ARTIGO “O sistema europeu de reconhecimento facial: o dispositivo banóptico e as novas faces do positivismo”

ARTICLE “The European facial recognition system: the banoptic device and the new faces of positivism”.

Augusto Jobim do Amaral[1]

Gabriel Saad Travassos[2]

Resumo: A Europa estabeleceu, recentemente, um novo regime para a captura, o armazenamento e o compartilhamento de dados de imagens faciais, estruturado a partir do Regulamento Prum II. O artigo tem como problema de pesquisa analisar como este regime remasteriza estratégias do positivismo criminológico, desenvolvendo uma governamentalidade banóptica com bases discriminatórias. O método é hipotético-dedutivo e, a partir da pesquisa qualitativa, avalia a hipótese de que o sistema de vigilância europeu investe no policiamento dos corpos em um regime de inquietação e mal-estar permanente próprio de um novo tipo de governamentalidade. A discriminação algorítmica produzida pelas tecnologias de reconhecimento facial corporifica a ameaça e submete determinados perfis às lógicas do dispositivo banóptico. Com base na revisão bibliográfica, na pesquisa documental e no estudo de caso, analisamos este novo regime tecnopolítico criminal.

Palavras-chave: Sistema europeu de reconhecimento facial. Governamentalidade. Dispositivo Banóptico. Discriminação algorítmica.

Abstract: Europe recently established a new regime for the capture, storage and sharing of facial image data, based on the Prum II Regulation. The article's research problem is to analyze how this regime remasters strategies of criminological positivism, developing a banoptic governmentality with discriminatory bases. The method is hypothetical-deductive and, supported on qualitative research, evaluates the hypothesis that the European surveillance system invests in policing on the bodies in a regime of permanent unrest and unease typical of a new type of governmentality. The algorithmic discrimination produced by facial recognition technologies embodies the threat and subjects certain profiles to the logic of the banoptic device. Based on the literature review, documentary research and case study, we analyze this new criminal techno-political regime.

Keywords: Europeuan facial recognition system. Governmentality. Banoptic device. Algorithmic discrimination.

[1] Professor do Programa de Pós-Graduação em Ciências Criminais e do Programa de Pós-Graduação em Filosofia, ambos da PUC-RS. augusto.amaral@pucrs.br.

[2] Doutorando em Ciências Criminais (PUC-RS). Mestre em Direito e Justiça Social (FURG). Defensor Público Federal. travassosgabrielsaad@gmail.com.

INTRODUÇÃO

Estima-se que o mercado de tecnologias de reconhecimento facial movimentará 8,5 bilhões de dólares em 2025. Pesquisa conduzida por Paul Bischoff aponta que sete em cada dez países já se utilizam de tecnologias de reconhecimento facial em larga escala, com usos em espaços variados como aeroportos, estações de metrô, instituições bancárias e até mesmo em escolas[3].

A Agência da União Europeia para a Cooperação Policial (Europol) desenvolve atualmente um sistema europeu de base de dados de reconhecimento facial[4], agora normatizado pelo Regulamento n. 2024/982, do Parlamento Europeu e do Conselho, de 13 de março de 2024, conhecido como Regulamento de Prum II.

O artigo tem como problema de pesquisa analisar em qual medida o novo regime está inserido em uma linha de continuidade própria da modernidade e do positivismo criminológico, estruturando a governamentalidade a partir do dispositivo banóptico como método de gestão diferenciada da circulação.

Na primeira seção apresentamos o novo regime de controle no espaço europeu e as suas ligações com o positivismo criminológico e a biopolítica. Em seguida, analisamos em que medida esse regime se aproxima do conceito de dispositivo banóptico de que trata Didier Bigo.

Compreender esse dispositivo no cerne do policiamento global pautado pelo excepcionalismo e contenção de migrantes permitirá entender como a discriminação sistêmica é funcional à produção da liberdade no neoliberalismo. Assim, as violações de direitos humanos são assumidas como danos colaterais em prol de uma ideia de liberdade que é ativamente produzida como técnica política e forma de subjetividade.

O método é hipotético-dedutivo e, a partir da pesquisa qualitativa, avalia a hipótese de que o sistema de vigilância europeu normatiza um dispositivo banóptico que produz a liberdade a partir da discriminação algorítmica que, nesse diagrama, revela-se inerente ao

[3] BISCHOFF, Paul. **Facial recognition technology (FRT):** 100 countries analyzed. Comparitech, 24.Jan.2022. Available at: https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/#:~:text=Five%20countries. Access 25.02.2024.

[4] EUROPEAN UNION. EUROPEAN COMISSION. **The Commission welcomes the political agreement on automated data exchange for police cooperative**. Press release. 20.nov.23. Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5870. Acesso 17.06.2024.

modelo de policiamento dos corpos no espaço europeu. O paradoxo é evidenciado ao analisarmos, por meio do estudo de caso, o entendimento do órgão judicial da União Europeia para a interpretação dos direitos humanos.

Com base na revisão bibliográfica, na pesquisa documental e no estudo de caso, analisamos o novo regime no contexto da política criminal de excepcionalismos. A conclusão aponta para a necessidade de uma discussão profunda sobre as consequências de um modelo violento de controle que se estrutura a partir de discursos e práticas de liberdade seletiva e controle de grupos de risco.

1. O SISTEMA EUROPEU DE RECONHECIMENTO FACIAL COMO DISPOSITIVO BANÓPTICO E SUAS PRÁTICAS POSITIVISTAS

O sistema cruzado de dados de biometria facial atualmente em operação na Europa busca intercambiar dados armazenados de indivíduos submetidos à extração dos dados biométricos da face em qualquer dos países da União Europeia e, ainda, com os Estados Unidos. O fluxo de dados entre esses países não se limita à esfera criminal, alcançando também sistema de controle migratório.

O marco normativo sobre o intercâmbio de dados biométricos para políticas públicas ligadas ao sistema criminal ou ao sistema migratório é o Tratado de Prum, subscrito em 27 de maio de 2005, na Alemanha, e incorporado ao quadro normativo da União Europeia em 15 de fevereiro de 2007[5].

Referido tratado estabelece normas de cooperação entre os países subscritores em matéria de terrorismo, criminalidade transfronteiriça e imigração[6]. Em seu texto está disciplinado o intercâmbio de informações sobre DNA, impressões digitais, registro de veículos, dados pessoais e não pessoais para a cooperação policial entre as partes contratantes.

[5] PARLAMENTO EUROPEU. Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos. **Documento de trabalho sobre o projeto de decisão do Conselho relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras**. Relator Fausto Correia. 10.abr.2007. Disponível em: https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/660/660824/660824pt.pdf. Acesso em 20.06.2024.

[6] COUNCIL OF THE EUROPEAN UNION. **Prum Convention**. 27 May 2005. Available at: https://data.consilium.europa.eu/doc/document/ST-10900-2005-INIT/en/pdf. Access at 20.06.2024.

Recentemente, o Tratado de Prum sofreu novas alterações com o Regulamento n. 2024/982, do Parlamento Europeu e do Conselho, de 13 de março de 2024. Identificado como "Regulamento Prum II", o documento tratou das condições e procedimentos para a consulta e o intercâmbio automatizados de perfis de DNA, dados datiloscópicos, registro de veículos, imagens faciais e ficheiros policiais[7]. O Regulamento definiu um novo regime para o intercâmbio de informações entre as autoridades responsáveis pela prevenção, detecção ou investigação de infrações penais.

Nesse novo regime, as imagens faciais são objeto de consultas automatizadas para fins de prevenção, detecção ou investigação de uma infração penal desde que a pena aplicada ao delito seja igual ou superior a 01 (um) ano[8]. Para os demais dados biométricos não existe um patamar mínimo de pena, ou seja, qualquer delito é passível de investigação mediante a utilização da metodologia comparada entre esses dados.

A base de dados da Europol, estruturada a partir do Regulamento EU 2016/794, contém vasta gama de dados biométricos enviados por terceiros países, inclusive informações provenientes de zonas de guerra[9]. O Regulamento de Prum II armazena todos esses dados nessa gigantesca base e distribui a todos os países da União Europeia.

Muito embora o Regulamento 2016/794 vede que a Europol compartilhe dados pessoais das suas bases, admite que o órgão receba esses dados de países terceiros, inclusive de organismos privados. Não há uma delimitação sobre as condições materiais para o compartilhamento dos dados de países terceiros, e a avaliação da fiabilidade é feita pelo ente que forneceu a informação (art. 29). Não há no regulamento limites aos tipos de dados que podem ser recebidos pela Europol, como por exemplo no caso de um indivíduo que tenha seus dados compartilhados mesmo sem qualquer condenação contra si.

Se na consulta automatizada houver uma correspondência, cabe ao Estado requerente realizar a confirmação entre as duas imagens faciais. Após a confirmação, deve

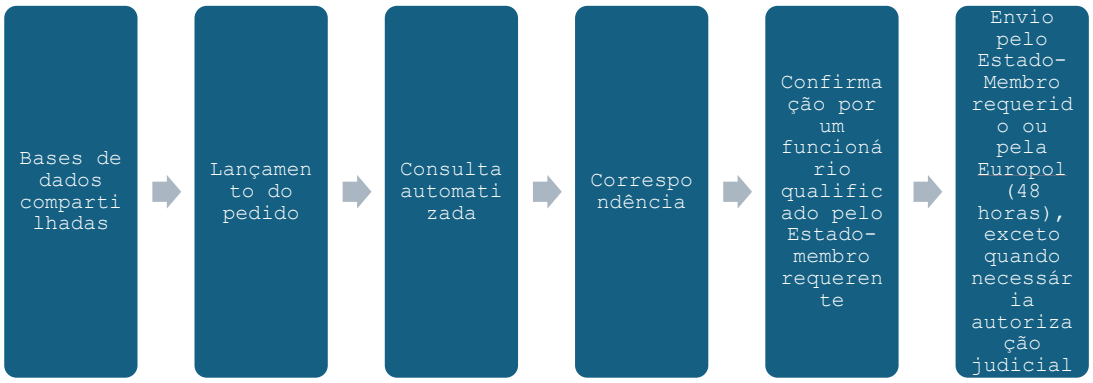
[7] UNIÃO EUROPEIA. Jornal Oficial da União Europeia**. Regulamento (UE) 2024/982 do Parlamento Europeu e do Conselho de 13 de março de 2024 relativo à consulta e ao intercâmbio automatizados de dados para efeitos de cooperação policial**. Disponível em http://data.europa.eu/eli/reg/2024/982/oj. Acesso em 20.06.2024.

[8] UNIÃO EUROPEIA. Jornal Oficial da União Europeia. **Regulamento (UE) 2024/982 do Parlamento Europeu e do Conselho de 13 de março de 2024 relativo à consulta e ao intercâmbio automatizados de dados para efeitos de cooperação policial**. Disponível em http://data.europa.eu/eli/reg/2024/982/oj. Acesso em 20.06.2024.

[9] UNIÃO EUROPEIA. Regulamento EU 2016/796 do Parlamento Europeu e do Conselho de 11 de maio de 2016. **Cria a Agência da União Europeia para a Cooperação Policial (Europol)**. Jornal Oficial da União Europeia. 24.5.2016.

informar ao Estado requerido e assegurar que pelo menos um funcionário qualificado efetue a verificação manual da correspondência.

Em termos esquemático, o procedimento de compartilhamento de imagens faciais pode ser assim sintetizado:



Fonte: elaboração própria

Percebe-se, nesse fluxo, um modelo de policiamento que investe na captura em massa de dados pessoais, sistematização e análise algorítmica das faces como sinais de identificação de risco. Esse fascínio pela categorização e armazenamento de imagens corpos identificados como de risco não é novo; tem bases no positivismo criminológico, na frenologia e na antropometria. Em 1886, Thomas Byrnes, então chefe do Departamento de Polícia de Nova Iorque, criou um álbum intitulado *Professional Criminals of America*, com 204 fotografias frontais de indivíduos identificados como criminosos[10].

Em 1879, Alphonse Bertillon estabelece um sistema de classificação fotográfico que padroniza o registro, o armazenamento e a troca de fichas criminais com a face dos suspeitos[11]. O modelo se concentrava em onze medidas antropométricas como altura, comprimento e largura da cabeça, comprimento dos braços, pés, orelhas e alguns dedos. O modelo foi objeto de efusivos elogios por Cesare Lombroso[12], que fez do estudo do criminoso atávico a base da sua obra "O homem delinquente", representativa do positivismo criminológico.

[10] FINN, Jonathan M. **Capturing the criminal image**: from mug shot to surveillance society. Minneapolis: University of Minnesota Press, 2009, p. 7.
[11] FINN, Jonathan M. **Capturing the criminal image**: from mug shot to surveillance society. Minneapolis: University of Minnesota Press, 2009, p. 23.
[12] FINN, Jonathan M. **Capturing the criminal image**: from mug shot to surveillance society. Minneapolis: University of Minnesota Press, 2009, p. 28

Após a adoção oficial pela Polícia de Paris em 1883, o sistema foi implementado na Europa, Canada e Estados Unidos. O compartilhamento e o armazenamento de dados biométricos tornaram-se uma obsessão das autoridades policiais e a meta principal da Associação Internacional de Chefes de Polícia, de 1902, era o estabelecimento de uma base centralizada de recursos para catalogar e compartilhar informações sobre criminosos[13].

No entanto, quanto às imagens faciais, um dos grandes problemas da época era a imprecisão das fotografias e a baixa capacidade de armazenamento. O processo de coleta dos diversos dados antropométricos também era exaustivo e contraproducente, o que foi decisivo para a gradual prevalência da biometria digital.

Atualmente, porém, com o desenvolvimento de tecnologias de reconhecimento facial que aliam a grande capacidade de armazenamento e processamento de dados com o aprendizado de máquina, o ideário positivista ganha novo fôlego, mas sob nova roupagem.

A gigantesca base de imagens faciais organizada e operacionalizada pelo Regulamento de Prum II evidencia uma política de controle e vigilância de um campo emergente de governamentalidade que, segundo Didier Bigo, é estabelecida a partir de um dispositivo do tipo *banóptico*[14].

Governamentalidade é um conceito foucaultiano que, dentre outros aspectos[15], caracteriza-se pelo conjunto de instituições, procedimentos, táticas, cálculos e análises que têm como alvo a população, cuja base epistêmica é a economia política e cujo instrumento técnico são os dispositivos de segurança[16]. Assim, quando Bigo alude à governamentalidade do mal-estar[17] desloca o eixo de análise para o tema central do policiamento global transnacional: governar condutas a partir do binômio ameaça e angústia.

---

[13] FINN, Jonathan M. **Capturing the criminal image**: from mug shot to surveillance society. Minneapolis: University of Minnesota Press, 2009, p. 37.
[14] BIGO, Didier. (In)segurança globalizada: o campo e o ban-opticon. In: **A cidade como máquina biopolítica**. Org.: Augusto Jobim do Amara *et al*. Tirant lo blanch, Valencia, 2022, p. 116-154.
[15] Governamentalidade, em Foucault, não se esgota nesse aspecto. Engloba também uma linha de força, uma tendência a um tipo de poder de governo sobre todos os demais a partir desses aparatos específicos e de uma série de saberes. Há também um sentido de governamentalidade como resultado do processo de transformação do Estado de Justiça da Idade Média para o Estado Administrativo e, finalmente, para a governamentalização deste último. FOUCAULT, Michel. **Segurança, território, população**: curso dado no Collège de France (1977-1978). Trad.: Eduardo Brandão. São Paulo: Martins Fontes, 2008, p. 143-144.
[16] FOUCAULT, Michel. **Segurança, território, população**: curso dado no Collège de France (1977-1978). Trad.: Eduardo Brandão. São Paulo: Martins Fontes, 2008, p. 143.
[17] O termo usado pelo autor no texto original é *governmentality of unease*. Apesar de algumas obras optarem pela tradução "governamentalidade do desconforto", buscamos uma expressão que alcançasse de modo mais amplo o sentido proposto por Bigo sobre os fundamentos, as características

Essa governamentalidade está no cerne do sistema europeu e se caracteriza a partir de três critérios: práticas de excepcionalismo, atos de perfilamento e contenção de estrangeiros, e um imperativo de mobilidade[18]. O discurso que a sustenta está fundado em estatísticas, tecnologias de biometria, classificação e priorização de ameaças.

Os profissionais da gestão do mal-estar produzem o poder-conhecimento sobre o dualismo segurança e insegurança a partir de um regime transnacional de verdade que sucede as clássicas razões de Estado e é acentuado na arena europeia[19]. É nesse regime que o discurso mescla guerra e militarização, terrorismo e ameaças internas, política criminal e migratória a partir de burocracias e agências que se apropriam de uma lógica de securitarização transfronteiriça.

Esse programa de (in)segurança performa como uma estratégia programática de escalada generalizada de vigilância tão globalizada quanto individualizada o quanto possível. É nesse ponto que Bigo se utiliza do conceito foucaultiano de dispositivo para reinterpretá-lo no panorama atual como um *Ban-opticon*.

Em *Vigiar e Punir,* Foucault analisa que o poder supõe um dispositivo que congregue técnicas que maximizem seus efeitos[20]. Uma arquitetura ou infraestrutura que automatiza e desindividualiza o poder: "há uma maquinaria que assegura a dissimetria, o desequilíbrio, a diferença. Pouco importa, consequentemente, quem exerce o poder"[21].

Nesse contexto, o panóptico, modelo de vigilância total atribuído a Jeremy Bentham em que a pessoa vigiada constantemente não sabe quando e quem a visualiza, produz uma sujeição automática ao poder. O panóptico estabelece uma vigilância pautada no princípio de que o poder deve ser inverificável: o vigiado é o objeto da informação, jamais sujeito da

---

e os efeitos desse modelo de governamentalidade que se estrutura a partir de práticas de exceção e banimento. *Unease,* nesse contexto, poderia ser mais associado ao mal-estar, à profunda inquietação, como uma dimensão mais ampla do impacto de atos de perfilamento e contenção de estrangeiros (extranĕus) como formas de biopolíticas. BIGO, Didier. Globalized (in)security: The field and the ban-opticon. In: **Terror, Insecurity and Liberty**: Illiberal Practices of Liberal Regimes After 9/11. Ed.: Bigo D. and Tsoukala A. New York: Routledge, p. 10-48.

[18] BIGO, Didier. (In)segurança globalizada: o campo e o ban-opticon. In: **A cidade como máquina biopolítica**. Org.: Augusto Jobim do Amara *et al*. Tirant lo blanch, Valencia, 2022, p. 116-154.

[19] BIGO, Didier. (In)segurança globalizada: o campo e o ban-opticon. In: **A cidade como máquina biopolítica**. Org.: Augusto Jobim do Amara *et al*. Tirant lo blanch, Valencia, 2022, p. 116-154.

[20] FOUCAULT, Michel. **Vigiar e Punir**: nascimento da prisão. Trad.: Raquel Ramalhete, 20ª Ed., Petrópolis: Vozes, 1987, p. 146.

[21] FOUCAULT, Michel. **Vigiar e Punir**: nascimento da prisão. Trad.: Raquel Ramalhete, 20ª Ed., Petrópolis: Vozes, 1987, p. 167.

comunicação; não deve nunca saber se está sendo observado, mas ter a certeza de sempre poder sê-lo[22].

A partir dessa relação que se estabelece entre poder e técnica, Bigo avalia como a sociedade atual convive com uma rede transfronteiriça de práticas heterogêneas e transversais que produzem o discurso e a (in)segurança. O autor se recusa a creditar tal cenário a um tipo de dominação imperial centralizada, apontando um campo fragmentado, heterogêneo e descentralizado nos processos políticos de conflito e convergência entre grandes corporações e agências burocráticas[23].

Tendo como marco referencial o 11 de setembro de 2001, Bigo analisa como se inaugura a partir dali um modelo de (in)segurança globalizada que mescla dois campos até então distintos: o universo da guerra, defesa nacional, ordem internacional e estratégia e o universo da segurança interna e da ordem pública policial[24]. O controle e a resposta ao delito assumem uma interface militarizada; são mediados por agências burocráticas e gestores do mal-estar provocado pela frequente ameaça do estrangeiro - na concepção etimológica do termo como *extranĕus* - e, por isso, um risco à segurança nacional.

O gerenciamento dessa engrenagem é cercado por práticas heterogêneas e transnacionais, coordenadas por agências a nível transnacional: autoridades alfandegárias, controles migratórios, políticas criminais, agências anti-terroristas, agentes infiltrados, tecnologias de controle e gestão à distância. Esse diagrama não se apresenta como um clássico panóptico a nível global, mas sim como um *Ban-opticon,* uma associação entre o termo "ban" de Jean Luc Nancy, refigurado por Agamben, com o *opticon* utilizado por Foucault:

> Essa formulação do *Ban-opticon* nos permite entender como uma rede de práticas heterogêneas e transversais funciona e faz sentido enquanto forma de (in)segurança ao nível transnacional. Permite-nos analisar a coleção de corpos heterogêneos de discursos (sobre ameaças, imigração, inimigo interno, quinta coluna imigrante, muçulmanos radicais versus bons muçulmanos, exclusão versus integração etc) de instituições (agências públicas, governos, organizações internacionais, ONGs, etc), de estruturas arquitetônicas (centros de detenção, zonas de espera e as pistas de trânsito em aeroportos da área de Schengen, redes integradas de videocâmera em

[22] FOUCAULT, Michel. **Vigiar e Punir**: nascimento da prisão. Trad.: Raquel Ramalhete, 20ª Ed., Petrópolis: Vozes, 1987, p. 167.
[23] BIGO, Didier. (In)segurança globalizada: o campo e o ban-opticon. In: **A cidade como máquina biopolítica**. Org.: Augusto Jobim do Amara *et al*. Tirant lo blanch, Valencia, 2022, p. 116-154.
[24] BIGO, Didier. Globalized (in)security: The field and the ban-opticon. In: **Terror, Insecurity and Liberty**: Illiberal Practices of Liberal Regimes After 9/11. Ed.: Bigo D. and Tsoukala A. New York: Routledge, p. 10-48.

> algumas cidades, redes eletrônicas munidas de instalações de segurança e vídeo-vigilância), de leis (...) e de medidas administrativas (...)[25].

O radical *ban,* de origem germânica, insere uma ideia de rejeição, exclusão, restrição, proscrição. Ban-dido e ban-ido são palavras utilizadas, respectivamente, para provocar as ideias de contrário à ordem e excluído dessa ordem. O banido não está apenas fora da lei, mas abandonado por ela, ou seja, "exposto e colocado em risco no limiar em que vida e direito, externo e interno, se confundem"[26].

No Banóptico a vigilância de todos não é um objetivo central, mas sim de grupos identificados como de risco no campo da mobilidade transnacional. Nesse dispositivo são permanentes os excepcionalismos do poder, manifestados nas leis de emergências, e o perfilamento de grupos indesejáveis a partir de práticas que sobrebujam a nação-Estado.

O discurso não é mais sobre a reforma do indivíduo, mas sobre o controle de grupos específicos que são vistos como uma ameaça ao solo europeu. Para lidar com essas classificações *ban,* as estruturas arquitetônicas não dependem do confinamento; são aplicadas no intenso fluxo de circulação para incidência sobre indivíduos específicos; as leis e medidas administrativas são adaptadas a conceitos genéricos que substituem a ideia de dano pela ideia de risco, associada a uma determinada imagem, aquela capturada pela tecnologia algorítmica de reconhecimento facial.

Estabelece-se um modelo de vigilância que é distribuída e imanente: não está em um ponto fixo tampouco restrita a um espaço de confinamento[27]. Investe-se no controle da circulação que é essencial ao produto *liberdade* que o neoliberalismo anuncia. O fluxo de pessoas e mercadorias – e, por consequência dados – é vital para a validação do produto. A gestão desse fluxo dependerá do cálculo de risco sobre grupos específicos[28].

Os dispositivos banópticos garantem a aparente circulação de todos a partir da exclusão de alguns, associados a partir dos perfis de risco, embasados na suposta neutralidade tecnológica. Legitimam a continuidade repressiva do modelo penal, com sua

[25] BIGO, Didier. (In)segurança globalizada: o campo e o ban-opticon. In: **A cidade como máquina biopolítica**. Org.: Augusto Jobim do Amara *et al*. Tirant lo blanch, Valencia, 2022, p. 116-154, p. 144.
[26] AGAMBEN, Giorgio. **Homo Sacer**: o poder soberano e a vida nua. Trad.: Henrique Burigo. Belo Horizonte: UFMG, 2002, p. 36.
[27] RODRÍGUEZ, Pablo Manolo. **Las Palabras en Las Cosas**: saber, poder y subjectivación entre algoritmos y biomoléculas. Buenos Aires: Cactus, 2009, p. 362.
[28] AMARAL. Augusto Jobim do; DIAS, Felipe da Veiga. **Tecnopolítica criminal**. 1ª Ed., São Paulo: Tirant lo Blanc, 2024, p. 39.

clientela habitual e recorte racial, ao mesmo tempo que formam outros grupos identificados como de risco para o manejo de táticas de vigilância e controle da circulação[29].

Desse modo, o dispositivo já não é um panóptico benthamiano, mas um banóptico que não depende da imobilização dos corpos nos espaços de confinamento, mas sim da produção virtual ou algorítmica de perfis que sinalizam a diferença[30]. O sistema europeu de identificação pessoal investe nessa marca da diferença, nessa tatuagem imagética produzida a partir das lentes focais sobre os corpos em movimento, garantindo uma nova roupagem robótica e digital para a velha antropometria criminal[31].

Ao contrário do que se possa acreditar em primeiro plano, como visto, essas discriminações sistêmicas, ligadas ao processo algorítmico que subjaz as tecnologias de reconhecimento facial, não são uma distorção da arte de governo (neo)liberal, mas a sua própria essência, com raízes no modelo policial que, desde o positivismo criminológico, buscou categorizar os corpos com bases em evolucionismos de natureza eugênica.

Ao invés de uma tecnologia disruptiva, o banco de imagens faciais dobra a aposta no sonho de antropometria criminal da Associação Internacional de Chefes de Polícia, de 1902, agora a partir de modelos algorítmicos e tecnologias que se anunciam inovadoras, mas estão estruturadas em bases ideológicas do início do século XX.

2. A DISCRIMINAÇÃO ALGORÍTIMICA E A SUA FUNCIONALIDADE AO DISPOSITIVO BANÓPTICO

Como diagnostica Foucault em *Segurança, Território e População*, no próprio interior do saber-poder existe uma divisão instrumental entre o nível pertinente da população e o nível não-pertinente[32]. O liberalismo faz a gestão econômica desses níveis tendo como objetivo final a população, ainda que para isso precise se valer de um grupo de indivíduos como instrumento ou condição para algo no nível da população.

[29] AMARAL. Augusto Jobim do; DIAS, Felipe da Veiga. **Tecnopolítica criminal**. 1ª Ed., São Paulo: Tirant lo Blanc, 2024, p. 39.
[30] BIGO, Didier. (In)segurança globalizada: o campo e o ban-opticon. In: **A cidade como máquina biopolítica**. Org.: Augusto Jobim do Amara *et al*. Tirant lo blanch, Valencia, 2022, p. 116-154.
[31] BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre, Sulina, 2013, p. 33.
[32] FOUCAULT, Michel. **Segurança, território, população**: curso dado no Collège de France (1977-1978). Trad.: Eduardo Brandão. São Paulo: Martins Fontes, 2008, p. 56.

No caso das tecnologias de reconhecimento facial, essa divisão instrumental entre o nível pertinente e não-pertinente fica bastante evidenciada se considerarmos o caráter discriminatório que contorna a lógica algorítmica.

Tarcizio Silva, na obra *Racismo algorítmico,* reporta estudos que indicam cerca de 63% de indivíduos abordados a partir de resultados equivocados (falsos positivos) de reconhecimento facial[33]. As taxas de falsos positivos, aponta ele, são de dez a cem vezes maiores para fotos de pessoas negras, asiáticas ou de povos originários.

Estudos conduzidos por Reva Schwartz apontam que os dados de treinamento extraídos de fontes da internet geralmente apresentam preconceitos de gênero, raciais, culturais e socioeconômicos[34]. A pesquisa alerta que muitos sistemas de inteligência artificial buscam produzir inferências sobre indivíduos a partir de características faciais sem base científica.

Outro estudo conduzido pelo *National Institute of Standards and Technology* (NIST) avaliou softwares de algoritmos de reconhecimento facial de 99 desenvolvedores de 189 organizações, incluindo Toshiba, Intel e Microsoft. A pesquisa utilizou 4 coleções de fotografias contendo mais de 18 milhões de imagens de aproximadamente 8,5 milhões de pessoas, proveniente do Departamento de Estado, do Departamento de Segurança Nacional e do FBI.

A análise considerou tanto a tecnologia de reconhecimento facial um-para-um, utilizada em *smartphones,* quanto a tecnologia um-para-muitos, utilizada em grandes eventos. A avaliação dos algoritmos considerou as ocorrências de falsos positivos e falsos negativos[35].

Os resultados apontaram que a maioria dos algoritmos de reconhecimento facial apresentam diferenças demográficas, isto é, a capacidade de comparação dos sistemas varia de um grupo – sexo, etnia, idade – para outro[36]. Na tecnologia de reconhecimento facial um-

[33] SILVA, Tarcízio. **Racismo algorítmico**: inteligência artificial e discriminação nas redes digitais. São Paulo: Sesc, 2022, p. 113.
[34] SCHWARTZ, Reva *et al*. **Towards a Standard for Identifying and Managing Bias in Artificial Intelligence. National Institute of Standards and Technology**. U.S. Department of Commerce. Available at https://doi.org/10.6028/NIST.SP.1270. Access 13.jun.2024.
[35] O falso positivo é verificado quando o sistema equivocadamente considera fotos de dois diferentes indivíduos como pertencentes a mesma pessoa; o falso negativo ocorre quando o sistema é incapaz de reconhecer fotos que estão na base de dados e pertencem a mesma pessoa.
[36] GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test – Part 3**: Demographic Effects. National Institute of Standards and Technology. U.S. Departmente of Commerce. Available at https://doi.org/10.6028/NIST.IR.8280. Access 13.jun.2024.

para-um os pesquisadores encontraram índices de falsos positivos de 10 a 100 vezes maiores para pessoas asiáticas ou negras em comparação com pessoas brancas. Na tecnologia de comparação um-para-muitos, os números apontam para altas taxas de falsos positivos entre mulheres negras.

Patrick Grother, um dos responsáveis pela pesquisa, observou que o falso negativo no sistema de um-para-um pode resultar em algum dissabor, como a impossibilidade de desbloquear um celular. No entanto, no caso de falsos positivos do sistema um-para-muitos o dano é maior, pois inclui a pessoa em lista de suspeitos[37].

No caso Bridges, por exemplo, a análise da tecnologia de reconhecimento facial empregada na Final da Liga dos Campeões da UEFA, em junho de 2018, apontou para 290 alertas gerados, dos quais 208 eram falsos positivos[38].

Essas tecnologias de reconhecimento se utilizam de processos algorítmicos para definir a correspondência (*match*) entre a imagem capturada e a imagem armazenada. Desse modo, prevalece no sistema um juízo de probabilidade que é feito a partir dos modelos algorítmicos aplicados[39].

Como anota Sarah Brayne ao tratar das tecnologias que se utilizam de algoritmos, essas não transcendem o meio social onde são desenvolvidas, mas antes são moldadas a partir de contextos institucionais e organizacionais que decidem quais dados coletar e analisar e para quais finalidades serão direcionados[40].

Augusto Jobim e Ana Clara Elesbão analisam como os procedimentos algorítmicos operam segundo uma lógica estritamente comercial que (re)produz resultados manifestamente racistas e sexistas[41]. O artigo dialoga com o trabalho de Safiya Noble que,

[37] NATIONAL INSTITUTE OF STANDARDS AND TECNHOLOGY. **NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software**. Dec.19.2019. Available at: https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. Access 13.jun.2024.

[38] R(Bridges) vs. South Wales Police. **Case No: C1/2019/2670**. Court of Appel (Civil Division). Royal Courts of Justice. 11.aug.2020. Available at: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf. Access 25.05.2024.

[39] SELWYN, Neil; ANDREJEVIC, Mark; O'NEILL, Chris; GU, Xin; SMITH, Gavin. Facial Recognition Technology: Key Issues and Emerging Concerns. In: **The Cambridge Handbook of Facial Recognition in the Modern State**. Org.: Rita Matulionyte and Monika Zalnieriute. Cambridge: Cambridge University Press, 2024.

[40] BRAYNE, Sarah. **Predict and Surveil**: data, discretion, and the future of policing. Oxford: Oxford University Press, 2021.

[41] AMARAL, Augusto Jobim do; ELESBÃO, Ana Clara. Racismo e Sexismo algorítmicos: um estudo de caso sobre o mecanismo comercial de busca do google. In: **Revista Eletrônica do Curso de Direito da UFSM**, v. 17, n.1/2022, p. 1-33.

a partir da teoria crítica da raça e da análise crítica do discurso, investigou os processos simbióticos de reificação da identidade racial negra de acordo com categorias discursivas moldadas para associar mulheres negras à pornografia.

Noble demonstra que, em 2011, o fato de o termo *Black Girls* (meninas negras) lançado na plataforma *Google* ter apresentado entre os primeiros resultados indexados sites de conteúdo pornográfico não foi uma aleatoriedade. Os resultados *(outputs*) da lógica algorítmica da plataforma, alegadamente neutra, reproduziram processos históricos racistas e sexistas, reforçando a prevalência desses mecanismos de silenciamento social e político:

> (...) é importante localizar as atuais dinâmicas de produção de sentido *online* no contexto histórico e social que reflete a hipersexualização das mulheres negras, servindo inclusive como tentativa de silenciamento social e político. No entanto, o sistema algorítmico responsável por gerar a lista de resultados não leva em consideração o significado mais amplo vinculado a tais associações[42].

Desse modo, não se pode perder de vista que a operação da coleta e cruzamento de dados no Regulamento de Prum II será conduzida pela lógica algorítmica, acarretando graves riscos de reprodução de discursos e práticas discriminatórias.

Curioso notar que o sistema adotado pelo Regulamento colide com o próprio entendimento da Corte Europeia de Direitos Humanos. No caso *Glukhin*, a Corte Europeia de Direitos Humanos enfrentou a questão da vigilância em massa e das violações aos direitos à privacidade e à livre expressão do pensamento e reunião.

Em maio de 2017 o prefeito de Moscou anunciou que um circuito fechado de câmeras foi instalado na cidade e que no ano seguinte tal circuito seria equipado com tecnologia de reconhecimento facial. Em 2018 as câmeras foram instaladas no metrô da cidade e em 2019 iniciaram os testes para um sistema de reconhecimento facial. Em 2022 o sistema de CCTV contava com 220.000 câmeras em operação com tecnologia de reconhecimento facial em tempo real[43].

Após a prisão de um ativista, Kostantin Kotov, Nikolay Glukhin iniciou protestos no metrô de Moscou. Com o apoio da tecnologia de reconhecimento facial, a polícia russa o

[42] AMARAL, Augusto Jobim do; ELESBÃO, Ana Clara. Racismo e Sexismo algorítmicos: um estudo de caso sobre o mecanismo comercial de busca do google. In: **Revista Eletrônica do Curso de Direito da UFSM**, v. 17, n.1/2022, p. 1-33.

[43] EUROPEAN COURT OF HUMAN RIGHTS (ECTHR). **Glukhin vs Russia**. Case number 11519/20. 04.jul.2023. Available at https://globalfreedomofexpression.columbia.edu/cases/glukhin-v-russia/. Access 25.05.2024.

acusou de quebrar as regras de conduta para eventos públicos. Ele foi julgado e condenado pelos tribunais russos, apresentando recurso à Corte Europeia de Direitos Humanos alegando a violação dos direitos à privacidade e à liberdade de expressão.

A Corte Europeia acolheu o recurso de Glukhin, asseverando que o direito à privacidade inclui a vida social privada que a coleta de dados individuais constitui uma interferência nesse direito. Ponderou que a imagem de uma pessoa é um dos principais atributos de sua personalidade e revela características únicas e distintivas do sujeito. Desse modo, todo ser humano titulariza o direito de opor-se à coleta, gravação, conservação e reprodução de sua imagem por autoridades ou indivíduos em particular, inclusive em espaços públicos[44].

Naquela ocasião o tribunal também recordou que o uso de tecnologia de reconhecimento facial altamente intrusiva para identificar e prender manifestantes pacífico pode ter um efeito devastador com relação aos direitos à liberdade de expressão e de reunião[45]. O Estado russo foi condenado a pagar uma indenização por danos morais cometidos contra o senhor Glukhin.

CONCLUSÃO

O artigo analisou o sistema europeu de reconhecimento facial, estruturado a partir do Regulamento de Prum II, como um dispositivo banóptico próprio da governamentalidade do mal-estar. Observou-se uma linha de continuidade com a antropometria criminal e o positivismo criminológico, discursos que produziram discriminação a partir da suposta neutralidade do saber científico.

Essa mesma neutralidade agora é levantada para defender o emprego das tecnologias algorítmicas de reconhecimento facial para fins de policiamento e controle migratório. Nesse contexto, o regime europeu de captura e análise de imagens faciais se apresenta como um dispositivo banóptico de instrumentalização de um tipo de governamentalidade que estimula a circulação ao mesmo que define zonas de exclusão.

[44] EUROPEAN COURT OF HUMAN RIGHTS (ECTHR). **Glukhin vs Russia**. Case number 11519/20. 04.jul.2023. Available at https://globalfreedomofexpression.columbia.edu/cases/glukhin-v-russia/. Access 25.05.2024.
[45] EUROPEAN COURT OF HUMAN RIGHTS (ECTHR). **Glukhin vs Russia**. Case number 11519/20. 04.jul.2023. Available at https://globalfreedomofexpression.columbia.edu/cases/glukhin-v-russia/. Access 25.05.2024.

O artigo aplicou conceitos foucaultianos para avaliar uma linha de continuidade entre discursos e práticas do neoliberalismo na gestão decomponível dos indivíduos em dados. O fascínio pelo registro e estoque dos corpos suspeitos não é novo; acompanha a história da antropometria e da criminologia positivista.

Essa ideologia assume novas formas com o desenvolvimento de novas tecnologias com capacidade inédita de coleta, processamento e armazenamento. O dispositivo banóptico está no cerne desse tipo de policiamento global, que investe em práticas de excepcionalismo e na contenção daqueles grupos identificados como perigosos.

Nesse contexto, a liberdade é produzida para aquele nível pertinente da população, ainda que por meio de dispositivos securitários que reproduzam discriminações sistêmicas contra o nível que, utilizando a terminologia foucaultiana, é visto como não-pertinente.

Conforme literatura especializada na matéria, as tecnologias de reconhecimento facial ainda apresentam pontos sensíveis de discriminação sistêmica que reproduzem modelos racistas, sexistas e xenofóbicos. O maior espanto é que esses modelos não são distorções do sistema, mas a própria lógica operativa da governamentalidade e dos dispositivos securitários que a operacionalizam.

O argumento securitário já foi utilizado por regimes totalitários para valer-se de modelos de gestão de população baseados em controle e punição. Assim, ao tempo em que a tecnologia de reconhecimento facial promete ser uma panaceia para a ideologia de defesa social e segurança nacional, existem riscos evidentes ao legado de direitos fundamentais e de proteção da pessoa humana decorrente desse uso amplo e intensivo.

REFERÊNCIAS

AGAMBEN, Giorgio. **Homo Sacer**: o poder soberano e a vida nua. Trad.: Henrique Burigo. Belo Horizonte: UFMG, 2002.

AMARAL, Augusto Jobim do. Biopolítica e Biocapitalismo: implicações da violência do controle. In: **Veritas**. Porto Alegre, v. 63, n. 2, maio-ago, 2018, p. 515-543.

AMARAL, Augusto Jobim do; ELESBÃO, Ana Clara. Racismo e Sexismo algorítmicos: um estudo de caso sobre o mecanismo comercial de busca do google. In: **Revista Eletrônica do Curso de Direito da UFSM**, v. 17, n.1/2022, p. 1-33.

AMARAL. Augusto Jobim do; DIAS, Felipe da Veiga. **Tecnopolítica criminal**. 1ª Ed., São Paulo: Tirant lo Blanc, 2024.

BIGO, Didier. (In)segurança globalizada: o campo e o ban-opticon. In: **A cidade como máquina biopolítica**. Org.: Augusto Jobim do Amaral *et al*. Tirant lo blanch, Valencia, 2022, p. 116-154.

BIGO, Didier. Globalized (in)security: The field and the ban-opticon. In: **Terror, Insecurity and Liberty**: Illiberal Practices of Liberal Regimes After 9/11. Ed.: Bigo D. and Tsoukala A. New York: Routledge, p. 10-48.

BISCHOFF, Paul. **Facial recognition technology (FRT)**: 100 countries analyzed. Comparitech, 24.Jan.2022. Available at: https://www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/#:~:text=Five%20countries. Access 25.02.2024.

BRAYNE, Sarah. **Predict and Surveil**: data, discretion, and the future of policing. Oxford: Oxford University Press, 2021.

BRUNO, Fernanda. **Máquinas de ver, modos de ser**: vigilância, tecnologia e subjetividade. Porto Alegre, Sulina, 2013.

COUNCIL OF THE EUROPEAN UNION. **Prum Convention**. 27 May 2005. Available at: https://data.consilium.europa.eu/doc/document/ST-10900-2005-INIT/en/pdf.

ENGLAND. **R(Bridges) vs. South Wales Police**. Case No: C1/2019/2670. Court of Appel (Civil Division). Royal Courts of Justice. 11.aug.2020. Available at: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf. Access 25.05.2024.

EUROPEAN COURT OF HUMAN RIGHTS. **Glukhin vs. Russia**. European Court of Human Rights (ECtHR). Case number 11519/20. 04.jul.2023. Available at https://globalfreedomofexpression.columbia.edu/cases/glukhin-v-russia/. Access 25.05.2024.

EUROPEAN PARLIAMENT. **Artificial Intelligence Act**: MEPs adopt landmark law. Press Releases. Available at https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law. Access 26.05.2024.

EUROPEAN UNION. EUROPEAN COMISSION. **The Commission welcomes the political agreement on automated data exchange for police cooperative**. Press release. 20.nov.23. Available at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5870. Access at 17.06.2024.

FINN, Jonathan M. **Capturing the criminal image**: from mug shot to surveillance society. Minneapolis: University of Minnesota Press, 2009.

FOUCAULT, Michel. **Vigiar e Punir**: nascimento da prisão. Trad.: Raquel Ramalhete, 20ª Ed., Petrópolis: Vozes, 1987.

FOUCAULT, Michel. **Segurança, território, população**: curso dado no Collège de France (1977-1978). Trad.: Eduardo Brandão. São Paulo: Martins Fontes, 2008.

GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. **Face Recognition Vendor Test - Part 3**: Demographic Effects. National Institute of Standards and Technology. U.S. Departmente of Commerce. Available at https://doi.org/10.6028/NIST.IR.8280. Access 13.jun.2024.

MATULIONYTE, Rita; ZALNIERIUTE, Monika. **The Cambridge Handbook of Facial Recognition in the Modern State**. Cambridge University Press. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECNHOLOGY. **NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software**. Dec.19.2019. Available at: https://www.nist.gov/news-

events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software. Access 13.jun.2024.

O'NEIL, Cathy. **Algoritmos de destruição em massa**: como o big data aumenta a desigualdade e ameaça a democracia. Trad.: Rafael Abraham, 1ª Ed., Santo André, SP: Editora Rua do Sabão, 2020.

PARLAMENTO EUROPEU. Comissão das Liberdades Cívicas, da Justiça e dos Assuntos Internos. **Documento de trabalho sobre o projeto de decisão do Conselho relativa ao aprofundamento da cooperação transfronteiras, em particular no domínio da luta contra o terrorismo e da criminalidade transfronteiras**. Relator Fausto Correia. 10.abr.2007. Disponível em: https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/660/660824/660824pt.pdf.

RODRÍGUEZ, Pablo Manolo. **Las Palabras en Las Cosas**: saber, poder y subjectivación entre algoritmos y biomoléculas. Buenos Aires: Cactus, 2009.

R(Bridges) vs. South Wales Police. **Case No: C1/2019/2670**. Court of Appel (Civil Division). Royal Courts of Justice. 11.aug.2020. Available at: https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf. Access 25.05.2024.

SCHWARTZ, Reva *et al*. **Towards a Standard for Identifying and Managing Bias in Artificial Intelligence**. National Institute of Standards and Technology. U.S. Department of Commerce. Available at https://doi.org/10.6028/NIST.SP.1270. Access 13.jun.2024.

SELWYN, Neil; ANDREJEVIC, Mark; O'NEILL, Chris; GU, Xin; SMITH, Gavin. Facial Recognition Technology: Key Issues and Emerging Concerns. In: **The Cambridge Handbook of Facial Recognition in the Modern State**. Org.: Rita Matulionyte and Monika Zalnieriute. Cambridge: Cambridge University Press, 2024.

SILVA, Tarcízio. **Racismo algorítmico**: inteligência artificial e discriminação nas redes digitais. São Paulo: Sesc, 2022.

THE ECONOMIST. **China: facial recognition and state control**. Available at: https://www.youtube.com/watch?v=lH2gMNrUuEY. Acesso em 20.06.2024.

UNIÃO EUROPEIA. Jornal Oficial da União Europeia. **Regulamento (UE) 2024/982 do Parlamento Europeu e do Conselho de 13 de março de 2024 relativo à consulta e ao intercâmbio automatizados de dados para efeitos de cooperação policial.** Disponível em http://data.europa.eu/eli/reg/2024/982/oj. Acesso em 20.06.2024.

UNIÃO EUROPEIA. Regulamento EU 2016/796 do Parlamento Europeu e do Conselho de 11 de maio de 2016. **Cria a Agência da União Europeia para a Cooperação Policial (Europol)**. Jornal Oficial da União Europeia. 24.5.2016.

UNIÃO EUROPEIA. **Regulamento EU 2016/796 do Parlamento Europeu e do Conselho de 11 de maio de 2016**. Cria a Agência da União Europeia para a Cooperação Policial (Europol). Jornal Oficial da União Europeia. 24.5.2016.