu que a informação de que o público viria a ter seus rostos identificados sem consentimento ofuscou as principais notícias sobre o festival: ao invés das bandas Slipknot, Muse ou Kiss, que se apresentaram no evento, estamparem as manchetes, foi o uso do sistema de reconhecimento facial pela agência policial.

Porter (2015) aponta para a necessidade de autoridades relevantes, como forças policiais e autoridades locais, estarem em conformidade com o Código de Conduta de Câmera de Vigilância (*Surveillance Camera Code of Practice*), pulicado pelo Ministério do Interior britânico em junho

de 2013. Apesar de acreditar que a maioria dos centros de CFTV em espaços públicos estão de acordo com o Código de Conduta ou bastante próximo, o comissário descobriu, por meio do levantamento do uso das câmeras de vigilância do centro de uma grande cidade britânica, que não havia avaliações de impacto de privacidade, revisões regulares e familiaridade com o Código de Conduta cuja atenção pela autoridade local é obrigação legal, além do desvio de finalidade do uso das câmeras para questões como de gestão de tráfego e de resíduos, e que não o surpreenderia se isso ocorresse em outras autoridades locais ao redor do Reino Unido.

No ano seguinte, o documento nomeado *Review of the impact and operation of the Surveillance Camera Code of Practice* (2016), levantou preocupação quanto a ausência de supervisão formal e independente do uso da TRF pelas autoridades policiais no Reino Unido, e trouxe nove recomendações de medidas de transparência ao operar sistemas de vigilância em espaços públicos, entre elas, que as autoridades locais apontem um responsável sênior para supervisionar se o uso de câmeras de vigilância pela organização está em conformidade com os requisitos do Código de Conduta; e a publicação pelas autoridades relevantes de uma cobertura da utilização de câmeras de vigilância, incluindo autoavaliações, dados numéricos, avaliações de impacto de privacidade e resultados de revisões anuais que destaquem a eficiência e a eficácia do sistema.

Em 2016 e 2017, as agências policiais britânicas passaram a utilizar a tecnologia de reconhecimento facial mais recorrentemente em uma série de eventos públicos, como o Carnaval de Notting Hill, em agosto de 2016 e 2017, pela Polícia Metropolitana de Londres; a final da UEFA Champion's League, em maio de 2017, pela Polícia de South Wales; e o Remembrance Sunday, em novembro de 2017, pela Polícia Metropolitana de Londres. O objetivo era encontrar, entre os milhares de rostos escaneados, criminosos foragidos ou suspeitos.

Na primeira utilização da tecnologia pela Polícia Metropolitana de Londres, nos dois dias de Carnaval de Notting Hill, em 2016, nenhum indivíduo foi corretamente identificado com o auxílio tecnológico, a despeito do investimento financeiro realizado. No ano seguinte, em nova tentativa, a Polícia Metropolitana já enfrentava forte resistência de organizações de direitos civis e de igualdade racial, bem como do público em geral, e o motivo é conhecido: o evento escolhido para ser o "modelo-piloto" do uso de FRT pela Polícia Metropolitana de Londres é também o maior evento afro-caribenho do Reino Unido e um símbolo para a cultura negra britânica. Assim, o

monitoramento facial no evento reascendeu o debate sobre a estigmatização do perfil racial criminoso e o excesso de policiamento das comunidades negras.

Após os protestos de organizações de direitos civis – tais como Big Brother Watch, Liberty e StopWatch, que advogam contra a vigilância pública – ganharem força, estas foram autorizadas a observar o funcionamento do sistema de reconhecimento facial adotado pela Met em tempo real no evento de 2017. O resultado foi que, no período de cinco a dez minutos de observação da tecnologia em ação, testemunhou-se dois falsos-positivos, isto é, duas mulheres sem histórico suspeitoso foram comparadas a homens criminosos no banco de dados. No mesmo dia, houve cerca de 35 resultados falso-positivos, e cerca de cinco indivíduos incorretamente identificados pelo sistema foram abordados até que suas identidades e, portanto, suas inocências fossem provadas. De fato, a polícia obteve duas correspondências positivas verdadeiras entre um indivíduo detectado no evento e seu registro no banco de dados, no entanto, nenhuma delas era um criminoso procurado. A primeira pessoa abordada, no Carnaval de Notting Hill 2017, não era mais procurada para prisão, pois os dados policiais utilizados no evento estavam desatualizados; já a segunda pessoa corretamente identificada, no Remembrance Sunday 2017, foi encontrada a partir de uma lista de observação relacionada à saúde mental do Centro de Avaliação de Ameaças Fixas (FTAC). Quanto a esse último caso, a polícia não havia consultado grupos ou conselhos apropriados de especialistas em saúde mental, de forma que o impacto que essa vigilância intrusiva e a intervenção policial poderia ter na saúde mental de indivíduos mentalmente vulneráveis foi completamente ignorada. Isso posto, aponta-se que, do montante total de 102 indivíduos detectados, a Polícia Metropolitana identificou corretamente apenas dois, obtendo um porcentual de 98% falsos positivos. (BIG BROTHER WATCH, 2018).

Por sua vez, a Polícia de South Wales (SWP), do País de Gales, assumiu a liderança nacional na implantação do reconhecimento facial automatizado. Após o investimento governamental de 2,6 milhões de euros para a implementação da tecnologia de reconhecimento facial, a força policial utilizou a tecnologia para fins de segurança pública em pelo menos 18 eventos de grandes proporções entre maio de 2017 e março de 2018. A primeira utilização ocorreu em junho de 2017, durante a partida final da UEFA Champions League, que ocorreu na cidade de Cardiff, capital do País de Gales. Dados divulgados pela organização policial galesa em 2018 mostraram que, de mais de 170.000 indivíduos presentes e 2.470 correspondências iniciais, 2.297

foram falsos positivos, isto é, cerca de 92% dos indivíduos detectados foram erroneamente atribuídos à falsas identificações (BIG BROTHER WATCH, 2018). A NEC, empresa por trás do algoritmo utilizado pela SWP, afirmou que listas de dados extensas tendem a gerar um alto número de falsos positivos. O chefe de soluções de reconhecimento facial da NEC Europa, Chris de Silva, comparou o resultado à um erro natural e humano, afinal "quantas vezes as pessoas já seguiram alguém na rua que pensavam ser alguém que conheciam, apenas para descobrir que não era essa pessoa?" (DUCKETT, 2017).

Nesse sentido, a Polícia de South Wales admitiu que "nenhum sistema de reconhecimento facial é 100% preciso", mas afirmou que a tecnologia levou a mais de 450 prisões entre 2017 e 2018, incluindo um indivíduo condenado a seis anos de prisão por roubo e outro condenado a quatro anos e meio por arrombamento para fins de roubo. No entanto, a força policial ignora os percentuais colossalmente maiores de falsos positivos com relação aos verdadeiros positivos que continuaram ocorrendo nos eventos seguintes, como as 46 pessoas erroneamente identificadas em uma luta de boxe de Anthony Joshua, em outubro de 2017, resultando em um total de 90% de falsos positivos; e as 42 pessoas falsamente identificadas no jogo de rugby Wales *vs* Australia, em novembro de 2017, somando um total de 87,5% falsos positivos (BURGESS, 2018).

Requerimentos de liberdade de informação solicitados pela Big Brother Watch (2018) à Polícia de South Wales revelaram que, entre maio de 2017 e março de 2018, menos de 9% (234) dos alertas emitidos pelo sistema de reconhecimento facial foram precisos, isto é, surpreendentes 91% dos alertas (2.451) foram responsáveis por dar falsa identificação a indivíduos inocentes do público. A investigação também revela que a Polícia de South Wales armazenou indiscriminadamente as fotos capturadas das correspondências de verdadeiros positivos e falsos positivos realizadas durante o período de 12 meses, isto é, ao menos 2.451 pessoas inocentes que tiveram seus rostos injustamente "combinados" foram mantidas nos bancos de dados policial sem o devido consentimento.

A partir de março de 2018, os cidadãos galeses foram submetidos a um controle de identidade e vigilância cada vez maior, quando a Polícia de South Wales anunciou que a TRF passaria a ser implementada não só em eventos controlados, como também no centro da cidade de Cardiff, afetando a livre locomoção de pedestres e transeuntes que optassem por não ter seu rosto escaneado. No mesmo mês, a força policial em questão utilizou o sistema de vigilância em uma

manifestação pacífica desarmamentista no lado de fora da Defense Procurement Research Technology Exhibition (DPRTE), em Cardiff, o principal evento de aquisição de defesa do Reino Unido. O caso chama atenção pela preocupação da força policial em utilizar seus esforços tecnológicos em um protesto pacífico de pequena proporção contra mecanismos de defesa violentos, demonstrando que, quando se trata de vigilância pública, "quem" importa mais do que "quantos", sobretudo quando esse "quem" é considerado um grupo problemático ou dissidente.

Contudo, toda a discussão levantada com relação a falta de acurácia e a violação do direito à privacidade e outras garantias civis de 2018 em diante não foi suficiente para cessar ou, ao menos, frear o uso incontido de sistemas de reconhecimento facial pelas forças policiais britânicas para fins criminais, ao contrário de grandes cidades, como São Francisco, Somerville e Oakland, nos Estados Unidos, que, no ano de 2019, aprovaram leis que proíbem o uso de reconhecimento facial por forças policiais. Indo na contramão dos casos de banimento da tecnologia, a Polícia Metropolitana de Londres gastou, entre 2016 e 2018, mais de 200 mil libras esterlinas para manter a tecnologia de reconhecimento facial em atividade – não resultando em nenhuma prisão bem-sucedida – e manteve a expansão do uso nos anos de 2019 e 2020 (DEADEN, 2019a).

Em 2019, dois casos envolvendo o uso da tecnologia chamam particular atenção. Em janeiro, na cidade de Londres, um homem foi abordado pela polícia depois de se opor a ser escaneado por câmeras de reconhecimento facial ao vivo e cobrir o rosto. O homem foi cercado por policiais e, ao protestar, recebeu uma multa de 90 libras esterlinas por uma suposta ofensa à ordem pública (DEARDEN, 2019b). No mesmo ano, também em Londres, um menino negro de 14 anos, em uniforme escolar, teve seu rosto erroneamente identificado por um sistema de reconhecimento facial. Consequentemente, o estudante foi cercado por quatro policiais à paisana, teve seus braços segurados e sua identidade questionada, sendo liberado apenas após dez inquisitórios minutos, quando a polícia percebeu que havia identificado a pessoa errada. Assustado, o rapaz afirmou ter se sentido assediado pela polícia (BIG BROTHER WATCH, 2020).

Foi também em 2019 que dois importantes estudos sobre a eficiência do uso da tecnologia por parte da Polícia Metropolitana de Londres surgiram. Em maio de 2019, requerimentos de liberdade de informação da organização Big Brother Watch revelaram que o uso de reconhecimento facial pela Polícia Metropolitana de Londres havia identificado membros do público incorretamente em 96% das vezes entre 2016 e 2018.

Por sua vez, os professores Pete Fussey e Daragh Murray, especialistas em vigilância da Universidade de Essex, localizada na cidade de Colchester, no Reino Unido, conduziram uma revisão independente do uso da tecnologia de reconhecimento facial por parte da Polícia Metropolitana de Londres. O estudo observou seis experiências cuja TRF foi utilizada pela Met, entre 2018 e 2019. Como resultado, descobriram que, de 42 indivíduos identificados pela força policial com o auxílio tecnológico, apenas 8 foram corretamente identificados –uma taxa de erro de 81% no total. Além disso, do montante total, 14 indivíduos foram abordados erroneamente e tiveram suas identidades questionadas (FUSSEY; MURRAY, 2019, p. 68-71). O estudo também apontou uma série de problemáticas na incorporação da tecnologia por parte da Met, entre elas, a carência de uma base legal explícita e a necessidade de incorporar efetivas considerações de direitos humanos em todas as etapas dos processos de tomada de decisão da força policial:

> As detailed in this report, it is highly possible that the LFR trial process adopted bt the MPS would be held unlawful if challenged before the courts. In particular, this report concludes that the implicit legal authorisation claimed by the MPS for the use of LFR - coupled with the absence of publicly available, clear, online guidance - is likely inadequate when compared with the 'in accordance with the law' requirement establised under human rights law. This demonstrates how the trialling or incorporation of new technology and policing practices is approached by the MPS, and underlines the need for the effective incorporation of human rights considerations into all stages of the MPS' decision making processes, including with respect to if, and how, trials should be undertaken. (FUSSEY, MURRAY, 2019, p. 5).

Os estudos, no entanto, não incutiram nenhum efeito imediato, já que em janeiro de 2020 a Polícia Metropolitana de Londres anunciou que iniciaria uma utilização ostensiva e em tempo real da tecnologia de reconhecimento facial na cidade. O objetivo inicial era implantar a ferramenta em locais com alto índice de criminalidade e violência. Em fevereiro de 2020, ausente o consentimento dos indivíduos presentes, a polícia londrina escaneou 8.600 rostos na Oxford Circus, uma das regiões comerciais mais movimentadas de Londres, resultando em sete falsas identificações e uma prisão. A força informou sobre o uso com apenas duas horas de antecedência. Conforme dados da Met apurados pelo Big Brother Watch, 86% dos alertas emitidos foram falsos-positivos e 71% das identificações incorretas resultaram na abordagem de indivíduos pela polícia e sua consequente necessidade de identificação (HAMILTON, 2020).

Ainda em fevereiro de 2020, a comissária da Polícia Metropolitana de Londres, Cressida Dick, rejeitou as críticas quanto ao reconhecimento facial representar ameaças à privacidade e às

liberdades civis, afirmando que críticos da tecnologia são mal informados (SIDDIQUE, 2020). Ressalta-se que dois anos depois, em fevereiro de 2022, a comissária renunciou ao cargo após o resultado de um relatório do Gabinete Independente de Conduta Policial (IOPC, em inglês), que revelou diversos casos de discriminação racial, misoginia, assédio sexual e antissemitismo por parte de agentes da corporação policial londrina, além da condenação de um agente a prisão perpétua pelos crimes de estupro e assassinato. O escândalo resultou em uma séria crise de confiança da população londrina em sua força policial, que, ao invés de protegê-la, envolveu-se em recorrentes acusações de abusos verbais e físicos em suas abordagens, além da cultura de discriminação racial e de gênero em algumas de suas unidades policiais. Como anteriormente debatido, é certo afirmar que a tecnologia é a soma do resultado dos indivíduos que a desenvolvem, a implementam e monitoram o seu uso, não podendo ser melhor ou pior do que os detentores do poder de controlá-la.

3.3. DIRETRIZES E BASES LEGAIS DO USO DE RECONHECIMENTO FACIAL NO REINO UNIDO

À medida que se observa a magnitude política do Reino Unido, uma das nações de maior desenvolvimento socioeconômico mundial e pioneira na utilização de sistemas de câmera de vigilância e reconhecimento facial no ocidente, imagina-se que esta seja exemplo na consolidação de bases legais, legislativas e regulatórias que compõem o uso apropriado da ferramenta, em cuidadosa observância a não violação das liberdades civis e dos princípios fundamentais inerentes ao ser humano, tais como a não discriminação. No entanto, em uma breve análise, é possível observar que, embora uma série de diretrizes legais e recomendações governamentais ou independentes sejam utilizadas como base legal e teórica em uma justificativa de garantia do exercício das atribuições legais das principais instituições governamentais que fazem uso da ferramenta para fins de segurança pública, não há uma regulação clara e específica quanto ao uso desses sistemas por essas instituições, além de que a correta fiscalização e autoavaliação de seu cumprimento é aquém do esperado.

No contexto da ausência de uma legislação britânica específica com relação ao uso de sistemas de reconhecimento facial para fins de vigilância pública, o Gabinete do Comissário de Câmeras de Vigilância do Reino Unido publicou, em novembro de 2020, um “guia de orientações e boas práticas para o uso policial de sistemas de câmera de vigilância ostensiva que utilizam

reconhecimento facial para localizar pessoas em listas de vigilância em espaços públicos na Inglaterra e no País de Gales". Nesse guia, estabeleceu-se a principal estrutura legal que sustenta o uso ostensivo da tecnologia de reconhecimento facial em locais públicos, sendo amplamente utilizada pelas forças policiais britânicas (SURVEILLANCE, 2020):

i) Common Law;
ii) Protection of Freedoms Act 2012;
iii) Surveillance Camera Code of Practice;
iv) Data Protection Act 2018;
v) Documentos das políticas das forças policiais que utilizam o reconhecimento facial para fins de vigilância.

Destaca o Comissário de Câmeras de Vigilância que as forças policiais britânicas devem ser transparentes e adequadamente explícitas quanto à base legal em que busca se basear para justificar sua conduta, devendo abordar esse ponto específico como parte de suas considerações ao estabelecer políticas (SURVEILLANCE, 2020).

Ainda, nota-se que o Parlamento do Reino Unido delegou ao Parlamento Escocês, ao Parlamento Galês e à Assembleia da Irlanda do Norte o poder de legislar, nos seus respectivos territórios, sobre matérias internas que não tenha reservado para si próprio.

3.3.1. PROTECTION OF FREEDOMS ACT 2012 E SURVEILLANCE CAMERA CODE OF PRACTICE

Nesse sentido, a primeira legislação a prever questões especificamente ligadas à vigilância pública e dados biométricos no contexto britânico foi a Protection of Freedoms Act 2012 (PoFa), de maio de 2012. O ato foi responsável por prever a destruição, retenção, uso e outras regulamentações de certos materiais probatórios, como impressões digitais e perfis de DNA; impor consentimento e outros requisitos em relação a certos processamentos de informações biométricas relacionadas a crianças; e fornecer um código de prática sobre sistemas de câmeras de vigilância. Ademais, foi responsável por estabelecer o cargo de Comissário de Câmeras de Vigilância, a ser nomeado pelo Ministro do Interior. Estabeleceu-se como papel do Comissário garantir a segurança dos cidadãos no uso dos sistemas de câmeras de vigilância (CFTV) em locais públicos. O mandato

do Comissário aplica-se à Inglaterra e País de Gales, e, em 2014, Tony Porter foi nomeado o primeiro Comissário para esse fim.

O Protection of Freedoms Act 2012 foi responsável por definir, pela primeira vez, o conceito de "sistemas de câmeras de vigilância", significado dado pela Seção 29, que incluiu, em seu texto: a) sistemas de circuito fechado de televisão (CFTV) ou sistemas de reconhecimento automático de placas; b) quaisquer outros sistemas para gravação ou visualização de imagens visuais para fins de vigilância; c) quaisquer sistemas para armazenar, receber, transmitir, processar ou verificar as imagens ou informações obtidas pelos itens 'a' ou 'b'; d) quaisquer outros sistemas associados ou de outra forma relacionados com os itens 'a', 'b' ou 'c'.

Conjuntamente, em junho de 2013, foi publicado pelo governo britânico o Surveillance Camera Code of Practice (SC Code), que passou a prever doze princípios orientadores quanto a utilização de sistemas de câmeras de vigilância. Na íntegra:

> 1. O uso de sistemas de câmeras de vigilância deve ser sempre para um propósito específico que persegue um objetivo legítimo e necessário para atender a uma necessidade premente identificada.
> 2. O uso de um sistema de câmeras de vigilância deve levar em conta seu efeito sobre os indivíduos e sua privacidade, com revisões regulares para garantir que seu uso seja justificado.
> 3. Deve haver a maior transparência possível no uso de um sistema de câmeras de vigilância, incluindo a publicação de um ponto de contato para acesso a informações e reclamações.
> 4. Deve haver clara responsabilidade e prestação de contas por todas as atividades do sistema de câmeras de vigilância, incluindo imagens e informações coletadas, mantidas e usadas.
> 5. Regras, políticas e procedimentos claros devem estar em vigor antes de um sistema de câmera de vigilância ser usado, e estes devem ser comunicados a todos que precisam cumpri-los.
> 6. Não devem ser armazenadas mais imagens e informações além daquelas estritamente necessárias para o propósito declarado de um sistema de câmeras de vigilância, e tais imagens e informações devem ser excluídas assim que seus propósitos forem cumpridos.
> 7. O acesso às imagens e informações retidas deve ser restrito e deve haver regras claramente definidas sobre quem pode obter acesso e para que finalidade esse acesso é concedido; a divulgação de imagens e informações só deve ocorrer quando for necessária para tal finalidade ou para fins de aplicação da lei.
> 8. Os operadores do sistema de câmeras de vigilância devem considerar quaisquer padrões operacionais, técnicos e de competência aprovados relevantes para um sistema e sua finalidade e trabalho para atender e manter esses padrões.
> 9. As imagens e informações do sistema de câmeras de vigilância devem estar sujeitas a medidas de segurança apropriadas para proteger contra acesso e uso não autorizados.
> 10. Deve haver mecanismos eficazes de revisão e auditoria para garantir que os requisitos legais, políticas e padrões sejam cumpridos na prática, e relatórios regulares devem ser publicados.

11. Quando o uso de um sistema de câmeras de vigilância for em busca de um objetivo legítimo, e houver uma necessidade premente de seu uso, ele deve ser utilizado da forma mais eficaz para apoiar a segurança pública e a aplicação da lei com o objetivo de processar imagens e informações de valor probatório.
12. Quaisquer informações usadas para dar suporte a um sistema de câmeras de vigilância que utilize um banco de dados de referência para fins de correspondência devem ser precisas e mantidas atualizadas. (HOME OFFICE, 2013, tradução nossa)

Esse feito, portanto, consolidou uma série de recomendações de base principiológica que auxiliaram as instituições públicas na utilização de sistemas de monitoramento e no fomento de boas práticas, representando um "marco legal" com relação às câmeras de vigilância pública, que, apesar de contarem com um documento governamental denominado CCTV Operational Requirements Manual 2009, ainda careciam de princípios bem definidos para além do operacional. Quando se analisa o fato de que sistemas de câmeras de vigilância passaram a ser utilizados no Reino Unido desde 1953, quando o governo britânico passou a implantar sistemas de circuito fechado de televisão para fins de segurança da Família Real, fica claro que tal ato ocorreu de forma bastante tardia, impulsionada pelo aumento da discussão na implementação de novas tecnologias de vigilância.

Apesar de fomentar uma interessante base legal para as câmeras de vigilância pública, o Surveillance Camera Code of Practice (HOME OFFICE, 2013, pp. 16; 21; 24) faz apenas três referências quanto à tecnologia de reconhecimento facial. Na primeira, tece que qualquer uso de reconhecimento facial ou outras ferramentas de reconhecimento de características biométricas deve ser claramente justificado e proporcionado para cumprir o objetivo declarado, devendo ser devidamente validado; e que o uso deve sempre envolver a intervenção humana, antes que sejam tomadas decisões que afetem um indivíduo adversamente. Na segunda, afirma que podem haver padrões adicionais aplicáveis quando o sistema possui recursos avançados específicos, como sistemas analíticos de vídeo ou sistemas de reconhecimento facial. Por fim, argumenta que qualquer uso de tecnologias, como sistemas de reconhecimento automático de placas de matrícula (ANPR) e ferramentas de reconhecimento facial que possam contar com a precisão das informações geradas em outros locais, como bancos de dados fornecidos por terceiros, não deve ser introduzido sem uma avaliação regular, para garantir que os dados subjacentes sejam adequados.

Observa-se que na época de publicação do Protection of Freedoms Act 2012 e do Surveillance Camera Code of Practice 2013, a utilização ostensiva da tecnologia de reconhecimento facial por parte das forças policiais britânicas para fins de vigilância em massa ainda não era uma realidade, tampouco o uso dessa tecnologia era o foco dessas diretrizes. Foi apenas em 2015 que o tema voltou para o cenário de vigilância policial, quando a Polícia de Leicestershire utilizou a TRF em um grande evento público na tentativa de encontrar indivíduos suspeitos ou foragidos, sendo a ação posteriormente seguida por outras forças policiais britânicas e rapidamente se espalhando pelo Reino Unido.

Nesse contexto, em setembro de 2017, quando a parlamentar Layla Moran submeteu uma pergunta escrita ao Ministério do Interior sobre a avaliação que ele faz da eficácia da legislação atual que regulamenta o uso de câmeras de vigilância com TRF, o até então ministro de Estado do Ministério do Interior do Reino Unido, Nick Hurd, respondeu o seguinte: "não há legislação que regule o uso de câmeras de vigilância com reconhecimento facial e recursos biométricos"[37]. Para contornar o caso, o ministro afirmou, em seguida, que "qualquer uso policial de reconhecimento facial deve ser justificado e proporcional ao propósito declarado", e que "a retenção policial de imagens faciais é regida pela legislação de proteção de dados e pela Prática Profissional Autorizada (*Authorised Professional Practice - APP*) do Colégio de Policiamento". Apesar da Prática Profissional Autorizada guiar as condutas profissionais dos agentes policiais da Inglaterra e do País de Gales, o guia não trazia orientações quanto a condução de sistemas de reconhecimento facial na segurança pública até então, deixando evidente a lacuna de uma orientação profissional clara e transparente quanto a uma ferramenta que já estava em vigente uso pelos seus agentes.

O documento governamental Review of the Use and Retention of Custody Images, publicado em fevereiro de 2017, estabeleceu que pessoas não condenadas por um crime têm o direito de solicitar que uma imagem de custódia seja excluída de todos os bancos de dados da polícia, com a presunção geral de que ela deve ser removida. Por sua vez, as imagens de custódia armazenadas de pessoas condenadas devem ser automaticamente revisadas pela polícia de acordo com os períodos de revisão de cronogramas estabelecidos na Prática Profissional Autorizada do Colégio de Policiamento (HOME OFFICE, 2017).

[37] Disponível em: https://questions-statements.parliament.uk/written-questions/detail/2017-09-04/8098/

Em março de 2018, o Presidente do Comitê de Ciência e Tecnologia do Parlamento do Reino Unido, Norman Lamb, afirmou que há uma abordagem insatisfatória para a retenção de imagens faciais em comparação com a abordagem usada para registros de DNA e impressões digitais, dessa forma, "o governo deve rever urgentemente sua abordagem e implementar processos adequados e infraestrutura digital" (UK PARLIAMENT, 2018).

A Polícia Metropolitana de Londres também reconheceu que "não existe uma estrutura legal específica para o uso desta tecnologia", e que o uso de sistemas de reconhecimento facial pela instituição tem como principal base legal o Protection of Freedoms Act 2012 e o Data Protection Act 2018 (BIG BROTHER WATCH, 2020). Em verdade, o Protection of Freedoms Act 2012 foi responsável por regular pela primeira vez o uso de câmeras de vigilância de CFTV em espaços públicos na Inglaterra e no País de Gales. No entanto, embora forneça uma diretriz legal para o uso de câmeras de vigilância pública, o ato não prevê de forma clara e específica o uso de sistemas reconhecimento facial para fins de vigilância em massa, tampouco acompanhou a evolução do uso da tecnologia no contexto britânico.

Por sua vez, em julho de 2018, após as recentes polêmicas do uso da tecnologia pela Polícia Metropolitana de Londres e pela Polícia de South Wales, o Painel de Ética Policial de Londres (LPEP) estabeleceu um relatório independente, denominado LPEP Report 2018, com um conjunto de recomendações de conduta para a Polícia Metropolitana de Londres, visando uma maior transparência e melhora na comunicação da instituição com os cidadãos londrinos. Entre as principais recomendações, determinou que as informações sobre os testes realizados sejam encontradas de forma rápida e fácil no site da instituição, garantindo o acesso à informação; que os locais de teste sejam selecionados para minimizar percepções de preconceito contra certas comunidades; que os indivíduos sejam informados que a recusa em ser escaneado não seria vista como motivo de suspeita e; como condição para continuar o uso, que a Polícia Metropolitana de Londres forneça informações sobre como tomará decisões futuras com relação à onde e quando a tecnologia será utilizada.

Entre outros, o caso do homem inglês que foi abordado e multado pela Polícia Metropolitana de Londres em janeiro de 2019 por cobrir seu rosto em zona onde o reconhecimento facial estava em uso é um exemplo de que, mesmo anos após a publicação das primeiras diretrizes quanto ao uso de câmeras de vigilância e seis meses após a publicação do relatório que previa que

a recusa em ser escaneado não seria considerada um motivo de suspeita contra o indivíduo, as recomendações não forneceram grandes mudanças na liberdade e no consentimento dos indivíduos com relação ao uso do aparato tecnológico (DEARDEN, 2019). Conforme observa o Instituto Igarapé (2018), o consentimento da comunidade quanto a vigilância em espaços públicos não pode ser simplesmente presumida, de forma que a força operadora do sistema deve imprimir esforços para sua obtenção.

3.3.2. DATA PROTECTION ACT 2018 E A DIRETIVA 2016/680 UE

Com relação a estrutura legal britânica de proteção de dados, o Data Protection Act 2018, legislação que substituiu o Data Protection Act 1998, não possui uma única menção à proteção de dados pessoais gerados pelo monitoramento facial em tempo real e o uso de bancos de dados por sistemas de reconhecimento facial para fins de vigilância pública. O ato se limita a definir o conceito de dados biométricos, sendo estes "os dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de um indivíduo, que permita ou confirme a identificação única desse indivíduo, como imagens faciais ou dados dactiloscópicos" (2018, p.122). Define, ainda, que os dados biométricos são considerados dados sensíveis, devendo, portanto, receber maior proteção.

Em escrito submetido pelo Comissário de Câmeras de Vigilância ao Comitê de Ciência e Tecnologia em março de 2019, afirma-se que o Data Protection Act 2018, por si só, não é capaz de fornecer uma base legal para o uso da tecnologia de reconhecimento facial nem a conclusão de uma Avaliação de Impacto de Proteção de dados (DPIA), fornecendo, nesse caso, apenas uma estrutura para a gestão dos dados recolhidos.

Por sua vez, em 2019, o Gabinete do Comissário de Informação (ICO) publicou um parecer sobre a utilização de reconhecimento facial ao vivo pelas forças policiais e esclareceu que seu uso é regido pela Parte 3 do Data Protection Act 2018, que abrange o processamento de dados para a execução da lei. No entanto, ressalta que o processamento de dados biométricos deve ser justo e possuir base na lei, de forma que sua justificativa legal seja clara e precisa. Além disso, exige-se, para que a tecnologia seja aplicada, o consentimento explícito do indivíduo ou o uso "estritamente

necessário" para fins de aplicação da lei. Esse último, no entanto, não deve fundamentar toda a prática policial, de forma que a força policial deve possuir um documento de política apropriado.

Ao passo que o uso desgovernado e sem consentimento de dados pessoais sensíveis não ser uma preocupação recente no ambiente das discussões acadêmicas e legislativas, foi apenas em maio de 2018 que o Regulamento Geral sobre a Proteção de Dados (RGPD; ou GDPR, em inglês), uma lei de proteção de dados válida para toda a União Europeia, intitulada Regulamento Geral sobre a Proteção de Dados (RGPD; ou GDPR, em inglês), entrou em vigor. Apesar de simbolizar um importante marco legal e fortalecer a luta dos cidadãos europeus e de organizações pelos direitos civis na transparência e no respeito à privacidade quanto ao manuseio de dados pessoais por instituições públicas e privadas, o Regulamento Geral de Proteção de Dados europeu não é responsável – e nem possui a pretensão – de servir como base legal específica na utilização de dados pessoais sensíveis por tecnologias de reconhecimento facial, quanto menos quando a sua utilização remete a fins de vigilância pública, questão que exige redobrada atenção quanto a sua regulação.

Nesse sentido, em 2016 o conselho da União Europeia estabeleceu a Diretiva 2016/680, responsável pela regulamentação do tratamento de proteção de dados pessoais por instituições públicas e privadas para fins de segurança pública. Entre seus principais feitos, a diretiva determinou, em seu art. 4º, os princípios orientadores do tratamento de dados sensíveis – como os princípios da segurança e integridade da informação, da necessidade, da finalidade e da transparência – no uso ostensivo da segurança pública.

Insta ressaltar que, com a saída do Reino Unido da União Europeia, a partir do dia 1º de janeiro de 2021, o processamento de dados realizado por empresas e instituições britânicas passou a não estar mais sujeito ao Regulamento Geral de Proteção de Dados (RGPD ou GDPR, em inglês), exceto se estas estiverem baseadas no Espaço Econômico Europeu ou processarem dados de europeus. Segundo o Gabinete do Comissário de Informação (ICO), autoridade independente do Reino Unido, a nova legislação doméstica de proteção de dados britânica, a UK GDPR, é uma versão similar à GDPR da União Europeia, mas o Reino Unido possui independência para manter a estrutura legislativa sob revisão. O Data Protection Act 2018 (DPA 2018), que atualmente complementa e adapta a GDPR no Reino Unido, portanto, continuará sendo aplicado.

Além disso, a Comissão Europeia adotou, no dia 28 de junho de 2021, duas decisões de adequação visando o Reino Unido: uma ao abrigo do Regulamento Geral sobre a Proteção de Dados e outra nos termos da Diretiva 2016/680, isto é, apesar do *brexit*, essas decisões de adequação da Comissão Europeia permitem que a maioria dos dados possam continuar a fluir da União Europeia e do Espaço Econômico Europeu sem a necessidade de proteções ou adequações adicionais, o que representa mais segurança para a legislação de proteção de dados britânica, visto que pode contar com a legislação tanto europeia quanto britânica para fomentar a proteção de seus cidadãos (EUROPEAN COMMISSION, 2021).

Salienta-se também que, em abril de 2021, a Comissão Europeia propôs um projeto de lei sobre o uso de inteligência artificial, incluindo a proibição da maioria das vigilâncias, em uma tentativa de estabelecer padrões globais da tecnologia-chave dominada pela China e pelos EUA (CHEE, 2021). A proposta, no entanto, permitiria que aplicações de inteligência artificial de alto risco fossem usadas em áreas migratórias e de maior "aplicação da lei", isto é, áreas cujo policiamento é mais ostensivo. O projeto também permitiria o uso dessas tecnologias em atividades governamentais. Em resposta, a Autoridade Europeia para a Proteção de Dados (AEPD) levantou o posicionamento de que o reconhecimento facial deveria ser proibido em atividades de vigilância pública, em face de sua profunda e não democrática intrusão na vida privada dos indivíduos. A AEPD também firmou a necessidade de uma abordagem mais rígida com relação ao uso de inteligência artificial e bancos de dados na persecução penal, dado que, em face de possíveis violações discriminatórias concedidas por erros em sua acurácia, a biometria facial apresenta riscos extremamente elevados aos direitos fundamentais dos indivíduos detectados.

3.3.3. O CASO ED BRIDGES V POLÍCIA DE SOUTH WALES

Na estrutura legal elencada pelo Comissário de Câmeras de Vigilância para regulamentar o uso de sistemas de reconhecimento facial no Reino Unido, o sistema de Direito – que no Reino Unido é representado pela *common law*, ou direito comum – figurava entre as bases legais amplamente aceitas para fundamentar o uso da tecnologia pelas instituições policiais. Nesse sentido, as sentenças proferidas pelas altas cortes do Reino Unido possuem especial papel na consolidação de precedentes e orientações jurídicas, que se desenvolvem conforme as complexas relações na sociedade também avançam.

Nesse sentido, o Reino Unido não contava com precedentes jurídicos que orientassem as tomadas de decisão institucionais com relação à utilização da tecnologia de reconhecimento facial na vigilância pública até o ano de 2018, quando Ed Bridges, morador de Cardiff, no País de Gales, desafiou o status quo presente até então e levou a Polícia de South Wales para a justiça, constituindo o considerado primeiro caso jurídico mundial enfrentado por uma instituição policial com base no seu uso da tecnologia.

O estopim para Bridges levar o caso adiante foi ter seu rosto escaneado duas vezes pelo sistema de vigilância da força policial galesa. A primeira vez teria sido em uma movimentada rua no centro da cidade de Cardiff, em dezembro 2017, e a segunda ocorreu quando participava de um protesto, em março de 2018, onde uma van com câmera de reconhecimento facial monitorava os manifestantes. De maio de 2017 a maio de 2019, a polícia de South Wales utilizou a tecnologia em pelo menos 70 oportunidades, que vão de eventos públicos ao policiamento de rotina, e pode ter obtido dados biométricos faciais sensíveis de mais de 500.000 pessoas sem o seu consentimento.

O principal argumento trazido pelo requerente, que foi representado judicialmente pela organização de direitos civis Liberty, reside na ausência de legalidade da ferramenta de controle e na violação das bases legais que regulamentam os direitos à igualdade, privacidade e proteção de dados, incluindo o artigo 8 da Convenção Europeia de Direitos Humanos – CEDH, que dispõe sobre o direito à privacidade. Segundo Bridges, sem aviso, a polícia utilizou a TRF invasivamente contra manifestantes pacíficos e outras milhares de pessoas em suas atividades diárias, sem fornecer uma correta explicação de como funciona e nenhuma oportunidade de consentimento. Ressalta, ainda, que o uso indiscriminado da tecnologia de reconhecimento facial pela polícia torna os seus direitos à privacidade inúteis, forçando os indivíduos a alterarem os seus comportamentos.

Em setembro de 2019, a Corte Superior[38] britânica decidiu que embora o reconhecimento facial interfira nos direitos de privacidade dos indivíduos detectados, a utilização de reconhecimento facial pela Polícia de South Wales não é considerada ilegal, pois sua estrutura legal oferece garantias suficientes. Na decisão, os juízes Haddon-Cave e Swift concluíram que o atual regime legal é adequado para "garantir o uso apropriado e não arbitrário da TRF" e que o uso da

[38] High Court, em inglês. É o terceiro mais alto tribunal do Reino Unido. Trata de casos cíveis e recursos de decisões proferidas em tribunais inferiores.

força da tecnologia até o momento tem sido consistente com os direitos humanos e as legislações de proteção de dados (REINO UNIDO, 2020b).

A defesa de Ed Bridges discordou e recorreu da sentença. Na apelação, alegou que a justificativa utilizada na sentença onde "não havia razão para a Polícia de South Wales ter percebido que qualquer software de TRF poderia operar de forma indiretamente discriminatória" é claramente inconsistente com as evidências apresentadas, tendo em vista o histórico de falsos positivos da força policial. Além disso, discordou da conclusão onde o uso da tecnologia de reconhecimento facial estava de acordo com o artigo 8 da CEDH e outras bases legais, e afirmou que está bem estabelecido o viés como uma característica comum dos sistemas de TRF, pois, como o Dr. Jain, especialista, afirma em seu relatório para a Corte: "o risco de haver diferenças significativas nas taxas de erro não é marginal ou trivial" (REINO UNIDO, 2020a, p. 21).

Por sua vez, em agosto de 2020, o Tribunal de Apelação[39] concordou com as alegações de defesa de Ed Bridges e anulou a decisão anterior, concluindo que o uso da tecnologia de reconhecimento facial pela Polícia de South Wales foi responsável por violar as bases legais britânicas de igualdade, privacidade e proteção de dados. O Tribunal considerou que havia "deficiências fundamentais" na estruturação legal e que os direitos de Bridges foram violados como resultado. Uma das principais fundamentações da decisão reside no fato de que a Polícia de South Wales nunca buscou se certificar, seja diretamente ou por meio de verificações independentes, de que o sistema de reconhecimento facial não possuía, no caso apresentado, um inaceitável viés racial e de gênero (REINO UNIDO, 2020a).

Sendo assim, a força policial de South Wales, mesmo aplicando a ferramenta há anos na detecção de rostos da população galesa, não possuía como uma de suas principais preocupações o impacto discriminatório da tecnologia de reconhecimento facial contra grupos minoritários, além de ter falhado em cumprir as obrigações previstas na lei quanto ao princípio da igualdade. A decisão, portanto, consolidou-se como um importante precedente e marco legal para novas ações jurídicas no Reino Unido e no mundo que vierem a questionar as violações – existentes ou iminentes – aos direitos fundamentais do indivíduo por meio de sistemas de reconhecimento facial.

[39] Court of Appeal, em inglês.

Como resultado da decisão, em novembro de 2021 a atualização do Surveillance Camera Code of Practice foi apresentada ao Parlamento do Reino Unido, de acordo com a Seção 31(3) do Protection of Freedoms Act 2012. Devido à aprovação parlamentar, o código atualizado entrou em vigor em 12 de janeiro de 2022. Em particular, o Comissário de Câmeras de Vigilância expressou que o Surveillance Camera Code of Practice está atualizado para fornecer orientações sobre o uso adequado de sistemas de câmeras de vigilância pelas autoridades locais e pela polícia, à luz das mudanças decorrentes do Data Protection Act 2019 e da decisão do caso Ed Bridges v Polícia de South Wales (2020). O resultado dessas mudanças, ainda recentes, deve ser acompanhado por organizações de liberdades civis, defensores dos direitos humanos, pesquisadores em privacidade e tecnologia e pelos cidadãos em geral, tendo em vista que o estrito cumprimento das previsões legais no uso da tecnologia de reconhecimento facial, para garantir a não violação de direitos pelas instituições que monopolizam o poder, deve estar em permanente observância.

CONCLUSÃO

A utilização de artefatos de controle no contexto da vigilância pública sempre esteve atrelada, entre outros, a um conceito de segurança – seja para muitos, seja para poucos. Para fins de segurança, no século XVIII, as prisões tomaram o protagonismo dos métodos punitivos na Europa e Bentham desenvolveu um dos modelos mais conhecidos de arquitetura de instituições de controle. Para fins de segurança, no século XIX, os criminólogos positivistas previam a separação de indivíduos considerados criminosos natos ou loucos do convívio social, a partir de prisões perpétuas, manicômios ou pena capital. Para fins de segurança, no século XX, Foucault demonstrou, num exercício de retomada da teoria panóptica, que o controle do homem não mais necessita de uma punição física, corporal, pois, para a gestão e disciplinamento do comportamento humano, a vigilância é um dos mecanismos mais eficazes. Para fins de segurança, no século XXI, observou-se um crescimento colossal nos mecanismos de poder aliados a novas tecnologias, em especial os registros biométricos e câmeras de vigilância com sistemas de reconhecimento facial, na medida que questões evidenciadas pela era pós-moderna – como o terrorismo e a crise imigratória – tornavam-se um progressivo distúrbio a ser solucionado.

À medida que mecanismos de punição e controle sempre existiram, dado que a história da sociedade é intrinsecamente ligada à dominação de povos e territórios para a manutenção do poder político, econômico e social, a tecnologia de reconhecimento facial se revelou não somente um mecanismo que, se bem utilizado, pode trazer benefícios para a sociedade (como para fins de otimização de diagnósticos médicos e identificação de doenças raras[40]), mas também um mecanismo que, quando utilizado para fins de segurança pública, pode trazer sérias consequências – como a violação do direito à igualdade, à privacidade, à livre locomoção e outros direitos e liberdades fundamentais – que ultrapassam qualquer benefício.

Uma questão observada é que, tal como os indivíduos que eram analisados pelos estudiosos da criminologia positivista – em especial Cesare Lombroso – e possuíam suas características catalogadas de acordo com uma classificação de perfil criminal, isto é, ter determinadas características fisionômicas e psicológicas designavam o nível de inocência e sanidade que um

[40] Para ver mais: RYAN, Joe. Reports of misogyny and sexual harassment in the Metropolitan Police. House of Commons Library. 1 mar. 2022.

indivíduo poderia vir a possuir, a tecnologia de reconhecimento facial, quando utilizada para propósitos de segurança pública, acaba por esbarrar em uma lógica similar.

Isso porque os indivíduos mormente procurados pelos sistemas de reconhecimento facial como criminosos foragidos, terroristas ou suspeitos são também os mesmos que constam nas bases de dados e fotos de custódia das forças policiais e instituições de segurança pública. Isto é, a tecnologia, tal como os estudos de Lombroso, que partem de uma lógica eficientista do crime, não é responsável por encontrar, em um contexto geral, indivíduos criminosos, mas sim indivíduos criminalizados, o que nos faz refletir sobre a quem interessa o desenvolvimento de tais mecanismos de poder.

Se, tal como Foucault observou a vigilância pode ser considerada um dos mecanismos mais eficazes da manutenção do poder disciplinar, importa observar que a implementação da tecnologia de reconhecimento facial pode, de igual modo, servir para a manutenção de um panoptismo moderno, isto é, ao invés do controle ocorrer somente por meio de barreiras físicas – como observado inicialmente no modelo panóptico de Bentham – mantem-se, na era pós-moderna, o controle dos indivíduos em qualquer lugar, limitando a locomoção e o espaço daqueles considerados indesejados. A mesma lógica não se aplica à cifra oculta, isto é, os milhares de crimes que não chegam ao conhecimento da polícia, dado que, para os sistemas de reconhecimento facial, importa reconhecer apenas aqueles indivíduos que já estão inseridos na máquina punitiva, ainda que isso signifique um alto índice de erros de identificação de indivíduos que possuem as características dos mais criminalizados – jovens, negros, imigrantes, entre outros.

Conforme comtemplou-se nos índices de falsos positivos e no resultado dos estudos relacionados à discriminação algorítmica, quanto mais o indivíduo se afasta do fenótipo de homem caucasiano (cujos índices de acerto são mais precisos), mais chances há da tecnologia de reconhecimento facial falhar em o reconhecer, o que ocorre sobretudo em face desses sistemas não possuírem uma base de dados diversificada e não ser desenvolvida, desde sua concepção, em observância a possíveis discriminações e violações à direitos fundamentais. A discriminação algorítmica não é uma discussão meramente no campo das possibilidades, pois, como observado, não há neutralidade tecnológica: a tecnologia de reconhecimento facial é desenvolvida por seres humanos e, como estes, possui defeitos.

É sob essa lógica de neutralidade tecnológica que o uso de sistemas de reconhecimento facial passou a ser aceito como uma alternativa à segurança pública em diversos países do mundo,

em especial no Reino Unido. Sob um fundamento utilitarista de combate ao crime, credita-se à tecnologia o dever de proteger os cidadãos "contra o mal'. Dentro dessa lógica eficientista, acredita-se que mais ferramentas de controle nas mãos das forças policiais resulta em mais eficiência contra o crime, e mais câmeras representa um maior nível de segurança do cidadão, afinal, segundo uma lógica comum, quem não deve não possuir o que temer. A lógica, no entanto, provou-se falha.

Nesse sentido, pode-se constatar que o Reino Unido possui um amplo histórico de vigilância, que vai da década de 1950, com a instalação das primeiras câmeras de circuito fechado de televisão, as recentes implementações de uso pelas forças policias britânicas, em especial as polícias de South Wales, no País de Gales, e a Polícia Metropolitana de Londres, na Inglaterra. No entanto, os resultados encontrados a partir de estudos realizados por instituições independentes e organizações de direitos civis com os dados apresentados pelas próprias forças policiais em relatórios de livre informação demonstraram taxas de erro entre 81% e 98% do número de indivíduos identificados, um número alarmante e que não pode ser ignorado.

Além disso, observou-se que o Reino Unido, apesar de possuir recomendações, guias de condutas e legislações para o uso de ferramentas de vigilância, principalmente as já conhecidas câmeras de CFTV, não possui uma base legal clara e robusta para permitir o uso de sistemas de reconhecimento facial por parte de suas forças policiais. O resultado disso, para além dos estudos que indicam a falta de precisão da ferramenta, provou-se principalmente na corte, onde o Tribunal de Apelação do Reino Unido considerou ilegal o uso de sistemas de TRF pela Polícia de South Wales, sobretudo pela instituição policial em comento não possuir diretrizes claras para impedir a violação a direitos fundamentais, como o direito à privacidade e o direito a não discriminação.

Por fim, salienta-se que é a radicalização dessa ideia de que nós podemos nos separar totalmente do perigo – o que não é verdade – que se desenvolvem ferramentas de poder e vigilância pública tais como a analisada no presente trabalho. Enquanto a tecnologia de reconhecimento facial for aplicada dentro de uma estratégia de controle seletivo e programado, que viabiliza a liberdade de alguns indivíduos em detrimento da paralisação de outros, inclusive inocentes, e que fortalece a criminalização de indivíduos que representam a maioria dentro dos presídios, não há que se pensar em uma perspectiva positiva do uso dessa tecnologia dentro do contexto da segurança pública.

Sugere-se, para fins de uma pesquisa futura, que seja analisado se novas diretrizes e bases legais que vierem a ser desenvolvidas após a decisão de Ed Bridges v. Polícia de South Wales com o fim de viabilizar, de forma segura e em respeito aos direitos estabelecidos na Convenção Europeia dos Direitos Humanos, a utilização da tecnologia no contexto da vigilância pública no Reino Unido. Espera-se que um eventual projeto regulatório da tecnologia de reconhecimento facial busque dialogar com a sociedade, entidades e organizações de direitos civis, a fim de reduzir ao máximo os riscos discriminatórios especialmente para fins de segurança pública, onde potenciais imprecisões podem vir a se tornar extremamente prejudiciais. Além disso, mostra-se necessário observar não somente o uso da tecnologia de reconhecimento facial após adquirida pelas instituições de poder, mas o desenvolvimento dessas tecnologias desde a sua concepção, isto é, desde a elaboração do algoritmo, do código e das bases de dados utilizadas. Para esse fim, sugere-se que a representatividade de indivíduos esteja inserida não só nos bancos de dados, de forma a reduzir imprecisões e aumentar a checagem de pontos cegos, mas também nas equipes de cientistas da computação, técnicos de dados, desenvolvedores de softwares entre outros responsáveis por dar vida à tecnologia.

REFERÊNCIAS

ADORNO, Theodor W.; HORKHEIMER, Max. **Dialética do Esclarecimento: fragmentos filosóficos.** Tradução de Guido Antônio de Almeida. Rio de Janeiro: Jorge Zahar, 1985.

AI HLEG. **Ethics Guidelines for Trustworthy AI**. European Commission. Abril 2019.

ANGWIN, J. et al. **How We Analyzed the COMPAS Recidivism Algorithm.** ProPublica. Maio 2016.

ANGWIN, J. et al. **Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks**. ProPublica. Maio 2016

ANITUA, Gabriel Ignacio. **Histórias dos pensamentos criminológicos.** Tradução Sérgio Lamarão. – Rio de Janeiro: Revan: Instituto Carioca de Criminologia, 2008.

ARTIACH, Pilar Fernandez. **El Trabajo de los Internos en Establecimientos Penitenciarios.** Tirant lo Blanch y Universitat de Valencia. 2006.

ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 02/2012 on Facial Recognition in Online and Mobile services.** 00727/12/EN WP 192. 22. Mar. 2012. Disponível em: <www.ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf> Acesso em: 30 mai. 2021.

ATICK, Joseph J.; GRIFFIN, Paul A.; REDLICH, A. Norman. Facelt: face recognition from static and live video for law enforcement. IN: **Human Detection and Positive Identification: Methods and Technologies.** Vol. 2932. Jan.1997, p. 176-187.

BARATTA, Alessandro. **Criminologia Crítica e Crítica do Direito Penal: introdução à sociologia do direito penal.** Tradução de Juarez Cirino dos Santos. Rio de Janeiro: Editora Revan: Instituto Carioca de Criminologia, 6ª edição, 2011. 2ª reimpressão, 2014.

BARRY-JESTER, Anna Maria; CASSELMAN, Ben; GOLDSTEIN, Dana. **The New Science of Sentencing. Should prison sentences be based on crimes that haven't been committed yet?** The Marshall Project, 2015.

BATISTA, André Filipe M; CHIAVEGATTO FILHO, Alexandre Dias P. Machine Learning aplicado à Saúde. In: ABRAHÃO, et al. **Livro de Minicursos [do] 19º Simpósio Brasileiro de Computação Aplicada à Saúde.** Sociedade Brasileira de Computação. Artur Ziviani, Natalia Castro Fernandes e Débora Christina Muchaluat Saade [Org]. Niterói: jun. 2019. p. 1-42.

BATISTA, Vera Malaguti. **Introdução Crítica à Criminologia Brasileira.** Rio de Janeiro: Editora Revan, 2011.

BAUMAN, Zygmunt. **Entrevista concedida a Fernando Schüler e Mário Mazzilli na Conferência Fronteiras do Pensamento.** Inglaterra, 25 de julho, 2011. Disponível em: <youtu.be/POZcBNo-D4A>. Acesso em: 03 mar 2022.

BAUMAN, Zygmunt. **Estranhos à Nossa Porta.** Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Ed., 2017.

BAUMAN, Zygmunt. **Globalização: as consequências humanas.** Tradução de Marcus Penchel. Rio de Janeiro: Jorge Zahar Ed., 1999.

BAUMAN, Zygmunt. **Vida para Consumo: a transformação das pessoas em mercadoria.** Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Jorge Zahar Ed., 2008.

BBC. **How we are being watched.** Nov. 2006. Disponível em: <www.news.bbc.co.uk/2/hi/uk_news/6110866.stm> Acesso em 16 ago. 2021.

BECCARIA, Cesare. **Dos Delitos e das Penas.** Tradução de Torrieri Guimarães. Hemus Editora. 1983.

BENENSON, Fred**. 'Mathwashing,' Facebook and the zeitgeist of data worship.** Entrevista concedida a Tyler Woods. Tecnical.ly. 8 jun. 2016. Disponível em: <www.technical.ly/brooklyn/2016/06/08/fred-benenson-mathwashing-facebook-data-worship/>. Acesso em 16 ago. 2021.

BENTHAM, Jeremy. **O Panóptico ou a Casa de Inspeção.** In: SILVA, Tomaz Tadeu da (org.). O Panóptico. Traduções de Guacira Lopes Louro; M. D. Magno; Tomaz Tadeu. 2. ed. Belo Horizonte: Autêntica Editora, 2008.

BIG BROTHER WATCH. **Big Brother Watch Briefing on facial recognition surveillance.** Londres: jun. 2020.

BIG BROTHER WATCH. **Face Off. The lawless growth of facial recognition in UK policing**. Londres: maio 2018.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal: parte geral, 1.** São Paulo, Saraiva, 2011.

BLEDSOE, W. W. **The Model Method in Facial Recognition**, Technical Report PRI 15, Panoramic Research, Inc., Palo Alto, California. 1964.

BLEDSOE, W. W.; CHAN, H. **A Man-Machine Facial Recognition System-Some Preliminary Results**, Technical Report PRI 19A, Panoramic Research, Inc., Palo Alto, California. 1965.

BLEDSOE, W. **Man-Machine Facial Recognition: Report on a Large-Scale Experiment**. Technical Report PRI 22, Panoramic Research, Inc. 1966a.

BLEDSOE, W. **Some Results on Multicategory Patten Recognition.** Journal of the Association for Computing Machinery. Volume 13. Edição 2. 1966b.

BOCCIA, Yoram, et al. **History of Facial Recognition.** Facial Recognition, Imperial College London, 2017.

BOWER, J. L., and C. M. CHRISTENSEN. **Disruptive Technologies: Catching the Wave**. Harvard Business Review 73, no. 1. 1995, p. 43–53.

BREY, Philip. **Ethical aspects of facial recognition systems in public places.** Journal of Information, Communication and Ethics in Society, 2(2), 2004, p. 97–109.

BROUSSARD, Meredith. **Artificial Unintelligence: How Computers Misunderstand the World.** MIT Press, 2018.

BUOLAMWINI, Joy. **How I'm fighting bias in algorithms**. TEDxBeaconStreet. Nov. 2016. Disponível em: <www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms>. Acesso em: 29 ago. 2021.

BUOLAMWINI, Joy; GEBRU, Timnit. **Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification.** Proceedings of Machine Learning Research, 2018.

BURGESS, Matt. **Facial recognition tech used by UK police is making a ton of mistakes.** Wired. 4 maio 2018. Disponível em: <www.wired.co.uk/article/face-recognition-police-uk-south-wales-met-notting-hill-carnival>. Acesso em: 13 abr. 2022.

CARLO, Silkie. **Britain Has More Surveillance Cameras Per Person Than Any Country Except China. That's a Massive Risk to Our Free Society.** Time. 2019. Disponível em: <time.com/5590343/uk-facial-recognition-cameras-china/>. Acesso em: 30 mar. 2022.

CARRARA, Francesco. **Programa del Curso de Derecho Criminal.** Parte General. tr. del italiano por Octavio Béeche Arguello y Alberto Gallegos Pacheco. 1ª Ed. San José, C. R: Editorial Jurídica Continental, 2000.

CARRARA, Francesco. **Programa do Curso de Direito Criminal.** Parte geral. Tradução por José Luiz V. de A. Fransceschini e J.R. Prestes Barra. São Paulo: Saraiva, 1956.

CARVALHO, Salo de. **Reprobalidade e segregação: as rupturas provocadas pela antipsiquiatria nas Ciências Criminais** in: LIMA, Joel Corrêa de; CASARA, Rubens R. R., Temas para uma perspectiva crítica do Direito: Homenagem ao Professor Geraldo Prado. Rio de Janeiro: Lumen Juris, 1ª ed., 2010.

CASTRO, Edgardo. **Introdução a Foucault**. Tradução de Beatriz de Almeida Magalhães. Belo Horizonte: Autêntica Editora, 1ª ed, 2014.

CHEE, Foo Yun. **EU privacy watchdogs call for ban on facial recognition in public spaces.** Reuters. Jun 2021. Disponível em: <www.reuters.com/technology/eu-privacy-watchdogs-call-ban-facial-recognition-public-spaces-2021-06-21/. Acesso em: 7 abr. 2022.

CHIRINOS, A. **Finding the Balance between Liberty and Security: The Lord's Decision on Britain's Anti-terrorism Act.** Harvard Human Rights Journal, 18, 2005, p. 265-276.

CIRINO DOS SANTOS, Juarez. **Criminologia e Luta de Classes.** Instituto de Criminologia e Política Criminal. 2015.

DEARDEN, Lizzie. **UK's largest police force spends over £200,000 on facial recognition trials that resulted in no arrests**. 19 jan. 2019a. Disponível em: <www.independent.co.uk/news/uk/home-news/facial-recognition-uk-police-met-arrests-london-cost-false-positives-accuracy-a8723756.html>. Acesso em: 6 abr. 2022.

DEARDEN, Lizzie. **Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested.** The Independent. 31 jan. 2019b. Disponível em: <www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html>. Acesso em: 7 abr. 2022.

DEVLIN, Hannah. **We are hurtling towards a surveillance state: the rise of facial recognition technology.** The Guardian. 5 out. 2019. Disponível em: <www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state>. Acesso em: 6 abr. 2022.

DIAMANDIS, Peter H.; KOTLER, Steven. **Abundance: the Future Is Better than You Think**. Free Press, 2012.

DIAMANDIS, Peter H.; KOTLER, Steven. **Bold: How to Go Big, Create Wealth and Impact the World.** New York: Simon & Schuster, 2015.

DRESSEL, J. FARID, H. **The accuracy, fairness, and limits of predicting recidivism.** Sci. Adv. 4, 2018.

DUARTE, Evandro Piza. **Paradigmas em criminologia e relações raciais.** Cadernos do CEAS, Salvador, n. 238, 2016, p. 500 –526.

DUCKETT, Chris. **Too many false alarms for population-wide facial surveillance: NEC.** ZD Net. 24 out. 2017. Disponível em: <www.zdnet.com/article/too-many-false-alarms-for-population-wide-facial-surveillance-nec/>. Acesso em: 13 abr. 2022.

EIJKMAN, Q. A., & WEGGEMANS, D. **Visual surveillance and the prevention of terrorism: What about the checks and balances?** International Review of Law, Computers & Technology. 2011, p. 143-150.

EIJKMAN, Q. **Preventive counter-terrorism and non-discrimination assessment in the European Union.** Security and Human Rights. 2011, p. 89-101.

EUROPEAN COMMISSION. **Data protection: Commission adopts adequacy decisions for the UK**. European Commission. Brussels, 28 jun. 2021.

FERREIRA, Leonardo Tajes. **A mudança no direito moderno no Brasil a partir do debate das relações morais do "mundo da vida".** Revista Debates Insubmissos. Caruaru, PE, Brasil, Ano 3, v. 3, nº 11, set/dez. 2020.

FOUCAULT, Michel. **A ordem do discurso: aula inaugural no Collège de France, pronunciada em 2 de dezembro de 1970.** Tradução de Laura Fraga de Almeida Sampaio. São Paulo: Edições Loyola, 3ª ed., 1996.

FOUCAULT, Michel. **Em defesa da sociedade: Curso no Collège de France (1975-1976).** Org. de Mauro Bertani e Alessandro Fontana. Trad. de Maria Ermantina Galvão. São Paulo: Martins Fontes, 2005, p. 285-315.

FOUCAULT, Michel. **Vigiar e Punir. Nascimento da Prisão.** Tradução de Raquel Ramalhete. Editora Vozes, 20ª Edição. Petrópolis, 1999.

FRANCISCO, Pedro Augusto P.; HUREL, Louise M.; RIELLI, Mariana M. **Regulação do reconhecimento facial no setor público: avaliação de experiências internacionais.** Instituto Igarapé e Data Privacy Brasil. Jun. 2020.

FRIEDMAN, Batya; NISSENBAUM, Helen. **Bias in Computer Systems.** ACM Transactions on Information Systems, Vol. 14, No. 3, jul. 1996, p. 330–347.

FUSSEY, Peter; MURRAY, Daragh. **Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology**. Project Report. University of Essex Human Rights Centre. 2019.

GARCIA, Megan. **Racist in the Machine: The Disturbing Implications of Algorithmic Bias**. World Policy Journal 33, no.4. Duke University Press. 2016.

GARVIE, Clare; BEDOYA, Alvaro; FRANKLE, Jonathan. **The Perpetual Line-up. Unregulated Police Face Recognition in America.** Center on Privacy & Technology, 2016.

GARVIE, Clare; FRANKLE, Jonathan. **Facial-Recognition Software Might Have a Racial Bias Problem.** Atlantic, 2016.

GATES, Kelly A. **Our biometric future: facial recognition technology and the culture of surveillance.** New York University Press. 2011.

GATES, Kelly. **The Past Perfect Promise of Facial Recognition Technology**. Institute of Communications Research. University of Illinois. Urbana-Champaign. Jun. 2004.

GOMES, Luiz Flávio. **Direito penal, v. 1. Introdução e princípios fundamentais.** São Paulo. Revista dos Tribunais, 2007.

HAMILTON, Isobel Asher. **British police scanned 8,600 people's faces in London without their consent, resulting in just 1 arrest and 7 false positives**. Insider. 4 mar. 2020. Disponível em: <https://www.businessinsider.com/met-police-scans-8600-faces-resulting-in-1-arrest-2020-3> Acesso em: 10 abr. 2022.

HARVEY, Adam E. **CV Dazzle.** Photography and visualization of face detection software. 2020.

HARVEY. Adam E. **HyperFace Prototype.** Rendering by Ece Tankal, 2017. Disponível em: <www.ahprojects.com/hyperface/>. Acesso em: 12 jul. 2021.

HOLDER, Jr. Eric H. **Attorney General Eric Holder Speaks at the National Association of Criminal Defense Lawyers 57th Annual Meeting and 13th State Criminal Justice Network Conference.** Ago. 2014. Disponível em: www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-national-association-criminal-defense-lawyers-57th. Acesso em: 12 jul. 2021.

HOME OFFICE. **Review of the Use and Retention of Custody Images.** Londres: fev. 2017.

HOME OFFICE. **Surveillance Camera Code of Practice.** Presented to Parliament Pursuant to Section 30 (1) (a) of the Protection of Freedoms Act 2012. Londres: jun. 2013.

HOWARD, John. **The State of the Prisons in England and Wales.** Warrington, 1777, p. 236 – 237.

INFORMATION COMMISSIONER'S OFFICE. **Information Commissioner's Opinion: The use of live facial recognition technology by law enforcement in public places.** 31 out. 2019.

INNES, Joanna. Prisons for the Poor: English Bridewells, 1555-1800. IN: SNYDER, F; HAY, D. eds, **Labour, Law and Crime: an historical perspective**. 1987.

INTRONA, Lucas D. NISSENBAUM, Helen. **Facial Recognition Technology. A Survey of Policy and Implementation Issues.** CCPR. New York University. 2009.

INTRONA, Lucas D. WOOD, David. **Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems.** Surveillance & Society. CCTV Special. Eds. Norris, McCahill and Wood. 2002.

JOHNSON, R.; BONSOR, K. **How Facial Recognition Systems Work**. How stuff works. 9 mar. 2006.

JOSEPH, George. LIPP, Kenneth. **IBM used NYPD Surveillance Footage to develop technology that lets police search by skin color.** The Intercept. Set. 2018.

KAISER, Brittany. **Manipulados: como a Cambridge Analytica e o Facebook invadiram a privacidade de milhões e botaram a democracia em xeque.** Ed. HarperCollins. 1ª ed., 2019.

KESARI, Ganes. How AI Is Using Facial Detection To Spot Rare Diseases In Children. **Forbes.** 29 mar. 2022. Disponível em: <www.forbes.com/sites/ganeskesari/2022/03/29/how-ai-is-using-facial-detection-to-spot-rare-diseases-in-children/> Acesso em: 24 abr. 2022.

KIRBY, M.; SIROVICH, L. **Application of the Karhunen-Loeve procedure for the characterization of human faces.** IEEE Trans. Patt. Anal. Mach. Intelli. 2 (1), 103108. 1990.

KLARE ET AL. **Face Recognition Performance: Role of Demographic Information.** IEEE Transactions on Information Forensics and Security. Dez. 2012.

KRANZBERG, Melvin. **Technology and History: Kranzberg's Laws.** Tech Culture, v. 27, n. 3. 1986.

LACCHÈ, Luigi. **Un Code Pénal Pour l'Unité Italienne: le code Zanardelli (1889) – La Genèse, le Débat, le Projet Juridique.** Sequência (Florianópolis), n. 68. Jun. 2014, p. 37–57.

LAPLAZA, Francisco. **Francesco Carrara. Sumo Maestro del Derecho Penal.** Buenos Aires, Depalma, 1950.

LOMBROSO, Cesare. **O Homem Delinquente.** Tradução Sebastião José Roque – São Paulo: Ícone. Coleção Fundamentos do Direito. 2007. 1ª reimpressão, 2010.

LONDON POLICING ETHICS PANEL. **Interim Report on Live Facial Recognition.** Jul. 2018. Disponível em:

<www.policingethicspanel.london/uploads/4/4/0/7/44076193/lpep_report_-_live_facial_recognition.pdf>. Acesso em: 16 abr. 2022.

LOPES, Ana Isabel; SANTOS, Sónia. **Da Sociedade disciplinar à Sociedade de Controle.** Coordenação de Olga Pombo. Faculdade de Ciências da Universidade de Lisboa, 2001.

LUCENA, Pedro Arthur Capelari de. **Policiamento Preditivo, discriminação algorítmica e racismo: potencialidades e reflexos no Brasil.** VI Simpósio Internacional LAVITS 2019. Assimetrias e (in)visibilidades: vigilância, gênero e raça. Salvador, 2019.

LUM, Kristian; ISAAC, William. **To predict and serve?** Royal Statistical Society, 7 out. 2016.

LYDICK, Neil. **A Brief Overview of Facial Recognition.** University of Michigan, 4 apr. 2007.

LYNCH, J. **Face Off: Law Enforcement Use of Face Recognition Technology.** San Francisco: Electronic Frontier Foundation, 2018.

MASTERMAN, J. C. **The Double-Cross System in the War of 1939 to 1945**. Australian National University Press. Canberra: 1972.

MATHIESEN, Thomas. **The Viewer Society: Michel Foucault's 'Panopticon' revisited.** Theoretical Criminology, v. 1, n. 2, 1997, p.215–234.

MCCARTHY, John. **What is artificial intelligence?** Stanford, 2007. Disponível em: <www-formal.stanford.edu/jmc/whatisai.pdf> Acesso em: 30 mar. 2021.

MEEK, James. **Robo cop.** The Guardian. 13 jun. 2002. Disponível em: <www.theguardian.com/uk/2002/jun/13/ukcrime.jamesmeek>. Acesso em: 6 abr. 2022.

MILAZZO, Bernardo Luiz M. Imperialismo e Romanização: Britânia Romana e Camulodunum. IN: **Roma e as sociedades da antiguidade: política, cultura e economia.** Maria Regina Candido (org.) - Rio de Janeiro: NEA/UERJ, 2008, p. 9-14.

MILLER, Jacques-Alain. A Máquina Panóptica de Jeremy Bentham. Tradução de M. D. Magno. IN: BENTHAM, Jeremy. **O Panóptico.** Organização de Tomaz Tadeu. Traduções de Guacira Lopes Louro; M. D. Magno; Tomaz Tadeu. 2. ed. Belo Horizonte: Autêntica Editora, 2008.

MOTTA, Fernando C. Prestes; ALCADIPANI, Rafael. **O pensamento de Michel Foucault na teoria das organizações.** R. Adm., São Paulo, v.39, n.2, abr./maio/jun. 2004, p.117–128.

OPENCV. **FaceRecognizer - Face Recognition with OpenCV.** OpenCV 2.4.13.7 documentation. 2016.

O'REILLY, Tim. **What is Web 2.0: design patterns and business models for the next generation of software.** O'Reilly Media, Inc. 30 set. 2005.

OSOBA, Osonde; WELSER IV, William. **An intelligence in our image.** Santa Mônica: RAND Corporation, 2017.

PARISER, Eli. **The Filter Bubble: What the Internet Is Hiding from You.** London: Penguin Press. 2011.

PHILLIPS, Jonathon P.; et al. **An Other-Race Effect for Face Recognition Algorithms.** ACM Trans. Appl. Percept. 8, 2, Article 14. 2011.

PORTER, Tony. **Speech to Security Twenty 15.** Security Twenty 15 conference. Newcastle: 10 jul. 2015. Disponível em: <www.gov.uk/government/speeches/speech-to-security-twenty-15> Acesso em: 8 abr. 2022.

POWER, Carol. **Big Brother is watching and analysing.** The Irish Times. 7 set. 2001. Disponível em: <www.irishtimes.com/business/big-brother-is-watching-and-analysing-1.326273>. Acesso em: 6 abr. 2022.

QUATTROCOLO, Serena. **An introduction to AI and criminal justice in Europe.** Rev. Bras. de Direito Processual Penal, Porto Alegre, vol. 5, n. 3, set-dez. 2019, p. 1519–1554.

REINO UNIDO. **General Data Protection Regulation.** GDPR Advisor. 2022. Disponível em: <https://uk-gdpr.org/>. Acesso em: 16 abr. 2022.

REINO UNIDO. **R (on the application of Edward Bridges) v The Chief Constable of South Wales Police. UK Court of Appeal (Civil Division) C1/2019/2670**; EWCA Civ 1058 [210]. Ago, 2020b. Disponível em: </www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment-1.pdf>. Acesso em: 14 abr. 2022.

REINO UNIDO. **R (on the application of Edward Bridges) v The Chief Constable of South Wales Police. UK Court of Appeal. Appellant's Replacement Skeleton Argument.** 2 abr. 2020a. Disponível em: <http://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Appellants-Skeleton-Argument-in-the-Court-of-Appeal.pdf>. Acesso em: 14 abr. 2022.

REINO UNIDO. **Data Protection Act 2018** (c. 12). UK Public General Acts.

RUSSELL, Stuart J.; NORVIG, Peter. **Inteligência Artificial**, 3ª ed, Trad. Regina Célia Simille. Elsevier. Rio de Janeiro: 2013.

RYAN, Joe. **Reports of misogyny and sexual harassment in the Metropolitan Police.** House of Commons Library. 1 mar. 2022.

SABBATINI, Renato M.E. **Frenologia: A História da Localização Cerebral.** Centro de Informática Biomédica. Universidade Estadual de Campinas. Revista Cérebro & Mente No. 1, mar/maio 1997.

SHARIF, et al., **Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition.** Pittsburgh, PA, USA. 2016.

SHECAIRA, Sérgio Salomão. **Criminologia.** São Paulo: Editora Revista dos Tribunais, 2011.

SIDDIQUE, Haroon. **Met police chief: facial recognition technology critics are ill-informed.** The Guardian. 24 fev. 2020. Disponível em: <www.theguardian.com/technology/2020/feb/24/met-police-chief-cressida-dick-facial-recognition-technology-critics-ill-informed>. Acesso em: 11 abr. 2022.

SILVA, Tarcízio. **Visão Computacional e Vieses Racializados: Branquitude como Padrão no Aprendizado de Máquina.** Anais do II Congresso de Pesquisadores/as Negros/as do Nordeste - COPENE. João Pessoa, Paraíba, 2019.

SURVEILLANCE CAMERA COMMISSIONER. **Facing the Camera.** Nov. 2020. Disponível em:<https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940386/6.7024_SCC_Facial_recognition_report_v3_WEB.pdf>. Acesso em: 16 abr. 2022.

SURVEILLANCE CAMERA COMMISSIONER. **Review of the impact and operation of the Surveillance Camera Code of Practice.** Fev. 2016. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/502893/Draft_Review_FINAL.pdf> Acesso em: 8 abr. 2022.

TISTARELLI, M., LI, S. Z., & Chellappa, R. **Handbook of Remote Biometrics. Advances in Pattern Recognition.** 2009.

TREVISOL, Joviles Vitório. **A dimensão humana da globalização.** Plural; Sociologia, USP. São Paulo, 2000.

TRINDADE, Gabriel Garmendia da; NUNES, Lauren de Lacerda. **Resenha O Panóptico/Jeremy Bentham.** Problemata: Rev. Int. de Filosofia. Vol. 02. n. 02. 2011, p. 343–349.

TURING, A. M. **Computing Machinery and Intelligence**, Mind, Volume LIX, Issue 236, Out. 1950, p. 433–460.

TURK, M.; PENTLAND, A. **Eigenfaces for recognition.** Journal of Cognitive Neuroscience 3, nº 1, 1991, p. 71–86.

WERMUTH, Maiquel. **Política criminal atuarial: contornos biopolíticos da exclusão penal.** Rev. Direito e Práx., Rio de Janeiro, Vol. 08, N. 3, 2017, p. 2043-2073.

WILMER et. al. **Human face recognition ability is specific and highly heritable.** Proceedings of the National Academy of Sciences. 2010.

Woodward, John D., et al. **Biometrics: A Look at Facial Recognition.** Santa Monica, CA: RAND Corporation, 2003.

YAMADA, T. GOHSHI, S. ECHIZEN, I. **Privacy Visor: Method Based on Light Absorbing and Reflecting Properties for Preventing Face Image Detection**, IEEE International Conference on Systems, Man, and Cybernetics, 2013, p. 1572–1577.

ZACKSESKI, Cristina. Capítulo 1 - A Criminologia Crítica e a Política Criminal Alternativa diante do desafio da segurança urbana. (p. 19-66). IN: ZACKSESKI, Cristina. **A Construção do Conceito de Ordem Pública nas Políticas de Segurança dos Distritos Federais do Brasil e do México (1908 – 2005)**. 400 f., il. Tese (Doutorado em Ciências Sociais) - Universidade de Brasília, Brasília, 2006.

ZACKSESKI, Cristina; DUARTE, Evandro Piza. **Garantismo e Eficientismo Penal: Dissenso e convergência nas políticas de segurança urbana.** Anais do XXI Encontro Nacional do CONPEDI UFU, 7112-7143. Florianópolis: 2012.

ZAFFARONI, Eugenio Raúl; et al. **Direito Penal Brasileiro: primeiro volume – Teoria Geral do Direito Penal**, Rio de Janeiro: Revan, 2003, 4ª edição, 2011. 3ª reimpressão, 2017.

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. **Manual de Direito Penal Brasileiro [livro eletrônico]: Parte Geral.** 14. ed. -- São Paulo: Thomson Reuters Brasil, 2021.

ZIMMER, Marco Vinício. **O Panóptico está superado? Estudo etnográfico sobre a vigilância eletrônica.** Tese de Doutorado apresentada ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande do Sul. Orientador Prof. Dr. Norberto Hoppen. Porto Alegre: 2009.